

THE CYPHERNOMICON

1. Introduction

1.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

1.2. Foreword

- The Cypherpunks have existed since September, 1992. In that time, a vast amount has been written on cryptography, key escrow, Clipper, the Net, the Information Superhighway, cyber terrorists, and crypto anarchy. We have found ourselves (or placed ourselves) at the center of the storm.
- This FAQ may help to fill in some gaps about what we're about, what motivates us, and where we're going. And maybe some useful knowledge on crypto, remailers, anonymity, digital cash, and other interesting things.
- + The Basic Issues
 - + Great Divide: privacy vs. compliance with laws
 - + free speech and privacy, even if means some criminals cannot be caught (a stand the U.S. Constitution was strongly in favor of, at one time)
 - a man's home is his castle...the essence of the Magna Carta systems...rights of the individual to be secure from random searches
 - + or invasive tactics to catch criminals, regulate behavior, and control the population
 - the legitimate needs to enforce laws, to respond to situations
 - + this parallels the issue of self-protection vs. protection by law and police
 - as seen in the gun debate
 - crypto = guns in the sense of being an individual's preemptive protection
 - past the point of no return
 - Strong crypto as building material for a new age
- + Transnationalism and Increased Degrees of Freedom
 - governments can't hope to control movements and communications of citizens; borders are transparent
- + Not all list members share all views
 - This is not "the Official Cypherpunks FAQ." No such thing can exist. This is the FAQ I wanted written. Views expressed are my own, with as much input from others, as much consensus, as I can manage. If you want a radically different FAQ, write it yourself. If you don't like this FAQ, don't read it. And tell your friends not to read it. But don't bog down my mailbox, or the 500 others on the list, with messages about how you would have worded Section 12.4.7.2 slightly differently, or how Section 6.9.12 does not fully reflect your views. For obvious reasons.
 - All FAQs are the products of a primary author, sometimes of a committee. For this FAQ, I am the sole author. At least of the version you are reading now. Future versions may

- have more input from others, though this makes me nervous (I favor new authors writing their own stuff, or using hypertext links, rather than taking my basic writing and attaching their name to it--it is true that I include the quotes of many folks here, but I do so by explicitly quoting them in the chunk they wrote....it will be tough for later authors to clearly mark what Tim May wrote without excessively cluttering the text. The revisionist's dilemma.
- The list has a lot of radical libertarians, some anarcho-capitalists, and even a few socialists
 - Mostly computer-related folks, as might be expected. (There are some political scientists, classical scholars, etc. Even a few current or ex-lawyers.)
- + Do I Speak for Others?
- As I said, no. But sometimes I make claims about what "most" list members believe, what "many" believe, or what "some" believe.
 - "Most" is my best judgment of what the majority believe, at least the vocal majority in Cypherpunks discussions (at the physical meetings, parties, etc.) and on the List. "Many" means fewer, and "some" fewer still. "A few" will mean a distinct minority. Note that this is from the last 18 months of activity (so don't send in clarifications now to try to "sway the vote").
 - In particular, some members may be quite uncomfortable being described as anarchists, crypto anarchists, money launderers, etc.
- + My comments won't please everyone
- on nearly every point ever presented, some have disagreed
 - feuds, battles, flames, idee fixes
 - on issues ranging from gun control to Dolphin Encrypt to various pet theories held dearly
 - Someone once made a mundane joke about pseudonyms being like multiple personality disorder--and a flame came back saying: "That's not funny. I am MPD and my SO is MPD. Please stop immediately!"
 - can't be helped....can't present all sides to all arguments
- + Focus of this FAQ is U.S.-centric, for various reasons
- most on list are in U.S., and I am in U.S.
 - NSA and crypto community is largely centered in the U.S., with some strong European activities
 - U.S. law is likely to influence overseas law
- + We are at a fork in the road, a Great Divide
- Surveillance vs. Freedom
 - nothing in the middle...either strong crypto and privacy is strongly limited, or the things I describe here will be done by some people....hence the "tipping factor" applies (point of no return, horses out of the barn)
- + I make no claim to speaking "for the group." If you're offended, write your own FAQ. My focus on things loosely called "crypto anarchy" is just that: my focus. This focus naturally percolates over into something like this FAQ, just as someone primarily interested in the mechanics of PGP would devote more space to PGP issues than I have.
- Gary Jeffers, for example, devotes most of his "CEB" to issues surrounding PGP.

- + Will leave out some of the highly detailed items...
 - Clipper, LEAF, escrow, Denning, etc.
 - a myriad of encryption programs, bulk ciphers, variants on PGP, etc. Some of these I've listed...others I've had to throw my hands over and just ignore. (Keeping track of zillions of versions for dozens of platforms...)
 - easy to get lost in the details, buried in the bullshit

1.3. Motivations

1.3.1. With so much material available, why another FAQ?

1.3.2. No convenient access to archives of the list....and who could read 50 MB of stuff anyway?

1.3.3. Why not Web? (Mosaic, Http, URL, etc.)

- Why not a navigable Web document?
- This is becoming trendy. Lots of URLs are included here, in fact. But making all documents into Web documents has downsides.

+ Reasons why not:

- No easy access for me.
- Many others also lack access. Text still rules.
- Not at all clear that a collection of hundreds of fragments is useful
- I like the structured editors available on my Mac (specifically, MORE, an outline editor)

-

1.3.4. What the Essential Points Are

- It's easy to lose track of what the core issues are, what the really important points are. In a FAQ like this, a vast amount of "cruft" is presented, that is, a vast amount of miscellaneous, tangential, and epiphenomenal material. Names of PGP versions, variants on steganography, and other such stuff, all of which will change over the next few months and years.

+ And yet that's partly what a FAQ is for. The key is just not to lose track of the key ideas. I've mentioned what I think are the important ideas many times. To wit:

- that many approaches to crypto exist
- that governments essentially cannot stop most of these approaches, short of establishing a police state (and probably not even then)
- core issues of identity, authentication, pseudonyms, reputations, etc.

1.4. Who Should Read This

1.4.1. "Should I read this?"

- Yes, reading this will point you toward other sources of information, will answer the most commonly asked questions, and will (hopefully) head off the reappearance of the same tired themes every few months.
- Use a search tool if you have one. Grep for the things that interest you, etc. The granularity of this FAQ does not lend itself to Web conversion, at least not with present tools.

+ What Won't Be Covered Here

- + basic cryptography
 - + many good texts, FAQs, etc., written by full-time cryptologists and educators

- in particular, some of the ideas are not simple, and take several pages of well-written text to get the point across
- not the focus of this FAQ
- basic political rants

1.5. Comments on Style and Thoroughness

1.5.1. "Why is this FAQ not in Mosaic form?"

- because the author (tcmay, as of 7/94) does not have Mosaic access, and even if did, would not necessarily....
- linear text is still fine for some things...can be read on all platforms, can be printed out, and can be searched with standard grep and similar tools

1.5.2. "Why the mix of styles?"

- + There are three main types of styles here:
 - Standard prose sections, explaining some point or listing things. Mini-essays, like most posts to Cypherpunks.
- + Short, outline-style comments
 - that I didn't have time or willpower to expand into prose format
 - that work best in outline format anyway
 - like this
- + Quotes from others
 - Cypherpunks are a bright group. A lot of clever things have been said in the 600 days x 40 posts/day = 24,000 posts, and I am trying to use what I can.
- + Sadly, only a tiny fraction can be used
 - because I simply cannot read even a fraction of these posts over again (though I've only saved several thousand of the posts)
 - and because including too many of these posts would simply make the FAQ too long (it's still too long, I suppose)
- I hope you can handle the changes in tone of voice, in styles, and even in formats. It'll just too much time to make it all read uniformly.

1.5.3. Despite the length of this thing, a vast amount of stuff is missing. There have been hundreds of incisive analyses by Cypherpunks, dozens of survey articles on Clipper, and thousands of clever remarks. Alas, only a few of them here.

- And with 25 or more books on the Internet, hundreds of FAQs and URLs, it's clear that we're all drowning in a sea of information about the Net.
- Ironically, good old-fashioned books have a lot more relevant and timeless information.

1.5.4. Caveats on the completeness or accuracy of this FAQ

- + not all points are fully fleshed out...the outline nature means that nearly all points could be further added-to, subdivided, taxonomized, and generally fleshed-out with more points, counterpoints, examples
 - like a giant tree...branches, leaves, tangled hierarchies
- + It is inevitable that conflicting points will be made in a document of this size
 - views change, but don't get corrected in all places
 - different contexts lead to different viewpoints
 - simple failure by me to be fully consistent
 - and many points raised here would, if put into an essay

for the Cypherpunks list, generate comments, rebuttals, debate, and even acrimony....I cannot expect to have all sides represented fully, especially as the issues are often murky, unresolved, in dispute, and generally controversial

- inconsistencies in the points here in this FAQ

1.6. Corrections and Elaborations

+ "How to handle corrections or clarifications?"

- While I have done my best to ensure accuracy, errors will no doubt exist. And as anyone can see from reading the Cypherpunks list, nearly *any* statement made about any subject can produce a flurry of rebuttals, caveats, expansions, and whatnot. Some subjects, such as the nature of money, the role of Cypherpunks, and the role of reputations, produce dozens of differing opinions every time they come up!
- So, it is not likely that my points here will be any different. Fortunately, the sheer number of points here means that not every one of them will be disagreed with. But the math is pretty clear: if every reader finds even one thing to disagree with and then posts his rebuttal or elaboration....disaster! (Especially if some people can't trim quotes properly and end up including a big chunk of text.)

+ Recommendations

- Send corrections of fact to me
- If you disagree with my opinion, and you think you can change my mind, or cause me to include your opinion as an elaboration or as a dissenting view, then send it. If your point requires long debate or is a deep disagreement, then I doubt I have the time or energy to debate. If you want your views heard, write your own FAQ!
- Ultimately, send what you want. But I of course will evaluate comments and apply a reputation-based filter to the traffic. Those who send me concise, well-reasoned corrections or clarifications are likelier to be listened to than those who barrage me with minor clarifications and elaborations.
- In short, this is not a group project. The "stone soup FAQ" is not what this is.

+ More information

- Please don't send me e-mail asking for more information on a particular topic--I just can't handle custom research. This FAQ is long enough, and the Glossary at the end contains additional information, so that I cannot expand upon these topics (unless there is a general debate on the list). In other words, don't assume this FAQ is an entry point into a larger data base I will generate. I hate to sound so blunt, but I've seen the requests that come in every time I write a fairly long article.

+ Tips on feedback

- Comments about writing style, of the form "I would have written it this way," are especially unwelcome.

+ Credit issues

- inevitable that omissions or collisions will occur

- ideas have many fathers
- some ideas have been "in the air" for many years
- + slogans are especially problematic
 - "They can have my...."...I credit Barlow with this, but I've heard others use it independently (I think; at least I used it before hearing Barlow used it)
 - "If crypto is outlawed, only outlaws will have crypto"
 - "Big Brother Inside"
- if something really bothers you, send me a note

1.7. Acknowledgements

1.7.1. Acknowledgements

- My chief thanks go to the several hundred active Cypherpunks posters, past and present.
- All rights reserved. Copyright Timothy C. May. Don't try to sell this or incorporate it into anything that is sold. Quoting brief sections is "fair use"...quoting long sections is not.

1.8. Ideas and Notes (not to be printed)

1.8.1. Graphics for cover

- two blocks...plaintext to cryptotext
- Cypherpunks FAQ
- compiled by Timothy C. May, tcmay@netcom.com
- with help from many Cypherpunks
- with material from other sources
- <credited in angle brackets>

1.8.2. "So don't ask"

1.9. Things are moving quickly in crypto and crypto policy

1.9.1. hard to keep this FAQ current, as info changes

1.9.2. PGP in state of flux

1.9.3. new versions of tools coming constantly

1.9.4. And the whole Clipper thing has been turned on its head recently by the Administration's backing off...lots of points already made here are now rendered moot and are primarily of historical interest only.

- Gore's letter to Cantwell
- Whit Diffie described a conference on key escrow systems in Karlsruhe, Germany, which seemed to contain new ideas
- TIS? (can't use this info?)

1.10. Notes: The Cyphernomicon: the CypherFAQ and More

1.10.1. 2.3.1. "The Book of Encyphered Names"

- Ibn al-Taz Khallikak, the Pine Barrens Horror.
- Liber Grimoiris....Cifur???
- spreading from the Sumerian sands, through the gate of Ishtar, to the back alleys of Damascus, tempered with the blood of Westerners
- Keys of Solomon, Kool John Dee and the Rapping Cryps Gone to Croatan
- Peter Kryptokin, the Russian crypto anarchist
- Twenty-nine Primes, California

1.10.2. 2.3.2. THE CYPHERNOMICON: a Cypherpunk FAQ and More--- Version 0.666

1.10.3. 1994-09-01, Copyright Timothy C. May, tcmay@netcom.com

1.10.4.

- Written and compiled by Tim May, except as noted by credits. (Influenced by years of good posts on the Cypherpunks list.) Permission is granted to post and distribute this document in an unaltered and complete state, for non-profit and educational purposes only. Reasonable quoting under "fair use" provisions is permitted. See the detailed disclaimer of responsibilities and liabilities in the Introduction chapter.

2. MFAQ--Most Frequently Asked Questions

2.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

2.2. SUMMARY: MFAQ--Most Frequently Asked Questions

2.2.1. Main Points

- These are the main questions that keep coming up. Not necessarily the most basic question, just the ones that get asked a lot. What most FAQs are.

2.2.2. Connections to Other Sections

2.2.3. Where to Find Additional Information

- newcomers to crypto should buy Bruce Schneier's "Applied Cryptography"...it will save many hours worth of unnecessary questions and clueless remarks about cryptography.
- the various FAQs published in the newsgroups (like sci.crypt, alt.security.pgp) are very helpful. (also at rtfm.mit.edu)

2.2.4. Miscellaneous Comments

- I wasn't sure what to include here in the MFAQ--perhaps people can make suggestions of other things to include.
- My advice is that if something interests you, use your editing/searching tools to find the same topic in the main section. Usually (but not always) there's more material in the main chapters than here in the MFAQ.

2.3. "What's the 'Big Picture'?"

2.3.1. Strong crypto is here. It is widely available.

2.3.2. It implies many changes in the way the world works. Private channels between parties who have never met and who never will meet are possible. Totally anonymous, unlinkable, untraceable communications and exchanges are possible.

2.3.3. Transactions can only be *voluntary*, since the parties are untraceable and unknown and can withdraw at any time. This has profound implications for the conventional approach of using the threat of force, directed against parties by governments or by others. In particular, threats of force will fail.

2.3.4. What emerges from this is unclear, but I think it will be a form of anarcho-capitalist market system I call "crypto anarchy." (Voluntary communications only, with no third parties butting in.)

2.4. Organizational

2.4.1. "How do I get on--and off--the Cypherpunks list?"

- Send a message to "cypherpunks-request@toad.com"
- Any auto-processed commands?
- don't send requests to the list as a whole....this will mark you as "clueless"

2.4.2. "Why does the Cypherpunks list sometimes go down, or lose the subscription list?"

- The host machine, toad.com, owned by John Gilmore, has had the usual problems such machines have: overloading, shortages of disk space, software upgrades, etc. Hugh Daniel has done an admirable job of keeping it in good shape, but problems do occur.
- Think of it as warning that lists and communication systems remain somewhat fragile....a lesson for what is needed to make digital money more robust and trustable.
- There is no paid staff, no hardware budget for improvements. The work done is strictly voluntarily.

2.4.3. "If I've just joined the Cypherpunks list, what should I do?"

- Read for a while. Things will become clearer, themes will emerge, and certain questions will be answered. This is good advice for any group or list, and is especially so for a list with 500 or more people on it. (We hit 700+ at one point, then a couple of list outages knocked the number down a bit.)
- Read the references mentioned here, if you can. The sci.crypt FAQ should be read. And purchase Bruce Schneier's "Applied Cryptography" the first chance you get.
- Join in on things that interest you, but don't make a fool of yourself. Reputations matter, and you may come to regret having come across as a tedious fool in your first weeks on the list. (If you're a tedious fool after the first few weeks, that may just be your nature, of course.)
- Avoid ranting and raving on unrelated topics, such as abortion (pro or con), guns (pro or con), etc. The usual topics that usually generate a lot of heat and not much light. (Yes, most of us have strong views on these and other topics, and, yes, we sometimes let our views creep into discussions. There's no denying that certain resonances exist. I'm just urging caution.)

2.4.4. "I'm swamped by the list volume; what can I do?"

- This is a natural reaction. Nobody can follow it all; I spend entirely too many hours a day reading the list, and I certainly can't follow it all. Pick areas of expertise and then follow them and ignore the rest. After all, not seeing things on the list can be no worse than not even being subscribed to the list!
 - Hit the "delete" key quickly
 - find someone who will digest it for you (Eric Hughes has repeatedly said anyone can retransmit the list this way; Hal Finney has offered an encrypted list)
- + Better mailers may help. Some people have used mail-to-news systems and then read the list as a local newsgroup, with threads.
- I have Eudora, which supports off-line reading and sorting features, but I generally end up reading with an online mail program (elm).
 - The mailing list may someday be switched over to a

newsgroup, a la "alt.cypherpunks." (This may affect some people whose sites do not carry alt groups.)

2.4.5. "It's very easy to get lost in the morass of detail here. Are there any ways to track what's *really* important?"

- First, a lot of the stuff posted in the Usenet newsgroups, and on the Cypherpunks list, is peripheral stuff, epiphenomenal cruft that will blow away in the first strong breeze. Grungy details about PGP shells, about RSA encryption speeds, about NSA supercomputers. There's just no reason for people to worry about "weak IDEA keys" when so many more pressing matters exist. (Let the experts worry.) Little of this makes any real difference, just as little of the stuff in daily newspapers is memorable or deserves to be memorable.
- Second, "read the sources." Read "1984," "The Shockwave Rider," "Atlas Shrugged," "True Names." Read the Chaum article on making Big Brother obsolete (October 1985, "Communications of the ACM").
- Third, don't lose sight of the core values: privacy, technological solutions over legal solutions, avoiding taxation, bypassing laws, etc. (Not everyone will agree with all of these points.)
- Fourth, don't drown in the detail. Pick some areas of interest and follow them. You may not need to know the inner workings of DES or all the switches on PGP to make contributions in other areas. (In fact, you surely don't.)

2.4.6. "Who are the Cypherpunks?"

- A mix of about 500-700
- + Can find out who by sending message to majordomo@toad.com with the message body text "who cypherpunks" (no quotes, of course).
- Is this a privacy flaw? Maybe.
- Lots of students (they have the time, the Internet accounts). Lots of computer science/programming folks. Lots of libertarians.
- quote from Wired article, and from "Whole Earth Review"

2.4.7. "Who runs the Cypherpunks?"

- Nobody. There's no formal "leadership." No ruler = no head = an arch = anarchy. (Look up the etymology of anarchy.)
- However, the mailing list currently resides on a physical machine, and this machine creates some nexus of control, much like having a party at someone's house. The list administrator is currently Eric Hughes (and has been since the beginning). He is helped by Hugh Daniel, who often does maintenance of the toad.com, and by John Gilmore, who owns the toad.com machine and account.
- In an extreme situation of abuse or neverending ranting, these folks could kick someone off the list and block them from resubscribing via majordomo. (I presume they could-- it's never happened.)
- To emphasize: nobody's ever been kicked off the list, so far as I know. Not even Detweiler...he asked to be removed (when the list subscribers were done manually).
- As to who sets policy, there is no policy! No charter, no agenda, no action items. Just what people want to work on themselves. Which is all that can be expected. (Some people get frustrated at this lack of consensus, and they

sometimes start flaming and ranting about "Cypherpunks never do anything," but this lack of consensus is to be expected. Nobody's being paid, nobody's got hiring and firing authority, so any work that gets done has to be voluntary. Some volunteer groups are more organized than we are, but there are other factors that make this more possible for them than it is for us. C'est la vie.)

- Those who get heard on the mailing list, or in the physical meetings, are those who write articles that people find interesting or who say things of note. Sounds fair to me.

2.4.8. "Why don't the issues that interest me get discussed?"

- Maybe they already have been--several times. Many newcomers are often chagrined to find arcane topics being discussed, with little discussion of "the basics."
- This is hardly surprising....people get over the "basics" after a few months and want to move on to more exciting (to them) topics. All lists are like this.
- In any case, after you've read the list for a while--maybe several weeks--go ahead and ask away. Making your topic fresher may generate more responses than, say, asking what's wrong with Clipper. (A truly overworked topic, naturally.)

2.4.9. "How did the Cypherpunks group get started?"

2.4.10. "Where did the name 'Cypherpunks' come from?"

- + Jude Milhon, aka St. Jude, then an editor at "Mondo 2000," was at the earliest meetings...she quipped "You guys are just a bunch of cypherpunks." The name was adopted immediately.
- The 'cyberpunk' genre of science fiction often deals with issues of cyberspace and computer security ("ice"), so the link is natural. A point of confusion is that cyberpunks are popularly thought of as, well, as "punks," while many Cyberpunks are frequently libertarians and anarchists of various stripes. In my view, the two are not in conflict.
- Some, however, would prefer a more staid name. The U.K. branch calls itself the "U.K. Crypto Privacy Association." <check this> However, the advantages of the name are clear. For one thing, many people are bored by staid names. For another, it gets us noticed by journalists and others.
-
- We are actually not very "punkish" at all. About as punkish as most of our cyberpunk cousins are, which is to say, not very.

+ the name

- Crypto Cabal (this before the sci.crypt FAQ folks appeared, I think), Crypto Liberation Front, other names
- not everybody likes the name...such is life

2.4.11. "Why doesn't the Cypherpunks group have announced goals, ideologies, and plans?"

- The short answer: we're just a mailing list, a loose association of folks interested in similar things
- no budget, no voting, no leadership (except the "leadership of the soapbox")
- How could such a consensus emerge? The usual approach is for an elected group (or a group that seized power) to

write the charter and goals, to push their agenda. Such is not the case here.

- Is this FAQ a de facto statement of goals? Not if I can help it, to be honest. Several people before me planned some sort of FAQ, and had they completed them, I certainly would not have felt they were speaking for me or for the group. To be consistent, then, I cannot have others think this way about this FAQ!

2.4.12. "What have the Cypherpunks actually done?"

- spread of crypto: Cypherpunks have helped (PGP)...publicity, an alternative forum to sci.crypt (in many ways, better...better S/N ratio, more polite)
- Wired, Whole Earth Review, NY Times, articles
- remailers, encrypted remailers
- + The Cypherpunk- and Julf/Kleinpaste-style remailers were both written very quickly, in just days
 - Eric Hughes wrote the first Cypherpunks remailer in a weekend, and he spent the first day of that weekend learning enough Perl to do the job.
- + Karl Kleinpaste wrote the code that eventually turned into Julf's remailer (added to since, of course) in a similarly short time:
 - "My original anon server, for godiva.nectar.cs.cmu.edu 2 years ago, was written in a few hours one bored afternoon. It wasn't as featureful as it ended up being, but it was "complete" for its initial goals, and bug-free."
[Karl_Kleinpaste@cs.cmu.edu, alt.privacy.anon-server, 1994-09-01]
- That other interesting ideas, such as digital cash, have not yet really emerged and gained use even after years of active discussion, is an interesting contrast to this rapid deployment of remailers. (The text-based nature of both straight encryption/signing and of remailing is semantically simpler to understand and then use than are things like digital cash, DC-nets, and other crypto protocols.)
- ideas for Perl scripts, mail handlers
- general discussion, with folks of several political persuasions
- concepts: pools, Information Liberation Front, BlackNet
-

2.4.13. "How Can I Learn About Crypto and Cypherpunks Info?"

2.4.14. "Why is there sometimes disdain for the enthusiasm and proposals of newcomers?"

- None of us is perfect, so we sometimes are impatient with newcomers. Also, the comments seen tend to be issues of disagreement--as in all lists and newsgroups (agreement is so boring).
- But many newcomers also have failed to do the basic reading that many of us did literally years before joining this list. Cryptology is a fairly technical subject, and one can no more jump in and expect to be taken seriously without any preparation than in any other technical field.
- Finally, many of us have answered the questions of newcomers too many times to be enthusiastic about it

- anymore. Familiarity breeds contempt.
- + Newcomers should try to be patient about our impatience. Sometimes recasting the question generates interest. Freshness matters. Often, making an incisive comment, instead of just asking a basic question, can generate responses. (Just like in real life.)
 - "Clipper sux!" won't generate much response.
- 2.4.15. "Should I join the Cypherpunks mailing list?"
- If you are reading this, of course, you are most likely on the Cypherpunks list already and this point is moot--you may instead be asking if you should leave the List!
 - Only if you are prepared to handle 30-60 messages a day, with volumes fluctuating wildly
- 2.4.16. "Why isn't the Cypherpunks list encrypted? Don't you believe in encryption?"
- what's the point, for a publically-subscribable list?
 - except to make people jump through hoops, to put a large burden on toad (unless everybody was given the same key, so that just one encryption could be done...which underscores the foolishness)
 - + there have been proposals, mainly as a stick to force people to start using encryption...and to get the encrypted traffic boosted
 - involving delays for those who choose not or can't use crypto (students on terminals, foreigners in countries which have banned crypto, corporate subscribers....)
- 2.4.17. "What does 'Cypherpunks write code' mean?"
- a clarifying statement, not an imperative
 - technology and concrete solutions over bickering and chatter
 - if you don't write code, fine. Not everyone does (in fact, probably less than 10% of the list writes serious code, and less than 5% writes crypto or security software)
- 2.4.18. "What does 'Big Brother Inside' Mean?"
- devised by yours truly (tcmay) at Clipper meeting
 - Matt Thomlinson, Postscript
 - printed by
- 2.4.19. "I Have a New Idea for a Cipher---Should I Discuss it Here?"
- Please don't. Ciphers require careful analysis, and should be in paper form (that is, presented in a detailed paper, with the necessary references to show that due diligence was done, the equations, tables, etc. The Net is a poor substitute.
 - Also, breaking a randomly presented cipher is by no means trivial, even if the cipher is eventually shown to be weak. Most people don't have the inclination to try to break a cipher unless there's some incentive, such as fame or money involved.
 - And new ciphers are notoriously hard to design. Experts are the best folks to do this. With all the stuff waiting to be done (described here), working on a new cipher is probably the least effective thing an amateur can do. (If you are not an amateur, and have broken other people's ciphers before, then you know who you are, and these comments don't apply. But I'll guess that fewer than a handful of folks on this list have the necessary background to do cipher design.)

- There are a vast number of ciphers and systems, nearly all of no lasting significance. Untested, undocumented, unused- and probably unworthy of any real attention. Don't add to the noise.
- 2.4.20. Are all the Cypherpunks libertarians?
- 2.4.21. "What can we do?"
- Deploy strong crypto, to ensure the genie cannot be put in the bottle
 - Educate, lobby, discuss
 - Spread doubt, scorn..help make government programs look foolish
 - Sabotage, undermine, monkeywrench
 - Pursue other activities
- 2.4.22. "Why is the list unmoderated? Why is there no filtering of disrupters like Detweiler?"
- technology over law
 - each person makes their own choice
 - also, no time for moderation, and moderation is usually stultifying
- + anyone who wishes to have some views silenced, or some posters blocked, is advised to:
- contract with someone to be their Personal Censor, passing on to them only approved material
 - subscribe to a filtering service, such as Ray and Harry are providing
- 2.4.23. "What Can I Do?"
- politics, spreading the word
 - writing code ("Cypherpunks write code")
- 2.4.24. "Should I publicize my new crypto program?"
- "I have designed a crypting program, that I think is unbreakable. I challenge anyone who is interested to get in touch with me, and decrypt an encrypted message."
- "With highest regards,
Babak Sehari." [Babak Sehari, sci.crypt, 6-19-94]
- 2.4.25. "Ask Emily Post Crypt"
- + my variation on "Ask Emily Postnews"
- for those that don't know, a scathing critique of clueless postings
- + "I just invented a new cipher. Here's a sample. Bet you can't break it!"
- By all means post your encrypted junk. We who have nothing better to do with our time than respond will be more than happy to spend hours running your stuff through our codebreaking Crays!
 - Be sure to include a sample of encrypted text, to make yourself appear even more clueless.
- + "I have a cypher I just invented...where should I post it?"
- + "One of the very most basic errors of making ciphers is simply to add
- layer upon layer of obfuscation and make a cipher which is nice and
 - "complex". Read Knuth on making random number generators for the
 - folly in this kind of approach. " <Eric Hughes, 4-17-94, Cypherpunks>

- + "Ciphers carry the presumption of guilt, not innocence.
 - Ciphers
 - designed by amateurs invariably fail under scrutiny by experts. This
 - sociological fact (well borne out) is where the presumption of
 - insecurity arises. This is not ignorance, to assume that this will
 - change. The burden of proof is on the claimer of security, not upon
 - the codebreaker. <Eric Hughes, 4-17-94, Cypherpunks>
- + "I've just gotten very upset at something--should I vent my anger on the mailing list?"
 - By all means! If you're fed up doing your taxes, or just read something in the newspaper that really angered you, definitely send an angry message out to the 700 or so readers and help make them angry!
 - Find a bogus link to crypto or privacy issues to make it seem more relevant.
- 2.4.26. "What are some main Cypherpunks projects?"
 - + remailers
 - + better remailers, more advanced features
 - digital postage
 - padding, batching/latency
 - agent features
 - more of them
 - offshore (10 sites in 5 countries, as a minimum)
 - tools, services
 - digital cash in better forms
 -
- 2.4.27. "What about sublists, to reduce the volume on the main list."
 - There are already half a dozen sub-lists, devoted to planning meetings, to building hardware, and to exploring DC-Nets. There's one for remailer operators, or there used to be. There are also lists devoted to similar topics as Cypherpunks, including Robin Hanson's "AltInst" list (Alternative Institutions), Nick Szabo's "libtech-1" list, the "IMP-Interest" (Internet Mercantile Protocols) list, and so on. Most are very low volume.
 - + That few folks have heard of any of them, and that traffic volumes are extremely low, or zero, is not all that surprising, and matches experiences elsewhere. Several reasons:
 - Sublists are a bother to remember; most people forget they exist, and don't think to post to them. (This "forgetting" is one of the most interesting aspects of cyberspace; successful lists seem to be Schelling points that accrete even more members, while unsuccessful lists fade away into nothingness.)
 - There's a natural desire to see one's words in the larger of two forums, so people tend to post to the main list.
 - The sublists were sometimes formed in a burst of exuberance over some topic, which then faded.
 - Topics often span several subinterest areas, so posting to the main list is better than copying all the relevant sublists.
 - In any case, the Cypherpunks main list is "it," for now,

and has driven other lists effectively out of business. A kind of Gresham's Law.

2.5. Crypto

2.5.1. "Why is crypto so important?"

- + The three elements that are central to our modern view of liberty and privacy (a la Diffie)
 - protecting things against theft
 - proving who we say we are
 - expecting privacy in our conversations and writings
- Although there is no explicit "right of privacy" enumerated in the U.S. Constitution, the assumption that an individual is to be secure in his papers, home, etc., absent a valid warrant, is central. (There has never been a ruling or law that persons have to speak in a language that is understandable by eavesdroppers, wiretappers, etc., nor has there ever been a rule banning private use of encryption. I mention this to remind readers of the long history of crypto freedom.)
- "Information, technology and control of both is power. *Anonymous* telecommunications has the potential to be the greatest equalizer in history. Bringing this power to as many as possible will forever change the discourse of power in this country (and the world)." [Matthew J Miszewski, ACT NOW!, 1993-03-06]

2.5.2. "Who uses cryptography?"

- Everybody, in one form or another. We see crypto all around us...the keys in our pockets, the signatures on our driver's licenses and other cards, the photo IDs, the credit cards. Lock combinations, door keys, PIN numbers, etc. All are part of crypto (although most might call this "security" and not a very mathematical thing, as cryptography is usually thought to be).
- Whitticism: "those who regularly conspire to participate in the political process are already encrypting." [Whit Diffie]

2.5.3. "Who needs crypto? What have they got to hide?"

- + honest people need crypto because there are dishonest people
 - and there may be other needs for privacy
- There are many reasons why people need privacy, the ability to keep some things secret. Financial, personal, psychological, social, and many other reasons.
- Privacy in their papers, in their diaries, in their personal lives. In their financial choices, their investments, etc. (The IRS and tax authorities in other countries claim to have a right to see private records, and so far the courts have backed them up. I disagree.)
- people encrypt for the same reason they close and lock their doors
 - Privacy in its most basic forms

2.5.4. "I'm new to crypto--where should I start?"

- books...Schneier
- soda
- sci.crypt
- talk.politics.crypto
- FAQs other than this one

2.5.5. "Do I need to study cryptography and number theory to make a contribution?"

- Absolutely not! Most cryptographers and mathematicians are so busy doing their thing that they have little time or interest for political and entrepreneurial activities. Specialization is for insects and researchers, as someone's .sig says.
- Many areas are ripe for contribution. Modularization of functions means people can concentrate in other areas, just as writers don't have to learn how to set type, or cut quill pens, or mix inks.
- Nonspecialists should treat most established ciphers as "black boxes" that work as advertised. (I'm not saying they do, just that analysis of them is best left to experts...a little skepticism may not hurt, though).

2.5.6. "How does public key cryptography work, simply put?"

- Plenty of articles and textbooks describe this, in ever-increasing detail (they start out with the basics, then get to the juicy stuff).

+ I did find a simple explanation, with "toy numbers," from Matthew Ghio:

- "You pick two prime numbers; for example 5 and 7. Multiply them together, equals 35. Now you calculate the product of one less than each number, plus one. $(5-1)(7-1)+1=21$. There is a mathematical relationship that says that $x = x^{21} \pmod{35}$ for any x from 0 to 34. Now you factor 21, yeilds 3 and 7.

"You pick one of those numbers to be your private key and the other one is your public key. So you have:

Public key: 3
Private key: 7

"Someone encrypts a message for you by taking plaintext message m to make ciphertext message c : $c=m^3 \pmod{35}$

"You decrypt c and find m using your private key: $m=c^7 \pmod{35}$

"If the numbers are several hundred digits long (as in PGP), it is nearly impossible to guess the secret key."

[Matthew Ghio, alt.anonymous, 1994-09-03]

- (There's a math error here...exercise left for the student.)

2.5.7. "I'm a newcomer to this stuff...how should I get started?"

- Start by reading some of the material cited. Don't worry too much about understanding it all.
- Follow the list.
- Find an area that interests you and concentrate on that. There is no reason why privacy advocates need to understand Diffie-Hellman key exchange in detail!

+ More Information

- + Books
 - Schneier
 - Brassard
- + Journals, etc
 - Proceedings

- Journal of Cryptology
 - Cryptologia
 - Newsgroups
 - ftp sites
- 2.5.8. "Who are Alice and Bob?"
- 2.5.9. "What is security through obscurity"?
- adding layers of confusion, indirection
 - rarely is strong in an information-theoretic or cryptographic sense
 - and may have "shortcuts" (like a knot that looks complex but which falls open if approached the right way)
 - encryption algorithms often hidden, sites hidden
 - Make no mistake about it, these approaches are often used. And they can add a little to the overall security (using file encryption programs like FolderBolt on top of PGP is an example)...
- 2.5.10. "Has DES been broken? And what about RSA?"
- DES: Brute-force search of the keyspace in chosen-plaintext attacks is feasible in around 2^{47} keys, according to Biham and Shamir. This is about 2^9 times easier than the "raw" keyspace. Michael Wiener has estimated that a machine of special chips could crack DES this way for a few thousand dollars per key. The NSA may have such machines.
 - In any case, DES was not expected to last this long by many (and, in fact, the NSA and NIST proposed a phaseout some years back, the "CCEP" (Commercial COMSEC Endorsement Program), but it never caught on and seems forgotten today. Clipper and EES seem to have grabbed the spotlight.
 - IDEA, from Europe, is supposed to be much better.
 - As for RSA, this is unlikely. Factoring is not yet proven to be NP-co
- 2.5.11. "Can the NSA Break Foo?"
- DES, RSA, IDEA, etc.
 - Can the government break our ciphers?
- 2.5.12. "Can brute-force methods break crypto systems?"
- depends on the system, the keyspace, the ancillary information available, etc.
 - processing power generally has been doubling every 12-18 months (Moore's Law), so....
 - Skipjack is 80 bits, which is probably safe from brute force attack for $2^{24} = 1.68e7$ times as long as DES is. With Wiener's estimate of 3.5 hours to break DES, this implies 6700 years using today's hardware. Assuming an optimistic doubling of hardware power per year (for the same cost), it will take 24 years before the hardware costs of a brute force attack on Skipjack come down to what it now costs to attack DES. Assuming no other weaknesses in Skipjack.
 - And note that intelligence agencies are able to spend much more than what Wiener calculated (recall Norm Hardy's description of Harvest)
- 2.5.13. "Did the NSA know about public key ideas before Diffie and Hellman?"
- + much debate, and some sly and possibly misleading innuendo
 - Simmons claimed he learned of PK in Gardner's column, and he certainly should've been in a position to know (weapons, Sandia)

-
- + Inman has claimed that NSA had a P-K concept in 1966
 - fits with Dominik's point about sealed cryptosystem boxes with no way to load new keys
 - and consistent with NSA having essentially sole access to nation's top mathematicians (until Diffies and Hellmans foreswore government funding, as a result of the anti-Pentagon feelings of the 70s)
- 2.5.14. "Did the NSA know about public-key approaches before Diffie and Hellman?"
 - comes up a lot, with some in the NSA trying to slyly suggest that of course they knew about it...
 - Simmons, etc.
 - Bellovin comments (are good)
- 2.5.15. "Can NSA crack RSA?"
 - Probably not.
 - Certainly not by "searching the keyspace," an idea that pops up every few months . It can't be done. 1024-bit keys implies roughly 512-bit primes, or 153-decimal digit primes. There are more than 10^{150} of them! And only about 10^{73} particles in the entire universe.
 - Has the factoring problem been solved? Probably not. And it probably won't be, in the sense that factoring is probably in NP (though this has not been proved) and P is probably not NP (also unproved, but very strongly suspected). While there will be advances in factoring, it is extremely unlikely (in the religious sense) that factoring a 300-digit number will suddenly become "easy."
 - Does the RSA leak information so as to make it easier to crack than it is to factor the modulus? Suspected by some, but basically unknown. I would bet against it. But more iffy than the point above.
- + "How strong is strong crypto?"
 - Basically, stronger than any of the hokey "codes" so beloved of thriller writers and movie producers. Modern ciphers are not crackable by "telling the computer to run through all the combinations" (more precisely, the number of combinations greatly exceeds the number of atoms in the universe).
- 2.5.16. "Won't more powerful computers make ciphers breakable?"
 - + The effects of increasing computer power confer even **greater** advantage to the cipher user than to the cipher breaker. (Longer key lengths in RSA, for example, require polynomially more time to use, but exponentially more time to break, roughly speaking.) Stuningly, it is likely that we are close to being able to use key lengths which cannot be broken with all the computer power that will ever exist in the universe.
 - + Analogous to impenetrable force fields protecting the data, with more energy required to "punch through" than exists in the universe
 - Vernor Vinge's "bobbles," in "The Peace War."
 - Here I am assuming that no short cuts to factoring exist...this is unproven, but suspected. (No major shortcuts, i.e., factoring is not "easy.")
 - + A modulus of thousands of decimal digits may require more total "energy" to factor, using foreseeable approaches,

than is available

- reversible computation may help, but I suspect not much
- Shor's quantum-mechanical approach is completely untested...and may not scale well (e.g., it may be marginally possible to get the measurement precision to use this method for, say, 100-digit numbers, but utterly impossible to get it for 120-digit numbers, let alone 1000-digit numbers)

2.5.17. "Will strong crypto help racists?"

- Yes, this is a consequence of having secure virtual communities. Free speech tends to work that way!
- The Aryan Nation can use crypto to collect and disseminate information, even into "controlled" nations like Germany that ban groups like Aryan Nation.
- Of course, "on the Internet no one knows you're a dog," so overt racism based on superficial external characteristics is correspondingly harder to pull off.
- But strong crypto will enable and empower groups who have different beliefs than the local majority, and will allow them to bypass regional laws.

2.5.18. Working on new ciphers--why it's not a Cypherpunks priority (as I see it)

- It's an issue of allocation of resources. ("All crypto is economics." E. Hughes) Much work has gone into cipher design, and the world seems to have several stable, robust ciphers to choose from. Any additional work by crypto amateurs--which most of us are, relative to professional mathematicians and cipher designers--is unlikely to move things forward significantly. Yes, it could happen...but it's not likely.
- + Whereas there are areas where professional cryptologists have done very little:
 - PGP (note that PRZ did **not** take time out to try to invent his own ciphers, at least not for Version 2.0)...he concentrated on where his efforts would have the best payoff
 - implementation of remailers
 - issues involving shells and other tools for crypto use
 - digital cash
 - related issues, such as reputations, language design, game theory, etc.
- These are the areas of "low-hanging fruit," the areas where the greatest bang for the buck lies, to mix some metaphors (grapeshot?).

2.5.19. "Are there any unbreakable ciphers?"

- One time pads are of course information-theoretically secure, i.e., unbreakable by computer power.
- + For conventional ciphers, including public key ciphers, some ciphers may not be breakable in our universe, in any amount of time. The logic goes as follows:
 - Our universe presumably has some finite number of particles (currently estimated to be 10^{73} particles). This leads to the "even if every particle were a Cray Y-MP it would take..." sorts of thought experiments.

But I am considering energy here. Ignoring reversible computation for the moment, computations dissipate energy

(some disagree with this point). There is some upper limit on how many basic computations could ever be done with the amount of free energy in the universe. (A rough calculation could be done by calculating the energy output of stars, stuff falling into black holes, etc., and then assuming about kT per logical operation. This should be accurate to within a few orders of magnitude.) I haven't done this calculation, and won't here, but the result would likely be something along the lines of X joules of energy that could be harnessed for computation, resulting in Y basic primitive computational steps.

I can then find a modulus of 3000 digits or 5000 digits, or whatever, that takes *more* than this number of steps to factor. Therefore, unbreakable in our universe.

- Caveats:

1. Maybe there are really shortcuts to factoring. Certainly improvements in factoring methods will continue. (But of course these improvements are not things that convert factoring into a less than exponential-in-length problem...that is, factoring appears to remain "hard.")

2. Maybe reversible computations (a la Landauer, Bennett, et. al.) actually work. Maybe this means a "factoring machine" can be built which takes a fixed, or very slowly growing, amount of energy. In this case, "forever" means Lefty is probably right.

3. Maybe the quantum-mechanical idea of Peter Shor is possible. (I doubt it, for various reasons.)

2.5.20. "How safe is RSA?" "How safe is PGP?" "I heard that PGP has bugs?"

- This cloud of questions is surely the most common sort that appears in sci.crypt. It sometimes gets no answers, sometimes gets a rude answer, and only occasionally does it lead to a fruitful discussion.
- The simple answer: These ciphers appear to be safe, to have no obvious flaws.
- More details can be found in various question elsewhere in this FAQ and in the various FAQs and references others have published.

2.5.21. "How long does encryption have to be good for?"

- This obviously depends on what you're encrypting. Some things need only be safe for short periods of time, e.g., a few years or even less. Other things may come back to haunt you--or get you thrown in prison--many years later. I can imagine secrets that have to be kept for many decades, even centuries (for example, one may fear one's descendents will pay the price for a secret revealed).
- It is useful to think now about the computer power likely to be available in the year 2050, when many of you reading this will still be around. (I'm not arguing that parallelism, etc., will cause RSA to fall, only that some key lengths (e.g., 512-bit) may fall by then. Better be safe and use 1024 bits or even more. Increased computer

power makes longer keys feasible, too.).

2.6. PGP

2.6.1. There's a truly vast amount of information out there on PGP, from current versions, to sites, to keyserver issues, and so on. There are also several good FAQs on PGP, on MacPGP, and probably on nearly every major version of PGP. I don't expect to compete here with these more specialized FAQs.

- I'm also not a PGP expert, using it only for sending and receiving mail, and rarely doing much more with it.
- The various tools, for all major platforms, are a specialty unto themselves.

2.6.2. "Where do I get PGP?"

2.6.3. "Where can I find PGP?"

- Wait around for several days and a post will come by which gives some pointers.
- Here are some sites current at this writing: (watch out for changes)

2.6.4. "Is PGP secure? I heard someone had...."

- periodic reports, urban legend, that PGP has been compromised, that Phil Z. has been "persuaded" to....
- + implausible for several reasons
 - Phil Z no longer controls the source code by himself
 - the source code is available and can be inspected...would be very difficult to slip in major back doors that would not be apparent in the source code
 - Phil has denied this, and the rumors appear to come from idle speculation

+ But can PGP be broken?

- has not been tested independently in a thorough, cryptanalytic way, yet (opinion of tcmay)
- NSA isn't saying

+ Areas for attack

+ IDEA

- some are saying doubling of the number of rounds should be donee
- the random number generators...Colin Plumb's admission

2.6.5. "Should I use PGP and other crypto on my company's workstations?"

- machines owned by corporations and universities, usually on networks, are generally not secure (that is, they may be compromised in various ways)
- ironically, most of the folks who sign all their messages, who use a lot of encryption, are on just such machines
- PCs and Macs and other nonnetworked machines are more secure, but are harder to use PGP on (as of 1994)
- these are generalizations--there are insecure PCs and secure workstations

2.6.6. "I just got PGP--should I use it for all my mail?"

- No! Many people cannot easily use PGP, so if you wish to communicate with them, don't encrypt everything. Use encryption where it matters.
- If you just want more people to use encryption, help with the projects to better integrate crypto into existing mailers.

2.6.7. NSA is apparently worried about PGP, worried about the spread of PGP to other countries, and worried about the growth of

"internal communities" that communicate via "black pipes" or "encrypted tunnels" that are impenetrable to them.

2.7. Clipper

2.7.1. "How can the government do this?"

- incredulity that bans, censorship, etc. are legal
- + several ways these things happen
 - not tested in the courts
 - wartime regulations
- + conflicting interpretations
 - e.g., "general welfare" clause used to justify restrictions on speech, freedom of association, etc.
- + whenever public money or facilities used (as with churches forced to hire Satanists)
 - and in this increasingly interconnected world, it is sometimes very hard to avoid overlap with public funding, facilities, etc.

2.7.2. "Why don't Cypherpunks develop their own competing encryption chip?"

- + Many reasons not to:
 - cost
 - focus
 - expertise
 - hard to sell such a competing standard
- better to let market as a whole make these choices

2.7.3. "Why is crypto so frightening to governments?"

- + It takes away the state's power to snoop, to wiretap, to eavesdrop, to control
 - Priestly confessionals were a major way the Church kept tabs on the locals...a worldwide, grassroots system of ecclesiastical narcs
- + Crypto has high leverage
 - + Unlike direct assaults with bombs, HERF and EMP attacks, sabotage, etc, crypto is self-spreading...a bootstrap technology
 - people use it, give it to others, put it on networks
 - others use it for their own purposes
 - a cascade effect, growing geometrically
 - and undermining confidence in governments, allowing the spread of multiple points of view (especially unapproved views)

2.7.4. "I've just joined the list and am wondering why I don't see more debate about Clipper?"

- Understand that people rarely write essays in response to questions like "Why is Clipper bad?" For most of us, mandatory key escrow is axiomatically bad; no debate is needed.
- Clipper was thoroughly trashed by nearly everyone within hours and days of its announcement, April 16, 1993. Hundreds of articles and editorials have condemned it. Cyperpunks currently has no active supporters of mandatory key escrow, from all indications, so there is nothing to debate.

2.8. Other Ciphers and Crypto Products

2.9. Remailers and Anonymity

2.9.1. "What are remailers?"

2.9.2. "How do remailers work?" (a vast number of postings have dealt with this)

- The best way to understand them is to "just do it," that is, send a few remailed message to yourself, to see how the syntax works. Instructions are widely available--some are cited here, and up to date instructions will appear in the usual Usenet groups.
- The simple view: Text messages are placed in envelopes and sent to a site that has agreed to remail them based on the instructions it finds. Encryption is not necessary--though it is of course recommended. These "messages in bottles" are passed from site to site and ultimately to the intended final recipient.
- The message is pure text, with instructions contained in the text itself (this was a fortuitous choice of standard by Eric Hughes, in 1992, as it allowed chaining, independence from particular mail systems, etc.).
- A message will be something like this:

```
::  
Request-Remailing-To: remailer@bar.baz
```

Body of text, etc., etc. (Which could be more remailing instructions, digital postage, etc.)

- These nested messages make no assumptions about the type of mailer being used, so long as it can handle straight ASCII text, which all mailers can of course. Each mail message then acts as a kind of "agent," carrying instructions on where it should be mailed next, and perhaps other things (like delays, padding, postage, etc.)
- It's very important to note that any given remailer cannot see the contents of the envelopes he is remailing, provided encryption is used. (The original sender picks a desired trajectory through the labyrinth of remailers, encrypts in the appropriate sequence (last is innermost, then next to last, etc.), and then the remailers sequentially decrypt the outer envelopes as they get them. Envelopes within envelopes.)

2.9.3. "Can't remailers be used to harass people?"

- Sure, so can free speech, anonymous physical mail ("poison pen letters"), etc.
- With e-mail, people can screen their mail, use filters, ignore words they don't like, etc. Lots of options. "Sticks and stones" and all that stuff we learned in Kindergarten (well, I'm never sure what the the Gen Xers learned...).
- Extortion is made somewhat easier by anonymous mailers, but extortion threats can be made in other ways, such as via physical mail, or from payphones, etc.
- Physical actions, threats, etc. are another matter. Not the domain of crypto, per se.

2.10. Surveillance and Privacy

2.10.1. "Does the NSA monitor this list?"

- Probably. We've been visible enough, and there are many

avenues for monitoring or even subscribing to the List.
Many aliases, many points of presence.

- some concerns that Cypherpunks list has been infiltrated and is a "round up list"
- There have even been anonymous messages purporting to name likely CIA, DIA, and NSA spooks. ("Be aware.")
- Remember, the list of subscribers is not a secret--it can be gotten by sending a "who cypherpunks" message to majordomo@toad.com. Anyone in the world can do this.

2.10.2. "Is this list illegal?"

- Depends on the country. In the U.S., there are very strong protections against "prior restraint" for published material, so the list is fairly well -protected....shutting it down would create a First Amendment case of major importance. Which is unlikely. Conspiracy and sedition laws are more complex to analyze; there are no indications that material here or on the list is illegal.
- Advocacy of illegal acts (subversion of export laws, espionage, etc.) is generally legal. Even advocating the overthrow of the government.
- The situation in other countries is different. Some countries ban unapproved encryption, so this list is suspect.
- Practically speaking, anyone reading this list is probably in a place which either makes no attempt to control encryption or is unable to monitor what crosses its borders.

2.10.3. "Can keystrokes really be monitored remotely? How likely is this?"

- Yes. Van Eck, RF, monitors, easy (it is claimed) to build this
- How likely? Depends on who you are. Ames, the KGB spy, was probably monitored near the end, but I doubt many of us are. The costs are simply too high...the vans outside, the personnel needed, etc.
- the real hazards involve making it "easy" and "almost automatic" for such monitoring, such as with Clipper and EES. Then they essentially just flip a switch and the monitoring happens...no muss, no fuss.

2.10.4. "Wouldn't some crimes be stopped if the government could monitor what it wanted to?"

- Sure. This is an old story. Some criminals would be caught if their diaries could be examined. Television cameras in all homes would reduce crimes of (Are you listening, Winston?).
- Orwell, fascism, surveillance states, what have you got to hide, etc.

2.11. Legal

2.11.1. "Can encryption be banned?"

- ham operators, shortwave
- il gelepal, looi to waptime aolditolq
- + how is this any different from requiring speech in some language?
 - Navaho code talkers of WW2,,,,modern parallel

2.11.2. "Will the government try to ban encryption?"

- This is of course the major concern most of us have about

Clipper and the Escrowed Encryption Standard in general. Even if we think the banning of crypto will ultimately be a failure ("worse than Prohibition," someone has said), such a ban could make things very uncomfortable for many and would be a serious abridgement of basic liberties.

- We don't know, but we fear something along these lines. It will be difficult to enforce such a ban, as so many avenues for communication exist, and encrypted messages may be hard to detect.
- Their goal, however, may be control and the chilling effect that using "civil forfeiture" may have on potential crypto users. Like the drug laws. (Whit Diffie was the first to emphasize this motivation.)

2.11.3. "How could encryption be banned?"

- most likely way: restrictions on networks, a la airwaves or postal service
- could cite various needs, but absent a mechanism as above, hard to do
- an outright ban, enforced with civil forfeiture penalties
- wartime sorts of policies (crypto treated as sedition, treason...some high-profile prison sentences)
- scenario posted by Sandfort?

2.11.4. "What's the situation about export of crypto?"

- + There's been much debate about this, with the case of Phil Zimmermann possibly being an important test case, should charges be filed.
 - as of 1994-09, the Grand Jury in San Jose has not said anything (it's been about 7-9 months since they started on this issue)
- Dan Bernstein has argued that ITAR covers nearly all aspects of exporting crypto material, including codes, documentation, and even "knowledge." (Controversially, it may be in violation of ITAR for knowledgeable crypto people to even leave the country with the intention of developing crypto tools overseas.)
- The various distributions of PGP that have occurred via anonymous ftp sources don't imply that ITAR is not being enforced, or won't be in the future.

2.11.5. "What's the legal status of digital signatures?"

- Not yet tested in court. Ditto for most crypto protocols, including digital timestamping, electronic contracts, issues of lost keys, etc.

2.11.6. "Can't I just claim I forgot my password?"

2.11.7. "Is it dangerous to talk openly about these ideas?"

- Depends on your country. In some countries, perhaps no. In the U.S., there's not much they can do (though folks should be aware that the Cypherpunks have received a lot of attention by the media and by policy makers, and so a vocal presence on this list very likely puts one on a list of crypto trouble makers).
- Some companies may also feel views expressed here are not consistent with their corporate policies. Your mileage may vary.
- Sedition and treason laws are not likely to be applicable.
- some Cypherpunks think so
- Others of us take the First Amendment pretty seriously: that all talk is permissible

- NSA agents threatened to have Jim Bidzos killed
- 2.11.8. "Does possession of a key mean possession of *identity*?"
 - If I get your key, am I you?
 - Certainly not outside the context of the cryptographic transaction. But within the context of a transaction, yes. Additional safeguards/speedbumps can be inserted (such as biometric credentials, additional passphrases, etc.), but these are essentially part of the "key," so the basic answer remains "yes." (There are periodically concerns raised about this, citing the dangers of having all identity tied to a single credential, or number, or key. Well, there are ways to handle this, such as by adopting protocols that limit one's exposure, that limits the amount of money that can be withdrawn, etc. Or people can adopt protocols that require additional security, time delays, countersigning, etc.)
 - + This may be tested in court soon enough, but the answer for many contracts and crypto transactions will be that possession of key = possession of identity. Even a court test may mean little, for the types of transactions I expect to see.
 - That is, in anonymous systems, "who ya gonna sue?"
 - So, guard your key.

2.12. Digital Cash

2.12.1. "What is digital money?"

2.12.2. "What are the main uses of strong crypto for business and economic transactions?"

- Secure communications. Ensuring privacy of transaction records (avoiding eavesdroppers, competitors)
- Digital signatures on contracts (will someday be standard)
- Digital cash.
- Reputations.
- Data Havens. That bypass local laws about what can be stored and what can't (e.g., silly rules on how far back credit records can go).

2.12.3. "What are smart cards and how are they used?"

- + Most smart cards as they now exist are very far from being the anonymous digital cash of primary interest to us. In fact, most of them are just glorified credit cards.
 - with no gain to consumers, since consumers typically don't pay for losses by fraud
 - (so to entice consumers, will they offer inducements?)
- Can be either small computers, typically credit-card-sized, or just cards that control access via local computers.
- + Tamper-resistant modules, e.g., if tampered with, they destroy the important data or at the least give evidence of having been tampered with.
- + Security of manufacturing
 - some variant of "cut-and-choose" inspection of premises
- + Uses of smart cards
 - conventional credit card uses
 - bill payment
 - postage
 - bridge and road tolls
 - payments for items received electronically (not

necessarily anonymously)

2.13. Crypto Anarchy

2.13.1. "What is Crypto Anarchy?"

- Some of us believe various forms of strong cryptography will cause the power of the state to decline, perhaps even collapse fairly abruptly. We believe the expansion into cyberspace, with secure communications, digital money, anonymity and pseudonymity, and other crypto-mediated interactions, will profoundly change the nature of economies and social interactions.

Governments will have a hard time collecting taxes, regulating the behavior of individuals and corporations (small ones at least), and generally coercing folks when it can't even tell what `_continent_` folks are on!

Read Vinge's "True Names" and Card's "Ender's Game" for some fictional inspirations. "Galt's Gulch" in cyberspace, what the Net is rapidly becoming already.

I call this set of ideas "crypto anarchy" (or "crypto-anarchy," as you wish) and have written about this extensively. The magazines "Wired" (issue 1.2), "Whole Earth Review" (Summer, 1993), and "The Village Voice" (Aug. 6th, 1993) have all carried good articles on this.

2.13.2. The Crypto Anarchist Manifesto

- a complete copy of my 1988 pastiche of the Communisto Manifesto is included in the chapter on Crypto Anarchy.
- it needs rewriting, but for historical sake I've left it unchanged.
- I'm proud that so much of it remains accurate.

2.13.3. "What is BlackNet?"

- BlackNet -- an experiment in information markets, using anonymous message pools for exchange of instructions and items. Tim May's experiment in guerilla ontology.
- BlackNet -- an experimental scheme devised by T. May to underscore the nature of anonymous information markets. "Any and all" secrets can be offered for sale via anonymous mailers and message pools. The experiment was leaked via remailer to the Cypherpunks list (not by May) and thence to several dozen Usenet groups by Detweiler. The authorities are said to be investigating it.

2.13.4. "What effect will crypto have on governments?"

- A huge topic, one I've been thinking about since late 1987 when it dawned on me that public key crypto and anonymous digital cash systems, information markets, etc. meant the end of governments as we know them. (I called this development "crypto anarchy." Not everyone is a fan of it. But it's coming, and fast.)
- "Putting the NSA out of business," as the NYT article put it
- Espionage is changing. To pick one example, "digital dead drops." Any message can be sent through an untraceable path with remailers....and then posted in encrypted form in a newsgroup readable in most countries, including the Former Soviet Union. This means the old stand by of the microfilm

in a Coke can left by a certain tree on a rural road--a method fraught with delays, dangers, and hassles--is now passe. The same message can be send from the comfort of one's home securely and untraceably. Even with a a digital signature to prevent spoofing and disinformation. This spy can be a Lockheed worker on the Aurora program, a SIGINT officer at Woomera, or a disgruntled chip designer at Motorola. (Yes, a countermeasure is to limit access to personal computers, to run only standard software that has no such crypto capability. Such embargoes may already apply to some in sensitive positions, and may someday be a condition of employment.)

- Money-laundering
 - Tax collection. International consultants. Perpetual tourists. Virtual corporations.
 - Terrorism, assassination, crime, Triads, Yakuza, Jamaicans, Russian Mafia...virtual networks... Aryan Nation gone digital
- 2.13.5. "How quickly could something like crypto anarchy come?"
- Parts of it are happening already, though the changes in the world are not something I take any credit for. Rather, there are ongoing changes in the role of nations, of power, and of the ability to coerce behaviors. When people can drop out of systems they don't like, can move to different legal or tax jurisdictions, then things change.
 - + But a phase change could occur quickly, just as the Berlin Wall was impregnable one day, and down the next.
 - "Public anger grows quietly and explodes suddenly. T.C. May's "phase change" may be closer than we think. Nobody in Russia in 1985 really thought the country would fall apart in 6 years." [Mike Ingle, 1994-01-01]
- 2.13.6. "Could strong crypto be used for sick and disgusting and dangerous purposes?"
- Of course. So can locked doors, but we don't insist on an "open door policy" (outside of certain quaint sorority and rooming houses!) So do many forms of privacy allow plotters, molesters, racists, etc. to meet and plot.
 - Crypto is in use by the Aryan Nation, by both pro- and anti-abortion groups, and probably by other kinds of terrorists. Expect more uses in the future, as things like PGP continue to spread.
 - Many of us are explicit anti-democratic, and hope to use encryption to undermine the so-called democratic governments of the world
- 2.13.7. "What is the Dining Cryptographers Problem, and why is it so important?"
- + This is dealt with in the main section, but here's David Chaum's Abstract, from his 1988 paper"
 - Abstract: "Keeping confidential who sends which messages, in a world where any physical transmission can be traced to its origin, seems impossible. The solution presented here is unconditionally or cryptographically secure, depending on whether it is based on one-time-use keys or on public keys. respectively. It can be adapted to address efficiently a wide variety of practical considerations." ["The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," David

Chaum, Journal of Cryptology, I, 1, 1988.]

-
- DC-nets have yet to be implemented, so far as I know, but they represent a "purer" version of the physical remailers we are all so familiar with now. Someday they'll have a major impact. (I'm a bigger fan of this work than many seem to be, as there is little discussion in sci.crypt and the like.)
- 2.13.8. "Why won't government simply ban such encryption methods?"
 - + This has always been the Number One Issue!
 - raised by Stiegler, Drexler, Salin, and several others (and in fact raised by some as an objection to my even discussing these issues, namely, that action may then be taken to head off the world I describe)
 - + Types of Bans on Encryption and Secrecy
 - Ban on Private Use of Encryption
 - Ban on Store-and-Forward Nodes
 - Ban on Tokens and ZKIPS Authentication
 - Requirement for public disclosure of all transactions
 - + Recent news (3-6-92, same day as Michaelangelo and Lawnmower Man) that government is proposing a surcharge on telcos and long distance services to pay for new equipment needed to tap phones!
 - S.266 and related bills
 - this was argued in terms of stopping drug dealers and other criminals
 - but how does the government intend to deal with the various forms of end-user encryption or "confusion" (the confusion that will come from compression, packetizing, simple file encryption, etc.)
 - + Types of Arguments Against Such Bans
 - The "Constitutional Rights" Arguments
 - + The "It's Too Late" Arguments
 - PCs are already widely scattered, running dozens of compression and encryption programs...it is far too late to insist on "in the clear" broadcasts, whatever those may be (is program code distinguishable from encrypted messages? No.)
 - encrypted faxes, modem scramblers (albeit with some restrictions)
 - wireless LANs, packets, radio, IR, compressed text and images, etc....all will defeat any efforts short of police state intervention (which may still happen)
 - + The "Feud Within the NSA" Arguments
 - COMSEC vs. PROD
 - + Will affect the privacy rights of corporations
 - and there is much evidence that corporations are in fact being spied upon, by foreign governments, by the NSA, etc.
 - + They Will Try to Ban Such Encryption Techniques
 - + Stings (perhaps using viruses and logic bombs)
 - or "barium," to trace the code
 - + Legal liability for companies that allow employees to use such methods
 - perhaps even in their own time, via the assumption that employees who use illegal software methods in their own time are perhaps couriers or agents for their

corporations (a tenuous point)

2.13.9. "Could anonymous markets facilitate repugnant services, such as killings for hire?"

- Yes, though there are some things which will help lessen the full impact.
- To make this brutally concrete, here's how escrow makes murder contracts much safer than they are today to negotiate. Instead of one party being caught in an FBI sting, as is so often the case when amateurs try to arrange hits, they can use an escrow service to insulate themselves from:

1. From being traced, because the exchanges are handled via pseudonyms

2. From the killer taking the money and then not performing the hit, because the escrow agent holds the money until the murder is verified (according to some protocol, such as a newspaper report...again, an area for more work, thankfully).

3. From being arrested when the money is picked up, as this is all done via digital cash.

There are some ways to reduce the popularity of this Murder, Incorporated system. (Things I've been thinking about for about 6 years, and which we discussed on the Cypherpunks list and on the Extropians list.)

2.14. Miscellaneous

2.14.1. "Why can't people just agree on an approach?"

- "Why can't everyone just support my proposal?"
- "I've proposed a new cipher, but nobody's interested...you Cypherpunks just never do anything!"
- This is one of the most consistently divisive issues on the list. Often a person will become enamored of some approach, will write posts exhorting others to become similarly enamored, urging others to "do something!", and will then, when no interest is evidenced, become irate. To be more concrete, this happens most often with various and sundry proposals for "digital money." A close second is for various types of "Cypherpunks activism," with proposals that we get together and collect a few million dollars to run Ross Perot-type advertisements urging people to use PGP, with calls for a "Cypherpunks radio show," and so on. (Nothing wrong with people doing these things, I suppose. The problem lies in the exhortation of others to do these things.)
- This collective action is always hard to achieve, and rightly so, in my opinion. Emergent behavior is more natural, and more efficient. And hence better.
- + the nature of markets, agents, different agendas and goals
 - real standards and markets evolve
 - sometimes because of a compelling exemplar (the Walkman, PGP), sometimes because of hard work by standards committees (NTSC, electric sockets, etc.)
 - but almost never by simple appeals to correctness or

ideological rightness

2.14.2. "What are some of the practical limits on the deployment of crypto, especially things like digital cash and remailers?"

+ Lack of reliable services

- Nodes go down, students go home for the summer, downtime for various reasons

- Lack of robustness

2.14.3. "Is crypto dominated by mistrust? I get the impression that everything is predicated on mutual mistrust."

- We lock our doors...does this mean we are lacking in trust?

No, it means we understand there are some out there who will exploit unlocked doors. Ditto for the crypto world.

- "Trust, but verify," as Ronald Reagan used to say. Mutual mistrust can actually make for a more trustworthy environment, paradoxical as that may sound. "Even paranoids have enemies."

- The danger in a trusting environment that lacks other mechanisms is that "predators" or "defectors" (in game-theoretic terms) can exploit this trusting environment. Confidence games, scams, renegeing on deals, and even outright theft.

- Crypto offers the opportunity for "mutually suspicious agents" to interact without explicit "trust."

2.14.4. "Who is Detweiler?"

+ S. Boxx, an12070, ldxxyyy, Pablo Escobar, Hitler, Linda Lollipop, Clew Lance Simpleton, tmp@netcom.com, Jim Riverman

- often with my sig block, or variants of it, attached

- even my phone number

- he lost his ColoState account for such tactics...

- electrocrisis

- cypherwonks

2.14.5. "Who is Sternlight?"

- A retired policy analyst who is often contentious in Usenet groups and supportive of government policies on crypto policy. Not nearly as bad as Detweiler.

2.15. More Information and References

2.15.1. "Where can I find more information?"

- Well, this is a start. Also, lots of other FAQs and Mosaic home pages (URLs) exist, encompassing a vast amount of knowledge.

- As long as this FAQ is, it can only scratch the surface on many topics. (I'm especially amused when someone says they've looked for a FAQ on some obscure topic. No FAQ is likely to answer all questions, especially obscure ones.)

- Many articles and papers are available at the ftp.csua.berkeley.edu site, in pub/cypherpunk. Look around there. The 1981 Chaum paper on untraceable e-mail is not (too many equations for easy scanning), but the 1988 paper on Dining Cryptographers Nets is. (I laboriously scanned it and OCR'd it, back when I used to have the energy to do such thankless tasks.)

+ Some basic sources:

+ Sci.crypt FAQ, published regularly, Also available by anonymous ftp at rtfm.mit.edu. And in various URLs, including:

- URLs for sci.crypt FAQ: xxxxxx
 - RSA Data Security Inc. FAQ
 - Bruce Schneier's "Applied Cryptography" book, 1993. Every reader of this list should get this book!
 - The "online generation" tends to want all material online, I know, but most of the good stuff is to be found in paper form, in journals and books. This is likely to be the case for many years to come, given the limitation of ASCII, the lack of widespread standards (yes, I know about LaTeX, etc.), and the academic prestige associated with bound journals and books. Fortunately, you can all find universit libraries within driving range. Take my advice: if you do not spend at least an entire Saturday immersing yourself in the crypto literature in the math section of a large library, perusing the "Proceedings of the Crypto Conference" volumes, scanning the textbooks, then you have a poor foundation for doing any crypto work.
- 2.15.2. "Things are changing quickly. Not all of the addresses and URLs given here are valid. And the software versions... How do I get the latest information?"
- Yes, things are changing quickly. This document can't possibly keep up with the rapid changes (nor can its author!).
 - Reading the various newsgroups is, as always, the best way to hear what's happening on a day to day basis. Web pages, gopher, archie, veronica, etc. should show the latest versions of popular software packages.
- 2.15.3. "FUQs: "Frequently Unanswered Questions"?"
- (more to be added)
 - With 700 or more people on the Cypherpunks list (as of 94-09), it is inevitable that some FAQs will go unanswered when newbies (or others) ask them. Sometimes the FUQs are ignored because they're so stale, other times because to answer them is to continue and unfruitful thread.
- + "P = NP?"
- Steve Smale has called this the most important new unsolved problem of the past half-century.
 - If P were (unexpectedly) proved to be NP
- + Is RSA and factoring in NP?
- not yet proved
 - factoring might be easier
 - and RSA might be easier than factoring in general (e.g., chosen- and known-plaintext may provide clues)
- "Will encryption be outlawed? What will happen?"
- + "Is David Sternlight an NSA agent?"
- Seriously, David S. is probably what he claims: a retired economist who was once very senior in government and corporate policy circles. I have no reason to doubt him.
 - He has views at odds with most of us, and a baiting style of expressing his views, but this does not mean he is a government agent as so many people claim.
 - Not in the same class as Detweiler.

3. Cypherpunks -- History, Organization, Agenda

3.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666,

1994-09-10, Copyright Timothy C. May. All rights reserved.
See the detailed disclaimer. Use short sections under "fair
use" provisions, with appropriate credit, but don't put your
name on my words.

3.2. SUMMARY: Cypherpunks -- History, Organization, Agenda

3.2.1. Main Points

- Cypherpunks formed in September, 1992
- formed at an opportune time, with PGP 2.0, Clipper, etc.
hitting
- early successes: Cypherpunks remailers, publicity

3.2.2. Connections to Other Sections

3.2.3. Where to Find Additional Information

- "Wired," issue 1.2, had a cover story on Cypherpunks.
- "Whole Earth Review," Summer 1993, had a long article on
crypto and Cypherpunks (included in the book "Out of
Control," by Kevin Kelly.
- "Village Voice," August 6th (?). 1993, had cover story on
"Crypto Rebels" (also reprinted in local weeklies)
- and numerous articles in various magazines

3.2.4. Miscellaneous Comments

- the best way to get a feel for the List is to simply read
it for a while; a few months should do.

3.3. The Cypherpunks Group and List

3.3.1. What is it?

- + Formal Rules, Charter, etc.?
 - no formal rules or charter
 - no agreed-upon mission

3.3.2. "Who are the Cypherpunks?"

- A mix of about 500-700
- + Can find out who by sending message to majordomo@toad.com
with the message body text "who cypherpunks" (no quotes, of
course).
 - Is this a privacy flaw? Maybe.
- Lots of students (they have the time, the Internet
accounts). Lots of computer science/programming folks. Lots
of libertarians.
- quote from Wired article, and from "Whole Earth Review"

3.3.3. "How did the Cypherpunks group get started?"

- + History?
 - Discussions between Eric Hughes and me, led to Eric's
decision to host a gathering
- + First meeting was, by coincidence, the same week that PGP
2.0 was released...we all got copies that day
 - morning session on basics
 - sitting on the floor
- + afternoon we played the "Crypto Game"
 - remailers, digital money, information for sale, etc.
- John Gilmore offered his site to host a mailing list, and
his company's offices to hold monthly meetings
- The mailing list began almost immediately
- The Name "Cypherpunks"?

3.3.4. "Should I join the Cypherpunks mailing list?"

- If you are reading this, of course, you are most likely on
the Cypherpunks list already and this point is moot--you
may instead be asking if you should_leave_ the List!

- Only if you are prepared to handle 30-60 messages a day, with volumes fluctuating wildly
- 3.3.5. "How can I join the Cypherpunk mailing list?"
 - send message to "majordomo@toad.com" with a `_body_text` of "subscribe cypherpunks" (no quote marks in either, of course).
- 3.3.6. "Membership?"
 - about 500-700 at any given time
 - many folks join, are overwhelmed, and quit
 - other groups: Austin, Colorado, Boston, U.K.
- 3.3.7. "Why are there so many libertarians on the Cypherpunks list?"
 - + The same question is often asked about the Net in general. Lots of suggested reasons:
 - A list like Cypherpunks is going to have privacy and freedom advocates. Not all privacy advocates are libertarians (e.g., they may want laws restricting data collection), but many are. And libertarians naturally gravitate to causes like ours.
 - Net grew anarchically, with little control. This appeals to free-wheeling types, used to making their own choices and building their own worlds.
 - Libertarians are skeptical of central control structures, as are most computer programming types. They are skeptical that a centrally-run control system can coordinate the needs and desires of people. (They are of course more than just "skeptical" about this.)
 - In any case, there's not much of a coherent "opposition camp" to the anarcho-capitalist, libertarian ideology. Forgive me for saying this, my non-libertarian friends on the list, but most non-libertarian ideologies I've seen expressed on the list have been fragmentary, isolated, and not coherent...comments about "how do we take care of the poor?" and Christian fundamentalism, for example. If there is a coherent alternative to a basically libertarian viewpoint, we haven't seen it on the list.
 - (Of course, some might say that the libertarians outshout the alternatives...I don't think this is really so.)
- 3.3.8. "How did the mailing list get started?"
 - Hugh Daniel, Eric Hughes, and I discussed this the day after the first meeting
 - mailing list brought together diverse interests
 - How to hoin?
- 3.3.9. "How did Cypherpunks get so much early publicity?"
 - started at the right time, just as PGP was gaining popularity, as plans for key escrow were being laid (I sounded an alarm in October, 1992, six months before the Clipper announcement), and just as "Wired" was preparing its first issue
 - Kevin Kelly and Steven Levy attended some of our early meetings, setting the stage for very favorable major stories in "Wired" (issue 1.2, the cover story), and "Whole Earth Review" (Summer, 1993)
 - a niche for a "renegade" and "monkey-wrenching" group, with less of a Washington focus
 - publicity in "Wired," "The Whole Earth Review," "The Village Voice"
 - + Clipper bombshell occupied much of our time, with some

- effect on policy
 - climate of repudiation
 - links to EFF, CPSR, etc.
- 3.3.10. "Why the name?"
 - Jude Milhon nicknames us
 - cypherpunkts? (by analogy with Mikropunkts, microdots)
- 3.3.11. "What were the early meetings like?"
 - cypherspiel, Crypto Anarchy Game
- 3.3.12. "Where are places that I can meet other Cypherpunkts?"
 - physical meetings
 - start your own...pizza place, classroom
 - + other organizations
 -
 - + "These kind of meetings (DC 2600 meeting at Pentagon City Mall, 1st Fri. of
 - every month in the food court, about 5-7pm or so) might be good places for
 - local cypherpunkts gatherings as well. I'm sure there are a lot of other
 - such meetings, but the DC and Baltimore ones are the ones I know of. <Stanton McCandlish, 7 April 1994>
 - (note that the DC area already meets...)
 - Hackers, raves
 - regional meetings
- 3.3.13. "Is the Cypherpunkts list monitored? Has it been infiltrated?"
 - Unknown. It wouldn't be hard for anyone to be monitoring the list.
 - As to infiltration, no evidence for this. No suspicious folks showing up at the physical meetings, at least so far as I can see. (Not a very reliable indication.)
- 3.3.14. "Why isn't there a recruiting program to increase the number of Cypherpunkts?"
 - Good question. The mailing list reached about 500 subscribers a year or so ago and has remained relatively constant since then; many subscribers learned of the list and its address in the various articles that appeared.
 - Informal organizations often level out in membership because no staff exists to publicize, recruit, etc. And size is limited because a larger group loses focus. So, some stasis is achieved. For us, it may be at the 400-700 level. It seems unlikely that list membership would ever get into the tens of thousands.
- 3.3.15. "Why have there been few real achievements in crypto recently?"
 - + Despite the crush of crypto releases--the WinPGPs, SecureDrives, and dozen other such programs--the fact is that most of these are straightforward variants on what I think have been the two major product classes to be introduced in the last several years"
 - PGP, and variants.
 - Remailers, and variants.
 - These two main classes account for about 98% of all product- or version-oriented debate on the Net, epitomized by the zillions of "Where can I find PGP2.6ui for the Amiga?" sorts of posts.
 - + Why is this so? Why have these dominated? What else is needed?

- + First, PGP gave an incredible impetus to the whole issue of public use of crypto. It brought crypto to the masses, or at least to the Net-aware masses. Second, the nearly simultaneous appearance of remailers (the Kleinpaste/Julf-style and the Cypherpunks "mix"-style) fit in well with the sudden awareness about PGP and crypto issues. And other simultaneous factors appeared:
 - the appearance of "Wired" and its spectacular success, in early 1993
 - the Clipper chip firestorm, beginning in April 1993
 - the Cypherpunks group got rolling in late 1992, reaching public visibility in several articles in 1993. (By the end of '93, we seemed to be a noun, as Bucky might've said.)
- + But why so little progress in other important areas?
 - digital money, despite at least a dozen reported projects, programs (only a few of which are really anything like Chaum's "digital cash")
 - data havens, information markets, etc.
 - money-laundering schemes, etc.
- + What could change this?
 - Mosaic, WWW, Web
 - A successful digital cash effort

3.4. Beliefs, Goals, Agenda

3.4.1. "Is there a set of beliefs that most Cypherpunks support?"

- + There is nothing official (not much is), but there is an emergent, coherent set of beliefs which most list members seem to hold:
 - * that the government should not be able to snoop into our affairs
 - * that protection of conversations and exchanges is a basic right
 - * that these rights may need to be secured through technology rather than through law
 - * that the power of technology often creates new political realities (hence the list mantra: "Cypherpunks write code")
- + Range of Beliefs
 - Many are libertarian, most support rights of privacy, some are more radical in approach

3.4.2. "What are Cypherpunks interested in?"

- privacy
- technology
- encryption
- politics
- crypto anarchy
- digital money
- protocols

3.4.3. Personal Privacy and Collapse of Governments

- There seem to be two main reasons people are drawn to Cypherpunks, besides the general attractiveness of a "cool" group such as ours. The first reason is personal privacy. That is, tools for ensuring privacy, protection from a surveillance society, and individual choice. This reason is widely popular, but is not always compelling (after all, why worry about personal privacy and then join a list that

has been identified as a "subversive" group by the Feds?
Something to think about.)

- The second major is personal liberty through reducing the power of governments to coerce and tax. Sort of a digital Galt's Gulch, as it were. Libertarians and anarchocapitalists are especially drawn to this vision, a vision which may bother conventional liberals (when they realize strong crypto means things counter to welfare, AFDC, antidiscrimination laws....).
- This second view is more controversial, but is, in my opinion, what really powers the list. While others may phrase it differently, most of us realize we are on to something that will change--and already is changing--the nature of the balance of power between individuals and larger entities.

3.4.4. Why is Cypherpunks called an "anarchy"?

- Anarchy means "without a leader" (head). Much more common than people may think.
- The association with bomb-throwing "anarchists" is misleading.

3.4.5. Why is there no formal agenda, organization, etc.?

- no voting, no organization to administer such things
- "if it ain't broke, don't fix it"
- and it's how it all got started and evolved
- also, nobody to arrest and hassle, no nonsense about filling out forms and getting tax exemptions, no laws about campaign law violations (if we were a formal group and lobbied against Senator Foo, could be hit with the law limiting "special interests," conceivably)

3.4.6. How are projects proposed and completed?

- If an anarchy, how do things get done?
- The way most things get done: individual actions and market decisions.

3.4.7. Future Needs for Cyberspace

- + Mark Pesci's ideas for VR and simulations
 - distributed, high bandwidth
 - a billion users
 - spatial ideas....coordinates...servers...holographic models
 - WWW plus rendering engine = spatial VR (Library of Congress)
 - "The Labyrinth"
- + says to avoid head-mounted displays and gloves (bad for you)
 - + instead, "perceptual cybernetics".
 - phi--fecks--psi (phi is external world, Fx = facts are effectuators and sensors, psi is your internal state)

3.4.8. Privacy, Credentials without identity

3.4.9. "Cypherpunks write code"

- "Cypherpunks break the laws they don't like"
- "Don't get mad, get even. Write code."

3.4.10. Digital Free Markets

- + strong crypto changes the nature and visibility of many economic transactions, making it very difficult for governments to interfere or even to enforce laws, contracts, etc.
- thus, changes in the nature of contract enforcement

- + (Evidence that this is not hopeless can be found in several places:
 - criminal markets, where governments obviously cannot be used
 - international markets, a la "Law Merchant"
- "uttering a check"
- shopping malls in cyberspace...no identifiable national or regional jurisdiction...overlapping many borders...
- + caveat emptor (though rating agencies, and other filter agents, may be used by wary customers...ironically, reputation will matter even more than it now does)
 - no ability to repudiate a sale, to be an Indian giver
- in all kinds of information....
- 3.4.11. The Role of Money
 - in monetarizing transactions, access, remailers---digital postage
- 3.4.12. Reductions on taxation
 - offshore entities already exempt
 - tax havens
 - cyberspace localization is problematic
- 3.4.13. Transnationalism
 - rules of nations are ignored
- 3.4.14. Data Havens
 - credit, medical, legal, renter, etc.
- 3.4.15. MOOs, MUDs, SVRs, Habitat cyberspaces
 - "True Names" and "Snow Crash"
 - What are
 - + Habitat....Chip and Randy
 - Lucasfilm, Fujitsu
 - started as game environment...
 - many-user environments
 - communications bandwidth is a scarce resource
 - object-oriented data representation
 - + implementation platform unimportant...range of capabilities
 - pure text to Real ity Engines
 - never got as far as fully populating the reality
 - "detailed central planning is impossible; don't even try"
 - 2-D grammar for layouts
 - + "can't trust anyone"
 - someone disassembled the code and found a way to make themselves invisible
 - ways to break the system (extra money)
 - + future improvements
 - multimedia objects, customizable objects, local turfs, multiple interfaces
 - "Global Cyberspace Infrastructure" (Fujitsu, FINE)
 - + more bandwidth means more things can be done
 - B-ISDN will allow video on demand, VR, etc.
 - protocol specs, Joule (secure concurrent operating system)
 - interreaction spaces, topological (not spatial)
- + Xerox, Pavel Curtis
 - + LambdaMOO
 - 1200 different users per day, 200 at a time, 5000 total users
 - "social virtual realities"--virtual communities

- how emergent properties emerge
- pseudo-spatial
- rooms, audio, video, multiple screens
- policing, wizards, mediation
- effective telecommuting
- need the richness of real world markets...people can sell to others
- + Is there a set of rules or basic ideas which can form the basis of a powerfully replicable system?
 - this would allow franchises to be distributed around the world
 - networks of servers? distinction between server and client fades...
 - money, commercialization?
 - Joule language
- 3.4.16. "Is personal privacy the main interest of Cypherpunks?"
 - Ensuring the right and the technological feasibility is more of the focus. This often comes up in two contexts:
 1. Charges of hypocrisy because people either use pseudonyms or, paradoxically, that they don't use pseudonyms, digital signatures
- 3.4.17. "Shouldn't crypto be regulated?"
 - Many people make comparisons to the regulation of automobiles, of the radio spectrum, and even of guns. The comparison of crypto to guns is especially easy to make, and especially dangerous.
 -
 - + A better comparison is "use of crypto = right to speak as you wish."
 - That is, we cannot demand that people speak in a language or form that is easily understandable by eavesdroppers, wiretappers, and spies.
 - + If I choose to speak to my friends in Latvian, or in Lithuanian, or in
 - triple DES, that's my business. (Times of true war, as in World War
 - II, may be slightly different. As a libertarian, I'm not advocating
 - that, but I understand the idea that in times of war speaking in code
 - + is suspect. We are not in a time of war, and haven't been.)
 -
 - Should we have "speech permits"? After all, isn't the regulation of
 - + speech consistent with the regulation of automobiles?
 -
 - I did a satirical essay along these lines a while back. I won't
 - included it here, though. (My speech permit for satire expired and I
 - + haven't had time to get it renewed.)
 -
 - In closing, the whole comparison of cryptography to armaments is
 - misleading. Speaking or writing in forms not readily understandable to

- your enemies, your neighbors, your spouse, the cops, or your local
 - eavesdropper is as old as humanity.
- 3.4.18. Emphasize the "voluntary" nature of crypto
- + those that don't want privacy, can choose not to use crypto
 - just as they can take the locks of their doors, install wiretaps on their phones, remove their curtains so as not to interfere with peeping toms and police surveillance teams, etc.
 - as PRZ puts it, they can write all their letters on postcards, because they have "nothing to hide"
 - what we want to make sure doesn't happen is others insisting that we cannot use crypto to maintain our own privacy
 - + "But what if criminals have access to crypto and can keep secrets?"
 - this comes up over and over again
 - does this mean locks should not exist, or.....?
- 3.4.19. "Are most Cypherpunks anarchists?"
- Many are, but probably not most. The term "anarchy" is often misunderstood.
 - As Perry Metzger puts it "Now, it happens that I am an anarchist, but that isn't what most people associated with the term "cypherpunk" believe in, and it isn't fair to paint them that way -- hell, many people on this mailing list are overtly hostile to anarchism." [P.M., 1994-07-01]
 - comments of Sherry Mayo, others
 - But the libertarian streak is undeniably strong. And libertarians who think about the failure of politics and the implications of cryptgraphy generally come to the anarcho-capitalist or crypto-anarchist point of view.
 - In any case, the "other side" has not been very vocal in espousing a consistent ideology that combines strong crypto and things like welfare, entitlements, and high tax rates. (I am not condemning them. Most of my leftist friends turn out to believe in roughly the same things I believe in...they just attach different labels and have negative reactions to words like "capitalist.")
- 3.4.20. "Why is there so much ranting on the list?"
- Arguments go on and on, points get made dozens of times, flaming escalates. This has gotten to be more of a problem in recent months. (Not counting the spikes when Detweiler was around.)
 - + Several reasons:
 - + the arguments are often matters of opinion, not fact, and hence people just keep repeating their arguments
 - made worse by the fact that many people are too lazy to do off-line reading, to learn about what they are expressing an opinion on
 - since nothing ever gets resolved, decided, vote upon, etc., the debates continue
 - since anyone is free to speak up at any time, some people will keep making the same points over and over again, hoping to win through repetition (I guess)
 - + since people usually don't personally know the other members of the list, this promotes ranting (I've noticed that the people who know each other, such as the Bay Area

folks, tend not to be as rude to each other...any sociologist or psychologist would know why this is so immediately).

- + the worst ranters tend to be the people who are most isolated from the other members of the list community; this is generally a well-known phenomenon of the Net
 - and is yet more reason for regional Cypherpunks groups to occasionally meet, to at least make some social and conversational connections with folks in their region.
 - on the other hand, rudeness is often warranted; people who assault me and otherwise plan to deprive me of my property of deserving of death, not just insults [Don't be worried, there are only a handful of people on this list I would be happy to see dead, and on none of them would I expend the \$5000 it might take to buy a contract. Of course, rates could drop.]
- 3.4.21. The "rejectionist" stance so many Cypherpunks have
- that compromise rarely helps when very basic issues are involved
 - the experience with the NRA trying compromise, only to find ever-more-repressive laws passed
 - the debacle with the EFF and their "EFF Digital Telephony Bill" ("We couldn't have put this bill together without your help") shows the corruption of power; I'm ashamed to have ever been a member of the EFF, and will of course not be renewing my membership.
 - I have jokingly suggested we need a "Popular Front for the Liberation of Crypto," by analogy with the PFLP.
- 3.4.22. "Is the Cypherpunks group an illegal or seditious organization?"
- Well, there are those "Cypherpunk Criminal" t-shirts a lot of us have...
 - Depends on what country you're in.
 - Probably in a couple of dozen countries, membership would be frowned on
 - the material may be illegal in other countries
 - and many of us advocate things like using strong crypto to avoid and evade txxes, to bypass laws we dislike, etc.
- 3.5. Self-organizing Nature of Cypherpunks
- 3.5.1. Contrary to what people sometimes claim, there is no ruling clique of Cypherpunks. Anybody is free to do nearly anything, just not free to commit others to course of action, or control the machine resources the list now runs on, or claim to speak for the "Cypherpunks" as a group (and this last point is unenforceable except through reputation and social repercussions).
- 3.5.2. Another reason to be glad there is no formal Cypherpunks structure, ruling body, etc., is that there is then no direct target for lawsuits, ITAR violation charges, defamation or copyright infringement claims, etc.
- 3.6. Mechanics of the List
- 3.6.1. Archives of the Cypherpunks List
- Karl Barrus has a selection of posts at the site chaos.bsu.edu, available via

- gopher. Look in the "Cypherpunks gopher site" directory.
- 3.6.2. "Why isn't the list sent out in encrypted form?"
- Too much hassle, no additional security, would only make people jump through extra hoops (which might be useful, but probably not worth the extra hassle and ill feelings).
 - "We did this about 8 years ago at E&S using DEC VMS NOTES. We used a plain vanilla secret key algorithm and a key shared by all legitimate members of the group. We could do it today -- but why bother? If you have a key that widespread, it's effectively certain that a "wrong person" (however you define him/her) will have a copy of the key." [Carl Ellison, Encrypted BBS?, 1993-08-02]
- 3.6.3. "Why isn't the list moderated?"
- This usually comes up during severe flaming episodes, notably when Detweiler is on the list in one of his various personnas. Recently, it has not come up, as things have been relatively quiet.
 - + Moderation will *not* happen
 - nobody has the time it takes
 - nobody wants the onus
 - + hardly consistent with many of our anarchist leanings, is it?
 - (Technically, moderation can be viewed as "my house, my rules, and hence OK, but I think you get my point.)
 - "No, please let's not become a 'moderated' newsgroup. This would be the end of freedom! This is similar to giving the police more powers because crime is up. While it is a tactic to fight off the invaders, a better tactic is knowledge." [RWGreene@vnet.net, alt.gathering.rainbow, 1994-07-06]"
- 3.6.4. "Why isn't the list split into smaller lists?"
- What do you call the list outages?
 - + Seriously, several proposals to split the list into pieces have resulted in not much
 - a hardware group...never seen again, that I know of
 - a "moderated cryptography" group, ditto
 - a DC-Net group...ditto
 - several regional groups and meeting planning groups, which are apparently moribund
 - a "Dig Lib" group...ditto
 - use Rishab's comment:
 - + Reasons are clear: one large group is more successful in traffic than smaller, low-volume groups...out of sight, out of mind
 - and topics change anyway, so the need for a "steganography" mailing list (argued vehemently for by one person, not Romana M., by the way) fades away when the debate shifts. And so on.
- 3.6.5. Critical Addresses, Numbers, etc.
- + Cypherpunks archives sites
 - soda
 - mirror sites
 - ftp sites
 - PGP locations
 - Infobot at Wired
 - majordomo@toad.com; "help" as message body
- 3.6.6. "How did the Cypherpunk remailers appear so quickly?"

- remailers were the first big win...a weekend of Perl hacking

3.7. Publicity

3.7.1. "What kind of press coverage have the Cypherpunks gotten?"

- " I concur with those who suggest that the solution to the ignorance manifested in many of the articles concerning the Net is education. The coverage of the Cypherpunks of late (at least in the Times) shows me that reasonable accuracy is possible." [Chris Walsh, news.admin.policy, 1994-07-04]

3.8. Loose Ends

3.8.1. On extending the scope of Cypherpunks to other countries

- a kind of crypto underground, to spread crypto tools, to help sow discord, to undermine corrupt governments (to my mind, all governments now on the planet are intrinsically corrupt and need to be undermined)
- links to the criminal underworlds of these countries is one gutsy thing to consider....fraught with dangers, but ultimately destabilizing of governments

4. Goals and Ideology -- Privacy, Freedom, New Approaches

4.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

4.2. SUMMARY: Goals and Ideology -- Privacy, Freedom, New Approaches

4.2.1. Main Points

4.2.2. Connections to Other Sections

- Crypto Anarchy is the logical outgrowth of strong crypto.

4.2.3. Where to Find Additional Information

- Vernor Vinge's "True Names"
- David Friedman's "Machinery of Freedom"

4.2.4. Miscellaneous Comments

- Most of the list members are libertarians, or leaning in that direction, so the bias toward this is apparent.
- (If there's a coherent _non_-libertarian ideology, that's also consistent with supporting strong crypto, I'm not sure it's been presented.)

4.3. Why a Statement of Ideology?

4.3.1. This is perhaps a controversial area. So why include it? The main reason is to provide some grounding for the later comments on many issues.

4.3.2. People should not expect a uniform ideology on this list.

Some of us are anarcho-capitalist radicals (or "crypto anarchists"), others of us are staid Republicans, and still others are Wobblies and other assorted leftists.

4.4. "Welcome to Cypherpunks"

4.4.1. This is the message each new subscriber to the Cypherpunks lists gets, by Eric Hughes:

4.4.2. "Cypherpunks assume privacy is a good thing and wish there

were more of it. Cypherpunks acknowledge that those who want privacy must create it for themselves and not expect governments, corporations, or other large, faceless organizations to grant them privacy out of beneficence. Cypherpunks know that people have been creating their own privacy for centuries with whispers, envelopes, closed doors, and couriers. Cypherpunks do not seek to prevent other people from speaking about their experiences or their opinions.

"The most important means to the defense of privacy is encryption. To encrypt is to indicate the desire for privacy. But to encrypt with weak cryptography is to indicate not too much desire for privacy. Cypherpunks hope that all people desiring privacy will learn how best to defend it.

"Cypherpunks are therefore devoted to cryptography. Cypherpunks wish to learn about it, to teach it, to implement it, and to make more of it. Cypherpunks know that cryptographic protocols make social structures. Cypherpunks know how to attack a system and how to defend it. Cypherpunks know just how hard it is to make good cryptosystems.

"Cypherpunks love to practice. They love to play with public key cryptography. They love to play with anonymous and pseudonymous mail forwarding and delivery. They love to play with DC-nets. They love to play with secure communications of all kinds.

"Cypherpunks write code. They know that someone has to write code to defend privacy, and since it's their privacy, they're going to write it. Cypherpunks publish their code so that their fellow cypherpunks may practice and play with it. Cypherpunks realize that security is not built in a day and are patient with incremental progress.

"Cypherpunks don't care if you don't like the software they write. Cypherpunks know that software can't be destroyed. Cypherpunks know that a widely dispersed system can't be shut down.

"Cypherpunks will make the networks safe for privacy." [Eric Hughes, 1993-07-21 version]

4.5. "Cypherpunks Write Code"

4.5.1. "Cypherpunks write code" is almost our mantra.

4.5.2. This has come to be a defining statement. Eric Hughes used it to mean that Cypherpunks place more importance in actually changing things, in actually getting working code out, than in merely talking about how things "ought" to be.

- Eric Hughes statement needed here:
- Karl Kleinpaste, author of one of the early anonymous posting services (Charcoal) said this about some proposal made: "If you've got serious plans for how to implement such a thing, please implement it at least skeletally and deploy it. Proof by example, watching such a system in

action, is far better than pontification about it."

[Karl_Kleinpaste@cs.cmu.edu, news.admin.policy, 1994-06-30]

4.5.3. "The admonition, "Cypherpunks write code," should be taken metaphorically. I think "to write code" means to take unilateral effective action as an individual. That may mean writing actual code, but it could also mean dumpster diving at Mycrotronx and anonymously releasing the recovered information. It could also mean creating an offshore digital bank. Don't get too literal on us here. What is important is that Cypherpunks take personal responsibility for empowering themselves against threats to privacy." [Sandy Sandfort, 1994-07-08]

4.5.4. A Cypherpunks outlook: taking the abstractions of academic conferences and making them concrete

- One thing Eric Hughes and I discussed at length (for 3 days of nearly nonstop talk, in May, 1992) was the glacial rate of progress in converting the cryptographic primitive operations of the academic crypto conferences into actual, workable code. The basic RSA algorithm was by then barely available, more than 15 years after invention. (This was before PGP 2.0, and PGP 1.0 was barely available and was disappointing, with RSA Data Security's various products in limited niches.) All the neat stuff on digital cash, DC-Nets, bit commitment, olivious transfer, digital mixes, and so on, was completely absent, in terms of available code or "crypto ICs" (to borrow Brad Cox's phrase). If it took 10-15 years for RSA to really appear in the real world, how long would it take some of the exciting stuff to get out?
- We thought it would be a neat idea to find ways to reify these things, to get actual running code. As it happened, PGP 2.0 appeared the week of our very first meeting, and both the Kleinpaste/Julf and Cypherpunks remailers were quick, if incomplete, implementations of David Chaum's 1981 "digital mixes." (Right on schedule, 11 years later.)
- Sadly, most of the abstractions of cryptology remain residents of academic space, with no (available) implementations in the real world. (To be sure, I suspect many people have cobbled-together versions of many of these things, in C code, whatever. But their work is more like building sand castles, to be lost when they graduate or move on to other projects. This is of course not a problem unique to cryptology.)
- Today, various toolkits and libraries are under development. Henry Strickland (Strick) is working on a toolkit based on John Ousterhout's "TCL" system (for Unix), and of course RSADSI provides RSAREF. Product Cypher has "PGP Tools." Other projects are underway. (My own longterm interest here is in building objects which act as the cryptography papers would have them act...building block objects. For this, I'm looking at Smalltalk of some flavor.)
- It is still the case that most of the modern crypto papers discuss theoretical abstractions that are not even close to being implemented as reusable, robust objects or routines. Closing the gap between theoretical papers and practical realization is a major Cypherpunk emphasis.

4.5.5. Prototypes, even if fatally flawed, allow for evolutionary learning and improvement. Think of it as engineering in action.

4.6. Technological empowerment

4.6.1. (more needed here....)

4.6.2. As Sandy Sandfort notes, "The real point of Cypherpunks is that it's better to use strong crypto than weak crypto or no crypto at all. Our use of crypto doesn't have to be totally bullet proof to be of value. Let *them* worry about the technicalities while we make sure they have to work harder and pay more for our encrypted info than they would if it were in plaintext." [S.S. 1994-07-01]

4.7. Free Speech Issues

4.7.1. Speech

- "Public speech is not a series of public speeches, but rather one's own words spoken openly and without shame....I desire a society where all may speak freely about whatever topic they will. I desire that all people might be able to choose to whom they wish to speak and to whom they do not wish to speak. I desire a society where all people may have an assurance that their words are directed only at those to whom they wish. Therefore I oppose all efforts by governments to eavesdrop and to become unwanted listeners." [Eric Hughes, 1994-02-22]
- "The government has no right to restrict my use of cryptography in any way. They may not forbid me to use whatever ciphers I may like, nor may they require me to use any that I do not like." [Eric Hughes, 1993-06-01]

4.7.2. "Should there be any limits whatsoever on a person's use of cryptography?"

- No. Using the mathematics of cryptography is merely the manipulation of symbols. No crime is involved, ipso facto.
- Also, as Eric Hughes has pointed out, this is another of those questions where the normative "should" or "shouldn't" invokes "the policeman inside." A better way to look at is to see what steps people can take to make any question of "should" this be allowed just moot.
- The "crimes" are actual physical acts like murder and kidnapping. The fact that crypto may be used by plotters and planners, thus making detection more difficult, is in no way different from the possibility that plotters may speak in an unusual language to each other (ciphers), or meet in a private home (security), or speak in a soft voice when in public (steganography). None of these things should be illegal, and *none of them would be enforceable* except in the most rigid of police states (and probably not even there).
- "Crypto is thoughtcrime" is the effect of restricting cryptography use.

4.7.3. Democracy and censorship

- Does a community have the right to decide what newsgroups or magazines it allows in its community? Does a nation have the right to do the same? (Tennessee, Iraq, Iran, France. Utah?)

- This is what bypasses with crypto are all about: taking these majoritarian morality decisions out of the hands of the bluenoses. Direct action to secure freedoms.

4.8. Privacy Issues

4.8.1. "Is there an agenda here beyond just ensuring privacy?"

- Definitely! I think I can safely say that for nearly all political persuasions on the Cypherpunks list. Left, right, libertarian, or anarchist, there's much more to strong crypto than simple privacy. Privacy qua privacy is fairly uninteresting. If all one wants is privacy, one can simply keep to one's self, stay off high-visibility lists like this, and generally stay out of trouble.
- Many of us see strong crypto as the key enabling technology for a new economic and social system, a system which will develop as cyberspace becomes more important. A system which dispenses with national boundaries, which is based on voluntary (even if anonymous) free trade. At issue is the end of governments as we know them today. (Look at interactions on the Net--on this list, for example--and you'll see many so-called nationalities, voluntary interaction, and the almost complete absence of any "laws." Aside from their being almost no rules per se for the Cypherpunks list, there are essentially no national laws that are invocable in any way. This is a fast-growing trend.)

+ Motivations for Cypherpunks

- Privacy. If maintaining privacy is the main goal, there's not much more to say. Keep a low profile, protect data, avoid giving out personal information, limit the number of bank loans and credit applications, pay cash often, etc.
- Privacy in activism.
- + New Structures. Using cryptographic constructs to build new political, economic, and even social structures.
 - Political: Voting, polling, information access, whistleblowing
 - Economic: Free markets, information markets, increased liquidity, black markets
 - Social: Cyberspatial communities, True Names
- Publically inspectable algorithms always win out over private, secret algorithms

4.8.2. "What is the American attitude toward privacy and encryption?"

- + There are two distinct (and perhaps simultaneously held) views that have long been found in the American psyche:
 - "A man's home is his castle." "Mind your own business." The frontier and Calvinist sprit of keeping one's business to one's self.
 - "What have you got to hide?" The nosiness of busybodies, gossiping about what others are doing, and being suspicious of those who try too hard to hide what they are doing.
- + The American attitude currently seems to favor privacy over police powers, as evidenced by a Time-CNN poll:
 - "In a Time/CNN poll of 1,000 Americans conducted last week by Yankelovich Partners, two-thirds said it was more

important to protect the privacy of phone calls than to preserve the ability of police to conduct wiretaps. When informed about the Clipper Chip, 80% said they opposed it." [Philip Elmer-Dewitt, "Who Should Keep the Keys," TIME, 1994-03-04.]

- The answer given is clearly a function of how the question is phrased. Ask folks if they favor "unbreakable encryption" or "fortress capabilities" for terrorists, pedophiles, and other malefactors, and they'll likely give a quite different answer. It is this tack now being taken by the Clipper folks. Watch out for this!
- Me, I have no doubts.
- As Perry Metzger puts it, "I find the recent disclosures concerning U.S. Government testing of the effects of radiation on unknowing human subjects to be yet more evidence that you simply cannot trust the government with your own personal safety. Some people, given positions of power, will naturally abuse those positions, often even if such abuse could cause severe injury or death. I see little reason, therefore, to simply "trust" the U.S. government -- and given that the U.S. government is about as good as they get, its obvious that NO government deserves the blind trust of its citizens. "Trust us, we will protect you" rings quite hollow in the face of historical evidence. Citizens must protect and preserve their own privacy -- the government and its centralized cryptographic schemes emphatically cannot be trusted." [P.M., 1994-01-01]

4.8.3. "How is 1994 like 1984?"

- The television ad for Clipper: "Clipper--why 1994 will be like 1984"
- + As Mike Ingle puts it:
 - 1994: Wiretapping is privacy
 - Secrecy is openness
 - Obscurity is security

4.8.4. "We anticipate that computer networks will play a more and more important role in many parts of our lives. But this increased computerization brings tremendous dangers for infringing privacy. Cypherpunks seek to put into place structures which will allow people to preserve their privacy if they choose. No one will be forced to use pseudonyms or post anonymously. But it should be a matter of choice how much information a person chooses to reveal about himself when he communicates. Right now, the nets don't give you that much choice. We are trying to give this power to people." [Hal Finney, 1993-02-23]

4.8.5. "If cypherpunks contribute nothing else we can create a real privacy advocacy group, advocating means of real self-empowerment, from crypto to nom de guerre credit cards, instead of advocating further invasions of our privacy as the so-called privacy advocates are now doing!" [Jim Hart, 1994-09-08]

4.9. Education Issues

4.9.1. "How can we get more people to use crypto?"

- telling them about the themes of Cypherpunks
- surveillance, wiretapping, Digital Telephony, Clipper, NSA, FinCEN, etc....these things tend to scare a lot of folks

- making PGP easier to use, better integration with mailers, etc.
- (To be frank, convincing others to protect themselves is not one of my highest priorities. Then why have I written this megabyte-plus FAQ? Good question. Getting more users is a general win, for obvious reasons.)

4.9.2. "Who needs to encrypt?"

- + Corporations
 - competitors...fax transmissions
- + foreign governments
 - Chobetsu, GCHQ, SDECE, Mossad, KGB
- + their own government
 - NSA intercepts of plans, investments
- + Activist Groups
 - Aryan Nation needs to encrypt, as FBI has announced their intent to infiltrate and subvert this group
 - RU-486 networks
 - Amnesty International
- + Terrorists and Drug Dealers
 - clearly are clueless at times (Pablo Escobar using a cellphone!)
 - Triads, Russian Mafia, many are becoming crypto-literate
 - (I've been approached-'nuff said)
- + Doctors, lawyers, psychiatrists, etc.
 - to preserve records against theft, snooping, casual examination, etc.
 - in many cases, a legal obligation has been attached to this (notably, medical records)
 - the curious situation that many people are essentially required to encrypt (no other way to ensure standards are met) and yet various laws exists to limit encryption...ITAR, Clipper, EES
 - (Clipper is a partial answer, if unsatisfactory)

4.9.3. "When should crypto be used?"

- It's an economic matter. Each person has to decide when to use it, and how. Me, I dislike having to download messages to my home machine before I can read them. Others use it routinely.

4.10. Libertarian Issues

4.10.1. A technological approach to freedom and privacy:

- "Freedom is, practically, given as much (or more) by the tools we can build to protect it, as it is by our ability to convince others who violently disagree with us not to attack us. On the Internet we have tools like anon remailers and PGP that give us a great deal of freedom from coercion even in the midst of censors. Thus, these tools piss off fans of centralized information control, the defenders of the status quo, like nothing else on the Internet." [an50@desert.hacktic.nl] (Nobody), libtech-1@netcom.com, 1994-06-08]
- + Duncan Frissell, as usual, put it cogently:
 - "If I withhold my capital from some country or enterprise I am not threatening to kill anyone. When a "Democratic State" decides to do something, it does so with armed men. If you don't obey, they tend to shoot....[I]f technological change enhances the powers of individuals,

their power is enhanced no matter what the government does.

"If the collective is weakened and the individual strengthened by the fact that I have the power of cheap guns, cars, computers, telecoms, and crypto then the collective has been weakened and we should ease the transition to a society based on voluntary rather than coerced interaction.

"Unless you can figure out a new, improved way of controlling others; you have no choice." [D.F., Decline and Fall, 1994-06-19]

4.10.2. "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."
[Benjamin Franklin]

4.10.3. a typical view of government

- "As I see it, it's always a home for bullies masquerading as a collective defense. Sometimes it actually it actually has to perform its advertised defense function. Like naked quarks, purely defensive governments cannot exist. They are bipolar by nature, with some poles (i.e., the bullying part) being "more equal than others." [Sandy Sandfort, 1994-09-06]

4.10.4. Sadly, several of our speculative scenarios for various laws have come to pass. Even several of my own, such as:

- "(Yet Another May Prediction Realized)...The text of a "digital stalking bill" was just sent to Cyberia-1." [L. Todd Masco, 1994-08-31] (This was a joking prediction I made that "digital stalking" would soon be a crime; there had been news articles about the horrors of such cyberspatial stalkings, regardless of there being no real physical threats, so this move is not all that surprising. Not surprising in an age when free speech gets outlawed as "assault speech.")

4.10.5. "Don't tread on me."

4.10.6. However, it's easy to get too negative on the situation, to assume that a socialist state is right around the corner. Or that a new Hitler will come to power. These are unlikely developments, and not only because of strong crypto. Financial markets are putting constraints on how fascist a government can get...the international bond markets, for example, will quickly react to signs like this. (This is the theory, at least.)

4.10.7. Locality of reference, cash, TANSTAAFL, privacy

- closure, local computation, local benefits
- no accounting system needed
- markets clear
- market distortions like rationing, coupons, quotas, all require centralized record-keeping
- anything that ties economic transactions to identity (rationing, entitlements, insurance) implies identity-tracking, credentials, etc.
- + Nonlocality also dramatically increases the opportunities for fraud, for scams and con jobs
- because something is being promised for future delivery

- (the essence of many scams) and is not verifiable locally
- because "trust" is invoked
- Locality also fixes the "policeman inside" problem: the costs of decisions are borne by the decider, not by others.

4.11. Crypto Anarchy

4.11.1. The Crypto Anarchy Principle: Strong crypto permits unbreakable encryption, unforgeable signatures, untraceable electronic messages, and unlinkable pseudonymous identities. This ensures that some transactions and communications can be entered into only voluntarily. External force, law, and regulation cannot be applied. This is "anarchy," in the sense of no outside rulers and laws. Voluntary arrangements, back-stopped by voluntarily-arranged institutions like escrow services, will be the only form of rule. This is "crypto anarchy."

4.11.2. crypto allows a return to contracts that governments cannot breach

- based on reputation, repeat business
- example: ordering illegal material untraceably and anonymously,,, governments are powerless to do anything
- private spaces, with the privacy enforced via cryptographic permissions (access credentials)
- escrows (bonds)

4.11.3. Technological solutions over legalistic regulations

+ Marc Ringuette summarized things nicely:

- "What we're after is some "community standards" for cyberspace, and what I'm suggesting is the fairly libertarian standard that goes like this:

" Prefer technological solutions and self-protection solutions over rule-making, where they are feasible.

"This is based on the notion that the more rules there are, the more people will call for the "net police" to enforce them. If we can encourage community standards which emphasize a prudent level of self-protection, then we'll be able to make do with fewer rules and a less intrusive level of policing." [Marc Ringuette, 1993-03-14]

+ Hal Finney has made cogent arguments as to why we should not become too complacent about the role of technology vis-a-vis politics. He warns us not to grow too confident:

- "Fundamentally, I believe we will have the kind of society that most people want. If we want freedom and privacy, we must persuade others that these are worth having. There are no shortcuts. Withdrawing into technology is like pulling the blankets over your head. It feels good for a while, until reality catches up. The next Clipper or Digital Telephony proposal will provide a rude awakening." [Hal Finney, POLI: Politics vs Technology, 1994-01-02]

- "The idea here is that the ultimate solution to the low signal-to-noise ratio on the nets is not a matter of forcing people to "stand behind their words". People can stand behind all kinds of idiotic ideas. Rather, there will need to be developed better systems for filtering news

and mail, for developing "digital reputations" which can be stamped on one's postings to pass through these smart filters, and even applying these reputations to pseudonyms. In such a system, the fact that someone is posting or mailing pseudonymously is not a problem, since nuisance posters won't be able to get through." [Hal Finney, 1993-02-23]

4.11.4. Reputations

4.11.5. I have a moral outlook that many will find unacceptable or repugnant. To cut to the chase: I support the killing of those who break contracts, who steal in serious enough ways, and who otherwise commit what I think of as crimes.

+ I don't mean this abstractly. Here's an example:

- Someone is carrying drugs. He knows what he's involved in. He knows that theft is punishable by death. And yet he steals some of the merchandise.
- Dealers understand that they cannot tolerate this, that an example must be made, else all of their employees will steal.
- Understand that I'm not talking about the state doing the killing, nor would I do the killing. I'm just saying such things are the natural enforcement mechanism for such markets. Realpolitik.
- (A meta point: the drug laws makes things this way. Legalize all drugs and the businesses would be more like "ordinary" businesses.)
- In my highly personal opinion, many people, including most Congressrodents, have committed crimes that earn them the death penalty; I will not be sorry to see anonymous assassination markets used to deal with them.

4.11.6. Increased espionage will help to destroy nation-state-empires like the U.S., which has gotten far too bloated and far too dependent on throwing its weight around; nuclear "terrorism" may knock out a few cities, but this may be a small price to pay to undermine totally the socialist welfare states that have launched so many wars this century.

4.12. Loose Ends

4.12.1. "Why take a "no compromise" stance?"

- Compromise often ends up in the death of a thousand cuts. Better to just take a rejectionist stance.
- The National Rifle Association (NRA) learned this lesson the hard way. EFF may eventually learn it; right now they appear to be in the "coopted by the power center" mode, luxuriating in their inside-the-Beltway access to the Veep, their flights on Air Force One, and their general schmoozing with the movers and shakers...getting along by going along.
- Let's not compromise on basic issues. Treat censorship as a problem to be routed around (as John Gilmore suggests), not as something that needs to be compromised on. (This is directed at rumblings about how the Net needs to "police itself," by the "reasonable" censorship of offensive posts, by the "moderation" of newsgroups, etc. What should concern us is the accomodation of this view by well-meaning civil liberties groups, which are apparently willing to play a role in this "self-policing" system. No thanks.)

- (And since people often misunderstand this point, I'm not saying private companies can't set whatever policies they wish, that moderated newsgroups can't be formed, etc. Private arrangements are just that. The issue is when censorship is forced on those who have no other obligations. Government usually does this, often aided and abetted by corporations and lobbying groups. This is what we need to fight. Fight by routing around, via technology.)

4.12.2. The inherent evils of democracy

- To be blunt about it, I've come to despise the modern version of democracy we have. Every issue is framed in terms of popular sentiment, in terms of how the public would vote. Mob rule at its worst.
- Should people be allowed to wear blue jeans? Put it to a vote. Can employers have a policy on blue jeans? Pass a law. Should health care be provided to all? Put it to a vote. And so on, whittling away basic freedoms and rights. A travesty. The tyranny of the majority.
- De Toqueville warned of this when he said that the American experiment in democracy would last only until citizens discovered they could pick the pockets of their neighbors at the ballot box.
- But maybe we can stop this nonsense. I support strong crypto (and its eventual form, crypto anarchy) because it undermines this form of democracy. It takes some (and perhaps many) transactions out of the realm of popularity contests, beyond the reach of will of the herd. (No, I am not arguing there will be a complete phase change. As the saying goes, "You can't eat cyberspace." But a lot of consulting, technical work, programming, etc., can in fact be done with crypto anarchic methods, with the money gained transferred in a variety of ways into the "real world." More on this elsewhere.)
- + Crypto anarchy effectively allows people to pick and choose which laws they support, at least in cyberspatial contexts. It empowers people to break the local bonds of their majoritarian normative systems and decide for themselves which laws are moral and which are bullshit.
- I happen to have faith that most people will settle on a relatively small number of laws that they'll (mostly) support, a kind of Schelling point in legal space.

4.12.3. "Is the Cypherpunks agenda too extreme?"

- Bear in mind that most of the "Cypherpunks agenda," to the extent we can identify it, is likely to provoke ordinary citizens into outrage. Talk of anonymous mail, digital money, money laundering, information markets, data havens, undermining authority, transnationalism, and all the rest (insert your favorite idea) is not exactly mainstream.

4.12.4. "Crypto Anarchy sounds too wild for me."

- I accept that many people will find the implications of crypto anarchy (which follows in turn from the existence of strong cryptography, via the Crypto Anarchy Principle) to be more than they can accept.
- This is OK (not that you need my OK!). The house of Cypherpunks has many rooms.

5. Cryptology

5.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

5.2. SUMMARY: Cryptology

5.2.1. Main Points

- gaps still exist here...I treated this as fairly low priority, given the wealth of material on cryptography

5.2.2. Connections to Other Sections

- detailed crypto knowledge is not needed to understand many of the implications, but it helps to know the basics (it heads off many of the most wrong-headed interpretations)
- in particular, everyone should learn enough to at least vaguely understand how "blinding" works

5.2.3. Where to Find Additional Information

- + a dozen or so major books
 - Schneier, "Applied Cryptography"--is practically "required reading"
 - Denning
 - Brassard
 - Simmons
 - Welsh, Dominic
 - Salomaa
 - "CRYPTO" Proceedings
 - Other books I can take or leave
- many ftp sites, detailed in various places in this doc
- sci.crypt, alt.privacy.gpg, etc.
- sci.crypt.research is a new group, and is moderated, so it should have some high-quality, technical posts
- FAQs on sci.crypt, from RSA, etc.
- Dave Banisar of EPIC (Electronic Privacy Information Center) reports: "...we have several hundred files on encryption available via ftp/wais/gopher/WWW from cpsr.org /cpsr/privacy/crypto." [D.B., sci.crypt, 1994-06-30]

5.2.4. Miscellaneous Comments

- details of algorithms would fill several books...and do
- hence, will not cover crypto in depth here (the main focus of this doc is the implications of crypto, the Cypherpunkian aspects, the things not covered in crypto textbooks)
- beware of getting lost in the minutiae, in the details of specific algorithms...try to keep in the mind the important aspects of any system

5.3. What this FAQ Section Will Not Cover

5.3.1. Why a section on crypto when so many other sources exist?

- A good question. I'll be keeping this section brief, as many textbooks can afford to do a much better job here than I can.
- not just for those who read number theory books with one hand

5.3.2. NOTE: This section may remain disorganized, at least as compared to some of the later sections. Many excellent

sources on crypto exist, including readily available FAQs (sci.crypt, RSADSI FAQ) and books. Schneier's books is especially recommended, and should be on every Cypherpunk's bookshelf.

5.4. Crypto Basics

5.4.1. "What is cryptology?"

- we see crypto all around us...the keys in our pockets, the signatures on our driver's licenses and other cards, the photo IDs, the credit cards
- + cryptography or cryptology, the science of secret writing...but it's a lot more...consider I.D. cards, locks on doors, combinations to safes, private information...secrecy is all around us
 - some say this is bad--the tension between "what have you got to hide?" and "none of your business"
- some exotic stuff: digital money, voting systems, advanced software protocols
- of importance to protecting privacy in a world of localizers (a la Bob and Cherie), credit cards, tags on cars, etc....the dossier society
- + general comments on cryptography
 - chain is only as strong as its weakest link
 - assume opponnent knows everything except the secret key
 -
- Crypto is about economics
- + Codes and Ciphers
 - + Simple Codes
 - Code Books
 - + Simple Ciphers
 - + Substitution Ciphers (A=C, B=D, etc.)
 - Caesar Shift (blocks)
 - + Keyword Ciphers
 - + Vigenere (with Caesar)
 - + Rotor Machines
 - Hagelin
 - Enigma
 - Early Computers (Turing, Colossus)
- + Modern Ciphers
 - + 20th Century
 - + Private Key
 - + One-Time Pads (long strings of random numbers, shared by both parties)
 - + not breakable even in principle, e.g., a one-time pad with random characters selected by a truly random process (die tosses, radioactive decay, certain types of noise, etc.)
 - and ignoring the "breakable by break-ins" approach of stealing the one-time pad, etc. ("Black bag cryptography")
 - Computer Media (Floppies)
 - + CD-ROMs and DATs
 - "CD ROM is a terrible medium for the OTP key stream. First, you want exactly two copies of the random stream. CD ROM has an economic advantage only for large runs. Second, you want to destroy the part of the stream already used.

CD ROM has no erase facilities, outside of physical destruction of the entire disk."
[Bryan G. Olson, sci.crypt, 1994-08-31]

- + DES--Data Encryption Standard
 - Developed from IBM's Lucifer, supported by NSA
 - a standard since 1970s
 - + But is it "Weak"?
 - + DES-busting hardware and software studied
 - + By 1990, still cracked
 - But NSA/NIST has ordered a change
 - + Key Distribution Problem
 - + Communicating with 100 other people means distributing and securing 100 keys
 - and each of those 100 must keep their 100 keys secure
 - no possibility of widespread use
 - + Public Key
 - + 1970s: Diffie, Hellman, Merkle
 - + Two Keys: Private Key and Public Key
 - + Anybody can encrypt a message to Receiver with Receiver's PUBLIC key, but only the Receiver's PRIVATE key can decrypt the message
 - + Directories of public keys can be published (solves the key distribution problem)
 - + Approaches
 - + One-Way Functions
 - Knapsack (Merkle, Hellman)
 - + RSA (Rivest, Shamir, Adleman)
 - relies on difficulty of factoring large numbers (200 decimal digits)
 - believed to be "NP-hard"
 - + patented and licensed to "carefully selected" customers
 - RSA, Fiat-Shamir, and other algorithms are not freely usable
 - search for alternatives continues
- 5.4.2. "Why does anybody need crypto?"
- + Why the Need
 - electronic communications...cellular phones, fax machines, ordinary phone calls are all easily intercepted...by foreign governments, by the NSA, by rival drug dealers, by casual amateurs
 - + transactions being traced....credit card receipts, personal checks, I.D. cards presented at time of purchase...allows cross-referencing, direct mail data bases, even government raids on people who buy greenhouse supplies!
 - in a sense, encryption and digital money allows a return to cash
 - Why do honest people need encryption? Because not everyone is honest, and this applies to governments as well. Besides, some things are no one else's business.
 - Why does anybody need locks on doors? Why aren't all diaries available for public reading?
 - + Whit Diffie, one of the inventors of public key cryptography (and a Cypherpunk) points out that human interaction has largely been predicated on two important

aspects:

- that you are who you say you are
 - expectation of privacy in private communications
 - Privacy exists in various forms in various cultures. But even in police states, certain concepts of privacy are important.
 - Trust is not enough...one may have opponents who will violate trust if it seems justified
 - + The current importance of crypto is even more striking
 - + needed to protect privacy in cyberspace, networks, etc.
 - many more paths, links, interconnects
 - read Vinge's "True Names" for a vision
 - + digital money...in a world of agents, knowbots, high connectivity
 - (can't be giving out your VISA number for all these things)
 - + developing battle between:
 - privacy advocates...those who want privacy
 - government agencies...FBI, DOJ, DEA, FINCEN, NSA
 - + being fought with:
 - attempts to restrict encryption (S.266, never passed)
 - Digital Telephony Bill, \$10K a day fine
 - trial balloons to require key registration
 - future actions
 - + honest people need crypto because there are dishonest people
 - and there may be other needs for privacy
 - Phil Zimmerman's point about sending all mail, all letters, on postcards--"What have you got to hide?" indeed!
 - the expectation of privacy in our homes and in phone conversations
 - + Whit Diffie's main points:
 - + proving who you say you are...signatures, authentications
 - like "seals" of the past
 - protecting privacy
 - locks and keys on property and whatnot
 - + the three elements that are central to our modern view of liberty and privacy (a la Diffie)
 - protecting things against theft
 - proving who we say we are
 - expecting privacy in our conversations and writings
- 5.4.3. What's the history of cryptology?
- 5.4.4. Major Classes of Crypto
- (these sections will introduce the terms in context, though complete definitions will not be given)
 - + Encryption
 - privacy of messages
 - using ciphers and codes to protect the secrecy of messages
 - DES is the most common symmetric cipher (same key for encryption and decryption)
 - RSA is the most common asymmetric cipher (different keys for encryption and decryption)
 - + Signatures and Authentication
 - proving who you are
 - proving you signed a document (and not someone else)
 - + Authentication

- + Seals
 - + Signatures (written)
 - + Digital Signatures (computer)
 - Example: Numerical codes on lottery tickets
 - + Using Public Key Methods (see below)
 - Digital Credentials (Super Smartcards)
 - Tamper-responding Systems
 - + Credentials
 - ID Cards, Passports, etc.
 - + Biometric Security
 - Fingerprints, Retinal Scans, DNA, etc.
- + Untraceable Mail
 - untraceable sending and receiving of mail and messages
 - focus: defeating eavesdroppers and traffic analysis
 - DC protocol (dining cryptographers)
- + Cryptographic Voting
 - focus: ballot box anonymity
 - credentials for voting
 - issues of double voting, security, robustness, efficiency
- + Digital Cash
 - focus: privacy in transactions, purchases
 - unlinkable credentials
 - blinded notes
 - "digital coins" may not be possible
- + Crypto Anarchy
 - using the above to evade gov't., to bypass tax collection, etc.
 - a technological solution to the problem of too much government
- + Security
 - + Locks
 - Key Locks
 - + Combination Locks
 - Cardkey Locks
 - + Tamper-responding Systems (Seals)
 - + Also known as "tamper-proof" (misleading)
 - Food and Medicine Containers
 - Vaults, Safes (Alarms)
 - + Weapons, Permissive Action Links
 - Nuclear Weapons
 - Arms Control
 - Smartcards
 - Currency, Checks
 - + Cryptographic Checksums on Software
 - But where is it stored? (Can spoof the system by replacing the whole package)
 - + Copy Protection
 - Passwords
 - Hardware Keys ("dongles")
 - Call-in at run-time
 - + Access Control
 - Passwords, Passphrases
 - Biometric Security, Handwritten Signatures
 - For: Computer Accounts, ATMs, Smartcards
- 5.4.5. Hardware vs. Software
 - NSA says only hardware implementations can really be considered secure, and yet most Cypherpunks and ordinary

- crypto users favor the software approach
- Hardware is less easily spoofable (replacement of modules)
- Software can be changed more rapidly, to make use of newer features, faster modules, etc.
- Different cultures, with ordinary users (many millions) knowing they are less likely to have their systems black-bag spoofed (midnight engineering) than are the relatively fewer and much more sensitive military sites.
- 5.4.6. "What are 'tamper-resistant modules' and why are they important?"
 - These are the "tamper-proof boxes" of yore: display cases, vaults, museum cases
 - that give evidence of having been opened, tampered with, etc.
 - + modern versions:
 - display cases
 - smart cards
 - + chips
 - layers of epoxy, abrasive materials, fusible links, etc.
 - (goal is to make reverse engineering much more expensive)
 - nuclear weapon "permissive action links" (PALs)
- 5.4.7. "What are "one way functions"?"
 - functions with no inverses
 - crypto needs functions that are seemingly one-way, but which actually have an inverse (though very hard to find, for example)
 - one-way function, like "bobbles" (Vinge's "Marooned in Realtime")
- 5.4.8. When did modern cryptology start?
 - + "What are some of the modern applications of cryptology?"
 - + "Zero Knowledge Interactive Proof Systems" (ZKIPS)
 - since around 1985
 - "minimum disclosure proofs"
 - + proving that you know something without actually revealing that something
 - + practical example: password
 - + can prove you have the password without actually typing it in to computer
 - hence, eavesdroppers can't learn your password
 - like "20 questions" but more sophisticated
 - abstract example: Hamiltonian circuit of a graph
 - + Digital Money
 - + David Chaum: "RSA numbers ARE money"
 - checks, cashiers checks, etc.
 - can even know if attempt is made to cash same check twice
 - + so far, no direct equivalent of paper currency or coins
 - but when combined with "reputation-based systems," there may be
 - + Credentials
 - + Proofs of some property that do not reveal more than just that property
 - age, license to drive, voting rights, etc.
 - "digital envelopes"

- + Fiat-Shamir
 - passports
- + Anonymous Voting
 - protection of privacy with electronic voting
 - politics, corporations, clubs, etc.
 - peer review of electronic journals
 - consumer opinions, polls
- + Digital Pseudonyms and Untraceable E-Mail
 - + ability to adopt a digital pseudonym that is:
 - unforgeable
 - authenticatable
 - untraceable
 - Vinge's "True Names" and Card's "Ender's Game"
- + Bulletin Boards, Samizdats, and Free Speech
 - + banned speech, technologies
 - e.g., formula for RU-486 pill
 - bootleg software, legally protected material
 - + floating opinions without fears for professional position
 - can even later "prove" the opinions were yours
- + "The Labyrinth"
 - store-and-forward switching nodes
 - + each with tamper-responding modules that decrypt incoming messages
 - + accumulate some number (latency)
 - + retransmit to next address
 - and so on....
 - + relies on hardware and/or reputations
 - + Chaum claims it can be done solely in software
 - "Dining Cryptographers"

5.4.9. What is public key cryptography?

5.4.10. Why is public key cryptography so important?

- + The chief advantage of public keys cryptosystems over conventional symmetric key (one key does both encryption and decryption) is one connectivity to recipients: one can communicate securely with people without exchanging key material.
 - by looking up their public key in a directory
 - by setting up a channel using Diffie-Hellman key exchange (for example)

5.4.11. "Does possession of a key mean possession of *identity*?"

- If I get your key, am I you?
- Certainly not outside the context of the cryptographic transaction. But within the context of a transaction, yes. Additional safeguards/speedbumps can be inserted (such as biometric credentials, additional passphrases, etc.), but these are essentially part of the "key," so the basic answer remains "yes." (There are periodically concerns raised about this, citing the dangers of having all identity tied to a single credential, or number, or key. Well, there are ways to handle this, such as by adopting protocols that limit one's exposure, that limits the amount of money that can be withdrawn, etc. Or people can adopt protocols that require additional security, time delays, countersigning, etc.)
- + This may be tested in court soon enough, but the answer for many contracts and crypto transactions will be that

possession of key = possession of identity. Even a court test may mean little, for the types of transactions I expect to see.

- That is, in anonymous systems, "who ya gonna sue?"
- So, guard your key.
- 5.4.12. What are digital signatures?
 - + Uses of Digital Signatures
 - Electronic Contracts
 - Voting
 - Checks and other financial instruments (similar to contracts)
 - Date-stamped Transactions (augmenting Notary Publics)
- 5.4.13. Identity, Passports, Fiat-Shamir
 - Murdoch, is-a-person, national ID cards, surveillance society
 - + "Chess Grandmaster Problem" and other Frauds and Spoofs
 - of central importance to proofs of identity (a la Fiat-Shamir)
 - "terrorist" and "Mafia spoof" problems
- 5.4.14. Where else should I look?
- 5.4.15. Crypto, Technical
 - + Ciphers
 - traditional
 - one-time pads, Vernams ciphers, information-theoretically secure
 - + "I Have a New Idea for a Cipher---Should I Discuss it Here?"
 - Please don't. Ciphers require careful analysis, and should be in paper form (that is, presented in a detailed paper, with the necessary references to show that due diligence was done, the equations, tables, etc. The Net is a poor substitute.
 - Also, breaking a randomly presented cipher is by no means trivial, even if the cipher is eventually shown to be weak. Most people don't have the inclination to try to break a cipher unless there's some incentive, such as fame or money involved.
 - And new ciphers are notoriously hard to design. Experts are the best folks to do this. With all the stuff waiting to be done (described here), working on a new cipher is probably the least effective thing an amateur can do. (If you are not an amateur, and have broken other people's ciphers before, then you know who you are, and these comments don't apply. But I'll guess that fewer than a handful of folks on this list have the necessary background to do cipher design.)
 - There are a vast number of ciphers and systems, nearly all of no lasting significance. Untested, undocumented, unused--and probably unworthy of any real attention. Don't add to the noise.
 - What is DES and can it be broken?
- + ciphers
 - RC4, stream cipher
- + DolphinEncrypt
 -
 - + "Last time Dolphin Encrypt reared its insecure head in this forum,

- these same issues came up. The cipher that DE uses is not public and
- was not designed by a person of known cryptographic competence. It
- should therefore be considered extremely weak.
 - <Eric Hughes, 4-16-94, Cypherpunks>
- + RSA
 - What is RSA?
 - Who owns or controls the RSA patents?
 - Can RSA be broken?
 - What alternatives to RSA exist?
- + One-Way Functions
 - like diodes, one-way streets
 - multiplying two large numbers together is easy....factoring the product is often very hard
 - (this is not enough for a usable cipher, as the recipient must be able to perform the reverse operation..it turns out that "trapdoors" can be found)
- Digital Signatures
- + Digital Cash
 - What is digital cash?
 - How does digital cash differ from VISA and similar electronic systems?
 - Clearing vs. Doublespending Detection
- Zero Knowledge
- Mixes and Remailers
- Dining Cryptographers
- + Steganography
 - invisible ink
 - microdots
 - images
 - sound files
- + Random Number Generators
 - + von Neumann quote about living in a state of sin
 - also paraphrased (I've heard) to include analog methods, presumably because the nonrepeating (from an initial seed/start) nature makes repeating experiments impossible
- + Blum-Blum-Shub
 - + How it Works
 - "The Blum-Blum-Shub PRNG is really very simple. There is source floating around on the crypto ftp sites, but it is a set of scripts for the Unix bignum calculator "bc", plus some shell scripts, so it is not very portable.

"To create a BBS RNG, choose two random primes p and q which are congruent to 3 mod 4. Then the RNG is based on the iteration $x = x*x \text{ mod } n$. x is initialized as a random seed. (x should be a quadratic residue, meaning that it is the square of some number mod n, but that can be arranged by iterating the RNG once before using its output.)"

[Hal Finney, 1994-05-14]
 - Look for blum-blum-shub-strong-randgen.shar and related files in pub/crypt/other at ripem.msu.edu. (This site is chock-full of good stuff. Of course, only Americans

- are allowed to use these random number generators, and even they face fines of \$500,000 and imprisonment for up to 5 years for inappropriate use of random numbers.)
 - source code at ripem ftp site
 - "If you don't need high-bandwidth randomness, there are several good PRNG, but none of them run fast. See the chapter on PRNG's in "Cryptology and Computational Number Theory"." [Eric Hughes, 1994-04-14]
 - + "What about hardware random number generators?"
 - + Chips are available
 -
 - + "Hughes Aircraft also offers a true non-deterministic chip (16 pin DIP).
 - For more info contact me at kephart@sirena.hac.com"
 - <7 April 94, sci.crypt>
 - + "Should RNG hardware be a Cypherpunks project?"
 - Probably not, but go right ahead. Half a dozen folks have gotten all fired up about this, proposed a project--then let it drop.
 - can use repeated applications of a cryptographic hash function to generate pretty damn good PRNs (the RSAREF library has hooks for this)
 - + "I need a pretty good random number generator--what should I use?"
 - "While Blum-Blum-Shub is probably the cool way to go, RSAREF uses repeated iterations of MD5 to generate its pseudo-randoms, which can be reasonably secure and use code you've probably already got hooks from perl for. [BillStewart,1994-04-15]
 - + Libraries
 - Scheme code: ftp://ftp.cs.indiana.edu/pub/scheme-repository/scm/rand.scm
 - + P and NP and all that jazz
 - complexity, factoring,
 - + can quantum mechanics help?
 - probably not
 - + Certification Authorities
 - hierarchy vs. distributed web of trust
 - in hierarchy, individual businesses may set themselves up as CAs, as CommerceNet is talking about doing
 - + Or, scarily, the governments of the world may insist that they be "in the loop"
 - several ways to do this: legal system invocation, tax laws, national security....I expect the legal system to impinge on CAs and hence be the main way that CAs are partnered with the government
 - I mention this to give people some chance to plan alternatives, end-runs
 - This is one of the strongest reasons to support the decoupling of software from use (that is, to reject the particular model RSADSI is now using)
- 5.4.16. Randomness
- A confusing subject to many, but also a glorious subject (ripe with algorithms, with deep theory, and readily understandable results).
 - + Bill Stewart had a funny comment in sci.crypt which also shows how hard it is to know if something's really random

or not: "I can take a simple generator $X[i] = \text{DES}(X[i-1], K)$, which will produce nice random white noise, but you won't be able to see that it's non-random unless you rent time on NSA's DES-cracker." [B.S. 1994-09-06]

- In fact, many seemingly random strings are actually "cryptoregular": they are regular, or nonrandom, as soon as one uses the right key. Obviously, most strings used in crypto are cryptoregular in that they appear to be random, and pass various randomness measures, but are not.
- + "How can the randomness of a bit string be measured?"
 - It can roughly be estimated by entropy measures, how compressible it is (by various compression programs), etc.
 - It's important to realize that measures of randomness are, in a sense, "in the eye of the beholder"--there just is no proof that a string is random...there's always room for cleverness, if you will
- + Chaitin-Kolmogoroff complexity theory makes this clearer. To use someone else's words:
 - "Actually, it can't be done. The consistent measure of entropy for finite objects like a string or a (finite) series of random numbers is the so-called ``program length complexity''. This is defined as the length of the shortest program for some given universal Turing machine which computes the string. It's consistent in the sense that it has the familiar properties of ``ordinary'' (Shannon) entropy. Unfortunately, it's uncomputable: there's no algorithm which, given an arbitrary finite string S , computes the program-length complexity of S .

Program-length complexity is well-studied in the literature. A good introductory paper is ``A Theory of Program Size Formally Identical to Information Theory'' by G. J. Chaitin, Journal of the ACM, 22 (1975) reprinted in Chaitin's book Information Randomness & Incompleteness, World Scientific Publishing Co., 1990." [John E. Kreznar, 1993-12-02]

- + "How can I generate reasonably random numbers?"
 - I say "reasonably" because of the point above: no number or sequence is provably "random." About the best that can be said is that a number or string is the result of a process we call "random." If done algorithmically, and deterministically, we call this process "pseudo-random." (And pseudorandom is usually more valuable than "really random" because we want to be able to generate the same sequence repeatedly, to repeat experiments, etc.)
- 5.4.17. Other crypto and hash programs
- + MDC, a stream cipher
 - Peter Gutman, based on NIST Secure Hash Algorithm
 - uses longer keys than IDEA, DES
 - MD5
 - Blowfish
 - DolphinEncrypt
- 5.4.18. RSA strength

- casual grade, 384 bits, 100 MIPS-years (Paul Leyland, 3-31-94)
 - RSA-129, 425 bits, 4000 MIPS-years
 - 512 bits...20,000 MIPS-years
 - 1024 bits...
- 5.4.19. Triple DES
- "It involves three DES cycles, in encrypt-decrypt-encrypt order. The keys used may be either K1/K2/K3 or K1/K2/K1. The latter is sometimes called "double-DES". Combining two DES operations like this requires twice as much work to break as one DES, and a lot more storage. If you have the storage, it just adds one bit to the effective key size. " [Colin Plumb, colin@nyx10.cs.du.edu, sci.crypt, 4-13-94]
- 5.4.20. Tamper-resistant modules (TRMs) (or tamper-responding)
- + usually "tamper-indicating", a la seals
 - very tough to stop tampering, but relatively easy to see if seal has been breached (and then not restored faithfully)
 - possession of the "seal" is controlled...this is the historical equivalent to the "private key" in a digital signature system, with the technological difficulty of forging the seal being the protection
 - + usually for crypto. keys and crypto. processing
 - nuclear test monitoring
 - smart cards
 - ATMs
 - + one or more sensors to detect intrusion
 - vibration (carborundum particles)
 - pressure changes (a la museum display cases)
 - electrical
 - stressed-glass (Corning, Sandia)
 - + test ban treaty verification requires this
 - fiber optic lines sealing a missile...
 - scratch patterns...
 - decals....
 - + Epoxy resins
 - a la Intel in 1970s (8086)
 - + Lawrence Livermore: "Connoisseur Project"
 - gov't agencies using this to protect against reverse engineering, acquisition of keys, etc.
 - + can't stop a determined effort, though
 - etches, solvents, plasma ashing, etc.
 - but can cause cost to be very high (esp. if resin formula is varied frequently, so that "recipe" can't be logged)
 - + can use clear epoxy with "sparkles" in the epoxy and careful 2-position photography used to record pattern
 - perhaps with a transparent lid?
 - + fiber optic seal (bundle of fibers, cut)
 - bundle of fibers is looped around device, then sealed and cut so that about half the fibers are cut; the pattern of lit and unlit fibers is a signature, and is extremely difficult to reproduce
 - nanotechnology may be used (someday)
- 5.4.21. "What are smart cards?"
- Useful for computer security, bank transfers (like ATM)

- cards), etc.
- may have local intelligence (this is the usual sense)
- microprocessors, observor protocol (Chaum)
- + Smart cards and electronic funds transfer
 - Tamper-resistant modules
- + Security of manufacturing
 - some variant of "cut-and-choose" inspection of premises
- + Uses of smart cards
 - conventional credit card uses
 - bill payment
 - postage
 - bridge and road tolls
 - payments for items received electronically (not necessarily anonymously)

5.5. Cryptology-Technical, Mathematical

5.5.1. Historical Cryptography

- + Enigma machines
 - cracked by English at Bletchley Park
 - a secret until mid-1970s
- + U.K. sold hundreds of seized E. machines to embassies, governments, even corporations, in late 1940s, early 1950s
 - could then crack what was being said by allies
- + Hagelin, Boris (?)
 - U.S. paid him to install trapdoors, says Kahn
- + his company, Crypto A.G., was probably an NSA front company
 - Sweden, then U.S., then Sweden, then Zug
 - rotor systems cracked

5.5.2. Public-key Systems--HISTORY

- + Inman has admitted that NSA had a P-K concept in 1966
 - fits with Dominik's point about sealed cryptosystem boxes with no way to load new keys
 - and consistent with NSA having essentially sole access to nation's top mathematicians (until Diffies and Hellmans foreswore government funding, as a result of the anti-Pentagon feelings of the 70s)
- Merkle's "puzzle" ideas, circa mid-70s
- Diffie and Hellman
- Rivest, Shamir, and Adleman

5.5.3. RSA and Alternatives to RSA

- + RSA and other P-K patents are strangling development and dissemination of crypto systems
 - perhaps out of marketing stupidity, perhaps with the help of the government (which has an interest in keeping a monopoly on secure encryption)
- + One-way functions and "deposit-only envelopes"
 - one-way functions
 - deposit-only envelopes: allow additions to envelopes and only addressee can open
- hash functions are easy to implement one-way functions (with no need for an inverse)

5.5.4. Digital Signatures

- + Uses of Digital Signatures
 - Electronic Contracts

- Voting
 - Checks and other financial instruments (similar to contracts)
 - Date-stamped Transactions (augmenting Notary Publics)
 - Undeniable digital signatures
 - + Unforgeable signatures, even with unlimited computational power, can be achieved if the population is limited (a finite set of agents)
 - using an untraceable sending protocol, such as "the Dining Cryptographers Problem" of Chaum
- 5.5.5. Randomness and incompressibility
- + best definition we have is due to Chaitin and Kolmogoroff: a string or any structure is "random" if it has no shorter description of itself than itself.
 - (Now even specific instances of "randomly generated strings" sometimes will be compressible--but not very often. Cf. the works of Chaitin and others for more on these sorts of points.)
- 5.5.6. Steganography: Methods for Hiding the Mere Existence of Encrypted Data
- + in contrast to the oft-cited point (made by crypto purists) that one must assume the opponent has full access to the cryptotext, some fragments of decrypted plaintext, and to the algorithm itself, i.e., assume the worst
 - a condition I think is practically absurd and unrealistic
 - assumes infinite intercept power (same assumption of infinite computer power would make all systems besides one-time pads breakable)
 - in reality, hiding the existence and form of an encrypted message is important
 - + this will be all the more so as legal challenges to crypto are mounted...the proposed ban on encrypted telecom (with \$10K per day fine), various governmental regulations, etc.
 - RICO and other broad brush ploys may make people very careful about revealing that they are even using encryption (regardless of how secure the keys are)
 - + steganography, the science of hiding the existence of encrypted information
 - secret inks
 - microdots
 - thwarting traffic analysis
 - LSB method
 - + Packing data into audio tapes (LSB of DAT)
 - + LSB of DAT: a 2GB audio DAT will allow more than 100 megabytes in the LSBs
 - less if algorithms are used to shape the spectrum to make it look even more like noise
 - but can also use the higher bits, too (since a real-world recording will have noise reaching up to perhaps the 3rd or 4th bit)
 - + will manufacturers investigate "dithering" circuits? (a la fat zero?)
 - but the race will still be on
 - + Digital video will offer even more storage space (larger tapes)
 - DVI, etc.

- HDTV by late 1990s
- + Messages can be put into GIFF, TIFF image files (or even noisy faxes)
 - using the LSB method, with a 1024 x 1024 grey scale image holding 64KB in the LSB plane alone
 - with error correction, noise shaping, etc., still at least 50KB
 - scenario: already being used to transmit message through international fax and image transmissions
- + The Old "Two Plaintexts" Ploy
 - one decoding produces "Having a nice time. Wish you were here."
 - other decoding, of the same raw bits, produces "The last submarine left this morning."
 - any legal order to produce the key generates the first message
- + authorities can never prove-save for torture or an informant-that another message exists
 - unless there are somehow signs that the encrypted message is somehow "inefficiently encrypted, suggesting the use of a dual plaintext pair method" (or somesuch spookspeak)
 - again, certain purist argue that such issues (which are related to the old "How do you know when to stop?" question) are misleading, that one must assume the opponent has nearly complete access to everything except the actual key, that any scheme to combine multiple systems is no better than what is gotten as a result of the combination itself
- and just the overall bandwidth of data...
- + Several programs exist:
 - Stego
 - etc. (described elsewhere)

5.5.7. The Essential Impossibility of Breaking Modern Ciphers and Codes

- this is an important change from the past (and from various thriller novels that have big computers cracking codes)
- granted, "unbreakable" is a misleading term
- + recall the comment that NSA has not really broken any Soviet systems in many years
 - except for the cases, a la the Walker case, where plaintext versions are gotten, i.e., where human screwups occurred
- the image in so many novels of massive computers breaking codes is absurd: modern ciphers will not be broken (but the primitive ciphers used by so many Third World nations and their embassies will continue to be child's play, even for high school science fair projects...could be a good idea for a small scene, about a BCC student who has his project pulled)
- + But could novel computational methods crack these public key ciphers?
 - + some speculative candidates
 - + holographic computers, where large numbers are factored-or at least the possibilities are somehow narrowed-by using arrays that (somehow) represent the numbers to be factored

- perhaps with diffraction, channeling, etc.
 - neural networks and evolutionary systems (genetic algorithms)
 - the idea is that somehow the massive computations can be converted into something that is inherently parallel (like a crystal)
 - + hyperspeculatively: finding the oracle for these problems using nonconventional methods such as ESP and lucid dreaming
 - some groups feel this is worthwhile
- 5.5.8. Anonymous Transfers
- Chaum's digital mixes
 - "Dining Cryptographers"
 - + can do it with exchanged diskettes, at a simple level
 - wherein each person can add new material
 - + Alice to Bob to Carol....Alice and Carol can conspire to determine what Bob had added, but a sufficient "mixing" of bits and pieces is possible such that only if everybody conspires can one of the participants be caught
 - perhaps the card-shuffling results?
 - + may become common inside compute systems...
 - by this vague idea I mean that various new OS protocols may call for various new mechanisms for exchanging information
- 5.5.9. Miscellaneous Abstract Ideas
- can first order logic predicates be proven in zero knowledge?
 - Riemann hypothesis
 - + $P = NP$?
 - would the universe change?
 - Smale has shown that if the squares have real numbers in them, as opposed to natural numbers (integers), then $P = NP$; perhaps this isn't surprising, as a real implies sort of a recursive descent, with each square having unlimited computer power
 - + oracles
 - speculatively, a character asks if Tarot cards, etc., could be used (in addition to the normal idea that such devices help psychologically)
 - "a cascade of changes coming in from hundreds of decimal places out"
 - + Quantum cryptography
 - bits can be exchanged-albeit at fairly low efficiencies-over a channel
 - with detection of taps, via the change of polarizations
 - + Stephen Wiesner wrote a 1970 paper, half a decade before the P-K work, which outlined this-not published until much later
 - speculate that the NSA knew about this and quashed the publication
 - + But could novel computational methods crack these public key ciphers?
 - + some speculative candidates
 - + holographic computers, where large numbers are factored-or at least the possibilities are somehow narrowed-by using arrays that (somehow) represent the numbers to be factored

- perhaps with diffraction, channeling, etc.
- neural networks and evolutionary systems (genetic algorithms)
- the idea is that somehow the massive computations can be converted into something that is inherently parallel (like a crystal)
- + hyperspeculatively: finding the oracle for these problems using nonconventional methods such as ESP and lucid dreaming
 - some groups feel this is worthwhile
- links to knot theory
- "cut and choose" protocols (= zero knowledge)
- + can a "digital coin" be made?
 - this is formally similar to the idea of an active agent that is unforgeable, in the sense that the agent or coin is "standalone"
- + bits can always be duplicated (unless tied to hardware, as with TRMs), so must look elsewhere
 - + could tie the bits to a specific location, so that duplication would be obvious or useless
 - the idea is vaguely that an agent could be placed in some location...duplications would be both detectable and irrelevant (same bits, same behavior, unmodifiable because of digital signature)
- + coding theory and cryptography at the "Discrete Mathematics"
 - <http://www.win.tue.nl/win/math/dw/index.html>
- 5.5.10. Tamper-resistant modules (TRMs) (or tamper-responding)
 - + usually "tamper-indicating", a la seals
 - very tough to stop tampering, but relatively easy to see if seal has been breached (and then not restored faithfully)
 - possession of the "seal" is controlled...this is the historical equivalent to the "private key" in a digital signature system, with the technological difficulty of forging the seal being the protection
 - + usually for crypto. keys and crypto. processing
 - nuclear test monitoring
 - smart cards
 - ATMs
 - + one or more sensors to detect intrusion
 - vibration (carborundum particles)
 - pressure changes (a la museum display cases)
 - electrical
 - stressed-glass (Corning, Sandia)
 - + test ban treaty verification requires this
 - fiber optic lines sealing a missile...
 - scratch patterns...
 - decals....
 - + Epoxy resins
 - a la Intel in 1970s (8086)
 - + Lawrence Livermore: "Connoisseur Project"
 - gov't agencies using this to protect against reverse engineering, acquisition of keys, etc.
 - + can't stop a determined effort, though
 - etches, solvents, plasma ashing, etc.
 - but can cause cost to be very high (esp. if resin

- formula is varied frequently, so that "recipe" can't be logged)
 - + can use clear epoxy with "sparkles" in the epoxy and careful 2-position photography used to record pattern
 - perhaps with a transparent lid?
 - + fiber optic seal (bundle of fibers, cut)
 - bundle of fibers is looped around device, then sealed and cut so that about half the fibers are cut; the pattern of lit and unlit fibers is a signature, and is extremely difficult to reproduce
 - nanotechnology may be used (someday)

5.6. Crypto Programs and Products

5.6.1. PGP, of course

- it's own section, needless to say

5.6.2. "What about hardware chips for encryption?"

- Speed can be gotten, for sure, but at the expense of limiting the market dramatically. Good for military uses, not so good for civilian uses (especially as most civilians don't have a need for high speeds, all other things being equal).

5.6.3. Carl Ellison's "tran" and mixing various ciphers in chains

- "tran.shar is available at ftp.std.com:/pub/cme
- des | tran | des | tran | des
- to make the job of the attacker much harder, and to make differential cryptanalysis harder
- "it's in response to Eli's paper that I advocated prngxor, as in:
 - des | prngxor | tran | des | tran | des
 with the DES instances in ECB mode (in acknowledgement of Eli's attack). The prngxor destroys any patterns from the input, which was the purpose of CBC, without using the feedback path which Eli exploited." [Carl Ellison, 1994-07-15]

5.6.4. The Blum-Blum-Shub RNG

- about the strongest algorithmic RNG we know of, albeit slow (if they can predict the next bit of BBS, they can break RSA, so....
- ripem.msu.edu:/pub/crypt/other/blum-blum-shub-strong-randgen.shar

5.6.5. the Blowfish cipher

- + BLOWFISH.ZIP, written by Bruce Schneier, 1994. subject of an article in Dr. Dobb's Journal:
 - ftp.dsi.unimi.it:/pub/security/crypt/code/schneier-blowfish.c.gz

5.7. Related Ideas

5.7.1. "What is "blinding"?"

- + This is a basic primitive operation of most digital cash systems. Any good textbook on crypto should explain it, and cover the math needed to understand it in detail. Several people have explained it (many times) on the list; here's a short explanation by Karl Barrus:
 - "Conceptually, when you blind a message, nobody else can read it. A property about blinding is that under the right circumstances if another party digitally signs a

blinded message, the unblinded message will contain a valid digital signature.

"So if Alice blinds the message "I owe Alice \$1000" so that it reads (say) "a;dfafq)(*&" or whatever, and Bob agrees to sign this message, later Alice can unblind the message Bob signed to retrieve the original. And Bob's digital signature will appear on the original, although he didn't sign the original directly.

"Mathematically, blinding a message means multiplying it by a number (think of the message as being a number). Unblinding is simply dividing the original blinding factor out." [Karl Barrus, 1993-08-24]

- + And another explanation by Hal Finney, which came up in the context of how to delink pharmacy prescriptions from personal identity (fears of medial dossiers:
 - "Chaum's "blinded credential" system is intended to solve exactly this kind of problem, but it requires an extensive infrastructure. There has to be an agency where you physically identify yourself. It doesn't have to know anything about you other than some physical ID like fingerprints. You and it cooperate to create pseudonyms of various classes, for example, a "go to the doctor" pseudonym, and a "go to the pharmacy" pseudonym. These pseudonyms have a certain mathematical relationship which allows you to re-blind credentials written to one pseudonym to apply to any other. But the agency uses your physical ID to make sure you only get one pseudonym of each kind....So, when the doctor gives you a prescription, that is a credential applied to your "go to the doctor" pseudonym. (You can of course also reveal your real name to the doctor if you want.) Then you show it at the pharmacy using your "go to the pharmacy" pseudonym. The credential can only be shown on this one pseudonym at the pharamacy, but it is unlinkable to the one you got at the doctor's. " [Hal Finney, 1994-09-07]

5.7.2. "Crypto protocols are often confusing. Is there a coherent theory of these things?"

- Yes, crypto protocols are often expressed as scenarios, as word problems, as "Alice and Bob and Eve" sorts of complicated interaction protocols. Not exactly game theory, not exactly logic, and not exactly anything else in particular...its own area.
- Expert systems, proof-of-correctness calculi, etc.
- spoofing, eavesdropping, motivations, reputations, trust models
- + In my opinion, much more work is needed here.
 - Graphs, agents, objects, capabilities, goals, intentions, logic
 - evolutionary game theory, cooperation, defection, tit-for-tat, ecologies, economies
 - mostly ignored, to date, by crypto community

5.7.3. The holder of a key *is* the person, basically

- that's the bottom line
- those that worry about this are free to adopt stronger, more elaborate systems (multi-part, passphrases, biometric

security, limits on account access, etc.)

- whoever has a house key is essentially able to gain access (not saying this is the legal situation, but the practical one)

5.7.4. Strong crypto is helped by huge increases in processor power, networks

- + Encryption *always wins out* over cryptanalysis...gap grows greater with time
 - "the bits win"
- + Networks can hide more bits...gigabits flowing across borders, stego, etc.
 - faster networks mean more "degrees of freedom," more avenues to hide bits in, exponentially increasing efforts to eavesdrop and track
 - (However, these additional degrees of freedom can mean greater chances for slipping up and leaving clues that allow correlation. Complexity can be a problem.)
- + "pulling the plug" hurts too much...shuts down world economy to stop illegal bits ("naughty bits"?)
 - one of the main goals is to reach the "point of no return," beyond which pulling the plug hurts too much
 - this is not to say they won't still pull the plug, damage be damned

5.7.5. "What is the "Diffie-Hellman" protocol and why is it important?"

- + What it is
 - Diffie-Hellman, first described in 1976, allows key exchange over insecure channels.
- + Steve Bellovin was one of several people to explain D-H to the list (every few months someone does!). I'm including his explanation, despite its length, to help readers who are not cryptologists get some flavor of the type of math involved. The thing to notice is the use of *exponentiations* and *modular arithmetic* (the "clock arithmetic" of our "new math" childhoods, except with really, really big numbers!). The difficulty of inverting the exponentiation (the discrete log problem) is what makes this a cryptographically interesting approach.
 - "The basic idea is simple. Pick a large number p (probably a prime), and a base b that is a generator of the group of integers modulo p . Now, it turns out that given a known p , b , and $(b^x) \bmod p$, it's extremely hard to find out x . That's known as the discrete log problem.

"Here's how to use it. Let two parties, X and Y, pick random numbers x and y , $1 < x, y < p$. They each calculate

$$(b^x) \bmod p$$

and

$$(b^y) \bmod p$$

and transmit them to each other. Now, X knows x and $(b^y) \bmod p$, so s/he can calculate $(b^y)^x \bmod p =$

$(b^{xy}) \bmod p$. Y can do the same calculation. Now they both know $(b^{xy}) \bmod p$. But eavesdroppers know only $(b^x) \bmod p$ and $(b^y) \bmod p$, and can't use those quantities to recover the shared secret. Typically, of course, X and Y will use that shared secret as a key to a conventional cryptosystem.

"The biggest problem with the algorithm, as outlined above, is that there is no authentication. An attacker can sit in the middle and speak that protocol to each legitimate party.

"One last point -- you can treat x as a secret key, and publish $(b^X) \bmod p$ as a public key. Proof is left as an exercise for the reader." [Steve Bellovin, 1993-07-17]

- Why it's important
 - + Using it
 - + Matt Ghio has made available Phil Karn's program for generating numbers useful for D-H:
 - ftp cs.cmu.edu:
/afs/andrew.cmu.edu/usr12/mg5n/public/Karn.DH.generator
 - + Variants and Comments
 - + Station to Station protocol
 - "The STS protocol is a regular D-H followed by a (delicately designed) exchange of signatures on the key exchange parameters. The signatures in the second exchange that they can't be separated from the original parameters.....STS is a well-thought out protocol, with many subtleties already arranged for. For the issue at hand, though, which is Ethernet sniffing, it's authentication aspects are not required now, even though they certainly will be in the near future."
[Eric Hughes, 1994-02-06]
- 5.7.6. groups, multiple encryption, IDEA, DES, difficulties in analyzing
- 5.7.7. "Why and how is "randomness" tested?"
- Randomness is a core concept in cryptography. Ciphers often fail when things are not as random as designers thought they would be.
 - Entropy, randomness, predictability. Can never actually prove a data set is random, though one can be fairly confident (cf. Kolmogorov-Chaitin complexity theory).
 - Still, tricks can make a random-looking text block look regular....this is what decryption does; such files are said to be cryptoregular.
 - + As to how much testing is needed, this depends on the use, and on the degree of confidence needed. It may take millions of test samples, or even more, to establish randomness in set of data. For example:
 - "The standard tests for 'randomness' utilized in govt systems requires 1×10^6 samples. Most of the tests are standard probability stuff and some are classified. "
[Wray Kephart, sci.crypt, 1994-08-07]
 - never assume something is really random just because it looks random! (Dynamic Markov compressors can find

nonrandomness quickly.)

5.7.8. "Is it possible to tell if a file is encrypted?"

- Not in general. Undecideability and all that. (Can't tell in general if a virus exists in code, Adleman showed, and can't tell in general if a file is encrypted, compressed, etc. Goes to issues of what we mean by encrypted or compressed.)
- + Sometimes we can have some pretty clear signals:
 - headers are attached
 - other characteristic signs
 - entropy per character
- + But files encrypted with strong methods typically look random; in fact, randomness is closely related to encryption.
 - + regularity: all symbols represented equally, in all bases (that is, in doubles, triples, and all n-tuples)
 - "cryptoregular" is the term: file looks random (regular) until proper key is applied, then the randomness vanishes. Charles Bennett, "Physics of Computation Workshop," 1993]
 - "entropy" near the maximum (e.g., near 6 or 7 bits per character, whereas ordinary English has roughly 1.5-2 bits per character of entropy)

5.7.9. "Why not use CD-ROMs for one-time pads?"

- The key distribution problem, and general headaches. Theft or compromise of the keying material is of course the greatest threat.
- And one-time pads, being symmetric ciphers, give up the incredible advantages of public key methods.
- "CD ROM is a terrible medium for the OTP key stream. First, you want exactly two copies of the random stream. CD ROM has an economic advantage only for large runs. Second, you want to destroy the part of the stream already used. CD ROM has no erase facilities, outside of physical destruction of the entire disk." [Bryan G. Olson, sci.crypt, 1994-08-31]
- If you have to have a one-time pad, a DAT makes more sense; cheap, can erase the bits already used, doesn't require pressing of a CD, etc. (One company claims to be selling CD-ROMs as one-time pads to customers...the security problems here should be obvious to all.)

5.8. The Nature of Cryptology

5.8.1. "What are the truly basic, core, primitive ideas of cryptology, crypto protocols, crypto anarchy, digital cash, and the things we deal with here?"

- I don't just mean things like the mechanics of encryption, but more basic conceptual ideas.

5.8.2. Crypto is about the creation and linking of private spaces...

5.8.3. The "Core" Ideas of Cryptology and What we Deal With

- Physics has mass, energy, force, momentum, angular momentum, gravitation, friction, the Uncertainty Principle, Complementarity, Least Action, and a hundred other such concepts and principles, some more basic than others. Ditto for any other field.
- + It seems to many of us that crypto is part of a larger study of core ideas involving: identity, proof, complexity,

- randomness, reputations, cut-and-choose protocols, zero knowledge, etc. In other words, the buzzwords.
- But which of these are "core" concepts, from which others are derived?
- Why, for example, do the "cut-and-choose" protocols work so well, so fairly? (That they do has been evident for a long time, and they literally are instances of Solomonic wisdom. Game theory has explanations in terms of payoff matrices, Nash equilibria, etc. It seems likely to me that the concepts of crypto will be recast in terms of a smaller set of basic ideas taken from these disparate fields of economics, game theory, formal systems, and ecology. Just my hunch.)
- + statements, assertions, belief, proof
 - "I am Tim"
 - + possession of a key to a lock is usually treated as proof of...
 - not always, but that's the default assumption, that someone who unlocks a door is one of the proper people..access privileges, etc.
- 5.8.4. We don't seem to know the "deep theory" about why certain protocols "work." For example, why is "cut-and-choose," where Alice cuts and Bob chooses (as in fairly dividing a pie), such a fair system? Game theory has a lot to do with it. Payoff matrices, etc.
 - But many protocols have not been fully studied. We know they work, but I think we don't know fully why they work. (Maybe I'm wrong here, but I've seen few papers looking at these issues in detail.)
 - Economics is certainly crucial, and tends to get overlooked in analysis of crypto protocols....the various "Crypto Conference Proceedings" papers typically ignore economic factors (except in the area of measuring the strength of a system in terms of computational cost to break).
 - "All crypto is economics."
 - We learn what works, and what doesn't. My hunch is that complex crypto systems will have emergent behaviors that are discovered only after deployment, or good simulation (hence my interest in "protocol ecologies").
- 5.8.5. "Is it possible to create ciphers that are unbreakable in any amount of time with any amount of computer power?"
 - + Information-theoretically secure vs. computationally-secure
 - + not breakable even in principle, e.g., a one-time pad with random characters selected by a truly random process (die tosses, radioactive decay, certain types of noise, etc.)
 - and ignoring the "breakable by break-ins" approach of stealing the one-time pad, etc. ("Black bag cryptography")
 - not breakable in "reasonable" amounts of time with computers
 - Of course, a one-time pad (Vernam cipher) is theoretically unbreakable without the key. It is "information-theoretically secure."
 - RSA and similar public key algorithms are said to be only "computationally-secure," to some level of security dependent on modulus length, computer resources and time

available, etc. Thus, given enough time and enough computer power, these ciphers are breakable.

- However, they may be practically impossible to break, given the amount of energy in the universe. Not to split universes here, but it is interesting to consider that some ciphers may not be breakable in our universe, in any amount of time. Our universe presumably has some finite number of particles (currently estimated to be 10^{73} particles). This leads to the "even if every particle were a Cray Y-MP it would take..." sorts of thought experiments.

But I am considering energy here. Ignoring reversible computation for the moment, computations dissipate energy (some disagree with this point). There is some upper limit on how many basic computations could ever be done with the amount of free energy in the universe. (A rough calculation could be done by calculating the energy output of stars, stuff falling into black holes, etc., and then assuming about kT per logical operation. This should be accurate to within a few orders of magnitude.) I haven't done this calculation, and won't today, but the result would likely be something along the lines of X joules of energy that could be harnessed for computation, resulting in Y basic primitive computational steps.

I can then find a modulus of 3000 digits or 5000 digits, or whatever, that takes more than this number of steps to factor.

Caveats:

1. Maybe there are really shortcuts to factoring. Certainly improvements in factoring methods will continue. (But of course these improvements are not things that convert factoring into a less than exponential-in-length problem...that is, factoring appears to remain "hard.")
2. Maybe reversible computations (a la Landauer, Bennett, et. al.) actually work. Maybe this means a "factoring machine" can be built which takes a fixed, or very slowly growing, amount of energy.
3. Maybe the quantum-mechanical idea of Shore is possible. (I doubt it, for various reasons.)

I continue to find it useful to think of very large numbers as creating "force fields" or "bobbles" (a la Vinge) around data. A 5000-decimal-digit modulus is as close to being unbreakable as anything we'll see in this universe.

5.9. Practical Crypto

5.9.1. again, this stuff is covered in many of the FAQs on PGP and on security that are floating around...

5.9.2. "How long should crypto be valid for?"

- + That is, how long should a file remain uncrackable, or a digital signature remain unforgeable?
- probabilistic, of course, with varying confidence levels

- depends on breakthroughs, in math and in computer power
 - + Some messages may only need to be valid for a few days or weeks. Others, for decades. Certain contracts may need to be unforgeable for many decades. And given advances in computer power, what appears to be a strong key today may fail utterly by 2020 or 2040. (I'm of course not suggesting that a 300- or 500-digit RSA modulus will be practical by then.)
 - + many people only need security for a matter of months or so, while others may need it (or think they need it) for decades or even for generations
 - they may fear retaliation against their heirs, for example, if certain communications were ever made public
 - "If you are signing the contract digitally, for instance, you would want to be sure that no one could forge your signature to change the terms after the fact -- a few months isn't enough for such purposes, only something that will last for fifteen or twenty years is okay." [Perry Metzger, 1994-07-06]
- 5.9.3. "What about commercial encryption programs for protecting files?"
- ViaCrypt, PGP 2.7
 - Various commercial programs have existed for years (I got "Sentinel" back in 1987-8...long since discontinued). Check reviews in the leading magazines.
 - + Kent Marsh, FolderBolt for Macs and Windows
 - "The best Mac security program...is CryptoMactic by Kent Marsh Ltd. It uses triple-DES in CBC mode, hashes an arbitrary-length password into a key, and has a whole lot of Mac-interface features. (The Windows equivalent is FolderBolt for Windows, by the way.)" [Bruce Schneier, sci.crypt, 1994-07-19]
- 5.9.4. "What are some practical steps to take to improve security?"
- Do you, like most of us, leave backup diskettes laying around?
 - Do you use multiple-pass erasures of disks? If not, the bits may be recovered.
 - (Either of these can compromise all encrypted material you have, all with nothing more than a search warrant of your premises.)
- 5.9.5. Picking (and remembering) passwords
- Many of the issues here also apply to choosing remailers, etc. Things are often trickier than they seem. The "structure" of these spaces is tricky. For example, it may seem really sneaky (and "high entropy" to permute some words in a popular song and use that as a pass phrase....but this is obviously worth only a few bits of extra entropy. Specifically, the attacker will like take the thousand or so most popular songs, thousand or so most popular names, slogans, speeches, etc., and then run many permutations on each of them.
 - bits of entropy
 - lots of flaws, weaknesses, hidden factors
 - avoid simple words, etc.
 - hard to get 100 or more bits of real entropy
 - As Eli Brandt puts it, "Obscurity is no substitute for

- strong random numbers." [E.B., 1994-07-03]
- Cryptanalysis is a matter of deduction, of forming and refining hypotheses. For example, the site "bitbucket@ee.und.ac.za" is advertised on the Net as a place to send "NSA food" to...mail sent to it gets discarded. So , a great place to send cover traffic to, no? No, as the NSA will mark this site for what it is and its usefulness is blown. (Unless its usefulness is actually something else, in which case the recursive descent has begun.)
 - Bohdan Tashchuk suggests [1994-07-04] using telephone-like numbers, mixed in with words, to better fit with human memorization habits; he notes that 30 or more bits of entropy are routinely memorized this way.
- 5.9.6. "How can I remember long passwords or passphrases?"
- Lots of security articles have tips on picking hard-to-guess (high entropy) passwords and passphrases.
 - + Just do it.
 - People can learn to memorize long sequences. I'm not good at this, but others apparently are. Still, it seems dangerous, in terms of forgetting. (And writing down a passphrase may be vastly more risky than a shorter but more easily memorized passphrase is. I think theft of keys and keystroke capturing on compromised machines are much more important practical weaknesses.)
 - + The first letters of long phrases that have meaning only to the owner.
 - e.g., "When I was ten I ate the whole thing."---> "wiwtiatwt" (Purists will quibble that prepositional phrases like "when i was" have lower entropy. True, but better than "Joshua.")
 - + Visual systems
 - Another approach to getting enough entropy in passwords/phrases is a "visual key" where one mouses from position to position in a visual environment. That is, one is presented with a scene containg some number of nodes, perhaps representing familiar objects from one's own home, and a path is chosen. The advantage is that most people can remember fairly complicated (read: high entropy) "stories." Each object triggers a memory of the next object to visit. (Example: door to kitchen to blender to refrigerator to) This is the visual memory system said to be favored by Greek epic poets. This also gets around the keyboard-monitoring trick (but not necessarily the CRT-reading trick, of course).

It might be an interesting hack to offer this as a front end for PGP. Even a simple grid of characters which could be moused on could be an assist in using long passphrases.

5.10. DES

5.10.1. on the design of DES

- Biham and Shamir showed how "differential cryptanalysis"

could make the attack easier than brute-force search of the 2^{56} keyspace. Wiener did a thought experiment design of a "DES buster" machine (who ya gonna call?) that could break a DES key in a matter of days. (Similar to the Diffie and Hellman analysis of the mid-70s, updated to current technology.)

- + The IBM designers knew about differential cryptanalysis, it is now clear, and took steps to optimize DES. After Shamir and Biham published, Don Coppersmith acknowledged this. He's written a review paper:
 - Coppersmith, D., "The Data Encryption Standard (DES) and its strength against attacks." IBM Journal of Research and Development. 38(3): 243-250. (May 1994)

5.11. Breaking Ciphers

5.11.1. This is not a main Cypherpunks concern, for a variety of reasons (lots of work, special expertise, big machines, not a core area, ciphers always win in the long run). Breaking ciphers is something to consider, hence this brief section.

5.11.2. "What are the possible consequences of weaknesses in crypto systems?"

- maybe reading messages
- maybe forging messages
- maybe faking timestamped documents
- maybe draining a bank account in seconds
- maybe winning in a crypto gambling system
- maybe matters of life and death

5.11.3. "What are the weakest places in ciphers, practically speaking?"

- Key management, without a doubt. People leave their keys lying around, write down their passphrases. etc.

5.11.4. Birthday attacks

5.11.5. For example, at Crypto '94 it was reported in a rump session (by Michael Wiener with Paul van Oorschot) that a machine to break the MD5 ciphers could be built for about \$10 M (in 1994 dollars, of course) and could break MD5 in about 20 days. (This follows the 1993 paper on a similar machine to break DES.)

- Hal Finney did some calculations and reported to us:
- "I mentioned a few days ago that one of the "rump session" papers at the crypto conference claimed that a machine could be built which would find MD5 collisions for \$10M in about 20 days.....The net result is that we have taken virtually no more time (the 2^{64} creations of MD5 will dominate) and virtually no space (compared to 2^{64} stored values) and we get the effect of a birthday attack. This is another cautionary data point about the risks of relying on space costs for security rather than time costs." [Hal Finney, 1994-09-09]

5.11.6. pkzip reported broken

- "I finally found time to take a closer look at the encryption algorithm by Roger Schlafly that is used in PKZIP and have developed a practical known plaintext attack that can find the entire 96-bit internal state." [Paul Carl Kocher, comp.risks, 1994-09-04]

5.11.7. Gaming attacks, where loopholes in a system are exploited

- contests that are defeated by automated attacks

- the entire legal system can be viewed this way, with competing teams of lawyers looking for legal attacks (and the more complex the legal code, the more attacks can be mounted)
 - ecologies, where weaknesses are exploited ruthlessly, forcing most species into extinction
 - economies, ditto, except must faster
 - the hazards for crypto schemes are clear
 - + And there are important links to the issue of overly formal systems, or systems in which ordinary "discretion" and "choice" is overridden by rules from outside
 - as with rules telling employers in great detail when and how they can discharge employees (cf. the discussion of "reasonable rules made mandatory," elsewhere)
 - such rules get exploited by employees, who follow the "letter of the law" but are performing in a way unacceptable to the employer
 - related to "locality of reference" points, in that problem should be resolved locally, not with intervention from afar.
 - things will never be perfect, from the perspective of all parties, but meddling from outside makes things into a game, the whole point of this section
 - + Implications for digital money: overly complex legal systems, without the local advantages of true cash (settled locally)
 - + may need to inject some supra-legal enforcement mechanisms into the system, to make it converge
 - offshore credit databases, beyond reach of U.S. and other laws
 - + physical violence (one reason people don't "play games" with Mafia, Triads, etc., is that they know the implications)
 - it's not unethical, as I see it, for contracts in which the parties understand that a possible or even likely consequence of their failure to perform is death
- 5.11.8. Diffie-Hellman key exchange vulnerabilities
- "man-in-the-middle" attack
 - + phone systems use voice readback of LCD indicated number
 - as computer power increases, even this may be insufficient
- 5.11.9. Reverse engineering of ciphers
- A5 code used in GSM phones was reverse engineered from a hardware description
 - Graham Toal reports (1994-07-12) that GCHQ blocked a public lectures on this
- 5.12. Loose Ends
- 5.12.1. "Chess Grandmaster Problem" and other Frauds and Spoofs
- of central importance to proofs of identity (a la Fiat-Shamir)
 - "terrorist" and "Mafia spoof" problems
6. The Need For Strong Crypto
- 6.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666,
1994-09-10, Copyright Timothy C. May. All rights reserved.
See the detailed disclaimer. Use short sections under "fair
use" provisions, with appropriate credit, but don't put your
name on my words.

6.2. SUMMARY: The Need For Strong Crypto

6.2.1. Main Points

- Strong crypto reclaims the power to decide for one's self,
to deny the "Censor" the power to choose what one reads,
watches, or listens to.

6.2.2. Connections to Other Sections

6.2.3. Where to Find Additional Information

6.2.4. Miscellaneous Comments

- this section is short, but is less focussed than other
sections; it is essentially a "transition" chapter.

6.3. General Uses of and Reasons for Crypto

6.3.1. (see also the extensive listing of "Reasons for Anonymity," which makes many points about the need and uses for strong crypto)

6.3.2. "Where is public key crypto really needed?"

- "It is the case that there is relatively little need for
asymmetric key cryptography in small closed populations.
For example, the banks get along quite well without. The
advantage of public key is that it permits private
communication in a large and open population and with a
minimum of prearrangement." [WHMurray, sci.crypt, 1994-08-
25]
- That is, symmetric key systems (such as conventional
ciphers, one time pads, etc.) work reasonably well by
prearrangement between parties. And of course one time pads
have the additional advantage of being information-
theoretically secure. But asymmetric or public key methods
are incredibly useful when: the parties have not met
before, when key material has not been exchanged, and when
concerns exist about storing the key material. The so-
called "key management problem" when N people want to
communicate pairwise with each other is well-founded.
- And of course public key crypto makes possible all the
other useful stuff like digital money, DC-Nets, zero
knowledge proofs, secret sharing, etc.

6.3.3. "What are the main reasons to use cryptography?"

- people encrypt for the same reason they close and lock
their doors
- + Privacy in its most basic forms
 - text -- records, diaries, letters, e-mail
 - sound -- phone conversations
 - other --video
- + phones, intercepts, cellular, wireless, car phones,
scanners
 - + making listening illegal is useless (and wrong-headed)
 - and authorities are exempt from such laws
- people need to protect, end to end
- + "How should I protect my personal files, and my phone
calls?"
 - Personally, I don't worry too much. But many people do.

- Encryption tools are widely available.
- Cellular telephones are notoriously insecure, as are cordless phones (even less secure). There are laws about monitoring, small comfort as that may be. (And I'm largely opposed to such laws, for libertarian reasons and because it creates a false sense of security.)
- Laptops are probably less vulnerable to Van Eck types of RF monitoring than are CRTs. The trend to lower power, LCDs, etc., all works toward decreasing vulnerability. (However, computer power for extracting weak signals out of noise is increasing faster than RF are decreasing....tradeoffs are unclear.)
- + encrypting messages because mail delivery is so flaky
 - that is, mail is misdelivered, via hosts incorrectly processing the addresses
 - encryption obviously prevents misunderstandings (though it does little to get the mail delivered correctly)
- + Encryption to Protect Information
 - the standard reason
 - + encryption of e-mail is increasing
 - the various court cases about employers reading ostensibly private e-mail will sharpen this debate (and raise the issue of employers forbidding encryption; resonances with the mostly-settled issue of reasonable use of company phones for private calls-more efficient to let some personal calls be made than to lose the time of employees going to public phones)
 - + encryption of faxes will increase, too, especially as technology advances and as the dangers of interception become more apparent
 - also, tighter links between sender and receive, as opposed to the current "dial the number and hope it's the right one" approach, will encourage the additional use of encryption
 - "electronic vaulting" of large amounts of information, sent over T1 and T3 data networks, e.g., backup material for banks and large corporations
- + the miles and miles of network wiring within a corporation-LANs, WANs, Novell, Ethernet, TCP-IP, Banyan, and so on-cannot all be checked for taps...who would even have the records to know if some particular wire is going where it should? (so many undocumented hookups, lost records, ad hoc connections, etc.)
 - the solution is to have point-to-point encryption, even withing corporations (for important items, at least)
- wireless LANs
- + corporations are becoming increasingly concerned about interception of important information-or even seemingly minor information-and about hackers and other intruders
 - calls for network security enhancement
 - they are hiring "tiger teams" to beef up security
- + cellular phones
 - interceptions are common (and this is becoming publicized)
 - modifications to commercial scanners are describe in newsletters

- something like Lotus Notes may be a main substrate for the effective introduction of crypto methods (ditto for hypertext)
- encryption provides "solidity" to cyberspace, in the sense of creating walls, doors, permanent structures
- there may even be legal requirements for better security over documents, patient files, employee records, etc.
- + Encryption of Video Signals and Encryption to Control Piracy
 - this is of course a whole technology and industry
 - Videocypher II has been cracked by many video hackers
 - a whole cottage industry in cracking such cyphers
 - note that outlawing encryption would open up many industries to destruction by piracy, which is yet another reason a wholesale ban on encryption is doomed to failure
- Protecting home videos--several cases of home burglaries where private x-rated tapes of stars were taken, then sold (Leslile Visser, CBS Sports)
- these general reasons will make encryption more common, more socially and legally acceptable, and will hence make eventual attempts to limit the use of crypto anarchy methods moot
- + Digital Signatures and Authentication
 - + for electronic forms of contracts and digital timestamping
 - not yet tested in the courts, though this should come soon (perhaps by 1996)
 - + could be very useful for proving that transactions happened at a certain time (Tom Clancy has a situation in "Debt of Honor" in which all Wall Street central records of stock trades are wiped out in a software scheme: only the records of traders are useful, and they are worried about these being fudged to turn profits...timestamping would help immensely)
 - though certain spoofs, a la the brilliant penny scam, are still possible (register multiple trades, only reveal the profitable ones)
 - negotiations
 - AMIX, Xanadu, etc.
- + is the real protection against viruses (since all other scanning methods will increasingly fail)
 - software authors and distributors "sign" their work...no virus writer can possibly forge the digital signature
- + Proofs of identity, passwords, and operating system use
 - ZKIPS especially in networks, where the chances of seeing a password being transmitted are much greater (an obvious point that is not much discussed)
- + operating systems and databases will need more secure procedures for access, for agents and the like to pay for services, etc.
 - unforgeable tokens
- + Cyberspace will need better protection
 - to ensure spoofing and counterfeiting is reduced (recall Habitat's problems with people figuring out the loopholes)

- + if OH is also working on "world- building" at Los Alamos, he may be using evolutionary systems and abstract math to help build better and more "coherent" worlds
 - agents, demons, structures, persistent objects
 - encryption to protect these structures
 - + the abstract math part of cyberspace: abstract measure spaces, topologies, distance metrics
 - may figure in to the balance between user malleability and rigidity of the space
 - Chaitin's AIT...he has obtained measures for these
 - + Digital Contracts
 - e-mail too easily forged, faked (and lost, misplaced)
 - + Anonymity
 - remailing
 - law avoidance
 - samizdats,
 - Smart cards, ATMs, etc.
 - Digital Money
 - Voting
 - + Information Markets
 - data havens, espionage
 - + Privacy of Purchases
 - for general principles, to prevent a surveillance society
 - + specialized mailing lists
 - vendors pay to get names (Crest labels)
 - Smalltalk job offers
 - in electronic age, will be much easier to "troll" for specialized names
 - people will want to "selectively disclose" their interests (actually, some will, some won't)
- 6.3.4. "What may limit the use of crypto?"
- + "It's too hard to use"
 - multiple protocols (just consider how hard it is to actually send encrypted messages between people today)
 - the need to remember a password or passphrase
 - + "It's too much trouble"
 - the argument being that people will not bother to use passwords
 - partly because they don't think anything will happen to them
 - + "What have you got to hide?"
 - e.g.,, imagine some comments I'd have gotten at Intel had I encrypted everything
 - and governments tend to view encryption as ipso facto proof that illegalities are being committed: drugs, money laundering, tax evasion
 - recall the "forfeiture" controversy
 - + Government is taking various steps to limit the use of encryption and secure communication
 - some attempts have failed (S.266), some have been shelved, and almost none have yet been tested in the courts
 - see the other sections...
 - + Courts Are Falling Behind, Are Overcrowded, and Can't Deal Adequately with New Issues-Such as Encryption and Cryonics
 - which raises the issue of the "Science Court" again

- and migration to private adjudication (regulatory arbitration)
- BTW, anonymous systems are essentially the ultimate merit system (in the obvious sense) and so fly in the face of the "hiring by the numbers" de facto quota systems now creeping in to so many areas of life....there may be rules requiring all business dealings to keep track of the sex, race, and "ability group" (I'm kidding, I hope) of their employees and their consultants

6.3.5. "What are some likely future uses of crypto?"

- Video conferencing: without crypto, or with government access, corporate meetings become public...as if a government agent was sitting in a meeting, taking notes. (There may be some who think this is a good idea, a check on corporate shenanigans. I don't. Much too high a price to pay for marginal or illusory improvements.)
- presenting unpopular views
- + getting and giving medical treatments
 - with or without licenses from the medical union (AMA)
 - unapproved treatments
- bootleg medical treatments
- information markets
- + sanctuary movements, underground railroads
 - for battered wives
 - and for fathers taking back their children
 - (I'm not taking sides)
- smuggling
- tax evasion
- data havens
- bookies, betting, numbers games
- remailers, anonymity
- religious networks (digital confessionals)
- digital cash, for privacy and for tax evasion
- digital hits
- newsgroup participation -- archiving of Netnews is commonplace, and increases in storage density make it likely that in future years one will be able to purchase disks with "Usenet, 1985-1995" and so forth (or access, search, etc. online sites)

6.3.6. "Are there illegal uses of crypto?"

- Currently, there are no blanket laws in the U.S. about encryption.
- + There are specific situations in which encryption cannot be freely used (or the use is spelled out)
 - over the amateur radio airwave...keys must be provided
- + Carl Ellison has noted many times that cryptography has been in use for many centuries; the notion that it is a "military" technology that civilians have somehow gotten ahead of is just plain false.
 - and even public key crypto was developed in a university (Stanford, then MIT)

6.4. Protection of Corporate and Financial Privacy

- #### 6.4.1. corporations are becoming increasingly concerned about interception of important information-or even seemingly minor information-and about hackers and other intruders
- calls for network security enhancement

- they are hiring "tiger teams" to beef up security
 - + cellular phones
 - interceptions are common (and this is becoming publicized)
 - modifications to commercial scanners are describe in newsletters
 - something like Lotus Notes may be a main substrate for the effective introduction of crypto methods (ditto for hypertext)
- 6.4.2. Corporate Espionage (or "Business Research")
- + Xeroxing of documents
 - recall the way Murray Woods inspected files of Fred Buch, suspecting he had removed the staples and Xeroxed the documents for Zilog (circa late 1977)
 - a precedent: shapes of staples
 - + colors of the paper and ink...blues, for example
 - but these low-tech schemes are easy to circumvent
 - + Will corporations crack down on use of modems?
 - + after all, the specs of a chip or product could be mailed out of the company using the companies own networks!
 - applies to outgoing letters as well (and I've never heard of any company inspecting to this detail, though it may happen at defense contractors)
 - + and messages can still be hidden (covert channels)
 - albeit at much lower bandwidths and with more effort required (it'll stop the casual leakage of information)
 - the LSB method (though this still involves a digital storage means, e.g., a diskette, which might be restricted)
 - various other schemes: buried in word processing format (at low bandwidth)
 - subtleties such as covert channels are not even considered by corporations-too many leakage paths!
 - + it seems likely that government workers with security clearances will face restrictions on their access to AMIX-like systems, or even to "private" use of conventional databases
 - at least when they use UseNet, the argument will go, they can be overseen to some extent
 - + Offsite storage and access of stolen material
 - + instead of storing stolen blueprints and schematics on company premises, they may be stored at a remote location
 - possibly unknown to the company, via cryptoanarchy techniques
 - + "Business research" is the euphemism for corporate espionage
 - often hiring ex-DIA and CIA agents
 - + American companies may step up their economic espionage once it is revealed just how extensive the spying by European and Japanese companies has been
 - Chobetsu reports to MITI
 - Mossad aids Israeli companies, e.g., Elscint. Elbit
 - + Bidzos calls this "a digital Pearl Harbor" (attacks on network security)
 - would be ironic if weaknesses put into encryption gear came back to haunt us
 - + corporations will want an arms length relationship with

corporate spies, to protect themselves against lawsuits, criminal charges, etc.

- third party research agencies will be used

6.4.3. Encryption to Protect Information

- the standard reason
- + encryption of e-mail is increasing
 - the various court cases about employers reading ostensibly private e-mail will sharpen this debate (and raise the issue of employers forbidding encryption; resonances with the mostly-settled issue of reasonable use of company phones for private calls-more efficient to let some personal calls be made than to lose the time of employees going to public phones)
- + encryption of faxes will increase, too, especially as technology advances and as the dangers of interception become more apparent
 - also, tighter links between sender and receive, as opposed to the current "dial the number and hope it's the right one" approach, will encourage the additional use of encryption
- "electronic vaulting" of large amounts of information, sent over T1 and T3 data networks, e.g., backup material for banks and large corporations
- + the miles and miles of network wiring within a corporation-LANs, WANs, Novell, Ethernet, TCP-IP, Banyan, and so on-cannot all be checked for taps...who would even have the records to know if some particular wire is going where it should? (so many undocumented hookups, lost records, ad hoc connections, etc.)
 - the solution is to have point-to-point encryption, even withing corporations (for important items, at least)
- wireless LANs
- encryption provides "solidity" to cyberspace, in the sense of creating walls, doors, permanent structures
- there may even be legal requirements for better security over documents, patient files, employee records, etc.

6.4.4. U.S. willing to seize assets as they pass through U.S. (Haiti, Iraq)

6.4.5. Privacy of research

- attacks on tobacco companies, demanding their private research documents be turned over to the FDA (because tobacco is "fair game" for all such attacks, ...)

6.4.6. Using crypto-mediated business to bypass "deep pockets" liability suits, abuse of regulations, of the court system, etc.

- + Abuses of Lawsuits: the trend of massive judgments...several million for a woman burned when she spilled hot coffee at a MacDonald's (\$160K for damages, the rest for "punitive damages")
 - billions of dollars for various jury decisions
 - "deep pockets" lawsuits are a new form of populism, of de Tocqueville's pocket-picking
- + For example, a shareware author might collect digital cash without being traceable by those who feel wronged
 - Is this "right"? Well, what does the contract say? If the customer bought or used the product knowing that the author/seller was untraceable, and that no additional

warranties or guarantees were given, what fraud was committed?

+ crypto can, with some costs, take interactions out of the reach of courts

- replacing the courts with PPL-style private-produced justice

6.4.7. on anonymous communication and corporations

- Most corporations will avoid anonymous communications, fearing the repercussions, the illegality (vis-a-vis antitrust law), and the "unwholesomeness" of it

+ Some may use it to access competitor intelligence, offshore data havens, etc.

- Even here, probably through "arm's length" relationships with outside consultants, analogous to the cutouts used by the CIA and whatnot to insulate themselves from charges

- Boldest of all will be the "crypto-zaibatsu" that use strong crypto of the crypto anarchy flavor to arrange collusive deals, to remove competitors via force, and to generally pursue the "darker side of the force," to coin a phrase.

6.5. Digital Signatures

6.5.1. for electronic forms of contracts

- not yet tested in the courts, though this should come soon (perhaps by 1996)

6.5.2. negotiations

6.5.3. AMIX, Xanadu, etc.

6.5.4. is the real protection against viruses (since all other scanning methods will increasingly fail)

- software authors and distributors "sign" their work...no virus writer can possibly forge the digital signature

6.6. Political Uses of Crypto

6.6.1. Dissidents, Amnesty International

- Most governments want to know what their subjects are saying...

- Strong crypto (including steganography to hide the existence of the communications) is needed

- Myanmar (Burma) dissidents are known to be using PGP

6.6.2. reports that rebels in Chiapas (Mexico, Zapatistas) are on the Net, presumably using PGP

- (if NSA can really crack PGP, this is probably a prime target for sharing with the Mexican government)

6.6.3. Free speech has declined in America--crypto provides an antidote

- people are sued for expressing opinions, books are banned ("Loompanics Press" facing investigations, because some children ordered some books)

+ SLAPP suits (Strategic Lawsuits Against Public

Participation), designed to scare off differing opinions by threatening legal ruination in the courts

- some judges have found for the defendants and ordered the SLAPPers to pay damages themselves, but this is still a speech-chilling trend

- crypto untraceability is good immunity to this trend, and is thus *real* free speech

6.7. Beyond Good and Evil, or, Why Crypto is Needed

6.7.1. "Why is cryptography good? Why is anonymity good?"

- These moral questions pop up on the List once in a while, often asked by someone preparing to write a paper for a class on ethics or whatnot. Most of us on the list probably think the answers are clearly "yes," but many in the public may not think so. The old dichotomy between "None of your damned business" and "What have you got to hide?"
- "Is it good that people can write diaries unread by others?" "Is it good that people can talk to each other without law enforcement knowing what they're saying?" "Is it good that people can lock their doors and hide from outsiders?" These are all essentially equivalent to the questions above.
- Anonymity may not be either good or not good, but the outlawing of anonymity would require a police state to enforce, would impinge on basic ideas about private transactions, and would foreclose many options that some degree of anonymity makes possible.
- "People should not be anonymous" is a normative statement that is impractical to enforce.

6.7.2. Speaking of the isolation from physical threats and pressures

that cyberspace provides, Eric Hughes writes: "One of the whole points of anonymity and pseudonymity is to create immunity from these threats, which are all based upon the human body and its physical surroundings. What is the point of a system of anonymity which can be pierced when something "bad" happens? These systems do not reject the regime of violence; rather, they merely mitigate it slightly further and make their morality a bit more explicit.....I desire systems which do not require violence for their existence and stability. I desire anonymity as an ally to break the hold of morality over culture." [Eric Hughes, 1994-08-31]

6.7.3. Crypto anarchy means prosperity for those who can grab it,

those competent enough to have something of value to offer for sale; the clueless 95% will suffer, but that is only just. With crypto anarchy we can painlessly, without initiation of aggression, dispose of the nonproductive, the halt and the lame. (Charity is always possible, but I suspect even the liberal do-gooders will throw up their hands at the prospect of a nation of mostly unskilled and essentially illiterate and innumerate workers being unable to get meaningful, well-paying jobs.)

6.7.4. Crypto gets more important as communication increases and as computing gets distributed

- + with bits and pieces of one's environment scattered around
 - have to worry about security
 - others have to also protect their own products, and yet still provide/sell access
- private spaces needed in disparate locations...multinationals, teleconferencing, video

6.8. Crypto Needed for Operating Systems and Networks

6.8.1. Restrictions on cryptography--difficult as they may be to enforce--may also impose severe hardships on secure operating system design, Norm Hardy has made this point several times.

- Agents and objects inside computer systems will likely need security, credentials, robustness, and even digital money for transactions.

6.8.2. Proofs of identity, passwords, and operating system use

- ZKIPS especially in networks, where the chances of seeing a password being transmitted are much greater (an obvious point that is not much discussed)
- + operating systems and databases will need more secure procedures for access, for agents and the like to pay for services, etc.
 - unforgeable tokens

6.8.3. An often unmentioned reason why encryption is needed is for the creation of private, or virtual, networks

- so that channels are independent of the "common carrier"
- + to make this clear: prospects are dangerously high for a consolidation under government control of networks
 - in parallel with roads
 - + and like roads, may insist on equivalent of licenses
 - is-a-person
 - bans on encryption
 - The Nightmare Scenario: "We own the networks, we won't let anyone install new networks without our approval, and we will make the laws about what gets carried, what encryption can be used, and how taxes will be collected."
 - Fortunately, I doubt this is enforceable...too many ways to create virtual networks...satellites like Iridium, fiber optics, ways to hide crypto or bury it in other traffic
- + cyberspace walls...
 - + more than just crypto: physical security is needed (and for much the same reason no "digital coin" exists)
 - processes running on controlled-access machines (as with remailers)
 - access by crypto
 - + a web of mutually suspicious machines may be sufficient
 - robust cyberspaces built with DC-Net ("dining cryptographers") methods?

6.9. Ominous Trends

6.9.1. Ever-increasing numbers of laws, complexities of tax codes, etc.

- individuals no longer can navigate

6.9.2. National ID cards

- work permits, immigration concerns, welfare fraud, stopping terrorists, collecting taxes
- USPS and other proposals

6.9.3. Key Escrow

6.9.4. Extension of U.S. law around the world

- Now that the U.S. has vanquished the U.S.S.R., a free field ahead of it for spreading the New World Order, led of course by the U.S.A. and its politicians.
 - treaties, international agreements
 - economic hegemony
 - U.N. mandates, forces, "blue helmets"

6.9.5. AA BBS case means cyberspace is not what we thought it was

6.10. Loose Ends

- 6.10.1. "Why don't most people pay more attention to security issues?"
 - Fact is, most people never think about real security.
 - Safe manufacturers have said that improvements in safes (the metal kind) were driven by insurance rates. A direct incentive to spend more money to improve security (cost of better safe < cost of higher insurance rate).
 - Right now there is almost no economic incentive for people to worry about PIN security, about protecting their files, etc. (Banks eat the costs and pass them on...any bank which tried to save a few bucks in losses by requiring 10-digit PINs--which people would *write down* anyway!--would lose customers. Holograms and pictures on bank cards are happening because the costs have dropped enough.)
 - Crypto is economics. People will begin to really care when it costs them.

- 6.10.2. What motivates an attackers is not the intrinsic value of the data but his perception of the value of the data.
- 6.10.3. Crypto allows more refinement of permissions...access to groups, lists
 - beyond such crude methods as banning domain names or "edu" sorts of accounts
- 6.10.4. these general reasons will make encryption more common, more socially and legally acceptable, and will hence make eventual attempts to limit the use of crypto anarchy methods moot
- 6.10.5. protecting reading habits..
 - (Imagine using your MicroSoftCashCard for library checkouts...)
- 6.10.6. Downsides
 - loss of trust
 - markets in unsavory things
 - espionage
 - + expect to see new kinds of con jobs
 - confidence games
 - "Make Digital Money Fast"
- 6.10.7. Encryption of Video Signals and Encryption to Control Piracy
 - this is of course a whole technology and industry
 - Videocypher II has been cracked by many video hackers
 - a whole cottage industry in cracking such cyphers
 - note that outlawing encryption would open up many industries to destruction by piracy, which is yet another reason a wholesale ban on encryption is doomed to failure

7. PGP -- Pretty Good Privacy

7.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

7.2. SUMMARY: PGP -- Pretty Good Privacy

7.2.1. Main Points

- PGP is the most important crypto tool there is, having single-handedly spread public key methods around the world
- many other tools are being built on top of it

7.2.2. Connections to Other Sections

- ironically, almost no understanding of how PGP works in detail is needed; there are plenty of experts who specialize in that

7.2.3. Where to Find Additional Information

- newsgroups carry up to date comments; just read them for a few weeks and many things will float by
- various FAQs on PGP

+ even an entire book, by Simpson Garfinkel:

- PGP: Pretty Good Privacy
by Simson Garfinkel
1st Edition November 1994 (est.)
250 pages (est), ISBN: 1-56592-098-8, \$17.95 (est)

7.2.4. Miscellaneous Comments

- a vast number of ftp sites, URLs, etc., and these change
- this document can't possibly stay current on these--see the pointers in the newsgroups for the most current sites

7.3. Introduction

7.3.1. Why does PGP rate its own section?

- Like Clipper, PGP is too big a set of issues not to have its own section

7.3.2. "What's the fascination in Cypherpunks with PGP?"

- Ironically, our first meeting, in September 1992, coincided within a few days of the release of PGP 2.0. Arthur Abraham provided diskettes of 2.0, complete with laser-printed labels. Version 2.0 was the first truly useful version of PGP (so I hear....I never tried Version 1.0, which had limited distribution). So PGP and Cypherpunks shared a history--and Phil Zimmermann has been to some physical meetings.
- A practical, usable, understandable tool. Fairly easy to use. In contrast, many other developments are more abstract and do not lend themselves to use by hobbyists and amateurs. This alone ensures PGP an honored place (and might be an object lesson for developers of other tools).

7.3.3. The points here focus on PGP, but may apply as well to similar crypto programs, such as commercial RSA packages (integrated into mailers, commercial programs, etc.).

7.4. What is PGP?

7.4.1. "What is PGP?"

7.4.2. "Why was PGP developed?"

7.4.3. Who developed PGP?

7.5. Importance of PGP

7.5.1. PGP 2.0 arrived at an important time

- in September 1992, the very same week the Cypherpunks had their first meeting, in Oakland, CA. (Arthur Abraham printed up professional-looking diskette labels for the PGP 2.0 diskettes distributed. A general feeling that we were

forming at the "right time.")

- just 6 months before the Clipper announcement caused a firestorm of interest in public key cryptography

7.5.2. PGP has been the catalyst for major shifts in opinion

- has educated tens of thousands of users in the nature of strong crypto
- has led to other tools, including encrypted remailers, experiments in digital money, etc.

7.5.3. "If this stuff is so important, how come not everyone is digitally signing their messages?"

- (Me, for example. I never sign my messages, and this FAQ is not signed. Maybe I will, later.)
- convenience, ease of use, "all crypto is economics"
- insecurity of host Unix machines (illusory)
- better integration with mailers needed

7.5.4. Ripem appears to be dead; traffic in alt.security.ripen is almost zero. PGP has obviously won the hearts and minds of the user community; and now that it's "legal"...

7.6. PGP Versions

7.6.1. PGP Versions and Implementations

- 2.6ui is the version compatible with 2.3
- + What is the difference between versions 2.6 and 2.6ui?
 - "PGP 2.6 is distributed from MIT and is legally available to US and Canadian residents. It uses the RSAREF library. It has code that will prevent interoperation with earlier versions of PGP.

"PGP 2.6ui is a modified version of PGP 2.3a which functions almost identically to MIT PGP 2.6, without the "cripple code" of MIT PGP 2.6. It is legally available outside the US and Canada only." [Rat <ratinox@ccs.neu.edu>, alt.security.pgp, 1994-07-03]

+ DOS

- Versions

+ Pretty Good Shell

- "When your Microsoft Mail supports an external Editor, you might want to try PGS (Pretty Good Shell), available as PGS099B.ZIP at several ftp sites. It enables you to run PGP from a shell, with a easy way to edit/encrypt files." [HHM LIMPENS, 1994-07-01]

- Windows

+ Sun

- "I guess that you should be able to use PGPsendmail, available at ftp.atnf.csiro.au:/pub/people/rgooch' [eric@terra.hacktic.nl (Eric Veldhuyzen), PGP support for Sun's Mailtool?, alt.security.pgp, 1994-06-29]

+ Mark Grant <mark@unicorn.com> has been working on a tool to replace Sun's mailtool. "Privtool ("Privacy Tool") is intended to be a PGP-aware replacement for the standard Sun Workstation mailtool program, with a similar user interface and automagick support for PGP-signing and PGP-encryption." [MG, 1994-07-03]

- "At the moment, the Beta release is available from ftp.c2.org in /pub/privtool as privtool-0.80.tar.Z, and I've attached the README.1ST file so that you can check out the features and bugs before you download it. Currently the program requires the Xview toolkit to

build, and has only been compiled on SunOS 4.1 and Solaris 2.1."

+ MacPGP

- 2.6ui: reports of problems, bombs (remove Preferences set by previous versions from System folder)
- "MacPGP 2.6ui is fully compatible with MIT's MacPGP 2.6, but offers several advantages, a chief one being that MacPGP 2.6ui is controllable via AppleScript. This is a very powerful feature, and pre-written AppleScripts are already available. A set of AppleScripts called the Interim Macintosh PGP Interface (IMPI) support encryption, decryption, and signing of files via drag-n-drop, finder selection, the clipboard, all accessible from a system-wide menu. Eudora AppleScripts also exist to interface MacPGP with the mail program Eudora.

"MacPGP 2.6ui v1.2 is available via anonymous ftp from:

FTP SITE	DIRECTORY
CONTENTS	
-----	-----

ftp.darmstadt.gmd.de	pub/crypto/macintosh/MacPGP
MacPGP 2.6ui, source	

AppleScripts for 2.6ui are available for U.S. and Canadian citizens ONLY via anonymous ftp from:

FTP SITE	DIRECTORY
CONTENTS	
-----	-----

ftp.csn.net	mpj
IMPI & Eudora scripts	

MacPGP 2.6ui, source
[phinely@uhunix.uhcc.Hawaii.Edu (Peter Hinely),
alt.security.pgp, 1994-06-28]

- Amiga

+ VMS

- 2.6ui is said to compile and run under VMS.

+ German version

- MaaPGP0,1T1,1
- dtp8//dtp,dapmqtadt,gmd,de/ilaomilg/MaaP
- Ahpiqtoph_Pagalies@hh2.maus.
- (source: andreas.elbert@gmd.de (A.Elbert). by way of qwerty@netcom.com (==Xenon==), 3-31-94

7.6.2. What versions of PGP exist?

- PGP 2.7 is ViaCrypt's commercial version of PGP 2.6

7.6.3. PGP 2.6 issues

- There has been much confusion, in the press and in discussion groups, about the issues surrounding 2.5, 2.6, 2.6ui, and various versions of these. Motivations, conspiracies, etc., have all been discussed. I'm not involved as others on our list are, so I'm often confused

too.

- + Here are some comments by Phil Zimmermann, in response to a misleading press report:
 - "PGP 2.6 will always be able to read messages, signatures, and keys from olderversions, even after September 1st. The older versions will not be able to read messages, signatures and keys produced by PGP 2.6 after September 1st. This is an entirely different situation. There is every reason for people to switch to PGP 2.6, because it will be able to handle both data formats, while the older versions will not. Until September, the new PGP will continue to produce the old format that can be read by older versions, but will start producing the new format after that date. This delay allows time for everyone to obtain the new version of PGP, so that they will not be affected by the change. Key servers will still be able to carry the keys made in the old format, because PGP 2.6 will still read them with no problems." [Phil Zimmermann, 1994-07-07, also posted to Usenet groups] [all dates here refer to 1994]
 - "I developed PGP 2.6 to be released by MIT, and I think this new arrangement is a breakthrough in the legal status of PGP, of benefit to all PGP users. I urge all PGP users to switch to PGP 2.6, and abandon earlier versions. The widespread replacement of the old versions with this new version of PGP fits in with future plans for the creation of a PGP standard." [Phil Zimmermann, 1994-07-07, also posted to Usenet groups]

7.6.4. PGP version 2.6.1

- "MIT will be releasing Pretty Good Privacy (PGP) version 2.6.1 real soon now. By tomorrow, I think. The MSDOS release filename will be pgp261.zip, and the source code will be in pgp261s.zip. The MIT FTP site is net-dist@mit.edu, in the pub/PGP directory." [corrected by Derek Atkins to be: net-dist.mit.edu, not net-dist@mit.edu.]

"This new version has a lot of bug fixes over version 2.6. I hope this is the final release of this family of PGP source code. We've been working on an entirely new version of PGP, rewritten from scratch, which is much cleaner and faster, and better suited for the future enhancements we have planned. All PGP development efforts will be redirected toward this new code base, after this 2.6.1 release." [Phil Zimmermann, Cypherpunks list, 1994-09-02]

7.7. Where to Get PGP?

7.7.1. "Where can I get PGP on CompuServe?"

- Note: I can't keep track of the major ftp sites for the various crypto packages, let alone info on services like this. But, here it is;
- "Current as of 5-Jul-1994:"
 - GO EURFORUM / Utilities PGP26UI.ZIP PGP 2.6ui

GO PWOFORUM / New uploads PGP26.ZIP PGP 2.6
PWOFORUM also has the source code and documentation, plus a number of shell utilities for PGP. Version 2.3a is also still around." [cannon@panix.com, Kevin Martin, PGP on Compuserve??, alt.security.pgp, 1994-07-08]

7.7.2. Off line PGP

- + ftp.informatik.uni-hamburg.de:/pub/virus/crypt/pgp/tools/pgp-elm.zip
- another place: Crosspoint: ftp.uni-kl.de:/pub3/pc/dos/terminal/xpoint XP302*.EXE
- + "I highly recommend Offline AutoPGP v2.10. It works seamlessly with virtually any offline mail reader that supports .QWK packets. Shareware registration is \$10.00 US. The author is Staale Schumacher, a student at the University of Oslo, is reachable at staale@ifi.uio.no . The program should be pretty widely available on US bbs's by now. I use the program constantly for bbs mail. It's really quite a slick piece of work. If you have any trouble finding it, drop me a note."
[bhowatt@eis.calstate.edu Brent H. Howatt, PGP in an offline reader?, alt.security.pgp, 1994-07-05]
- oak.oakland.edu in /pub/msdos/offline, version 2.11
- ftp.informatik.uni-hamburg.de:/pub/virus/crypt/pgp/tools/apgp211.zip

7.7.3. "Should I worry about obtaining and compiling the PGP sources?"

- Well, unless you're an expert on the internals of PGP, why bother? And a subtle bug in the random number generator eluded even Colin Plumb for a while.
- The value of the source being available is that others can, if they wish, make the confirmation that the executable correspond to the source. That this can be done is enough for me. (Strategy: Hold on to the code for a while, wait for reports of flaws or holes, then use with confidence.)
- Signatures can be checked. Maybe timestamped versions, someday.
- Frankly, the odds are much higher that one's messages or pseudonymous identity will be exposed in others ways than that PGP has been compromised. Slip-ups in sending messages sometimes reveal identities, as do inadvertent comments and stylistic cues.

7.8. How to Use PGP

7.8.1. How does PGP work?

7.8.2. "How should I store the secret part of my key? Can I memorize it?"

- Modern ciphers use keys that are far beyond memorization (or even typing in!). The key is usually stored on one's home machine, or a machine that is reasonably secure, or on diskette. The passphrase should always be memorized or written down (ugh) in one's wallet or other such place. Secure "dongles" worn around the neck, or a ring or watch, may eventually be used. Smartcards and PDAs are a more likely intermediate solution (many PCs now have PCMCIA card slots).

7.8.3. "How do I sign messages?"

- cf. the PGP docs

+ however, this has come up on the List, and:

-
- + pgp -sta +clearsig=on message.txt
-
- That's from pgpdoc2.txt. Hope it helps. You might wish to set up your mail
- user agent to invoke this command upon exiting your default message editor,
- with "message.txt" set to whatever your editor calls the temporary message
- file. <Russell Whitaker, whitaker@sgi.com, 4-15-94, Cypherpunks>

7.8.4. Why isn't PGP easier to use?

- Compared to other possible crypto applications (like digital money or voting systems), it is actually very easy to use
- semantic gap...learning

7.8.5. How should I learn PGP?

7.8.6. "What's the status of PGP integration with other programs?"

+ Editors

+ emacs

- + emacs supports pgp, probably in various flavors (I've seen several reports of different packages)..the built-in language certainly helps
- Rick Busdiecker <rfb@lehman.com> has an emacs front end to PGP available
- Jin S. Choi <jsc@monolith.MIT.EDU> once described a package he wrote in elisp which supported GNU emacs: "mailcrypt"
- there are probably many more

+ Mailers

- That is, are there any mailers that have a good link to PGP? Hooks into existing mailers are needed

+ emacs

- + emacs supports pgp, probably in various flavors (I've seen several reports of different packages)..the built-in language certainly helps
- Rick Busdiecker <rfb@lehman.com> has an emacs front end to PGP available
- Jin S. Choi <jsc@monolith.MIT.EDU> once described a package he wrote in elisp which supported GNU emacs: "mailcrypt"
- there are probably many more

- elm

- Eudora

+ PGP sendmail, etc.

- "Get the PGPsendmail Suite, announced here a few days ago. It's available for anonymous ftp from:
ftp.atnf.csiro.au: pub/people/rgooch (Australia)
ftp.dhp.com: pub/crypto/pgp/PGPsendmail(U.S.A.)
ftp.ox.ac.uk: src/security (U.K.)... It works by wrapping around the regular sendmail programme, so you get automatic encryption for all mailers, not just Rmail. " [Richard Gooch, alt.security.pgp, 1994-07-10]

+ MIME

- MIME and PGP <Derek Atkins, 4-6-94>
- [the following material taken from an announcement

forwarded to the Cypherpunks list by
remijn@athena.research.ptt.nl, 1994-07-05]

- "MIME [RFC-1341, RFC-1521] defines a format and general framework for the representation of a wide variety of data types in Internet mail. This document defines one particular type of MIME data, the application/pgp type, for "pretty good" privacy, authentication, and encryption in Internet mail. The application/pgp MIME type is intended to facilitate the wider interoperability of private mail across a wide variety of hardware and software platforms.

+ Newsreaders

- useful for automatic signing/verification, and e-mail from within newsreader
- yarn
- tin
- The "yarn" newsreader reportedly has PGP built in.

7.8.7. "How often should I change my key or keys?"

- Hal Finney points out that many people seem to think PGP keys are quasi-permanent. In fact, never changing one's key is an invitation to disaster, as keys may be compromised in various ways (keystroke capture programs, diskettes left lying around, even rf monitoring) and may conceivably be cracked.
- "
- + "What is a good interval for key changes? I would suggest every year or so
- makes sense, especially if infrastructure can be developed to make it easier
- to propagate key changes. Keys should be overlapped in time, so that you make
- a new key and start using it, while continuing to support the old key for a
- time. <Hal Finney, hfinney@shell.portal.com, 4-15-94, cypherpunks>
- Hal also recommends that remailer sites change their keys even more frequently, perhaps monthly.

7.9. Keys, Key Signings, and Key Servers

7.9.1. Web of trust vs. hierarchical key management

- A key innovation of Phil Zimmermann was the use of a "web of trust" model for distributed trust in keys.
- locality, users bear costs
- by contrast, government estimates \$1-2 B a year to run key certification agencies for a large fraction of the population
- "PGP is about choice and constructing a web of trust that suits your needs. PGP supports a completely decentralized, personalized web of trust and also the most highly structured bureaucratic centralized scheme you could imagine. One problem with relying solely on a personalized web of trust is that it limits your universe of correspondents. We can't expect Phil Zimmermann and a few well-known others to sign everyone's key, and I would not want to limit my private correspondence to just those people I know and trust plus those people whose keys have been signed by someone I know and trust." [William

Stallings, SLED key verification, alt.security.pgp, 1994-09-01]

7.9.2. Practical approaches to signing the keys of others

- + sign keys of folks you know and wish to communicate with
 - face-to-face encounters ("Here is my key.")
- + trust--to varying extents--the keys signed by others you know
 - web-of-trust
- trust--to a lesser extent--the keys of people in key registries

7.9.3. Key Servers

- + There are several major sites which appear to be stable
 - + MIT PGP Public Key Server
 - via www.eff.org
 - + Vesselin Bontchev at University of Hamburg operates a very stable one:
 - Ftp: [ftp.informatik.uni-hamburg.de](ftp://ftp.informatik.uni-hamburg.de)
 - IP: 134.100.4.42
 - Dir: /pub/virus/encrypt/pgp/
 - File: pubkring.pgp
 - E-Mail: pgp-public-keys@fbihh.informatik.uni-hamburg.de
 - pgpkeys.io.com
- + <http://martigny.ai.mit.edu/~bal/pks-commands.html>
- This is a PGP keyserver in Zurich. <Russell Whitaker, 7 April 1994>

-

7.9.4. Use of PGP key fingerprints

- "One of the better uses for key fingerprints is for inclusion in signature files and other places that a key itself is too bulky. By widespread dissemination of the fingerprint, the chances of a bogus key being undetected are decreased, since there are more channels for the fingerprint to get to recipients, and more channels for the owner of a key to see any bogus fingerprints out on the net. [Bill Stewart, 1994-08-31]

7.9.5. "How should address changes be handled? Do old keys have to be revoked?"

- Future versions of PGP may handle better
- One way is to issue "User-id revocation certificates are a *good* idea and the PGP key format allows for them - maybe one day PGP will do something about it." [Paul Allen, alt.security.pgp, 1994-07-01]
- Persistent e-mail addresses is one approach. Some people are using organization like the ACM to provide this (e.g., Phil Zimmermann is prz@acm.org). Others are using remapping services. For example, "I signed up with the SLED (Stable Large E-mail Database), which is a cross-referencing database for linking old, obsolete E-mail addresses with current ones over the course of time.... Anyone using this key will always be able to find me on the SLED by conducting a search with "blbrooks..." as the keyword. Thus my key and associated sigs always remain good.... If you are interested in the SLED, its address is sled@drebes.com." [Robert Brooks, alt.security.pgp, 1994-07-01]

7.9.6. "How can I ensure that my keys have not been tampered with?"

- + Keep your private key secure

- + if on an unsecured machine, take steps to protect it
 - offline storage (Perry Metzger loads his key(s) every morning, and removes it when he leaves the machine)
- + memorize your PGP passphrase and don't write it down, at least not anywhere near where the private key is available
 - sealed envelopes with a lawyer, safe deposit boxes, etc., are possibilities
 - given the near-impossibility of recovering one's files if the passphrase is lost permanently, I recommend storing it someplace, despite the slight loss in security (this is a topic of debate...I personally feel a lot more comfortable knowing my memory is backed up somewhere)
- Colin Plumb has noted that if someone has access to your personal keyring, they also probably have access to your PGP program and could make modifications to it **directly**.
- Derek Atkins answered a similar question on sci.crypt:

"Sure. You can use PGP to verify your keyring, and using the web-of-trust, you can then have it verify your signatures all the keys that you signed, and recurse through your circle-of-friends. To verify that your own key was not munged, you can sign something with your secret key and then try to verify it. This will ensure that your public key wasn't munged." [Derek Atkins, sci.crypt, 1994-07-06]
- 7.9.7. "Why are key revocations needed?"
 - Key revocation is the "ebb-of-trust"
 - "There are a number of real reasons. Maybe you got coerced into signing the key, or you think that maybe the key was signed incorrectly, or maybe that person no longer uses that email address, because they lost the account, or that maybe you don't believe that the binding of key to userID is valid for any number of reasons." [Derek Atkins, 4-28-94]
- 7.9.8. "Is-a-person" registries
 - + There have been proposals that governments could and should create registries of "legal persons." This is known in the crypto community as "is-a-person" credentialling, and various papers (notably Fiat-Shamir) have dealt with issues
 - of spoofing by malicious governments
 - of the dangers of person-tracking
 - + We need to be very careful here!
 - this could limit the spread of 'ad hoc crypto' (by which I mean the use of locally-generated keys for reasons other than personal use...digital cash, pseudonyms etc.)
 - any system which "issues" permission slips to allow keys to be generated is dangerous!
 - + Could be an area that governments want to get into.
 - a la Fiat-Shamir "passport" issues (Murdoch, Libyan example)
 - I favor free markets--no limitations on which registries I can use
- 7.9.9. Keyservers (this list is constantly changing, but most share keys, so all one needs is one). Send "help" message. For current information, follow alt.security.pgp.
 - about 6000 keys on the main keyservers, as of 1994-08.

- pgp-public-keys@martigny.ai.mit.edu
- pgp-public-keys@dsi.unimi.it
- pgp-public-keys@kub.nl
- pgp-public-keys@sw.oz.au
- pgp-public-keys@kiaae.su
- pgp-public-keys@fbihh.informatick.uni-hamburg.de
- and wasabi.io.com offers public keys by finger (I couldn't get it to work)

7.9.10. "What are key fingerprints and why are they used?"

- "Distributing the key fingerprint allows J. Random Human to correlate a key supplied via one method with that supplied via another. For example, now that I have the fingerprint for the Betsi key, I can verify whether any other alleged Betsi key I see is real or not.....It's a lot easier to read off & cross-check 32-character fingerprints than the entire key block, especially as signatures are added and the key block grows in size." [Paul Robichaux, 1994-08-29]

7.9.11. Betsi

- Bellcore
- key signing

7.9.12. on attacks on key servers...

- + flooding attacks on the key servers have started; this may be an attempt to have the key servers shut down by using obscene, racist, sexist phrases as key names (Cypherpunks would not support shutting down a site for something so trivial as abusive, offensive language, but many others would.)
- "It appears that some childish jerk has had a great time generating bogus PGP keys and uploading them to the public key servers. Here are some of the keys I found on a keyserver:...[keys elided]..." [staalesc@ifi.uio.no, alt.security.pgp, 1994-09-05]

7.10. PGP Front Ends, Shells, and Tools

7.10.1. Many can be found at this ftp site:

- + ftp.informatik.uni-hamburg.de:/pub/virus/crypt/pgp/shells/
- for various shells and front-ends for PGP

7.10.2. William Stallings had this to say in a Usenet post:

- "PGPShell: runs directly on the DOS version, doesn't need Windows. Nice, simple interface. freeware

"PGP Winfront: freeware windows front end. Uses a "control panel" style, with many options displayed in a compact fashion.

"WinPGP: shareware (\$45). Uses a drop-down menu style, common to many Windows applications." [William Stallings, Looking for PGP front end, alt.security, 1994-08-31]

7.10.3. Rick Busdiecker <rfb@lehman.com> has an emacs front end to PGP available

7.10.4. Pr0duct Cypher's tools:

- + ftp.informatik.uni-hamburg.de:/pub/virus/crypt/pgp/tools/PGPTools.tar.gz
- Pr0duct Cypher's tools, and other tools in general

7.11. Other Crypto Programs And Tools

7.11.1. Other Ciphers and Tools

- RIPEM
 - PEM
 - MD5
 - + SFS (Secure FileSystem) 1.0
 - "SFS (Secure FileSystem) is a set of programs which create and manage a number of encrypted disk volumes, and runs under both DOS and Windows. Each volume appears as a normal DOS drive, but all data stored on it is encrypted at the individual-sector level....SFS 1.1 is a maintenance release which fixes a few minor problems in 1.0, and adds a number of features suggested by users. More details on changes are given in in the README file." [Peter Gutmann, sci.crypt, 1994-08-25]
 - not the same thing as CFS!
 - 512-bit key using a MDC/SHS hash. (Fast)
 - only works on a386 or better (says V. Bontchev)
 - source code not available?
 - implemented as a device driver (rather than a TSR, like SecureDrive)
 - "is vulnerable to a special form of attack, which was mentioned once here in sci.crypt and is described in details in the SFS documentation. Take a look at the section "Encryption Considerations"." [Vesselin Bontchev, sci.crypt, 1994-07-01]
 - Comparing SFS to SecureDrive: "Both packages are approximately equal in terms of user interface, but SFS seems to be quite a bit faster. And comments from various people (previous message thread) seems to indicate that it is more "secure" as well." [Bill Couture <coutu001@gold.tc.umn.edu> , sci.crypt, 1994-0703]
 - + SecureDrive
 - encrypts a disk (always be very careful!)
 - SecureDrive 1.3D, 128-bit IDEA cypher is based on an MD5 hash of the passphrase
 - implemented as a TSR (rather than a device driver, like CFS)
 - source code available
 - + Some problems reported (your mileage may vary)
 - "I have been having quite a bit of difficulty with my encrypted drive mangling files. After getting secure drive 1.3d installed on my hard drive, I find that various files are being corrupted and many times after accessing the drive a bunch of crosslinked files are present." [Vaccinia@uncvxl.oit.unc.edu, 1994-07-01]
 - Others report being happy with, under both DOS and Windows
 - no OS/2 or Mac versions reported; some say an OS/2 device driver will have to be used (such as Stacker for OS/2 uses)
 - + SecureDevice
 - "If you can't find it elsewhere, I have it at ftp://ftp.ee.und.ac.za/pub/crypto/secdev13.arj, but that's at the end of a saturated 64kbps link." [Alan Barrett, 1994-07-01]
- 7.11.2. MDC and SHS (same as SHA?)
- "The MDC cyphers are believed to be as strong as it is difficult to invert the cryptographic hash function they

are using. SHS was designed by the NSA and is believed to be secure. There might be other ways to attack the MDC cyphers, but nobody who is allowed to speak knows such methods." [Vesselin Bontchev, sci.crypt, 1994-07-01]

- + Secure Hash Standard's algorithm is public, and hence can be analyzed and tested for weaknesses (in strong contrast with Skipjack).
 - may replace MD5 in future versions of PGP (a rumor)
- Speed of MDC: "It's a speed tradeoff. MDC is a few times faster than IDEA, so SFS is a few times faster than SecureDrive. But MDC is less proven." [Colin Plumb, sci.crypt, 1994-07-04]
- + Rumors of problems with SHA
 - "The other big news is a security problem with the Secure Hash Algorithm (SHA), discussed in the Apr 94 DDJ. The cryptographers at NSA have found a problem with the algorithm. They won't tell anyone what it is, or even how serious it is, but they promise a fix soon. Everyone is waiting with baited breath." [Bruce Schneier, reprot on Eurocrypt '94, 1994-07-01]

7.11.3. Stego programs

- + DOS
 - S-Tools (or Stools?). DOS? Encrypts in .gif and .wav (SoundBlaster format) files. Can set to not indicate encrypted files are inside.
- Windows
- + Macintosh
 - Stego
 - + sound programs
 - marielsn@Hawaii.Edu (Nathan Mariels) has written a program which "takes a file and encrypts it with IDEA using a MD5 hash of the password typed in by the user. It then stores the file in the lowest bit (or bits, user selectable) of a sound file."

7.11.4. "What about "Pretty Good Voice Privacy" or "Voice PGP" and Other Speech Programs?"

- + Several groups, including one led by Phil Zimmermann, are said to be working on something like this. Most are using commercially- and widely-available sound input boards, a la "SoundBlaster" boards.
 - proprietary hardware or DSPs is often a lose, as people won't be able to easily acquire the hardware; a software-only solution (possibly relying on built-in hardware, or readily-available add-in boards, like SoundBlasters) is preferable.
- + Many important reasons to do such a project:
 - proliferate more crypto tools and systems
 - get it out ahead of "Digital Telephony II" and Clipper-type systems; make the tools so ubiquitous that outlawing them is too difficult
 - people understand voice communications in a more natural way than e-,mail, so people who don't use PGP may nevertheless use a voice encryption system
- + Eric Blossom has his own effort, and has demonstrated hardware at Cypherpunks meetings:
 - "At this moment our primary efforts are on developing a family of extensible protocols for both encryption and

voice across point to point links. We intend to use existing standards where ever possible.

"We are currently planning on building on top of the RFCs for PPP (see RFCs 1549, 1548, and 1334). The basic idea is to add a new Link Control Protocol (or possibly a Network Control Protocol) that will negotiate base and modulus and perform DH key exchange. Some forms of Authentication are already supported by RFCs. We're looking at others." [Eric Blossom, 1994-04-14]

- + Building on top of multimedia capabilities of Macintoshes and Windows may be an easier approach
 - nearly all Macs and Windows machines will be multimedia/audiovisual-capable soon
 - "I realize that it is quite possible to design a secure phone with a Vocoder, a modem and some cpu power to do the encryption, but I think that an easier solution may be on the horizon.I believe that Microsoft and many others are exploring hooking phones to PCs so people can do things like ship pictures of their weekend fun to friends. When PC's can easily access phone communications, then developing encrypted conversations should be as easy as programming for Windows :-)." [Peter Wayner, 1993--07-08]

7.11.5. Random Number Generators

- A huge area...
- + Chaotic systems, pendula
 - may be unexpected periodicities (phase space maps show basins of attraction, even though behavior is seemingly random)

7.11.6. "What's the situation on the dispute between NIST and RSADSI over the DSS?"

- NIST claims it doesn't infringe patents
- RSADSI bought the Schnorr patent and claims DSS infringes it
- NIST makes no guarantees, nor does it indemnify users [Reginald Braithwaite-Lee, talk.politics.crypto, 1994-07-04]

7.11.7. "Are there any programs like telnet or "talk" that use pgp?"

- "Don't know about Telnet, but I'd like to see "talk" secured like that... It exists. (PGP-ized ytalk, that is.) Have a look at ftp.informatik.uni-hamburg.de:/pub/virus/crypto/pgp/tools/pgptalk.2.0.tar.gz" [Vesselin Bontchev, alt.security.pgp, 1994-07-4]

7.11.8. Digital Timestamping

- + There are two flavors:
 - toy or play versions
 - real or comercial version(s)
- + For a play version, send a message to "timestamp@lorax.mv.com" and it will be timestamped and returned. Clearly this is not proof of much, has not been tested in court, and relies solely on the reputation of the timestamper. (A fatal flaw: is trivial to reset system clocks on computes and thereby alter dates.)
- "hearsay" equivalent: time stamps by servers that are **not** using the "widely witnessed event" approach of

Haber and Stornetta

- The version of Haber and Stornetta is of course much more impressive, as it relies on something more powerful than mere trust that they have set the system clocks on their computers correctly!

7.12. Legal Issues with PGP

7.12.1. "What is RSA Data Security Inc.'s position on PGP?"

- I. They were strongly opposed to early versions
- II. objections
 - infringes on PKP patents (claimed infringements, not tested in court, though)
 - breaks the tight control previously seen
 - brings unwanted attention to public key approaches (I think PGP also helped RSA and RSADSI)
 - bad blood between Zimmermann and Bidzos
- III. objections
 - infringes on PKP patents (claimed infringements, not tested in court, though)
 - breaks the tight control previously seen
 - brings unwanted attention to public key approaches (I think PGP also helped RSA and RSADSI)
 - bad blood between Zimmermann and Bidzos
- IV. Talk of lawsuits, actions, etc.
- V. The 2.6 MIT accomodation may have lessened the tension; purely speculative

7.12.2. "Is PGP legal or illegal"?

7.12.3. "Is there still a conflict between RSADSI and PRZ?"

- Apparently not. The MIT 2.6 negotiations seem to have buried all such rancor. At least officially. I hear there's still animosity, but it's no longer at the surface. (And RSADSI is now facing lawsuits and patent suits.)

7.13. Problems with PGP, Flaws, Etc.

7.13.1. Speculations on possible attacks on PGP

- + There are periodically reports of problems, most just rumors. These are swatted-down by more knowledgeable people, for the most part. True flaws may exist, of course, as in any piece of software.
- Colin Plumb acknowledged a flaw in the random number generation process in PGP 2.6, to be fixed in later versions.
- + spreading fear, uncertainty and doubt
 - rumors about security of PGP versions
 - selective prosecution of PGP users
 - death threats (a la against Bidzos)
- sowing confusion in the user community
- fragmenting it (perhaps via multiple, noninteroperable versions...such as we're beginning to see now?)

7.13.2. What does the NSA know about flaws in PGP?

- They're not saying. Ironically, this violates the part of their charter that deals with making commercial security stronger. Now that PGP is kosher, they should help to make it stronger, and certainly should not keep mum about weaknesses they know about. But for them to help strengthen PGP is not really too likely.

7.13.3. The PGP timebomb

- (As I've said elsewhere, it all gets very confusing. Many versions, many sites, many viewpoints, many tools, many shells, many other things. Fortunately, most of it is flotsam.)
 - I take no point of view--for various reasons--on avoiding the "timebomb" by using 2.6ui. Here's someone else's comment: "I would like to take this time to encourage you to upgrade to 2.6ui which will overcome mit's timebomb and not exclude PGP 2.3a from decrypting messages.....DON'T USE MIT's 2.6, use PGP 2.6ui available from soda.berkeley.edu : /pub/cypherpunks/pgp" [Matrix at Cypherpunks, BLACK THURSAY!, alt.security.pgp, 1994-09-01]
 - + can also be defeated with the "legal kludge":
 - ftp.informatik.uni-hamburg.de :
 - /pub/virus/crypt/pgp/legal_kludge.txt
- 7.13.4. Spoofing
- "Suitable timing constraints, and in particular real-time constraints, can be used to hinder, and perhaps defeat, spoofing attacks. But with a store-and-forward e-mail system (such as PGP is designed to work with) these constraints cannot, in general, be set." [Ken Pizzini , sci.crypt, 1994-07-05]
- 7.13.5. "How do we know that PGP doesn't have a back door or some other major flaw? After all, not all of us are programmers or cryptologists."
- Yes, but many of us are. Many folks have analyzed the source code in PGP, have compiled the code themselves (a fairly common way to get the executable), and have examined the random number generators, the selection of primes, and all of the other math.
 - + It would take only a single sharp-eyed person to blow the whistle on a conspiracy to insert flaws or backdoors. This has not been done. (Though Colin Plumb acknowledged a slight weakness in the RNG of 2.6...being fixed.)
 - "While having source code available doesn't guarantee that the program is secure, it helps a lot. Even though many users are not programmers or cryptographers, others are, and many of these will examine the code carefully and publicly yell about weaknesses that they notice or think they notice. For example, apparently there was a big discussion here about the xorbytes() bug in PGP 2.6. Contrast this with a commercial program, where such a bug might go undetected for years." [Paul Rubin, alt.security.pgp, 1994-09-06]
- 7.13.6. "Can I run PGP on a machine I don't control, e.g., the campus computer system?"
- Sure, but the sysops and others may then have access to your key and passphrase. Only machines the user directly controls, and that are adequately firewalled from other machines, offer reasonable amounts of security. Arguing about whether 1024-bit keylengths are "enough" is rather moot if the PGP program is being run on a corporate computer, or a university network. The illusion of security may be present, but no real security. Too many people are kidding themselves that their messages are secure. That their electronic identities cannot be spoofed.
 - I'm not interested in the various elm and emacs PGP

packages (several such shells and wrappers exist). Any sysop can not only obtain your secret key, stored on his system, but he can also capture your passphrase as you feed it to the PGP program (assuming you do...many people automate this part as well). Since this sysop or one of his cronies can then compromise your mail, sign messages and contracts as "you," I consider this totally unacceptable. Others apparently don't.

- What can be done? Many of us only run PGP on home machines, or on machines we directly control. Some folks who use PGP on such machines at least take steps to better secure things....Perry Metzger, for example, once described the multi-stage process he went through each day to reload his key material in a way he felt was quasi-safe.
- Until the "Internet-in-a-box" or TIA-type products are more widespread, many people will be connecting home or office machines to other systems they don't control. (To put this in sharper focus: do you want your electronic money being run out of an account that your sysop and his friends can monitor? Not hardly. "Electronic purses," which may be smart cards, Newton-like PDAs, or dongle-like rings or pendants, are clearly needed. Another entire discussion.)

7.14. The Future of PGP

7.14.1. "Does PGP help or hurt public key methods in general and RSA Data Security Inc. in particular?"

- The outcome is not final, but on balance I think the position of RSADSI is helped by the publicity PGP has generated. Users of PGP will "graduate" to fully-licensed versions, in many cases. Corporations will then use RSADSI's products.
- + Interestingly, PGP could do the "radical" things that RSADSI was not prepared to do. (Uses familiar to Cypherpunks.)
 - bypassing export restrictions is an example of this
 - incorporation into experimental digital cash systems
- Parasitism often increases the rate of evolution. Certainly PGP has helped to light a fire under RSADSI.

7.14.2. Stealth PGP

- Xenon, Nik, S-Tools,

7.14.3. "Should we work on a more advanced version, a *Really Good Privacy*?"

- easier said than done...strong committment of time
- not clear what is needed...

7.14.4. "Can changes and improvements be made to PGP?"

- I consider it one of the supreme ironies of our age that Phil Zimmermann has denounced Tom Rollins for making various changes to a version of PGP he makes available.

+ Issues:

- Phil's reputation, and that of PGP
- intellectual property
- GNU Public license
- the mere name of PGP
- Consider that RSA said much the same thing, that PGP would degrade the reputation of public key (esp. as Phil was an "amateur," the same exact phrasing PRZ uses to criticize Tom Rollins!)

- I'm not taking a stand here....I don't know the details.
Just some irony.

7.15. Loose Ends

7.15.1. Security measures on login, passwords, etc.

- Avoid entering passwords over the Net (such as in rlogins or telnets). If someone or some agent asks for your password, be paranoid.
- Can use encrypted telnet, or something like Kerberos, to avoid sending passwords in the clear between machines. Lots of approaches, almost none of them commonly used (at least I never see them).

8. Anonymity, Digital Mixes, and Remailers

8.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

8.2. SUMMARY: Anonymity, Digital Mixes, and Remailers

8.2.1. Main Points

- Remailers are essential for anonymous and pseudonymous systems, because they defeat traffic analysis
- Cypherpunks remailers have been one of the major successes, appearing at about the time of the Kleinpaste/Julf remailer(s), but now expanding to many sites
- To see a list of sites: finger remailer-list@kiwi.cs.berkeley.edu
(or <http://www.cs.berkeley.edu/~raph/remailer-list.html>)
- Anonymity in general is a core idea

8.2.2. Connections to Other Sections

- Remailers make the other technologies possible

8.2.3. Where to Find Additional Information

- Very little has been written (formally, in books and journals) about remailers
- David Chaum's papers are a start

8.2.4. Miscellaneous Comments

- This remains one of the most jumbled and confusing sections, in my opinion. It needs a lot more reworking and reorganizing.
- + Partly this is because of several factors
 - a huge number of people have worked on remailers, contributing ideas, problems, code, and whatnot
 - there are many versions, many sites, and the sites change from day to day
 - lots of ideas for new features
 - in a state of flux
- This is an area where actual experimentation with remailers is both very easy and very instructive...the "theory" of remailers is straightforward (compared to, say, digital cash) and the learning experience is better than theory anyway.
- There are a truly vast number of features, ideas, proposals, discussion points, and other such stuff. No FAQ

could begin to cover the ground covered in the literally thousands of posts on remailers.

8.3. Anonymity and Digital Pseudonyms

8.3.1. Why is anonymity so important?

- It allows escape from past, an often-essential element of straightening out (an important function of the Western frontier, the French Foreign Legion, etc., and something we are losing as the dossiers travel with us wherever we go)
- It allows new and diverse types of opinions, as noted below
- More basically, anonymity is important because identity is not as important as has been made out in our dossier society. To wit, if Alice wishes to remain anonymous or pseudonymous to Bob, Bob cannot "demand" that she provide here "real" name. It's a matter of negotiation between them. (Identity is not free...it is a credential like any other and cannot be demanded, only negotiated.)
- Voting, reading habits, personal behavior...all are examples where privacy (= anonymity, effectively) are critical. The next section gives a long list of reasons for anonymity.

8.3.2. What's the difference between anonymity and pseudonymity?

- + Not much, at one level...we often use the term "digital pseudonym" in a strong sense, in which the actual identity cannot be deduced easily
 - this is "anonymity" in a certain sense
- But at another level, a pseudonym carries reputations, credentials, etc., and is not "anonymous"
- people use pseudonyms sometimes for whimsical reasons (e.g., "From spaceman.spiff@calvin.hobbes.org Sep 6, 94 06:10:30"), sometimes to keep different mailing lists separate (different personnas for different groups), etc.

8.3.3. Downsides of anonymity

- libel and other similar dangers to reputations
- + hit-and-runs actions (mostly on the Net)
 - + on the other hand, such rantings can be ignored (KILL file)
 - positive reputations
- accountability based on physical threats and tracking is lost
- + Practical issue. On the Cypherpunks list, I often take "anonymous" messages less seriously.
 - They're often more bizarre and inflammatory than ordinary posts, perhaps for good reason, and they're certainly harder to take seriously and respond to. This is to be expected. (I should note that some pseudonyms, such as Black Unicorn and Pr0duct Cypher, have established reputable digital personnas and are well worth replying to.)
- repudiation of debts and obligations
- + infantile flames and run-amok postings
 - racism, sexism, etc.
 - like "Rumormonger" at Apple?
- but these are reasons for pseudonym to be used, where the reputation of a pseudonym is important
- + Crimes...murders, bribery, etc.
 - These are dealt with in more detail in the section on

crypto anarchy, as this is a major concern (anonymous markets for such services)

8.3.4. "How will privacy and anonymity be attacked?"

- the downsides just listed are often cited as a reason we can't have "anonymity"
- like so many other "computer hacker" items, as a tool for the "Four Horsemen": drug-dealers, money-launderers, terrorists, and pedophiles.
- as a haven for illegal practices, e.g., espionage, weapons trading, illegal markets, etc.
- + tax evasion ("We can't tax it if we can't see it.")
 - same system that makes the IRS a "silent partner" in business transactions and that gives the IRS access to-- and requires--business records
- + "discrimination"
 - that it enables discrimination (this used to be OK)
 - exclusionary communities, old boy networks

8.3.5. "How will random accusations and wild rumors be controlled in anonymous forums?"

- First off, random accusations and hearsay statements are the norm in modern life; gossip, tabloids, rumors, etc. We don't worry obsessively about what to do to stop all such hearsay and even false comments. (A disturbing trend has been the tendency to sue, or threaten suits. And increasingly the attitude is that one can express opinions, but not make statements "unless they can be proved." That's not what free speech is all about!)
- Second, reputations matter. We base our trust in statements on a variety of things, including: past history, what others say about veracity, external facts in our possession, and motives.

8.3.6. "What are the legal views on anonymity?"

- + Reports that Supreme Court struck down a Southern law requiring pamphlet distributors to identify themselves. 9I don't have a cite on this.)
- However, Greg Broiles provided this quote, from Talley v. State of California, 362 U.S. 60, 64-65, 80 S.Ct. 536, 538-539 (1960) : "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all."

Greg adds: "It later says "Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names. It is plain that anonymity has sometimes been assumed for the most constructive purposes." [Greg Broiles, 1994-04-12]

- + And certainly many writers, journalists, and others use pseudonyms, and have faced no legal action.
 - Provided they don't use it to evade taxes, evade legal judgments, commit fraud, etc.
- I have heard (no cites) that "going masked for the purpose of going masked" is illegal in many jurisdictions. Hard to believe, as many other disguises are just as effective and

are presumably not outlawed (wigs, mustaches, makeup, etc.). I assume the law has to do with people wearing ski masks and such in "inappropriate" places. Bad law, if real.

8.3.7. Some Other Uses for Anonymous Systems:

- + Groupware and Anonymous Brainstorming and Voting
 - systems based on Lotus Notes and designed to encourage wild ideas, comments from the shy or overly polite, etc.
 - these systems could initially start in meeting and then be extended to remote sites, and eventually to nationwide and international forums
 - the NSA may have a heart attack over these trends...
- + "Democracy Wall" for encrypted messages
 - possibly using time-delayed keys (where even the public key, for reading the plaintext, is not distributed for some time)
 - under the cover of an electronic newspaper, with all of the constitutional protections that entails: letters to the editor can be anonymous, ads need not be screened for validity, advertising claims are not the responsibility of the paper, etc.
- + Anonymous reviews and hypertext (for new types of journals)
 - + the advantages
 - honesty
 - increased "temperature" of discourse
 - + disadvantages
 - increased flames
 - intentional misinformation
- + Store-and-forward nodes
 - used to facilitate the anonymous voting and anonymous inquiry (or reading) systems
 - Chaum's "mix"
- + telephone forwarding systems, using digital money to pay for the service
 - and TRMs?
- + Fiber optics
 - + hard to trace as millions of miles are laid, including virtually untraceable lines inside private buildings
 - suppose government suspects encrypted packets are going in to the buildings of Apple...absent any direct knowledge of crimes being aided and abetted, can the government demand a mapping of messages from input to output?
 - That is, will the government demand full disclosure of all routings?
 - high bandwidth means many degrees of freedom for such systems to be deployed
- + Within systems, i.e., user logs on to a secure system and is given access to his own processor
 - in a 288-processor system like the NCR/ATT 3600 (or even larger)
 - under his cryptonym he can access certain files, generate others, and deposit message untraceably in other mail locations that other agents or users can later retrieve and forward....
 - in a sense, he can use this access to launch his own agent processes (anonymity is essential for many agent-based systems, as is digital money)

- + Economic incentives for others to carry mail to other sites...
 - further diffusion and hiding of the true functions
- + Binary systems (two or more pieces needed to complete the message)
 - possibly using viruses and worms to handle the complexities of distributing these messages
 - agents may handle the transfers, with isolation between the agents, so routing cannot be traced (think of scene in "Double-Crossed" where bales of marijuana are passed from plane to boat to chopper to trucks to cars)
 - this protects against conspiracies
- + Satellites
 - + physical security, in that the satellites would have to be shot down to halt the broadcasting
 - + scenario: WARC (or whomever) grants broadcast rights in 1996 to some country or consortium, which then accepts any and all paying customers
 - cold cash
 - the BCCI of satellite operators
 - + VSATs, L-Band, Satellites, Low-Earth Orbit
 - Very Small Aperture Terminals
 - L-Band...what frequency?
 - + LEO, as with Motorola's Iridium, offers several advantages
 - lower-power receivers and smaller antennas
 - low cost to launch, due to small size and lower need for 10-year reliability
 - avoidance of the "orbital slot" licensing morass (though I presume some licensing is still involved)
 - can combine with impulse or nonsinusoidal transmissions
- 8.3.8. "True Names"
- 8.3.9. Many ways to get pseudonyms:
 - Telnet to "port 25" or use SLIP connections to alter domain name; not very secure
 - Remailers
- 8.3.10. "How is Pseudonymity Compromised?"
 - slip-ups in style, headers, sig blocks, etc.
 - inadvertent revealing, via the remailers
 - traffic analysis of remailers (not very likely, at least not for non-NSA adversaries)
 - correlations, violations of the "indistinguishability principle"
- 8.3.11. Miscellaneous Issues
 - Even digital pseudonyms can get confusing...someone recently mistook "Tommy the Tourist" for being such an actual digital pseudonym (when of course that is just attached to all posts going through a particular remailer).
- 8.4. Reasons for Anonymity and Digital Pseudonyms (and Untraceable E-Mail)
 - 8.4.1. (There are so many reasons, and this is asked so often, that I've collected these various reasons here. More can be added, of course.)
 - 8.4.2. Privacy in general
 - 8.4.3. Physical Threats
 - + "corporate terrorism" is not a myth: drug dealers and

- other "marginal" businessmen face this every day
- extortion, threats, kidnappings
- + and many businesses of the future may well be less "gentlemanly" than the conventional view has it
- witness the bad blood between Intel and AMD, and then imagine it getting ten times worse
- and national rivalries, even in ostensibly legal businesses (think of arms dealers), may cause more use of violence
- + Mafia and other organized crime groups may try to extort payments or concessions from market participants, causing them to seek the relative protection of anonymous systems
 - with reputations
- + Note that calls for the threatened to turn to the police for protection has several problems
 - the activities may be illegal or marginally illegal (this is the reason the Mafia can often get involved and why it may even sometimes have a positive effect, acting as the cop for illegal activities)
 - the police are often too busy to get involved, what with so much physical crime clogging the courts
- extortion and kidnappings can be done using these very techniques of cryptoanarchy, thus causing a kind of arms race
- + battered and abused women and families may need the equivalent of a "witness protection program"
- + because of the ease of tracing credit card purchases, with the right bribes and/or court orders (or even hacking), battered wives may seek credit cards under pseudonyms
 - and some card companies may oblige, as a kind of politically correct social gesture
- + or groups like NOW and Women Against Rape may even offer their own cards
 - perhaps backed up by some kind of escrow fund
 - could be debit cards
- + people who participate in cyberspace businesses may fear retaliation or extortion in the real world
 - threats by their governments (for all of the usual reasons, plus kickbacks, threats to close them down, etcl)
 - ripoffs by those who covet their success...

8.4.4. Voting

- We take it for granted in Western societies that voting should be "anonymous"--untraceable, unlinkable
- we don't ask people "What have you got to hide?" or tell them "If you're doing something anonymously, it must be illegal."
- Same lesson ought to apply to a lot of things for which the government is increasingly demanding proof of identity for
- + Anonymous Voting in Clubs, Organizations, Churches, etc.
 - + a major avenue for spreading CA methods: "electronic blackballing," weighted voting (as with number of shares)
 - + e.g., a corporation issues "voting tokens," which can be used to vote anonymously
 - or even sold to others (like selling shares, except selling only the voting right for a specific election

- is cheaper, and many people don't much care about elections)
- + a way to protect against deep pockets lawsuits in, say, race discrimination cases
 - wherein a director is sued for some action the company takes-anonymity will give him some legal protection, some "plausible deniability"
- + is possible to set up systems (cf. Salomaa) in which some "supervotes" have blackball power, but the use of these vetos is indistinguishable from a standard majority rules vote
 - i.e., nobody, except the blackballer(s), will know whether the blackball was used!
- + will the government seek to limit this kind of protocol?
 - claiming discrimination potential or abuse of voting rights?
- + will Justice Department (or SEC) seek to overturn anonymous voting?
 - as part of the potential move to a "full disclosure" society?
 - related to antidiscrimination laws, accountability, etc.
- + Anonymous Voting in Reputation-Based Systems (Journals, Markets)
 - + customers can vote on products, on quality of service, on the various deals they've been involved in
 - not clear how the voting rights would get distributed
 - the idea is to avoid lawsuits, sanctions by vendors, etc. (as with the Bose suit)
 - + Journals
 - a canonical example, and one which I must include, as it combines anonymous refereeing (already standard, in primitive forms), hypertext (links to reviews), and basic freedom of speech issues
 - this will likely be an early area of use
 - this whole area of consumer reviews may be a way to get CA bandwidth up and running (lots of PK-encrypted traffic sloshing around the various nets)
- 8.4.5. Maintenance of free speech
 - protection of speech
 - + avoiding retaliation for controversial speech
 - this speech may be controversial, insulting, horrific, politically incorrect, racist, sexist, speciesist, and other horrible...but remailers and anonymity make it all impossible to stop
 - whistleblowing
 - + political speech
 - KKK, Aryan Resistance League, Black National Front, whatever
 - cf. the "debate" between "Locke" and "Demosthenes" in Orson Scott Card's novel, "Ender's Game."
 - (Many of these reasons are also why 'data havens' will eventually be set up...indeed, they already exist...homolka trial, etc.)
- 8.4.6. Adopt different personnas, pseudonyms
- 8.4.7. Choice of reading material, viewing habits, etc.

- to prevent dossiers on this being formed, anonymous purchases are needed (cash works for small items, not for video rentals, etc.)
- + video rentals
 - (Note: There are "laws" making such releases illegal, but...)
- cable t.v. viewing habits
- + mail-order purchases
 - yes, they need your address to ship to, but there may be cutouts that delink (e.g., FedEx might feature such a service, someday)
- 8.4.8. Anonymity in Requesting Information, Services, Goods
- + a la the controversy over Caller ID and 900 numbers: people don't want their telephone numbers (and hence identities) fed into huge consumer-preference data banks
 - of the things they buy, the videos they rent, the books they read. etc. (various laws protect some of these areas, like library books, video rentals)
 - subscription lists are already a booming resale market...this will get faster and more finely "tuned" with electronic subscriptions: hence the desire to subscribe anonymously
- + some examples of "sensitive" services that anonymity may be desired in (especially related to computers, modems, BBSes)
- + reading unusual or sensitive groups: alt.sex.bondage, etc.
 - or posting to these groups!
 - recent controversy over NAMBLA may make such protections more desirable to some (and parallel calls for restrictions!)
 - posting to such groups, especially given that records are perpetual and that government agencies read and file postings (an utterly trivial thing to do)
 - requesting help on personal issues (equivalent to the "Name Withheld" seen so often)
- + discussing controversial political issues (and who knows what will be controversial 20 years later when the poster is seeking a political office, for example?)
 - given that some groups have already (1991) posted the past postings of people they are trying to smear!
- + Note: the difference between posting to a BBS group or chat line and writing a letter to an editor is significant
 - partly technological: it is vastly easier to compile records of postings than it is to cut clippings of letters to editors (though this will change rapidly as scanners make this easy)
 - partly sociological: people who write letters know the letters will be with the back issues in perpetuity, that bound issues will preserve their words for many decades to come (and could conceivably come back to haunt them), but people who post to BBSes probably think their words are temporary
- + and there are some other factors
 - no editing
 - no time delays (and no chance to call an editor and retract a letter written in haste or anger)

- + and letters can, and often are, written with the "Name Withheld" signature-this is currently next to impossible to do on networks
 - though some "forwarding" services have informally sprung up
- + Businesses may wish to protect themselves from lawsuits over comments by their employees
- + the usual "The opinions expressed here are not those of my employer" may not be enough to protect an employer from lawsuits
 - imagine racist or sexist comments leading to lawsuits (or at least being brought up as evidence of the type of "attitude" fostered by the company, e.g., "I've worked for Intel for 12 years and can tell you that blacks make very poor engineers.")
- + employees may make comments that damage the reputations of their companies
 - Note: this differs from the current situation, where free speech takes priority over company concerns, because the postings to a BBS are carried widely, may be searched electronically (e.g., AMD lawyers search the UseNet postings of 1988-91 for any postings by Intel employees besmirching the quality or whatever of AMD chips),
 - and so employees of corporations may protect themselves, and their employers, by adopting pseudonyms
- + Businesses may seek information without wanting to alert their competitors
 - this is currently done with agents, "executive search firms," and lawyers
 - but how will it evolve to handle electronic searches?
- + there are some analogies with filings of "Freedom of Information Act" requests, and of patents, etc.
 - + these "fishing expeditions" will increase with time, as it becomes profitable for companies to search though mountains of electronically-filed materials
 - environmental impact studies, health and safety disclosures, etc.
 - could be something that some companies specialize in
- + Anonymous Consultation Services, Anonymous Stringers or Reporters
 - + imagine an information broker, perhaps on an AMIX-like service, with a network of stringers
 - + think of the arms deal newsletter writer in Hallahan's The Trade, with his network of stringers feeding him tips and inside information
 - instead of meeting in secretive locations, a very expensive proposition (in time and travel), a secure network can be used
 - with reputations, digital pseudonyms, etc.
- + they may not wish their actual identities known
 - threats from employers, former employers, government agencies
- + harassment via the various criminal practices that will become more common (e.g., the ease with which assailants and even assassins can be contracted for)
 - part of the overall move toward anonymity

- fears of lawsuits, licensing requirements, etc.
- + Candidates for Such Anonymous Consultation Services
- + An arms deals newsletter
 - an excellent reputation for accuracy and timely information
- + sort of like an electronic form of Jane's
 - with scandals and government concern
- but nobody knows where it comes from
- + a site that distributes it to subscribers gets it
 - with another larger batch of forwarded material
 - NSA, FBI, Fincen, etc. try to track it down
- + "Technology Insider" reports on all kinds of new technologies
 - patterned after Hoffler's Microelectronics News, the Valley's leading tip sheet for two decades
 - the editor pays for tips, with payments made in two parts: immediate, and time-dependent, so that the accuracy of a tip, and its ultimate importance (in the judgment of the editor) can be proportionately rewarded
- + PK systems, with contributors able to encrypt and then publicly post (using their own means of diffusion)
 - with their messages containing further material, such as authentications, where to send the payments, etc.
- + Lundberg's Oil Industry Survey (or similar)
 - i.e., a fairly conventional newsletter with publicly known authors
 - in this case, the author is known, but the identities of contributors is well-protected
- + A Conspiracy Newsletter
 - reporting on all of the latest theories of misbehavior (as in the "Conspiracies" section of this outline)
- + a wrinkle: a vast hypertext web, with contributors able to add links and nodes
 - + naturally, their real name-if they don't care about real-world repercussions-or one of their digital pseudonyms (may as well use cryptonyms) is attached
- + various algorithms for reputations
 - sum total of everything ever written, somehow measured by other comments made, by "voting," etc.
 - a kind of moving average, allowing for the fact that learning will occur, just as a researcher probably gets better with time, and that as reputation-based systems become better understood, people come to appreciate the importance of writing carefully
- + and one of the most controversial of all: Yardley's Intelligence Daily
 - though it may come out more than daily!
- + an ex-agent set this up in the mid-90s, soliciting contributions via an anonymous packet-switching system
 - refined over the next couple of years
 - combination of methods

- government has been trying hard to identify the editor, "Yardley"
- he offers a payback based on value of the information, and even has a "Requests" section, and a Classified Ad section
- a hypertext web, similar to the Conspiracy Newsletter above
- + Will Government Try to Discredit the Newsletter With False Information?
 - of course, the standard ploy in reputation-based systems
 - + but Yardley has developed several kinds of filters for this
 - digital pseudonyms which gradually build up reputations
 - cross-checking of his own sort
 - he even uses language filters to analyze the text
 - + and so what?
 - the world is filled with disinformation, rumors, lies, half-truths, and somehow things go on....
- + Other AMIX-like Anonymous Services
 - + Drug Prices and Tips
 - tips on the quality of various drugs (e.g., "Several reliable sources have told us that the latest Maui Wowie is very intense, numbers below...")
 - + synthesis of drugs (possibly a separate subscription)
 - designer drugs
 - home labs
 - avoiding detection
 - + The Hackers Daily
 - tips on hacking and cracking
 - anonymous systems themselves (more tips)
 - Product evaluations (anonymity needed to allow honest comments with more protection against lawsuits)
- + Newspapers Are Becoming Concerned with the Trend Toward Paying for News Tips
 - by the independent consultation services
 - but what can they do?
 - + lawsuits are tried, to prevent anonymous tips when payments are involved
 - their lawyers cite the tax evasion and national security aspects
- + Private Data Bases
 - + any organization offering access to data bases must be concerned that somebody-a disgruntled customer, a whistleblower, the government, whoever-will call for an opening of the files
 - under various "Data Privacy" laws
 - or just in general (tort law, lawsuits, "discovery")
 - + thus, steps will be taken to isolate the actual data from actual users, perhaps via cutouts
 - + e.g., a data service sells access, but subcontracts out the searches to other services via paths that are untraceable
 - + this probably can't be outlawed in general-though any

specific transaction might later be declared illegal, etc., at which time the link is cut and a new one is established-as this would outlaw all subcontracting arrangements!

- i.e., if Joe's Data Service charges \$1000 for a search on widgets and then uses another possibly transitory (meaning a cutout) data service, the most a lawsuit can do is to force Joe to stop using this untraceable service
- levels of indirection (and firewalls that stop the propagation of investigations)
- + Medical Polls (a la AIDS surveys, sexual practices surveys, etc.)
- + recall the method in which a participant tosses a coin to answer a question...the analyst can still recover the important ensemble information, but the "phase" is lost
 - i.e., an individual answering "Yes" to the question "Have you ever had xyz sex?" may have really answered "No" but had his answer flipped by a coin toss
- + researchers may even adopt sophisticated methods in which explicit diaries are kept, but which are then transmitted under an anonymous mailing system to the researchers
 - obvious dangers of authentication, validity, etc.
- + Medical testing: many reasons for people to seek anonymity
 - AIDS testing is the preeminent example
 - but also testing for conditions that might affect insurability or employment (e.g., people may go to medical havens in Mexico or wherever for tests that might lead to uninsurability should insurance companies learn of the "precondition")
 - + except in AIDS and STDs, it is probably both illegal and against medical ethics to offer anonymous consultations
 - perhaps people will travel to other countries
- 8.4.9. Anonymity in Belonging to Certain Clubs, Churches, or Organizations
 - + people fear retaliation or embarrassment should their membership be discovered, now or later
 - e.g., a church member who belongs to controversial groups or clubs
 - mainly, or wholly, those in which physical contact or other personal contact is not needed (a limited set)
 - similar to the cell-based systems described elsewhere
 - + Candidates for anonymous clubs or organizations
 - Earth First!, Act Up, Animal Liberation Front, etc.
 - NAMBLA and similar controversial groups
 - all of these kinds of groups have very vocal, very visible members, visible even to the point of seeking out television coverage
 - but there are probably many more who would join these groups if their identities could be shielded from public group, for the sake of their careers, their families, etc.
 - + ironically, the corporate crackdown on outside activities considered hostile to the corporation (or exposing them to secondary lawsuits, claims, etc.) may cause greater use of anonymous systems
 - cell-based membership in groups
 - the growth of anonymous membership in groups (using

pseudonyms) has a benefit in increasing membership by people otherwise afraid to join, for example, a radical environmental group

8.4.10. Anonymity in Giving Advice or Pointers to Information

- suppose someone says who is selling some illegal or contraband product...is this also illegal?
- hypertext systems will make this inevitable

8.4.11. Reviews, Criticisms, Feedback

- "I am teaching sections for a class this term, and tomorrow I am going to: 1) tell my students how to use a remailer, and 2) solicit anonymous feedback on my teaching.

"I figure it will make them less apprehensive about making honest suggestions and comments (assuming any of them bother, of course)." [Patrick J. LoPresti patl@lcs.mit.edu, alt.privacy.anon-server, 1994-09-08]

8.4.12. Protection against lawsuits, "deep pockets" laws

- + by not allowing the wealth of an entity to be associated with actions
 - this also works by hiding assets, but the IRS frowns on that, so unlinking the posting or mailing name with actual entity is usually easier
- + "deep pockets"
 - it will be in the interest of some to hide their identities so as to head off these kinds of lawsuits (filed for whatever reasons, rightly or wrongly)
 - postings and comments may expose the authors to lawsuits for libel, misrepresentation, unfair competition, and so on (so much for free speech in these beknighted states)
- + employers may also be exposed to the same suits, regardless of where their employees posted from
 - on the tenuous grounds that an employee was acting on his employer's behalf, e.g., in defending an Intel product on Usenet
 - this, BTW, is another reason for people to seek ways to hide some of their assets--to prevent confiscation in deep pockets lawsuits (or family illnesses, in which various agencies try to seize assets of anybody they can)
 - and the same computers that allow these transactions will also allow more rapid determination of who has the deepest pockets!
- + by insulating the entity from repercussions of "sexist" or "racist" comments that might provoke lawsuits, etc.
 - (Don't laugh--many companies are getting worried that what their employees write on Usenet may trigger lawsuits against the companies.)
- + many transactions may be deemed illegal in some jurisdictions
 - + even in some that the service or goods provider has no control over
 - example: gun makers being held liable for firearms deaths in the District of Columbia (though this was recently cancelled)
 - the maze of laws may cause some to seek anonymity to protect themselves against this maze
- + Scenario: Anonymous organ donor banks
 - + e.g., a way to "market" rare blood types, or whatever,

without exposing one's self to forced donation or other sanctions

- "forced donation" involves the lawsuits filed by the potential recipient
- at the time of offer, at least...what happens when the deal is consummated is another domain
- and a way to avoid the growing number of government stings

8.4.13. Journalism and Writing

- + writers have had a long tradition of adopting pseudonyms, for a variety of reasons
 - because they couldn't get published under their True Names, because they didn't want their true names published, for the fun of it, etc.
 - George Elliot, Lewis Carroll, Saki, Mark Twain, etc.
 - reporters
 - + radio disc jockeys
 - a Cypherpunk who works for a technology company uses the "on air persona" of "Arthur Dent" ("Hitchhiker's Guide") for his part-time radio broadcasting job...a common situation, he tells me
 - + whistleblowers
 - this was an early use
 - + politically sensitive persons
 - "
 - + I subsequently got myself an account on anon.penet.fi as the "Lt.
 - Starbuck" entity, and all later FAQ updates were from that account.
 - For reasons that seemed important at the time, I took it upon myself to
 - become the moderator/editor of the FAQ."
 - <an54835@anon.penet.fi, 4-3-94, alt.fan.karla-homolka>
 - + Example: Remailers were used to skirt the publishing ban on the Karla Homolka case
 - various pseudonymous authors issued regular updates
 - much consternation in Canada!
 - + avoidance of prosecution or damage claims for writing, editing, distributing, or selling "damaging" materials is yet another reason for anonymous systems to emerge: those involved in the process will seek to immunize themselves from the various tort claims that are clogging the courts
 - producers, distributors, directors, writers, and even actors of x-rated or otherwise "unacceptable" material may have to have the protection of anonymous systems
 - imagine fiber optics and the proliferation of videos and talk shows....bluenoses and prosecutors will use "forum shopping" to block access, to prosecute the producers, etc.
- #### 8.4.14. Academic, Scientific, or Professional
- protect other reputations (professional, authorial, personal, etc.)
 - wider range of actions and behaviors (authors can take chances)
 - floating ideas out under pseudonyms
 - later linking of these pseudonyms to one's own identity, if needed (a case of credential transfer)

- floating unusual points of view
- Peter Wayner writes: "I would think that many people who hang out on technical newsgroups would be very familiar with the anonymous review procedures practiced by academic journals. There is some value when a reviewer can speak their mind about a paper without worry of revenge. Of course everyone assures me that the system is never really anonymous because there are always only three or four people qualified to review each paper. :-) ...Perhaps we should go out of our way to make anonymous, technical comments about papers and ideas in the newsgroups to facilitate the development of an anonymous commenting culture in cyberspace." [Peter Wayner, 1993-02-09]
- 8.4.15. Medical Testing and Treatment
 - anonymous medical tests, a la AIDS testing
- 8.4.16. Abuse, Recovery
 - + personal problem discussions
 - incest, rape, emotional, Dear Abby, etc.
- 8.4.17. Bypassing of export laws
 - Anonymous remailers have been useful for bypassing the ITARs...this is how PGP 2.6 spread rapidly, and (we hope!) untraceably from MIT and U.S. sites to offshore locations.
- 8.4.18. Sex groups, discussions of controversial topics
 - the various alt.sex groups
 - People may feel embarrassed, may fear repercussions from their employers, may not wish their family and friends to see their posts, or may simply be aware that Usenet is archived in many, many places, and is even available on CD-ROM and will be trivially searchable in the coming decades
 - + the 100% traceability of public postings to UseNet and other bulletin boards is very stifling to free expression and becomes one of the main justifications for the use of anonymous (or pseudonymous) boards and nets
 - there may be calls for laws against such compilation, as with the British data laws, but basically there is little that can be done when postings go to tens of thousands of machines and are archived in perpetuity by many of these nodes and by thousands of readers
 - readers who may incorporate the material into their own postings, etc. (hence the absurdity of the British law)
- 8.4.19. Avoiding political espionage
 - + TLAs in many countries monitor nearly all international communications (and a lot of domestic communications, too)
 - companies and individuals may wish to avoid reprisals, sanctions, etc.
 - PGP is reported to be in use by several dissident groups, and several Cypherpunks are involved in assisting them.
 - "...one legitimate application is to allow international political groups or companies to exchange authenticated messages without being subjected to the risk of espionage/compromise by a three letter US agency, foreign intelligence agency, or third party." [Sean M. Dougherty, alt.privacy.anon-server, 1994-09-07]
- 8.4.20. Controversial political discussion, or membership in political groups, mailing lists, etc.
 - + Recall House UnAmerican Activities Committee
 - and it's modern variant: "Are you now, or have you ever

been, a Cypherpunk?"

8.4.21. Preventing Stalking and Harassment

- avoid physical tracing (harassment, "wannafucks," stalkers, etc.)
- women and others are often sent "wannafuck?" messages from the males that outnumber them 20-to-1 in many newsgroups-- pseudonyms help.
- given the ease with which net I.D.s can be converted to physical location information, many women may be worried.
- + males can be concerned as well, given the death threats issued by, for example, S. Boxx/Detweiler.
 - as it happens, S. Boxx threatened me, and I make my home phone number and location readily known...but then I'm armed and ready.

8.4.22. pressure relief valve: knowing one can flee or head for the frontier and not be burdened with a past

- perhaps high rate of recidivism is correlated with this inability to escape...once a con, marked for life (certainly denied access to high-paying jobs)

8.4.23. preclude lawsuits, subpoenas, entanglement in the legal machinery

8.4.24. Business Reasons

- + Corporations can order supplies, information, without tipping their hand
 - the Disney purchase of land, via anonymous cutouts (to avoid driving the price way up)
 - secret ingredients (apocryphally, Coca Cola)
- avoiding the "deep pockets" syndrome mentioned above
- to beat zoning and licensing requirements (e.g., a certain type of business may not be "permitted" in a home office, so the homeowner will have to use cutouts to hide from enforcers)
- protection from (and to) employers
- + employees of corporations may have to do more than just claim their view are not those of their employer
 - e.g., a racist post could expose IBM to sanctions, charges
- + thus, many employees may have to further insulate their identities
 - blanc@microsoft.com is now blanc@pylon.com...coincidence?
- + moonlighting employees (the original concern over Black Net and AMIX)
 - employers may have all kinds of concerns, hence the need for employees to hide their identities
 - note that this intersects with the licensing and zoning aspects
- publishers, service-providers
- + Needed for Certain Kinds of Reputation-Based Systems
 - + a respected scientist may wish to float a speculative idea
 - and be able to later prove it was in fact his idea

8.4.25. Protection against retaliation

- whistleblowing
- + organizing boycotts
 - (in an era of laws regulating free speech, and "SLAPP" lawsuits)

- + the visa folks (Cantwell and Siegel) threatening those who comment with suits
 - the law firm that posted to 5,000 groups....also raises the issue again of why the Net should be subsidized
 - participating in public forums
 - + as one person threatened with a lawsuit over his Usenet comments put it:
 - "And now they are threatening me. Merely because I openly expressed my views on their extremely irresponsible behaviour. Anyways, I have already cancelled the article from my site and I publicly apologize for posting it in the first place. I am scared :) I take all my words back. Will use the anonymous service next time :)"
 - 8.4.26. Preventing Tracking, Surveillance, Dossier Society
 - + avoiding dossiers in general
 - too many dossiers being kept; anonymity allows people to at least hold back the tide a bit
 - + headhunting, job searching, where revealing one's identity is not always a good idea
 - some headhunters are working for one's current employer!
 - dossiers
 - 8.4.27. Some Examples from the Cypherpunks List
 - + S, Boxx, aka Sue D. Nym, Pablo Escobar, The Executioner, and an12070
 - but Lawrence Detweiler by any other name
 - + he let slip his pseudonym-true name links in several ways
 - stylistic cues
 - mention of things only the "other" was likely to have heard
 - + sysops acknowledged certain linkings
 - *not* Julf, though Julf presumably knew the identity of "an12070"
 - + Pr0duct Cypher
 - Jason Burrell points out: "Take Pr0duct Cypher, for example. Many believe that what (s)he's doing(*) is a Good Thing, and I've seen him/her using the Cypherpunk remailers to conceal his/her identity....* If you don't know, (s)he's the person who wrote PGPTOOLS, and a hack for PGP 2.3a to decrypt messages written with 2.6. I assume (s)he's doing it anonymously due to ITAR regulations." [J.B., 1994-09-05]
 - + Black Unicorn
 - Is the pseudonym of a Washington, D.C. lawyer (I think), who has business ties to conservative bankers and businessmen in Europe, especially Liechtenstein and Switzerland. His involvement with the Cypherpunks group caused him to adopt this pseudonym.
 - Ironically, he got into a battle with S. Boxx/Detweiler and threatened legal action. This cause a rather instructive debate to occur.
- 8.5. Untraceable E-Mail
- 8.5.1. The Basic Idea of Remailers
- Messages are encrypted, envelopes within envelopes, thus making tracing based on external appearance impossible. If the remailer nodes keep the mapping between inputs and outputs secret, the "trail" is lost.

8.5.2. Why is untraceable mail so important?

- + Bear in mind that "untraceable mail" is the default situation for ordinary mail, where one seals an envelope, applies a stamp, and drops it anonymously in a letterbox. No records are kept, no return address is required (or confirmed), etc.
 - regional postmark shows general area, but not source mailbox
- + Many of us believe that the current system of anonymous mail would not be "allowed" if introduced today for the first time
 - Postal Service would demand personalized stamps, verifiable return addresses, etc. (not foolproof, or secure, but...)
- + Reasons:
 - to prevent dossiers of who is contacting whom from being compiled
 - to make contacts a personal matter
 - many actual uses: maintaining pseudonyms, anonymous contracts, protecting business dealings, etc.

8.5.3. How do Cypherpunks remailers work?

8.5.4. How, in simple terms, can I send anonymous mail?

8.5.5. Chaum's Digital Mixes

- How do digital mixes work?

8.5.6. "Are today's remailers secure against traffic analysis?"

- Mostly not. Many key digital mix features are missing, and the gaps can be exploited.
- + Depends on features used:
 - Reordering (e.g., 10 messages in, 10 messages out)
 - Quantization to fixed sizes (else different sizes give clues)
 - Encryption at all stages (up to the customer, of course)
 - But probably not, given that current remailers often lack necessary features to deter traffic analysis. Padding is iffy, batching is often not done at all (people cherish speed, and often downcheck remailers that are "too slow")
 - Best to view today's remailers as experiments, as prototypes.

8.6. Remailers and Digital Mixes (A Large Section!)

8.6.1. What are remailers?

8.6.2. Cypherpunks remailers compared to Julf's

- + Apparently long delays are mounting at the penet remailer. Complaints about week-long delays, answered by:
 - "Well, nobody is stopping you from using the excellent series of cypherpunk remailers, starting with one at remail@vox.hacktic.nl. These remailers beat the hell out of anon.penet.fi. Either same day or at worst next day service, PGP encryption allowed, chaining, and gateways to USENET." [Mark Terka, The normal delay for anon.penet.fi?, alt.privacy.anon-server, 1994-08-19]
- + "How large is the load on Julf's remailer?"
 - "I spoke to Julf recently and what he really needs is \$750/month and one off \$5000 to upgrade his feed/machine. I am looking at the possibility of sponsorship (but don't let that stop other people trying).....Julf has built up a loyal, trusting following of over 100,000 people and

6000 messages/day. Upgrading him seems a good idea.....Yes, there are other remailers. Let's use them if we can and lessen the load on Julf." [Steve Harris, alt.privacy.anon-server, 1994-08-22]

- (Now if the demand on Julf's remailer is this high, seems like a great chance to deploy some sort of fee-based system, to pay for further expansion. No doubt many of the users would drop off, but such is the nature of business.)

8.6.3. "How do remailers work?"

- (The MFAQ also has some answers.)
- Simply, they work by taking an incoming text block and looking for instructions on where to send the remaining text block, and what to do with it (decryption, delays, postage, etc.)
- + Some remailers can process the Unix mail program(s) outputs directly, operating on the mail headers
 - names of programs...
- + I think the ":::" format Eric Hughes came up with in his first few days of looking at this turned out to be a real win (perhaps comparable to John McCarthy's decision to use parenthesized s-expressions in Lisp?).
 - it allows arbitrary chaining, and all mail messages that have text in standard ASCII--which is all mailers, I believe--can then use the Cypherpunks remailers

8.6.4. "What are some uses of remailers?"

- This is mostly answered in other sections, outlining the uses of anonymity and digital pseudonyms: remailers are of course the enabling technology for anonymity.
- + using remailers to foil traffic analysis
 - An interesting comment from someone not part of our group, in a discussion of proposal to disconnect U.K. computers from Usenet (because of British laws about libel, about pornography, and such): "PGP hides the target. The remailers discard the source info. The more paranoid remailers introduce a random delay on resending to foil traffic analysis. You'd be surprised what can be done :-).If you use a chain then the first remailer knows who you are but the destination is encrypted. The last remailer knows the destination but cannot know the source. Intermediate ones know neither." [Malcolm McMahon, JANET (UK) to ban USENET?, comp.org.eff.talk, 1994-08-30]
 - So, word is spreading. Note the emphasis on Cypherpunks-type remailers, as opposed to Julf-style anonymous services.
- + options for distributing anonymous messages
 - + via remailers
 - the conventional approach
 - upsides: recipient need not do anything special
 - downsides: that's it--recipient may not welcome the message
 - + to a newsgroup
 - a kind of message pool
 - upsides: worldwide dist
 - to an ftp site, or Web-reachable site
 - a mailing list

8.6.5. "Why are remailers needed?"

+ Hal Finney summarized the reasons nicely in an answer back in early 1993.

- "There are several different advantages provided by anonymous remailers. One of the simplest and least controversial would be to defeat traffic analysis on ordinary email.....Two people who wish to communicate privately can use PGP or some other encryption system to hide the content of their messages. But the fact that they are communicating with each other is still visible to many people: sysops at their sites and possibly at intervening sites, as well as various net snoopers. It would be natural for them to desire an additional amount of privacy which would disguise who they were communicating with as well as what they were saying.

"Anonymous remailers make this possible. By forwarding mail between themselves through remailers, while still identifying themselves in the (encrypted) message contents, they have even more communications privacy than with simple encryption.

"(The Cypherpunk vision includes a world in which literally hundreds or thousands of such remailers operate. Mail could be bounced through dozens of these services, mixing in with tens of thousands of other messages, re-encrypted at each step of the way. This should make traffic analysis virtually impossible. By sending periodic dummy messages which just get swallowed up at some step, people can even disguise when they are communicating.)" [Hal Finney, 1993-02-23]

"The more controversial vision associated with anonymous remailers is expressed in such science fiction stories as "True Names", by Vernor Vinge, or "Ender's Game", by Orson Scott Card. These depict worlds in which computer networks are in widespread use, but in which many people choose to participate through pseudonyms. In this way they can make unpopular arguments or participate in frowned-upon transactions without their activities being linked to their true identities. It also allows people to develop reputations based on the quality of their ideas, rather than their job, wealth, age, or status." [Hal Finney, 1993-02-23]

- "Other advantages of this approach include its extension to electronic on-line transactions. Already today many records are kept of our financial dealings - each time we purchase an item over the phone using a credit card, this is recorded by the credit card company. In time, even more of this kind of information may be collected and possibly sold. One Cypherpunk vision includes the ability to engage in transactions anonymously, using "digital cash", which would not be traceable to the participants. Particularly for buying "soft" products, like music, video, and software (which all may be deliverable over the net eventually), it should be possible to engage in such transactions

- anonymously. So this is another area where anonymous mail is important." [Hal Finney, 1993-02-23]
- 8.6.6. "How do I actually use a remailer?"
- + (Note: Remailer instructions are posted frequently. There is no way I can keep up to date with them here. Consult the various mailing lists and finger sites, or use the Web docs, to find the most current instructions, keys, uptimes, etc.)
 - + Raph Levien's finger site is very impressive:
 - + Raph Levien has an impressive utility which pings the remailers and reports uptime:
 - finger remailer-list@kiwi.cs.berkeley.edu
 - or use the Web at <http://www.cs.berkeley.edu/~raph/remailer-list.html>
 - Raph Levien also has a remailer chaining script at <ftp://kiwi.cs.berkeley.edu/pub/raph/premail-0.20.tar.gz>
 - + Keys for remailers
 - remailer-list@chaos.bsu.edu (Matthew Ghio maintains)
 - + "Why do remailers only operate on headers and not the body of a message? Why aren't signatures stripped off by remailers?"
 - "The reason to build mailers that faithfully pass on the entire body of the message, without any kind of alteration, is that it permits you to send ANY body through that mailer and rely on its faithful arrival at the destination." [John Gilmore, 93-01-01]
 - The "::-" special form is an exception
 - Signature blocks at the end of message bodies specifically should not be stripped, even though this can cause security breaches if they are accidentally left in when not intended. Attempting to strip sigs, which come in many flavors, would be a nightmare and could strip other stuff, too. Besides, some people may want a sig attached, even to an encrypted message.
 - As usual, anyone is of course free to have a remailer which munges message bodies as it sees fit, but I expect such remailers will lose customers.
 - Another possibility is another special form, such as "::-End", that could be used to delimit the block to be remailed. But it'll be hard getting such a "frill" accepted.
 - + "How do remailers handle subject lines?"
 - In various ways. Some ignore it, some preserve it, some even can accept instructions to create a new subject line (perhaps in the last remailer).
 - There are reasons not to have a subject line propagated through a chain of remailers: it tags the message and hence makes traffic analysis trivial. But there are also reasons to have a subject line--makes it easier on the recipient--and so these schemes to add a subject line exist.
 - + "Can nicknames or aliases be used with the Cypherpunks remailers?"
 - Certainly digitally signed IDs are used (Pr0duct Cypher,

for example), but not nicknames preserved in fields in the remailing and mail-to-Usenet gateways.

- This could perhaps be added to the remailers, as an extra field. (I've heard the mail fields are more tolerant of added stuff than the Netnews fields are, making mail-to-News gateways lose the extra fields.)
- + Some remailer sites support them
 - "If you want an alias assigned at vox.hacktic.nl, one - only- needs to send some empty mail to <ping@vox.hacktic.nl> and the address the mail was sent from will be included in the data-base.....Since vox.hacktic.nl is on a UUCP node the reply can take some time, usually something like 8 to 12 hours." [Alex de Joode, <usura@vox.hacktic.nl>, 1994-08-29]
- + "What do remailers do with the various portions of messages? Do they send stuff included after an encrypted block? Should they? What about headers?"
- + There are clearly lots of approaches that may be taken:
 - Send everything as is, leaving it up to the sender to ensure that nothing incriminating is left
 - Make certain choices
 - I favor sending everything, unless specifically told not to, as this makes fewer assumptions about the intended form of the message and thus allows more flexibility in designing new functions.
- + For example, this is what Matthew Ghio had to say about his remailer:
 - "Everything after the encrypted message gets passed along in the clear. If you don't want this, you can remove it using the cutmarks feature with my remailer. (Also, remail@extropia.wimsey.com doesn't append the text after the encrypted message.) The reason for this is that it allows anonymous replies. I can create a pgp message for a remailer which will be delivered to myself. I send you the PGP message, you append some text to it, and send it to the remailer. The remailer decrypts it and remails it to me, and I get your message. [M.G., alt.privacy.anon-server, 1994-07-03]

8.6.7. Remailer Sites

- There is no central administrator of sites, of course, so a variety of tools are the best ways to develop one's own list of sites. (Many of us, I suspect, simply settle on a dozen or so of our favorites. This will change as hundreds of remailers appear; of course, various scripting programs will be used to generate the trajectories, handled the nested encryption, etc.)
- The newsgroups alt.privacy.anon-server, alt.security.pgp, etc. often report on the latest sites, tools, etc.
- + Software for Remailers
 - + Software to run a remailer site can be found at:
 - soda.csua.berkeley.edu in /pub/cypherpunks/remailer/
 - chaos.bsu.edu in /pub/cypherpunks/remailer/
- + Instructions for Using Remailers and KeyServers
 - + on how to use keyServers
 - "If you have access to the World Wide Web, see this URL: <http://draco.centerline.com:8080/~franl/pgp/pgp-keyservers.html>" [Fran Litterio, alt.security.pgp, 1994-

09-02]

+ Identifying Remailer Sites

- + finger remailer-list@chaos.bsu.edu
 - returns a list of active remailers
 - for more complete information, keys, and instructions, finger remailer.help.all@chaos.bsu.edu
 - gopher://chaos.bsu.edu/
- + Raph Levien has an impressive utility which pings the remailers and reports uptime:
 - finger remailer-list@kiwi.cs.berkeley.edu
 - or use the Web at <http://www.cs.berkeley.edu/~raph/remailer-list.html>
 - Raph Levien also has a remailer chaining script at <ftp://kiwi.cs.berkeley.edu/pub/raph/premail-0.20.tar.gz>

+ Remailer pinging

- "I have written and installed a remailer pinging script which collects detailed information about remailer features and reliability.

To use it, just finger remailer-list@kiwi.cs.berkeley.edu

There is also a Web version of the same information, at:
<http://www.cs.berkeley.edu/~raph/remailer-list.html>
[Raph Levien, 1994-08-29]

+ Sites which are down??

- tamsun.tamu.edu and tamaix.tamu.edu

8.6.8. "How do I set up a remailer at my site?"

- This is not something for the casual user, but is certainly possible.
- "Would someone be able to help me install the remailer scripts from the archives? I have no Unix experience and have *no* idea where to begin. I don't even know if root access is needed for these. Any help would be appreciated." [Robert Luscombe, 93-04-28]
- Sameer Parekh, Matthew Ghio, Raph Levien have all written instructions....

8.6.9. "How are most Cypherpunks remailers written, and with what tools?"

- as scripts which manipulate the mail files, replacing headers, etc.
- Perl, C, TCL
- "The cypherpunks remailers have been written in Perl, which facilitates experimenting and testing of new interfaces. The idea might be to migrate them to C eventually for efficiency, but during this experimental phase we may want to try out new ideas, and it's easier to modify a Perl script than a C program." [Hal Finney, 93-01-09]
- "I do appreciate the cypherpunks stuff, but perl is still not a very widely used standard tool, and not everyone of us want to learn the ins and outs of yet another language... So I do applaud the C version..." [Johan Helsingius, "Julf," 93-01-09]

8.6.10. Dealing with Remailer Abuse

- + The Hot Potato
 - a remailer who is being used very heavily, or suspects abuse, may choose to distribute his load to other remailers. Generally, he can instead of remailing to the next site, add sites of his own choosing. Thus, he can both reduce the spotlight on him and also increase cover traffic by scattering some percentage of his traffic to other sites (it never reduces his traffic, just lessens the focus on him).
- + Flooding attacks
 - denial of service attacks
 - like blowing whistles at sports events, to confuse the action
 - DC-Nets, disruption (disruption of DC-Nets by flooding is a very similar problem to disruption of remailers by mail bombs)
- + "How can remailers deal with abuse?"
 - Several remailer operators have shut down their remailers, either because they got tired of dealing with the problems, or because others ordered them to.
 - Source level blocking
 - Paid messages: at least this makes the abusers pay and stops certain kinds of spamming/bombing attacks.
 - Disrupters are dealt with in anonymous ways in Chaum's DC-Net schemes; there may be a way to use this here.
- + Karl Kleinpaste was a pioneer (circa 1991-2) of remailers. He has become disenchanted:
 - "There are 3 sites out there which have my software: anon.penet.fi, tygra, and uiuc.edu. I have philosophical disagreement with the "universal reach" policy of anon.penet.fi (whose code is now a long-detached strain from the original software I gave Julf -- indeed, by now it may be a complete rewrite, I simply don't know); ...Very bluntly, having tried to run anon servers twice, and having had both go down due to actual legal difficulties, I don't trust people with them any more." [Karl_Kleinpaste@cs.cmu.edu, alt.privacy.anon-server, 1994-08-29]
 - see discussions in alt.privacy.anon-server for more on his legal problems with remailers, and why he shut his down

8.6.11. Generations of Remailers

- + First Generation Remailer Characteristics--Now (since 1992)
 - Perl scripts, simple processing of headers, crypto
- + Second Generation Remailer Characteristics--Maybe 1994
 - digital postage of some form (perhaps simple coupons or "stamps")
 - more flexible handling of exceptions
 - mail objects can tell remailer what settings to use (delays, latency, etc.)
- + Third Generation Remailer Characteristics--1995-7?
 - protocol negotiation
- + Chaum-like "mix" characteristics
 - tamper-resistant modules (remailer software runs in a sealed environment, not visible to operator)
- + Fourth Generation Remailer Characteristics--1996-9?
 - Who knows?

- Agent-based (Telescript?)
 - DC-Net-based
- 8.6.12. Remailer identity escrow
- + could have some uses...
 - what incentives would anyone have?
 - recipients could source-block any remailer that did not have some means of coping with serious abuse...a perfect free market solution
 - could also be mandated
- 8.6.13. Remailer Features
- + There are dozens of proposed variations, tricks, and methods which may or may not add to overall remailer security (entropy, confusion). These are often discussed on the list, one at a time. Some of them are:
 - + Using one's self as a remailer node. Route traffic back through one's own system.
 - even if all other systems are compromised...
 - Random delays, over and above what is needed to meet reordering requirements
 - MIRVing, sending a packet out in multiple pieces
 - Encryption is of course a primary feature.
 - + Digital postage.
 - Not so much a feature as an incentive/inducement to get more remailers and support them better.
 - + "What are features of a remailer network?"
 - A vast number of features have been considered; some are derivative of other, more basic features (e.g., "random delays" is not a basic feature, but is one proposed way of achieving "reordering," which is what is really needed. And "reordering" is just the way to achieve "decorrelation" of incoming and outgoing messages).
 - + The "Ideal Mix" is worth considering, just as the "ideal op amp" is studied by engineers, regardless of whether one can ever be built.
 - a black box that decorrelates incoming and outgoing packets to some level of diffusion
 - tamper-proof, in that outside world cannot see the internal process of decorrelation (Chaum envisioned tamper-resistant or tamper-responding circuits doing the decorrelation)
 - + Features of Real-World Mixes:
 - + Decorrelation of incoming and outgoing messages. This is the most basic feature of any mix or remailer: obscuring the relationship between any message entering the mix and any message leaving the mix. How this is achieved is what most of the features here are all about.
 - "Diffusion" is achieved by batching or delaying (danger: low-volume traffic defeats simple, fixed delays)
 - For example, in some time period, 20 messages enter a node. Then 20 or so (could be less, could be more...there is no reason not to add messages, or throw away some) messages leave.
 - + Encryption should be supported, else the decorrelation is easily defeated by simple inspection of packets.
 - public key encryption, clearly, is preferred (else

- the keys are available outside)
 - forward encryption, using D-H approaches, is a useful idea to explore, with keys discarded after transmission....thus making subpoenas problematic (this has been used with secure phones, for example).
- + Quantized packet sizes. Obviously the size of a packet (e.g., 3137 bytes) is a strong cue as to message identity. Quantizing to a fixed size destroys this cue.
- + But since some messages may be small, and some large, a practical compromise is perhaps to quantize to one of several standards:
 - small messages, e.g., 5K
 - medium messages, e.g., 20K
 - large messages....handled somehow (perhaps split up, etc.)
 - More analysis is needed.
- + Reputation and Service
 - How long in business?
 - Logging policy? Are messages logged?
 - the expectation of operating as stated
- + The Basic Goals of Remailer Use
 - + decorrelation of ingoing and outgoing messages
 - indistinguishability
 - + "remailed messages have no hair" (apologies to the black hole fans out there)
 - no distinguishing characteristics that can be used to make correlations
 - no "memory" of previous appearance
 - + this means message size padding to quantized sizes, typically
 - how many distinct sizes depends on a lot fo things, like traffic, the sizes of other messages, etc.
- + Encryption, of course
 - PGP
 - otherwise, messages are trivially distinguishable
- + Quantization or Padding: Messages
 - padded to standard sizes, or dithered in size to obscure original size. For example, 2K for typical short messages, 5K for typical Usenet articles, and 20K for long articles. (Messages much longer are hard to hide in a sea of much shorter messages, but other possibilities exist: delaying the long messages until N other long messages have been accumulated, splitting the messages into smaller chunks, etc.)
- + "What are the quanta for remailers? That is, what are the preferred packet sizes for remailed messages?"
 - In the short term, now, the remailed packet sizes are pretty much what they started out to be, e.g, 3-6KB or so. Some remailers can pad to quantized levels, e.g., to 5K or 10K or more. The levels have not been settled on.
 - In the long term, I suspect much smaller packets will be selected. Perhaps at the granularity of ATM packets. "ATM Remailers" are likely to be coming. (This changes the nature of traffic analysis a bit, as the number of remailed packets increases.
 - A dissenting argument: ATM networks don't give sender

- the control over packets...
 - Whatever, I think packets will get smaller, not larger. Interesting issues.
 - "Based on Hal's numbers, I would suggest a reasonable quantization for message sizes be a short set of geometrically increasing values, namely, 1K, 4K, 16K, 64K. In retrospect, this seems like the obvious quantization, and not arithmetic progressions." [Eric Hughes, 1994-08-29]
 - (Eudora chokes at 32K, and so splits messages at about 25K, to leave room for comments without further splitting. Such practical considerations may be important to consider.)
- + Return Mail
 - A complicated issue. May have no simple solution.
 - + Approaches:
 - Post encrypted message to a pool. Sender (who provided the key to use) is able to retrieve anonymously by the nature of pools and/or public posting.
 - + Return envelopes, using some kind of procedure to ensure anonymity. Since software is by nature never secure (can always be taken apart), the issues are complicated. The security may be gotten by arranging with the remailers in the return path to do certain things to certain messages.
 - sender sends instructions to remailers on how to treat messages of certain types
 - the recipient who is replying cannot deduce the identity, because he has no access to the instructions the remailers have.
 - Think of this as Alice sending to Bob sending to Charles....sending to Zeke. Zeke sends a reply back to Yancy, who has instructions to send this back to Xavier, and so on back up the chain. Only if Bob, Charles, ..., Yancy collude, can the mapping in the reverse direction be deduced.
 - Are these schemes complicated? Yes. But so are lot of other protocols, such as getting fonts from a screen to a laser printer
- + Reordering of Messages is Crucial
 - + latency or fanout in remailers
 - + much more important than "delay"
 - do some calculations!
 - + the canard about "latency" or delay keeps coming up
 - a "delay" of X is neither necessary nor sufficient to achieve reordering (think about it)
 - essential for removing time correlation information, for removing a "distinguishing mark" ("ideal remailed messages have no hair")
 - + The importance of pay as you go, digital postage
 - + standard market issues
 - markets are how scarce resources are allocated
 - reduces spamming, overloading, bombing
 - congestion pricing
 - incentives for improvement
 - + feedback mechanisms
 - in the same way the restaurants see impacts quickly

- applies to other crypto uses besides remailers
- + Miscellaneous
 - by having one's own nodes, further ensures security (true, the conspiring of all other nodes can cause traceability, but such a conspiracy is costly and would be revealed)
 - + the "public posting" idea is very attractive: at no point does the last node know who the next node will be...all he knows is a public key for that node
 - + so how does the next node in line get the message, short of reading all messages?
 - first, security is not much compromised by sorting the public postings by some kind of order set by the header (e.g., "Fred" is shorthand for some long P-K, and hence the recipient knows to look in the Fs...obviously he reads more than just the Fs)
 - + outgoing messages can be "broadcast" (sent to many nodes, either by a literal broadcast or public posting, or by randomly picking many nodes)
 - this "blackboard" system means no point to point communication is needed
 - + Timed-release strategies
 - + encrypt and then release the key later
 - "innocuously" (how?)
 - through a remailing service
 - DC-Net
 - via an escrow service or a lawyer (but can the lawyer get into hot water for releasing the key to controversial data?)
 - with a series of such releases, the key can be "diffused"
 - some companies may specialize in timed-release, such as by offering a P-K with the private key to be released some time later
 - in an ecology of cryptoid entities, this will increase the degrees of freedom
 - + this reduces the legal liability of retransmitters...they can accurately claim that they were only passing data, that there was no way they could know the content of the packets
 - of course they can already claim this, due to the encrypted nature
 - + One-Shot Remailers
 - "You can get an anonymous address from mg5n+getid@andrew.cmu.edu. Each time you request an anon address, you get a different one. You can get as many as you like. The addresses don't expire, however, so maybe it's not the ideal 'one-shot' system, but it allows replies without connecting you to your 'real name/address' or to any of your other posts/nyms." [Matthew Ghio, 1994-04-07]

8.6.14. Things Needed in Remailers

- + return receipts
 - Rick Busdiecker notes that "The idea of a Return-Receipt-To: field has been around for a while, but the semantics have never been pinned down. Some mailer daemons generate replies meaning that the bits were delivered."

[R.B., 1994-08-08]

- + special handling instructions
 - agents, daemons
 - negotiated procedures
 - + digital postage
 - of paramount importance!
 - solves many problems, and incentivizes remailers
 - + padding
 - + padding to fixed sizes
 - padding to fixed powers of 2 would increase the average message size by about a third
 - lots of remailers
 - multiple jurisdictions
 - robustness and consistency
 - + running in secure hardware
 - no logs
 - no monitoring by operator
 - wipe of all temp files
 - instantiated quickly, fluidly
 - better randomization of remailers
- 8.6.15. Miscellaneous Aspects of Remailers
- + "How many remailer nodes are actually needed?"
 - We strive to get as many as possible, to distribute the process to many jurisdictions and with many operators.
 - Curiously, as much theoretical diffusivity can occur with a single remailer (taking in a hundred messages and sending out a hundred, for example) as with many remailers. Our intuition is, I think, that many remailers offer better diffusivity and better hiding. Why this is so (if it is) needs more careful thinking than I've seen done so far.
 - At a meta-level, we think multiple remailers lessens the chance of them being compromised (this, however, is not directly related to the diffusivity of a remailer network-
-important, but not directly related).
 - (By the way, a kind of sneaky idea is to try to always declare one's self to be a remailer. If messages were somehow traced back to one's own machine, one could claim: 'Yes, I'm a remailer.'" In principle, one could be the only remailer in the universe and still have high enough diffusion and confusion. In practice, being the only remailer would be pretty dangerous.)
 - + Diffusion and confusion in remailer networks
 - + Consider a single node, with a message entering, and two messages leaving; this is essentially the smallest "remailer op"
 - From a proof point of view, either outgoing message could be the one
 - and yet neither one can be proved to be
 - Now imagine those two messages being sent through 10 remailers...no additional confusion is added...why?
 - So, with 10 messages gong into a chain of 10 remailers, if 10 leave...
 - The practical effect of N remailers is to ensure that compromise of some fraction of them doesn't destroy overall security
 - + "What do remailers do with misaddressed mail?"

- Depends on the site. Some operators send notes back (which itself causes concern), some just discard defective mail. This is a fluid area. At least one remailer (wimsey) can post error messages to a message pool--this idea can be generalized to provide "delivery receipts" and other feedback.
 - Ideal mixes, a la Chaum, would presumably discard improperly-formed mail, although agents might exist to prescreen mail (not mandatory agents, of course, but voluntarily-selected agents)
 - As in so many areas, legislation is not needed, just announcement of policies, choice by customers, and the reputation of the remailer.
 - A good reason to have robust generation of mail on one's own machine, so as to minimize such problems.
 - + "Can the NSA monitor remailers? Have they?"
 - + Certainly they can in various ways, either by directly monitoring Net traffic or indirectly. Whether they do is unknown.
 - There have been several rumors or forgeries claiming that NSA is routinely linking anonymous IDs to real IDs at the penet remailer.
 - + Cypherpunks remailers are, if used properly, more secure in key ways:
 - many of them
 - not used for persistent, assigned IDs
 - support for encryption: incoming and outgoing messages look completely unlike
 - batching, padding, etc. supported
 - And properly run remailers will obscure/diffuse the connection between incoming and outgoing messages--the main point of a remailer!
 - + The use of message pools to report remailer errors
 - A good example of how message pools can be used to anonymously report things.
 - "The wimsey remailer has an ingenious method of returning error messages anonymously. Specify a subject in the message sent to wimsey that will be meaningful to you, but won't identify you (like a set of random letters). This subject does not appear in the remailed message. Then subscribe to the mailing list

errors-request@extropia.wimsey.com

by sending a message with Subject: subscribe. You will receive a msg for ALL errors detected in incoming messages and ALL bounced messages." [anonymous, 93-08-23]
- This is of course like reading a classified ad with some cryptic message meaningful to you alone. And more importantly, untraceable to you.
- + there may be role for different types of remailers
 - those that support encryption, those that don't
 - + as many in non-U.S. countries as possible
 - especially for the *last* hop, to avoid subpoena issues
 - first-class remailers which remail to *any* address
 - + remailers which only remail to *other remailers*

- useful for the timid, for those with limited support, etc.
-
- + "Should mail faking be used as part of the remailer strategy?"
 - "1. If you fake mail by talking SMTP directly, the IP address or domain name of the site making the outgoing connection will appear in a Received field in the header somewhere."
 - "2. Fake mail by devious means is generally frowned upon. There's no need to take a back-door approach here--it's bad politically, as in Internet politics." [Eric Hughes, 94-01-31]
 - And if mail can really be consistently and robustly faked, there would be less need for remailers, right? (Actually, still a need, as traffic analysis would likely break any "Port 25" faking scheme.)
 - Furthermore, such a strategy would not likely to be robust over time, as it relies on exploiting transitory flaws and vendor specifics. A bad idea all around.
- + Difficulties in getting anonymous remailer networks widely deployed
 - "The tricky part is finding a way to preserve anonymity where the majority of sites on the Internet continue to log traffic carefully, refuse to install new software (especially anon-positive software), and are administrated by people with simplistic and outdated ideas about identity and punishment. " [Greg Broiles, 1994-08-08]
- + Remailer challenge: insulating the last leg on a chain from prosecution
 - + Strategy 1: Get them declared to be common carriers, like the phone company or a mail delivery service
 - + e.g., we don't prosecute an actual package delivery person, or even the company they work for, for delivery of an illegal package
 - contents assumed to be unknown to the carrier
 - (I've heard claims that only carriers who make other agreements to cooperate with law enforcement can be treated as common carriers.)
 - + Strategy 2: Message pools
 - + ftp sites
 - with plans for users to "subscribe to" all new messages (thus, monitoring agencies cannot know which, if any, messages are being sought)
 - this gets around the complaint about too much volume on the Usenet (text messages are a tiny fraction of other traffic, especially images, so the complaint is only one of potentiality)
 - + Strategy 3: Offshore remailers as last leg
 - probably set by sender, who presumably knows the destination
 - A large number of "secondary remailers" who agree to remail a limited number...
- + "Are we just playing around with remailers and such?"
 - It pains me to say this, but, yes, we are just basically

- playing around here!
- Remailer traffic is so low, padding is so haphazard, that making correlations between inputs and outputs is not cryptographically hard to do. (It might seem hard, with paper and pencil sorts of calculations, but it'll be child's play for the Crays at the Fort.)
- Even if this is not so for any particular message, maintaining a persistent ID--such as Pr0duct Cypher does, with digital sigs--without eventually providing enough clues will be almost impossible. At this time.
- Things will get better. Better and more detailed "cryptanalysis of remailer chains" is sorely needed. Until then, we are indeed just playing. (Play can be useful, though.)
- + The "don't give em any hints" principle (for remailers)
 - avoid giving any information
 - don't say which nodes are sources and which are sinks; let attackers assume everyone is a remailer, a source
 - don't say how long a password is
 - don't say how many rounds are in a tit-for-tat tournament

8.7. Anonymous Posting to Usenet

8.7.1. Julf's penet system has historically been the main way to post anonymously to Usenet (used by no less a luminary than L. Detweiler, in his "an12070/S. Boxx" persona). This has particularly been the case with postings to "support" groups, or emotional distress groups. For example, alt.sexual.abuse.recovery.

8.7.2. Cryptographically secure remails are now being used increasingly (and scaling laws and multiple jurisdictions suggest even more will be used in the future).

8.7.3. finger remailer.help.all@chaos.bsu.edu gives these results [as of 1994-09-07--get a current result before using!]

- "Anonymous postings to usenet can be made by sending anonymous mail to one of the following mail-to-usenet gateways:

```
group.name@demon.co.uk
group.name@news.demon.co.uk
group.name@bull.com
group.name@cass.ma02.bull.com
group.name@undergrad.math.uwaterloo.ca
group.name@charm.magnus.acs.ohio-state.edu
group.name@comlab.ox.ac.uk
group.name@nic.funet.fi
group.name@cs.dal.ca
group.name@ug.cs.dal.ca
group.name@paris.ics.uci.edu (removes headers)
group.name.usenet@decwrl.dec.com (Preserves all headers)"
```

8.8. Anonymous Message Pools, Newsgroups, etc.

8.8.1. "Why do some people use message pools?"

- Provides untracable communication
- messages
- secrets
- transactions

- + Pr0duct Cypher is a good example of someone who communicates primarily via anonymous pools (for messages to him). Someone recently asked about this, with this comment:
 - "Pr0duct Cypher chooses to not link his or her "real life" identity with the 'nym used to sign the software he or she wrote (PGP Tools, Magic Money, ?). This is quite an understandable sentiment, given that bad apples in the NSA are willing to go far beyond legal hassling, and make death threats against folks with high public visibility (see the threads about an NSA agent threatening to run Jim Bidzos of RSA over in his parking lot)." [Richard Johnson, alt.security.pgp, 1994-07-02]

8.8.2. alt.anonymous.messages is one such pool group

- though it's mainly used for test messages, discussions of anonymity (though there are better groups), etc.

8.8.3. "Could there be truly anonymous newsgroups?"

- One idea: newgroup a moderated group in which only messages sans headers and other identifiers would be accepted. The "moderator"--which could be a program--would only post messages after this was ensured. (Might be an interesting experiment.)

+ alt.anonymous.messages was newgrouped by Rick Busdiecker, 1994-08.

- Early uses were, predictably, by people who stumbled across the group and imputed to it whatever they wished.

8.9. Legal Issues with Remailers

8.9.1. What's the legal status of remailers?

- There are no laws against it at this time.
- No laws saying people have to put return addresses on messages, on phone calls (pay phones are still legal), etc.
- And the laws pertaining to not having to produce identity (the "flier" case, where leaflet distributors did not have to produce ID) would seem to apply to this form of communication.

+ However, remailers may come under fire:

+ Sysops, MIT case

- potentially serious for remailers if the case is decided such that the sysop's creation of group that was conducive to criminal pirating was itself a crime...that could make all involved in remailers culpable

8.9.2. "Can remailer logs be subpoenaed?"

- Count on it happening, perhaps very soon. The FBI has been subpoenaing e-mail archives for a Netcom customer (Lewis De Payne), probably because they think the e-mail will lead them to the location of uber-hacker Kevin Mitnick. Had the parties used remailers, I'm fairly sure we'd be seeing similar subpoenas for the remailer logs.
- There's no exemption for remailers that I know of!

+ The solutions are obvious, though:

- use many remailers, to make subpoenaing back through the chain very laborious, very expensive, and likely to fail (if even one party won't cooperate, or is outside the court's jurisdiction, etc.)
- offshore, multi-jurisdictional remailers (selected by the user)

- no remailer logs kept...destroy them (no law currently says anybody has to keep e-mail records! This may change....)
 - "forward secrecy," a la Diffie-Hellman forward secrecy
- 8.9.3. How will remailers be harassed, attacked, and challenged?
- 8.9.4. "Can pressure be put on remailer operators to reveal traffic logs and thereby allow tracing of messages?"
- + For human-operated systems which have logs, sure. This is why we want several things in remailers:
 - * no logs of messages
 - * many remailers
 - * multiple legal jurisdictions, e.g., offshore remailers (the more the better)
 - * hardware implementations which execute instructions flawlessly (Chaum's digital mix)
- 8.9.5. Calls for limits on anonymity
- + Kids and the net will cause many to call for limits on nets, on anonymity, etc.
 - "But there's a dark side to this exciting phenomenon, one that's too rarely understood by computer novices. Because they offer instant access to others, and considerable anonymity to participants, the services make it possible for people - especially computer-literate kids - to find themselves in unpleasant, sexually explicit social situations.... And I've gradually come to adopt the view, which will be controversial among many online users, that the use of nicknames and other forms of anonymity must be eliminated or severely curbed to force people online into at least as much accountability for their words and actions as exists in real social encounters." [Walter S. Mossberg, Wall Street Journal, 6/30/94, provided by Brad Dolan]
 - Eli Brandt came up with a good response to this: "The sound-bite response to this: do you want your child's name, home address, and phone number available to all those lurking pedophiles worldwide? Responsible parents encourage their children to use remailers."
 - Supreme Court said that identity of handbill distributors need not be disclosed, and pseudonyms in general has a long and noble tradition
 - BBS operators have First Amendment protections (e.g.. registration requirements would be tossed out, exactly as if registration of newspapers were to be attempted)
- 8.9.6. Remailers and Choice of Jurisdictions
- The intended target of a remailed message, and the subject material, may well influence the set of remailers used, especially for the very important "last remailer" (Note: it should never be necessary to tell remailers if they are first, last, or others, but the last remailer may in fact be able to tell he's the last...if the message is in plaintext to the recipient, with no additional remailer commands embedded, for example.)

- A message involving child pornography might have a remailer site located in a state like Denmark, where child porn laws are less restrictive. And a message critical of Islam might not be best sent through a final remailer in Teheran. Eric Hughes has dubbed this "regulatory arbitrage," and to various extents it is already common practice.
- Of course, the sender picks the remailer chain, so these common sense notions may not be followed. Nothing is perfect, and customs will evolve. I can imagine schemes developing for choosing customers--a remailer might not accept as a customer certain abusers, based on digital pseudonyms < hairy).

8.9.7. Possible legal steps to limit the use of remailers and anonymous systems

- hold the remailer liable for content, i.e., no common carrier status
- insert provisions into the various "anti-hacking" laws to criminalize anonymous posts

8.9.8. Crypto and remailers can be used to protect groups from "deep pockets" lawsuits

- products (esp. software) can be sold "as is," or with contracts backed up by escrow services (code kept in an escrow repository, or money kept there to back up commitments)
- + jurisdictions, legal and tax, cannot do "reach backs" which expose the groups to more than they agreed to
 - as is so often the case with corporations in the real world, which are taxed and fined for various purposes (asbestos, etc.)
 - (For those who panic at the thought of this, the remedy for the cautious will be to arrange contracts with the right entities...probably paying more for less product.)

8.9.9. Could anonymous remailers be used to entrap people, or to gather information for investigations?

- First, there are so few current remailers that this is unlikely. Julf seems a non-narc type, and he is located in Finland. The Cypherpunks remailers are mostly run by folks like us, for now.
- However, such stings and set-ups have been used in the past by narcs and "red squads." Expect the worse from Mr. Policeman. Now that evilhackers are identified as hazards, expect moves in this direction. "Cryps" are obviously "crack" dealers.
- But use of encryption, which CP remailers support (Julf's does not), makes this essentially moot.

8.10. Cryptanalysis of Remailer Networks

8.10.1. The Need for More Detailed Analysis of Mixes and Remailers

- + "Have remailer systems been adequately cryptanalyzed?"
 - Not in my opinion, no. Few calculations have been done, just mostly some estimates about how much "confusion" has been created by the remailer nodes.
 - But thinking that a lot of complication and messiness makes a strong crypto system is a basic mistake...sort of like thinking an Enigma rotor machine makes a good cipher system, by today's standards, just because millions of combinations of pathways through the rotor system are

possible. Not so.

- + Deducing Patterns in Traffic and Deducing Nyms
 - The main lesson of mathematical cryptology has been that seemingly random things can actually be shown to have structure. This is what cryptanalysis is all about.
 - The same situation applies to "seemingly random" message traffic, in digital mixes, telephone networks, etc. "Cryptanalysis of remailers" is of course possible, depending on the underlying model. (Actually, it's always possible, it just may not yield anything, as with cryptanalysis of ciphers.)
- + on the time correlation in remailer cryptanalysis
 - imagine Alice and Bob communicating through remailers...an observer, unable to follow specific messages through the remailers, could still notice pairwise correlations between messages sent and received by these two
 - + like time correlations between events, even if the intervening path or events are jumbled
 - e.g., if within a few hours of every submarine's departure from Holy Loch a call is placed to Moscow, one may make draw certain conclusions about who is a Russian spy, regardless of not knowing the intermediate paths
 - or, closer to home, correlating withdrawals from one bank to deposits in another, even if the intervening transfers are jumbled
 - + just because it seems "random" does not mean it is
 - Scott Collins speculates that a "dynamic Markov compressor" could discern or uncover the non-randomness in remailer uses
- Cryptanalysis of remailers has been woefully lacking. A huge fraction of posts about remailer improvements make hand-waving arguments about the need for more traffic, longer delays, etc. (I'm not pointing fingers, as I make the same informal, qualitative comments, too. What is needed is a rigorous analysis of remailer security.)
- We really don't have any good estimates of overall security as a function of number of messages circulating, the latency (number of stored messages before resending), the number of remailer hops, etc. This is not cryptographically "exciting" work, but it's still needed. There has not been much focus in the academic community on digital mixes or remailers, probably because David Chaum's 1981 paper on "Untraceable E-Mail" covered most of the theoretically interesting material. That, and the lack of commercial products or wide usage.
- + Time correlations may reveal patterns that individual messages lack. That is, repeated communication between Alice and Bob, even if done through remailers and even if time delays/dwell times are built-in, may reveal nonrandom correlations in sent/received messages.
 - Scott Collins speculates that a dynamic Markov compressor applied to the traffic would have reveal such correlations. (The application of such tests to digital cash and other such systems would be useful to look at.)
 - Another often overlooked weakness is that many people

send test messages to themselves, a point noted by Phil Karn: "Another way that people often let themselves be caught is that they inevitably send a test message to themselves right before the forged message in question. This shows up clearly in the sending system's sendmail logs. It's a point to consider with remailer chains too, if you don't trust the last machine on the chain." [P.K., 1994-09-06]

+ What's needed:

- agreement on some terminology (this doesn't require consensus, just a clearly written paper to de facto establish the terminology)
- a formula relating degree of untraceability to the major factors that go into remailers: packet size and quantization, latency (# of messages), remailer policies, timing, etc.
- Also, analysis of how deliberate probes or attacks might be mounted to deduce remailer patterns (e.g., Fred always remails to Josh and Suzy and rarely to Zeke).
- I think this combinatorial analysis would be a nice little monograph for someone to write.

8.10.2. A much-needed thing. Hal Finney has posted some calculations (circa 1994-08-08), but more work is sorely needed.

8.10.3. In particular, we should be skeptical of hand-waving analyses of the "it sure looks complicated to follow the traffic" sort. People think that by adding "messy" tricks, such as MIRVing messages, that security is increased. Maybe it is, maybe it isn't. But it needs formal analysis before claims can be confidently believed.

8.10.4. Remailers and entropy

- What's the measure of "mixing" that goes on in a mix, or remailer?
 - Hand-waving about entropy and reordering may not be too useful.
- + Going back to Shannon's concept of entropy as measuring the degree of uncertainty...
- + trying to "guess" or "predict" where a message leaving one node will exit the system
 - not having clear entrance and exit points adds to the difficulty, somewhat analogously to having a password of unknown length (an attacker can't just try all 10-character passwords, as he has no idea of the length)
 - the advantages of every node being a remailer, of having no clearly identified sources and sinks
- + This predictability may depend on a series of messages sent between Alice and Bob...how?
- it seems there may be links to Persi Diaconis' work on "perfect shuffles" (a problem which seemed easy, but which eluded solving until recently...should give us comfort that our inability to tackle the real meat of this issue is not too surprising)

8.10.5. Scott Collins believes that remailer networks can be cryptanalyzed roughly the same way as pseudorandom number generators are analyzed, e.g., with dynamic Markov compressors (DNCs). (I'm more skeptical: if each remailer is using an information-theoretically secure RNG to reorder the messages, and if all messages are the same size and (of

course) are encrypted with information-theoretically secure (OTP) ciphers, then it seems to me that the remaining would itself be information-theoretically secure.)

8.11. Dining Cryptographers

8.11.1. This is effectively the "ideal digital mix," updated from Chaum's original hardware mix form to a purely software-based form.

8.11.2. David Chaum's 1988 paper in Journal of Cryptology (Vol 1, No 1) outlines a way for completely untraceable communication using only software (no tamper-resistant modules needed)

- participants in a ring (hence "dining cryptographers")
- Chaum imagines that 3 cryptographers are having dinner and are informed by their waiter that their dinner has already been paid for, perhaps by the NSA, or perhaps by one of themselves...they wish to determine which of these is true, without revealing which of them paid!
- everyone flips a coin (H or T) and shows it to his neighbor on the left
- + everyone reports whether he sees "same" or "different"
 - note that with 2 participants, they both already know the other's coin (both are to the left!)
- however, someone wishing to send a message, such as Chaum's example of "I paid for dinner," instead says the opposite of what he sees
- + some analysis of this (analyze it from the point of view of one of the cryptographers) shows that the 3 cryptographers will know that one of them paid (if this protocol is executed faithfully), but that the identity can't be "localized"
 - a diagram is needed...
- + this can be generalized...
 - + longer messages
 - use multiple rounds of the protocol
 - + faster than coin-flipping
 - each participant and his left partner share a list of "pre-flipped" coins, such as truly random bits (radioactive decay, noise, etc.) stored on a CD-ROM or whatever
 - they can thus "flip coins" as fast as they can read the disk
 - + simultaneous messages (collision)
 - use back-off and retry protocols (like Ethernet uses)
 - + collusion of participants
 - an interesting issue...remember that participants are not restricted to the simple ring topology
 - various subgraphs can be formed
 - a participant who fears collusion can pick a subgraph that includes those he doubts will collude (a tricky issue)
 - + anonymity of receiver
 - can use P-K to encrypt message to some P-K and then "broadcast" it and force every participant to try to decrypt it (only the anonymous recipient will actually succeed)
- Chaum's complete 1988 "Journal of Cryptology" article is available at the Cypherpunks archive site,

ftp.soda.csua.edu, in /pub/cypherpunks

8.11.3. What "DC-Net" Means

- a system (graph, subgraphs, etc.) of communicating participants, who need not be known to each other, can communicate information such that neither the sender nor the recipient is known
- + unconditional sender untraceability
 - the anonymity of the broadcaster can be information-theoretically secure, i.e., truly impossible to break and requiring no assumptions about public key systems, the difficulty of factoring, etc.
- + receiver untraceability depends on public-key protocols, so traceability is computationally-dependent
 - but this is believed to be secure, of course
- + bandwidth can be increased by several means
 - shared keys
 - block transmission by accumulating messages
 - hierarchies of messages, subgraphs, etc.

8.12. Future Remailers

8.12.1. "What are the needed features for the Next Generation Remailer?"

- + Some goals
 - generally, closer to the goals outlined in Chaum's 1981 paper on "Untraceable E-Mail"
 - Anonymity
 - Digital Postage, pay as you go, ,market pricing
 - Traffic Analysis foiled
- + Bulletproof Sites:
 - Having offshore (out of the U.S.) sites is nice, but having sites resistant to pressures from universities and corporate site administrators is of even greater practical consequence. The commercial providers, like Netcom, Portal, and Panix, cannot be counted on to stand and fight should pressures mount (this is just my guess, not an aspersion against their backbones, whether organic or Internet).
 - Locating remailers in many non-U.S. countries is a Good Idea. As with money-laundering, lots of countries means lots of jurisdictions, and the near impossibility of control by one country.
- + Digital Postage, or Pay-as-you-Go Services:
 - Some fee for the service. Just like phone service, modem time, real postage, etc. (But unlike highway driving, whose usage is largely subsidized.)
 - This will reduce spamming, will incentivize remailer services to better maintain their systems, and will
 - Rates would be set by market process, in the usual way. "What the traffic will bear." Discounts, favored customers, rebates, coupons, etc. Those that don't wish to charge, don't have to (they'll have to deal with the problems).
- + Generations
 - 1st Gen--Today's Remailer:
 - 2nd Gen--Near Future (c. 1995)
 - 3rd Gen-
 - 4th Gen--

8.12.2. Remailing as a side effect of mail filtering

- Dean Tribble has proposed...
- "It sounds like the plan is to provide a convenient mail filtering tool which provides remailer capability as a SIDE EFFECT! What a great way to spread remailers!" [Hal Finney, 93-01-03]

8.12.3. "Are there any remailers which provide you with an anonymous account to which other people may send messages, which are then forwarded to you in a PGP-encrypted form?" [Mikolaj Habryn, 94-04]

- "Yes, but it's not running for real yet. Give me a few months until I get the computer + netlink for it. (It's running for testing though, so if you want to test it, mail me, but it's not running for real, so don't *use* it.)" [Sameer Parekh, 94-04-03]

8.12.4. "Remailer Alliances"

- + "Remailer's Guild"
 - to make there be a cost to flakiness (expulsion) and a benefit to robustness, quality, reliability, etc. (increased business)
 - pings, tests, cooperative remailing
 - spreading the traffic to reduce effectiveness of attacks
- which execute protocols
- e.g., to share the traffic at the last hop, to reduce attacks on any single remailer

8.13. Loose Ends

8.13.1. Digital espionage

- + spy networks can be run safely, untraceably, undetectably
 - anonymous contacts, pseudonyms
 - digital dead drops, all done electronically...no chance of being picked up, revealed as an "illegal" (a spy with no diplomatic cover to save him) and shot
- + so many degrees of freedom in communications that controlling all of them is essentially impossible
 - Teledesic/Iridium/etc. satellites will increase this capability further
- + unless crypto is blocked--and relatively quickly and ruthlessly--the situation described here is unstoppable
 - what some call "espionage" others would just call free communication
 - (Some important lessons for keeping corporate or business secrets...basically, you can't.)

8.13.2. Remailers needs some "fuzziness," probably

- + for example, if a remailer has a strict policy of accumulating N messages, then reordering and remailing them, an attacker can send N - 1 messages in and know which of the N messages leaving is the message they want to follow; some uncertainty helps here
 - the mathematics of how this small amount of uncertainty, or scatter, could help is something that needs a detailed analysis
- it may be that leaving some uncertainty, as with the keylength issue, can help

8.13.3. Trying to confuse the eavesdroppers, by adding keywords they will probably pick up on

- + the "remailer@csua.berkeley.edu" remailer now adds actual

paragraphs, such as this recent example:

- "I fixed the SKS. It came with a scope and a Russian night scope. It's killer. My friend knows about a really good gunsmith who has a machinshop and knows how to convert stuff to automatic."

- How effective this ploy is is debatable

8.13.4. Restrictions on anonymous systems

- Anonymous AIDS testing. Kits for self-testing have been under FDA review for 5 years, but counseling advocates have delayed release on the grounds that some people will react badly and perhaps kill themselves upon getting a positive test result...they want the existing system to prevail. (I mention this to show that anonymous systems are sometimes opposed for ideological reasons.)

9. Policy: Clipper, Key Escrow, and Digital Telephony

9.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

9.2. SUMMARY: Policy: Clipper, Key Escrow, and Digital Telephony

9.2.1. Main Points

- Clipper has been a main unifying force, as 80% of all Americans, and 95% of all computer types, are opposed.
- "Big Brother Inside"

9.2.2. Connections to Other Sections

- the main connections are legal
- some possible implications for limits on crypto

9.2.3. Where to Find Additional Information

- There have been hundreds of articles on Clipper, in nearly all popular magazines. Many of these were sent to the Cypherpunks list and may be available in the archives. (I have at least 80 MB of Cypherpunks list stuff, a lot of it newspaper and magazine articles on Clipper!)

+ more Clipper information can be found at:

- "A good source is the Wired Online Clipper Archive. Send e-mail to info-rama@wired.com. with no subject and the words 'get help' and 'get clipper/index' in the body of the message." [students@unsw.EDU.AU, alt.privacy.clipper, 1994-09-01]

9.2.4. Miscellaneous Comments

- As with a couple of other sections, I won't try to be as complete as some might desire. Just too many thousands of pages of stuff to consider.

9.3. Introduction

9.3.1. What is Clipper?

- government holds the skeleton keys
- analogies to other systems

9.3.2. Why do most Cypherpunks oppose Clipper?

- fear of restrictions on crypto, derailing so many wonderful possibilities

9.3.3. Why does Clipper rate its own section?

- The announcement of the "Escrowed Encryption Standard," EES, on April 16, 1993, was a galvanizing event for Cypherpunks and for a large segment of the U. S. population. The EES was announced originally as "Clipper," despite the use of the name Clipper by two major products (the Intergraph CPU and a dBase software tool), and the government backed off on the name. Too late, though, as the name "Clipper" had become indelibly linked to this whole proposal.

9.3.4. "Is stopping Clipper the main goal of Cypherpunks?"

- It certainly seems so at times, as Clipper has dominated the topics since the Clipper announcement in April, 1993.
- + it has become so, with monkeywrenching efforts in several areas
 - lobbying and education against it (though informal, such lobbying has been successful...look at NYT article)
 - "Big Brother Inside" and t-shirts
 - technical monkeywrenching (Matt Blaze...hesitate to claim any credit, but he has been on our list, attended a meeting, etc.)
- Although it may seem so, Clipper is just one aspect...step...initiative.
- Developing new software tools, writing code, deploying remailers and digital cash are long-range projects of great importance.
- The Clipper key escrow proposal came along (4-93) at an opportune time for Cypherpunks and became a major focus. Emergency meetings, analyses, etc.

9.4. Crypto Policy Issues

9.4.1. Peter Denning on crypto policy:

- + provided by Pat Farrell, 1994-08-20; Denning comments are 1992-01-22, presented at Computers, Freedom, and Privacy 2. Peter D. uses the metaphor of a "clearing," as in a forest, for the place where people meet to trade, interact, etc. What others call markets, agoras, or just "cyberspace."
- "Information technology in producing a clearing in which individuals and corporations are key players besides government. Any attempt by government to control the flow of information over networks will be ignored or met with outright hostility. There is no practical way that government can control information except information directly involved in the business of governing. It should not try." [Peter Denning, PUBLIC POLICY FOR THE 21ST CENTURY, DRAFT 1/22/92]
- No word on how this view squares with his wife's control freak views.

9.4.2. Will government and NSA in particular attempt to acquire some kind of control over crypto companies?

- + speculations, apparently unfounded, that RSA Data Security is influenced by NSA wishes
 - weaknesses in the DES keys picked?
- and companies may be dramatically influenced by contracts (and the withholding of them)

9.4.3. NIST and DSS

9.4.4. Export restrictions, Munitions List, ITAR

9.4.5. old crypto machines sold to Third World governments, cheaply
- perhaps they think they can make some changes and outsmart
the NSA (which probably has rigged it so any changes are
detectable and can be factored in)

- and just knowing the type of machine is a huge advantage

9.4.6. 4/28/97 The first of several P-K and RSA patents expires

+ U.S. Patent Number: 4200770

- Title: Cryptographic Apparatus and Method

- Inventors: Hellman, Diffie, Merkle

- Assignee: Stanford University

- Filed: September 6, 1977

- Granted: April 29, 1980

- [Expires: April 28, 1997]

+ remember that any one of these several patents held by
Public Key Partners (Stanford and M.I.T., with RSA Data
Security the chief dispenser of licenses) can block an
effort to bypass the others

- though this may get fought out in court

9.4.7. encryption will be needed inside computer systems

- for operating system protection

- for autonomous agents (active agents)

- for electronic money

9.5. Motivations for Crypto Laws

9.5.1. "What are the law enforcement and FBI worries?"

- "FBI Director Louis Freeh is worried. The bad guys are
beginning to see the light, and it is digital. ... Freeh
fears some pretty nasty folks have discovered they can
commit highway robbery and more, without even leaving home.
Worse, to Freeh and other top cops, by using some pretty
basic technologies, savvy criminals can do their crimes
without worrying about doing time.

"Some crooks, spies, drug traffickers, terrorists and
frauds already use the tools of the information age to
outfox law enforcement officers. Hackers use PBXs to hide
their tracks as they rip off phone companies and poke
around in other people's files. Reprogrammed cellular
phones give cops fits." [LAN Magazine, "Is it 1984?," by Ted
Bunker, August 1994]

- Their fears have some validity...in the same way that the
rulers in Gutenberg's time could have some concerns about
the implications of books (breaking of guilds, spread of
national secrets, pornography, atheism, etc.).

9.5.2. "What motivated Clipper? What did the Feds hope to gain?"

- ostensibly to stop terrorists (only the unsophisticated
ones, if alternatives are allowed)

- to force a standard on average Americans

- possibly to limit crypto development

+ Phil Karn provides an interesting motivation for Clipper:

"Key escrow exists only because the NSA doesn't want to
risk blame if some terrorist or drug dealer were to use an
unescrowed NSA-producedThe fact that a terrorist or
drug dealer can easily go elsewhere and obtain other strong
or stronger algorithms without key escrow is irrelevant.
The NSA simply doesn't care as long as *they* can't be
blamed for whatever happens. Classic CYA, nothing

more.....A similar analysis applies to the export control regulations regarding cryptography." [Phil Karn, 1994-08-31]

- Bill Sommerfeld notes: "If this is indeed the case, Matt Blaze's results should be particularly devastating to them." [B.S., 1994-09-01]

9.5.3. Steve Witham has an interesting take on why folks like Dorothy Denning and Donn Parker support key escrow so ardently:

- "Maybe people like Dot and Don think of government as a systems-administration sort of job. So here they are, security experts advising the sys admins on things like...

setting permissions
allocating quotas
registering users and giving them passwords.....
deciding what utilities are and aren't available
deciding what software the users need, and installing it
(grudgingly, based on who's yelling the loudest)
setting up connections to other machines
deciding who's allowed to log in from "foreign hosts"
getting mail set up and running
buying new hardware from vendors
specifying the hardware to the vendors
...

"These are the things computer security experts advise on. Maybe hammer experts see things as nails.

"Only a country is not a host system owned and administered by the government, and citizens are not guests or users."
[Steve Witham, Government by Sysadmin, 1994-03-23]

9.5.4. Who would want to use key escrow?

9.5.5. "Will strong crypto really thwart government plans?"

- Yes, it will give citizens the basic capabilities that foreign governments have had for many years
- + Despite talk about codebreakers and the expertise of the NSA, the plain fact is that no major Soviet ciphers have been broken for many years
- + recall the comment that NSA has not really broken any Soviet systems in many years
 - except for the cases, a la the Walker case, where plaintext versions are gotten, i.e., where human screwups occurred
- the image in so many novels of massive computers breaking codes is absurd: modern ciphers will not be broken (but the primitive ciphers used by so many Third World nations and their embassies will continue to be child's play, even for high school science fair projects...could be a good idea for a small scene, about a BCC student who has his project pulled)

9.5.6. "Why does the government want short keys?"

- Commercial products have often been broken by hackers. The NSA actually has a charter to help businesses protect their secrets; just not so strongly that the crypto is unbreakable by them. (This of course has been part of the

tension between the two sides of the NSA for the past couple of decades.)

- + So why does the government want crippled key lengths?
 - "The question is: how do you thwart hackers while permitting NSA access? The obvious answer is strong algorithm(s) and relatively truncated keys." [Grady Ward, sci.crypt, 1994-08-15]

9.6. Current Crypto Laws

9.6.1. "Has crypto been restricted in countries other than the U.S.?"

- Many countries have restrictions on civilian/private use of crypto. Some even insist that corporations either send all transmissions in the clear, or that keys be provided to the government. The Phillipines, for example. And certainly regimes in the Communists Bloc, or what's left of it, will likely have various laws restricting crypto. Possibly draconian laws....in many cultures, use of crypto is tantamount to espionage.

9.7. Crypto Laws Outside the U.S.

9.7.1. "International Escrow, and Other Nation's Crypto Policies?"

- The focus throughout this document on U.S. policy should not lull non-Americans into complacency. Many nations already have more Draconian policies on the private use of encryption than the U.S. is even contemplating (publically). France outlaws private crypto, though enforcement is said to be problematic (but I would not want the DGSE to be on my tail, that's for sure). Third World countries often have bans on crypto, and mere possession of random-looking bits may mean a spying conviction and a trip to the gallows.

- + There are also several reports that European nations are preparing to fall in line behind the U.S. on key escrow

- Norway
- Netherlands
- Britain

- + A conference in D.C. in 6/94, attended by Whit Diffie (and reported on to us at the 6/94 CP meeting) had international escrow arrangements as a topic, with the crypto policy makers of NIST and NSA describing various options

- bad news, because it could allow bilateral treaties to supercede basic rights

- could be plan for getting key escrow made mandatory

- + there are also practical issues

- + who can decode international communications?

- do we really want the French reading Intel's communications? (recall Matra-Harris)

- satellites? (like Iridium)

- what of multi-national messages, such as an encrypted message posted to a message pool on the Internet...is it to be escrowed with each of 100 nations?

9.7.2. "Will foreign countries use a U.S.-based key escrow system?"

- Lots of pressure. Lots of evidence of compliance.

9.7.3. "Is Europe Considering Key Escrow?"

- Yes, in spades. Lots of signs of this, with reports coming in from residents of Europe and elsewhere. The Europeans

tend to be a bit more quiet in matters of public policy (at least in some areas).

- "The current issue of `Communications Week International' informs us that the European Union's Senior Officials Group for Security of Information Systems has been considering plans for standardising key escrow in Europe.

"Agreement had been held up by arguments over who should hold the keys. France and Holland wanted to follow the NSA's lead and have national governments assume this role; other players wanted user organisations to do this." [rja14@cl.cam.ac.uk (Ross Anderson), sci.crypt, Key Escrow in Europe too, 1994-06-29]

9.7.4. "What laws do various countries have on encryption and the use of encryption for international traffic?"

- + "Has France really banned encryption?"
 - There are recurring reports that France does not allow unfettered use of encryption.
 - Hard to say. Laws on the books. But no indications that the many French users of PGP, say, are being prosecuted.
 - a nation whose leader, Francois Mitterand, was a Nazi collaborationist, working with Petain and the Vichy government (Klaus Barbie involved)
- + Some Specific Countries
 - (need more info here)
 - + Germany
 - BND cooperates with U.S.
 - Netherlands
 - Russia
- + Information
 - "Check out the ftp site at csrc.ncsl.nist.gov for a document named something like "laws.wp" (There are several of these, in various formats.) This contains a survey of the positions of various countries, done for NIST by a couple of people at Georgetown or George Washington or some such university." [Philip Fites, alt.security.pgp, 1994-07-03]

9.7.5. France planning Big Brother smart card?

- "PARIS, FRANCE, 1994 MAR 4 (NB) -- The French government has confirmed its plans to replace citizen's paper-based ID cards with credit card-sized "smart card" ID cards.

.....

"The cards contain details of recent transactions, as well as act as an "electronic purse" for smaller value transactions using a personal identification number (PIN) as authorization. "Purse transactions" are usually separate from the card credit/debit system, and, when the purse is empty, it can be reloaded from the card at a suitable ATM or retailer terminal." (Steve Gold/19940304)" [this was forwarded to me for posting]

9.7.6. PTTs, local rules about modem use

9.7.7. "What are the European laws on "Data Privacy" and why are they such a terrible idea?"

- Various European countries have passed laws about the compiling of computerized records on people without their explicit permission. This applies to nearly all computerized records--mailing lists, dossiers, credit

records, employee files, etc.--though some exceptions exist and, in general, companies can find ways to compile records and remain within the law.

- The rules are open to debate, and the casual individual who cannot afford lawyers and advisors, is likely to be breaking the laws repeatedly. For example, storing the posts of people on the Cypherpunks list in any system retrievable by name would violate Britain's Data Privacy laws. That almost no such case would ever result in a prosecution (for practical reasons) does not mean the laws are acceptable.
- To many, these laws are a "good idea." But the laws miss the main point, give a false sense of security (as the real dossier-compilers are easily able to obtain exemptions, or are government agencies themselves), and interfere in what people do with information that properly and legally comes there way. (Be on the alert for "civil rights" groups like the ACLU and EFF to push for such data privacy laws. The irony of Kapor's connection to Lotus and the failed "Marketplace" CD-ROM product cannot be ignored.)
- Creating a law which bans the keeping of certain kinds of records is an invitation to having "data inspectors" rummaging through one's files. Or some kind of spot checks, or even software key escrow.
- (Strong crypto makes these laws tough to enforce. Either the laws go, or the counties with such laws will then have to limit strong crypto....not that that will help in the long run.)
- The same points apply to well-meaning proposals to make employer monitoring of employees illegal. It sounds like a privacy-enhancing idea, but it tramples upon the rights of the employer to ensure that work is being done, to basically run his business as he sees fit, etc. If I hire a programmer and he's using my resources, my network connections, to run an illegal operation, he exposes my company to damages, and of course he isn't doing the job I paid him to do. If the law forbids me to monitor this situation, or at least to randomly check, then he can exploit this law to his advantage and to my disadvantage. (Again, the dangers of rigid laws, nonmarket solutions, (lied game theory.)

9.7.8. on the situation in Australia

- + Matthew Gream [M.Gream@uts.edu.au] informed us that the export situation in Oz is just as best as in the U.S. [1994-09-06] (as if we didn't know...much as we all like to dump on Amerika for its fascist laws, it's clear that nearly all countries are taking their New World Order Marching Orders from the U.S., and that many of them have even more repressive crypto laws already in place...they just don't get the discussion the U.S. gets, for apparent reasons)
 - "Well, fuck that for thinking I was living under a less restrictive regime -- and I can say goodbye to an international market for my software.]
 - (I left his blunt language as is, for impact.)

9.7.9. "For those interested, NIST have a short document for FTP, 'Identification & Analysis of Foreign Laws & Regulations Pertaining to the Use of Commercial Encryption Products for

Voice & Data Communications'. Dated Jan 1994." [Owen Lewis,
Re: France Bans Encryption, alt.security.pgp, 1994-07-07]

9.8. Digital Telephony

9.8.1. "What is Digital Telephony?"

- The Digital Telephony Bill, first proposed under Bush and again by Clinton, is in many ways much worse than Clipper. It has gotten less attention, for various reasons.
- For one thing, it is seen as an extension by some of existing wiretap capabilities. And, it is fairly abstract, happening behind the doors of telephone company switches.
- The implications are severe: mandatory wiretap and pen register (who is calling whom) capabilities, civil penalties of up to \$10,000 a day for insufficient compliance, mandatory assistance must be provided, etc.
- If it is passed, it could dictate future technology. Telcos who install it will make sure that upstart technologies (e.g., Cypherpunks who find ways to ship voice over computer lines) are also forced to "play by the same rules." Being required to install government-accessible tap points even in small systems would of course effectively destroy them.
- On the other hand, it is getting harder and harder to make Digital Telephony workable, even by mandate. As Jim Kallstrom of the FBI puts it: ""Today will be the cheapest day on which Congress could fix this thing," Kallstrom said. "Two years from now, it will be geometrically more expensive."" [LAN Magazine, "Is it 1984?" by Ted Bunker, August 1994]
- This gives us a goal to shoot for: sabotage the latest attempt to get Digital Telephony passed into law and it may make it too intractable to *ever* be passed.
- + "Today will be the cheapest day on which
 - Congress could fix this thing," Kallstrom said. "Two years from now,
 - it will be geometrically more expensive."
- The message is clear: delay Digital Telephony. Sabotage it in the court of public opinion, spread the word, make it flop. (Reread your "Art of War" for Sun Tsu's tips on fighting your enemy.)

9.8.2. "What are the dangers of the Digital Telephony Bill?"

- It makes wiretapping invisible to the tappee.
- + If passed into law, it makes central office wiretapping trivial, automatic.
 - "What should worry people is what isn't in the news (and probably never will until it's already embedded in comm systems). A true 'Clipper' will allow remote tapping on demand. This is very easily done to all-digital communications systems. If you understand network routers and protocol it's easy to envision how simple it would be to 're-route' a copy of a target comm to where ever you want it to go..." [domonkos@access.digex.net (andy domonkos), comp.org.eff.talk, 1994-06-29]

9.8.3. "What is the Digital Telephony proposal/bill?"

- proposed a few years ago...said to be inspiration for PGP
- reintroduced Feb 4, 1994

- earlier versrion:
- + "1) DIGITAL TELEPHONY PROPOSAL
 - "To ensure law enforcement's continued ability to conduct court-
 - authorized taps, the administration, at the request of the
 - Dept. of Justice and the FBI, proposed ditigal telephony
 - legislation. The version submitted to Congress in Sept. 1992
 - would require providers of electronic communication services
 - and private branch exchange (PBX) operators to ensure that the
 - government's ability to lawfully intercept communications is not
 - curtailed or prevented entirely by the introduction of advanced
 - technology."

9.9. Clipper, Escrowed Encyption Standard

9.9.1. The Clipper Proposal

- A bombshell was dropped on April 16, 1993. A few of us saw it coming, as we'd been debating...

9.9.2. "How long has the government been planning key escrow?"

- since about 1989
- ironically, we got about six months advance warning
- my own "A Trial Balloon to Ban Encryption" alerted the world to the thinking of D. Denning....she denies having known about key escrow until the day before it was announced, which I find implausible (not calling her a liar, but...)

+ Phil Karn had this to say to Professor Dorothy Denning, several weeks prior to the Clipper announcement:

- "The private use of strong cryptography provides, for the very first time, a truly effective safeguard against this sort of government abuse. And that's why it must continue to be free and unregulated.
- "I should credit you for doing us all a very important service by raising this issue. Nothing could have lit a bigger fire under those of us who strongly believe in a citizens' right to use cryptography than your proposals to ban or regulate it. There are many of us out here who share this belief *and* have the technical skills to turn it into practice. And I promise you that we will fight for this belief to the bitter end, if necessary." [Phil Karn, 1993-03-23]

-
-

9.9.3. Technically, the "Escrowed Encryption Standard," or EES. But early everyone still calls it "Clipper, " even if NSA belatedly realized Intergraph's won product has been called this for many years, a la the Fairchild processor chip of the same name. And the database product of the same name. I pointed this out within minutes of hearing about this on April 16th, 1993, and posted a comment to this effect on sci.crypt. How clueless can they be to not have seen in many months of work what many of us saw within seconds?

- 9.9.4. Need for Clipper
- 9.9.5. Further "justifications" for key escrow
 - + anonymous consultations that require revealing of identities
 - suicide crisis intervention
 - confessions of abuse, crimes, etc. (Tarasoff law)
 - corporate records that Feds want to look at
 - + Some legitimate needs for escrowed crypto
 - for corporations, to bypass the passwords of departed, fired, deceased employees,
- 9.9.6. Why did the government develop Clipper?
- 9.9.7. "Who are the designated escrow agents?"
 - Commerce (NIST) and Treasury (Secret Service).
- 9.9.8. Whit Diffie
 - Miles Schmid was architect
 - + international key escrow
 - Denning tried to defend it....
- 9.9.9. What are related programs?
- 9.9.10. "Where do the names "Clipper" and "Skipjack" come from?"
 - First, the NSA and NIST screwed up big time by choosing the name "Clipper," which has long been the name of the 32-bit RISC processor (one of the first) from Fairchild, later sold to Intergraph. It is also the name of a database compiler. Most of us saw this immediately.
 -
 - + Clippers are boats, so are skipjacks ("A small sailboat having a
 - bottom shaped like a flat V and vertical sides" Am Heritage. 3rd).
 - Suggests a nautical theme, which fits with the Cheseapeake environs of
 - the Agency (and small boats have traditionally been a way for the
 - + Agencies to dispose of suspected traitors and spies).
 -
 - However, Capstone is not a boat, nor is Tessera, so the trend fails.
- 9.10. Technical Details of Clipper, Skipjack, Tessera, and EES
- 9.10.1. Clipper chip fabrication details
 - + ARM6 core being used
 - but also rumors of MIPS core in Tessera
 - MIPS core reportedly being designed into future versions
 - National also built (and may operate) a secure wafer fab line for NSA, reportedly located on the grounds of Ft. Meade--though I can't confirm the location or just what National's current involvement still is. May only be for medium-density chips, such as key material (built under secure conditions).
- 9.10.2. "Why is the Clipper algorithm classified?"
 - to prevent non-escrow versions, which could still use the (presumably strong) algorithm and hardware but not be escrowed
 - cryptanalysis is always easier if the algorithms are known :-}
 - general government secrecy
 - backdoors?

- 9.10.3. If Clipper is flawed (the Blaze LEAF Blower), how can it still be useful to the NSA?
- by undermining commercial alternatives through subsidized costs (which I don't think will happen, given the terrible PR Clipper has gotten)
 - mandated by law or export rules
 - and the Blaze attack is--at present--not easy to use (and anyone able to use it is likely to be sophisticated enough to use preencryption anyway)
- 9.10.4. What about weaknesses of Clipper?
- In the views of many, a flawed approach. That is, arguing about wrinkles plays into the hands of the Feds.
- 9.10.5. "What are some of the weaknesses in Clipper?"
- the basic idea of key escrow is an infringement on liberty
 - + access to the keys
 - "
 - + "There's a big door in the side with a
 - big neon sign saying "Cops and other Authorized People Only";
 - the trapdoor is the fact that anybody with a fax machine can make
 - themselves and "Authorized Person" badge and walk in. <Bill Stewart, bill.stewart@pleasantonca.ncr.com, 4-15-94, sci.crypt>
 - possible back doors in the Skipjace algorithm
 - + generation of the escrow keys
 -
 - + "There's another trapdoor, which is that if you can predict the escrow
 - keys by stealing the parameters used by the Key Generation Bureau to
 - set them, you don't need to get the escrow keys from the keymasters,
 - you can gen them yourselves. " <Bill Stewart, bill.stewart@pleasantonca.ncr.com, 4-15-94, sci.crypt>
- 9.10.6. Mykotronx
- MYK-78e chip, delays, VTI, fuses
 - National Semiconductor is working with Mykotronx on a faster implementation of the Clipper/Capstone/Skipjack/whatever system. (May or may not be connected directly with the iPower product line. Also, the MIPS processor core may be used, instead of the ARM core, which is said to be too slow.)
- 9.10.7. Attacks on EES
- sabotaging the escrow data base
 - + stealing it, thus causing a collapse in confidence
 - Perry Metzger's proposal
 - FUD
- 9.10.8. Why is the algorithm secret?
- 9.10.9. Skipjack is 80 bits, which is 24 bits longer than the 56 bits of DES. so
- 9.10.10. "What are the implications of the bug in Tessera found by Matt Blaze?"
- Technically, Blaze's work was done on a Tessera card, which implements the Skipjace algorithm. The Clipper phone system may be slightly different and details may vary; the Blaze attack may not even work, at least not practically.

- " The announcement last month was about a discovery that, with a half-hour or so of time on an average PC, a user could forge a bogus LEAF (the data used by the government to access the back door into Clipper encryption). With such a bogus LEAF, the Clipper chip on the other end would accept and decrypt the communication, but the back door would not work for the government." [Steve Brinich, alt.privacy.clipper, 1994-07-04]
- "The "final" pre-print version (dated August 20, 1994) of my paper, "Protocol Failure in the Escrowed Encryption Standard" is now available. You can get it in PostScript form via anonymous ftp from research.att.com in the file /dist/mab/eesproto.ps . This version replaces the preliminary draft (June 3) version that previously occupied the same file. Most of the substance is identical, although few sections are expanded and a few minor errors are now corrected." [Matt Blaze, 1994-09-04]

9.11. Products, Versions -- Tessera, Skipjack, etc.

9.11.1. "What are the various versions and products associated with EES?"

- Clipper, the MYK-78 chip.
- Skipjack.
- + Tessera. The PCMCIA card version of the Escrowed Encryption Standard.
 - the version Matt Blaze found a way to blow the LEAF
 - National Semiconductor "iPower" card may or may not support Tessera (conflicting reports).

9.11.2. AT&T Surety Communications

- NSA may have pressured them not to release DES-based products

9.11.3. Tessera cards

- iPower
- Specifications for the Tessera card interface can be found in several places, including " csrc.ncsl.nist.gov"--see the file cryptcal.txt [David Koontz, 1994-08-08].

9.12. Current Status of EES, Clipper, etc.

9.12.1. "Did the Administration really back off on Clipper? I heard that Al Gore wrote a letter to Rep. Cantwell, backing off."

- No, though Clipper has lost steam (corporations weren't interested in buying Clipper phones, and AT&T was very late in getting "Surety" phones out).
- The Gore announcement may actually indicate a shift in emphasis to "software key escrow" (my best guess).
- Our own Michael Froomkin, a lawyer, writes: "The letter is a nullity. It almost quotes from testimony given a year earlier by NIST to Congress. Get a copy of Senator Leahy's reaction off the eff www server. He saw it for the empty thing it is....Nothing has changed except Cantwell dropped her bill for nothing." [A.Michael Froomkin, alt.privacy.clipper, 1994-09-05]

9.13. National Information Infrastructure, Digital Superhighway

9.13.1. Hype on the Information Superhighway

- It's against the law to talk about the Information Superhighway without using at least one of the overworked

- metaphors: road kill, toll booths, passing lanes, shoulders, on-ramps, off-ramps, speeding, I-way, Infobahn, etc.
 - Most of what is now floating around the suddenly-trendy idea of the Digital Superduperway is little more than hype. And mad metaphors. Misplaced zeal, confusing tangential developments with real progress. Much like libertarians assuming the space program is something they should somehow be working on.
 - For example, the much-hyped "Pizza Hut" on the Net (home pizza pages, I guess). It is already being dubbed "the first case of true Internet commerce." Yeah, like the Coke machines on the Net so many years ago were examples of Internet commerce. Pure hype. Madison Avenue nonsense. Good for our tabloid generation.
- 9.13.2. "Why is the National Information Infrastructure a bad idea?"
- NII = Information Superhighway = Infobahn = Iway = a dozen other supposedly clever and punning names
 - + Al Gore's proposal:
 - links hospitals, schools, government
 - + hard to imagine that the free-wheeling anarchy of the Internet would persist..more likely implications:
 - "is-a-person" credentials, that is, proof of identity, and hence tracking, of all interactions
 - the medical and psychiatric records would be part of this (psychiatrists are leery of this, but they may have no choice but to comply under the National Health Care plans being debated)
 - + There are other bad aspects:
 - government control, government inefficiency, government snooping
 - distortion of markets ("universal access')
 - restriction of innovation
 - is not needed...other networks are doing perfectly well, and will be placed where they are needed and will be locally paid for
- 9.13.3. NII, Video Dialtone
- + "Dialtone"
 - phone companies offer an in-out connection, and charge for the connection, making no rulings on content (related to the "Common Carrier" status)
 - + for video-cable, I don't believe there is an analogous set-up being looked at
 - + cable t.v.
 - Carl Kadie's comments to Sternlight
- 9.13.4. The prospects and dangers of Net subsidies
- "universal access," esp. if same happens in health care
 - those that pay make the rules
 - + but such access will have strings attached
 - limits on crypto
 -
 - universal access also invites more spamming, a la the "Freenet" spams, in which folks keep getting validated as new users: any universal access system that is not pay-as-you-go will be sensitive to this *or* will result in calls for universal ID system (is-a-person credentialling)
- 9.13.5. NII, Superhighway, I-way
- crypto policy

- regulation, licensing

9.14. Government Interest in Gaining Control of Cyberspace

9.14.1. Besides Clipper, Digital Telephony, and the National Information Infrastructure, the government is interested in other areas, such as e-mail delivery (US Postal Service proposal) and maintenance of network systems in general.

9.14.2. Digital Telephony, ATM networks, and deals being cut

- Rumblings of deals being cut
- a new draft is out [John Gilmore, 1994-08-03]
- Encryption with hardware at full ATM speeds
- and SONET networks (experimental, Bay Area?)

9.14.3. The USPS plans for mail, authentication, effects on competition, etc.

- + This could have a devastating effect on e-mail and on cyberspace in general, especially if it is tied in to other government proposals in an attempt to gain control of cyberspace.
 - Digital Telephony, Clipper, pornography laws and age enforcement (the Amateur Action case), etc.
- + "Does the USPS really have a monopoly on first class mail?"
 - and on "routes"?
 - "The friendly PO has recently been visiting the mail rooms of 2) The friendly PO has recently been visiting the mail rooms of corporations in the Bay Area, opening FedEx, etc. packages (not protected by the privacy laws of the PO's first class mail), and fining companies (\$10,000 per violation, as I recall), for sending non-time-sensitive documents via FedEx when they could have been sent via first-class mail." [Lew Glendenning, USPS digital signature announcement, sci.crypt, 1994-08-23] (A citation or a news story would make this more credible, but I've heard of similar spot checks.)
 - The problems with government agencies competing are well-known. First, they often have shoddy service..civil service jobs, unfireable workers, etc. Second, they often cannot be sued for nonperformance. Third, they often have government-granted monopolies.
- + The USPS proposal may be an opening shot in an attempt to gain control of electronic mail...it never had control of e-mail, but its monopoly on first-class mail may be argued by them to extend to cyberspace.
 - Note: FedEx and the other package and overnight letter carriers face various restrictions on their service; for example, they cannot offer "routes" and the economies that would result in.
 - A USPS takeover of the e-mail business would mean an end to many Cypherpunks objectives, including remailers, digital postage, etc.
 - The challenge will be to get these systems deployed as quickly as possible, to make any takeover by the USPS all the more difficult.

9.15. Software Key Escrow

9.15.1. (This section needs a lot more)

9.15.2. things are happening fast....

9.15.3. TIS, Carl Ellison, Karlsruhe

9.15.4. objections to key escrow

- "Holding deposits in real estate transactions is a classic example. Built-in wiretaps are *not* escrow, unless the government is a party to your contract. As somebody on the list once said, just because the Mafia call themselves "businessmen" doesn't make them legitimate; calling extorted wiretaps "escrow" doesn't make them a service.

"The government has no business making me get their permission to talk to anybody about anything in any language I choose, and they have no business insisting I buy "communication protection service" from some of their friends to do it, any more than the aforementioned "businessmen" have any business insisting I buy "fire insurance" from *them*." [Bill Stewart, 1994-07-24]

9.15.5. Micali's "Fair Escrow"

- various efforts underway
- need section here
- Note: participants at Karlsruhe Conference report that a German group may have published on software key escrow years before Micali filed his patent (reports that NSA officials were "happy")

9.16. Politics, Opposition

9.16.1. "What should Cypherpunks say about Clipper?"

- A vast amount has been written, on this list and in dozens of other forums.
- Eric Hughes put it nicely a while back:
- "The hypothetical backdoor in clipper is a charlatan's issue by comparison, as is discussion of how to make a key escrow system 'work.' Do not be suckered into talking about an issue that is not important. If someone want to talk about potential back doors, refuse to speculate. The existence of a front door (key escrow) make back door issues pale in comparison.

"If someone wants to talk about how key escrow works, refuse to elaborate. Saying that this particular key escrow system is bad has a large measure of complicity in saying that escrow systems in general are OK. Always argue that this particular key escrow system is bad because it is a key escrow system, not because it has procedural flaws.

"This right issue is that the government has no right to my private communications. Every other issue is the wrong issue and detracts from this central one. If we defeat one particular system without defeating all other possible such systems at the same time, we have not won at all; we have delayed the time of reckoning." [Eric Hughes, Work the work!, 1993-06-01]

9.16.2. What do most Americans think about Clipper and privacy?"

- insights into what we face
- + "In a Time/CNN poll of 1,000 Americans conducted last week by Yankelovich
- Partners, two-thirds said it was more important to

- protect the privacy of phone
 - calls than to preserve the ability of police to conduct wiretaps.
 - When informed about the Clipper Chip, 80% said they opposed it."
 - Philip Elmer-Dewitt, "Who Should Keep the Keys", Time, Mar. 4, 1994
- 9.16.3. Does anyone actually support Clipper?
 - + There are actually legitimate uses for forms of escrow:
 - corporations
 - other partnerships
- 9.16.4. "Who is opposed to Clipper?"
 - Association for Computing Machinery (ACM). "The USACM urges the Administration at this point to withdraw the Clipper Chip proposal and to begin an open and public review of encryption policy. The escrowed encryption initiative raises vital issues of privacy, law enforcement, competitiveness and scientific innovation that must be openly discussed." [US ACM, DC Office" <usacm_dc@acm.org>, USACM Calls for Clipper Withdrawal, press release, 1994-06-30]
- 9.16.5. "What's so bad about key escrow?"
 - + If it's truly voluntary, there can be a valid use for this.
 - + Are trapdoors justified in some cases?
 - + Corporations that wish to recover encrypted data
 - + several scenarios
 - employee encrypts important files, then dies or is otherwise unavailable
 - + employee leaves company before decrypting all files
 - some may be archived and not needed to be opened for many years
 - employee may demand "ransom" (closely related to virus extortion cases)
 - files are found but the original encryptor is unknown
 - + Likely situation is that encryption algorithms will be mandated by corporation, with a "master key" kept available
 - like a trapdoor
 - the existence of the master key may not even be publicized within the company (to head off concerns about security, abuses, etc.)
 - + Government is trying to get trapdoors put in
 - S.266, which failed ultimately (but not before creating a ruckus)
 - + If the government requires it...
 - Key escrow means the government can be inside your home without you even knowing it
 - and key escrow is not really escrow...what does one get back from the "escrow" service?
- 9.16.6. Why governments should not have keys
 - can then set people up by faking messages, by planting evidence
 - can spy on targets for their own purposes (which history tells us can include bribery, corporate espionage, drug-running, assassinations, and all manner of illegal and sleazy activities)

- can sabotage contracts, deals, etc.
 - would give them access to internal corporate communications
 - undermines the whole validity of such contracts, and of cryptographic standards of identity (shakes confidence)
 - giving the King or the State the power to impersonate another is a gross injustice
 - imagine the government of Iran having a backdoor to read the secret journals of its subjects!
 - 4th Amendment
 - attorney-client privilege (with trapdoors, no way to know that government has not breached confidentiality)
- 9.16.7. "How might the Clipper chip be foiled or defeated?"
- Politically, market-wise, and technical
 - If deployed, that is
- + Ways to Defeat Clipper
- preencryption or superencryption
 - LEAF blower
 - plug-compatible, reverse-engineered chip
 - sabotage
 - undermining confidence
 - Sun Tzu
- 9.16.8. How can Clipper be defeated, politically?
- 9.16.9. How can Clipper be defeated, in the market?
- 9.16.10. How can Clipper be defeated, technologically?
- 9.16.11. Questions
- + Clipper issues and questions
- a vast number of questions, comments, challenges, tidbits, details, issues
 - entire newsgroups devoted to this
- + "What criminal or terrorist will be smart enough to use encryption but dumb enough to use Clipper?"
- This is one of the Great Unanswered Questions. Clipper's supporter's are mum on this one. Suggesting....
- + "Why not encrypt data before using the Clipper/EES?"
- "Why can't you just encrypt data before the clipper chip?"

Two answers:

1) the people you want to communicate with won't have hardware to decrypt your data, statistically speaking. The beauty of clipper from the NSA point of view is that they are leveraging the installed base (they hope) of telephones and making it impossible (again, statistically) for a large fraction of the traffic to be untappable.

2) They won't license bad people like you to make equipment like the system you describe. I'll wager that the chip distribution will be done in a way to prevent significant numbers of such systems from being built, assuring that (1) remains true." [Tom

Knight, sci.crypt, 6-5-93]

-
- + What are the implications of mandatory key escrow?
 - + "escrow" is misleading...
 - wrong use of the term
 - implies a voluntary, and returnable, situation
 - + "If key escrow is "voluntary," what's the big deal?"
 - Taxes are supposedly "voluntary," too.
 - A wise man prepares for what is possible and even likely, not just what is announced as part of public policy; policies can and do change. There is plenty of precedent for a "voluntary" system being made mandatory.
 - The form of the Clipper/EES system suggests eventual mandatory status; the form of such a ban is debatable.
 - + "What is 'superencipherment,' and can it be used to defeat Clipper?"
 - preencrypting
 - could be viewed as a non-English language
 - + how could Clipper chip know about it (entropy measures?)
 - far-fetched
 - wouldn't solve traffic anal. problem
 - What's the connection between Clipper and export laws?
 - + "Doesn't this make the Clipper database a ripe target?"
 - for subversion, sabotage, espionage, theft
 - presumably backups will be kept, and these will also be targets
 - + "Is Clipper just for voice encryption?"
 - Clipper is a data encryption chip, with the digital data supplied by an ADC located outside the chip. In principle, it could thus be used for data encryption in general.
 - In practice, the name Clipper is generally associated with telephone use, while "Capstone" is the data standard (some differences, too). The "Skipjack" algorithm is used in several of these proposed systems (Tessera, also).
- 9.16.12. "Why is Clipper worse than what we have now?"
 - + John Gilmore answered this question in a nice essay. I'm including the whole thing, including a digression into cellular telephones, because it gives some insight--and names some names of NSA liars--into how NSA and NIST have used their powers to thwart true security.
 - "It's worse because the market keeps moving toward providing real encryption.

"If Clipper succeeds, it will be by displacing real secure encryption. If real secure encryption makes it into mass market communications products, Clipper will have failed. The whole point is not to get a few Clippers used by cops; the point is to make it a worldwide standard, rather than having 3-key triple-DES with RSA and Diffie-Hellman become the worldwide standard.

"We'd have decent encryption in digital cellular phones *now*, except for the active intervention of Jerry Rainville of NSA, who `hosted' a meeting of the standards

committee inside Ft. Meade, lied to them about export control to keep committee documents limited to a small group, and got a willing dupe from Motorola, Louis Finkelstein, to propose an encryption scheme a child could break. The IS-54 standard for digital cellular doesn't describe the encryption scheme -- it's described in a separate document, which ordinary people can't get, even though it's part of the official accredited standard. (Guess who accredits standards bodies though - - that's right, the once pure NIST.)

"The reason it's secret is because it's so obviously weak. The system generates a 160-bit "key" and then simply XORs it against each block of the compressed speech. Take any ten or twenty blocks and recover the key by XORing frequent speech patterns (like silence, or the letter "A") against pieces of the blocks to produce guesses at the key. You try each guess on a few blocks, and the likelihood of producing something that decodes like speech in all the blocks is small enough that you'll know when your guess is the real key.

"NSA is continuing to muck around in the Digital Cellular standards committee (TR 45.3) this year too. I encourage anyone who's interested to join the committee, perhaps as an observer. Contact the Telecommunications Industry Association in DC and sign up. Like any standards committee, it's open to the public and meets in various places around the country. I'll lend you a lawyer if you're a foreign national, since the committee may still believe that they must exclude foreign nationals from public discussions of cryptography. Somehow the crypto conferences have no trouble with this; I think it's called the First Amendment. NSA knows the law here -- indeed it enforces it via the State Dept -- but lied to the committee." [John Gilmore, "Why is clipper worse than "no encryption like we have," comp.org.eff.talk, 1994-04-27]

9.16.13. on trusting the government

- "WHAT AM THE MORAL OF THE STORY, UNCLE REMUS?....When the government makes any announcement (ESPECIALLY a denial), you should figure out what the government is trying to get you to do--and do the opposite. Contrarianism with a vengeance. Of all the advice I've offered on the Cypherpunks Channel, this is absolutely the most certain." [Sandy Sandfort, 1994-07-17]
- if the Founders of the U.S. could see the corrupt, socialist state this nation has degenerated to, they'd be breaking into missile silos and stealing nukes to use against the central power base.
- + can the government be trusted to run the key escrow system?
 - "I just heard on the news that 1300 IRS employees have been disciplined for unauthorized accesses to electronically filed income tax returns. ..I'm sure they will do much better, though, when the FBI runs the phone system, the Post Office controls digital identity and Hillary takes care of our health." [Sandy Sandfort, 1994-

07-19]

- This is just one of many such examples: Watergate ("I am not a crook!"), Iran-Contra, arms deals, cocaine shipments by the CIA, Teapot Dome, graft, payoffs, bribes, assassinations, Yankee-Cowboy War, Bohemian Grove, Casolaro, more killings, invasions, wars. The government that is too chicken to ever admit it lost a war, and conspicuously avoids diplomatic contact with enemies it failed to vanquish (Vietnam, North Korea, Cuba, etc.), while quickly becoming sugar daddy to the countries it did vanquish...the U.S. appears to be lacking in practicality. (Me, I consider it wrong for anyone to tell me I can't trade with folks in another country, whether it's Haiti, South Africa, Cuba, Korea, whatever. Crypto anarchy means we'll have some of the ways of bypassing these laws, of making our own moral decisions without regard to the prevailing popular sentiment of the countries in which we live at the moment.)

9.17. Legal Issues with Escrowed Encryption and Clipper

- 9.17.1. As John Gilmore put it in a guest editorial in the "San Francisco Examiner," "...we want the public to see a serious debate about why the Constitution should be burned in order to save the country." [J.G., 1994-06-26, quoted by S. Sandfort]
- 9.17.2. "I don't see how Clipper gives the government any powers or capabilities it doesn't already have. Comments?"
- 9.17.3. Is Clipper really voluntary?
- 9.17.4. If Clipper is voluntary, who will use it?
- 9.17.5. Restrictions on Civilian Use of Crypto
- 9.17.6. "Has crypto been restricted in the U.S.?"
- 9.17.7. "What legal steps are being taken?"
 - Zimmermann
 - ITAR
- 9.17.8. reports that Department of Justice has a compliance enforcement role in the EES [heard by someone from Dorothy Denning, 1994-07], probably involving checking the law enforcement agencies...
- 9.17.9. Status
 - + "Will government agencies use Clipper?"
 - Ah, the embarrassing question. They claim they will, but there are also reports that sensitive agencies will not use it, that Clipper is too insecure for them (key length, compromise of escrow data, etc.). There may also be different procedures (all agencies are equal, but some are more equal than others).
 - Clipper is rated for unclassified use, so this rules out many agencies and many uses. An interesting double standard.
 - + "Is the Administration backing away from Clipper?"
 - + industry opposition surprised them
 - groups last summer, Citicorp, etc.
 - public opinion
 - editorial remarks
 - so they may be preparing alternative
 - and Gilmore's FOIA, Blaze's attack, the Denning

- nonreview, the secrecy of the algorithm
- + will not work
 - spies won't use it, child pornographers probably won't use it (if alternatives exist, which may be the whole point)
 - terrorists won't use it
- Is Clipper in trouble?
- 9.17.10. "Will Clipper be voluntary?"
 - Many supporters of Clipper have cited the voluntary nature of Clipper--as expressed in some policy statements--and have used this to counter criticism.
- + However, even if truly voluntary, some issues
 - + improper role for government to try to create a commercial standard
 - though the NIST role can be used to counter this point, partly
 - government can and does make it tough for competitors
 - export controls (statements by officials on this exist)
- + Cites for voluntary status:
 - original statement says it will be voluntary
 - (need to get some statements here)
- + Cites for eventual mandatory status:
 - "Without this initiative, the government will eventually become helpless to defend the nation." [Louis Freeh, director of the FBI, various sources]
 - Steven Walker of Trusted Information Systems is one of many who think so: "Based on his analysis, Walker added, 'I'm convinced that five years from now they'll say 'This isn't working,' so we'll have to change the rules.'" Then, he predicted, Clipper will be made mandatory for all encoded communications." [
- + Parallels to other voluntary programs
 - taxes
- 9.18. Concerns
 - 9.18.1. Constitutional Issues
 - 4th Amend
 - privacy of attorney-client, etc.
 - + Feds can get access without public hearings, records
 - secret intelligence courts
 -
 - + "It is uncontested (so far as I have read) that under certain circum-
 - stances, the Federal intelligence community will be permitted to
 - obtain Clipper keys without any court order on public record. Only
 - internal, classified proceedings will protect our privacy." <Steve Waldman, steve@vesheu.sar.usf.edu, sci.crypt, 4-13-94>
 - 9.18.2. "What are some dangers of Clipper, if it is widely adopted?"
 - + sender/receiver ID are accessible without going to the key escrow
 - this makes traffic analysis, contact lists, easy to generate
 - + distortions of markets ("chilling effects") as a plan by government

- make alternatives expensive, hard to export, grounds for suspicion
 - use of ITAR to thwart alternatives (would be helped if Cantwell bill to liberalize export controls on cryptography (HR 3627) passes)
 - + VHDL implementations possible
 - speculates Lew Glendenning, sci.crypt, 4-13-94
 - and recall MIPS connection (be careful here)
- 9.18.3. Market Issues
- 9.18.4. "What are the weaknesses in Clipper?"
- + Carl Ellison analyzed it this way:
 - "It amuses the gallows-humor bone in me to see people busily debating the quality of Skipjack as an algorithm and the quality of the review of its strength.

Someone proposes to dangle you over the Grand Canyon using

```

        sewing thread
tied to
        steel chain
tied to
        knitting yarn

```

and you're debating whether the steel chain has been X-rayed properly to see if there are flaws in the metal.

"Key generation, chip fabrication, court orders, distribution of keys once acquired from escrow agencies and safety of keys within escrow agencies are some of the real weaknesses. Once those are as strong as my use of 1024-bit RSA and truly random session keys in keeping keys on the two sides of a conversation with no one in the middle able to get the key, then we need to look at the steel chain in the middle: Skipjack itself." [Carl Ellison, 1993-08-02]

```

+ Date: Mon, 2 Aug 93 17:29:54 EDT
  From: cme@ellisun.sw.stratus.com (Carl Ellison)
  To: cypherpunks@toad.com
  Subject: cross-post
  Status: OR

```

```

Path: transfer.stratus.com!ellisun.sw.stratus.com!cme
From: cme@ellisun.sw.stratus.com (Carl Ellison)
Newsgroups: sci.crypt
Subject: Skipjack review as a side-track
Date: 2 Aug 1993 21:25:11 GMT
Organization: Stratus Computer, Marlboro MA
Lines: 28
Message-ID: <23k0nn$8gk@transfer.stratus.com>
NNTP-Posting-Host: ellisun.sw.stratus.com

```

It amuses the gallows-humor bone in me to see people busily debating the quality of Skipjack as an algorithm and the quality of the review of its

strength.

Someone proposes to dangle you over the Grand Canyon using

 sewing thread
tied to
 steel chain
tied to
 knitting yarn

and you're debating whether the steel chain has been X-rayed properly to see if there are flaws in the metal.

Key generation, chip fabrication, court orders, distribution of keys once acquired from escrow agencies and safety of keys within escrow agencies are some of the real weaknesses. Once those are as strong as my use of 1024-bit RSA and truly random session keys in keeping keys on the two sides of a conversation with no one in the middle able to get the key, then we need to look at the steel chain in the middle: Skipjack itself.

- "Key generation, chip fabrication, court orders, distribution of keys once acquired from escrow agencies and safety of keys within escrow agencies are some of the real weaknesses. Once those are as strong as my use of 1024-bit RSA and truly random session keys in keeping keys on the two sides of a conversation with no one in the middle able to get the key, then we need to look at the steel chain in the middle: Skipjack itself."

9.18.5. What it Means for the Future

9.18.6. Skipjack

9.18.7. National security exceptions

- grep Gilmore's FOIA for mention that national security people will have direct access and that this will not be mentioned to the public
- + "The "National Security" exception built into the Clipper proposal
 - leaves an extraordinarily weak link in the chain of procedures designed
 - to protect user privacy. To place awesome powers of surveillance
 - technologically within the reach of a few, hoping that so weak a chain
 - will bind them, would amount to dangerous folly. It flies in the face
 - of history. <Steve Waldman, steve@vesheu.sar.usf.edu, 4-14-94, talk.politics.crypto>

9.18.8. In my view, any focus on the details of Clipper instead of the overall concept of key escrow plays into their hands.

This is not to say that the work of Blaze and others is misguided....in fact, it's very fine work. But a general focus on the details of Skipjack does nothing to allay my concerns about the principle of government-mandated crypto.

If it were "house key escrow" and there were missing details about the number of teeth allowed on the keys, would we then all breathe a sigh of relief if the details of the teeth were clarified? Of course not. Me, I will never use a key escrow system, even if a blue ribbon panel of hackers and Cypherpunks studies the design and declares it to be cryptographically sound.

9.18.9. Concern about Clipper

- allows past communications to be read
- + authorities could--maybe--read a lot of stuff, even illegally, then use this for other investigations (the old "we had an anonymous tip" ploy)
- "The problem with Clipper is that it provides police agencies with dramatically enhanced target acquisition. There is nothing to prevent NSA, ATF, FBI (or the Special Projects division of the Justice Department) from reviewing all internet traffic, as long as they are willing to forsake using it in a criminal prosecution."
[dgard@netcom.com, alt.privacy.clipper, 1994-07-05]

9.18.10. Some wags have suggested that the new escrow agencies be

chosen from groups like Amnesty International and the ACLU. Most of us are opposed to the "very idea" of key escrow (think of being told to escrow family photos, diaries, or house keys) and hence even these kinds of skeptical groups are unacceptable as escrow agents.

9.19. Loose Ends

9.19.1. "Are trapdoors--or some form of escrowed encryption--justified in some cases?"

- + Sure. There are various reasons why individuals, companies, etc. may want to use crypto protocols that allow them to decrypt even if they've lost their key, perhaps by going to their lawyer and getting the sealed envelope they left with him, etc.
- or using a form of "software key escrow" that allows them access
- + Corporations that wish to recover encrypted data
- + several scenarios
 - employee encrypts important files, then dies or is otherwise unavailable
 - + employee leaves company before decrypting all files
 - some may be archived and not needed to be opened for many years
 - employee may demand "ransom" (closely related to virus extortion cases)
 - files are found but the original encryptor is unknown
- + Likely situation is that encryption algorithms will be mandated by corporation, with a "master key" kept available
 - like a trapdoor
 - the existence of the master key may not even be publicized within the company (to head off concerns about security, abuses, etc.)

- The mandatory use of key escrow, a la a mandatory Clipper system, or the system many of us believe is being developed for software key escrow (SKE, also called "GAK," for "government access to keys, by Carl Ellison) is completely different, and is unacceptable. (Clipper is discussed in many places here.)

9.19.2. DSS

- + Continuing confusion over patents, standards, licensing, etc.
 - "FIPS186 is DSS. NIST is of the opinion that DSS does not violate PKP's patents. PKP (or at least Jim Bidzos) takes the position that it does. But for various reasons, PKP won't sue the government. But Bidzos threatens to sue private parties who infringe. Stay tuned...." [Steve Wildstrom, sci.crypt, 1994-08-19]
 - even Taher ElGamal believes it's a weak standard
 - subliminal channels issues

9.19.3. The U.S. is often hypocritical about basic rights

- plans to "disarm" the Haitians, as we did to the Somalians (which made those we disarmed even more vulnerable to the local warlords)
- government officials are proposing to "silence" a radio station in Ruanda they feel is sending out the wrong message! (Heard on "McNeil-Lehrer News Hour," 1994-07-21]

9.19.4. "is-a-person" and RSA-style credentials

- + a dangerous idea, that government will insist that keys be linked to persons, with only one per person
 - this is a flaw in AOCE system
 - many apps need new keys generated many times

10. Legal Issues

10.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

10.2. SUMMARY: Legal Issues

10.2.1. Main Points

10.2.2. Connections to Other Sections

- Sad to say, but legal considerations impinge on nearly every aspect of crypto

10.2.3. Where to Find Additional Information

10.2.4. Miscellaneous Comments

- "I'm a scientist, Jim, not an attorney." Hence, take my legal comments here with a grain of salt, representing only hints of the truth as I picked them up from the discussions on the various forums and lists.

10.3. Basic Legality of Encryption

10.3.1. "Is this stuff legal or illegal?"

- Certainly the talking about it is mostly legal, at least in the U.S. and at the time of this writing. In other countries, you prison term may vary.
- + The actions resulting from crypto, and crypto anarchy, may

well be illegal. Such is often the case when technology is applied without any particular regard for what the laws say is permitted. (Pandora's Box and all that.)

- Cypherpunks really don't care much about such ephemera as the "laws" of some geographic region. Cypherpunks make their own laws.
 - + There are two broad ways of getting things done:
 - First, looking at the law and regulations and finding ways to exploit them. This is the tack favored by lawyers, of which are many in this country.
 - Second, "just do it." In areas where the law hasn't caught up, this can mean unconstrained technological development. Good examples are the computer and chip business, where issues of legality rarely arose (except in the usual areas of contract enforcement, etc.). More recently the chip business has discovered lawyering, with a vengeance.
 - In other areas, where the law is centrally involved, "just do it" can mean many technical violations of the law. Examples: personal service jobs (maids and babysitters), contracting jobs without licenses, permissions, etc., and so on. Often these are "illegal markets," putatively.
 - And bear in mind that the legal system can be used to hassle people, to pressure them to "plead out" to some charges, to back off, etc. (In the firearms business, the pressures and threats are also used to cause some manufacturers, like Ruger, to back off on a radical pro-gun stance, so as to be granted favors and milder treatment. Pressure on crypto-producing companies are probably very similar. Play ball, or we'll run you over in the parking lot.)
- 10.3.2. "Why is the legal status of crypto so murky?"
- First, it may be murkier to me than it is to actual lawyers like Mike Godwin and Michael Froomkin, both of whom have been on our list at times. (Though my impression from talking to Godwin is that many or even most of these issues have not been addressed in the courts, let alone resolved definitively.)
 - Second, crypto issues have not generally reached the courts, reflecting the nascent status of most of the things talked about it here. Things as "trivial" as digital signatures and digital timestamping have yet to be challenged in courts, or declared illegal, or anything similar that might produce a precedent-setting ruling. (Stu Haber agrees that such tests are lacking.)
 - Finally, the issues are deep ones, going to the heart of issues of self-incrimination (disclosure of keys, contempt), of intellectual property and export laws (want to jail someone for talking about prime numbers?), and the incredibly byzantine world of money and financial instruments.
 - A legal study of crypto--which I hear Professor Froomkin is doing--could be very important.
- 10.3.3. "Has the basic legality of crypto and laws about crypto been tested?"
- As usual, a U.S. focus here. I know little of the situation

- in non-U.S. countries (and in many of them the law is whatever the rulers say it is).
- And I'm not a lawyer.
- + Some facts:
 - no direct Constitutional statement about privacy (though many feel it is implied)
 - crypto was not a major issue (espionage was, and was dealt with harshly, but encrypting things was not a problem per se)
- + only in the recent past has it become important...and it will become much more so
 - as criminals encrypt, as terrorists encrypt
 - as tax is avoided via the techniques described here
 - collusion of business ("crypto interlocking directorates," price signalling)
 - black markets, information markets
- + Lawrence Tribe..new amendment
 - scary, as it may place limits.... (but unlikely to happen)
- + Crypto in Court
 - mostly untested
 - can keys be compelled?
 - Expect some important cases in the next several years
- 10.3.4. "Can authorities force the disclosure of a key?"
- + Mike Godwin, legal counsel for the EFF, has been asked this question many times:
 - "Note that a court could cite you for contempt for not complying with a subpoena duces tecum (a subpoena requiring you to produce objects or documents) if you fail to turn over subpoenaed backups....To be honest, I don't think **any** security measure is adequate against a government that's determined to overreach its authority and its citizens' rights, but crypto comes close." [Mike Godwin, 1993-06-14]
- + Torture is out (in many countries, but not all). Truth serum, etc., ditto.
 - "Rubber hose cryptography"
- + Constitutional issues
 - self-incrimination
- + on the "Yes" side:
 - + is same, some say, as forcing combination to a safe containing information or stolen goods
 - but some say-and a court may have ruled on this-that the safe can always be cut open and so the issue is mostly moot
 - while forcing key disclosure is compelled testimony
 - and one can always claim to have forgotten the key
 - i.e., what happens when a suspect simply clams up?
 - but authorities can routinely demand cooperation in investigations, can seize records, etc.
- + on the "No" side:
 - can't force a suspect to talk, whether about where he hid the loot or where his kidnap victim is hidden
 - practically speaking, someone under indictment cannot be forced to reveal Swiss bank accounts....this would seem to be directly analogous to a cryptographic key
 - thus, the key to open an account would seem to be the

- same thing
 - a memorized key cannot be forced, says someone with EFF or CPSR
 - + "Safe" analogy
 - + You have a safe, you won't tell the combination
 - you just refuse
 - you claim to have forgotten it
 - you really don't know it
 - cops can cut the safe open, so compelling a combination is not needed
 - "interfering with an investigation"
 - on balance, it seems clear that the disclosure of cryptographic keys cannot be forced (though the practical penalty for nondisclosure could be severe)
 - + Courts
 - + compelled testimony is certainly common
 - if one is not charged, one cannot take the 5th (may be some wrinkles here)
 - contempt
 - + What won't immunize disclosure:
 - + clever jokes about "I am guilty of money laundering"
 - can it be used?
 - does judge declaring immunity apply in this case?
 - Eric Hughes has pointed out that the form of the statement is key: "My key is: "I am a murderer."" is not a legal admission of anything.
 - (There may be some subtleties where the key does contain important evidence--perhaps the location of a buried body--but I think these issues are relatively minor.)
 - but this has not really been tested, so far as I know
 - and many people say that such cooperation can be demanded...
 - Contempt, claims of forgetting
- 10.3.5. Forgetting passwords, and testimony
- + This is another area of intense speculation:
 - "I forgot. So sue me."
 - "I forgot. It was just a temporary file I was working on, and I just can't remember the password I picked." (A less in-your-face approach.)
 - + "I refuse to give my password on the grounds that it may tend to incriminate me."
 - + Canonical example: "My password is: 'I sell illegal drugs.'"
 - Eric Hughes has pointed out this is not a real admission of guilt, just a syntactic form, so it is nonsense to claim that it is incriminating. I agree. I don't know if any court tests have confirmed this.
 - + Sandy Sandfort theorizes that this example might work, or at least lead to an interesting legal dilemma:
 - "As an example, your passphrase could be:

I shot a cop in the back and buried his body
 under
 the porch at 123 Main St., anywhere USA. The gun
 is
 wrapped in an oily cloth in my mother's attic.

"I decline to answer on the grounds that my passphrase is a statement which may tend to incriminate me. I will only give my passphrase if I am given immunity from prosecution for the actions to which it alludes."

"Too cute, I know, but who knows, it might work." [S.S., 1994-0727]

10.3.6. "What about disavowal of keys? Of digital signatures? Of contracts?"

- In the short term, the courts are relatively silent, as few of these issues have reached the courts. Things like signatures and contract breaches would likely be handled as they currently are (that is, the judge would look at the circumstances, etc.)
- + Clearly this is a major concern. There are two main avenues of dealing with this"
 - The "purist" approach. You **are** your key. Caveat emptor. Guard your keys. If your signature is used, you are responsible. (People can lessen their exposure by using protocols that limit risk, analogous to the way ATM systems only allow, say, \$200 a day to be withdrawn.)
 - The legal system can be used (maybe) to deal with these issues. Maybe. Little of this has been tested in courts. Conventional methods of verifying forged signatures will not work. Contract law with digital signatures will be a new area.
 - The problem of **repudiation** or **disavowal** was recognized early on in cryptologic circles. Alice is confronted with a digital signature, or whatever. She says; "But I didn't sign that" or "Oh, that's my old key--it's obsolete" or "My sysadmin must have snooped through my files," or "I guess those key escrow guys are at it again."
 - I think that only the purist stance will hold water in the long run. (A hint of this: untraceable cash means, for most transactions of interest with digital cash, that once the crypto stuff has been handled, whether the sig was stolen or not is moot, because the money is gone...no court can rule that the sig was invalid and then retrieve the cash!)

10.3.7. "What are some arguments for the freedom to encrypt?"

- bans are hard to enforce, requiring extensive police intrusions
- private letters, diaries, conversations
- in U.S., various provisions
- anonymity is often needed

10.3.8. Restrictions on anonymity

- "identity escrow" is what Eric Hughes calls it
- limits on mail drops, on anonymous accounts, and--perhaps ultimately--on cash purchases of any and all goods

10.3.9. "Are bulletin boards and Internet providers "common carriers" or not?"

- Not clear. BBS operators are clearly held more liable for content than the phone company is, for example.

10.3.10. Too much cleverness is passing for law

- Many schemes to bypass tax laws, regulations, etc., are, as the British like to say, "too cute by half." For example, claims that the dollar is defined as 1/35th of an ounce of gold and that the modern dollar is only 1/10th of this. Or

that Ohio failed to properly enter the Union, and hence all laws passed afterward are invalid. The same could be said of schemes to deploy digital cash be claiming that ordinary laws do not apply. Well, those who try such schemes often find out otherwise, sometimes in prison. Tread carefully.

10.3.11. "Is it legal to advocate the overthrow of governments or the breaking of laws?"

- Although many Cypherpunks are not radicals, many others of us are, and we often advocate "collapse of governments" and other such things as money laundering schemes, tax evasion, new methods for espionage, information markets, data havens, etc. This raises obvious concerns about legality.
- First off, I have to speak mainly of U.S. issues...the laws of Russia or Japan or whatever may be completely different. Sorry for the U.S.-centric focus of this FAQ, but that's the way it is. The Net started here, and still is dominantly here, and the laws of the U.S. are being propagated around the world as part of the New World Order and the collapse of the other superpower.
- Is it legal to advocate the replacement of a government? In the U.S., it's the basic political process (though cynics might argue that both parties represent the same governing philosophy). Advocating the *violent overthrow* of the U.S. government is apparently illegal, though I lack a cite on this.
- + Is it legal to advocate illegal acts in general? Certainly much of free speech is precisely this: arguing for drug use, for boycotts, etc.
- + The EFF gopher site has this on "Advocating Lawbreaking, Brandenburg v. Ohio. " :
 - "In the 1969 case of Brandenburg v. Ohio, the Supreme Court struck down the conviction of a Ku Klux Klan member under a criminal syndicalism law and established a new standard: Speech may not be suppressed or punished unless it is intended to produce 'imminent lawless action' and it is 'likely to produce such action.' Otherwise, the First Amendment protects even speech that advocates violence. The Brandenburg test is the law today. "

10.4. Can Crypto be Banned?

10.4.1. "Why won't government simply _ban such encryption methods?"

- + This has always been the Number One Issue!
 - raised by Stiegler, Drexler, Salin, and several others (and in fact raised by some as an objection to my even discussing these issues, namely, that action may then be taken to head off the world I describe)
- + Types of Bans on Encryption and Secrecy
 - Ban on Private Use of Encryption
 - Ban on Store-and-Forward Nodes
 - Ban on Tokens and ZKIPS Authentication
 - Requirement for public disclosure of all transactions
- + Recent news (3-6-92, same day as Michaelangelo and Lawnmower Man) that government is proposing a surcharge on telcos and long distance services to pay for new equipment needed to tap phones!
 - S.266 and related bills

- this was argued in terms of stopping drug dealers and other criminals
- but how does the government intend to deal with the various forms of end-user encryption or "confusion" (the confusion that will come from compression, packetizing, simple file encryption, etc.)
- + Types of Arguments Against Such Bans
 - The "Constitutional Rights" Arguments
 - + The "It's Too Late" Arguments
 - PCs are already widely scattered, running dozens of compression and encryption programs...it is far too late to insist on "in the clear" broadcasts, whatever those may be (is program code distinguishable from encrypted messages? No.)
 - encrypted faxes, modem scramblers (albeit with some restrictions)
 - wireless LANs, packets, radio, IR, compressed text and images, etc....all will defeat any efforts short of police state intervention (which may still happen)
 - + The "Feud Within the NSA" Arguments
 - COMSEC vs. PROD
 - + Will affect the privacy rights of corporations
 - and there is much evidence that corporations are in fact being spied upon, by foreign governments, by the NSA, etc.
 - + They Will Try to Ban Such Encryption Techniques
 - + Stings (perhaps using viruses and logic bombs)
 - or "barium," to trace the code
 - + Legal liability for companies that allow employees to use such methods
 - perhaps even in their own time, via the assumption that employees who use illegal software methods in their own time are perhaps couriers or agents for their corporations (a tenuous point)
- 10.4.2. The long-range impossibility of banning crypto
 - stego
 - direct broadcast to overhead satellites
 - samizdat
 - compression, algorithms,all made plaintext hard to find
- 10.4.3. Banning crypto is comparable to
 - + banning ski masks because criminals can hide their identity
 - Note: yes, there are laws about "going masked for the purpose of being masked," or somesuch
 - + insisting that all speech be in languages understandable by eavesdroppers
 - (I don't mean "official languages" for dealing with the Feds, or what employers may reasonably insist on)
 - outlawing curtains, or at least requiring that "Clipper curtains" be bought (curtains which are transparent at wavelengths the governments of the world can use)
 - position escrow, via electronic bracelets like criminals wear
 - restrictions on books that possibly help criminals
 - banning body armor (proposed in several communities)
 - banning radar detectors
 - (Note that these bans become more "reasonable" when the

items like body armor and radar detectors are reached, at least to many people. Not to me, of course.)

10.4.4. So Won't Governments Stop These Systems?

- Citing national security, protection of private property, common decency, etc.
- + Legal Measures
 - Bans on ownership and operation of "anonymous" systems
- + Restrictions on cryptographic algorithms
 - RSA patent may be a start
- + RICO, civil suits, money-laundering laws
 - FINCEN, Financial Crimes Information Center
 - IRS, Justice, NSA, FBI, DIA, CIA
 - attempts to force other countries to comply with U.S. banking laws

10.4.5. Scenario for a ban on encryption

- "Paranoia is cryptography's occupational hazard." [Eric Hughes, 1994-05-14]
- + There are many scenarios. Here is a graphic one from Sandy Sandfort:
 - "Remember the instructions for cooking a live frog. The government does not intend to stop until they have effectively eliminated your privacy.

STEP 1: Clipper becomes the de facto encryption standard.

STEP 2: When Cypherpunks and other "criminals" eschew Clipper in favor of trusted strong crypto, the government is "forced" to ban non-escrowed encryption systems. (Gotta catch those pedophiles, drug dealers and terrorists, after all.)

STEP 3: When Cypherpunks and other criminals use superencryption with Clipper or spoof LEAFs, the government will regretably be forced to engage in random message monitoring to detect these illegal techniques.

Each of these steps will be taken because we wouldn't passively accept such things as unrestricted wiretaps and reasonable precautions like digital telephony. It will be portrayed as our fault. Count on it." [Sandy Sandfort, 6-14-94]

10.4.6. Can the flow of bits be stopped? Is the genie really out of the bottle?

- Note that Carl Ellison has long argued that the genie was never in the bottle, at least not in the U.S. in non-wartime situations (use of cryptography, especially in communications, in wartime obviously raises eyebrows)

10.5. Legal Issues with PGP

7.12.1. "What is RSA Data Security Inc.'s position on PGP?"

- I. They were strongly opposed to early versions
- II. objections
 - infringes on PKP patents (claimed infringements, not tested in court, though)
 - breaks the tight control previously seen

- brings unwanted attention to public key approaches (I think PGP also helped RSA and RSADSI)
- bad blood between Zimmermann and Bidzos

III. objections

- infringes on PKP patents (claimed infringements, not tested in court, though)
- breaks the tight control previously seen
- brings unwanted attention to public key approaches (I think PGP also helped RSA and RSADSI)
- bad blood between Zimmermann and Bidzos

IV. Talk of lawsuits, actions, etc.

- V. The 2.6 MIT accommodation may have lessened the tension; purely speculative

7.12.2. "Is PGP legal or illegal"?

7.12.3. "Is there still a conflict between RSADSI and PRZ?"

- Apparently not. The MIT 2.6 negotiations seem to have buried all such rancor. At least officially. I hear there's still animosity, but it's no longer at the surface. (And RSADSI is now facing lawsuits and patent suits.)

10.6. Legal Issues with Remailers

8.9.1. What's the legal status of remailers?

- There are no laws against it at this time.
- No laws saying people have to put return addresses on messages, on phone calls (pay phones are still legal), etc.
- And the laws pertaining to not having to produce identity (the "flier" case, where leaflet distributors did not have to produce ID) would seem to apply to this form of communication.

+ However, remailers may come under fire:

+ Sysops, MIT case

- potentially serious for remailers if the case is decided such that the sysop's creation of group that was conducive to criminal pirating was itself a crime...that could make all involved in remailers culpable

8.9.2. "Can remailer logs be subpoenaed?"

- Count on it happening, perhaps very soon. The FBI has been subpoenaing e-mail archives for a Netcom customer (Lewis De Payne), probably because they think the e-mail will lead them to the location of uber-hacker Kevin Mitnick. Had the parties used remailers, I'm fairly sure we'd be seeing similar subpoenas for the remailer logs.

- There's no exemption for remailers that I know of!

+ The solutions are obvious, though:

- use many remailers, to make subpoenaing back through the chain very laborious, very expensive, and likely to fail (if even one party won't cooperate, or is outside the court's jurisdiction, etc.)
- offshore, multi-jurisdictional remailers (selected by the user)
- no remailer logs kept...destroy them (no law currently says anybody has to keep e-mail records! This may change....)
- "forward secrecy," a la Diffie-Hellman forward secrecy

8.9.3. How will remailers be harassed, attacked, and challenged?

8.9.4. "Can pressure be put on remailer operators to reveal traffic

logs and thereby allow tracing of messages?"

+ For human-operated systems which have logs, sure. This is why we want several things in remailers:

- * no logs of messages
- * many remailers
- * multiple legal jurisdictions, e.g., offshore remailers (the more the better)
- * hardware implementations which execute instructions flawlessly (Chaum's digital mix)

8.9.5. Calls for limits on anonymity

- + Kids and the net will cause many to call for limits on nets, on anonymity, etc.
 - "But there's a dark side to this exciting phenomenon, one that's too rarely understood by computer novices. Because they offer instant access to others, and considerable anonymity to participants, the services make it possible for people - especially computer-literate kids - to find themselves in unpleasant, sexually explicit social situations.... And I've gradually come to adopt the view, which will be controversial among many online users, that the use of nicknames and other forms of anonymity must be eliminated or severely curbed to force people online into at least as much accountability for their words and actions as exists in real social encounters." [Walter S. Mossberg, Wall Street Journal, 6/30/94, provided by Brad Dolan]
 - Eli Brandt came up with a good response to this: "The sound-bite response to this: do you want your child's name, home address, and phone number available to all those lurking pedophiles worldwide? Responsible parents encourage their children to use remailers."
 - Supreme Court said that identity of handbill distributors need not be disclosed, and pseudonyms in general has a long and noble tradition
 - BBS operators have First Amendment protections (e.g.. registration requirements would be tossed out, exactly as if registration of newspapers were to be attempted)

8.9.6. Remailers and Choice of Jurisdictions

- The intended target of a remailed message, and the subject material, may well influence the set of remailers used, especially for the very important "last remailer" (Note: it should never be necessary to tell remailers if they are first, last, or others, but the last remailer may in fact be able to tell he's the last...if the message is in plaintext to the recipient, with no additional remailer commands embedded, for example.)
- A message involving child pornography might have a remailer site located in a state like Denmark, where child porn laws are less restrictive. And a message critical of Islam might not be best sent through a final remailer in Teheran. Eric Hughes has dubbed this "regulatory arbitrage," and to various extents it is already common practice.

- Of course, the sender picks the remailer chain, so these common sense notions may not be followed. Nothing is perfect, and customs will evolve. I can imagine schemes developing for choosing customers--a remailer might not accept as a customer certain abusers, based on digital pseudonyms < hairy).
- 8.9.7. Possible legal steps to limit the use of remailers and anonymous systems
 - hold the remailer liable for content, i.e., no common carrier status
 - insert provisions into the various "anti-hacking" laws to criminalize anonymous posts
- 8.9.8. Crypto and remailers can be used to protect groups from "deep pockets" lawsuits
 - products (esp. software) can be sold "as is," or with contracts backed up by escrow services (code kept in an escrow repository, or money kept there to back up commitments)
 - + jurisdictions, legal and tax, cannot do "reach backs" which expose the groups to more than they agreed to
 - as is so often the case with corporations in the real world, which are taxed and fined for various purposes (asbestos, etc.)
 - (For those who panic at the thought of this, the remedy for the cautious will be to arrange contracts with the right entities...probably paying more for less product.)
- 8.9.9. Could anonymous remailers be used to entrap people, or to gather information for investigations?
 - First, there are so few current remailers that this is unlikely. Julf seems a non-narc type, and he is located in Finland. The Cypherpunks remailers are mostly run by folks like us, for now.
 - However, such stings and set-ups have been used in the past by narcs and "red squads." Expect the worse from Mr. Policeman. Now that evil hackers are identified as hazards, expect moves in this direction. "Cryps" are obviously "crack" dealers.
 - But use of encryption, which CP remailers support (Julf's does not), makes this essentially moot.
- 10.7. Legal Issues with Escrowed Encryption and Clipper
 - 9.17.1. As John Gilmore put it in a guest editorial in the "San Francisco Examiner," "...we want the public to see a serious debate about why the Constitution should be burned in order to save the country." [J.G., 1994-06-26, quoted by S. Sandfort]
 - 9.17.2. "I don't see how Clipper gives the government any powers or capabilities it doesn't already have. Comments?"
 - 9.17.3. Is Clipper really voluntary?
 - 9.17.4. If Clipper is voluntary, who will use it?
 - 9.17.5. Restrictions on Civilian Use of Crypto
 - 9.17.6. "Has crypto been restricted in the U.S.?"
 - 9.17.7. "What legal steps are being taken?"
 - Zimmermann
 - ITAR
 - 9.17.8. reports that Department of Justice has a compliance enforcement role in the EES [heard by someone from Dorothy

Denning, 1994-07], probably involving checking the law enforcement agencies...

9.17.9. Status

- + "Will government agencies use Clipper?"
 - Ah, the embarrassing question. They claim they will, but there are also reports that sensitive agencies will not use it, that Clipper is too insecure for them (key length, compromise of escrow data, etc.). There may also be different procedures (all agencies are equal, but some are more equal than others).
 - Clipper is rated for unclassified use, so this rules out many agencies and many uses. An interesting double standard.
- + "Is the Administration backing away from Clipper?"
 - + industry opposition surprised them
 - groups last summer, Citicorp, etc.
 - public opinion
 - editorial remarks
 - so they may be preparing alternative
 - and Gilmore's FOIA, Blaze's attack, the Denning nonreview, the secrecy of the algorithm
 - + will not work
 - spies won't use it, child pornographers probably won't use it (if alternatives exist, which may be the whole point)
 - terrorists won't use it
 - Is Clipper in trouble?

9.17.10. "Will Clipper be voluntary?"

- Many supporters of Clipper have cited the voluntary nature of Clipper--as expressed in some policy statements--and have used this to counter criticism.
- + However, even if truly voluntary, some issues
 - + improper role for government to try to create a commercial standard
 - though the NIST role can be used to counter this point, partly
 - government can and does make it tough for competitors
 - export controls (statements by officials on this exist)
- + Cites for voluntary status:
 - original statement says it will be voluntary
 - (need to get some statements here)
- + Cites for eventual mandatory status:
 - "Without this initiative, the government will eventually become helpless to defend the nation." [Louis Freeh, director of the FBI, various sources]
 - Steven Walker of Trusted Information Systems is one of many who think so: "Based on his analysis, Walker added, 'I'm convinced that five years from now they'll say 'This isn't working,' so we'll have to change the rules.'" Then, he predicted, Clipper will be made mandatory for all encoded communications." [
- + Parallels to other voluntary programs
 - taxes

10.8. Legal Issues with Digital Cash

10.8.1. "What's the legal status of digital cash?"

- It hasn't been tested, like a lot of crypto protocols. It

- may be many years before these systems are tested.
- 10.8.2. "Is there a tie between digital cash and money laundering?"
- There doesn't have to be, but many of us believe the widespread deployment of digital, untraceable cash will make possible new approaches
 - Hence the importance of digital cash for crypto anarchy and related ideas.
 - (In case it isn't obvious, I consider money-laundering a non-crime.)
- 10.8.3. "Is it true the government of the U.S. can limit funds transfers outside the U.S.?"
- Many issues here. Certainly some laws exist. Certainly people are prosecuted every day for violating currency export laws. Many avenues exist.
 - "LEGALITY - There isn't and will never be a law restricting the sending of funds outside the United States. How do I know? Simple. As a country dependant on international trade (billions of dollars a year and counting), the American economy would be destroyed." [David Johnson, privacy@well.sf.ca.us, "Offshore Banking & Privacy," alt.privacy, 1994-07-05]
- 10.8.4. "Are "alternative currencies" allowed in the U.S.? And what's the implication for digital cash of various forms?"
- Tokens, coupons, gift certificates are allowed, but face various regulations. Casino chips were once treated as cash, but are now more regulated (inter-casino conversion is no longer allowed).
 - Any attempt to use such coupons as an alternative currency face obstacles. The coupons may be allowed, but heavily regulated (reporting requirements, etc.).
 - Perry Metzger notes, bearer bonds are now illegal in the U.S. (a bearer bond represented cash, in that no name was attached to the bond--the "bearer" could sell it for cash or redeem it...worked great for transporting large amounts of cash in compact form).
- + Note: Duncan Frissell claims that bearer bonds are not illegal.
- "Under the Tax Equity and Fiscal Responsibility Act of 1982 (TEFRA), any interest payments made on **new** issues of domestic bearer bonds are not deductible as an ordinary and necessary business expense so none have been issued since then. At the same time, the Feds administratively stopped issuing treasury securities in bearer form. Old issues of government and corporate debt in bearer form still exist and will exist and trade for 30 or more years after 1982. Additionally, US residents can legally buy foreign bearer securities." [Duncan Frissell, 1994-08-10]
 - Someone else has a slightly different view: "The last US Bearer Bond issues mature in 1997. I also believe that to collect interest, and to redeem the bond at maturity, you must give your name and tax-id number to the paying agent. (I can check with the department here that handles it if anyone is interested in the pertinent OCC regs that apply)" [prig0011@gold.tc.umn.edu, 1994-08-10]
 - I cite this gory detail to give readers some idea about how much confusion there is about these subjects. The

usual advice is to "seek competent counsel," but in fact most lawyers have no clear ideas about the optimum strategies, and the run-of-the-mill advisor may mislead one dangerously. Tread carefully.

- This has implications for digital cash, of course.

10.8.5. "Why might digital cash and related technologies take hold early in illegal markets? That is, will the Mob be an early adopter?"

- untraceability needed

- and reputations matter to them

- they've shown in the past that they will try new approaches, a la the money movements of the drug cartels, novel methods for security, etc.

10.8.6. "Electronic cash...will it have to comply with laws, and how?"

- Concerns will be raised about the anonymity aspects, the usefulness for evading taxes and reporting requirements, etc.

- a messy issue, sure to be debated and legislated about for many years

+ split the cash into many pieces...is this "structuring"? is it legal?

- some rules indicate the structuring per se is not

illegal, only tax evasion or currency control evasion

- what then of systems which automatically, as a basic feature, split the cash up into multiple pieces and move them?

10.8.7. Currency controls, flight capital regulations, boycotts, asset seizures, etc.

- all are pressures to find alternate ways for capital to flow

- all add to the lack of confidence, which, paradoxically to lawmakers, makes capital flight all the more likely

10.8.8. "Will banking regulators allow digital cash?"

- Not easily, that's for sure. The maze of regulations, restrictions, tax laws, and legal rulings is daunting. Eric Hughes spent a lot of time reading up on the laws regarding banks, commercial paper, taxes, etc., and concluded much the same. I'm not saying it's impossible--indeed, I believe it will someday happen, in some form--but the obstacles are formidable.

+ Some issues:

+ Will such an operation be allowed to be centered or based in the U.S.?

- What states? What laws? Bank vs. Savings and Loan vs.

Credit Union vs. Securities Broker vs. something else?

+ Will customers be able to access such entities offshore, outside the U.S.?

- strong crypto makes communication possible, but it may be difficult, not part of the business fabric, etc.

(and hence not so useful--if one has to send PGP-encrypted instructions to one's banker, and can't use the clearing infrastructure....)

+ Tax collection, money-laundering laws, disclosure laws,

"know your customer" laws....all are areas where a

"digital bank" could be shut down forthwith. Any bank not filling out the proper forms (including mandatory

- reporting of transactions of certain amounts and types, and the Social Security/Taxpayer Number of customers) faces huge fines, penalties, and regulatory sanctions.
 - and the existing players in the banking and securities business will not sit idly by while newcomers enter their market; they will seek to force newcomers to jump through the same hoops they had to (studies indicate large corporations actually like red tape, as it helps them relative to smaller companies)
 - Conclusion: Digital banks will not be "launched" without a *lot* of work by lawyers, accountants, tax experts, lobbyists, etc. "Lemonade stand digital banks" (TM) will not survive for long. Kids, don't try this at home!
 - (Many new industries we are familiar with--software, microcomputers--had very little regulation, rightly so. But the effect is that many of us are unprepared to understand the massive amount of red tape which businesses in other areas, notably banking, face.)
- 10.8.9. Legal obstacles to digital money. If governments don't want anonymous cash, they can make things tough.
- + As both Perry Metzger and Eric Hughes have said many times, regulations can make life very difficult. Compliance with laws is a major cost of doing business.
 - ~"The cost of compliance in a typical USA bank is 14% of operating costs."~ [Eric Hughes, citing an "American Banker" article, 1994-08-30]
 - + The maze of regulations is navigable by larger institutions, with staffs of lawyers, accountants, tax specialists, etc., but is essentially beyond the capabilities of very small institutions, at least in the U.S.
 - this may or may not remain the case, as computers proliferate. A "bank-in-a-box" program might help. My suspicion is that a certain size of staff is needed just to handle the face-to-face meetings and hoop-jumping.
 - + "New World Order"
 - U.S. urging other countries to "play ball" on banking secrecy, on tax evasion extradition, on immigration, etc.
 - this is closing off the former loopholes and escape hatches that allowed people to escape repressive taxation...the implications for digital money banks are unclear, but worrisome.
- 10.9. Legality of Digital Banks and Digital Cash?
- 10.9.1. In terms of banking laws, cash reporting regulations, money laundering statutes, and the welter of laws connected with financial transactions of all sorts, the Cypherpunks themes and ideas are basically illegal. Illegal in the sense that anyone trying to set up his own bank, or alternative currency system, or the like would be shut down quickly. As an informal, unnoticed experiment, such things are reasonably safe...until they get noticed.
- 10.9.2. The operative word here is "launch," in my opinion. The "launch" of the BankAmericard (now VISA) in the 1960s was not done lightly or casually...it required armies of lawyers, accountants, and other bureaucrats to make the launch both legal and successful. The mere "idea" of a credit card was

not enough...that was essentially the easiest part of it all.
(Anyone contemplating the launch of a digital cash system would do well to study BankAmericard as an example...and several other examples also.)

10.9.3. The same will be true of any digital cash or similar system which intends to operate more or less openly, to interface with existing financial institutions, and which is not explicitly intended to be a Cypherpunkish underground activity.

10.10. Export of Crypto, ITAR, and Similar Laws

10.10.1. "What are the laws and regulations about export of crypto, and where can I find more information?"

- "The short answer is that the Department of State, Office of Defense Trade Controls (DOS/DTC) and the National Security Administration (NSA) won't allow unrestricted export (like is being done with WinCrypt) for any encryption program that the NSA can't crack with less than a certain amount (that they are loathe to reveal) of effort. For the long answer, see <ftp://ftp.csn.net/cryptusa.txt.gz> and/or call DOS/DTC at 703-875-7041." [Michael Paul Johnson, sci.crypt, 1994-07-08]

10.10.2. "Is it illegal to send encrypted stuff out of the U.S.?"

- This has come up several times, with folks claiming they've heard this.
- In times of war, real war, sending encrypted messages may indeed be suspect, perhaps even illegal.
- But the U.S. currently has no such laws, and many of us send lots of encrypted stuff outside the U.S. To remailers, to friends, etc.
- Encrypted files are often tough to distinguish from ordinary compressed files (high entropy), so law enforcement would have a hard time.
- However, other countries may have different laws.

10.10.3. "What's the situation about export of crypto?"

- + There's been much debate about this, with the case of Phil Zimmermann possibly being an important test case, should charges be filed.
- as of 1994-09, the Grand Jury in San Jose has not said anything (it's been about 7-9 months since they started on this issue)
- Dan Bernstein has argued that ITAR covers nearly all aspects of exporting crypto material, including codes, documentation, and even "knowledge." (Controversially, it may be in violation of ITAR for knowledgeable crypto people to even leave the country with the intention of developing crypto tools overseas.)
- The various distributions of PGP that have occurred via anonymous ftp sources don't imply that ITAR is not being enforced, or won't be in the future.

10.10.4. Why and How Crypto is Not the Same as Armaments

- the gun comparison has advantages and disadvantages
- "right to keep and bear arms"
- but then this opens the door wide to restrictions, regulations, comparisons of crypto to nuclear weapons, etc.

-

- + "Crypto is not capable of killing people directly. Crypto consists
 - entirely of information (speech, if you must) that cannot be
 - interdicted. Crypto has civilian use.
 - -
 - <Robert Krawitz <rlk@think.com>, 4-11-94, sci.crypt>
- 10.10.5. "What's ITAR and what does it cover?"
 - + ITAR, the International Trafficking in Arms Regulations, is the defining set of rules for export of munitions--and crypto is treated as munitions.
 - regulations for interpreting export laws
 - + NSA may have doubts that ITAR would hold up in court
 - Some might argue that this contravenes the Constitution, and hence would fail in court. Again, there have been few if any solid tests of ITAR in court, and some indications that NSA lawyers are reluctant to see it tested, fearing it would not pass muster.
 - doubts about legality (Carl Nicolai saw papers, since confirmed in a FOIA)
 - Brooks statement
 - Cantwell Bill
 - not fully tested in court
 - + reports of NSA worries that it wouldn't hold up in court if ever challenged
 - Carl Nicolai, later FOIA results, conversations with Phil
 - + Legal Actions Surrounding ITAR
 - The ITAR laws may be used to fight hackers and Cypherpunks...the outcome of the Zimmermann indictment will be an important sign.
 - + What ITAR covers
 - "ITAR 121.8(f): ``Software includes but is not limited to the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test, operation, diagnosis and repair.' ' [quoted by Dan Bernstein, talk.politics.crypto, 1994-07-14]
 - joke by Bidzos about registering as an international arms dealer
 - + ITAR and code (can code be published on the Net?)
 - "Why does ITAR matter?"
 - Phil Karn is involved with this, as are several others here
 - + Dan Bernstein has some strongly held views, based on his long history of fighting the ITAR
 - "Let's assume that the algorithm is capable of maintaining secrecy of information, and that it is not restricted to decryption, banking, analog scrambling, special smart cards, user authentication, data authentication, data compression, or virus protection.
 - "The algorithm is then in USML Category XIII(b) (1).
 - "It is thus a defense article. ITAR 120.6. " [Dan Bernstein, posting code to sci.crypt, talk.politics.crypto, 1994-08-22]
 - "Sending a defense article out of the United States in

any manner (except as knowledge in your head) is export. ITAR 120.17(1).

"So posting the algorithm constitutes export. There are other forms of export, but I won't go into them here.

"The algorithm itself, without any source code, is software." [Dan Bernstein, posting code to sci.crypt, talk.politics.crypto, 1994-08-22]

- "The statute is the Arms Export Control Act; the regulations are the International Traffic in Arms Regulations. For precise references, see my ``International Traffic in Arms Regulations: A Publisher's Guide.''' [Dan Bernstein, posting code to sci.crypt, talk.politics.crypto, 1994-08-22]
- + "Posting code is fine. We do it all the time; we have the right to do it; no one seems to be trying to stop us from doing it." [Bryan G. Olson, posting code to sci.crypt, talk.politics.crypto, 1994-08-20]
- Bernstein agrees that few busts have occurred, but warns: "Thousands of people have distributed crypto in violation of ITAR; only two, to my knowledge, have been convicted. On the other hand, the gov'mint is rapidly catching up with reality, and the Phil Zimmermann case may be the start of a serious crackdown." [Dan Bernstein, posting code to sci.crypt, talk.politics.crypto, 1994-08-22]
- The common view that academic freedom means one is OK is probably not true.
- + Hal Finney neatly summarized the debate between Bernstein and Olsen:
 - "1) No one has ever been prosecuted for posting code on sci.crypt. The Zimmermann case, if anything ever comes of it, was not about posting code on Usenet, AFAIK.

"2) No relevant government official has publically expressed an opinion on whether posting code on sci.crypt would be legal. The conversations Dan Bernstein posted dealt with his requests for permission to export his algorithm, not to post code on sci.crypt.

"3) We don't know whether anyone will ever be prosecuted for posting code on sci.crypt, and we don't know what the outcome of any such prosecution would be." [Hal Finney, talk.politics.crypto, 1994-008-30]

10.10.6. "Can ITAR and other export laws be bypassed or skirted by doing development offshore and then importing strong crypto into the U.S.?"

- IBM is reportedly doing just this: developing strong crypto products for OS/2 at its overseas labs, thus skirting the export laws (which have weakened the keys to some of their network security products to the 40 bits that are allowed).
- + Some problems:
 - can't send docs and knowhow to offshore facilities (some obvious enforcement problems, but this is how the law reads)

- may not even be able to transfer knowledgeable people to offshore facilities, if the chief intent is to then have them develop crypto products offshore (some deep Constitutional issues, I would think...some shades of how the U.S.S.R. justified denying departure visas for "needed" workers)
- As with so many cases involving crypto, there are no defining legal cases that I am aware of.

10.11. Regulatory Arbitrage

- 10.11.1. Jurisdictions with more favorable laws will see claimants going there.
- 10.11.2. Similar to "capital flight" and "people voting with their feet."
- 10.11.3. Is the flip side of "jurisdiction shopping." wherein prosecutors shop around for a jurisdiction that will be likelier to convict. (As with the Amateur Action BBS case, tried in Memphis, Tennessee, not in California.)

10.12. Crypto and Pornography

- 10.12.1. There's been a lot of media attention given to this, especially pedophilia (pedophilia is not the same thing as porn, of course, but the two are often discussed in articles about the Net). As Rishab Ghosh put it: "I think the pedophilic possibilities of the Internet capture the imaginations of the media -- their deepest desires, perhaps." [R.G., 1994-07-01]
- 10.12.2. The fact is, the two are made for each other. The untraceability of remailers, the unbreakability of strong crypto if the files are intercepted by law enforcement, and the ability to pay anonymously, all mean the early users of commercial remailers will likely be these folks.
- 10.12.3. Avoid embarrassing stings! Keep your job at the elementary school! Get re-elected to the church council!
- 10.12.4. pedophilia, bestiality, etc. (morphed images)
- 10.12.5. Amateur Action BBS operator interested in crypto....a little bit too late
- 10.12.6. There are new prospects for delivery of messages as part of stings or entrapment attacks, where the bits decrypt into incriminating evidence when the right key is used. (XOR of course)
- 10.12.7. Just as the law enforcement folks are claiming, strong crypto and remailers will make new kinds of porn networks. The nexus or source will not be known, and the customers will not be known.
 - (An interesting strategy: claim customers unknown, and their local laws. Make the "pickup" the customer's responsibility (perhaps via agents).

10.13. Usenet, Libel, Local Laws, Jurisdictions, etc.

- 10.13.1. (Of peripheral importance to crypto themes, but important for issues of coming legislation about the Net, attempts to "regain control," etc. And a bit of a jumble of ideas, too.)
- 10.13.2. Many countries, many laws. Much of Usenet traffic presumably violates various laws in Iran, China, France, Zaire, and the U.S., to name a few places which have laws about what thoughts can be expressed.

- 10.13.3. Will this ever result in attempts to shut down Usenet, or at least the feeds into various countries?
- 10.13.4. On the subject of Usenet possibly being shut-down in the U.K. (a recent rumor, unsubstantiated), this comment: " What you have to grasp is that USENET type networks and the whole structure of the law on publishing are fundamentally incompatible. With USENET anyone can untracably distribute pornographic, libelous, blasphemous, copyright or even officially secret information. Now, which do you think HMG and, for that matter, the overwhelming majority of ordinary people in this country think is most important. USENET or those laws?" [Malcolm McMahon, malcolm@geog.leeds.ac.uk, comp.org.eff.talk, 1994--08-26]
- 10.13.5. Will it succeed? Not completely, as e-mail, gopher, the Web, etc., still offers access. But the effects could reach most casual users, and certainly affect the structure as we know it today.
- 10.13.6. Will crypto help? Not directly--see above.
- 10.14. Emergency Regulations
- 10.14.1. Emergency Orders
- various NSDDs and the like
 - "Seven Days in May" scenario
- 10.14.2. Legal, secrecy orders
- George Davida, U. of Wisconsin, received letter in 1978 threatening a \$10K per day fine
 - Carl Nicolai, PhasorPhone
 - The NSA has confirmed that parts of the EES are patented, in secrecy, and that the patents will be made public and then used to stop competitors should the algorithm become known.
- 10.14.3. Can the FCC-type Requirements for "In the clear" broadcasting (or keys supplied to Feds) be a basis for similar legislation of private networks and private use of encryption?
- this would seem to be impractical, given the growth of cellular phones, wireless LANs, etc....can't very well mandate that corporations broadcast their internal communications in the clear!
 - compression, packet-switching, and all kinds of other "distortions" of the data...requiring transmissions to be readable by government agencies would require providing the government with maps (of where the packets are going), with specific decompression algorithms, etc....very impractical
- 10.15. Patents and Copyrights
- 10.15.1. The web of patents
- what happens is that everyone doing anything substantive spends much of his time and money seeking patents
 - patents are essential bargaining chips in dealing with others
 - e.g., DSS, Schnorr, RSADSI, etc.
 - e.g., Stefan Brands is seeking patents
 - Cylink suing...
- 10.15.2. Role of RSA, Patents, etc.
- + Bidzos: "If you make money off RSA, we make money" is the simple rule
 - but of course it goes beyond this, as even "free" uses

- may have to pay
- Overlapping patents being used (apparently) to extent the life of the portfolio
- + 4/28/97 The first of several P-K and RSA patents expires
 - + U.S. Patent Number: 4200770
 - Title: Cryptographic Apparatus and Method
 - Inventors: Hellman, Diffie, Merkle
 - Assignee: Stanford University
 - Filed: September 6, 1977
 - Granted: April 29, 1980
 - [Expires: April 28, 1997]
 - + remember that any one of these several patents held by Public Key Partners (Stanford and M.I.T., with RSA Data Security the chief dispenser of licenses) can block an effort to bypass the others
 - though this may get fought out in court
- + 8/18/97 The second of several P-K and RSA patents expires
 - + U.S. Patent Number: 4218582
 - Title: Public Key Cryptographic Apparatus and Method
 - Inventors: Hellman, Merkle
 - Assignee: The Board of Trustees of the Leland Stanford Junior University
 - Filed: October 6, 1977
 - Granted: August 19, 1980
 - [Expires: August 18, 1997]
 - this may be disputed because it describe algortihms in broad terms and used the knapsack algorithm as the chief example
- + 9/19/00 The main RSA patent expires
 - + U.S. Patent Number: 4405829
 - Title: Cryptographic Communications System and Method
 - Inventors: Rivest, Shamir, Adleman
 - Assignee: Massachusetts Institute of Technology
 - Filed: December 14, 1977
 - Granted: September 20, 1983
 - [Expires: September 19, 2000]
- 10.15.3. Lawsuits against RSA patents
 - + several are brewing
 - Cylink is suing (strange rumors that NSA was involved)
 - Roger Schlafly
- 10.15.4. "What about the lawsuit filed by Cylink against RSA Data Security Inc.?"
 - Very curious, considering they are both part of Public Key Partners, the consortium of Stanford, MIT, Cylink, and RSA Data Security Inc. (RSADSI)
 - the suit was filed in the summer of 1994
 - + One odd rumor I heard, from a reputable source, was that the NSA had asked PKP to do something (?) and that Cylink had agreed, but RSADSI had refused, helping to push the suit along
 - any links with the death threats against Bidzos?
- 10.15.5. "Can the patent system be used to block government use of patents for purposes we don't like?"
 - Comes up especially in the context of S. Micali's patent on escrow techniques
 - "Wouldn't matter. The government can't be enjoined from using a patent. The federal government, in the final

analysis, can use any patent they want, without permission, and the only recourse of the patent owner is to sue for royalties in the Court of Claims." [Bill Larkins, talk.politics.crypto, 1994-07-14]

10.16. Practical Issues

10.16.1. "What if I tell the authorities I Forgot My Password?"

- (or key, or passphrase...you get the idea)
- This comes up repeatedly, but the answer remains murky

10.16.2. Civil vs. Criminal

- + "This is a civil matter, and the rights of private one have in criminal matter
 - tend to vanish in civil litigation. The parties to a lawsuit hate
 - tremendous power to do as they please to petition judicial power
 - to the state, <@pad Templeton, 4-1-94, aomp, opg, edd, tal

10.16.3. the law is essentially what the courts say it is

10.17. Free Speech is Under Assault

10.17.1. Censorship comes in many forms. Tort law, threats of grant or contract removal, all are limiting speech. (More reasons for anonymous speech, of course.)

10.17.2. Discussions of cryptography could be targets of future crackdowns. Sedition laws, conspiracy laws, RICO, etc. How long before speaking on these matters earns a warning letter from your university or your company? (It's the "big stick" of ultimate government action that spurs these university and company policies. Apple fears being shut down for having "involvement" with a terrorist plot, Emory University fears being sued for millions of dollars for "conspiring" to degrade women of color, etc.)

How long before "rec.guns" is no longer carried at many sites, as they fear having their universities or companies linked to discussions of "assault weapons" and "cop-killer bullets"? Prediction: Many companies and universities, under pressure from the Feds, will block groups in which encrypted files are posted. After all, if one encrypts, one must have something to hide, and that could expose the university to legal action from some group that feels aggrieved.

10.17.3. Free speech is under assault across the country. The tort system is being abused to stifle dissenting views (and lest you think I am only a capitalist, only a free marketer, the use of "SLAPP suits"--"Strategic Lawsuits Against Public Participation"--by corporations or real estate developers to threaten those who dare to publicly speak against their projects is a travesty, a travesty that the courts have only recently begun to correct).

We are becoming a nation of sheep, fearing the midnight raid, the knock on the door. We fear that if we tell a joke, someone will glare at us and threaten to sue us and our company! And so companies are adopting "speech codes" and other such baggage of the Orwell's totalitarian state. Political correctness is extending its tendrils into nearly every aspect of life in America.

10.18. Systems, Access, and the Law

10.18.1. Legal issues regarding access to systems

+ Concerns:

- access by minors to sexually explicit material
- + access from regions where access "should not be permitted"
 - export of crypto, for example
 - the Memphis access to California BBS

+ Current approach: taking the promise of the accessor

- "I will not export this outside the U.S. or Canada."
- "I am of legal age to access this material."

+ Possible future approaches:

- + Callbacks, to ensure accessor is from region stated
 - easy enough to bypass with cut-outs and remailers

+ "Credentials"

- a la the US Postal Service's proposed ID card (and others)

+ cryptographically authenticated credentials

- Chaum's credentials system (certainly better than many non-privacy-preserving credentials systems)

10.18.2. "What is a "common carrier" and how does a service become one?"

- (This topic has significance for crypto and remailers, vis a vis whether remailers are to be treated as common carriers.)
- Common carriers are what the phone and package delivery services are. They are not held liable for the contents of phone calls, for the contents of packages (drugs, pornography, etc.), or for illegal acts connected with their services. One of the deals is that common carriers not examine the insides of packages. Common carriers essentially agree to take all traffic that pays the fee and not to discriminate based on content. Thus, a phone service will not ask what the subject of a call is to be, or listen in, to decide whether to make the connection.
- Some say that to be a common carrier requires a willingness to work with law enforcement. That is, Federal Express is not responsible for contents of packages, but they have to cooperate in reasonable ways with law enforcement to open or track suspicious packages. Anybody have a cite for this? Is it true?
- Common carrier status is also cited for bookstores, which are not presumed to have read each and every one of the books they sell...so if somebody blows their hand off in a an experiment, the bookstore is not liable. (The author/publisher may be, but that's a ~~ant~~ issue.)
- How does one become a common carrier? Not clear. One view is that a service should "behave like" a common carrier and then hope and pray that a court sees it that way.
- + Are computer services common carriers? A topic of great interest.
 - "According to a discussion I had with Dave Lawrence (postmaster at UUNET, as well as moderator of news.admin.newgroups), UUNET is registered with the FCC as an "Enhanced Service Provider," which, according to Dave, amounts to similar protection as "Common Carrier."

("Common Carrier" seems to not be appropriate yet, since Congress is so behind the tech curve)." [L. Todd Masco, 1994-08-11]

- As for remailer networks being treated as common carriers, totally unclear at this time. Certainly the fact that packets are fully encrypted and unreadable goes to part of the issue about agreeing not to screen.
- + More on the common carrier debate:
 - "Ah, the eternal Common Carrier debate. The answer is the same as the last few times. "Common Carrier" status has little to do with exemption from liability. It has most to do with being unable to reject passengers, goods, or phone calls.....Plenty of non-common carrier entities are immune from prosecution for ideas that they unknowingly communicate -- bookstores for example (unless they are *knowingly* porno bookstores in the wrong jurisdiction)....Compuserve was held not liable for an (alleged) libel by one of its sysops. Not because of common carrier but because they had no knowledge or control....Remailers have no knowledge or control hence no scienter (guilty knowledge) hence no liability as a matter of law--not a jury question BTW." [Duncan Frissell, 1994-08-11]

10.19. Credentials

- 10.19.1. "Are credentials needed? Will digital methods be used?"
- 10.19.2. I take a radical view. Ask yourself why credentials are ever needed. Maybe for driving a car, and the like, but in those cases anonymity is not needed, as the person is in the car, etc.

Credentials for drinking age? Why? Let the parents enforce this, as the argument goes about watching sex and violence on t.v. (If one accepts the logic of requiring bars to enforce children's behavior, then one is on a slippery slope toward requiring television set makers to check smartcards of viewers, or of requiring a license to access the Internet, etc.)

In almost no cases do I see the need to carry "papers" with me. Maybe a driver's license, like I said. In other areas, why?

- 10.19.3. So Cypherpunks probably should not spend too much time worrying about how permission slips and "hall passes" will be handled. Little need for them.
- 10.19.4. "What about credentials for specific job performance, or for establishing time-based contracts?"
 - Credentials that prove one has completed certain classes, or reached certain skill levels, etc.?
 - In transactions where "future performance" is needed, as in a contract to have a house built, or to do some similar job, then of course the idea of on-line or immediate clearing is bogus...like paying a stranger a sum of money on his promise that he'll be back the next day to start building you a house.

Parties to such long-term, non-locally-cleared cases may

contract with an escrow agent, as I described above. This is like the "privately-produced law" we've discussed so many times. The essence: voluntary arrangements.

Maybe proofs of identity will be needed, or asked for, maybe not. But these are not the essence of the deal.

10.20. Escrow Agents

10.20.1. (the main discussion of this is under Crypto Anarchy)

10.20.2. Escrow Agents as a way to deal with contract renegeing

- On-line clearing has the possible danger implicit in all trades that Alice will hand over the money, Bob will verify that it has cleared into his account (in older terms, Bob would await word that his Swiss bank account has just been credited), and then Bob will fail to complete his end of the bargain. If the transaction is truly anonymous, over computer lines, then of course Bob just hangs up his modem and the connection is broken. This situation is as old as time, and has always involved protocols in which trust, repeat business, etc., are factors. Or escrow agents.
- Long before the "key escrow" of Clipper, true escrow was planned. Escrow as in escrow agents. Or bonding agents.
- Alice and Bob want to conduct a transaction. Neither trusts the other; indeed, they are unknown to each other. In steps "Esther's Escrow Service." She is also utraceable, but has established a digitally-signed presence and a good reputation for fairness. Her business is in being an escrow agent, like a bonding agency, not in "burning" either party. (The math of this is interesting: as long as the profits to be gained from any small set of transactions is less than her "reputation capital," it is in her interest to forego the profits from burning and be honest. It is also possible to arrange that Esther cannot profit from burning either Alice or Bob or both of them, e.g., by suitably encrypting the escrowed stuff.)
- Alice can put her part of the transaction into escrow with Esther, Bob can do the same, and then Esther can release the items to the parties when conditions are met, when both parties agree, when adjudication of some sort occurs, etc. (There a dozen issues here, of course, about how disputes are settled, about how parties satisfy themselves that Esther has the items she says she has, etc.)

10.21. Loose Ends

10.21.1. Legality of trying to break crypto systems

- + "What's the legality of breaking cyphers?"
 - Suppose I find some random-looking bits and find a way to apparently decrease their entropy, perhaps turning them into the HBO or Playboy channel? What crime have I committed?
 - "Theft of services" is what they'll get me for. Merely listening to broadcasts can now be a crime (cellular, police channels, satellite broadcasts). In my view, a chilling development, for practical reasons (enforcement means invasive monitoring) and for basic common sense ethics reasons: how can listening to what lands on your

- property be illegal?
- This also opens the door for laws banning listening to certain "outlaw" or "unlicensed" broadcast stations. Shades of the Iron Curtain. (I'm not talking about FCC licensing, per se.)
- + "Could it ever be illegal to try to break an encryption scheme, even if the actual underlying data is not "stolen"?"
- + Criminalizing *tools* rather than actions
 - The U.S. is moving in the direction of making mere possession of certain tools and methods illegal, rather than criminalizing actual actions. This has been the case--or so I hear, though I can't cite actual laws--with "burglar tools." (Some dispute this, pointing to the sale of lockpicks, books on locksmithing, etc. Still, see what happens if you try to publish a detailed book on how to counterfeit currency.)
 - Black's law term for this?
- + To some extent, it already is. Video encryption is this way. So is cellular.
 - attendees returning from a Bahamas conference on pirate video methods (guess why it was in the Bahamas) had their papers and demo materials seized by Customs
 - Counterfeiting is, I think, in this situation, too. Merely exploring certain aspects is verboten. (I don't claim that all aspects are, of course.)
 - Interception of broadcast signals may be illegal-- satellite or cellular phone traffic (and Digital Telephony Act may further make such intercepts illegal and punishable in draconian ways)
- + Outlawing of the breaking of encryption, a la the broadcast/scanner laws
 - (This came up in a thread with Steve Bellovin)
- + Aspects
 - + PPL side...hard to convince a PPL agent to "enforce" this
 - but market sanctions against those who publically use the information are of course possible, just as with those who overhear conversations and then gossip widely (whereas the act of overhearing is hardly a crime)
 - statutory enforcement leads to complacency, to below-par security
 - + is an unwelcome expansion of power of state to enforce laws against decryption of numbers
 - and may lead to overall restrictions on crypto use
- 10.21.2. wais, gopher, WWW, and implications
 - borders more transparent...not clear _where_ searches are taking place, files being transferred, etc. (well, it is deterministic, so some agent or program presumably knows, but it's likely that humans don't)
- 10.21.3. "Why are so many prominent Cypherpunks interested in the law?"
 - Beats me. Nothing is more stultifyingly boring to me than the craft and "found items" nature of the law.
 - However,, for a certain breed of hacker, law hacking is the ultimate challenge. And it's important for some Cypherpunks

- goals.
- 10.21.4. "How will crypto be fought?"
- The usual suspects: porn, pedophilia, terrorists, tax evaders, spies
 - + Claims that "national security" is at stake
 - As someone has said, "National security is the root password to the Constitution"
 - + claims of discrimination
 - as but one example, crypto allows offshore bank accounts, a la carte insurance, etc...these are all things that will shake the social welfare systems of many nations
- 10.21.5. Stego may also be useful in providing board operators with "plausible deniability"--they can claim ignorance of the LSB contents (I'm not saying this will stand up in court very well, but any port in a storm, especially port 25).
- 10.21.6. Can a message be proved to be encrypted, and with what key?
- 10.21.7. Legality of digital signatures and timestamps?
- Stu Haber confirms that this has not been tested, no precedents set
- 10.21.8. A legal issue about proving encryption exists
- The XOR point. Any message can be turned into any other message, with the proper XOR intermediate message. Implications for stego as well as for legal proof (difficulty of). As bits leave no fingerprints, the mere presence of a particular XOR pad on a defendant's disk is no proof that he put it there...the cops could have planted the incriminating key, which turns "gi6E2lf7DX01jT\$" into "Dope is ready." (I see issues of "chain of evidence" becoming even more critical, perhaps with use of independent "timestamping authorities" to make hashes of seized evidence--hashes in the cryptographic sense and not hashes in the usual police sense.)
- 10.21.9. "What are the dangers of standardization and official sanctioning?"
- The U.S. has had a disturbing tendency to standardize on some technology and then punish deviations from the standard. Examples: telephones, cable (franchises granted, competitors excluded)
 - Franchises, standards...
 - + My concern: Digital money will be blessed...home banking, Microsoft, other banks, etc. The Treasury folks will sign on, etc.
 - Competitors will have a hard time, as government throws roadblocks in front of them, as the U.S. makes international deals with other countries, etc.
- 10.21.10. Restrictions on voice encryption?
- + may arise for an ironic reason: people can use Net connections to talk worldwide for \$1 an hour or less, rather than \$1 a minute; this may cause telcos to clamor for restrictions
 - enforcing these restrictions then becomes problematic, unless channel is monitored
 - and if encrypted...
- 10.21.11. Fuzziness of laws
- It may seem surprising that a nation so enmeshed in complicated legalese as the U.S., with more lawyers per capita than any other large nation and with a legal code

that consists of hundreds of thousands of pages of regulations and interpretations, is actually a nation with a legal code that is hard to pin down.

- Any system with formal, rigid rules can be "gamed against" be an adversary. The lawmakers know this, and so the laws are kept fuzzy enough to thwart mechanistic gaming; this doesn't stop there from being an army of lawyers (in fact, it guarantees it). Some would say that the laws are kept fuzzy to increase the power of lawmakers and regulators.
- "Bank regulations in this country are kept deliberately somewhat vague. The regulator's word is the deciding principle, not a detailed interpretation of statute. The lines are fuzzy, and because they are fuzzy, the banks don't press on them nearly as hard as when there's clear statutory language available to be interpreted in a court.

"The uncertainty in the regulatory environment increases the hold the regulators have over the banks. And the regulators are known for being decidedly finicky. Their decisions are largely not subject to appeal (except for the flagrant stuff, which the regulators are smart enough not to do too often), and there's no protection against cross-linking issues. If a bank does something untoward in, say, mortgage banking, they may find, say, their interstate branching possibilities seem suddenly much dimmer.

"The Dept. of Treasury doesn't want untraceable transactions." [Eric Hughes, Cypherpunks list, 1994-8-03]

- Attempts to sneak around the laws, especially in the context of alternative currencies, Perry Metzger notes: "They are simply trying to stop you from playing games. The law isn't like geometry -- there aren't axioms and rules for deriving one thing from another. The general principle is that they want to track all your transactions, and if you make it difficult they will either use existing law to jail you, or will produce a new law to try to do the same." [Perry Metzger, 1994-08-10]
- This fuzziness and regulatory discretion is closely related to those wacky schemes to avoid taxes by claiming, for example, that the "dollar" is defined as 1/35th of an ounce of gold (and that hence one's earnings in "real dollars" are a tiny fraction of the ostensible earnings), that Ohio did not legally enter the Union and thus the income tax was never properly ratified,, etc. Lots of these theories have been tested--and rejected. I mention this because some Cypherpunks show signs of thinking "digital cash" offers similar opportunities. (And I expect to see similar scams.)
- (A related example. Can one's accumulation of money be taken out of the country? Depending on who you ask, "it depends." Taking it out in your suitcase raises all kind of possibilities of seizure (violation of currency export laws, money laundering, etc.). Wiring it out may invoke FinCEN triggers. The IRS may claim it is "capital flight" to avoid taxes--which it may well be. Basically, your own money is no longer yours. There may be ways to do this--I hope so--but the point remains that the rules are fuzzy, and the discretionary powers to seize assets are great.

Seek competent counsel, and then pray.)

10.21.12. role of Uniform Commercial Code (UCC)

- not discussed in crypto circles much, but the "rules of the road"
- in many way, an implementation of anarcho-capitalism, in that the UCC is a descendant (modulo some details) of the "Law Merchant" that handled relations between sovereign powers, trade at sea, etc.
- things like electronic funds transfere, checks, liabilities for forged sigs, etc.
- I expect eventual UCC involvement in digital money schemes

10.21.13. "What about the rush to legislate, to pass laws about cyberspace, the information superduperhighway, etc.?"

- + The U.S. Congress feels it has to "do something" about things that many of us feel don't need regulation or "help" from Congress.
 - crypto legislation
 - set-top boxes, cable access, National Information Infrastructure (Cable Version)
 - information access, parental lock-outs, violence ratings, sexually explicit materials, etc.
- Related to the "do something!" mentality on National Health Care, guns, violence, etc.
- Why not just not do anything?
- + Scary possibilities being talked about:
 - + giving television sets unique IDs ("V chips") with cable access through these chips
 - tying national ID cards to these, e.g., Joe Citizen, of Provo, Utah, would be "allowed" to view an NC-17 violence-rated program
 - This would be disastrous: records, surveillance, dossiers, permission, centralization
 - The "how can we fix it?" mindset is very damaging. Many things just cannot be "fixed" by central planners....look at economies for an example. The same is usually true of technologies.

10.21.14. on use of offshore escrow agents as protection against seizures

- contempt laws come into play, but the idea is to make yourself powerless to alter the situation, and hence not willfully disobeying the court
- + Can also tell offshore agents what to do with files, and when to release them
 - Eric Hughes proposes: "One solution to this is to give the passphrase (or other access information) to someone who won't give it back to you if you are under duress, investigation, court order, etc. One would desire that this entity be in a jurisdiction other than where an investigation might happen." [E.H., 1994-07-26]
 - Sandy Sandfort adds: "Prior to seizure/theft, you would make an arrangement with an offshore "escrow agent." After seizure you would send your computer the instruction that says, "encrypt my disk with the escrow agents public key." After that, only the escrow agent could decrypt your disk. Of course, the escrow agent would only do that when conditions you had stipulated were in effect." [S. S., 1994-07-27]

- related to data havens and offshore credit/P.I. havens
- 10.21.15. Can the FCC-type Requirements for "In the clear" broadcasting (or keys supplied to Feds) be a basis for similar legislation of private networks and private use of encryption?
 - this would seem to be impractical, given the growth of cellular phones, wireless LANs, etc....can't very well mandate that corporations broadcast their internal communications in the clear!
 - compression, packet-switching, and all kinds of other "distortions" of the data...requiring transmissions to be readable by government agencies would require providing the government with maps (of where the packets are going), with specific decompression algorithms, etc....very impractical
- 10.21.16. Things that could trigger a privacy flap or limitations on crypto
 - Anonymously publishing adoption records [suggested by Brian Williams, 1994-08-22]
 - nuclear weapons secrets (true secrets, not just the titillating stuff that any bright physics student can cobble together)
 - repugnant markets (assassinations, organ selling, etc.)
- 10.21.17. Pressures on civilians not to reveal crypto knowledge
 - + Example: mobile phone crypto standards.
 - "This was the official line until a few months ago - that A5 was strong and A5X a weakened export version....However, once we got hold of A5 we found that it was not particularly strong there is an easy 2^{40} attack. The government's line then changed to `you mustn't discuss this in public because it would harm British export sales'....Perhaps it was all a ploy to get Saddam to buy A5 chips off some disreputable arms dealer type. [Ross Anderson, "mobil phone in europe <gms-standard>, a precedence?," sci.crypt, 1994-08-15]
 - Now this example comes from Britain, where the intelligence community has always had more latitude than in the U.S. (an Official Secrets Act, limits on the press, no pesky Constitution to get in the way, and even more of an old boy's network than we have in the U.S. mil-industrial complex).
 - And the threat by NSA officials to have Jim Bidzos, the president of RSA Data Security, Inc., killed if he didn't play ball. {"The Keys to the Kingdom," San Jose Mercury News]
- 10.21.18. "identity escrow", Eric Hughes, for restrictions on e-mail accounts and electronic PO boxes (has been talked about, apparently...no details)

11. Surveillance, Privacy, And Intelligence Agencies

11.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

11.2. SUMMARY: Surveillance, Privacy, And Intelligence Agencies

11.2.1. Main Points

11.2.2. Connections to Other Sections

11.2.3. Where to Find Additional Information

- Bamford ("The Puzzle Palace"), Richelson (several books, including "U.S. Intelligence Agencies"), Burrows ("Deep Black," about the NRO and spy satellites), Covert Action Quarterly

11.2.4. Miscellaneous Comments

11.3. Surveillance and Privacy

11.3.1. We've come a long way from Secretary of State Stimpson's famous "Gentlemen do not read other gentlemen's mail" statement. It is now widely taken for granted that Americans are to be monitored, surveilled, and even wiretapped by the various intelligence agencies. The FBI, the National Security Agency, the CIA, the National Reconnaissance Office, etc. (Yes, these groups have various charters telling them who they can spy on, what legalities they have to meet, etc. But they still spy. And there's not an uproar--the "What have you got to hide?" side of the American privacy dichotomy.)

11.3.2. Duncan Frissell reminds us of Justice Jackson's 1948 dissenting opinion in some case:

- "The government could simplify criminal law enforcement by requiring every citizen "to keep a diary that would show where he was at all times, with whom he was, and what he was up to." [D.F. 1994-09-06, from an article in the WSJ]
- (It should be noted that tracking devices--collars, bracelets, implantable transmitters--exist and are in use with prisoners. Some parents are even installing them in children, it is rumored. A worry for the future?)

11.3.3. "What is the "surveillance state"?"

- the issue with crypto is the centralization of eavesdropping...much easier than planting bugs
- + "Should some freedom be given up for security?"
 - + "Those who are willing to trade freedom for security
 - deserve neither
 - + freedom nor security
 - Ben Franklin
 - the tradeoff is often illusory--police states result when the trains are made to run on time
- "It's a bit ironic that the Administration is crying foul so loudly over the Soviet/Russian spy in the CIA -- as if this was unfair -- while they're openly proclaiming the right to spy on citizens and foreigners via Clipper." [Carl Ellison, 1994-02-23]
- + Cameras are becoming ubiquitous
 - + cheap, integrated, new technologies
 - SDI fisheye lens
 - ATMs
 - traffic, speed traps, street corners
 - store security
 - Barcodes--worst fear of all...and not plausible
- + Automatic recognition is still lacking
 - getting better, slowly
 - neural nets, etc. (but these require training)

- 11.3.4. "Why would the government monitor my communications?"
- "Because of economics and political stability....You can build computers and monitoring devices in secret, deploy them in secret, and listen to everything. To listen to everything with bludgeons and pharmaceuticals would not only cost more in labor and equipment, but also engender a radicalizing backlash to an actual police state." [Eric Hughes, 1994-01-26]
 - Systems like Digital Telephony and Clipper make it much too easy for governments to routinely monitor their citizens, using automated technology that requires drastically less human involvement than previous police states required.
- 11.3.5. "How much surveillance is actually being done today?"
- + FBI and Law Enforcement Surveillance Activities
 - the FBI kept records of meetings (between American companies and Nazi interests), and may have used these records during and after the war to pressure companies
 - + NSA and Security Agency Surveillance Activities
 - collecting economic intelligence
 - in WW2, Economic Warfare Council (which was renamed Board of Economic Warfare) kept tabs on shipments of petroleum and other products
 - + MINARET, code word for NSA "watch list" material (intercepts)
 - SIGINT OPERATION MINARET
 - originally, watch list material was "TOP SECRET HANDLE VIA COMINT CHANNELS ONLY UMBRA GAMMA"
 - + NSA targeting is done primarily via a list called Intelligence Guidelines for COMINT Priorities (IGCP)
 - committee made up of representatives from several intelligence agencies
 - initiated in around 1966
 - + revelations following Pentagon Papers that national security elsur had picked up private conversations (part of the Papers)
 - timing of PP was late 1963, early 1964...about time UB was getting going
 - + F-3, the NSA's main antenna system for intercepting ASCII transmissions from un-TEMPESTed terminals and PCs
 - signals can be picked up through walls up to a foot thick (or more, considering how such impulses bounce around)
 - + Joint FBI/NSA Surveillance Activities
 - + Operation Shamrock was a tie between NSA and FBI
 - since 1945, although there had been earlier intercepts, too
 - COINTELPRO, dissidents, radicals
 - + 8/0/45 Operation Shamrock begins
 - a sub rosa effort to continue the monitoring arrangements of WW II
 - ITT Communications agreed to turn over all cables
 - + RCA Communications also turned over all cables
 - even had an ex-Signal Corps officer as a VP to handle the details
 - direct hookups to RCA lines were made, for careful monitoring by the ASA
 - cables to and from corporations, law firms,

- embassies, citizens were all kept
- + 12/16/47 Meeting between Sosthenes Behn of ITT, General Ingles of RCA, and Sec. of Defense James Forrestal
 - to discuss Operation Shamrock
 - to arrange exemptions from prosecution
- + 0/0/63 Operation Shamrock enters a new phase as RCA Global switches to computerized operation
 - coincident with Harvest at NSA
 - and perfect for start of UB/Severn operations
- + 1/6/67 Hoover officially terminates "black bag" operations
 - concerned about blowback
 - had previously helped NSA by stealing codes, ciphers, decrypted traffic, planting bugs on phone lines, etc.
 - from embassies, corporations
 - unclear as to whether these operations continued anyway
- + Plot Twist: may have been the motivation for NSA and UB/Severn to pursue other avenues, such as the use of criminals as cutouts
 - and is parallel to "Plumbers Unit" used by White House
- + 10/1/73 AG Elliot Richardson orders FBI and SS to stop requesting NSA surveillance material
 - NSA agreed to stop providing this, but didn't tell Richardson about Shamrock or Minaret
 - however, events of this year (1973) marked the end of Minaret
- + 3/4/77 Justice Dept. recommends against prosecution of any NSA or FBI personnel over Operations Shamrock and Minaret
 - decided that NSCID No. 9 (aka No. 6) gave NSA sufficient leeway
- 5/15/75 Operation Shamrock officially terminated
- and Minaret, of course
- + Operation Shamrock-Details
- + 8/0/45 Operation Shamrock begins
 - a sub rosa effort to continue the monitoring arrangements of WW II
 - ITT Communications agreed to turn over all cables
- + RCA Communications also turned over all cables
 - even had an ex-Signal Corps officer as a VP to handle the details
 - direct hookups to RCA lines were made, for careful monitoring by the ASA
 - cables to and from corporations, law firms, embassies, citizens were all kept
- + 12/16/47 Meeting between Sosthenes Behn of ITT, General Ingles of RCA, and Sec. of Defense James Forrestal
 - to discuss Operation Shamrock
 - to arrange exemptions from prosecution
- + 0/0/63 Operation Shamrock enters a new phase as RCA Global switches to computerized operation
 - coincident with Harvest at NSA
 - and perfect for start of UB/Severn operations

- + 8/18/66 (Thursday) New analysis site in New York for Operation Shamrock
- + Louis Tordella meets with CIA Dep. Dir. of Plans and arranges to set up a new listening post for analysis of the tapes from RCA and ITT (that had been being shipped to NSA and then back)
 - Tordella was later involved in setting up the watch list in 1970 for the BNDD, (Operation Minaret)
 - LPMEDLEY was code name, of a television tape processing shop (reminiscent of "Man from U.N.C.L.E.") but NSA had to move away later
- 5/15/75 Operation Shamrock officially terminated
- + 10/1/73 AG Elliot Richardson orders FBI and SS to stop requesting NSA surveillance material
 - NSA agreed to stop providing this, but didn't tell Richardson about Shamrock or Minaret
 - however, events of this year (1973) marked the end of Minaret
- Abzug committee prompted by New York Daily News report, 7/22/75, that NSA and FBI had been monitoring commercial cable traffic (Operation Shamrock)
- + 6/30/76 175 page report on Justice Dept. investigation of Shamrock and Minaret
 - only 2 copies prepared, classified TOP SECRET UMBRA, HANDLE VIA COMINT CHANNELS ONLY
- + 3/4/77 Justice Dept. recommends against prosecution of any NSA or FBI personnel over Operations Shamrock and Minaret
 - decided that NSCID No. 9 (aka No. 6) gave NSA sufficient leeway
- + the NSA program, begun in August 1945, to monitor all telegrams entering or leaving the U.S.
 - reminiscent of Yardley's arrangements in the 1920s (and probably some others)
 - known only to Louis Tordella and agents involved
 - compartmentalization
- + Plot Links of Operation Shamrock to Operation Ultra Black
 - many links, from secrecy, compartmentalization, and illegality to the methods used and the subversion of government power
 - "Shamrock was blown...Ultra Black burrowed even deeper."
- + NSA, FBI, and surveillance of Cuban sympathizers
 - "watch list" used
 - were there links to Meyer Lansky and Trafficante via the JFK-Mafia connection?
 - various Watergate break-in connections (Cubans used)
 - Hoover ended black-bag operations in 1967-8
- + NSA, FBI, and Dissenters (COINTELPRO-type activities)
- + 10/20/67 NSA is asked to begin collecting information related to civil disturbances, war protesters, etc.
 - Army Intelligence, Secret Service, CIA, FBI, DIA were all involved
 - arguably, this continues (given the success of FBI and Secret Service in heading off major acts of terrorism and attempted assassinations)

- + Huston Plan and Related Plans (1970-71)
 - 7/19/66 Hoover unofficially terminates black bag operations
 - + 1/6/67 Hoover officially terminates black bag operations
 - fearing blowback, concerned about his place in history
 - + 6/20/69 Tom C. Huston recommends increased intelligence activity on dissent
 - memo to NSA, CIA, DIA, FBI
 - this later becomes basis of Huston Plan
 - + 6/5/70 Meeting at White House to prepare for Huston Plan; Interagency Committee on Intelligence (Ad Hoc), ICI
 - Nixon, Huston, Ehrlichman, Haldeman, Noel Gayler of NSA, Richard Helms of CIA, J. Edgar Hoover of FBI, Donald V. Bennett of DIA
 - William Sullivan of FBI named to head ICI
 - + NSA enthusiastically supported ICI
 - PROD named Benson Buffham as liaison
 - sought increased surreptitious entries and elimination of legal restrictions on domestic surveillance (not that they had felt bound by legalisms)
 - recipients to be on "Bigot List" and with even more security than traditional TOP SECRET, HANDLE VIA COMINT CHANNELS ONLY
 -
 - + 7/23/70 Huston Plan circulated
 - 43 pages, entitled Domestic Intelligence Gathering Plan: Analysis and Strategy
 - urged increased surreptitious entries (for codes, ciphers, plans, membership lists)
 - targeting of embassies
 - + 7/27/70 Huston Plan cancelled
 - pressure by Attorney General John Mitchell
 - and perhaps by Hoover
 - Huston demoted; he resigned a year later
 - but the Plan was not really dead...perhaps Huston's mistake was in being young and vocal and making the report too visible and not deniable enough
 - + 12/3/70 Intelligence Evaluation Committee (IEC) meets (Son-of-Huston Plan)
 - John Dean arranged it in fall of '70
 - Robert C. Mardian, Assistant AG for Internal Security headed up the IEC
 - Benson Buffham of NSA/PROD, James Jesus Angleton of CIA, George Moore from FBI, Col. John Downie from DOD
 - essentially adopted all of Huston Plan
 - + 1/26/71 NSA issues NSA Contribution to Domestic Intelligence (as part of IEC)
 - increased scope of surveillance related to drugs (via BNDD and FBI), foreign nationals
 - "no indication of origin" on generated material
 - full compartmentalization, NSA to ensure compliance
 - + 8/4/71 G. Gordon Liddy attends IEC meeting, to get them to investigate leaks of Pentagon Papers

- channel from NSA/PROD to Plumber's Unit in White House, bypassing other agencies
 - + 6/7/73 New York Times reveals details of Huston Plan
 - full text published
 - trials of Weatherman jeopardized and ultimately derailed it
 - + 10/1/73 AG Elliot Richardson orders FBI and SS to stop requesting NSA surveillance material
 - NSA agreed to stop providing this, but didn't tell Richardson about Shamrock or Minaret
 - however, events of this year (1973) marked the end of Minaret
 - + FINCEN, IRS, and Other Economic Surveillance
 - set up in Arlington as a group to monitor the flows of money and information
 - + eventually these groups will see the need to actively hack into computer systems used by various groups that are under investigation
 - ties to the death of Alan Standorf? (Vint Hill)
 - Casolaro, Riconosciutto
- 11.3.6. "Does the government want to monitor economic transactions?"
- Incontrovertibly, they want to. Whether they have actual plans to do so is more debatable. The Clipper and Digital Telephony proposals are but two of the indications they have great plans laid to ensure their surveillance capabilities are maintained and extended.
 - The government will get increasingly panicky as more Net commerce develops, as trade moves offshore, and as encryption spreads.
- 11.3.7. A danger of the surveillance society: You can't hide
- seldom discussed as a concern
 - no escape valve, no place for those who made mistakes to escape to
 - (historically, this is a way for criminals to get back on a better track--if a digital identity means their record forever follows them, this may...)
 - + A growing problem in America and other "democratic" countries is the tendency to make mandatory what were once voluntary choices. For example, fingerprinting children to help in kidnapping cases may be a reasonable thing to do voluntarily, but some school districts are planning to make it mandatory.
 - This is all part of the "Let's pass a law" mentality.
- 11.3.8. "Should I refuse to give my Social Security Number to those who ask for it?"
- It's a bit off of crypto, but the question does keep coming up on the Cypherpunks list.
 - Actually, they don't even need to ask for it anymore....it's attached to so many other things that pop up when they enter your name that it's a moot point. In other words, the same dossiers that allow the credit card companies to send you "preapproved credit cards" every few days are the same dossiers that MCI, Sprint, AT&T, etc. are using to sign you up.
- 11.3.9. "What is 'Privacy 101'?"
- I couldn't think of a better way to introduce the topic of how individuals can protect their privacy, avoid

- interference by the government, and (perhaps) avoid taxes.
- Duncan Frissell and Sandy Sandfort have given out a lot of tips on this, some of them just plain common sense, some of them more arcane.
- + They are conducting a seminar, entitled "PRIVACY 101" and the archives of this are available by Web at:
 - <http://www.iquest.com/~fairgate/privacy/index.html>
- 11.3.10. Cellular phones are trackable by region...people are getting phone calls as they cross into new zones, "welcoming" them
 - but it implies that their position is already being tracked
- 11.3.11. Ubiquitous use of SSNs and other personal I.D.
- 11.3.12. cameras that can recognize faces are placed in many public places, e.g., airports, ports of entry, government buildings
 - and even in some private places, e.g., casinos, stores that have had problems with certain customers, banks that face robberies, etc.
- 11.3.13. speculation (for the paranoids)
 - covert surveillance by noninvasive detection methods...positron emission tomography to see what part of the brain is active (think of the paranoia possibility!)
 - typically needs special compounds, but...
- 11.3.14. Diaries are no longer private
 - + can be opened under several conditions
 - subpoena in trial
 - discovery in various court cases, including divorce, custody, libel, etc.
 - business dealings
 - psychiatrists (under Tarasoff ruling) can have records opened; whatever one may think of the need for crimes confessed to shrinks to be reported, this is certainly a new era
 - Packwood diary case establishes the trend: diaries are no longer sacrosanct
 - An implication for crypto and Cypherpunks topics is that diaries and similar records may be stored in encrypted forms, or located in offshore locations. There may be more and more use of offshore or encrypted records.
- 11.4. U.S. Intelligence Agencies: NSA, FinCEN, CIA, DIA, NRO, FBI
- 11.4.1. The focus here is on U.S. agencies, for various reasons. Most Cypherpunks are currently Americans, the NSA has a dominant role in surveillance technology, and the U.S. is the focus of most current crypto debate. (Britain has the GCHQ, Canada has its own SIGINT group, the Dutch have...., France has DGSE and so forth, and...)
- 11.4.2. Technically, not all are equal. And some may quibble with my calling the FBI an "intelligence agency." All have surveillance and monitoring functions, albeit of different flavors.
- 11.4.3. "Is the NSA involved in domestic surveillance?"
 - + Not completely confirmed, but much evidence that the answer is "yes":
 - * previous domestic surveillance (Operation Shamrock, telegraphs, ITT, collusion with FBI, etc.)
 - * reciprocal arrangements with GCHQ (U.K.)
 - * arrangements on Indian reservations for microwave intercepts

- * the general technology allows it (SIGINT, phone lines)
 - * the National Security Act of 1947, and later clarifications and Executive Orders, makes it likely
 - And the push for Digital Telephony.
- 11.4.4. "What will be the effects of widespread crypto use on intelligence collection?"
- Read Bamford for some stuff on how the NSA intercepts overseas communications, how they sold deliberately-crippled crypto machines to Third World nations, and how much they fear the spread of strong, essentially unbreakable crypto. "The Puzzle Palace" was published in 1982...things have only gotten worse in this regard since.
 - Statements from senior intelligence officials reflect this concern.
 - Digital dead drops will change the whole espionage game. Information markets, data havens, untraceable e-mail...all of these things will have a profound effect on national security issues.
 - I expect folks like Tom Clancy to be writing novels about how U.S. national security interests are being threatened by "unbreakable crypto." (I like some Clancy novels, but there's no denying he is a right-winger who's openly critical of social trends, and that he believes druggies should be killed, the government is necessary to ward off evil, and ordinary citizens ought not to have tools the government can't overcome.)
- 11.4.5. "What will the effects of crypto on conventional espionage?"
- Massive effects; watch out for this to be cited as a reason to ban or restrict crypto--however pointless that may be.
 - + Effects:
 - information markets, a la BlackNet
 - digital dead drops -- why use Coke cans near oak trees when you can put messages into files and post them worldwide, with untraceably? (but, importantly, with a digital signature!)
 - transparency of borders
 - arms trade, arms deals
 - virus, weaponry
- 11.4.6. NSA budget
- \$27 billion over 6 years, give or take
 - may actually increase, despite end of Cold War
 - new threats, smaller states, spread of nukes, concerns about trade, money-laundering, etc.
 - first rule of bureaucracies: they always get bigger
 - + NSA-Cray Computer supercomputer
 - + press release, 1994-08-17, gives some clues about the capabilities sought by the surveillance state
 - "The Cray-3/SSS will be a hybrid system capable of vector parallel processing, scalable parallel processing and a combination of both. The system will consist of a dual processor 256 million word Cray-3 and a 512,000 processor 128 million byte single instruction multiple data (SIMD) array.....SIMD arrays of one million processors are expected to be possible using the current version of the Processor-In-Memory (PIM) chips developed by the Supercomputing Research Center once the development project is completed. The PIM chip

contains 64 single-bit processors and 128 kilobyte bits of memory. Cray Computer will package PIM chips utilizing its advanced multiple chip module packaging technology. The chips are manufactured by National Semiconductor Corporation."

- This is probably the supercomputer described in the Gunter Ahrendt report

11.4.7. FINCEN, IRS, and Other Economic Surveillance

- Financial Crimes Enforcement Network, a consortium or task force made up of DEA, DOJ, FBI, CIA, DIA, NSA, IRS, etc.
- set up in Arlington as a group to monitor the flows of money and information
- eventually these groups will see the need to hack into computer systems used by various groups that are under investigation
- Cf. "Wired," either November or December, 1993

11.4.8. "Why are so many computer service, telecom, and credit agency companies located near U.S. intelligence agency sites?"

- + For example, the cluster of telecom and credit reporting agencies (TRW Credit, Transunion, etc.) in and around the McLean/Langley area of Northern Virginia (including Herndon, Vienna, Tyson's Corner, Chantilly, etc.)
- same thing for, as I recall, various computer network providers, such as UUCP (or whatever), America Online, etc.
- The least conspiratorial view: because all are located near Washington, D.C., for various regulatory, lobbying, etc. reasons
- + The most conspiratorial view: to ensure that the intelligence agencies have easy access to communications, direct landlines, etc.
- credit reporting agencies need to clear identities that are fabricated for the intelligence agencies, WitSec, etc. (the three major credit agencies have to be complicit in these creations, as the "ghosts" show up immediately when past records are cross-correlated)
- As Paul Ferguson, Cypherpunk and manager at US Sprint, puts it: "We're located in Herndon, Virginia, right across the street from Dulles Airport and a hop, skip & jump down the street from the new NRO office. , -)"
[P.F., 1994-08-18]

11.4.9. Task Force 157, ONI, Kissinger, Castle Bank, Nugan Hand Bank, CIA

11.4.10. NRO building controversy

- and an agency I hadn't seen listed until August, 1994: "The Central Imagery Office"

11.4.11. SIGINT listening posts

- + possible monkeywrenching?
 - probably too hard, even for an EMP bomb (non-nuclear, that is)

11.4.12. "What steps is the NSA taking?"

- * besides death threats against Jim Bidzos, that is
- * Clipper a plan to drive competitors out (pricing, export laws, harassment)
- * cooperation with other intelligence agencies, other nations
 - New World Order
- * death threats were likely just a case of bullying...but

could conceivably be part of a campaign of terror--to shut up critics or at least cause them to hesitate

11.5. Surveillance in Other Countries

11.5.1. Partly this overlaps on the earlier discussion of crypto laws in other countries.

11.5.2. Major Non-U.S. Surveillance Organizations

- + BnD -- Bundesnachrichtendienst
 - German security service
 - BND is seeking constitutional amendment, but may not need it, as the mere call for it told everyone what is already existing
 - "vacuum cleaner in the ether"
 - Gehlen...Eastern Front Intelligence
 - Pullach, outside Munchen
 - they have always tried to get the approval to do domestic spying...a key to power
- + Bundeskriminalamt (BKA) -- W. German FBI
 - HQ is at Wiesbaden
 - bomb blew up there when being examined, killing an officer (related to Pan Am/Lockerbie/PFLP-GC)
 - sign has double black eagles (back to back)
- BVD -- Binnenlandse Veiligheids Dienst, Dutch Internal Security Service
- + SDECE
 - French intelligence (foreign intelligence), linked to Greepeace ship bombing in New Zealand?
 - SDECE had links to the October Surprise, as some French agents were in on the negotiations, the arms shipments out of Marseilles and Toulon, and in meetings with Russbacher and the others
- DST, Direction de la Surveillance du Territoire, counterespionage arm of France (parallel to FBI)
- + DSGE, Direction G n rale de la S curit  Ext ri re
 - provides draft deferments for those who deliver stolen information
- + Sweden, Forsvarets Radioanstalt ("Radio Agency of the Defense")
 - cracked German communications between occupied Norway and occupied Denmark
 - Beurling, with paper and pencil only
- + Mossad, LAKAM, Israel
 - + HQ in Tel Aviv, near HQ of AMAN, military intelligence
 - doesn't HQ move around a lot?
 - LAKAM (sp?), a supersecret Israeli intelligence agency...was shown the PROMIS software in 1983
- + learned of the Pakistani success in building an atom bomb and took action against the Pakistani leadership: destruction of the plane carrying the President (Zia?) and some U.S. experts
 - Mossad knew of DIA and CIA involvement in BCCI financing of Pakistani atom bomb efforts (and links to other arms dealers that allowed triggers and the like to reach Pakistan)
- revelations by Vanunu were designed to scare the Arab and Muslim world--and to send a signal that the killing of President Zia was to be the fate of any Pakistani leader

who continued the program

11.5.3. They are very active, though they get less publicity than do the American CIA, NSA, FBI, etc.

11.6. Surveillance Methods and Technology

11.6.1. (some of this gets speculative and so may not be to everyone's liking)

11.6.2. "What is TEMPEST and what's the importance of it?"

- TEMPEST apparently stands for nothing, and hence is not an acronym, just a name. The all caps is the standard spelling.
- RF emission, a set of specs for complying
- Van Eyck (or Van Eck?) radiation
- + Mostly CRTs are the concern, but also LCD panels and the internal circuitry of the PCs, workstations, or terminals.
- "Many LCD screens can be read at a distance. The signal is not as strong as that from the worst vdis, but it is still considerable. I have demonstrated attacks on Zenith laptops at 10 metres or so with an ESL 400 monitoring receiver and a 4m dipole antenna; with a more modern receiver, a directional antenna and a quiet RF environment there is no reason why 100 metres should be impossible." [Ross Anderson, Tempest Attacks on Notebook Computers ???, comp.security.misc, 1994-08-31]

11.6.3. What are some of the New Technologies for Espionage and Surveillance

- + Bugs
 - + NSA and CIA have developed new levels of miniaturized bugs
 - e.g., passive systems that only dribble out intercepted material when interrogated (e.g., when no bug sweeps are underway)
 - many of these new bugging technologies were used in the John Gotti case in New York...the end of the Cold War meant that many of these technologies became available for use by the non-defense side
 - the use of such bugging technology is a frightening development: conversations can be heard inside sealed houses from across streets, and all that will be required is an obligatory warrant
- + DRAM storage of compressed speech...6-bit companded, frequency-limited, so that 1 sec of speech takes 50Kbits, or 10K when compressed, for a total of 36 Mbits per hour-this will fit on a single chip
 - readout can be done from a "mothership" module (a larger bug that sits in some more secure location)
 - or via tight-beam lasers
- + Bugs are Mobile
 - can crawl up walls, using the MIT-built technology for microrobots
 - some can even fly for short distances (a few clicks)
- + Wiretaps
 - so many approaches here
 - phone switches are almost totally digital (a la ESS IV)
 - again, software hacks to allow wiretaps
- + Vans equipped to eavesdrop on PCs and networks
- + TEMPEST systems

- + technology is somewhat restricted, companies doing this work are under limitations not to ship to some customers
 - no laws against shielding, of course
- these vans are justified for the "war on drugs" and weapons proliferation control efforts (N.E.S.T., anti-Iraq, etc.)
- + Long-distance listening
 - parabolic reflectors, noise cancellation (from any off-axis sources), high gain amplification, phoneme analysis
 - neural nets that learn the speech patterns and so can improve clarity
- + lip-reading
 - with electronically stabilized CCD imagers, 3000mm lenses
 - neural net-based lip-reading programs, with learning systems capable of improving performance
 - for those in sensitive positions, the availability of new bugging methods will accelerate the conversion to secure systems based on encrypted telecommunications and the avoidance of voice-based systems
- 11.6.4. Digital Telephony II is a major step toward easier surveillance
- 11.6.5. Citizen tracking
 - + the governments of the world would obviously like to trace the movements, or at least the major movements, of their subjects
 - makes black markets a bit more difficult
 - surfaces terrorists, illegal immigrants, etc. (not perfectly)
 - + allows tracking of "sex offenders"
 - who often have to register with the local police, announce to their neighbors their previous crimes, and generally wear a scarlet letter at all times--I'm not defending rapists and child molesters, just noting the dangerous precedent this is setting
 - because its the nature of bureaucracies to want to know where "their" subjects are (dossier society = accounting society...records are paramount)
 - + Bill Stewart has pointed out that the national health care systems, and the issuance of social security numbers to children, represent a way to track the movements of children, through hospital visits, schools, etc. Maybe even random check points at places where children gather (malls, schools, playgrounds, opium dens, etc.)
 - children in such places are presumed to have lesser rights, hence...
 - this could all be used to track down kidnapped children, non-custodial parents, etc.
 - this could be a wedge in the door: as the children age, the system is already in place to continue the tracking (about the right timetable, too...start the system this decade and by 2010 or 2020, nearly everybody will be in it)
 - (A true paranoid would link these ideas to the child photos many schools are requiring, many local police departments are officially assisting with, etc. A dossier society needs mug shots on all the perps.)

- These are all reasons why governments will continue to push for identity systems and will seek to derail efforts at providing anonymity
- + Surveillance and Personnel Identification
 - + cameras that can recognize faces are placed in many public places, e.g., airports, ports of entry, government buildings
 - and even in some private places, e.g., casinos, stores that have had problems with certain customers, banks that face robberies, etc.
 - + "suspicious movements detectors"
 - + cameras that track movements, loitering, eye contact with other patrons
 - + neural nets used to classify behaviors
 - legal standing not needed, as these systems are used only to trigger further surveillance, not to prove guilt in a court of law
 - example: banks have cameras, by 1998, that can identify potential bank robbers
 - camera images are sent to a central monitoring facility, so the usual ploy of stopping the silent alarm won't work
 - airports and train stations (fears of terrorists), other public places
- 11.6.6. Cellular phones are trackable by region...people are getting phone calls as they cross into new zones, "welcoming" them
 - but it implies that their position is already being tracked
- 11.6.7. coming surveillance, Van Eck, piracy, vans
 - An interesting sign of things to come is provided in this tale from a list member: "In Britain we have 'TV detector Vans'. These are to detect licence evaders (you need to pay an annual licence for the BBC channels). They are provided by the Department of Trade and Industry. They use something like a small minibus and use Van Eck principles. They have two steerable detectors on the van roof so they can triangulate. But TV shops have to notify the Government of buyers - so that is the basic way in which licence evaders are detected. ... I read of a case on a bulletin board where someone did not have a TV but used a PC. He got a knock on the door. They said he appeared to have a TV but they could not make out what channel he was watching! [Martin Spellman, <mspellman@cix.compulink.co.uk>, 1994-0703]
 - This kind of surveillance is likely to become more and more common, and raises serious questions about what other information they'll look for. Perhaps the software piracy enforcers (Software Publishers Association) will look for illegal copies of Microsoft Word or SimCity! (This area needs more discussion, obviously.)
- 11.6.8. wiretaps
 - supposed to notify targets within 90 days, unless extended by a judge
 - Foreign Intelligence Surveillance Act cases are exempt from this (it is likely that Cypherpunks wiretapped, if they have been, for crypto activities fall under this case...foreigners, borders being crossed, national security implications, etc. are all plausible reasons, under the

Act)

11.7. Surveillance Targets

11.7.1. Things the Government May Monitor

- besides the obvious things like diplomatic cable traffic, phone calls from and to suspected terrorists and criminals, etc.
- + links between Congressmen and foreign embassies
 - claims in NYT (c. 9-19-91) that CIA had files on Congressmen opposing aid to Contras
- + Grow lamps for marijuana cultivation
 - raids on hydroponic supply houses and seizure of mailing lists
 - records of postings to alt.drugs and alt.psychoactive
 - vitamin buyers clubs
- + Energy consumption
 - to spot use of grow lamps
 - + but also might be refined to spot illegal aliens being sheltered or any other household energy consumption "inconsistent with reported uses"
 - same for water, sewage, etc.
- + raw chemicals
 - as with monitors on ammonium nitrate and other bomb materials
 - or feedstock for cocaine production (recall various seizures of shipments of chemicals to Latin America)
 - checkout of books, a la FBI's "Library Awareness Program" of around 1986 or so
 - attendance at key conferences, such as Hackers Conference (could have scenes involving this), Computer Security Conference

11.7.2. Economic Intelligence (Spying on Corporations, Foreign and Domestic)

- + "Does the NSA use economic intelligence data obtained in intercepts?"
 - Some of us speculate that this is so, that this has been going on since the 1960s at least. For example, Bamford noted in 1982 that the NSA had foreknowledge of the plans by the British to devalue the pound in the late 1970s, and knowledge of various corporate plans.
 - The NSA clears codes used by the CIA, so it seem impossible for the NSA not to have known about CIA drug smuggling activities. The NSA is very circumspect, however, and rarely (or never) comments.
- + there have been calls for the government to somehow help American business and overall competitiveness by "levelling the playing field" via espionage
 - especially as the perceived threat of the Soviet bloc diminishes and as the perceived threat of Japan and Germany increases
- leaders of the NSA and CIA have even talked openly about turning to economic surveillance
- + Problems with this proposal:
 - illegal
 - unethical
- + who gets the intelligence information? Does NSA just call up Apple and say "We've intercepted some message from

Taiwan that describe their plans for factories. Are you interested?"

- the U.S. situation differs from Japan and MITI (which is often portrayed as the model for how this ought to work) in that we have many companies with little or no history of obeying government recommendations
- + and foreign countries will likely learn of this espionage and take appropriate measures
 - e.g., by increasing encryption

11.7.3. War on Drugs and Money Laundering is Causing Increase in Surveillance and Monitoring

- monitoring flows of capital, cash transactions, etc.
- cooperation with Interpol, foreign governments, even the Soviets and KGB (or whatever becomes of them)
- new radar systems are monitoring light aircraft, boats, etc.

11.8. Legal Issues

11.8.1. "Can my boss monitor my work?" "Can my bankruptcy in 1980 be used to deny me a loan?" etc.

- Libertarians have a very different set of answers than do many others: the answer to all these questions is mostly "yes," morally (sorry for the normative view).

11.8.2. Theme: to protect some rights, invasion of privacy is being justified

- e.g., by forcing employer records to be turned over, or of seizing video rental records (on the grounds of catching sexual deviants)
- various laws about employee monitoring

11.8.3. Government ID cards, ability to fake identities

- The government uses its powers to forge credentials, with the collusion of the major credit agencies (who obviously see these fake identities "pop into existence full-blown.")
- WitSec, FINCen, false IDs, ties to credit card companies
- DEA stings, Heidi in La Jolla, Tava, fake tax returns, fake bank applications, fake IDs
- the "above it all" attitude is typical of this...who guards the guardians?
- WitSec, duplicity

11.8.4. Legalities of NSA surveillance

- read Bamford for some circa 1982 poinra
- UK-USA
- ECPA
- national security exemptions
- lots of confusion; however, the laws have never had any real influence, and I cannot imagine the NSA being sued!

11.9. Dossiers and Data Bases

11.9.1. "The dossier never forgets"

- + any transgressions of any law in any country can be stored indefinitely, exposing the transgressor to arrest and detention anytime he enters a country with such a record on him
- (This came up with regard to the British having quaint ideas about computer security, hacking, and data privacy; it is quite possible that an American passing through London could be detained for some obscure violation years

in the past.)

- this is especially worrisome in a society in which legal codes fill entire rooms and in which nearly every day produces some violation of some law

11.9.2. "What about the privacy issues with home shopping, set-top boxes, advertisers, and the NII?"

- Do we want our preferences in toothpaste fed into databases so that advertisers can target us? Or that our food purchases be correlated and analyzed by the government to spot violations of the Dietary Health Act?
- First, laws which tell people what records they are "allowed" to keep are wrong-headed, and lead to police state inspections of disk drives, etc. The so-called "Data Privacy" laws of several European nations are a nightmare. Strong crypto makes them moot.
- Second, it is mostly up to people to protect what they want protected, not to pass laws demanding that others protect it for them.
- In practice, this means either use cash or make arrangements with banks and credit card companies that will protect privacy. Determining if they have or not is another issue, but various ideas suggest themselves (John Gilmore says he often joins groups under variants of his name, to see who is selling his name to mailing lists.)
- Absent any laws which forbid them, privacy-preserving credit card companies will likely spring up if there's a market demand. Digital cash is an example. Other variants abound. Cypherpunks should not allow such alternatives to be banned, and should of course work on their own such systems.

11.9.3. credit agencies

- TRW Credit, Transunion, Equifax
- links to WitSec

11.9.4. selling of data bases, linking of records...

- several states have admitted to selling their driver's license data bases

11.10. Police States and Informants

11.10.1. Police states need a sense of terror to help magnify the power or the state, a kind of "shrechlichkeit," as the Nazis used to call it. And lots of informants. Police states need willing accomplices to turn in their neighbors, or even their parents, just as little Pavel Morozov became a Hero of the Soviet People by sending his parents to their deaths in Stalin's labor camps for the crime of expressing negative opinions about the glorious State.

- (The canonization of Pavel Morozov was recently repudiated by current Russian leaders--maybe even by the late-Soviet era leaders, like Gorbachev--who pointed out the corrosive effects of encouraging families to narc on each other...something the U.S. has forgotten...will it be 50 years before our leaders admit that having children turn in Daddy for using "illegal crypto" was not such a good idea?)

11.10.2. Children are encouraged in federally-mandated D.A.R.E. programs to become Junior Narcs, nancing their parents out to the cops and counselors who come into their schools.

11.10.3. The BATF has a toll-free line (800-ATF-GUNS) for snitching on

neighbors who one thinks are violating the federal gun laws.
(Reports are this is backfiring, as gun owners call the number to report on local liberal politicians and gun-grabbers.)

11.10.4. Some country we live in, eh? (Apologies to non-U.S. readers, as always.)

11.10.5. The implications for use of crypto, for not trusting others, etc., are clear

11.10.6. Dangers of informants

- + more than half of all IRS prosecutions arise out of tips by spouses and ex-spouses...they have the inside dope, the motive, and the means
 - a sobering thought even in the age of crypto
- + the U.S. is increasing a society of narcs and stool pigeons, with "CIs" (confidential informants), protected witnesses (with phony IDs and lavish lifestyles), and with all sorts of vague threats and promises
 - in a system with tens of thousands of laws, nearly all behavior breaks at least some laws, often unavoidably, and hence a powerful sword hangs over everyone's head
- corrosion of trust, especially within families (DARE program in schools encourages children to narc on their parents who are "substance abusers"!)

11.11. Privacy Laws

11.11.1. Will proposed privacy laws have an effect?

- + I suspect just the opposite: the tangled web of laws-part of the totalitarian freezeout-will "marginalize" more people and cause them to seek ways to protect their own privacy and protect themselves from sanctions over their actions
 - + free speech vs. torts, SLAPP suits, sedition charges, illegal research, etc.
 - free speech is vanishing under a torrent of laws, licensing requirements, and even zoning rules
 - + outlawing of work on drugs, medical procedures, etc.
 - against the law to disseminate information on drug use (MDMA case at Stanford), on certain kinds of birth control
 - "If encryption is outlawed, only outlaws will have encryption."
 - + privacy laws are already causing encryption ("file protection") to be mandatory in many cases, as with medical records, transmission of sensitive files, etc.
 - by itself this is not in conflict with the government requirement for tappable access, but the practical implementation of a two-tier system-secure against civilian tappers but readable by national security tappers-is a nightmare and is likely impossible to achieve

11.11.2. "Why are things like the "Data Privacy Laws" so bad?"

- Most European countries have laws that limit the collection of computerized records, dossiers, etc., except for approved uses (and the governments themselves and their agents).
- Americans have no such laws. I've heard calls for this, which I think is too bad.

- While we may not like the idea of others compiling dossiers on us, stopping them is an even worse situation. It gives the state the power to enter businesses, homes, and examine computers (else it is completely unenforceable). It creates ludicrous situations in which, say, someone making up a computerized list of their phone contacts is compiling an illegal database! It makes e-mail a crime (those records that are kept).
- they are themselves major invasions of privacy
- are you going to put me in jail because I have data bases of e-mail, Usenet posts, etc.?
- In my opinion, advocates of "privacy" are often confused about this issue, and fail to realize that laws about privacy often take away the privacy rights of others. (Rights are rarely in conflict--contract plus self-privacy take care of 99% of situations where rights are purported to be in conflict.)

11.11.3. on the various "data privacy laws"

- many countries have adopted these data privacy laws, involving restrictions on the records that can be kept, the registration of things like mailing lists, and heavy penalties for those found keeping computer files deemed impermissible
- this leads to invasions of privacy....this very Cypherpunks list would have to be "approved" by a bureaucrat in many countries...the oportunites (and inevitabilities) of abuse are obvious
- "There is a central contradiction running through the dabase regulations proposed by many so-called "privacy advocates". To be enforceable they require massive government snooping into database activities on our workstatins and PCs, especially the activities of many small at-home businesses (such as mailing list entrepreneurs who often work out of the home).

"Thus, the upshot of these so-called "privacy" regulations is to destroy our last shreds of privacy against government, and calm us into blindly letting even more of the details of our personal lives into the mainframes of the major government agencies and credit reporting agenices, who if they aren't explicitly excepted from the privacy laws (as is common) can simply evade them by using offshore havens, mutual agreements with foreign investigators, police and intelligence agencies." [Jim Hart, 1994-09-08]

11.11.4. "What do Cypherpunks think about this?"

- + divided minds...while no one likes being monitored, the question is how far one can go to stop others from being monitored
- "Data Privacy Laws" as a bad example: tramples on freedom to write, to keep one's computer private

11.11.5. Assertions to data bases need to be checked (credit, reputation, who said what, etc.)

- if I merely assert that Joe Blow no longer is employed, and this spreads...

11.12. National ID Systems

- 11.12.1. "National ID cards are just the driver's licenses on the Information Superhighway." [unknown...may have been my coining]
- 11.12.2. "What's the concern?"
- 11.12.3. Insurance and National Health Care will Produce the "National ID" that will be Nearly Unescapable
- hospitals and doctors will have to have the card...cash payments will evoke suspicion and may not even be feasible
- 11.12.4. National ID Card Arguments
- "worker's permit" (another proposal, 1994-08, that would call for a national card authorizing work permission)
 - immigration, benefit
 - possible tie-in to the system being proposed by the US Postal Service: a registry of public keys (will they also "issue" the private-public key pair?)
 - software key escrow and related ideas
 - "I doubt that one would only have to "flash" your card and be on your way. More correctly, one would have to submit to being "scanned" and be on your way. This would also serve to be a convenient locator tag if installed in the toll systems and miscellaneous "security checkpoints". Why would anyone with nothing to hide care if your every move could be monitored? Its for your own good, right? Pretty soon sliding your ID into slots in everyplace you go will be common." [Korac MacArthur, comp.org.eff.talk, 1994-07-25]
- 11.12.5. "What are some concerns about Universal ID Cards?"
- "Papierrren, bitte! Schnell!
 - that they would allow traceability to the max (as folks used to say)... tracking of movements, erosion of privacy
 - that they would be required to be used for banking transactions, Net access, etc. (As usual, there may be workarounds, hacks, ...)
 - "is-a-person" credentially, where government gets involved in the issuance of cryptographic keys (a la the USPS proposal), where only "approved uses" are allowed, etc.
 - timestamps, credentials
- 11.12.6. Postal Service trial balloon for national ID card
- "While it is true that they share technology, their intent and purpose is very different. Chaum's proposal has as its intent and purpose to provide and protect anonymity in financial transactions. The intent and purpose of the US Postal Service is to identify and authenticate you to the government and to guarantee the traceability of all financial transactions." [WHMurray, alt.privacy, 1994-07-04]
- 11.12.7. Scenario for introduction of national ID cards
- Imagine that vehicle registrations require presentation of this card (gotta get those illegals out of their cars, or, more benignly, the bureaucracy simply makes the ID cars part of their process).
 - Instantly this makes those who refuse to get an ID card unable to get valid license tags. (Enforcement is already pretty good....I was pulled over a couple of times for either forgetting to put my new stickers on, or for driving with Oregon expired tags.)
- + The "National Benefits Card," for example, is then required

to get license plate tags.and maybe other things, like car and home insurance, etc. It would be very difficult to fight such a card, as one could not drive, could not pay taxes ("Awhh!" I hear you say, but consider the penalties, the tie-ins with employers, etc. You can run but you can't hide.)

- the national ID card would presumably be tied in to income tax filings, in various ways I won't go into here. The Postal Service, aiming to get into this area I guess, has floated the idea of electronic filing, ID systems, etc.

11.12.8. Comments on national ID cards

- That some people will be able to skirt the system, or that the system will ultimately be unenforceable, does not lessen the concern. Things can get real tough in the meantime.
- I see great dangers here, in tying a national ID card to transactions we are essentially unable to avoid in this society: driving, insurance (and let's not argue insurance...I mean it is unavoidable in the sense of legal issues, torts, etc.), border crossings, etc. Now how will one file taxes without such a card if one is made mandatory for interactions with the government? Saying "taxes are not collectable" is not an adequate answer. They may not be collectible for street punks and others who inhabit the underground economy, but they sure are for most of us.

11.13. National Health Care System Issues

11.13.1. Insurance and National Health Care will Produce the "National ID" that will be Nearly Unescapable

- hospitals and doctors will have to have the card...cash payments will evoke suspicion and may not even be feasible

11.13.2. I'm less worried that a pharmacist will add me to some database he keeps than that my doctor will be instructed to compile a dossier to government standards and then zip it off over the Infobahn to the authorities.

11.13.3. Dangers and issues of National Health Care Plan

- tracking, national ID card
- "If you think the BATF is bad, wait until the BHCRC goes into action. "What is the BHCRC?" you ask. Why, it the Burea of Health Care Reform Compliance Enforcement - the BATF, FBI, FDA, CIA and IRS all rolled into one." [Dave Feustel, talk.politics.guns, 1994-08-19]
- Bill Stewart has pointed out the dangers of children having social security numbers, of tracking systems in schools and hospitals, etc.

11.14. Credentials

11.14.1. This is one of the most overlooked and ignored aspects of cryptology, especially of Chaum's work. And no one in Cypherpunks or anywhere else is currently working on "blinded credentials" for everyday use.

11.14.2. "Is proof of identity needed?"

- This question is debated a lot, and is important. Talk of a national ID card (what wags call an "internal passport") is in the air, as part of health care, welfare, and immigration legislation. Electronic markets make this also

an issue for the ATM/smart card community. This is also closely tied in with the nature of anonymous reamailers (where physical identity is of course generally lacking).

- + First, "identity" can mean different things:
 - Conventional View of Identity: Physical person, with birthdate, physical characteristics, fingerprints, social security numbers, passports, etc.--the whole cloud of "identity" items. (Biometric.)
 - Pseudonym View of Identity: Persistent personnas, mediated with cryptography. "You are your key."
 - Most of us deal with identity as a mix of these views: we rarely check biometric credentials, but we also count on physical clues (voice, appearance, etc.). I assume that when I am speaking to "Duncan Frissell," whom I've never met in person, that he is indeed Duncan Frissell. (Some make the jump from this expectation to wanting the government enforce this claim, that is, provided I.D.)
 - + It is often claimed that physical identity is important in order to:
 - track down cheaters, welchers, contract breakers, etc.
 - permit some people to engage in some transactions, and forbid others to (age credentials, for drinking, for example, or---less benignly---work permits in some field)
 - taxation, voting, other schemes tied to physical existence
 - + But most of us conduct business with people without ever verifying their identity credentials...mostly we take their word that they are "Bill Stewart" or "Scott Collins," and we never go beyond that.
 - this could change as digital credentials proliferate and as interactions cause automatic checks to be made (a reason many of us have to support Chaum's "blinded credentials" idea--without some crypto protections, we'll be constantly tracked in all interactions).
 - + A guiding principle: Leave this question of whether to demand physical ID credentials up to the *parties involved*. If Alice wants to see Bob's "is-a-person" credential, and take his palmprint, or whatever, that's an issue for them to work out. I see no moral reason, and certainly no communal reason, for outsiders to interfere and insist that ID be produced (or that ID be forbidden, perhaps as some kind of "civil rights violation"). After all, we interact in cyberspace, on the Cypherpunks list, without any such external controls on identity.
 - and business contracts are best negotiated locally, with external enforcement contracted by the parties (privately-produced law, already seen with insurance companies, bonding agents, arbitration arrangements, etc.)
 - Practically speaking, i.e., not normatively speaking, people will find ways around identity systems. Cash is one way, remailers are another. Enforcement of a rigid identity-based system is difficult.
- 11.14.3. "Do we need "is-a-person" credentials for things like votes on the Net?"
- That is, any sysadmin can easily create as many user accounts as he wishes. And end users can sign up with various services under various names. The concern is that

this Chicago-style voting (fictitious persons) may be used to skew votes on Usenet.

- Similar concerns arise elsewhere.
- In my view, this is a mighty trivial reason to support "is-a-person" credentials.

11.14.4. Locality, credentials, validations

- + Consider the privacy implications of something so simple as a parking lot system. Two main approaches:
 - First Approach. Cash payment. Car enters lot, driver pays cash, a "validation" is given. No traceability exists. (There's a small chance that one driver can give his sticker to a new driver, and thus defraud the parking lot. This tends not to happen, due to the inconveniences of making a market in such stickers (coordinating with other car, etc.) and because the sticker is relatively inexpensive.)
 - Second Approach. Billing of driver, recording of license plates. Traceability is present, especially if the local parking lot is tied in to credit card companies, DMV, police, etc. (these link-ups are on the wish list of police agencies, to further "freeze out" fugitives, child support delinquents, and other criminals).
- These are the concerns of a society with a lot of electronic payments but with no mechanisms for preserving privacy. (And there is currently no great demand for this kind of privacy, for a variety of reasons, and this undercuts the push for anonymous credential methods.)
- An important property of true cash (gold, bank notes that are well-trusted) is that it settles immediately, requiring no time-binding of contracts (ability to track down the payer and collect on a bad transaction)

11.15. Records of all UseNet postings

11.15.1. (ditto for CompuServe, GEnie, etc.) will exist

11.15.2. "What kinds of monitoring of the Net is possible?"

- Archives of all Usenet traffic. This is already done by commercial CD-ROM suppliers, and others, so this would be trivial for various agencies.
- Mail archives. More problematic, as mail is ostensibly not public. But mail passes through many sites, usually in unencrypted form.
- Traffic analysis. Connections monitored. Telnet, ftp, e-mail, Mosaic, and other connections.
- Filtered scans of traffic, with keyword-matched text stored in archives.

11.15.3. Records: note that private companies can do the same thing, except that various "right to privacy" laws may try to interfere with this

- which causes its own constitutional privacy problems, of course

11.15.4. "How can you expect that something you sent on the UseNet to several thousand sites will not be potentially held against you? You gave up any pretense of privacy when you broadcast your opinions--and even detailed declarations of your activities--to an audience of millions. Did you really think that these public messages weren't being filed away? Any private citizen would find it almost straightforward to sort

a measly several megabytes a day by keywords, names of posters, etc." [I'm not sure if I wrote this, or if someone else who I forgot to make a note of did]

11.15.5. this issue is already coming up: a gay programmer who was laid-off discussed his rage on one of the gay boards and said he was thinking of turning in his former employer for widespread copying of Autocad software...an Autodesk employee answered him with "You just did!"

11.15.6. corporations may use GREP and On Location-like tools to search public nets for any discussion of themselves or their products

- by big mouth employees, by disgruntled customers, by known critics, etc.
- even positive remarks that may be used in advertising (subject to various laws)

11.15.7. the 100% traceability of public postings to UseNet and other bulletin boards is very stifling to free expression and becomes one of the main justifications for the use of anonymous (or pseudonymous) boards and nets

- there may be calls for laws against such compilation, as with the British data laws, but basically there is little that can be done when postings go to tens of thousands of machines and are archived in perpetuity by many of these nodes and by thousands of readers
- readers who may incorporate the material into their own postings, etc. (hence the absurdity of the British law)

11.16. Effects of Surveillance on the Spread of Crypto

11.16.1. Surveillance and monitoring will serve to increase the use of encryption, at first by people with something to hide, and then by others

- a snowballing effect
- and various government agencies will themselves use encryption to protect their files and their privacy

11.16.2. for those in sensitive positions, the availability of new bugging methods will accelerate the conversion to secure systems based on encrypted telecommunications and the avoidance of voice-based systems

11.16.3. Surveillance Trends

- + Technology is making citizen-unit surveillance more and more trivial
 - + video cameras on every street corners are technologically easy to implement, for example
 - or cameras in stores, in airports, in other public places
 - traffic cameras
 - tracking of purchases with credit cards, driver's licenses, etc.
 - monitoring of computer emissions (TEMPEST issues, often a matter of paranoid speculation)
- + interception of the Net...wiretapping, interception of unencrypted communications, etc.
 - and compilation of dossier entries based on public postings
- + This all makes the efforts to head-off a person-tracking, credentials-based society all the more urgent.
Monkeywrenching, sabotage, public education, and

development of alternatives are all needed.

- If the surveillance state grows as rapidly as it now appears to be doing, more desperate measures may be needed. Personally, I wouldn't shed any tears if Washington, D.C. and environs got zapped with a terrorist nuke; the innocents would be replaced quickly enough, and the death of so many political ghouls would surely be worth it. The destruction of Babylon.
- + We need to get the message about "blinded credentials" (which can show some field, like age, without showing all fields, including name and such) out there. More radically, we need to cause people to question why credentials are as important as many people seem to think.
 - I argue that credentials are rarely needed for mutually agreed-upon transactions

11.17. Loose Ends

11.17.1. USPS involvement in electronic mail, signatures, authentication (proposed in July-August, 1994)

- + Advantages:
 - many locations
 - a mission already oriented toward delivery
- + Disadvantages:
 - has performed terribly, compared to allowed competition (Federal Express, UPS, Airborne, etc.)
 - it's linked to the government (now quasi-independent, but not really)
 - could become mandatory, or competition restricted to certain niches (as with the package services, which cannot have "routes" and are not allowed to compete in the cheap letter regime)
 - a large and stultified bureaucracy, with union labor
- Links to other programs (software key escrow, Digital Telephony) not clear, but it seems likely that a quasi-government agency like the USPS would be cooperative with government, and would place limits on the crypto systems allowed.

11.17.2. the death threats

- + An NSA official threatened to have Jim Bidzos killed if he did not change his position on some negotiation underway. This was reported in the newspaper and I sought confirmation:
 - "Everything reported in the Merc News is true. I am certain that he wasnot speaking for the agency, but when it happened he was quite serious, at least appeared to be. There was a long silence after he made the threat, with a staring contest. He was quite intense.

"I respect and trust the other two who were in the room (they were shocked and literally speechless, staring into their laps) and plan to ask NSA for a written apology and confirmation that he was not speaking for the agency. We'll see if I get it. If the incident made it into their trip reports, I have a chance of getting a letter." [jim@RSA.COM (Jim Bidzos), personal communication, posted with permission to talk.politics.crypto, 1994-06-28]

11.17.3. False identities...cannot just be "erased" from the computer memory banks. The web of associations, implications, rule firings...all mean that simple removal (or insertion of a false identity) produces discontinuities, illogical developments, holes...history is not easily changed.

12. Digital Cash and Net Commerce

12.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

12.2. SUMMARY: Digital Cash and Net Commerce

12.2.1. Main Points

- strong crypto makes certain forms of digital cash possible
- David Chaum is, once again, centrally involved
- no real systems deployed, only small experiments
- the legal and regulatory tangle will likely affect deployment in major ways (making a "launch" of digital cash a nontrivial matter)

12.2.2. Connections to Other Sections

- reputations
- legal situation
- crypto anarchy

12.2.3. Where to Find Additional Information

- <http://digicash.support.nl/>

12.2.4. Miscellaneous Comments

- a huge area, filled with special terms
- many financial instruments
- the theory of digital cash is not complete, and confusion abounds
- this section is also more jumbled and confusing than I'd like; I'll clean it up in future releases.

12.3. The Nature of Money

12.3.1. The nature of money, of banking and finance, is a topic that suffuses most discussions of digital cash. Hardly surprising.

But also an area that is even more detailed than is crypto. And endless confusion of terms, semantic quibblings on the list, and so on. I won't be devoting much space to trying to explain economics, banking, and the deep nature of money.

12.3.2. There are of course many forms of cash or money today (these terms are not equivalent...)

- + coins, bills (presumed to be difficult to forge)
 - "ontological conservation laws"--the money can't be in two places at once, can't be double spent
 - this is only partly true, and forgery technology is making it all moot
- bearer bonds and other "immediately cashable" instruments
- diamonds, gold, works of art, etc. ("portable wealth")

12.3.3. Many forms of digital money. Just as there are dozens of major forms of instruments, so too will there be many forms of digital money. Niches will be filled.

12.3.4. The deep nature of money is unclear to me. There are days

when I think it's just a giant con game, with value in money only because others will accept it. Other days when I think it's somewhat tied to "real things" like gold and silver. And other days when I'm just unconcerned (so long as I have it, and it works).

12.3.5. The digital cash discussions get similarly confused by the various ideas about money. Digital cash is not necessarily a form of currency, but is instead a transfer mechanism. More like a "digital check," in fact (though it may give rise to new currencies, or to wider use of some existing currency...at some point, it may become indistinguishable from a currency).

12.3.6. I advise that people not worry overly much about the true and deep nature of money, and instead think about digital cash as a transfer protocol for some underlying form of money, which might be gold coins, or Swiss francs, or chickens, or even giant stone wheels.

12.3.7. Principle vs. Properties of Money

- Physical coins, as money, have certain basic properties:
 - difficult to counterfeit, pointless to counterfeit if made of gold or silver, fungibility, immediate settling (no need to clear with a distant bank, no delays, etc.), untraceability, etc.
- Digital cash, in various flavors, has dramatically different properties, e.g., it may require clearing, any single digital note is infinitely copyable, it may allow traceability, etc. A complicated mix of properties.
- + But why is physical money (specie) the way it is? What properties account for this? What are the core principles that imply these properties?
 - hardware (specie like gold) vs. software (bits, readily copyable)
 - immediate, local clearing, because of rational faith that the money will clear
 - limits on rate of transfer of physical money set by size, weight of money, whereas "wire fraud" and variants can drain an account in seconds
- My notion is that we spend too much time thinking about the principles (such as locality, transitivity, etc.) and expect to then derive the properties. Maybe we need to instead focus on the objects, the sets of protocol-derived things, and examine their emergent properties. (I have my own thinking along these lines, involving "protocol ecologies" in which agents bang against each other, a la Doug Lenat's old "Eurisko" system, and thus discover weaknesses, points of strength, and even are genetically programmed to add new methods which increase security. This, as you can guess, is a longterm, speculative project.)

12.3.8. "Can a "digital coin" be made?"

- The answer appears to be "no"
- + Software is infinitely copyable, which means a software representation of digital money could be replicated many times
 - this is not to say it could be spent many times, depending on the clearing process...but then this is not a "coin" in the sense we mean

- Software is trivially replicable, unlike gold or silver coins, or even paper currency. If and when paper currency becomes trivially replicable (and color copiers have almost gotten there), expect changes in the nature of cash. (Speculation: cash will be replaced by smart cards, probably not of the anonymous sort we favor.)
- + bits can always be duplicated (unless tied to hardware, as with TRMs), so must look elsewhere
- + could tie the bits to a specific location, so that duplication would be obvious or useless
 - the idea is vaguely that an agent could be placed in some location...duplications would be both detectable and irrelevant (same bits, same behavior, unmodifiable because of digital signature)
- (this is formally similar to the idea of an active agent that is unforgeable, in the sense that the agent or coin is "standalone")

12.3.9. "What is the 'granularity' of digital cash?"

- + fine granularity, e.g., sub-cent amounts
 - useful for many online transactions
 - inside computers
 - add-on fees by intermediaries
 - very small purchases
- + medium granularity
 - a few cents, up to a dollar (for example)
 - also useful for many small purchases
 - close equivalent to "loose change" or small bills, and probably useful for the same purposes
 - tolls, fees, etc.
 - This is roughly the level many DigiCash protocols are aimed at
- + large granularity
 - multiple dollars
 - more like a "conventional" online transaction
 -
 - the transaction costs are crucial; online vs. offline clearing
 - Digital Silk Road is a proposal by Dean Tribble and Norm Hardy to reduce transaction costs

12.3.10. Debate about money and finance gets complicated

- legal terms, specific accounting jargon, etc.
- I won't venture into this thicket here. It's a specialty unto itself, with several dozen major types of instruments and derivatives. And of course with big doses of the law.

12.4. Smart Cards

12.4.1. "What are smart cards and how are they used?"

- + Most smart cards as they now exist are very far from being the anonymous digital cash of primary interest to us. In fact, most of them are just glorified credit cards.
 - with no gain to consumers, since consumers typically don't pay for losses by fraud
 - (so to entice consumers, will they offer inducements?)
- Can be either small computers, typically credit-card-sized, or just cards that control access via local computers.
- + Tamper-resistant modules, e.g., if tampered with, they destroy the important data or at the least give evidence of

- having been tampered with.
- + Security of manufacturing
 - some variant of "cut-and-choose" inspection of premises
- + Uses of smart cards
 - conventional credit card uses
 - bill payment
 - postage
 - bridge and road tolls
 - payments for items received electronically (not necessarily anonymously)
- 12.4.2. Visa Electronic Purse
- 12.4.3. Mondex

- 12.5. David Chaum's "DigiCash"
- 12.5.1. "Why is Chaum so important to digital cash?"
 - Chaum's name appears frequently in this document, and in other Cypherpunk writings. He is without a doubt the seminal thinker in this area, having been very nearly the first to write about several areas: untraceable e-mail, digital cash, blinding, unlinkable credentials, DC-nets, etc.
 - I spoke to him at the 1988 "Crypto" conference, telling him about my interests, my 'labyrinth' idea for mail-forwarding (which he had anticipated in 1981, unbeknownst to me at the time), and a few hints about "crypto anarchy." It was clear to me that Chaum had thought long and deeply about these issues.
 - Chaum's articles should be read by all interested in this area. (No, his papers are not "on-line." Please see the "Crypto" Proceedings and related materials.)
 - [DIGICASH PRESS RELEASE, "World's first electronic cash payment over computer networks," 1994-05-27]
- 12.5.2. "What's his motivation?"
 - Chaum appears to be a libertarian, at least on social issues, and is very worried about "Big Brother" sorts of concerns (recall the title of his 1985 CACM article).
 - His work in Europe has mostly concentrated on unlinkable credentials for toll road payments, electronic voting, etc. His company, DigiCash, is working on various aspects of digital cash.
- 12.5.3. "How does his system work?"
 - There have been many summaries on the Cypherpunks list. Hal Finney has written at least half a dozen, and others have been contributed by Eric Hughes, Karl Barrus, etc. I won't be including any of them here....it just takes too many pages to explain how digital cash works in detail.
 - (The biggest problem people have with digital cash is in not taking the time to understand the basics of the math, of blinding, etc. They wrongly assume that "digital cash" can be understood by common-sense reasoning about existing cash, etc. This mistake has been repeated in several of the half-assed proposals for "net cash" and "digi dollars.")
- + Here's the opening few paragraphs from one of Hal's explanations, to provide a glimpse:
 - "Mike Ingle asks about digicash. The simplest system I know of that is anonymous is the one by Chaum, Fiat, and

Naor, which we have discussed here a few times. The idea is that the bank chooses an RSA modulus, and a set of exponents e_1, e_2, e_3, \dots , where each exponent e_i represents

a denomination and possibly a date. The exponents must be relatively prime to $(p-1)(q-1)$. PGP has a GCD routine which can be used to check for valid exponents..

"As with RSA, to each public exponent e_i corresponds a secret exponent d_i , calculated as the multiplicative inverse of $e_i \bmod (p-1)(q-1)$. Again, PGP has a routine to calculate multiplicative inverses.

"In this system, a piece of cash is a pair $(x, f(x)^{d_i})$, where $f()$ is a one-way function. MD5 would be a reasonable choice for $f()$, but notice that it produces a 128-bit result. $f()$ should take this 128-bit output of MD5 and "reblock" it to be an multi-precision number by padding it; PGP has a "preblock" routine which does this, following the PKCS standard.

"The way the process works, with the blinding, is like this. The user chooses a random x . This should probably be at least 64 or 128 bits, enough to preclude exhaustive search. He calculates $f(x)$, which is what he wants the bank to sign by raising to the power d_i . But rather than sending $f(x)$ to the bank directly, the user first blinds it by choosing a random number r , and calculating $D=f(x) * r^{e_i}$. (I should make it clear that \wedge is the power operator, not xor.) D is what he sends to the bank, along with some information about what e_i is, which tells the denomination of the cash, and also information about his account number." [Hal Finney, 1993-12-04]

12.5.4. "What is happening with DigiCash?"

- "Payment from any personal computer to any other workstation, over email or Internet, has been demonstrated for the first time, using electronic cash technology. "You can pay for access to a database, buy software or a newsletter by email, play a computer game over the net, receive \$5 owed you by a friend, or just order a pizza. The possibilities are truly unlimited" according to David Chaum, Managing Director of DigiCash TM, who announced and demonstrated the product during his keynote address at the first conference on the World Wide Web, in Geneva this week." [DIGICASH PRESS RELEASE, "World's first electronic cash payment over computer networks," 1994-05-27]
- DigiCash is David Chaum's company, set up to commercialize this work. Located near Amsterdam.
- + Chaum is also centrally involved in "CAFE," a European committee investigating ways to deploy digital cash in Europe
 - mostly standards, issues of privacy, etc.
 - toll roads, ferries, parking meters, etc.
- <http://digicash.support.nl/>
- info@digicash.nl
- People have been reporting that their inquiries are not being answered; could be for several reasons.

12.5.5. The Complexities of Digital Cash

- There is no doubt as to the complexity: many protocols, semantic confusion, many parties, chances for collusion, spoofing, repudiation, and the like. And many derivative entities: agents, escrow services, banks.
- There's no substitute for thinking hard about various scenarios. Thinking about how to arrange off-line clearing, how to handle claims of people who claim their digital money was stolen, people who want various special kinds of services, such as receipts, and so on. It's an ecology here, not just a set of simple equations.

12.6. Online and Offline Clearing, Double Spending

12.6.1. (this section still under construction)

12.6.2. This is one of the main points of division between systems.

12.6.3. Online Clearing

- (insert explanation)

12.6.4. Offline Clearing

- (insert explanation)

12.6.5. Double spending

- Some approaches involve constantly-growing-in-size coins at each transfer, so who spent the money first can be deduced (or variants of this). And N. Ferguson developed a system allowing up to N expenditures of the same coin, where N is a parameter. [Howard Gayle reminded me of this, 1994-08-29]
- "Why does everyone think that the law must immediately be invoked when double spending is detected?...Double spending is an informational property of digital cash systems. Need we find malicious intent in a formal property? The obvious moralism about the law and double spenders is inappropriate. It evokes images of revenge and retribution, which are stupid, not to mention of negative economic value." [Eric Hughes, 1994-08-27] (This also relates to Eric's good point that we too often frame crypto issue in terms of loaded terms like "cheating," "spoofing," and "enemies," when more neutral terms would carry less meaning-obscurating baggage and would not give our "enemies" (:~}) the ammunition to pass laws based on such terms.)

12.6.6. Issues

- + Chaum's double-spending detection systems
 - Chaum went to great lengths to develop system which preserve anonymity for single-spending instances, but which break anonymity and thus reveal identity for double-spending instances. I'm not sure what market forces caused him to think about this as being so important, but it creates many headaches. Besides being clumsy, it require physical ID, it invokes a legal system to try to collect from "double spenders," and it admits the extremely serious breach of privacy by enabling stings. For example, Alice pays Bob a unit of money, then quickly Alice spends that money before Bob can...Bob is then revealed as a "double spender," and his identity revealed to whomver wanted it...Alice, IRS, Gestapo, etc. A very broken idea. Acceptable mainly for small transactions.
- + Multi-spending vs. on-line clearing
 - I favor on-line clearing. Simply put: the first spending is the only spending. The guy who gets to the train

locker where the cash is stored is the guy who gets it. This ensure that the burden of maintaining the secret is on the secret holder.

- When Alice and Bob transfer money, Alice makes the transfer, Bob confirms it as valid (or verifies that his bank has received the deposit), and the transaction is complete.
- With network speeds increasing dramatically, on-line clearing should be feasible for most transactions. Off-line systems may of course be useful, especially for small transactions, the ones now handled with coins and small bills.

12.6.7. "How does on-line clearing of anonymous digital cash work?"

- There's a lot of math connected with blinding, exponentions, etc. See Schneier's book for an introduction, or the various papers of Chaum, Brands, Bos, etc.
- On-line clearing is similar to two parties in a transaction exchanging goods and money. The transaction is cleared locally, and immediately. Or they could arrange transfer of funds at a bank, and the banker could tell them over the phone that the transaction has cleared--true "on-line clearing." Debit cards work this way, with money transferred effectively immediately out of one account and into another. Credit cards have some additional wrinkles, such as the credit aspect, but are basically still on-line clearing.
- Conceptually, the guiding principle idea is simple: he who gets to the train locker where the cash is stored *first* gets the cash. There can never be "double spending," only people who get to the locker and find no cash inside. Chaumian blinding allows the "train locker" (e.g., Credit Suisse) to give the money to the entity making the claim without knowing how the number correlates to previous numbers they "sold" to other entities. Anonymity is preserved, absolutely. (Ignoring for this discussion issues of cameras watching the cash pickup, if it ever actually gets picked up.)
- Once the "handshaking" of on-line clearing is accepted, based on the "first to the money gets it" principle, then networks of such clearinghouses can thrive, as each is confident about clearing. (There are some important things needed to provide what I'll dub "closure" to the circuit. People need to ping the system, depositing and withdrawing, to establish both confidence and cover. A lot like remailer networks. In fact, very much like them.)
- In on-line clearing, only a number is needed to make a transfer. Conceptually, that is. Just a number. It is up to the holder of the number to protect it carefully, which is as it should be (for reasons of locality, or self-responsibility, and because any other option introduces repudiation, disavowal, and the "Twinkies made me do it" sorts of nonsense). Once the number is transferred and reblinded, the old number no longer has a claim on the money stored at Credit Suisse, for example. That money is now out of the train locker and into a new one. (People always ask, "But where is the money, really?" I see digital

cash as *claims* on accounts in existing money-holding places, typically banks. There are all kinds of "claims"-- Eric Hughes has regaled us with tales of his explorations of the world of commercial paper. My use of the term "claim" here is of the "You present the right number, you get access" kind. Like the combination to a safe. The train locker idea makes this clearer, and gets around the confusion about "digimarks" of "e\$" actually being any kind of money it and of itself.)

12.7. Uses for Digital Cash

12.7.1. Uses for digital cash?

- Privacy protection
- Preventing tracking of movements, contacts, preferences
- + Illegal markets
 - gambling
 - bribes, payoffs
 - assassinations and other contract crimes
 - fencing, purchases of goods
- + Tax avoidance
 - income hiding
 - offshore funds transfers
 - illegal markets
- Online services, games, etc.
- + Agoric markets, such as for allocation of computer resources
 - where programs, agents "pay" for services used, make "bids" for future services, collect "rent," etc.
- + Road tolls, parking fees, where unlinkability is desired. This press release excerpt should give the flavor of intended uses for road tolls:
 - "The product was developed by DigiCash TM Corporation's wholly owned Dutch subsidiary, DigiCash TM BV. It is related to the firm's earlier released product for road pricing, which has been licensed to Amtech TM Corporation, of Dallas, Texas, worldwide leader in automatic road toll collection. This system allows privacy protected payments for road use at full highway speed from a smart card reader affixed to the inside of a vehicle. Also related is the approach of the EU supported CAFE project, of which Dr. Chaum is Chairman, which uses tamper-resistant chips inserted into electronic wallets." [DIGICASH PRESS RELEASE, "World's first electronic cash payment over computer networks," 1994-05-27]

12.7.2. "What are some motivations for anonymous digital cash?"

- + Payments that are unlinkable to identity, especially for things like highway tolls, bridge tolls, etc.
 - where linkability would imply position tracking
 - (Why not use coins? This idea is for "smart card"-type payment systems, involving wireless communication. Singapore planned (and perhaps has implemented) such a system, except there were no privacy considerations.)
- + Pay for things while using pseudonyms
 - no point in having a pseudonym if the payment system reveals one's identity
- + Tax avoidance
 - this is the one the digicash proponents don't like to

talk about too loudly, but it's obviously a time-honored concern of all taxpayers

- + Because there is no compelling reason why money should be linked to personal identity
- a general point, subsuming others

12.8. Other Digital Money Systems

12.8.1. "There seem to be many variants....what's the story?"

- Lots of confusion. Lots of systems that are not at all anonymous, that are just extensions of existing systems. The cachet of digital cash is such that many people are claiming their systems are "digital cash," when of course they are not (at least not in the Chaum/Cypherpunk sense).
- So, be careful. Caveat emptor.

12.8.2. Crypto and Credit Cards (and on-line clearing)

- + Cryptographically secure digital cash may find a major use in effectively extending the modality of credit cards to low-level, person-to-person transactions.
- That is, the convenience of credit cards is one of their main uses (others being the advancing of actual credit, ignored here). In fact, secured credit cards and debit cards don't offer this advancement of credit, but are mainly used to accrue the "order by phone" and "avoid carrying cash" advantages.
- Checks offer the "don't carry cash" advantage, but take time to clear. Traveller's checks are a more pure form of this.
- But individuals (like Alice and Bob) cannot presently use the credit card system for mutual transactions. I'm not sure of all the reasons. How might this change?
- Crypto can allow unforgeable systems, via some variant of digital signatures. That is, Alice can accept a phoned payment from Bob without ever being able to sign Bob's electronic signature herself.
- "Crypto Credit Cards" could allow end users (customers, in today's system) to handle transactions like this, without having merchants as intermediaries.
- I'm sure the existing credit card outfits would have something to say about this, and there may be various roadblocks in the way. It might be best to buy off the VISA and MasterCard folks by working through them. (And they probably have studied this issue; what may change their positions is strong crypto, locally available to users.)
- (On-line clearing--to prevent double-spending and copying of cash--is an important aspect of many digital cash protocols, and of VISA-type protocols. Fortunately, networks are becoming ubiquitous and fast. Home use is still a can of worms, though, with competing standards based on video cable, fiber optics, ISDN, ATM, etc.)

12.8.3. Many systems being floated. Here's a sampling:

- + Mondex
 - "Unlike most other electronic purse systems, Mondex, like cash, is anonymous. The banks that issue Mondex cards will not be able to keep track of who gets the payments. Indeed, it is the only system in which two card holders can transfer money to each other.

"If you want to have a product that replaces cash, you have to do everything that cash does, only better," Mondex's senior executive, Michael Keegan said. "You can give money to your brother who gives it to the chap that sells newspapers, who gives it to charity, who puts it in the bank, which has no idea where it's been. That's what money is." [New York Times, 1994-09-06, provided by John Young]

+ CommerceNet

- allows Internet users to buy and sell goods.
- "I read in yesterday's L.A. Times about something called CommerceNet, where sellers and buyers of workstation level equipment can meet and conduct business....Near the end of the article, they talked about a proposed method for exchanging "digital signatures" via Moasic (so that buyers and sellers could know that they were who they said they were) and that they were going to "submit it to the Internet Standards body" [Cypher1@aol.com, 1994-06-23]

+ NetCash

- paper published at 1st ACM Conference on Computer and Communications Security, Nov. 93, available via anonymous ftp from PROSPERO.ISI.EDU as /pub/papers/security/netcash-cccs93.ps.Z
- "NetCash: A design for practical electronic currency on the Internet ... Gennady Medvinsky and Clifford Neuman

"NetCash is a framework that supports realtime electronic payments with provision of anonymity over an unsecure network. It is designed to enable new types of services on the Internet which have not been practical to date because of the absence of a secure, scalable, potentially anonymous payment method.

"NetCash strikes a balance between unconditionally anonymous electronic currency, and signed instruments analogous to checks that are more scalable but identify the principals in a transaction. It does this by providing the framework within which proposed electronic currency protocols can be integrated with the scalable, but non-anonymous, electronic banking infrastructure that has been proposed for routine transactions."

+ Hal Finney had a negative reaction to their system:

- "I didn't think it was any good. They have an incredibly simplistic model, and their "protocols" are of the order, A sends the bank some paper money, and B sends A some electronic cash in return.....They don't even do blinding of the cash. Each piece of cash has a unique serial number which is known to the currency provider. This would of course allow matching of withdrawn and deposited coins....These guys seem to have read the work in the field (they reference it) but they don't appear to have understood it." [Hal Finney, 1993-08-17]

+ VISA Electronic Purse

- (A lot of stuff appeared on this, including listings of the alliance partners (like Verifone), the technology,

the plans for deployment, etc. I regret that I can't include more here. Maybe when this FAQ is a Web doc, more can be included.)

- "PERSONAL FINANCE - Seeking the Card That Would Create A Cashless World. The Washington Post, April 03, 1994, FINAL Edition By: Albert B. Crenshaw, Washington Post ...

"Now that credit cards are in the hands of virtually every living, breathing adult in the country-not to mention a lot of children and the occasional family pet-and now that almost as many people have ATM cards, card companies are wondering where future growth will come from.

"At *Visa* International, the answer is: Replace cash with plastic.

"Last month, the giant association of card issuers announced it had formed a coalition of banking and technology companies to develop technical standards for a product it dubbed the "Electronic Purse," a plastic card meant to replace coins and bills in small transactions." [provided by Duncan Frissell, 1994-04-05]

- The talk of "clearinghouses" and the involvement of VISA International and the Usual Suspects suggest identity-blinding protocols are not in use. I also see no mention of DigiCash, or even RSA (but maybe I missed that-and the presence of RSA would not necessarily mean identity-blinding protocols were being planned).

Likely Scenario: This is *not* digital cash as we think of it. Rather, this is a future evolution of the cash ATM card and credit card, optimized for faster and cheaper clearing.

Scary Scenario: This could be the vehicle for the long-rumored "banning of cash." (Just because conspiracy theorists and Number of the Beast Xtian fundamentalists believe it doesn't render it implausible.)

- Almost nothing of interest for us. No methods for anonymity. Make no mistake, this is not the digital cash that Cypherpunks espouse. This gives the credit agencies and the government (the two work hand in hand) complete traceability of all purchases, automatic reporting of spending patterns, target lists for those who frequent about-to-be-outlawed businesses, and invasive surveillance of all inter-personal economic transactions. This is the AntiCash. Beware the Number of the AntiCash.

12.8.4. Nick Szabo:

- "Internet commercialization in itself is a huge issue full of pitfall and opportunity: Mom & Pop BBS's, commercial MUDs, data banks, for-profit pirate and porn boards, etc. are springing up everywhere like weeds, opening a vast array of both needs of privacy and ways to abuse privacy. Remailers, digital cash, etc. won't become part of this Internet commerce way of life unless they are deployed soon, theoretical flaws and all, instead of

waiting until The Perfect System comes along. Crypto-anarchy in the real world will be messy, "nature red in tooth and claw", not all nice and clean like it says in the math books. Most of the debugging will be done not in any ivory tower, but by the bankruptcy of businesses who violate their customer's privacy, the confiscation of BBS operators who stray outside the laws of some jurisdiction and screw up their privacy arrangements, etc. Anybody who thinks they can flesh out a protocol in secret and then deploy it, full-blown and working, is in for a world of hurt. For those who get their Pretty Good systems out there and used, there is vast potential for business growth -- think of the \$trillions confiscated every year by governments around the world, for example." [Nick Szabo, 1993-8-23]

12.8.5. "What about _non-anonymous_ digital cash?"

- a la the various extensions of existing credit and debit cards, traveller's checks, etc.
- + There's still a use for this, with several motivations"
 - * for users, it may be cheaper (lower transaction costs) than fully anonymous digital cash
 - * for banks, it may also be cheaper
 - * users may wish audit trails, proof, etc.
 - * and of course governments have various reasons for wanting traceable cash systems
 - law enforcement
 - taxes, surfacing the underground economy

12.8.6. Microsoft plans to enter the home banking business

- "PORTLAND, Ore. (AP) -- Microsoft Corp. wants to replace your checkbook with a home computer that lets the bank do all the work of recording checks, tallying up credit card charges and paying bills.... The service also tracks credit card accounts, withdrawals from automated teller machines, transfers from savings or other accounts, credit lines, debit cards, stocks and other investments, and bill payments." [Associated Press, 1994-07-04]
- Planned links with a consortium of banks, led by U.S. Bancorp, using its "Money" software package.
- Comment: Such moves as this--and don't forget the cable companies--could result in a rapid transition to a form of home banking and "digital money." Obviously this kind of digital money, as it is being planned today, is very from the kind of digital cash that interests us. In fact, it is the polar opposite of what we want.

12.8.7. Credit card clearing...individuals can't use the system

- if something nonanonymous like credit cards cannot be used by end users (Alice and Bob), why would we expect an anonymous version of this would be either easier to use or more possible?
- (And giving users encrypted links to credit agencies would at least stop the security problems with giving credit card numbers out over links that can be observed.)
- Mondex claims their system will allow this kind of person-to-person transfer of anonymous digital cash (I'll believe it when I see it).

12.9. Legal Issues with Digital Cash

- 10.8.1. "What's the legal status of digital cash?"
- It hasn't been tested, like a lot of crypto protocols. It may be many years before these systems are tested.
- 10.8.2. "Is there a tie between digital cash and money laundering?"
- There doesn't have to be, but many of us believe the widespread deployment of digital, untraceable cash will make possible new approaches
 - Hence the importance of digital cash for crypto anarchy and related ideas.
 - (In case it isn't obvious, I consider money-laundering a non-crime.)
- 10.8.3. "Is it true the government of the U.S. can limit funds transfers outside the U.S.?"
- Many issues here. Certainly some laws exist. Certainly people are prosecuted every day for violating currency export laws. Many avenues exist.
 - "LEGALITY - There isn't and will never be a law restricting the sending of funds outside the United States. How do I know? Simple. As a country dependant on international trade (billions of dollars a year and counting), the American economy would be destroyed." [David Johnson, privacy@well.sf.ca.us, "Offshore Banking & Privacy," alt.privacy, 1994-07-05]
- 10.8.4. "Are "alternative currencies" allowed in the U.S.? And what's the implication for digital cash of various forms?"
- Tokens, coupons, gift certificates are allowed, but face various regulations. Casino chips were once treated as cash, but are now more regulated (inter-casino conversion is no longer allowed).
 - Any attempt to use such coupons as an alternative currency face obstacles. The coupons may be allowed, but heavily regulated (reporting requirements, etc.).
 - Perry Metzger notes, bearer bonds are now illegal in the U.S. (a bearer bond represented cash, in that no name was attached to the bond--the "bearer" could sell it for cash or redeem it...worked great for transporting large amounts of cash in compact form).
- + Note: Duncan Frissell claims that bearer bonds are not illegal.
- "Under the Tax Equity and Fiscal Responsibility Act of 1982 (TEFRA), any interest payments made on **new** issues of domestic bearer bonds are not deductible as an ordinary and necessary business expense so none have been issued since then. At the same time, the Feds administratively stopped issuing treasury securities in bearer form. Old issues of government and corporate debt in bearer form still exist and will exist and trade for 30 or more years after 1982. Additionally, US residents can legally buy foreign bearer securities." [Duncan Frissell, 1994-08-10]
 - Someone else has a slightly different view: "The last US Bearer Bond issues mature in 1997. I also believe that to collect interest, and to redeem the bond at maturity, you must give your name and tax-id number to the paying agent. (I can check with the department here that handles it if anyone is interested in the pertinent OCC regs that apply)" [prig0011@gold.tc.umn.edu, 1994-08-10]

- I cite this gory detail to give readers some idea about how much confusion there is about these subjects. The usual advice is to "seek competent counsel," but in fact most lawyers have no clear ideas about the optimum strategies, and the run-of-the-mill advisor may mislead one dangerously. Tread carefully.
- This has implications for digital cash, of course.
- 10.8.5. "Why might digital cash and related technologies take hold early in illegal markets? That is, will the Mob be an early adopter?"
 - untraceability needed
 - and reputations matter to them
 - they've shown in the past that they will try new approaches, a la the money movements of the drug cartels, novel methods for security, etc.
- 10.8.6. "Electronic cash...will it have to comply with laws, and how?"
 - Concerns will be raised about the anonymity aspects, the usefulness for evading taxes and reporting requirements, etc.
 - a messy issue, sure to be debated and legislated about for many years
 - + split the cash into many pieces...is this "structuring"? is it legal?
 - some rules indicate the structuring per se is not illegal, only tax evasion or currency control evasion
 - what then of systems which automatically, as a basic feature, split the cash up into multiple pieces and move them?
- 10.8.7. Currency controls, flight capital regulations, boycotts, asset seizures, etc.
 - all are pressures to find alternate ways for capital to flow
 - all add to the lack of confidence, which, paradoxically to lawmakers, makes capital flight all the more likely
- 10.8.8. "Will banking regulators allow digital cash?"
 - Not easily, that's for sure. The maze of regulations, restrictions, tax laws, and legal rulings is daunting. Eric Hughes spent a lot of time reading up on the laws regarding banks, commercial paper, taxes, etc., and concluded much the same. I'm not saying it's impossible--indeed, I believe it will someday happen, in some form--but the obstacles are formidable.
 - + Some issues:
 - + Will such an operation be allowed to be centered or based in the U.S.?
 - What states? What laws? Bank vs. Savings and Loan vs. Credit Union vs. Securities Broker vs. something else?
 - + Will customers be able to access such entities offshore, outside the U.S.?
 - strong crypto makes communication possible, but it may be difficult, not part of the business fabric, etc. (and hence not so useful--if one has to send PGP-encrypted instructions to one's banker, and can't use the clearing infrastructure....)
 - + Tax collection, money-laundering laws, disclosure laws, "know your customer" laws....all are areas where a

- "digital bank" could be shut down forthwith. Any bank not filling out the proper forms (including mandatory reporting of transactions of certain amounts and types, and the Social Security/Taxpayer Number of customers) faces huge fines, penalties, and regulatory sanctions.
- and the existing players in the banking and securities business will not sit idly by while newcomers enter their market; they will seek to force newcomers to jump through the same hoops they had to (studies indicate large corporations actually like red tape, as it helps them relative to smaller companies)
 - Conclusion: Digital banks will not be "launched" without a **lot** of work by lawyers, accountants, tax experts, lobbyists, etc. "Lemonade stand digital banks" (TM) will not survive for long. Kids, don't try this at home!
 - (Many new industries we are familiar with--software, microcomputers--had very little regulation, rightly so. But the effect is that many of us are unprepared to understand the massive amount of red tape which businesses in other areas, notably banking, face.)
- 10.8.9. Legal obstacles to digital money. If governments don't want anonymous cash, they can make things tough.
- + As both Perry Metzger and Eric Hughes have said many times, regulations can make life very difficult. Compliance with laws is a major cost of doing business.
 - ~"The cost of compliance in a typical USA bank is 14% of operating costs."~ [Eric Hughes, citing an "American Banker" article, 1994-08-30]
 - + The maze of regulations is navigable by larger institutions, with staffs of lawyers, accountants, tax specialists, etc., but is essentially beyond the capabilities of very small institutions, at least in the U.S.
 - this may or may not remain the case, as computers proliferate. A "bank-in-a-box" program might help. My suspicion is that a certain size of staff is needed just to handle the face-to-face meetings and hoop-jumping.
 - + "New World Order"
 - U.S. urging other countries to "play ball" on banking secrecy, on tax evasion extradition, on immigration, etc.
 - this is closing off the former loopholes and escape hatches that allowed people to escape repressive taxation...the implications for digital money banks are unclear, but worrisome.
- 12.10. Prospects for Digital Cash Use
- 12.10.1. "If digital money is so great, why isn't it being used?"
- Hasn't been finished. Protocols are still being researched, papers are still being published. In any single area, such as toll road payments, it may be possible to deploy an application-specific system, but there is no "general" solution (yet). There is no "digital coin" or unforgeable object representing value, so the digital money area is more similar to the similarly nonsimple markets in financial instruments, commercial papers, bonds, warrants, checks, etc. (Areas that are not inherently simple and that have required lots of computerization and communications to

make manageable.)

- Flakiness of Nets. Systems crash, mail gets delayed inexplicably, subscriptions to lists get lunched, and all sorts of other breakages occur. Most interaction on the Nets involves a fair amount of human adaptation to changing conditions, screwups, workarounds, etc. These are not conditions that inspire confidence in automated money systems!
- Hard to Use. Few people will use systems that require generating code, clients, etc. Semantic gap (generating stuff on a Unix workstation is not at all like taking one's checkbook out). Protocols in crypto are generally hard to use and confusing.
- Lack of compelling need. Although people have tried various experiments with digital money tokens or coupons (Magic Money/Tacky Tokens, the HeX market, etc.), there is little real world incentive to experiment with them. And most of the denominated tokens are for truly trivial amounts of money, not for anything worth spending time learning. No marketplace for buyers to "wander around in." (You don't buy what you don't see.)
- Legal issues. The IRS does not look favorably on alternative currencies, especially if used in attempts to bypass ordinary tax collection schemes. This and related legal issues (redemptions into dollars) put a roadblock in front of serious plans to use digital money.
- Research Issues. Not all problems resolved. Still being developed, papers being published. Chaum's system does not seem to be fully ready for deployment, certainly not outside of well-defined vertical markets.

12.10.2. "Why isn't digital money in use?"

- The Meta Issue: *what* digital money? Various attempts at digital cash or digital money exist, but most are flawed, experimental, crufty, etc. Chaum's DigiCash was announced (Web page, etc.), but is apparently not even remotely usable.
- + Practical Reasons:
 - nothing to buy
 - no standard systems that are straightforward to use
 - advantages of anonymity and untraceability are seldom exploited
- The Magic Money/Tacky Tokens experiment on the Cypherpunks list is instructive. Lots of detailed work, lots of posts-- and yet not used for anything (granted, there's not much being bought and sold on the List, so...).
- Scenario for Use in the Near Future: A vertical application, such as a bridge toll system that offers anonymity. In a vertical app, the issues of compatibility, interfaces, and training can be managed.

12.10.3. "why isn't digital cash being used?"

- + many reasons, too many reasons!
 - + hard issues, murky issues
 - technical developments not final, Chaum, Brands, etc.
 - + selling the users
 - who don't have computers, PDAs, the means to do the local computations
 - who want portable versions of the same

- + The infrastructure for digital money (Chaum anonymous-style, and variants, such as Brands) does not now exist, and may not exist for several more years. (Of course, I thought it would take "several more years" back in 1988, so what do I know?)
 - The issues are familiar: lack of standards, lack of protocols, lack of customer experience, and likely regulatory hurdles. A daunting prospect.
 - Any "launches" will either have to be well-funded, well-planned, or done sub rosa, in some quasi-legal or even illegal market (such as gambling).
- "The American people keep claiming in polls that they want better privacy protection, but the fact is that most aren't willing to do anything about it: it's just a preference, not a solid imperative. Until something Really Bad happens to many people as a result of privacy loss, I really don't think much will be done that requires real work and inconvenience from people, like moving to something other than credit cards for long-distance transactions... and that's a tragedy." [L. Todd Masco, 1994-08-20]
- 12.10.4. "Is strong crypto needed for digital cash?"
 - Yes, for the most bulletproof form, the form of greatest interest to us and especially for agents, autonomous systems
 - + No, for certain weak versions (non-cryptographic methods of security, access control, biometric security, etc. methods)
 - for example, Internet billing is not usually done with crypto
 - and numbered Swiss accounts can be seen as a weak form of digital cash (with some missing features)
 - "warehouse receipts," as in gold or currency shipments
- 12.10.5. on why we may not have it for a while, from a non-Cypherpunk commenter:
 - "Government requires information on money flows, taxable items, and large financial transactions.....As a result, it would be nearly impossible to set up a modern anonymous digital cash system, despite the fact that we have the technology.....I think we have more of a right to privacy with digicash transactions, and I also think there is a market for anonymous digicash systems. " [Thomas Grant Edwards. talk.politics.crypto, 1994-09-06]
- 12.10.6. "Why do a lot of schemes for things like digital money have problems on the Net?"
 - + Many reasons
 - lack of commercial infrastructure in general on the Net...people are not used to buying things, advertising is discouraged (or worse), and almost everything is "free."
 - lack of robustness and completeness in the various protocols: they are "not ready for prime time" in most cases (PGP is solid, and some good shells exist for PGP, but the many other crypto protocols are mostly not implemented at all, at least not widely).
 - + The Net runs "open-loop," as a store-and-forward delivery system
 - The Net is mostly a store-and-forward network, at least at the granularity seen by the user in sending

- messages, and hence is "open loop." Messages may or may not be received in a timely way, and there is little opportunity for negotiaton on a real-time basis.
- This open-loop nature usually works...messages get through most of the time. And the "message in a bottle" nature fits in with anonymous remailers (with latency/delay), with message pools, and with other schemes to make traffic analysis harder. A "closed-loop," responsive system is likelier to be traffic-analyzed by correlation of packets, etc.
 - but the sender does not know if it gets through (return receipts not commonly implemented...might be a nice feature to incorporate; agent-based systems (Telescript?) will certainly do this)
 - this open-loop nature makes protocols, negotiation, digital cash very tough to use--too much human intervention needed
 - Note: These comments apply mainly to mail systems, which is where most of us have experimented with these ideas. Non-mail systems, such as Mosaic or telnet or the like, have better or faster feedback mechanisms and may be preferable for implementation of Cypherpunks goals. It may be that the natural focus on mailing lists, e-mail, etc., has distracted us. Perhaps a focus on MUDs, or even on ftp, would have been more fruitful...but we're a mailing list, and most people are much more familiar with e-mail than with archie or gopher or WAIS, etc.
 - The legal and regulatory obstacles to a real system, used for real transactions, are formidable. (The obstacles to a "play" system are not so severe, but then play systems tend not to get much developer attention.)
- 12.10.7. Scenario for deployment of digital cash
- Eric Hughes has spent time looking into this. Too many issues to go into here, but he had this interesting scenario, repeated almost in toto here:
 - "It's very unlikely that a USA bank will be the one to deploy anonymous digital dollars first. It's much more likely that the first dollar digital cash will be issued overseas, possibly London. By the same token, the non-dollar regulation on banks in this country is not the same as the dollar regulation, so it's quite possible that the New York banks may be the first issuers of digital cash, in pounds sterling, say.

"There will be two stages in actually deploying digital cash. By digital cash, here, I mean a retail phenomenon, available anybody. The first will be to digitize money, and the second will be to anonymize it. Efforts are already well underway to make more-or-less secure digital funds transfers with reasonably low transaction fees (not transaction costs, which are much more than just fees). These efforts, as long as they retain some traceability, will almost certainly succeed first in the marketplace, because (and this is vital) the regulatory environment against anonymity is not compromised.

"Once, however, money has been digitized, one of the services available for purchase can be the anonymous transfer of funds. I expect that the first digitization of money won't be fully fungible. For example, if you allow me to take money out of your checking account by automatic debit, there is risk that the money won't be there when I ask for it. Therefore that kind of money won't be completely fungible, because money authorized from one person won't be completely identical with money from another. It may be a risk issue, it may be a timeliness issue, it may be a fee issue; I don't know, but it's unlikely to be perfect.

"Now, as the characteristic size of a business decreases, the relative costs of dealing with whatever imperfection there is will be greater. To wit, the small player will still have some problem getting paid, although certainly less than now. Digital cash solves many of these problems. The clearing is immediate and final (no transaction reversals). The number of entities to deal with is greatly reduced, hopefully to one. The need and risk and cost of accounts receivables is eliminated. It's anonymous. There will be services which will desire these advantages, enough to support a digital cash infrastructure. [Eric Hughes, Cypherpunks list, 1994-08-03]

12.11. Commerce on the Internet

12.11.1. This has been a brewing topic for the past couple of years.

In 1994 thing heated up on several fronts:

- DigiCash announcement
- NetMarket announcement
- various other systems, including Visa Electronic Purse

12.11.2. I have no idea which ones will succeed...

12.11.3. NetMarket

- Mosaic connections, using PGP
- + "The NetMarket Company is now offering PGP-encrypted Mosaic sessions for securely transmitting credit card information over the Internet. Peter Lewis wrote an article on NetMarket on page D1 of today's New York Times (8/12/94). For more information on NetMarket, connect to <http://www.netmarket.com/> or, telnet netmarket.com." [Guy H. T. Haskin <guy@netmarket.com>, 1994-08-12]
- Uses PGP. Hailed by the NYT as the first major use of crypto for some form of digital money, but this is not correct.

12.11.4. CommerceNet

- allows Internet users to buy and sell goods.
- "I read in yesterday's L.A. Times about something called CommerceNet, where sellers and buyers of workstation level equipment can meet and conduct business....Near the end of the article, they talked about a proposed method for exchanging "digital signatures" via Mosaic (so that buyers and sellers could know that they were who they said they were) and that they were going to "submit it to the Internet Standards body" [Cypher1@aol.com, 1994-06-23]

12.11.5. EDI, purchase orders, paperwork reduction, etc.

- Nick Szabo is a fan of this approach

12.11.6. approaches

- send VISA numbers in ordinary mail....obviously insecure
- send VISA numbers in encrypted mail
- + establish two-way clearing protocols
 - better ensures that recipient will fulfill service...like a receipt that customer signs (instead of the "sig taken over the phone" approach)
 - various forms of digital money

12.11.7. lightweight vs. heavyweight processes for Internet commerce

- Chris Hibbert
- and the recurring issue of centralized vs. decentralized authentication and certification

12.12. Cypherpunks Experiments ("Magic Money")

12.12.1. What is Magic Money?

- "Magic Money is a digital cash system designed for use over electronic mail. The system is online and untraceable. Online means that each transaction involves an exchange with a server, to prevent double-spending. Untraceable means that it is impossible for anyone to trace transactions, or to match a withdrawal with a deposit, or to match two coins in any way."

"The system consists of two modules, the server and the client. Magic Money uses the PGP ascii-armored message format for all communication between the server and client. All traffic is encrypted, and messages from the server to the client are signed. Untraceability is provided by a Chaum-style blind signature. Note that the blind signature is patented, as is RSA. Using it for experimental purposes only shouldn't get you in trouble.

"Digicash is represented by discrete coins, the denominations of which are chosen by the server operator. Coins are RSA-signed, with a different e/d pair for each denomination. The server does not store any money. All coins are stored by the client module. The server accepts old coins and blind- signs new coins, and checks off the old ones on a spent list."

[...rest of excellent summary elided...highly recommended that you dig it up (archives, Web site?) and read it]

[PrOduct Cypher, Magic Money Digicash System, 1992-02-04]

+ Magic Money

- ftp://csn.org/pub/mpj/crypto_XXXXXX (or something like that) <Derek Atkins, 4-7-94>
- ftp://csn.org//mpj/I_will_not_export/crypto_??????/pgp_tools <Michael Paul Johnson, 4-7-94>

12.12.2. Matt Thomlinson experimented with a derivative version called "GhostMarks"

12.12.3. there was also a "Tacky Tokens" derivative

12.12.4. Typical Problems with Such Experiments

- Not worth anything...making the money meaningful is an obstacle to be overcome
- If worth anything, not worth the considerable effort to use it ("creating Magic Money clients" and other scary Unix stuff!)
- robustness...sites go down, etc.

- same problems were seen on Extropians list with "HEX" exchange and its currency, the "thorne." (I even paid real money to Edgar Swank to buy some thorned...alas, the market was too thinly traded and the thornes did me no good.)

12.13. Practical Issues and Concerns with Digital Cash

12.13.1. "Is physical identity proof needed for on-line clearing?"

- No, not if the cash outlook is taken. Cash is cash. Caveat emptor.
- The "first to the locker" approach causes the bank not to particularly care about this, just as a Swiss bank will allow access to a numbered account by presentation of the number, and perhaps a key. Identity proof *may* be needed, depending on the "protocol" they and the customer established, but it need not be. And the last thing the bank is worried about is being able to "find and prosecute" anyone, as there is no way they can be liable for a double spending incident. The beauties of local clearing! (Which is what gold coins do, and paper money if we really think we can pass it on to others.)

12.13.2. "Is digital cash traceable?"

- There are several flavors of "digital cash," ranging from versions of VISA cards to fully untraceable (Chaumian) digital cash.
- This comes up a lot, with people in Net newsgroups even warning others not to use digital cash because of the ease of traceability. Not so.
- "Not the kind proposed by David Chaum and his colleagues in the Netherlands. The whole thrust of their research over the last decade has been the use of cryptographic techniques to make electronic transactions secure from fraud while at the same time protecting personal privacy. They, and others, have developed a number of schemes for UNTRACEABLE digital cash." [Kevin Van Horn, talk.politics.crypto, 1994-07-03]

12.13.3. "Is there a danger that people will lose the numbers that they need to redeem money? That someone could steal the number and thus steal their money?"

- Sure. There's the danger that I'll lose my bearer bonds, or forget my Swiss bank account number, or lose my treasure map to where I buried my money (as Alan Turing supposedly did in WW II).
- People can take steps to limit risk. More secure computers. Dongles worn around their necks. Protocols that involve biometric authentication to their local computer or key storage PDA, etc. Limits on withdrawals per day, etc. People can store key numbers with people they trust, perhaps encrypted with other keys, can leave them with their lawyers, etc. All sorts of arrangements can be made. Personal identification is but one of these arrangements. Often used, but not essential to the underlying protocol. Again, the Swiss banks (maybe now the Liechtenstein anstalts are a better example) don't require physical ID for all accounts. (More generally, if Charles wants to create a bank in which deposits are made and then given out to the first person who sings the right tune, why should we care? This extreme example is useful in pointing out that

contractual arrangements need not involve governmental or societal norms about what constitutes proof of identity.)

12.14. Cyberspace and Digital Money

12.14.1. "You can't eat cyberspace, so what good is digital money?"

- This comes up a lot. People assume there is no practical way to transfer assets, when in fact it is done all the time. That is, money flows from the realm of the purely "informational" realm to the physical realm. Consultants, writers, traders, etc., all use their heads and thereby earn real money.
- Same will apply to cyberspace.

12.14.2. "How can I remain anonymous when buying physical items using anonymous digital cash?"

- Very difficult. Once you are seen, and your picture can be taken (perhaps unknown to you), databases will have you. Not much can be done about this.
- People have proposed schemes for anonymous shipment and pickup, but the plain fact is that physical delivery of any sort compromises anonymity, just as in the world today.
- The purpose of anonymous digital cash is partly to at least make it more difficult, to not give Big Brother your detailed itinerary from toll road movements, movie theater payments, etc. To the extent that physical cameras can still track cars, people, shipments, etc., anonymous digital cash doesn't solve this surveillance problem.

12.15. Outlawing of Cash

12.15.1. "What are the motivations for outlawing cash?"

- (Note: This has not happened. Many of us see signs of it happening. Others are skeptical.)
- + Reasons for the Elimination of Cash:
 - War on Drugs....need I say more?
 - surface the underground economy, by withdrawing paper currency and forcing all monetary transaction into forms that can be easily monitored, regulated, and taxed.
 - tax avoidance, under the table economy (could also be motive for tamper-resistant cash registers, with spot checks to ensure compliance)
- + welfare, disability, pension, social security auto-deposits
 - fraud, double-dipping
 - reduce theft of welfare checks, disability payments, etc....a problem in some locales, and automatic deposit/cash card approaches are being evaluated.
- general reduction in theft, pickpockets
- reduction of paperwork: all transfers electronic (could be part of a "reinventing government" initiative)
- + illegal immigrants, welfare cheats, etc. Give everyone a National Identity Card (they'll call it something different. to make it more palatable, such as "Social Services Portable Inventory Unit" or "Health Rights Document").
 - (Links to National Health Care Card, to Welfare Card, to other I.D. schemes designed to reduce fraud, track citizen-units, etc.)
- + rationing systems that depend on non-cash transactions

(as explained elsewhere, market distortions from rationing systems generally require identification, correlation to person or group, etc.)

- this rationing can include subsidized prices, denial of access (e.g., certain foods denied to certain people)

12.15.2. Lest this be considered paranoid ranting, let me point out that many actions have already been taken that limit the form of money (banking laws, money laundering, currency restrictions...even the outlawing of competing currencies itself)

12.15.3. Dangers of outlawing cash

- Would freeze out all transactions, giving Big Brother unprecedented power (unless the non-cash forms were anonymous, a la Chaum and the systems we support)
- Would allow complete traceability...like the cellular phones that got Simpson
- 666, Heinlein, Shockwave Rider, etc.

12.15.4. Given that there is no requirement for identity to be associated with money, we should fight any system which proposed to link the two.

12.15.5. The value of paying cash

- makes a transaction purely local, resolved on the spot
- the alternative, a complicated accounting system involving other parties, etc., is much less attractive
- too many transactions these days are no longer handled in cash, which increases costs and gets other parties involved where they shouldn't be involved.

12.15.6. "Will people accept the banning of cash?"

- There was a time when I would've said Americans, at least, would've rejected such a thing. Too many memories of "Papieren, bitte. Macht schnell!" But I now think most Americans (and Europeans) are so used to producing documents for every transaction, and so used to using VISA cards and ATM cards at gas stations, supermarkets, and even at flea markets, that they'll willingly--even eagerly--adopt such a system.

12.16. Novel Opportunities

12.16.1. Encrypted open books, or anonymous auditing

- Eric Hughes has worked on a scheme using a kind of blinding to do "encrypted open books," whereby observers can verify that a bank is balancing its books without more detailed looks at individual accounts. (I have my doubts about spoofs, attacks, etc., but such are always to be considered in any new protocol.)
- "Kent Hastings wondered how an offshore bank could provide assurances to depositors. I wondered the same thing a few months ago, and started working on what Perry calls the anonymous auditing problem. I have what I consider to be the core of a solution.
...The following is long.... [TCM Note: Too long to include here. I am including just enough to convince readers that some new sorts of banking ideas may come out of cryptography.]

"If we use the contents of the encrypted books at the

organizational boundary points to create suitable legal obligations, we can mostly ignore what goes on inside of the mess of random numbers. That is, even if double books were being kept, the legal obligations created should suffice to ensure that everything can be unwound if needed. This doesn't prevent networks of corrupt businesses from going down all at once, but it does allow networks of honest businesses to operate with more assurance of honesty." [Eric Hughes, PROTOCOL: Encrypted Open Books, 1993-08-16]

12.16.2. "How can software components be sold, and how does crypto figure in?"

- + Reusable Software, Brad Cox, Sprague, etc.
 - good article in "Wired" (repeated in "Out of Control")
- First, certainly software is sold. The issues is why the "software components" market has not yet developed, and why such specific instances of software as music, art, text, etc., have not been sold in smaller chunks.
- + Internet commerce is a huge area of interest, and future development.
 - currently developing very slowly
 - lots of conflicting information...several mailing lists...lots of hype
- + Digital cash is often cited as a needed enabling tool, but I think the answer is more complicated than that.
 - issues of convenience
 - issues of there being no recurring market (as there is in, say, the chip business...software doesn't get bought over and over again, in increasing unit volumes)

12.17. Loose Ends

12.17.1. Reasons to have no government involvement in commerce

- Even a small involvement, through special regulations, granted franchises, etc., produces vested interests. For example, those in a community who had to wait to get building permits want others to wait just as long, or longer. Or, businesses that had to meet certain standard, even if unreasonable, will demand that new businesses do so also. The effect is an ever-widening tar pit of rules, restrictions, and delays. Distortions of the market result.
- + Look at how hard it is for the former U.S.S.R. to disentangle itself from 75 years of central planning. They are now an almost totally Mafia-controlled state (by this I mean that "privatization" of formerly non-private enterprises benefitted those who had amassed money and influence, and that these were mainly the Russian Mafia and former or current politicians...the repercussions of this "corrupt giveaway" will be felt for decades to come).
 - An encouraging sign: The thriving black market in Russia--which all Cypherpunks of course cheer--will gradually displace the old business systems with new ones, as in all economies. Eventually the corruptly-bought businesses will sink or swim based on merit, and newly-created enterprises will compete with them.

12.17.2. "Purist" Approach to Keys, Cash, Responsibility

- + There are two main approaches to the issue:
 - Key owner is responsible for uses of his key

- or, Others are responsible
- + There may be mixed situations, such as when a key is stolen...but this needs also to be planned-for by the key owner, by use of protocols that limit exposure. For example, few people will use a single key that accesses immediately their net worth...most people will partition their holding and their keyed access in such a way as to naturally limit exposure if any particular key is lost or compromised. Or forgotten.
 - could involve their bank holding keys, or escrow agents
 - or n-out-of-m voting systems
- Contracts are the essence...what contracts do people voluntarily enter into?
- And locality--who better to keep keys secure than the owner? Anything that transfers blame to "the banks" or to "society" breaks the feedback loop of responsibility, provides an "out" for the lazy, and encourages fraud (people who disavow contracts by claiming their key was stolen).

13. Activism and Projects

13.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

13.2. SUMMARY: Activism and Projects

13.2.1. Main Points

13.2.2. Connections to Other Sections

13.2.3. Where to Find Additional Information

13.2.4. Miscellaneous Comments

13.3. Activism is a Tough Job

13.3.1. "herding cats"..trying to change the world through exhortation seems a particularly ineffective notion

13.3.2. There's always been a lot of wasted time and rhetoric on the Cypherpunks list as various people tried to get others to follow their lead, to adopt their vision. (Nothing wrong with this, if done properly. If someone leads by example, or has a particularly compelling vision or plan, this may naturally happen. Too often, though, the situation was that someone's vague plans for a product were declared by them to be the standards that others should follow. Various schemes for digital money, in many forms and modes, has always been the prime example of this.)

13.3.3. This is related also to what Kevin Kelley calls "the fax effect." When few people own fax machines, they're not of much use. Trying to get others to use the same tools one has is like trying to convince people to buy fax machines so that you can communicate by fax with them...it may happen, but probably for other reasons. (Happily, the interoperability of PGP provided a common communications medium that had been lacking with previous platform-specific cipher programs.)

13.3.4. Utopian schemes are also a tough sell. Schemes about using

digital money to make inflation impossible, schemes to collect taxes with anonymous systems, etc.

13.3.5. Harry Browne's "How I Found Freedom in an Unfree World" is well worth reading; he advises against getting upset and frustrated that the world is not moving in the direction one would like.

13.4. Cypherpunks Projects

13.4.1. "What are Cypherpunks projects?"

- Always a key part--perhaps the key part--of Cypherpunks activity. "Cypherpunks write code." From work on PGP to remailers to crypto toolkits to FOIA requests, and a bunch of other things, Cypherpunks hack the system in various ways.
- Matt Blaze's LEAF blower, Phil Karn's "swIPe" system, Peter Wayner's articles....all are examples. (Many Cypherpunks projects are also done, or primarily done, for other reasons, so we cannot in all cases claim credit for this work.)

13.4.2. Extensions to PGP

13.4.3. Spread of PGP and crypto in general.

- education
- diskettes containing essays, programs
- ftp sites
- raves, conventions, gatherings

13.4.4. Remailers

- + ideal Chaumian mix has certain properties
 - latency to foil traffic analysis
 - encryption
 - no records kept (hardware tamper-resistance, etc.)
- Cypherpunks remailers
- julf remailers
- + abuses
 - flooding, because mail transmission costs are not borne by sender
 - + anonymity produces potential for abuses
 - death threats, extortion
- Progress continues, with new features added. See the discussion in the remailers section.

13.4.5. Steganography

- hiding the existence of a message, for at least some amount of time
- security through obscurity
- invisible ink, microdots
- + Uses
 - in case crypto is outlawed, may be useful to avoid authorities
 - if enough people do it, increases the difficulty of enforcing anti-crypto laws (all
- + Stego
 - JSTEG:
soda.berkeley.edu:/pub/cypherpunks/applications/jsteg
 - Stego: sumex-aim.stanford.edu

13.4.6. Anonymous Transaction Systems

13.4.7. Voice Encryption, Voice PGP

- Clipper, getting genie out of bottle
- CELP, compression, DSPs

- SoundBlaster approach...may not have enough processing power
- + hardware vs. pure software
 - newer Macs, including av Macs and System 7 Pro, have interesting capabilities
- + Zimmermann's plans have been widely publicized, that he is looking for donations, that he is seeking programming help, etc.
 - which does not bode well for seeing such a product from him
 - frankly, I expect it will come from someone else
- Eric Blossom is pursuing own hardware board, based on 2105
- + "Is anyone building encrypted telephones?"
 -
 - + Yes, several such projects are underway. Eric Blossom even showed a
 - PCB of one at a Cypherpunks meeting, using an inexpensive DSP chip.
 -
 - + Software-only versions, with some compromises in speech quality
 - probably, are also underway. Phil Zimmermann described his progress at
 - + the last Cypherpunks meeting.
 -
 - ("Software-only" can mean using off-the-shelf, widely-available DSP
 - + boards like SoundBlasters.)
 -
 - And I know of at least two more such projects. Whether any will
 - + materialize is anyone's guess.
 -
 - And various hacks have already been done. NeXT users have had
 - voicemail for years, and certain Macs now offer something similar.
 - + Adding encryption is not a huge obstacle.
 -
 - A year ago, several Cypherpunks meeting sites around the U.S. were
 - linked over the Internet using DES encryption. The sound quality was
 - poor, for various reasons, and we turned off the DES in a matter of
 - minutes. Still, an encrypted audio conference call.

13.4.8. DC-Nets

- What it is, how it works
- Chaum's complete 1988 "Journal of Cryptology" article is available at the Cypherpunks archive site, ftp.soda.csua.edu, in /pub/cypherpunks
- + Dining Cryptographers Protocols, aka "DC Nets"
 - + "What is the Dining Cryptographers Problem, and why is it so important?"
 - + This is dealt with in the main section, but here's David Chaum's Abstract, from his 1988 paper"
 - Abstract: "Keeping confidential who sends which

messages, in a world where any physical transmission can be traced to its origin, seems impossible. The solution presented here is unconditionally or cryptographically secure, depending on whether it is based on one-time-use keys or on public keys. respectively. It can be adapted to address efficiently a wide variety of practical considerations." ["The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," David Chaum, Journal of Cryptology, I, 1, 1988.]

- DC-nets have yet to be implemented, so far as I know, but they represent a "purer" version of the physical remailers we are all so familiar with now. Someday they'll have have a major impact. (I'm a bigger fan of this work than many seem to be, as there is little discussion in sci.crypt and the like.)
- + "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," David Chaum, Journal of Cryptology, I, 1, 1988.
- available courtesy of the Information Liberation Front at the soda.csua.berkeley.edu site
- Abstract: "Keeping confidential who sends which messages, in a world where any physical transmission can be traced to its origin, seems impossible. The solution presented here is unconditionally or cryptographically secure, depending on whether it is based on one-time-use keys or on public keys. respectively. It can be adapted to address efficiently a wide variety of practical considerations." ["The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," David Chaum, Journal of Cryptology, I, 1, 1988.]
- Note that the initials "D.C." have several related meanings: Dining Cryptographers, Digital Cash/DigiCash, and David Chaum. Coincidence?
- + Informal Explanation
 - Note: I've posted this explanation, and variants, several times since I first wrote it in mid-1992. In fact, I first posted it on the "Extropians" mailing list, as "Cypherpunks" did not then exist.
 - Three Cypherpunks are having dinner, perhaps in Palo Alto. Their waiter tells them that their bill has already been paid, either by the NSA or by one of them. The waiter won't say more. The Cypherpunks wish to know whether one of them paid, or the NSA paid. But they don't want to be impolite and force the Cypherpunk payer to 'fess up, so they carry out this protocol (or procedure):

Each Cypherpunk flips a fair coin behind a menu placed upright between himself and the Cypherpunk on his right. The coin is visible to himself AND to the Cypherpunk on his left. Each Cypherpunk can see his own coin and the coin to his right. (STOP RIGHT HERE! Please take the time to make a sketch of the situation I've described. If you lost it here, all that follows

will be a blur. It's too bad the state of the Net today cannot support figures and diagrams easily.)

Each Cypherpunk then states out loud whether the two coins he can see are the SAME or are DIFFERENT, e.g., "Heads-Tails" means DIFFERENT, and so forth. For now, assume the Cypherpunks are truthful. A little bit of thinking shows that the total number of "DIFFERENCES" must be either 0 (the coins all came up the same), or 2. Odd parity is impossible.

Now the Cypherpunks agree that if one of them paid, he or she will SAY THE OPPOSITE of what they actually see. Remember, they don't announce what their coin turned up as, only whether it was the same or different as their neighbor.

Suppose none of them paid, i.e., the NSA paid. Then they all report the truth and the parity is even (either 0 or 2 differences). They then know the NSA paid.

Suppose one of them paid the bill. He reports the opposite of what he actually sees, and the parity is suddenly odd. That is, there is 1 difference reported. The Cypherpunks now know that one of them paid. But can they determine which one?

Suppose you are one of the Cypherpunks and you know you didn't pay. One of the other two did. You either reported SAME or DIFFERENT, based on what your neighbor to the right (whose coin you can see) had. But you can't tell which of the other two is lying! (You can see you right-hand neighbor's coin, but you can't see the coin he sees to his right!)

This all generalizes to any number of people. If none of them paid, the parity is even. If one of them paid, the parity is odd. But which one of them paid cannot be deduced. And it should be clear that each round can transmit a bit, e.g., "I paid" is a "1". The message "Attack at dawn" could thus be "sent" untraceably with multiple rounds of the protocol.

- The "Crypto Ouija Board": I explain this to people as a kind of ouija board. A message, like "I paid" or a more interesting "Transfer funds from.....," just "emerges" out of the group, with no means of knowing where it came from. Truly astounding.

+ Problems and Pitfalls

- In Chaum's paper, the explanation above is given quickly, in a few pages. The rest of the paper is then devoted to dealing with the many "gotchas" and attacks that come up and that must be dealt with before the DC protocol is even remotely possible. I think all those interested in protocol design should read this paper, and the follow-on papers by Bos, Pfitzmann, etc., as object lessons for dealing with complex crypto

protocols.

+ The Problems:

- 1. Collusion. Obviously the Cypherpunks can collude to deduce the payer. This is best dealt with by creating multiple subcircuits (groups doing the protocol amongst themselves). Lots more stuff here. Chaum devotes most of the paper to these kind of issues and their solutions.

2. With each round of this protocol, a single bit is transmitted. Sending a long message means many coin flips. Instead of coins and menus, the neighbors would exchange lists of random numbers (with the right partners, as per the protocol above, of course. Details are easy to figure out.)

3. Since the lists are essentially one-time pads, the protocol is unconditionally secure, i.e., no assumptions are made about the difficulty of factoring large numbers or any other crypto assumptions.

4. Participants in such a "DC-Net" (and here we are coming to the heart of the "crypto anarchy" idea) could exchange CD-ROMs or DATs, giving them enough "coin flips" for zillions of messages, all untraceable! The logistics are not simple, but one can imagine personal devices, like smart card or Apple "Newtons," that can handle these protocols (early applications may be for untraceable brainstorming comments, secure voting in corporate settings, etc.)

5. The lists of random numbers (coin flips) can be generated with standard cryptographic methods, requiring only a key to be exchanged between the appropriate participants. This eliminates the need for the one-time pad, but means the method is now only cryptographically secure, which is often sufficient. (Don't think "only cryptographically secure" means insecure....the messages may remain encrypted for the next billion years)

6. Collisions occur when multiple messages are sent at the same time. Various schemes can be devised to handle this, like backing off when you detect another sender (when even parity is seen instead of odd parity). In large systems this is likely to be a problem. Deliberate disruption, or spamming, is a major problem--a disruptor can shut down the DC-net by sending bits out. As with remails, anonymity means freedom from detection. (Anonymous payments to send a message may help, but the details are murky to me.)

+ Uses

- * Untraceable mail. Useful for avoiding censorship, for avoiding lawsuits, and for all kinds of crypto anarchy

- things.
 - * Fully anonymous bulletin boards, with no traceability of postings or responses. Illegal materials can be offered for sale (my 1987 canonical example, which freaked out a few people: "Stealth bomber blueprints for sale. Post highest offer and include public key."). Think for a few minutes about this and you'll see the profound implications.
 - * Decentralized nexus of activity. Since messages "emerge" (a la the ouija board metaphor), there is no central posting area. Nothing for the government to shut down, complete deniability by the participants.
 - * Only you know who your partners are....in any given circuit. And you can be in as many circuits as you wish. (Payments can be made to others, to create a profit motive. I won't deal with this issue, or with the issue of how reputations are handled, here.)
 - It should be clear that DC-nets offer some amazing opportunities. They have not been implemented at all, and have received almost no attention compared to ordinary Cypherpunks remailers. Why is this? The programming complexity (and the underlying cryptographic primitives that are needed) seems to be the key. Several groups have announced plans to imlement some form of DC-net, but nothing has appeared.
 - software vs. hardware,
 - Yanek Martinson, Strick, Austin group, Rishab
 - IMO, this is an ideal project for testing the efficacy of software toolkits. The primitives needed, including bit commitment, synchronization, and collusion handling, are severe tests of crypto systems. On the downside, I doubt that even the Pfaltzmanns or Bos has pulled off a running simulation...
- 13.4.9. D-H sockets, UNIX, swIPE
- + swIPE
 - Matt Blaze, John I. (did coding), Phil Karn, Perry Metzger, etc. are the main folks involved
 - evolved from "mobile IP," with radio links, routing
 - virtual networks
 - putting encryption in at the IP level, transparently
 - bypassing national borders
 - Karn
 - at soda site
 - + swIPE system, for routing packets
 - end to end, gateways, links, Mach, SunOS
- 13.4.10. Digital Money, Banks, Credit Unions
- Magic Money
 - Digital Bank
 - "Open Encrypted Books"
 - not easy to do...laws, regulations, expertise in banking
 - technical flaws, issues in digital money
 - + several approaches
 - clearing
 - tokens, stamps, coupons
 - anonymity-protected transactions
- 13.4.11. Data Havens
- + financial info, credit reports

- bypassing local jurisdictions, time limits, arcane rules
 - reputations
 - insider trading
 - medical
 - technical, scientific, patents
 - crypto information (recursively enough)
 - need not be any known location....distributed in cyberspace
 - One of the most commercially interesting applications.
- 13.4.12. Related Technologies
- Agorics
 - Evolutionary Systems
 - Virtual Reality and Cyberspace
 - Agents
 - + Computer Security
 - + Kerberos, Gnu, passwords
 - recent controversy
 - demon installed to watch packets
 - Cygnus will release it for free
 - GuardWire
 - + Van Eck, HERF, EMP
 - Once Cypherpunk project proposed early on was the duplication of certain NSA capabilities to monitor electronic communications. This involves "van Eck" radiation (RF) emitted by the CRTs and other electronics of computers.
 - + Probably for several reasons, this has not been pursued, at least not publically.
 - legality
 - costs
 - difficulty in finding targets of opportunity
 - not a very CPish project!
- 13.4.13. Matt Blaze, AT&T, various projects
- + a different model of trust...multiple universes
 - not heierarchical interfaces, but mistrust of interfaces
 - heterogeneous
 - where to put encryption, where to mistrust, etc.
 - + wants crypto at lowest level that is possible
 - almost everything should be mistrusted
 - every mistrusted interface should be cryptographically protected...authentication, encryption
 - + "black pages"---support for cryptographic communication
 - "pages of color"
 - a collection of network services that identify and deliver security information as needed....keys, who he trusts, protocols, etc.
 - + front end: high-level API for security requirements
 - like DNS? caching models?
 - trusted local agent....
 - + "people not even born yet" (backup tapes of Internet communications)
 - tapes stored in mountains, access by much more powerful computers
 - + "Cryptographic File System" (CFS)
 - file encryption
 - no single DES mode appears to be adequate...a mix of modes

- + swIPe system, for routing packets
 - end to end, gateways, links, Mach, SunOS
- 13.4.14. Software Toolkits
 - + Henry Strickland's TCL-based toolkit for crypto
 - other Cypherpunks, including Hal Finney and Marianne Mueller, have expressed good opinions of TCL and TCL-TK (toolkit)
 - Pr0duct Cypher's toolkit
 - C++ Class Libraries
 - VMX, Visual Basic, Visual C++
 - Smalltalk
- 13.5. Responses to Our Projects (Attacks, Challenges)
 - 13.5.1. "What are the likely attitudes toward mainstream Cypherpunks projects, such as remailers, encryption, etc.?"
 - Reaction has already been largely favorable. Journalists such as Steven Levy, Kevin Kelly, John Markoff, and Julian Dibbell have written favorably. Reaction of people I have talked to has also been mostly favorable.
 - 13.5.2. "What are the likely attitudes toward the more outre projects, such as digital money, crypto anarchy, data havens, and the like?"
 - Consternation is often met. People are frightened.
 - The journalists who have written about these things (those mentioned above) have gotten beyond the initial reaction and seem genuinely intrigued by the changes that are coming.
 - 13.5.3. "What kinds of attacks can we expect?"
 - + Depends on the projects, but some general sorts of attacks are likely. Some have already occurred. Examples:
 - * flooding of remailers, denial of service attacks--to swamp systems and force remailers to reconsider operations
 - this is fixed (mostly) with "digital postage" (if postage covers costs, and generates a profit, then the more the better)
 - * deliberately illegal or malicious messages, such as death threats
 - designed to put legal and sysop pressures on the remailer operator
 - several remailers have been attacked this way, or at least have had these messages
 - source-blocking sometimes works, though not of course if another remailer is first used (many issues here)
 - * prosecution for content of posts
 - + copyright violations
 - e.g., forwarding ClariNet articles through Hal Finney's remailer got Brad Templeton to write warning letters to Hal
 - pornography
 - ITAR violations, Trading with the Enemy Act
 - espionage, sedition, treason
 - corporate secrets,
 - These attacks will test the commitment and courage of remailer or anonymizing service operators

13.6. Deploying Crypto

13.6.1. "How can Cypherpunks publicize crypto and PGP?"

- articles, editorials, radio shows, talking with friends
- The Net itself is probably the best place to publicize the problems with Clipper and key escrow. The Net played a major role--perhaps the dominant role--in generating scorn for Clipper. In many way the themes debated here on the Net have tremendous influence on media reaction, on editorials, on organizational reactions, and of course on the opinion of technical folks. News spreads quickly, zillions of theories are aired and debated, and consensus tends to emerge quickly.
- raves, Draper
- Libertarian Party, anarchists...
- + conferences and trade shows
 - Arsen Ray Arachelian passed out diskettes at PC Expo

13.6.2. "What are the Stumbling Blocks to Greater Use of Encryption (Cultural, Legal, Ethical)?"

- + "It's too hard to use"
 - multiple protocols (just consider how hard it is to actually send encrypted messages between people today)
 - the need to remember a password or passphrase
- + "It's too much trouble"
 - the argument being that people will not bother to use passwords
 - partly because they don't think anything will happen to them
- + "What have you got to hide?"
 - e.g.,, imagine some comments I'd have gotten at Intel had I encrypted everything
 - and governments tend to view encryption as ipso facto proof that illegalities are being committed: drugs, money laundering, tax evasion
 - recall the "forfeiture" controversy
- BTW, anonymous systems are essentially the ultimate merit system (in the obvious sense) and so fly in the face of the "hiring by the numbers" de facto quota systems now creeping in to so many areas of life....there may be rules requiring all business dealings to keep track of the sex, race, and "ability group" (I'm kidding, I hope) of their employees and their consultants
- + Courts Are Falling Behind, Are Overcrowded, and Can't Deal Adequately with New Issues--Such as Encryption and Cryonics
 - which raises the issue of the "Science Court" again
 - and migration to private adjudication
 - scenario: any trials that are being decided in 1998-9 will have to have been started in 1996 and based on technology and decisions of around 1994
- + Government is taking various steps to limit the use of encryption and secure communication
 - some attempts have failed (S.266), some have been shelved, and almost none have yet been tested in the courts
 - see the other sections...

13.6.3. Practical Issues

- Education
- Proliferation
- Bypassing Laws

13.6.4. "How should projects and progress best be achieved?"

- This is a tough one, one we've been grappling with for a couple of years now. Lots of approaches.
- Writing code
- Organizational
- Lobbying
- I have to say that there's one syndrome we can probably do w, the Frustrated Cyperpunks Syndrome. Manifested by someone flaming the list for not jumping in to join them on their (usually) half-baked scheme to build a digital bank, or write a book, or whatever. "You guys just don't care!" is the usual cry. Often these flamers end up leaving the list.
- Geography may play a role, as folks in otherwise-isolated areas seem to get more attached to their ideas and then get angry when the list as a whole does not adopt them (this is my impression, at least).

13.6.5. Crypto faces the complexity barrier that all technologies face

- Life has gotten more complicated in some ways, simpler in other ways (we don't have to think about cooking, about shoeing the horses, about the weather, etc.). Crypto is currently fairly complicated, especially if multiple paradigms are used (encryption, signing, money, etc.).
- As a personal note, I'm practically drowning in a.c. adaptors and power cords for computers, laser printers, VCRs, camcorders, portable stereos, laptop computers, guitars, etc. Everything with a rechargeable battery has to be charged, but not overcharged, and not allowed to run-down...I forgot to plug in my old Powerbook 100 for a couple of months, and the lead-acid batteries went out on me. Personally, I'm drowning in this crap.
- I mention this only because I sense a backlash coming...people will say "screw it" to new technology that actually complicates their lives more than it simplifies their lives. "Crypto tweaks" who like to fool around with "creating a client" in order to play with digital cash will continue to do so, but 99% of the sought-after users won't. (A nation that can't--or won't--set its VCR clock will hardly embrace the complexities of digital cash. Unless things change, and use becomes as easy as using an ATM.)

13.6.6. "How can we get more people to worry about security in general and encryption in particular?"

- Fact is, most people never think about real security. Safe manufacturers have said that improvements in safes were driven by insurance rates. A direct incentive to spend more money to improve security (cost of better safe < cost of higher insurance rate).

Right now there is almost no economic incentive for people to worry about PIN security, about protecting their files, etc. (Banks eat the costs and pass them on...any bank which tried to save a few bucks in losses by requiring 10-digit PINs--which people would *write down* anyway!--would lose customers. Holograms and pictures on bank cards are happening because the costs have dropped enough.)

Personally, my main interests is in ensuring the Feds don't

tell me I can't have as much security as I want to buy. I don't share the concern quoted above that we have to find ways to give other people security.

- Others disagree with my nonchalance, pointing out that getting lots of other people to use crypto makes it easier for those who already protect themselves. I agree, I just don't focus on missionary work.
- For those so inclined, point out to people how vulnerable their files are, how the NSA can monitor the Net, and so on. All the usual scare stories.

13.7. Political Action and Opposition

13.7.1. Strong political action is emerging on the Net

- right-wing conspiracy theorists, like Linda Thompson
- + Net has rapid response to news events (Waco, Tienmen, Russia)
 - with stories often used by media (lots of reporters on Net, easy to cull for references, Net has recently become tres trendy)
- Aryan Nation in Cyberspace
- (These developments bother many people I mention them to. Nothing can be done about who uses strong crypto. And most fascist/racist situations are made worse by state sponsorship--apartheid laws, Hitler's Germany, Pol Pot's killing fields, all were examples of the state enforcing racist or genocidal laws. The unbreakable crypto that the Aryan Nation gets is more than offset by the gains elsewhere, and the undermining of central authority.)
- shows the need for strong crypto...else governments will infiltrate and monitor these political groups

13.7.2. Cypherpunks and Lobbying Efforts

- + "Why don't Cypherpunks have a lobbying effort?"
 - + we're not "centered" near Washington, D.C., which seems to be an essential thing (as with EFF, ACLU, EPIC, CPSR, etc.)
 - D.C. Cypherpunks once volunteered (April, 1993) to make this their special focus, but not much has been heard since. (To be fair to them, political lobbying is pretty far-removed from most Cypherpunks interests.)
 - no budget, no staff, no office
- + "herding cats" + no financial stakes = why we don't do more
 - + it's very hard to coordinate dozens of free-thinking, opinionated, smart people, especially when there's no whip hand, no financial incentive, no way to force them into line
 - I'm obviously not advocating such force, just noting a truism of systems
- + "Should Cypherpunks advocate breaking laws to achieve goals?"
 - "My game is to get cryptography available to all, without violating the law. This mean fighting Clipper, fighting idiotic export restraints, getting the government to change it's stance on cryptography, through arguements and letter pointing out the problems ... This means writing or promoting strong cryptography....By violating the law, you give them the chance to brand you

"criminal," and ignore/encourage others to ignore what you have to say." [Bob Snyder, 4-28-94]

13.7.3. "How can nonlibertarians (liberals, for example) be convinced of the need for strong crypto?"

- "For liberals, I would examine some pet cause and examine the consequences of that cause becoming "illegal." For instance, if your friends are "pro choice," you might ask them what they would do if the right to lifers outlawed abortion. Would they think it was wrong for a rape victim to get an abortion just because it was illegal? How would they feel about an abortion "underground railroad" organized via a network of "stations" coordinated via the Internet using "illegal encryption"? Or would they trust Clipper in such a situation?

"Everyone in America is passionate about something. Such passion usually dispenses with mere legalism, when it comes to what the believer feels is a question of fundamental right and wrong. Hit them with an argument that addresses their passion. Craft a pro-crypto argument that helps preserve the object of that passion." [Sandy Sandfort, 1994-06-30]

13.7.4. Tension Between Governments and Citizens

- governments want more monitoring...big antennas to snoop on telecommunications, "
- people who protect themselves are sometimes viewed with suspicion
- + Americans have generally been of two minds about privacy:
 - None of your damn business, a man's home is his castle..rugged individualism, self-sufficiency, Calvinism
 - What have you got to hide? Snooping on neighbors
- + These conflicting views are held simultaneously, almost like a tensor that is not resolvable to some resultant vector
 - this dichotomy cuts through legal decisions as well

13.7.5. "How does the Cypherpunks group differ from lobbying groups like the EFF, CPSR, and EPIC?"

- We're more disorganized (anarchic), with no central office, no staff, no formal charter, etc.
- And the political agenda of the aforementioned groups is often at odds with personal liberty. (support by them for public access programs, subsidies, restrictions on businesses, etc.)
- We're also a more radical group in nearly every way, with various flavors of political extremism strongly represented. Mostly anarcho-capitalists and strong libertarians, and many "no compromises" privacy advocates. (As usual, my apologies to any Maoists or the like who don't feel comfortable being lumped in with the libertarians....if you're out there, you're not speaking up.) In any case, the house of Cypherpunks has many rooms.
- We were called "Crypto Rebels" in Steven Levy's "Wired" article (issue 1.2, early 1993). We can represent a radical alternative to the Beltway lawyers that dominate EFF, EPIC, etc. No need to compromise on things like Clipper, Software Key Escrow, Digital Telephony, and the NII. But, of course, no input to the legislative process.

- But there's often an advantage to having a much more radical, purist body out in the wings, making the "rejectionist" case and holding the inner circle folks to a tougher standard of behavior.
 - And of course there's the omnipresent difference that we tend to favor direct action through technology over politicking.
- 13.7.6. Why is government control of crypto so dangerous?
- + dangers of government monopoly on crypto and sigs
 - can "revoke your existence"
 - no place to escape to (historically an important social relief valve)
- 13.7.7. NSA's view of crypto advocates
- "I said to somebody once, this is the revenge of people who couldn't go to Woodstock because they had too much trig homework. It's a kind of romanticism about privacy and the kind of, you know, "you won't get my crypto key until you pry it from my dead cold fingers" kind of stuff. I have to say, you know, I kind of find it endearing." [Stuart Baker, counsel, NSA, CFP '94]
- 13.7.8. EFF
- eff@eff.org
 - + How to Join
 - \$40, get form from many places, EFFector Online, membership@eff.org
 - + EFFector Online
 - [ftp.eff.org, pub/EFF/Newsletters/EFFector](ftp://ftp.eff.org/pub/EFF/Newsletters/EFFector)
 - + Open Platform
 - ftp://ftp.eff.org/pub/EFF/Policy/Open_Platform
 - National Information Infrastructure
- 13.7.9. "How can the use of cryptography be hidden?"
- + Steganography
 - microdots, invisible ink
 - where even the existence of a coded message gets one shot
 - + Methods for Hiding the Mere Existence of Encrypted Data
 - + in contrast to the oft-cited point (made by crypto purists) that one must assume the opponent has full access to the cryptotext, some fragments of decrypted plaintext, and to the algorithm itself, i.e., assume the worst
 - a condition I think is practically absurd and unrealistic
 - assumes infinite intercept power (same assumption of infinite computer power would make all systems besides one-time pads breakable)
 - in reality, hiding the existence and form of an encrypted message is important
 - + this will be all the more so as legal challenges to crypto are mounted...the proposed ban on encrypted telecom (with \$10K per day fine), various governmental regulations, etc.
 - RICO and other broad brush ploys may make people very careful about revealing that they are even using encryption (regardless of how secure the keys are)
 - + steganography, the science of hiding the existence of encrypted information
 - secret inks

- microdots
 - thwarting traffic analysis
 - LSB method
 - + Packing data into audio tapes (LSB of DAT)
 - + LSB of DAT: a 2GB audio DAT will allow more than 100 megabytes in the LSBs
 - less if algorithms are used to shape the spectrum to make it look even more like noise
 - but can also use the higher bits, too (since a real-world recording will have noise reaching up to perhaps the 3rd or 4th bit)
 - + will manufacturers investigate "dithering" circuits? (a la fat zero?)
 - but the race will still be on
 - + Digital video will offer even more storage space (larger tapes)
 - DVI, etc.
 - HDTV by late 1990s
 - + Messages can be put into GIFF, TIFF image files (or even noisy faxes)
 - using the LSB method, with a 1024 x 1024 grey scale image holding 64KB in the LSB plane alone
 - with error correction, noise shaping, etc., still at least 50KB
 - scenario: already being used to transmit message through international fax and image transmissions
 - + The Old "Two Plaintexts" Ploy
 - one decoding produces "Having a nice time. Wish you were here."
 - other decoding, of the same raw bits, produces "The last submarine left this morning."
 - any legal order to produce the key generates the first message
 - + authorities can never prove-save for torture or an informant-that another message exists
 - unless there are somehow signs that the encrypted message is somehow "inefficiently encrypted, suggesting the use of a dual plaintext pair method" (or somesuch spookspeak)
 - again, certain purist argue that such issues (which are related to the old "How do you know when to stop?" question) are misleading, that one must assume the opponent has nearly complete access to everything except the actual key, that any scheme to combine multiple systems is no better than what is gotten as a result of the combination itself
 - and just the overall bandwidth of data...
- 13.7.10. next Computers, Freedom and Privacy Conference will be March 1995, San Francisco
- 13.7.11. Places to send messages to
- cantwell@eff.org, Subject: I support HR 3627
 - Leahy@eff.org, Subject: I support hearings on Clipper
- 13.7.12. Thesis: Crypto can become unstoppable if critical mass is reached
- analogy: the Net...too scattered, too many countries, too many degrees of freedom
 - so scattered that attempts to outlaw strong crypto will be

futile...no bottlenecks, no "mountain passes" (in a race to the pass, beyond which the expansion cannot be halted except by extremely repressive means)

13.7.13. Keeping the crypto genie from being put in the bottle

- (though some claim the genie was never in the bottle, historically)
- ensuring that enough people are using it, and that the Net is using it
- a threshold, a point of no return

13.7.14. Activism practicalities

- + "Why don't we buy advertising time like Perot did?"
- + This and similar points come up in nearly all political discussions (I'm seeing in also in talk.politics.guns). The main reasons it doesn't happen are:
 - ads cost a lot of money
 - casual folks rarely have this kind of money to spend
 - "herding cats" comes to mind, i.e., it's nearly impossible to coordinate the interests of people to gather money, set up ad campaigns, etc.
- In my view, a waste of efforts. The changes I want won't come through a series of ads that are just fingers in the dike. (More cynically, Americans are getting the government they've been squealing for. My interest is in bypassing their avarice and repression, not in changing their minds.)
- Others feel differently, from posts made to the list. Practically speaking, though, organized political activity is difficult to achieve with the anarchic nonstructure of the Cypherpunks group. Good luck!

13.8. The Battle Lines are Being Drawn

13.8.1. Clipper met with disdain and scorn, so now new strategies are being tried...

13.8.2. Strategies are shifting, Plan B is being hauled out

- fear, uncertainty, and doubt
- fears about terrorists, pornographers, pedophiles, money launderers

13.8.3. corporate leaders like Grove are being enlisted to make the Clipper case

13.8.4. Donn Parker is spreading panic about "anarchy" (similar to my own CA)

13.8.5. "What can be done in the face of moves to require national ID cards, use official public key registries, adhere to key escrow laws, etc?"

- This is the most important question we face.
- Short of leaving the country (but for where?) or living a subsistence-level lifestyle below the radar screens of the surveillance state, what can be done?
- + Some possibilities, not necessarily good ones:
 - + civil disobedience
 - mutilation of cards, "accidental erasure," etc.
 - forgeries of cards...probably not feasible (we understand about digital sigs)
 - creation of large black markets...still doesn't cover everything, such as water, electricity, driver's licenses, etc....just too many things for a black market to handle
- lobby against these moves...but it appears the momentum

is too strong in the other direction

13.9. "What Could Make Crypto Use more Common?"

13.9.1. transparent use, like the fax machine, is the key

13.9.2. easier token-based key and/or physical metrics for security

- thumbprint readers
- tokens attached to employee badges
- rings, watches, etc. that carry most of key (with several bits remembered, and a strict "three strikes and you're out" system)

13.9.3. major security scares, or fears over "back doors" by the government, may accelerate the conversion

- all it may take are a couple of very large scandals

13.9.4. insurance companies may demand encryption, for several reasons

- to protect against theft, loss, etc.
- to provide better control against viruses and other modifications which expose the companies they ensure to liability suits
- same argument cited by safe makers: when insurance companies demanded better safes, that's when customers bought them (and not before)

13.9.5. Networks will get more complex and will make conventional security systems unacceptable

- "Fortress" product of Los Altos Technologies
- too many ways for others to see passwords being given to a remote host, e.g., with wireless LANs (which will necessitate ZKIPS)
- ZKIPS especially in networks, where the chances of seeing a password being transmitted are much greater (an obvious point that is not much discussed)
- the whole explosion in bandwidth

13.9.6. The revelations of surveillance and monitoring of citizens and corporations will serve to increase the use of encryption, at first by people with something to hide, and then by others. Cypherpunks are already helping by spreading the word of these situations.

- a snowballing effect
- and various government agencies will themselves use encryption to protect their files and their privacy

13.9.7. for those in sensitive positions, the availability of new bugging methods will accelerate the conversion to secure systems based on encrypted telecommunications and the avoidance of voice-based systems

13.9.8. ordinary citizens are being threatened because of what they say on networks, causing them to adopt pseudonyms

- lawsuits, ordinary threats, concerns about how their employers will react (many employers may adopt rules limiting the speech of their employees, largely because of concerns they'll get sued)

+ and some database providers are providing cross-indexed lists of who has posted to what boards-this is freely available information, but it is not expected by people that their postings will live forever

- some may see this as extortion
- but any proposed laws are unlikely to succeed
- so, as usual, the solution is for people to protect

themselves via technological means

13.9.9. "agents" that are able to retransmit material will make certain kinds of anonymous systems much easier to use

13.10. Deals, the EFF, and Digital Telephony Bill

13.10.1. The backroom deals in Washington are flying...apparently the Administration got burned by the Clipper fiasco (which they could partly write-off as being a leftover from the Bush era) and is now trying to "work the issues" behind the scenes before unveiling new and wide-reaching programs. (Though at this writing, the Health Bill is looking mighty amateurish and seems unlikely to pass.)

13.10.2. We are not hearing about these "deals" in a timely way. I first heard that a brand new, and "in the bag," deal was cooking when I was talking to a noted journalist. He told me that a new deal, cut between Congress, the telecom industry, and the EFF-type lobbying groups, was already a done deal and would be unveiled so. Sure enough, the New and Improved Digital Telephony II Bill appears a few weeks later and is said by EFF representatives to be unstoppable. [comments by S. McLandisht and others, comp.org.eff.talk, 1994-08]

13.10.3. Well, excuse me for reminding everyone that this country is allegedly still a democracy. I know politics is done behind closed doors, as I'm no naif, but deal-cutting like this deserves to be exposed and derided.

13.10.4. I've announced that I won't be renewing my EFF membership. I don't expect them to fight all battles, to win all wars, but I sure as hell won't help *pay* for their backrooms deals with the telcos.

13.10.5. This may me in trouble with my remaining friends at the EFF, but it's as if a lobbying groups in Germany saw the handwriting on the wall about the Final Solution, deemed it essentially unstoppable, and so sent their leaders to Berchtesgaden/Camp David to make sure that the death of the Jews was made as painless as possible. A kind of joint Administration/Telco/SS/IG Farben "compromise." While I don't equate Mitch, Jerry, Mike, Stanton, and others with Hitler's minions, I certainly do think the inside-the-Beltway dealmaking is truly disgusting.

13.10.6. Our freedoms are being sold out.

13.11. Loose ends

13.11.1. Deals, deals, deals!

- pressures by Administration...software key escrow, digital telephony, cable regulation
- + and suppliers need government support on legislation, benefits, spectrum allocation, etc
- reports that Microsoft is lobbying intensively to gain control of big chunks of spectrum...could fit with cable set-top box negotiations, Teledesic, SKE, etc.
- EFF even participates in some of these deals. Being "inside the Beltway" has this kind of effect, where one is either a "player" or a "non-player." (This is my interpretation of how power corrupts all groups that enter the Beltway.) Shmoozing and a desire to help.

13.11.2. using crypto to bypass laws on contacts and trade with other countries

- one day it's illegal to have contact with China, the next day it's encouraged
 - + one day it's legal to have contact with Haiti, the next day there's an embargo (and in the case of Haiti, the economic effects fall on the poor--the tens of thousands fleeing are not fleeing the rulers, but the poverty made worse by the boycott
 - (The military rulers are just the usual thugs, but they're not "our" thugs, for reasons of history. Aristide would almost certainly be as bad, being a Marxist priest. Thus, I consider the breakin of the embargo to be a morally good thing to do.
 - who's to say why Haiti is suddenly to be shunned? By force of law, no less!
- 13.11.3. Sun Tzu's "Art of War" has useful tips (more useful than "The Prince")
- work with lowliest
 - sabotage good name of enemy
 - spread money around
 - I think the events of the past year, including...
- 13.11.4. The flakiness of current systems...
- The current crypto infrastructure is fairly flaky, though the distributed web-of-trust model is better than some centralized system, of course. What I mean is that many aspects are slow, creaky, and conducive to errors.
 - In the area of digital cash, what we have now is not even as advanced as was seen with real money in Sumerian times! (And I wouldn't trust the e-mail "message in a bottle" approach for any nontrivial financial transactions.)
 - Something's got to change. The NII/Superhighway/Infobahn people have plans, but their plans are not likely to mesh well with ours. A challenge for us to consider.
- 13.11.5. "Are there dangers in being too paranoid?"
- + As Eric Hughes put it, "paranoia is cryptography's occupational hazard."
 - "The effect of paranoia is self-delusion of the following form--that one's possible explanations are skewed toward malicious attacks, by individuals, that one has the technical knowledge to anticipate. This skewing creates an inefficient allocation of mental energy, it tends toward the personal, downplaying the possibility of technical error, and it begins to close off examination of technicalities not fully understood.

"Those who resist paranoia will become better at cryptography than those who do not, all other things being equal. Cryptography is about epistemology, that is, assurances of truth, and only secondarily about ontology, that is, what actually is true. The goal of cryptography is to create an accurate confidence that a system is private and secure. In order to create that confidence, the system must actually be secure, but security is not sufficient. There must be confidence that the way by which this security becomes to be believed is robust and immune to delusion.

"Paranoia creates delusion. As a direct and fundamental

result, it makes one worse at cryptography. At the outside best, it makes one slower, as the misallocation of attention leads one down false trails. Who has the excess brainpower for that waste? Certainly not I. At the worst, paranoia makes one completely ineffective, not only in technical means but even more so in the social context in which cryptography is necessarily relevant."
[Eric Hughes, 1994-05-14]

- + King Alfred Plan, blacks
 - plans to round up 20 million blacks
 - RFK, links to LAPD, Western Goals, Birch, KKK
 - RFA #9, 23, 38
- + organized crime situation, perhaps intelligence community
 - damaging to blacks, psychological
- 13.11.6. The immorality of U.S. boycotts and sanctions
 - as with Haiti, where a standard and comparatively benign and harmless military dictatorship is being opposed, we are using force to interfere with trade, food shipments, financial dealings, etc.
 - invasion of countries that have not attacked other countries...a major new escalation of U.S. militarism
 - crypto will facilitate means of undermining imperialism
- 13.11.7. The "reasonableness" trap
 - making a reasonable thing into a mandatory thing
 - this applies to what Cypherpunks should ever be prepared to support
- + An example: A restaurant offers to replace dropped items (dropped on the floor, literally) for free...a reasonable thing to offer customers (something I see frequently). So why not make it the law? Because then the reasonable discretion of the restaurant owner would be lost, and some customers could "game against" (exploit the letter of the law) the system. Even threaten lawsuits.
 - (And libertarians know that "my house, my rules" applies to restaurants and other businesses, absent a contract spelling exceptions out.)
- A more serious example is when restaurants (again) find it "reasonable" to hire various sorts of qualified people. What may be "reasonable" is one thing, but too often the government decides to formalize this and takes away the right to choose. (In my opinion, no person or group has any "right" to a job unless the employer freely offers it. Yes, this could include discrimination against various groups. Yes, we may dislike this. But the freedom to choose is a much more basic right than achieving some ideal of equality is.)
 - And when "reasonableness" is enforced by law, the game-playing increases. In effect, some discretion is needed to reject claims that are based on gaming. Markets naturally work this way, as no "basic rights" or contracts are being violated.
 - Fortunately, strong crypto makes this nonsense impossible. Perforce, people will engage in contracts only voluntarily.
- 13.11.8. "How do we get agreement on protocols?"
 - Give this idea up immediately! Agreement to behave in certain ways is almost never possible.

- Is this an indictment of anarchy?
- No, because the way agreement is sort of reached is through standards or exemplars that people can get behind. Thus, we don't get "consensus" in advance on the taste of Coca Cola...somebody offers Coke for sale and then the rest is history.
- PGP is a more relevant example. The exemplar is on a "take it or leave it" basis, with minor improvements made by others, but within the basic format.

14. Other Advanced Crypto Applications

14.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

14.2. SUMMARY: Other Advanced Crypto Applications

14.2.1. Main Points

14.2.2. Connections to Other Sections

14.2.3. Where to Find Additional Information

- see the various "Crypto" Proceedings for various papers on topics that may come to be important

14.2.4. Miscellaneous Comments

14.3. Digital Timestamping

14.3.1. digital timestamping

- The canonical reference for digital timestamping is the work of Stu Haber and Scott Stornetta, of Bellcore. Papers presented at various Crypto conferences. Their work involves having the user compute a hash of the document he wishes to be stamped and sending the hash to them, where they merge this hash with other hashes (and all previous hashes, via a tree system) and then they *publish* the resultant hash in a very public and hard-to-alter forum, such as in an ad in the Sunday "New York Times."

In their parlance, such an ad is a "widely witnessed event," and attempts to alter all or even many copies of the newspaper would be very difficult and expensive. (In a sense, this WWE is similar to the "beacon" term Eric Hughes used.)

Haber and Stornetta plan some sort of commercial operation to do this.

This service has not yet been tested in court, so far as I know. The MIT server is an experiment, and is probably useful for experimenting. But it is undoubtedly even less legally significant, of course.

14.3.2. my summary

14.4. Voting

14.4.1. fraud, is-a-person, forging identities, increased "number" trends

14.4.2. costs also high

14.4.3. Chaum

14.4.4. voting isomorphic to digital money

- where account transfers are the thing being voted on, and the "eligible voters" are oneself...unless this sort of thing is outlawed, which would create other problems, then this makes a form of anonymous transfer possible (more or less)

14.5. Timed-Release Crypto

14.5.1. "Can anything like a "cryptographic time capsule" be built?"

- This would be useful for sealing diaries and records in such a way that no legal bodies could gain access, that even the creator/encryptor would be unable to decrypt the records. Call it "time escrow." Ironically, a much more correct use of the term "escrow" than we saw with the government's various "key escrow" schemes.
- Making records undecryptable is easy: just use a one-way function and the records are unreachable forever. The trick is to have a way to get them back at some future time.

+ Approaches:

- + Legal Repository. A lawyer or set of lawyers has the key or keys and is instructed to release them at some future time. (The key-holding agents need not be lawyers, of course, though that is the way things are now done.)
 - The legal system is a time-honored way of protecting secrets of various kinds, and any system based on cryptography needs to compete strongly with this simple to use, well-established system.
 - If the lawyer's identity is known, he can be subpoenaed. Depends on jurisdictional issues, future political climate, etc.
 - But identity-hiding protocols can be used, so that the lawyer cannot be reached. All that is known, for example, is that "somewhere out there" is an agent who is holding the key(s). Reputation-based systems should work well here: the agent gains little and loses a lot by releasing a key early, hence has no economic motivation to do so. (Picture also a lot of "pinging" going to "rate" the various time agents.)
- Cryptography with Beacons. A "beacon agent" makes very public a series of messages, somehow. Details fuzzy. [I have a hunch that using digital time-stamping services could be useful here.]
- + Difficulty of factoring, etc.
 - + The idea here is to-use a function which is presently hard to invert, but which may be easier in the future. This is fraught with problems, including unpredictability of the difficulty, imprecision in the timing of release, and general clumsiness. As Hal Finney notes:
 - "There was a talk on this topic at either the Crypto 92 or 93 conference, I forget which. It is available in the proceedings....The method used was similar to the idea here of encrypting with a public key and requiring factoring of the modulus to decrypt. But the author had more techniques he used, iterating

functions forward which would take longer to iterate backwards. The purpose was to give a more predictable time to decrypt.....One problem with this is that it does not so much put a time floor on the decryption, but rather a cost floor. Someone who is willing to spend enough can decrypt faster than someone who spends less. Another problem is the difficulty of forecasting the growth of computational power per dollar in the future." [Hal Finney, sci.crypt, 1994-8-04]

- + Tamper-resistant modules. A la the scheme to send the secrets to a satellite in orbit and expect that it will be prohibitively expensive to rendezvous and enter this satellite.
 - Or to gain access to tamper-resistant modules located in bank vaults, etc.
 - But court orders and black bag jobs still are factors.

14.5.2. Needs

- journalism
- + time-stamping is a kind of example
 - though better seen in the conventional analysis
- persistent institutions
- shell games for moving money around, untraceably

14.5.3. How

- beacons
- multi-part keys
- contracted-for services (like publishing keys)
- Wayner, my proposal, Eric Hughes

14.6. Traffic Analysis

14.6.1. digital form, and headers, LEAF fields, etc., make it vastly easier to know who has called whom, for how long, etc.

14.6.2. (esp. in contrast to purely analog systems)

14.7. Steganography

14.7.1. (Another one of the topics that gets a lot of posts)

14.7.2. Hiding messages in other messages

- "Kevin Brown makes some interesting points about steganography and steganalysis. The issue of recognizing whether a message has or might have a hidden message has two sides. One is for the desired recipient to be clued that he should try desteganizing and decrypting the message, and the other is for a possible attacker to discover illegal uses of cryptography.

"Steganography should be used with a "stealthy" cryptosystem (secret key or public key), one in which the cyphertext is indistinguishable from a random bit string. You would not want it to have any headers which could be used to confirm that a desteganized message was other than random noise." [Hal Finney, 1993-05-25]

14.7.3. Peter Wayner's "Mimic"

- "They encode a secret message inside a harmless looking ASCII text file. This is one of the very few times the UNIX tools "lex" and "yacc" have been used in cryptography, as far as I know. Peter Wayner, "Mimic Functions", CRYPTOLOGIA Volume 16, Number 3, pp. 193-214,

July 1992.[Michael Johnson, sci.crypt, 1994-09-05]

14.7.4. I described it in 1988 or 89 and many times since

- Several years ago I posted to sci.crypt my "novel" idea for packing bits into the essentially inaudible "least significant bits" (LSBs) of digital recordings, such as DATs and CDs. Ditto for the LSBs in an 8-bit image or 24-bit color image. I've since seen this idea reinvented several times on sci.crypt and elsewhere...and I'm willing to bet I wasn't the first, either (so I don't claim any credit).

A 2-hour DAT contains about 10 Gbits (2 hours x 3600 sec/hr x 2 channels x 16 bits/sample x 44K samples/sec), or about 1.2 Gbytes. A CD contains about half this, i.e., about 700 Mbytes. The LSB of a DAT is 1/16th of the 1.2 Gbytes, or 80 Mbytes. This is a lot of storage!

A home-recorded DAT--and I use a Sony D-3 DAT Walkman to make tapes--has so much noise down at the LSB level--noise from the A/D and D/A converters, noise from the microphones (if any), etc.--that the bits are essentially random at this level. (This is a subtle, but important, point: a factory recorded DAT or CD will have predetermined bits at all levels, i.e., the authorities could in principle spot any modifications. But home-recorded, or dubbed, DATs will of course not be subject to this kind of analysis.) Some care might be taken to ensure that the statistical properties of the signal bits resemble what would be expected with "noise" bits, but this will be a minor hurdle.

Adobe Photoshop can be used to easily place message bits in the "noise" that dominates things down at the LSB level. The resulting GIF can then be posted to UseNet or e-mailed. Ditto for sound samples, using the ideas I just described (but typically requiring sound sampling boards, etc.). I've done some experiments along these lines.

This doesn't mean our problems are solved, of course. Exchanging tapes is cumbersome and vulnerable to stings. But it does help to point out the utter futility of trying to stop the flow of bits.

14.7.5. Stego, other versions

- Romana Machado's Macintosh stego program is located in the compression files, /cmp, in the sumex-aim@stanford.edu info-mac archives.
- "Stego is a tool that enables you to embed data in, and retrieve data from, Macintosh PICT format files, without changing the appearance of the PICT file. Though its effect is visually undetectable, do not expect cryptographic security from Stego. Be aware that anyone with a copy of Stego can retrieve your data from your PICT file. Stego can be used as an "envelope" to hide a previously encrypted data file in a PICT file, making it much less likely to be detected." [Romana Machado, 1993-11-23]

14.7.6. WNSTORM, Arsen Ray Arachelian

- 14.7.7. talk about it being used to "watermark" images
- 14.7.8. Crypto and steganography used to plant false and misleading nuclear information
 - "Under a sub-sub-sub-contract I once worked on some phony CAD drawings for the nuclear weapons production process, plotting false info that still appears in popular books, some of which has been posted here....The docs were then encrypted and steganographed for authenticity. We were told that they were turned loose on the market for this product in other countries." [John Young, 1994-08-25]
 - Well...
- 14.7.9. Postscript steganography
 - where info is embedded in spacings, font characteristics (angles, arcs)
 - ftp://research.att.com/dist/brassil/infocom94.ps
 - the essential point: just another haystack to hide a needle
- 14.8. Hiding cyphertext
- 14.8.1. "Ciphertext can be "uncompressed" to impose desired statistical properties. A non-adaptive first-order arithmetic decompression will generate first-order symbol frequencies that emulate, for instance, English text." [Rick F. Hoselton, sci.crypt, 1994-07-05]
- 14.9. 'What are tamper-responding or tamper-resistant modules?'
- 14.9.1. The more modern name for what used to be called "tamper-proof boxes"
- 14.9.2. Uses:
 - alarmed display cases, pressure-sensitive, etc. (jewels, art, etc.)
 - + chips with extra layers, fuses, abrasive compounds in the packaging
 - to slow down grinding, etching, other depotting or decapping methods
 - VLSI Technology Inc. reportedly uses these methods in its implementation of the MYK-78 "Clipper" (EES) chip
 - nuclear weapons ("Permissive Action Links," a la Sandia, Simmons)
 - smartcards that give evidence of tampering, or that become inactive
 - + as an example, disk drives that erase data when plug is pulled, unless proper code is first entered
 - whew! pretty risky (power failures and all), but needed by some
 - like "digital flash paper"
- 14.9.3. Bypassing tamper-responding or tamper-resistant technologies
 - first, you have to know
- 14.10. Whistleblowing
- 14.10.1. This was an early proposed use (my comments on it go back to 1988 at least), and resulted in the creation of alt.whistleblowers.
 - So far, nothing too earth-shattering
- 14.10.2. outing the secret agents of a country, by posting them anonymously to a world-wide Net distribution....that ought to shake things up

14.11. Digital Confessionals

- 14.11.1. religious confessionals and consultations mediated by digital links...very hard for U.S. government to gain access
- 14.11.2. ditto for attorney-client conversations, for sessions with psychiatrists and doctors, etc.
- 14.11.3. (this does not mean these meetings are exempt from the law...witness Feds going after tainted legal fees, and bugging offices of attorneys suspected of being in the drug business)

14.12. Loose Ends

- 14.12.1. Feigenbaum's "Computing with Encrypted Instances" work...links to Eric Hughes's "encrypted open books" ideas.
 - more work needed, clearly

15. Reputations and Credentials

15.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

15.2. SUMMARY: Reputations and Credentials

15.2.1. Main Points

- "a man's word is his bond"
- reputations matter
- the expectation of future interaction/business is crucial

15.2.2. Connections to Other Sections

- see section on Crypto Anarchy for why reputations matter

15.2.3. Where to Find Additional Information

- very little published on this
- Bruce Benson's "The Enterprise of Law"

15.2.4. Miscellaneous Comments

- this is another "transition" chapter, laying the groundwork for Crypto Anarchy

15.3. The Nature of Reputations

15.3.1. The claim by many of us that "reputations" will take care of many problems in crypto anarchic markets is disputed by some (notably Eric Hughes). To be sure, it will not be a trivial issue. Institutions take years or decades to evolve.

15.3.2. However, think of how often we use reputations: friends, books, movies, restaurants, etc

15.3.3. Reputations and other institutions will take time to evolve. Saying "the market will take care of things" may be true, but this may take time. The "invisible hand" doesn't necessarily move swiftly.

15.3.4. "What are 'reputations' and why are they so important?"

- a vague concept related to degree of believability, of trust, etc.
- + "we know it when we see it"
 - (sorry for the cop out, but I don't have a good definition handy....James Donald says studying reputations is "nominalist hot air" [1994-09-02], but I think it's quite important)

- + obvious, in ordinary life, but in the cyberspatial context
 - reputation-based systems
 - escrow, expectations
 - "reputation capital"
 - like book or music recommendations
 - web of trust (is different than just "trust"---tensor, rather than scalar)
- + Actually very common: how most of us deal with our friends, our enemies, the books we read, the restaurants we frequent, etc.
 - we mentally downcheck and upcheck on the basis of experience; we learn
 - Are there examples?
 - Eric's objections
- 15.3.5. "How are reputations acquired, ruined, transferred, etc.?"
 - + First, reputations are not "owned" by the person to whom they are attached by others
 - + the algebra is tricky...maybe Eric Hughes or one of the other pure math types can help straighten out the "calculus of reputations"
 - reputations are not symmetric: just because Alice esteems Bob does mean the reverse is so
 - reputations are not transitive, though they are partially transitive: if Alice esteems Bob and Bob esteems Charles, this may cause Alice to be somewhat more esteemful of Charles.
 - a tensor matrix?
 - a graph?
 - + Any holder of a reputation can "spend" some of his reputation capital
 - in praise or criticism of another agent
 - in reviews (think of Siskel and Ebert "spending" some of their reputation capital in the praise of a movie, and how their own reputations will go up and down as a function of many things, including especially how much the viewing audience agrees with them)
- 15.3.6. "Are they foolproof? Are all the questions answered?"
 - Of course not.
 - And Eric Hughes has in the past said that too much importance is being invested in this idea of reputations, though many or even most of us (who comment on the matter) clearly think otherwise.
 - In any case, much more study is needed. Hal Finney and I have debated this a couple of times (first on the Extropians list, then a couple or more times on the Cypherpunks list), and we are mostly in agreement that this area is very promising and is deserving of much more thought--and even experimentation. (One of my interests in crypto simulations, in "protocol ecologies," is to simulate agents which play games involving reputations, spoofing, transfers of reputations, etc.)
- 15.3.7. Reputations have many aspects
 - + the trading firm which runs others people's money is probably less "reputable" in an important sense than the trading firm in which partners have their own personal fortunes riding....or at least I know which one I'd trust!
 - (But how to guarantee one isn't being fooled, by a spoof,

a sham? Hard to say. Perhaps the "encrypted open books" protocol Eric Hughes is working on will be of use here.)

15.4. Reputations, Institutions

15.5. Reputation-Based Systems and Agoric Open Systems

15.5.1. Evolutionary systems and markets

- + markets, emergent order, Hayek, connectionism
- many related ideas...spontaneous order, self interest, agents, etc.
- + a critique of "blind rationalism"
- or hyperrationalism, the idea that a form model can always be found
- order can develop even in anonymous systems, providing certain types of contacts are established, certain other things

15.5.2. shell games...who knows what?

15.5.3. key is that would-be "burners" must never know when they are actually being tested

- with devastating effects if they burn the tester
- + example: how to guarantee (to some degree of certainty) that an anonymous bank is not renegeing (or whatever)?
- e.g., a Swiss bank that denies knowledge of an account
- key is that bank never know when a withdrawal is just a test (and these tests may be done frequently)
- the importance of repeat business

15.5.4. another key: repeat business...when the gains from burning someone are greater than the expected future business.....

15.5.5. reputations are what keep CA systems from degenerating into flamefests

- digital pseudonyms mean a trail is left, kill files can be used, and people will take care about what they say
- and the systems will not be truly anonymous: some people will see the same other people, allowing the development of histories and continued interactions (recall that in cases where no future interaction is expected, rudeness and flaming creeps in)
- + "Rumormonger" at Apple (and elsewhere) always degenerates into flames and crudities, says Johann Strandberg
- but this is what reputations will partly offset

15.5.6. "brilliant pennies" scam

15.5.7. "reputation float" is how money can be pulled out of the future value of a reputation

15.5.8. Reputation-based systems and repeat business

- + reputations matter...this is the main basis of our economic system
- repeat business....people stop doing business with those they don't trust, or who mistreat them, or those who just don't seem to be reputable
- and even in centrally-controlled systems, reputations matter (can't force people to undertake some relations)
- credit ratings (even for pseudonyms) matter
- escrow agents, bonding, etc.
- criminal systems still rely on reputations and even on honor
- ironically, it is often in cases where there are restrictions on choice that the advantages of reputations

are lost, as when the government bans discrimination, limits choice, or insists on determining who can do business with who

- + Repeat business is the most important aspect
 - granularity of transactions, cash flow, game-theoretic analysis of advantages of "defecting"
 - anytime a transaction has a value that is very large (compared to expected future profits from transactions, or on absolute basis), watch out
 - ideally, a series of smaller transactions are more conducive to fair trading...for example, if one gets a bad meal at a restaurant, one avoids that restaurant in the future, rather than suing (even though one can claim to have been "damaged")
 - issues of contract as well

15.6. Reputations and Evolutionary Game Theory

15.6.1. game of "chicken," where gaining a rep as tough guy, or king of the hill, can head off many future challenges (and hence aid in survival, differential reproduction)

15.7. Positive Reputations

15.7.1. better than negative reputations, because neg reps can be discarded by pseudonym holdes (neg reps are like allowing a credit card to be used then abandoned with a debt on it)

15.7.2. "reputation capital"

15.8. Practical Examples

15.8.1. "Are there any actual examples of software-mediated reputation systems?"

- credit databases...positive and negative reputations

15.8.2. Absent laws which ban strong crypto (and such laws are themselves nearly unenforceable), it will be essentially impossible to stop anonymous transactions and purely reputation-based systems.

- For example, Pr0duct Cypher and Sue D. Nym will be able to use private channels of their own choosing (possibly using anonymous pools, etc.) to communicate and arrange deals. If some form of digital cash exists, they will even be able to transfer this cash. (If not, barter of informations, whatever.)
- So, the issues raised by Hal Finney and others, expressing doubts about the adequacy of reputation capital as a building block (and good concerns they are, by the way), become moot. Society cannot stop willing participants from using reputation and anonymity. This is a major theme of crypto anarchy: the bypassing of convention by willing participants.
- + If Alice and Bob don't care that their physical identities are unknown to each other, why should we care? That is, why should society step in and try to ban this arrangement?
 - they won't be using "our" court systems, so that's not an issue (and longer term, PPLs will take the place of courts, many of us feel)
 - only if Alice and Bob are counting on society, on third parties to the transaction, to do certain things, can society make a claim to be involved

- (A main reason to try to ban anonymity will be to stop "bad" activities, which is a separate issue; banning of "bad" activity is usually pointless, and leads to repressive states. But I digress.)

15.8.3. Part of the "phase change": people opt out of the permission-slip society via strong crypto, making their own decisions on who to trust, who to deal with, who to make financial arrangements with

- + example: credit rating agencies that are not traceable, not prosecutable in any court...people deal with them only if they think they are getting value for their money
- no silly rules that credit rating data can "only" go back some arbitrary number of years (7, in U.S.)...no silly rules about how certain bankruptcies "can't" be considered, how one's record is to be "cleared" if conditions are met, etc.
- rather, all data are considered....customer decides how to weight the data...(if a customer is too persnickety about past lapsed bills, or a bad debt many years in the past, he'll find himself never lending any money, so the "invisible hand" of the free market will tend to correct such overzealousnesses)
- + data havens, credit havens, etc. (often called "offshore data havens," as the current way to do this would be to locate in Caymans, Isle of Man, etc.)
- but clearly they can be "offshore in cyberspace" (anonymous links, etc.)

15.9. Credentials and Reputations

15.9.1. debate about credentials vs. reputations

- James Donald, Hal Finney, etc.
- (insert details of debate here)

15.9.2. Credentials are not as important as many people seem to think

- "Permission slips" for various behaviors: drinking age, admission to movie theaters, business licenses, licenses to drive taxicabs, to read palms (yes, here in Santa Cruz one must have a palm-reading license, separate from the normal "business license")

- + Such credentials often are inappropriate extensions of state power into matters which only parents should handle
- underage drinking? Not my problem! Don't force bars to be babysitters.
- underage viewing of movies? Ditto, even more so.

15.9.3. Proving possession of some credential

15.10. Fraud and False Accusations

15.10.1. "What if someone makes a false accusation?"

- one's belief in an assertion is an emergent phenomenon
- + assertion does not equal proof
- (even "proof" is variable, too)
- false claims eventually reflect on false claimant

15.10.2. Scams, Ponzi Schemes, and Oceania

- + Scams in cyberspace will abound
- anonymous systems will worsen the situation in some ways, but perhaps help in other ways
- certainly there is the risk of losing one's electronic cash very quickly and irretrievably (it's pretty far gone)

- once it's passed through several remailers)
- conpersons (can't say "con men" anymore!) will be there, too
- + Many of you will recall the hype about "Oceania," a proposed independent nation to be built on concrete pontoons, or somesuch. People were encouraged to send in donations. Apparently the scheme/scam collapsed:
 - + "It turned out to all be a scam, actually. The key people involved, Eric Kline and Chuck Geshlieder, allegedly had a scheme set up where they repeatedly paid themselves out of all of the proceeds." [anonymous post, altp.privacy, (reprint of Scott A. Kjar post on Compuserve), 1994-07-28]
 - or was it Eric Klein?

15.11. Loose Ends

15.11.1. Selective disclosure of truth

- More euphemestic than "lying."
- Consider how we react when someone asks us about something we consider overly personal, while a friend or loved one may routinely ask such questions.
- Is "personal" the real issue? Or is that we understand truth is a commodity with value, to be given out for something in return?
- At one extreme, the person who casually and consistently lies earns a poor reputation--anyone encountering them is never certain if the truth is being told. At the other extreme, the "always honest" person essentially gives too much away, revealing preferences, plans, and ideas without consideration.
- I'm all for secrets--and lies, when needed. I believe in selective disclosure of the truth, because the truth carries value and need not be "given away" to anyone who asks.

15.11.2. Cryptography allows virtual networks to arrange by

cryptographic collusion certain goals. Beyond just the standard "cell" system, it allows arrangements, plans, and execution.

- collecting money to have someone killed is an example, albeit a distasteful one

16. Crypto Anarchy

16.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

16.2. SUMMARY: Crypto Anarchy

16.2.1. Main Points

- "...when you want to smash the State, everything looks like a hammer."
- strong crypto as the "building material" for cyberspace (making the walls, the support beams, the locks)

16.2.2. Connections to Other Sections

- this section ties all the other sections together
- 16.2.3. Where to Find Additional Information
 - again, almost nothing written on this
 - Vinge, Friedman, Rand, etc.
- 16.2.4. Miscellaneous Comments
 - a very long section, possibly confusing to many
- 16.3. Introduction
 - 16.3.1. "The revolution will not be televised. The revolution *will*, however, be digitized." Welcome to the New Underworld Order! (a term I have borrowed from writer Claire Sterling.)
 - 16.3.2. "Do the views here express the views of the Cypherpunks as a whole?"
 - This section is controversial. Hence, even more warnings than usual about being careful not to confuse these comments with the beliefs of all or even most Cypherpunks.
 - In fairness, libertarianism is undeniably the most represented ideology on the list, as it is in so much of the Net. The reasons for this have been extensively debated over the years, but it's a fact. If other major ideologies exists, they are fairly hidden on the Cypherpunks list.
 - Yes, some quasi-socialist views are occasionally presented. My friend Dave Mandl, for example, has at times argued for a less-anarchocapitalist view (but I think our views are actually fairly similar...he just has a different language and thinks there's more of a difference than their actually is--insert smiley here).
 - And several Cypherpunks who've thought about the issues of crypto anarchy have been disturbed by the conclusions that seem inevitable (markets for corporate information, assassination made more liquid, data havens, espionage made much easier, and other such implications to be explored later in this section).
 - So, take this section with these caveats.
 - And some of the things I thing are inevitable, and in many cases positive, will be repugnant to some. The end of welfare, the end of subsidies of inner city breeders, for example. The smashing of the national security state through digital espionage, information markets, and selective assassinations are not things that everyone will take comfort in. Some may even call it illegal, seditious, and dangerous. So be it.
 - 16.3.3. "What are the Ideologies of Cyperpunks?"
 - + I mentioned this in an earlier section, but now that I'm discussing "crypto anarchy" in detail it's good to recap some points about the ideology of Cypherpunks.
 - an area fraught with dangers, as many Cypherpunks have differing views of what's important
 - + Two main foci for Cypherpunks:
 - Personal privacy in an increasingly watchful society
 - Undermining of states and governments
 - Of those who speak up, most seem to lean toward the libertarian position, often explicitly so (libertarians often are to be found on the Internet, so this correlation is not surprising)
 - + Socialists and Communitarians
 - Should speak up more than they have. Dave Mandl is the

only one I can recall who's given a coherent summary of his views.

+ My Personal Outlook on Laws and Ideology:

- (Obviously also scattered throughout this document.)

+ Non-coercion Principle

- avoid initiation of physical aggression

- "to each his own" (a "neo-Calvinist" perspective of letting each person pick his path, and not interfering)

- I support no law which can easily be circumvented.

(Traffic laws are a counterexample...I generally agree with basic traffic laws....)

- And I support no law I would not personally be willing to enforce and punish. Murder, rape, theft, etc, but not "victimless crimes," not drug laws, and not 99.9998% of the laws on the books.

- Crypto anarchy is in a sense a throwback to the pre-state days of individual choice about which laws to follow. The community exerted a strong force.

- With strong crypto ("fortress crypto," in law enforcement terms), only an intrusive police state can stop people from accessing "illegal" sites, from communicating with others, from using "unapproved" services, and so on. To pick one example, the "credit data haven" that keeps any and all financial records--rent problems from 1975, bankruptcy proceedings from 1983, divorce settlements, results from private investigators, etc. In the U.S., many such records are "unusable": can't use credit data older than 7 years (under the "Fair Credit Reporting Act"), PI data, etc. But if I am thinking about lending Joe Blow some money, how the hell can I be told I can't "consider" the fact that he declared bankruptcy in 1980, ran out on his debts in Haiti in 1989, and is being sued for all his assets by two ex-wives? The answer is simple: any law which says I am not allowed to take into account information which comes my way is flawed and should be bypassed. Dialing in to a credit haven in Belize is one approach--except wiretaps might still get me caught. Cyberspace allows much more convenient and secure bypasses of these laws.

- (For those of you who think such bypasses of laws are immoral, tough. Strong crypto allows this. Get used to it.)

16.3.4. Early history of crypto anarchy

+ 1987-8, AMIX, Salin, Manifesto

- discussed crypto implications with Phil Salin and Gayle Pergamit, in December of 1987

- with a larger group, including Marc Stiegler, Dave Ross, Jim Bennett, Phil Salin, etc., in June 1988.

- released "The Crypto Anarchist Manifesto" in August 1988.

- Fen LaBalme had "Guerillan Information Net" (GIN), which he and I discussed in 1988 at the Hackers Conference

+ "From Crossbows to Cryptography," 1987?

- made similar points, but some important differences

- TAZ also being written at this time

16.4. The Crypto Anarchist Manifesto

16.4.1. Unchanged since it's writing in mid-1988, except for my e-mail address.

- There are some changes I'd make, but...
 - It was written quickly, and in a style to deliberately mimic what I remembered of the "Communist Manifesto." (for ironic reasons)
 - Still., I'm proud that more than six years ago I correctly saw some major points which Cypherpunks have helped to make happen: remailers, anonymous communication, reputation-based systems, etc.
 - For history's sake, here it is:
- 16.4.2.

The Crypto Anarchist Manifesto

Timothy C. May
tcmay@netcom.com

A specter is haunting the modern world, the specter of crypto anarchy.

Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other. Interactions over networks will be untraceable, via extensive re-routing of encrypted packets and tamper-proof boxes which implement cryptographic protocols with nearly perfect assurance against any tampering. Reputations will be of central importance, far more important in dealings than even the credit ratings of today. These developments will alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation.

The technology for this revolution--and it surely will be both a social and economic revolution--has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. The focus has until now been on academic conferences in Europe and the U.S., conferences monitored closely by the National Security Agency. But only recently have computer networks and personal computers attained sufficient speed to make the ideas practically realizable. And the next ten years will bring enough additional speed to make the ideas economically feasible and essentially unstoppable. High-speed networks, ISDN, tamper-proof boxes, smart cards, satellites, Ku-band transmitters, multi-MIPS personal computers, and encryption chips now under development will be some of the enabling technologies.

The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. Many of these concerns will be

valid; crypto anarchy will allow national secrets to be traded freely and will allow illicit and stolen materials to be traded. An anonymous computerized market will even make possible abhorrent markets for assassinations and extortion. Various criminal and foreign elements will be active users of CryptoNet. But this will not halt the spread of crypto anarchy.

Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions. Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property.

Arise, you have nothing to lose but your barbed wire fences!

16.5. Changes are Coming

16.5.1. Technology is dramatically altering the nature of governments.

- It may sound like newage trendiness, but strong crypto is "technological empowerment." It literally gives power to individuals. Like Sam Colt, it makes them equal.
- "Politics has never given anyone lasting freedom, and it never will. Anything gained through politics will be lost again as soon as the society feels threatened. If most Americans have never been oppressed by the government (aside from an annual mugging) it is because most of them have never done anything to threaten the government's interests." [Mike Ingle, 1994-01-01]
- + Thesis: Strong crypto is a good thing
 - tool against governments of all flavors, left and right
 - religious freedom
 - personal choice

16.5.2. Dangers of democracy in general and electronic democracy in particular

- mob rule, rights of minority ignored
- too many things get decided by vote that have no business being voted on
- "don't tax me...", De Tocqueville's warning
- + electronic democracy is even worse
 - moves further from republican, representative system to electronic mob rule
 - too rapid a system
 - Detweiler's "electrocrazy" (spelling?)...brain-damaged, poorly thought-out

16.5.3. The collapse of democracy is predicted by many

- + the "tipping factor" exceeded, with real taxation rates at

50% or more in most developed countries, with conditions of "taxation without representation" far beyond anything in American colonial times

- with professional politicians...and mostly millionaires running for office
- the Cincinnatus (sp?) approach of going into government just for a few years, then returning to the farm or business, is a joke
- + rise of nominalism [argued by James Donald]
 - "After Athenian democracy self destructed, the various warring parties found that they could only have peace if they disowned omnipotent government. They put together a peace agreement that in part proclaimed limits to government, in part acknowledged inherent limits to what was proper for governments to do and in part guaranteed that the government would not go beyond what it was proper for government to do, that the majority could not do as it pleased with the minority, that not any act of power was a law, that law was not merely whatever the government willed.

They did not agree on a constitution but agreed to respect an unwritten constitution that already existed in some sense.

A similar arrangement underlies the American constitution (now defunct) and the English declaration of right (also defunct)

The problem with such formal peace agreements is that they can only be put together after government has substantially collapsed. Some of us wish to try other possibilities in the event of collapse.

The American constitution collapsed because of the rise of nominalist theories "The constitution says whatever the courts say that it says." [James Donald, 1994-08-31]

- War on Drugs, conspiracy charges, random searches, emergency preparedness orders (Operation Vampire Killer, Operation Night Train, REX-84). The killings of more than a dozen reporters and tipsters over the past decade, many of them covering the Iran-Contra story, the drug deals, the CIA's dealings...the Farm appears to be "swamping" more and more of these troublemakers in the headlong march toward fascism.
 - + De Tocqueville's warning that the American experiment in democracy would last only until voters discovered they could pick the pockets of others at the ballot box
 - a point reached about 60 years ago
 - (prior to the federal income tax and then the "New Deal," there were systemic limitations on this ability to the pockets of others, despite populist yearnings by some....after the New Deal, and the Great Society, the modern era of runaway taxation commenced.)
- 16.5.4. Depredations of the State
- + "Discrimination laws"..choice no longer allowed
 - the strip club in LA forced to install wheelchair access-

- for the dancers!
- age no longer allowed to be a factor...gag!
- + democracy run rampant....worst fears of Founders
- votes on everything...
- gun control, seizures, using zoning laws (with FFL inspections as informants)
- welfare state,...Murray, inner cities made worse...theft
- "currency export" laws...how absurd that governments attempt to control what folks do with their own money!
- 16.5.5. Things are likely to get worse, financially (a negative view, though there are also reasons to be optimistic)
- + a welfare state that is careening toward the edge of a cliff...escalating spending, constantly increasing national debt (with no signs that it will ever be paid down)
- pension burdens are rising dramatically, according to "Economist", 1994-08.
- the link to crypto is that folks had better find ways to immunize themselves from the coming crunch
- + Social Security, other pension plans are set to take 30-40% of all GDP
- too many promises, people living longer
- estimate: \$20 trillion in "unfunded liabilities"
- health care expectations... growing national debt
- 16.5.6. Borders are becoming transparent to data...terabytes a day are flowing across borders, with thousands of data formats and virtually indistinguishable from other messages. Compressed files, split files, images, sounds, proprietary encryption formats, etc. Once can almost pity the NSA in the hopelessness of their job.
- 16.6. Free Speech and Liberty--The Effects of Crypto
- 16.6.1. "What freedom of speech is becoming."
- + An increased willingness to limit speech, by attaching restrictions based on it being "commercial" or "hate speech."
- + advertising laws being the obvious example: smoking, alcohol, etc.
- doctors, lawyers, etc.
- sex, nudity
- even laws that say billboards can't show guns
- A chilling but all too common sentiment on the Net is shown by this quote: "Is it freedom of speech to spew racism, and stereotypes, just because you lack the intellectual capacity to comprehend that, perhaps, somewhere, there is a different way of life, which is not congruent with your pre-conceived notions?" [Andrew Beckwith, soc.culture.usa]
- 16.6.2. We don't really have free speech
- election laws
- advertising laws
- + "slander" and "libel"
- thankfully, anonymous systems will make this moot
- + permission needed...licensing, approval, certification
- "qualifications"
- granted, Supremes have made it clear that political comments cannot be restricted, but many other areas have
- often the distinction involves "for pay"
- Perhaps you are thinking that these are not really examples

of government censorship, just of other crimes and other rights taking precedence. Thus, advertisers can't make false or misleading claims, and can't advertise dangerous or otherwise unapproved items. And I can't make medical diagnoses, or give structural and geological advice, and so on...a dozen good examples. But these restrictions emasculate free speech, leaving only banal expression of appropriately-hedged "personal opinions" as the free speech that is allowed...and even that is often subject to crazy lawsuits and threats of legal action.

16.7. The Nature of Anarchies

16.7.1. Anarchy doesn't mean chaos and killing

- As J. Bruce Dawson put it in a review of Linux in the September, 1994 "Byte," "It's anarchy at its best."
- + Ironically, crypto anarchy does admit the possibility (and hence probability) of more contract killings as an ultimate enforcement mechanism for contracts otherwise unenforceable.
- which is what is occurring in drug and other crime situations: the parties cannot go to the police or courts for righting of wrongs, so they need to have the ultimate threat of death to enforce deals. It makes good sense from a reputation/game theory point of view.

16.7.2. Leftists can be anarchists, too

- In fact, this tends to be the popular interpretation of anarchy. (Besides the bomb-throwing, anti-Tsar anarchists of the 19th century, and the bomb-throwing anarchists of the U.S. early this century.)
- + "Temporary Autonomous Zones" (TAZ)
 - Hakim Bey (pseudonym for)
 - Mondo 2000, books, (check with Dave Mandl, who helps to publish them)

16.7.3. Anarchic development

- + Markets and emergent behaviors vs. planned development
 - principles of locality come into play (the local players know what they want and how much they'll pay for it)
 - central planners have "top-down" outlooks
 - Kevin Kelley's "Out of Control" (1994). Also, David Friedman's "Technologies of Freedom."
- An example I heard about recently was Carroll College, in Wisconsin. Instead of building pathways and sidewalks across the newly-constructed grounds, the ground was left bare. After some time, the "emergent pathways" chosen by students and faculty were then turned into paved pathways, neatly solving the problem of people not using the "planned" pathways. I submit that much of life works this way. So does the Net (the "information footpaths"?).
- anarchies are much more common than most people think...personal relationships, choices in life, etc.

16.7.4. The world financial system is a good example: beyond the reach of any single government, even the U.S. New World Order, money moves and flows as doubts and concerns appear. Statist governments are powerless to stop the devaluation of their currencies as investors move their assets (even slight moves can have large marginal effects).

- "anarchy" is not a term most would apply, but it's an

anarchy in the sense of there being no rulers ("an arch"), no central command structure.

16.8. The Nature of Crypto Anarchy

16.8.1. "What is Crypto Anarchy?"

- + "Why the name?"
 - + a partial pun on several things"
 - "crypto," meaning "hidden," as used in the term "crypto fascist" (Gore Vidal called William F. Buckley this)
 - "crypto anarchy" meaning the anarchy will be hidden, not necessarily visible
 - and of course cryptology is centrally involved
- + Motivation
 - Vernor Vinge's "True Names"
 - Ayn Rand was one of the prime motivators of crypto anarchy. What she wanted to do with material technology (mirrors over Galt's Gulch) is much more easily done with mathematical technology.

16.8.2. "Anarchy turns people off...why not a more palatable name?"

- people don't understand the term; if people understood the term, it might be more acceptable
- some have suggested I call it "digital liberty" or somesuch, but I prefer to stick with the historical term

16.8.3. Voluntary interactions involve Schelling points, mutually-agreed upon points of agreement

16.8.4. Crypto anarchy as an ideology rather than as a plan.

- Without false modesty, I think crypto anarchy is one of the few real contributions to ideology in recent memory. The notion of individuals becoming independent of states by bypassing ordinary channels of control is a new one. While there have been hints of this in the cyberpunk genre of writing, and related areas (the works of Vinge especially), the traditional libertarian and anarchist movements have mostly been oblivious to the ramifications of strong crypto.
- Interestingly, David Friedman, son of Milton and author of "The Machinery of Freedom," became a convert to the ideas. At least enough so as to give a talk in Los Angeles entitled "Crypto Anarchy and the State."
- Conventional political ideology has failed to realize the huge changes coming over the next several decades. Focussing on unwinnable battles at the ballot box, they fritter away their energies; they join the political process, but they have nothing to "deal" with, so they lose. The average American actually wants to pick the pockets of his neighbors (to pay for "free" health care, to stop companies from laying-off unneeded workers, to bring more pork back to the local economy), so the average voter is highly unlikely to ever vote for a principled Libertarian candidate.
- Fortunately, how people vote has little effect on certain "ground truths" that emerge out of new technologies and new economic developments.

16.9. Uses of Crypto Anarchy

16.9.1. Markets unfettered by local laws (digital black markets, at least for items that can be moved through cyberspace)

16.9.2. Espionage

16.10. The Implications-Negative and Positive-of Crypto Anarchy

16.10.1. "What are some implications of crypto anarchy?"

- + A return to contracts
 - whiners can't go outside contracts and complain
 - relates to: workers, terms of employment, actions, hurt feelings
 - with untraceable communication, virtual networks....
- + Espionage
 - + Spying is already changing dramatically.
 - + Steele's (or Steeler?) "open sources"
 - collecting info from thousands of Internet sources
 - Well, this cuts both ways..
 - + Will allow:
 - BlackNet-type solicitations for military secrets ("Will pay \$300,000 for xxxx")
 - + Digital Dead Drops
 - totally secure, untraceable (pools, BlackNet mode)
 - no Coke cans near the base of oak trees out on Route 42
 - no chalk marks on mailboxes to signal a message is ready
 - no "burning" of spies by following them to dead drops
 - No wonder the spooks are freaked out!
 - Strong crypto will also have a major effect on NSA, CIA, and FBI abilities to wiretap, to conduct surveillance, and to do domestic and foreign counterintelligence
 - This is not altogether a great thing, as there may be some counterintelligence work that is useful (I'm perhaps betraying my lingering biases), but there's really only one thing to say about it: get used to it. Nothing short of a totalitarian police state (and probably not even that, given the spread of strong crypto) can stop these trends.
 -
- + Bypassing sanctions and boycotts
 - Just because Bill Clinton doesn't like the rulers of Haiti is no reason for me to honor his "sanctions"
 - Individual choice, made possible by strong crypto (untraceable transactions, pseudonyms, black markets)
- + Information Markets and Data Havens
 - medical
 - scientific
 - corporate knowledge
 - dossiers
- + credit reports
 - without the absurd rules limiting what people can store on their computers (e.g., if Alice keeps records going back more than 7 years, blah blah, can be thrown in jail for violating the "Fair Credit Reporting Act")
 - bypassing such laws
 - true, governments can attempt to force disclosure of "reasons" for all decisions (a popular trend, where even one's maid cannot be dismissed without the "reasons" being called into question!); this means that anyone accessing such offshore (or in cyberspace...same

- difference) data bases must find some acceptable reason for the actions they take...shouldn't be too hard
 - (as with so many of these ideas, the beauty is that the using of such services is voluntary....)
 - + Consulting
 - increased liquidity of information
 - + illegal transactions
 - + untraceability and digital money means many "dark" possibilities
 - markets for assassinations
 - stolen property
 - copyright infringement
 - + Espionage
 - information markets (a la AMIX)
 - "digital dead drops"
 - Offshore accounts
 - Money-laundering
 - + Markets for Assassinations
 - This is one of the more disturbing implications of crypto anarchy. Actually, it arises immediately out of strong, unbreakable and untraceable communication and some form of untraceable digital cash. Disturbing it may be, but the implications are also interesting to consider...and inevitable.
 - And not all of the implications are wholly negative.
 - + should put the fear of God into politicians
 - "Day of the Jackal" made electronic
 - any interest group that can (anonymously) gather money can have a politician zapped. Positive and negative implications, of course.
 - The fact is, some people simply need killing. Shocking as that may sound to many, surely everyone would agree that Hitler deserved killing. The "rule of law" sounds noble, but when despicable people control the law, other measures are called for.
 - Personally, I hold that anyone who threatens what I think of as basic rights may need killing. I am held back by the repercussions, the dangers. With liquid markets for liquidations, things may change dramatically.
- 16.10.2. The Negative Side of Crypto Anarchy
- + Comment:
 - There are some very real negative implications; outweighed on the whole by the benefits. After all, free speech has negatives. Pornography has negatives. (This may not be very convincing to many....I can't do it here--the gestalt has to be absorbed and considered.)
 - + Abhorrent markets
 - contract killings
 - can collect money anonymously to have someone whacked...nearly anyone who is controversial can generate enough "contributions"
 - kidnapping, extortion
 - + Contracts and assassinations
 - "Will kill for \$5000"
 - + provides a more "liquid" market (pun intended)
 - sellers and buyers more efficiently matched
 - FBI stings (which are common in hiring hit men) are

- made almost impossible
- the canonical "dark side" example--Eric Drexler, when told of this in 1988, was aghast and claimed I was immoral to even continue working on the implications of crypto anarchy!
- made much easier by the inability to trace payments, the lack of physical meetings, etc.
- + Potential for lawlessness
 - bribery, abuse, blackmail
 - cynicism about who can manipulate the system
- + Solicitation of Crimes
 - untraceably, as we have seen
- + Bribery of Officials and Influencing of Elections
 - and direct contact with officials is not even needed...what if someone "lets it be known" that a council vote in favor of some desired project will result in campaign contributions?
- + Child molesters, pederasts, and rapists
 - encrypting their diaries with PGP (a real case, says the FBI)
 - this raises the privacy issue in all its glory...privacy protects illegality...it always has and it always will
- + Espionage is much easier
 - from the guy watching ships leave a harbor to the actual theft of defense secrets
 - job of defending against spies becomes much more difficult: and end to microdots and invisible ink, what with the LSB method and the like that even hides the very existence of encrypted messages!
- + Theft of information
 - from corporations and individuals
 - corporations as we know them today will have to change
 - liquidity of information
 - selling of corporate secrets, or personal information
- + Digilantes and Star Chambers
 - a risk of justice running amok?
- + Some killers are not rehabilitated and need to be disposed of through more direct means
 - + Price, Rhode Island, 21, 4 brutal killings
 - stabbings of children, mother, another
 - + for animals like this, vigilantism...discreet execution...is justified...
 - or, at least some of us will consider it justified
 - which I consider to be a good thing
 - this relates to an important theme: untraceable communication and markets means the ability to "opt out" of conventional morality
- + Loss of trust
 - + even in families, especially if the government offers bounties and rewards
 - recall Pavel Morozov in USSR, DARE-type programs (informing on parents)
 - more than 50% of all IRS suits involve one spouse informing to the IRS
- + how will taxes be affected by the increased black market?
 - a kind of Laffer curve, in which some threshold of taxation triggers disgust and efforts to evade the taxes

- not clear how large the current underground economy is....authorities are motivated to misstate the size (depending on their agenda)
 - + Tax Evasion (I'm not defending taxation, just pointing out what most would call a dark side of CA)
 - + By conducting business secretly, using barter systems, alternative currencies or credit systems, etc.
 - a la the lawyers who use AMIX-like systems to avoid being taxed on mutual consultations
 - + By doing it offshore
 - so that the "products" are all offshore, even though many or most of the workers are telecommuting or using CA schemes
 - recall that many musicians left Europe to avoid 90% tax rates
 - + the "nest egg" scam: drawing on a lump sum not reported
 - + Scenario: Alice sells something very valuable-perhaps the specs on a new product-to Bob. She deposits the fee, which is, say, a million dollars, in a series of accounts. This fee is not reported to the IRS or anyone else.
 - the fee could be in cash or in a "promise"
 - in multiple accounts, or just one
 - + regardless, the idea is that she is now paid, say, \$70,000 a year for the next 20 years (what with interest) as a "consultant" to the company which represents her funds
 - this of course does not CA of any form, merely some discreet lawyers
 - and of course Alice reports the income to the IRS-they never challenge the taxpayer to "justify" work done (and would be incapable of "disallowing" the work, as Alice could call it a "retainer," or as pay for Board of Directors duties, or whatever...in practice, it's easiest to call it consulting)
 - + these scams are closely related to similar scams for laundering money, e.g., by selling company assets at artificially low (or high) prices
 - an owner, Charles, could sell assets to a foreign company at low prices and then be rewarded in tax-free, under the table, cash deposited in a foreign account, and we're back to the situation above
 - + Collusion already is common; crypto methods will make some such collusions easier
 - antique dealers at an auction
 - + espionage and trading of national secrets (this has positive aspects as well)
 - "information markets" and anonymous digital cash
 - (This realization, in late 1987, was the inspiration for the ideas behind crypto anarchy.)
 - mistrust
 - widening gap between rich and poor, or those who can use the tools of the age and those who can't
- 16.10.3. The Positive Side of Crypto Anarchy
- (other positive reasons are implicitly scattered throughout this outline)

- + a pure kind of libertarianism
 - those who are afraid of CA can stay away (not strictly true, as the effects will ripple)
 - a way to bypass the erosion of morals, contracts, and commitments (via the central role of reputations and the exclusion of distorting governments)
 - individual responsibility
 - protecting privacy when using hypertext and cyberspace services (many issues here)
 - "it's neat" (the imp of the perverse that likes to see radical ideas)
 - + A return to 4th Amendment protections (or better)
 - Under the current system, if the government suspects a person of hiding assets, of conspiracy, of illegal acts, of tax evasion, etc., they can easily seize bank accounts, stock accounts, boats, cars, ec. In particular, the owner has little opportunity to protect these assets.
 - increased liquidity in markets
 - + undermining of central states
 - loss of tax revenues
 - reduction of control
 - freedom, personal liberty
 - data havens, to bypass local restrictive laws
 - + Anonymous markets for assassinations will have some good aspects
 - the liquidation of politicians and other thieves, the killing of those who have assisted in the communalization of private property
 - a terrible swift sword
- 16.10.4. Will I be sad if anonymous methods allow untraceable markets for assassinations? It depends. In many cases, people deserve death--those who have escaped justice, those who have broken solemn commitments, etc. Gun grabbing politicians, for example should be killed out of hand. Anonymous rodent removal services will be a tool of liberty. The BATF agents who murdered Randy Weaver's wife and son should be shot. If the courts won't do it, a market for hits will do it.
- (Imagine for a moment an "anonymous fund" to collect the money for such a hit. Interesting possibilities.)
 - "Crypto Star Chambers," or what might be called "digilantes," may be formed on-line, and untraceably, to mete out justice to those let off on technicalities. Not altogether a bad thing.
- 16.10.5. on interference in business as justified by "society supports you" arguments (and "opting out")
- + It has been traditionally argued that society/government has a right to regulate businesses, impose rules of behavior, etc., for a couple of reasons:
 - "to promote the general welfare" (a nebulous reason)
 - + because government builds the infrastructure that makes business possible
 - the roads, transportation systems, etc. (actually, most are privately built...only the roads and canal are publically built, and they certainly don't have to be)
 - the police forces, courts, enforcement of contracts, disputes, etc.

- protection from foreign countries, tariff negotiations, etc., even to the *physical* protection against invading countries
- + But with crypto anarchy, *all* of these reasons vanish!
 - society isn't "enabling" the business being transacted (after all, the parties don't even necessarily know what countries the other is in!)
 - no national or local courts are being used, so this set of reasons goes out the window
 - no threat of invasion...or if there is, it isn't something governments can address
- + So, in addition to the basic unenforceability of outlawing crypto anarchy--short of outlawing encryption--there is also no viable argument for having governments interfere on these traditional grounds.
 - (The reasons for them to interfere based on fears for their own future and fears about unsavory and abominable markets being developed (body parts, assassinations, trade secrets, tax evasion, etc.) are of course still "valid," viewed from their perspective, but the other reasons just aren't.)

16.11. Ethics and Morality of Crypto Anarchy

16.11.1. "How do you square these ideas with democracy?"

- I don't; democracy has run amok, fulfilling de Tocqueville's prediction that American democracy would last only until Americans discovered they could pick the pockets of their neighbors at the ballot box
- little chance of changing public opinion, of educating them
- crypto anarchy is a movement of individual opting out, not of mass change and political action

16.11.2. "Is there a moral responsibility to ensure that the overall effects of crypto anarchy are more favorable than unfavorable before promoting it?"

- I don't think so, any more than Thomas Jefferson should have analyzed the future implications of freedom before pushing it so strongly.
- All decisions have implications. Some even cost lives. By not becoming a doctor working in Sub-Saharan Africa, have I "killed thousands"? Certainly I might have saved the lives of thousands of villagers. But I did not kill them just because I chose not to be a doctor. Likewise, by giving money to starving peasants in Bangladesh, lives could undeniably be "saved." But not giving the money does not murder them.
- But such actions of omission are not the same, in my mind, as acts of commission. My freedom, via crypto anarchy, is not an act of force in and of itself.
- Developing an idea is not the same as aggression.
- Crypto anarchy is about personal withdrawal from the system, the "technologies of disconnection," in Kevin Kelly's words.

16.11.3. "Should individuals have the power to decide what they will reveal to others, and to authorities?"

- For many or even most of us, this has an easy answer, and is axiomatically true. But others have doubts, and more people may have doubts as some easily anticipated

- developments occur.
 - (For example, pedophiles using the much-feared "fortress crypto," terrorists communicating in unbreakable codes, tza evaders, etc. Lots of examples.)
 - But because some people use crypto to do putatively evil things, should basic rights be given up? Closed doors can hide criminal acts, but we don't ban closed doors.
- 16.11.4. "Aren't there some dangers and risks to letting people pick and choose their moralities?"
- (Related to questions about group consensus, actions of the state vs. actions of the individual, and the "herd.)
 - Indeed, there are dangers and risks. In the privacy of his home, my neighbor might be operating a torture dungeon for young children he captures. But absent real evidence of this, most nations have not sanctioned the random searches of private dwellings (not even in the U.S.S.R., so far as I know).
- 16.11.5. "As a member of a hated minority (crypto anarchists) I'd rather take my chances on an open market than risk official discrimination by the state.....Mercifully, the technology we are developing will allow everyone who cares to decline to participate in this coercive allocation of power." [Duncan Frissell, 1994-09-08]
- 16.11.6. "Are there technologies which should be "stopped" even before they are deployed?"
- Pandora's Box, "things Man was not meant to know," etc.
 - It used to be that my answer was mostly a clear "No," with nuclear and biological weapons as the only clear exception. But recent events involving key escrow have caused me to rethink things.
 - Imagine a company that's developing home surveillance cameras...perhaps for burglar prevention, child safety, etc. Parents can monitor Junior on ceiling-mounted cameras that can't easily be tampered with or disconnected, without sending out alarms. All well and good.
 - Now imagine that hooks are put into these camera systems to send the captured images to a central office. Again, not necessarily a bad idea--vacationers may want their security company to monitor their houses, etc.
 - The danger is that a repressive government could make the process mandatory....how else to catch sexual deviates, child molesters, marijuana growers, counterfeiters, and the like?
 - Sound implausible, unacceptable, right? Well, key escrow is a form of this.
 - The Danger. That OS vendors will put these SKE systems in place without adequate protections against key escrow being made mandatory at some future date.
- 16.11.7. "Won't crypto anarchy allow some people to do bad things?"
- Sure, so what else is new? Private rooms allows plotters to plot their plots. Etc.
 - Not to sound too glib, but most of the things we think of as basic rights allow various illegal, distasteful, or crummy things to go on. Part of the bargain we make.
 - "Of course you could prevent contract killings by requiring everyone to carry government "escrowed" tape recordings to record all their conversations and requiring them to keep a

diary at all times alibing their all their activities.
This would also make it much easier to stamp out child pornography, plutonium smuggling, and social discrimination against the politically correct." [James Donald, 1994-09-09]

16.12. Practical Problems with Crypto Anarchy

16.12.1. "What if "bad guys" use unbreakable crypto?"

- What if potential criminals are allowed to have locks on their doors? What if potential rapists can buy pornography? What if....
- These are all straw men used in various forms throughout history by tyrants to control their populations. The "sheepocracies" of the modern so-called democratic era are voting away their former freedoms in favor of cradle to grave safety and security.
- The latest tack is to propose limits on privacy to help catch criminals, pedophile, terrorists, and father rapers. God help us if this comes to pass. But Cypherpunks don't wait for God, they write code!

16.12.2. Dealing with the "Abhorrent Markets"

- such as markets for assassinations and extortion
- + Possibilities:
 - + physical protection, physical capture
 - make it risky
 - (on the other hand, sniping is easy)
 - + "flooding" of offers
 - "take a number" (meaning: get in line)
 - attacking reputations
- I agree that more thought is needed, more thorough analysis
- Some people have even pointed out the benefits of killing off tens of thousands of the corrupt politicians, narcs, and cops which have implemented fascist, collectivist policies for so long. Assassination markets may make this much more practical.

16.12.3. "How is *fraud* dealt with in crypto anarchy?"

- When the perpetrators can't even be identified.
- One of the most interesting problems.
- First, reputations matter. Repeat business is not assured. It is always best to not have too much at stake in any single transaction.

16.12.4. "How do we know that crypto anarchy will work? How do we know that it won't plunge the world into barbarism, nuclear war, and terror?"

- We don't know, of course. We never can.
- However, things are already pretty bad. Look at Bosnia, Ruanda, and a hundred other hellholes and flashpoints around the world. Look at the nuclear arsenals of the superpowers, and look at who starts the wars. In nearly all cases, statism is to blame. States have killed a hundred million or more people in this century alone--think of Hitler, Stalin, Mao, and Pol Pot--through forced starvation of entire provinces, liquidation of the peasantry, killing of intellectuals, and mass exterminations of religious and ethnic groups. It's hard to imagine crypto anarchy causing anything that bad!
- Crypto anarchy is a cyberspatially-mediated personal course

of action; by itself it involves no actions such as terrorism or nuclear blackmail. One could just as easily ask, "Will freedom lead to nuclear blackmail, weapons trading, and pedophilia?" The answer is the same: maybe, but so what?

16.12.5. It is true that crypto anarchy is not for everyone. Some will be too incompetent to prepare to protect themselves, and will want a protector. Others will have poor business sense.

16.12.6. "But what will happen to the poor people and those on welfare if crypto anarchy really succeeds?"

- "So?"
- Many of us would see this as a good thing. Not just for Calvinist-Randite reasons, but also because it would break the cycle of dependency which has actually made things worse for the underclass in America (at least). See Charles Murray's "Losing Ground" for more on this.
- And remember that a collapse of the tax system will mean more money left in the hands of former taxpayers, and hence more left over for true charity (for those who truly cannot help themselves).

16.13. Black Markets

16.13.1. "Why would anyone use black markets?"

- + when the advantages of doing so outweigh the disadvantages
 - including the chance of getting caught and the consequences
 - (As the chances decline, this suggests a rise in punishment severity)
- businesses will tend to shy away from illegal markets, unless...
- + Anonymous markets for medical products
 - to reduce liability, local ethical and religious laws
 - Example: Live AIDS vaccine...considered too risky for any company to introduce, due to inability to get binding waivers of liability (even for "fully informed" patients who face likely death)
 - markets in body parts...

16.13.2. Crypto anarchy opens up some exciting possibilities for collusion in financial deals, for insider trading, etc.

- I'm not claiming that this will mean instant riches, as markets are fairly efficient (*) and "insiders" often don't do well in the market. (* Some argue that relaxing laws against insider trading will make for an even fairer market...I agree with this.)
- What I am claiming is the SEC and FinCEN computers will be working overtime to try to keep up with the new possibilities crypto anarchy opens up. Untraceable cash, as in offshore bank accounts that one can send anonymous trading instructions to (or for), means insider trading simply can't be stopped...all that happens is that insiders see their bank accounts increase (to the extent they win because of the insider trading...like I said, a debatable point).
- Price signalling, a la the airline case of a few years back (which, you won't be surprised to hear, I have no problems with), will be easier. Untraceable communications, virtual meetings, etc.

16.13.3. Information Markets

- a la "information brokering," but mediated cryptographically
- recall the 1981 market in Exocet missile codes (France, Argentina--later of relevance when an Exocet sank a British ship)

16.13.4. Black Markets, Informal Economies, Export Laws

- + Transborder data flow, legal issues
- + complex..laws, copyrights, "national sovereignty"
 - e.g., Phillipines demanded in-the-clear transmissions during bank loan renegotiations..and several Latin American countries forbid encrypted transmissions.
- + Export, Technology Export, Export Control
 - Export Control Act
 - Office of Munitions (as in "Munitions Act", circa 1918)
- + export of some crypto gear shifted from Dept. of State, Office of Munitions, to Dept. of Commerce
 - Commodity Control List, allows s/w that is freely available to the public to be exported without additional paperwork
 - Munitions used to be stickier about export (some would say justifiably paranoid)
 - Commodity Jurisdiction request, to see whether product for export falls under State or Commerce regulations
 - Trading with the Enemy Act
 - Exocet codes--black market sales of emasculated chips

16.13.5. Smuggling and Black Markets

- + Black Markets in the USSR and Other Former East Bloc Nations
 - + a major issue, because the normal mechanisms for free markets--property laws, shops, stock markets, hard currencies, etc.-have not been in place
 - in Russia, have never really existed
- + Role of "Mafia"
 - various family-related groups (which is how trade always starts, via contacts and connections and family loyalty, until corporations and their own structures of loyalty and trust can evolve)
- + how the Mafia in Russia works
 - bribes to "lose" materials, even entire trainloads
 - black market currency (dollars favored)
- + This could cause major discontent in Russia
 - as the privileged, many of them ex-Communist officials, are best prepared to make the transition to capitalism
- + those in factory jobs, on pensions, etc., will not have the disposable income to take advantage of the new opportunities
 - America had the dual advantages of a frontier that people wanted to move to (Turner, Protestant ethic, etc.) and a high-growth era (industrialization)
 - plus, there was no exposure to other countries at vastly higher living standards
- + Smuggling in the EEC
 - + the dream of tariff-free borders has given way to the reality of a complex web of laws dictating what is politically correct and what is not:
 - animal growth hormones

- artificial sweeteners are limited after 1-93 to a small list of approved foods: and the British are finding that their cherished "prawn cocktail-flavored crisps" are to be banned (for export to EEC or completely?) because they're made with saccharin or aspartame
- "European content" in television and movies may limit American productions...as with Canada, isn't this a major abridgement of basic freedoms?
- + this may lead to a new kind of smuggling in "politically incorrect" items
 - could be argued that this is already the case with bans on drugs, animal skins, ivory, etc. (so tediously argued by Brin)
 - recall Turgut Ozal's refreshing comments about loosening up on border restrictions
- + as more items are declared bootleg, smuggling will increase...politically incorrect contraband (fur, ivory, racist and sexist literature)
- + the point about sexist and racist literature being contraband is telling: such literature (books, magazines) may not be formally banned, for that would violate the First Amendment, but may still be imported anonymously (smuggled) and distributed as if they were banned (!) for the reason of avoiding the "damage claims" of people who claim they were victimized, assaulted, etc. as a result of the literature!
- + avoidance of prosecution or damage claims for writing, editing, distributing, or selling "damaging" materials is yet another reason for anonymous systems to emerge: those involved in the process will seek to immunize themselves from the various tort claims that are clogging the courts
 - producers, distributors, directors, writers, and even actors of x-rated or otherwise "unacceptable" material may have to have the protection of anonymous systems
 - imagine fiber optics and the proliferation of videos and talk shows....bluenoses and prosecutors will use "forum shopping" to block access, to prosecute the producers, etc.
- + Third World countries may declare "national sovereignty over genetic resources" and thus block the free export and use of plant- and animal-derived drugs and other products
 - even when only a single plant is taken
 - royalties, taxes, fees, licenses to be paid to local gene banks
 - these gene banks would be the only ones allowed to do genetic cataloguing
 - the problem is of course one of enforcement
- + technology, programs
 - scenario: many useful programs are priced for corporations (as with hotel rooms, airline tickets, etc.), and price-sensitive consumers will not pay \$800 for a program they'll use occasionally to grind out term papers and church newsletters
- + Scenario: Anonymous organ donor banks

- + e.g., a way to "market" rare blood types, or whatever, without exposing one's self to forced donation or other sanctions
 - "forced donation" involves the lawsuits filed by the potential recipient
 - at the time of offer, at least...what happens when the deal is consummated is another domain
 - and a way to avoid the growing number of government stings
 - + the abortion and women's rights underground...a hopefully ally (amidst the generally antiliberty women's movement)
 - RU-486, underground abortion clinics (because many clinics have been firebombed, boycotted out of existence, cut off from services and supplies)
 - + Illegal aliens and immigration
 - "The Boxer Barrier" used to seal barriers...Barbara Boxer wants the military and national guard to control illegal immigration, so it would be poetic justice indeed if this program has her name on it
- 16.13.6. Organized Crime and Cryptoanarchy
- + How and Why
 - + wherever money is to be made, some in the underworld will naturally take an interest
 - loan sharking, numbers games, etc.
 - + they may get involved in the setup of underground banks, using CA protocols
 - shell games, anonymity
 - such Mafia involvement in an underground monetary system could really spread the techniques
 - + but then both sides may be lobbying with the Mafia
 - the CA advocates make a deal with the devil
 - and the government wants the Mob to help eradicate the methods
 - + Specific Programs
 - + False Identities
 - in the computerized world of the 90s, even the Mob (who usually avoid credit cards, social security numbers, etc.) will have to deal with how easily their movements can be traced
 - + so the Mob will involve itself in false IDs
 - as mentioned by Koontz
 - Money Laundering, naturally
 - + but some in the government see some major freelance opportunities in CA and begin to use it (this undermines the control of CA and actually spreads it, because the government is working at cross purposes)
 - analogous to the way the government's use of drug trade systems spread the techniques
- 16.13.7. "Digital Escrow" accounts for mutually suspicious parties, especially in illegal transactions
- drug deals, information brokering, inside information, etc.
 - + But why will the escrow entity be trusted?
 - + reputations
 - their business is being a reliable escrow holder, not it destroying their reputation for a bribe or a threat
 - + anonymity means the escrow company won't know who it's "burning," should it try to do so

- they never know when they themselves are being tested by some service
 - and potential bribers will not know who to contact, although mail could be addressed to the escrow company easily enough
- 16.13.8. Private companies are often allies of the government with regards to black markets (or grey markets)
- they see uncontrolled trade as undercutting their monopoly powers
 - a way to limit competition
- 16.14. Money Laundering and Tax Avoidance
- 16.14.1. Hopelessness of controlling money laundering
- + I see all this rise in moneylaunders as an incredibly hopeful trend, one that will mesh nicely with the use of cryptography
 - why should export of currency be limited?
 - what's wrong with tax evasion, anyway?
 - corrupting, affects all transactions
 - vast amounts of money flowing
 - 2000 banks in Russia, mostly money-laundering
 - + people and countries are so starved for hard currency that most banks outside the U.S. will happily take this money
 - no natural resources in many of these countries
 - hopeless to control
 - being presented as "profits vs. principals," but I think this is grossly misguided
 - + Jeffery Robinson, "The Landrymen," interviewed on CNN, 6-24-94
 - "closer to anarchy" (yeah!)
 - hopeless to control
 - dozens of new countries, starved for hard currency, have autonomy to set banking policies (and most European countries turn a blind eye toward most of the anti-laundering provisions)
- 16.14.2. Taxes and Crypto
- besides avoidance, there are also issues of tax records, sales tax, receipts, etc.
 - + this is another reason government may demand access to cyberspace:
 - to ensure compliance, a la a tamper-resistant cash register
 - to avoid under-the-table transactions
 - bribery, side payments, etc.
 - Note: It is unlikely that such access to records would stop all fraud or tax evasion. I'm just citing reasons for them to try to have access.
 - I have never claimed the tax system will collapse totally, or overnight, or without a fight. Things take time.
 - + tax compliance rates dropping
 - + the fabric has already unraveled in many countries, where the official standard of living is below the apparent standard of living (e.g., Italy).
 - tax evasion a major thing
 - money runs across the border into Switzerland and Austria
 - Frissell's figures

- media reports
- + Tax issues, and how strong crypto makes it harder and harder to enforce
 - hiding income, international markets, consultants, complexly structured transactions

16.14.3. Capital Flight

- "The important issue for Cypherpunks is how we should respond to this seemingly inevitable increased mobility of capital. Does it pose a threat to privacy? If so, let's write code to thwart the threat. Does it offer us any tools we can use to fight the efforts of nation-states to take away our privacy? If so, let's write code to take advantage of those tools." [Sandy Sandfort, Decline and Fall, 1994--06-19]

16.14.4. Money Laundering and Underground Banks

- + a vast amount of money is becoming available under the table: from skimming, from tax avoidance, and from illegal activities of all kinds
 - can be viewed as part of the internationalization of all enterprises: for example, the Pakistani worker who might have put his few rupees into some local bank now deposits it with the BCCI in Karachi, gaining a higher yield and also increasing the "multiplier" (as these rupees get lent out many times)
 - is what happened in the U.S. many years ago
 - this will accelerate as governments try to get more taxes from their most sophisticated and technical taxpayers, i.e., clever ways to hide income will be sought
- + BCCI, Money-Laundering, Front Banks, CIA, Organized Crime
- + Money Laundering
 - New York City is the main clearinghouse, Federal Reserve of New York oversees this
 - Fedwire system
 - trillions of dollars pass through this system, daily
- + How money laundering can work (a maze of techniques)
 - a million dollars to be laundered
 - agent wires it, perhaps along with other funds, to Panama or to some other country
 - bank in Panama can issue it to anyone who presents the proper letter
 - various ways for it to move to Europe, be issued as bearer stock, etc.
 - 1968, offshore mutual funds, Bernie Kornfield
- + CIA often prefers banks with Mob connections
 - because Mob banks already have the necessary security and anonymity
 - and are willing to work with the Company in ways that conventional banks may not be
- + links go back to OSS and Mafia in Italy and Sicily, and to heroin trade in SE Asia
 - Naval Intelligence struck a deal in WW2 with Mafia, whereby Meyer Lansky would protect the docks against strikes (presumably in exchange for a "cut"), if Lucky Luciano would be released at the end of the war (he was)
 - Operation Underworld: Mafia assisted Allied troops in Sicily

- "the Corse"
- + Luciano helped in 1947 to reopen Marseilles when Communist strikers had shut it down
 - continuing the pattern of cooperation begun during the war
 - thus establishing the French Connection!
- Nugan Hand Bank
- + BCCI and Bank of America favored by CIA
 - Russbacher says B of A a favored cover
 - + we will almost certainly discover that BCCI was the main bank used, with the ties to Bank of America offices in Vienna
 - + Bank of America has admitted to having had early ties with BCCI in the early 1970s, but claims to have severed those ties
 - however, Russbacher says that CIA used B of A as their preferred bank in Europe, especially since it had ties to companies like IBM that were used as covers for their covert ops
 - Vienna was a favored money-laundering center for CIA, especially using Bank of America
- + a swirl of paper fronts, hiding the flows from regulators and investors
 - "nominees" used to hide true owners and true activities
 - various nations have banking secrecy laws, creating the "veil" that cannot be pierced
- + CIA knew about all of the flights to South America (and probably elsewhere, too)
 - admitted Thomas Polgar, a senior ex-CIA official, in testimony on 9-19-91
 - this indicates that CIA knew about the arms deals, the drug deals, and the various other schemes and scams
- + Earlier CIA-Bank Scandals (Nugan Hand and Castle Bank)
 - + Nugan Hand Bank, Australia
 - + Frank Nugan, Sydney, Australia, died in 1980
 - + apparent suicide, but clearly rigged
 - Mercedes, rifle with no fingerprints, position all wrong
 - evidence that he'd had a change of heart-was praying daily, a la Charles Colson-and was thinking about getting out of the business
 - + set up Nugan Hand Bank in 1973
 - private banking services, tax-free deposits in Caymans
 - + used by CIA agents, both for Agency operations and for their own private slush/retirement funds
 - several CIA types on the payroll (listed their addresses as same as Air America)
 - William Colby on Board, and was their lawyer
 - + links to organized crime, e.g., Santo Trafficante, Jr.
 - Florida, heroin, links to JFK assassination
 - trafficante was known as "the Cobra" and handled many transactions for the CIA
- + money-laundering for Asian drug dealers
 - + Golden Triangle: N-H even had branches in GT
 - and branch in Chiang Mai, in Thailand

- links to arms dealers, like Edwin P. Wilson
- + U.S. authorities refused to cooperate with investigations
 - and when info was released, it was blacked out with a "B-1" note, implying national security implications
- + investigations by Australian Federal Bureau of Narcotics were thwarted-agents transferred and Bureau disbanded shortly thereafter
 - similar to "Don't fuck with us" message sent to FBI and DEA by CIA
- + N-H Bank had close working relation with Australian Security Intelligence Organization (ASIO)
 - NSA tapped phone conversations (speculative) of Nugan that indicated ASIO collusion with N-H Bank in the drug trade
- + Pine Gap facility, near Alice Springs (NSA, NRO)
 - P.M. Gough Whitlam's criticism of Pine Gap led to CIA-ASIO plot to destroy the Whitlam gov't.
 - November 1975 fall instigated with wiretaps and forgeries
- + Nugan Hand Bank was also involved with "Task Force 157," a Naval Intelligence covert operation, given the cover name "Pierce Morgan" (a good name?)
 - reported to Henry Kissinger
 - recall minor point that Navy is often the preferred service for the ruling elite (the real preppies)
- + and George Bush's son, George W. Bush, was involved with Nugan Hand:
 - linked to William Quasha, who handled N-H deals in Phillipines
- + owners of Harken Energy Corp. a Texas-based company that bought G.W. Bush's oil company "Spectrum 7" in 1986
 - later got offshore drilling rights to Bahrain's oil-with G.W. Bush on the Board of Directors
 - could this be another link to Gulf Crisis?
- + Castle Bank, Bahamas, Paul E. Helliwell
- + OSS (China). CIA
 - Mitch WerBell, White Russian specialist in assassination, silencers, worked for him in China
 - Howard Hunt worked for him
 - after WW2, set up Sea Supply Inc., CIA front in Miami
- + linked to Resorts International
 - law firm of Helliwell, Melrose and DeWolf
 - lent money to Bahamian P.M. Lynden Pindling in exchange for extension of gambling license
- + Robert Vesco, Bebe Rebozo, and Howard Hughes
 - in contrast to the "Eastern Establishment," these were Nixon's insiders
 - links with ex-CIA agent Robert Maheu (who worked for Hughes); involved with Trafficante, CIA plot to kill Castro, and possible links to JFK assassination
 - Vesco active in drug trade
- + also involved in purchase of land for Walt Disney World

- 27,000 acres near Orlando
- Castle Bank was a CIA conduit
- + Operation Tradewinds, IRS probe of bank money flows
 - late 60s
 - investigation of "brass plate" companies in Caymans, Bahamas
- + Plot Scenario: Operation Tradewinds uncovered many UltraBlack operations, forcing them to retrench and dig in deeper, sacrificing several hundred million
 - circa 1977 (Castle Bank shut down)
- + World Finance Corporation (WFC)
 - + started in 1971 in Coral Gables
 - first known as Republic National Corporation
 - Walter Surrey, ex-OSS, like Helliwell of Castle Bank, helped incorporate it
 - + Business
 - exploited cash flows in Florida
 - dealt with CIA, Vesco, Santo Trafficante, Jr.
 - also got loan deposits from Arabs
 - links to Narodny Bank, the Soviet bank that also pay agents
 - + a related company was Dominion Mortgage Company, located at same address as WFC
 - linked to narcotics flow into Las Vegas
 - and to Trafficante, Jr.
 - suitcases of cash laundered from Las Vegas to Miami
 - Jefferson Savings and Loan Association, Texas
- + Guillermo Hernandez Cartaya, ex-Havana banker, Cuban exile, was chief figure
 - veteran of Bay of Pigs (likely CIA contacts)
 - investigated by R. Jerome Sanford, Miami assistant U.S. attorney
 - Dade County Organized Crime Bureau also involved in the 1978 investigation
- Rewald and his banking deals
- BCCI was a successor to this bank
- + CIA and DEA Links to Drug Trade
 - former agents and drug traffickers were frequently recruited by DEA and CIA to run their own drug operation, sometimes with political motivations
 - Carlos Hernandez recruited by BNDD (Bureau of Narcotics and Dangerous drugs, predecessor to DEA) to form a death squad to assassinate other drug traffickers
- + possible links of the drug dealers to UltraBlack/Witness Security Program
 - agents in Florida, the stock broker killing in 1987
 - Seal was betrayed by the DEA and CIA, allowed to be killed by the Columbians
- + Afghan Rebels, Arms to Iran (and Iraq), CIA, Pakistan
 - there was a banking and arms-running network centered in Karachi, home of BCCI, for the various arms deals involving Afghan rebels
 - Karachi, Islamabad, other cities
- + Influence Peddling, Agents
 - a la the many senior lawyers hired by BCCI (Clark

- Clifford, Frank Manckiewicz [spelling?]
- + illustrates again the basic corruptability of a centralized command economy, where regulators and lawmakers are often in the pockets of corrupt enterprises
 - clearly some scandals and losses will occur in free markets, but at least the free markets will not be backed up with government coercion
- + Why CIA is Involved in So Many Shady Deals?
 - + ideal cover for covert operations
 - outside audit channels
 - links to underworld
 - + agents providing for their own retirements, their own private deals, and feathering their own nests
 - freedom from interference
 - greed
 - + deals like that of Noriega, in which CIA-supported dictators and agents provided for their own lavish lifestyles\
 - and the BCCI-Noriega links are believed to have contributed to the CIA's unwillingness to question the activities of the BCCI (actually, the Justice Department)
- + Role of Banks in Iraq and Gulf War, Iraq-Gate, Scandals
 - Export Import Bank (Ex-Im), CCC
 - implicated in the arming of Iraq
 - Banco Lavorzo Nazionale [spelling?]
- + CIA was using BNL to arrange \$5B in transfers, to arm Iraq, to ensure equality with Iran
 - because BNL wouldn't ask where it came from
 - federally guaranteed loans used to finance covert ops
- + the privatizing of covert ops by the CIA and NSA
 - deniability
 - they subcontracted the law-breaking
 - the darker side of capitalism did the real work
 - but the crooks learned quickly just how much they could steal...probably 75% of stolen money
 - insurance fraud...planes allowed to be stolen, then shipped to Contras, with Ollie North arguing that nobody was really hurt by this whole process
- + ironically, wealthy Kuwaitis were active in financing "instant banks" for money laundering and arms transactions, e.g., several in Channel Islands
 - Ahmad Al Babbain Group of Companies, Ltd., a Netherlands Antilles corporation
- Inslaw case fits in with this picture
- + Federal Reserve and SEC Lack the Power to "Peirce the Veil" on Foreign Banks
 - as the Morgenthau case in Manhattan develops
 - a well-known issue
- + But should we be so surprised?
 - haven't banks always funded wars and arms merchants?
 - and haven't some of them failed?
 - look at the Rothschilds
 - what is surprising is that so many people knew what it was doing, what its business was, and that it was even nicknamed "Banks of Crooks and Criminals International"

- + Using software agents for money laundering and other illegal acts
 - + these agents act as semi-autonomous programs that are a few steps beyond simple algorithms
 - it is not at all clear that these agents could do very much to run portfolio, because nothing really works
 - real use could be as "digital cutouts": transferring wealth to other agents (also controlled from afar, like marionettes)
 - advantage is that they can be programmed to perform operations that are perhaps illegal, but without traceability
 - + Information brokers as money launderers (the two are closely related)
 - the rise of AMIX-style information markets and Sterling-style "data havens" will provide new avenues for money laundering and asset-hiding
 - + information is intrinsically hard to value, hard to put a price tag on (it varies according to the needs of the buyers)
 - meaning that transnational flows of information cannot be accurately valued (assigned a cash value)
 - is closely related to the idea of informal consulting and the nontaxable nature of it
 - cardboard boxes filled with cash, taped and strapped, but still bursting open
 - gym bags carrying relatively tiny amounts of the skim: a mere hundred thousand in \$100s
 - + L.A. becoming a focus for much of this cash
 - nearness to Mexico, large immigrant communities
 - freeways and easy access
 - + hundreds of airstrips, dozens of harbors
 - though East Coast seems to have even more, so this doesn't seem like a compelling reason
 - Ventura County and Santa Barbara
- 16.14.5. Private Currencies, Denationalization of Money
- Lysander Spooner advocated these private currencies
 - and "denationalization of money" is a hot topic
 - + in effect, alternatives to normal currency already exist
 - coupons, frequent flier coupons, etc.
 - + telephone cards and coupons (widely used in Asia and parts of Europe)
 - ironically, U.S. had mostly opted for credit cards, which are fully traceable and offer minimal privacy, while other nations have embraced the anonymity of their kind of cards...and this seems to be carrying over to the toll booth systems being planned
 - barter networks
 - chop marks (in Asia)
 - + "reputations" and favors
 - if Al gives Bob some advice, is this taxable? (do lawyers who talk amongst themselves report the transactions/ of course not, and yet this is effectively either a barter transaction or an outright gift)
 - + sophisticated financial alternatives to the dollar

- various instruments
- futures, forward contracts, etc.
- "information" (more than just favors)
- + art works and similar physical items
 - not a liquid market, but for high rollers, an easy way to transfer hundreds of millions of dollars (even with the discounted values of a stolen item, and not all the items will be stolen...many people will be very careful to never travel with stolen art)
 - diamonds, gems have long been a form of transportable wealth
- + art works need not be declared at most (?) borders
 - this may change with time

16.14.6. Tax Evasion Schemes

- unreported income, e.g., banks like the BCCI obviously did not report what they or their customers were doing to the various tax authorities (or anyone else)
- deferred income, via the kind of trust funds discussed here (wherein payment is deferred and some kind of trust is used to pay smaller amounts per year)
- + Asset-Hiding, Illegal Payments, Bribes, and Tax Evasion Funds Can Be Protected in a "Retirement Fund"
 - + e.g., a politician or information thief-perhaps an Intel employee who sells something for \$1M-can buy shares in a crypto-fund that then ensures he is hired by a succession of consulting firms for yearly consulting...or even just placed on a "retainer" of, say, \$100K a year
 - + IRS may come to have doubts about such services, but unless the government steps in and demands detailed inspection of actual work done-and even then I think this would be impossible and/or illegal-such arrangements would seem to be foolproof
 - + why can't government demand proof of work done?
 - who judges the value of an employee?
 - of advice given, of reports generated, or of the value of having a consultant "on retainer"?
 - such interference would devastate many vested interests
 - + tax and other advantages of these "crypto annuities"
 - tax only paid on the yearly income, not on the lump sum
 - authorities are not alerted to the sudden receipt of a lump sum (an ex-intelligence official who receives a payment of \$1 M will come under suspicion, exactly as would a politician)
 - and a lump sum payment might well arouse suspicions and be considered evidence of some criminal activity
 - + the original lump sum is protected from confiscation by governments, by consideration in alimony or bankruptcy cases, etc.
 - such "consulting annuities" may be purchased just so as to insulate earnings from alimony, bankruptcy, etc.
 - as usual, I'm not defending these steps as moral or as good for the business climate of the world, just as inevitable consequences of many current trends and technical developments

- + the "shell game" is used to protect the funds
 - with periodic withdrawals or transfers
- note that this whole scheme can pretty much be done by attorneys and agents today, though they may be subpoenaed or otherwise encouraged to blab
- + it may not even be illegal for a consultant to take his fee over a period of many years
- + the IRS may claim the "discounted present value" as a lump sum, but other folks already do things like this
 - royalty streams (and nobody claims an author must agree with the IRS to some estimated value of this stream)
 - percentages of the gross (and the like)
 - engineers and other professionals are often kept on payrolls not so much for their instantaneous achievements as for their past and projected achievements—are we to treat future accomplishments in a lump sum way?
- + IRS and others may try to inspect the terms of the employment or consulting agreement, but these seems too invasive and cumbersome
- + it makes the government a third party in all negotiations, requiring agents to be present in all talks or at least to read and understand all paperwork
 - and even then, there could be claims that the government didn't follow the deals
 - not enough time or manpower to handle all these things
 - and the invasion of privacy is extreme!
- + Scenario: the Fincen-type agencies may deal with the growing threat of CA-type systems (and encryption in general) by involving the government in ostensibly private deals
 - analogous to the sales tax and bookkeeping arrangements (where gov't. is a third party to all transactions)
- + or EEOC, race and sex discrimination cases
 - will transcripts and recordings of all job interviews come to be required?
 - "laying track"
 - OSHA, pollution, etc.
- + software copying laws (more to the point):
 - government seems to have the power to enter a business to see if illegal copies are in use; this may first require a warrant
 - + how long before various kinds of software are banned?
 - with the argument being that some kinds of software are analogous to lockpicks and other banned burglar tools
 - "used to facilitate the illegal copying of protected software"
- + the threat of encryption for national security as well as for the money-laundering and illegal payments possibilities may cause the government to place restrictions on the use of crypto

- software for anything except approved uses
(external e-mail, etc.)
 - and even these uses can of course be subverted
 - and crypto techniques are not actually necessary: lawyers and other discreet agents will suffice
 - + furthermore, corporations have a fair amount of latitude in setting retirement policies and benefits, and so the methods I've described to shelter current income may become more widespread
 - + though there may be some proviso that if benefits exceed some percentage of yearly income, factoring in years on the job, that these benefits are taxed in some punitive way
 - e.g., a corporation that pays \$100K a year to a critical technical person for a year of work and then pays him \$60K a year for the next ten years could reasonably be believed to have set up a system to help him avoid taxes on a large lump sum payment
 - + Asset-hiding, to avoid seizure in bankruptcies, lawsuits
 - + e.g., funds placed in accounts which are secret, or in systems/schemes over which the asset-hider has control of some kind (voting, consulting, etc.)
 - this is obscure: what I'm thinking of is some kind of deal in which Albert is hired by Bob as an "advisor" on financial matters: but Bob's money comes from Albert and so the quid pro quo is that Bob will take Albert's advice....hence the effective laundering and protection
 - + May also be used to create "multi-tier" currency systems, e.g., where reported transactions are some fraction of actuals
 - suppose we agree to deal at some artificially low value: electricians and plumbers may barter with each other at a reported \$5 an hour, while using underground accounts to actually trade at more realistic levels
 - + government (IRS) has laws about "fair value"-but how could these laws be enforced for such intangibles as software?
 - if I sell a software program for \$5000, can the government declare this to be over or underpriced?
 - likewise, if a plumber charges \$5 an hour, can the government, suspecting tax evasion, force him to charge more?
 - once again, the nature of taxation in our increasingly many-dimensioned economy seems to necessitate major invasions of privacy
- 16.14.7. "Denationalization of Money"
- as with the old SF standby of "credits"
 - + cf. the books on denationalization of money, and the idea of competing currencies
 - digital cash can be denominated in these various currencies, so it makes the idea of competing currencies more practical
 - to some extent, it already exists
 - + the hard money advocates (gold bugs) are losing their faith, as they see money moving around and never really landing in any "hard" form

- of course, it is essential that governments and groups not have the ability to print more money
- international networks will probably denominate transactions in whatever currencies are the most stable and least inflationary (or least unpredictably inflationary)

16.15. Intellectual Property

- 16.15.1. Concepts of property will have to change
 - intellectual property; enforcement is becoming problematic
 - when thieves cannot be caught
- 16.15.2. Intellectual property debate
 - include my comment about airwaves
 - + work on payment for items...Brad Cox, Peter Sprague, etc.
 - Superdistribution, metered usage
 - propertarian
 - many issues

16.16. Markets for Contract Killings, Extortion, etc.

- 16.16.1. Note: This is a sufficiently important topic that it deserves its own heading. There's material on this scattered around this document, material I'll collect together when I get a chance.
- 16.16.2. This topic came up several times on then Extropians mailing list, where David Friedman (author of "The Machinery of Freedom" and son of Nobel Prize winner Milton Friedman) and Robin Hanson debated this with me.
- 16.16.3. Doug Cutrell summarized the concerns of many when he wrote:
 - "...the availability of truly secure anonymity, strong encryption, and untraceable digital cash could allow contract killing to be an openly conducted business. For example, an anonymous news post announces a public key which is to be used to encode a contract kill order, along with a digital cash payment. The person placing the contract need only anonymously place the encrypted message in alt.test. Perhaps it is even possible to make it impossible to tell that the message was encrypted with the contract killer's public key (the killer would have to attempt decryption of all similarly encoded messages on alt.test, but that might be quite feasible). Thus it could be completely risk free for anyone to place a contract on anyone else." [Doug Cutrell, 1994-09-09]
- 16.16.4. Abhorrent markets
 - contract killings
 - can collect money anonymously to have someone whacked...nearly anyone who is controversial can generate enough "contributions"
 - kidnapping, extortion
- 16.16.5. Dealing with Such Things:
 - + never link physical ID with pseudonyms! (they won't kill you if they don't know who you are)
 - and even if one pseudonym is linked, make sure your financial records are not linkable
 - trust no one
 - increased physical security...make the effort of killing much more potentially dangerous
 - flooding attacks..tell extortionists to "get in line" behind all the other extortionists

- + announce to world that one does not pay extortionists...set up protocol to ensure this
- yes, some will die as a result of this
- console yourself with the fact that though some may die, fewer are dying as a result of state-sponsored wars and terrorism (historically a bigger killer than contract killings!)

16.17. Persistent Institutions

16.17.1. Strong crypto makes possible the creation of institutions which can persist for very long periods of time, perhaps for centuries.

- such institutions already exist: churches (Catholics of several orders), universities, etc.

16.17.2. all of these "persistent" services (digital banks, escrow services, reputation servers, etc.) require much better protections against service outages, seizures by governments, natural disasters, and even financial collapse than do most existing computer services—an opportunity for offshore escrow-like services

- to maintain a distributed database, with unconditional privacy, etc.
- + again, it is imperative that escrow companies require all material placed in it to be encrypted
- to protect them against lawsuits and claims by authorities (that they stole information, that they censored material, that they are an espionage conduit, etc.)

16.17.3. Escrow Services

- + "Digital Escrow" accounts for mutually suspicious parties, especially in illegal transactions
- drug deals, information brokering, inside information, etc.
- + But why will the escrow entity be trusted?
 - + reputations
 - their business is being a reliable escrow holder, not it destroying their reputation for a bribe or a threat
 - + anonymity means the escrow company won't know who it's "burning," should it try to do so
 - they never know when they themselves are being tested by some service
 - and potential bribers will not know who to contact, although mail could be addressed to the escrow company easily enough
- like bonding agencies
- key is that these entities stand to gain very little by stealing from their customers, and much to lose (hinges on ratio of any single transaction to size of total market)
- useful for black markets and illegal transactions (a reliable third party that both sides can trust, albeit not completely)

16.17.4. Reputation-Based Systems

- + Credit Rating Services that are Immune from Meddling and Lawsuits
- + with digital pseudonyms, true credit rating data bases can be developed

- with none of the "5 year expirations" (I mean, who are you to tell me I must not hold it against a person that records show he's declares Chapter 7 every 5 years or so?...such information is information, and cannot be declared illegal, despite the policy issues that are involved)
 - + this could probably be done today, using offshore data banks, but then there might develop injunctions against use by Stateside companies
 - how could this be enforced? stings? entrapment?
 - + it may be that credit-granting entities will be forced to use rigid formulas for their decisions, with a complete audit trail available to the applicant
 - if any "discretion" or judgment is allowed, then these extralegal or offshore inputs can be used
 - related to "redlining" and other informal signalling mechanisms
 - remember that Prop. 103 attempted to bypass normal laws of economics
 - + AMIX-like services will offer multiple approaches here
 - + ranging from conventional credit data bases, albeit with lower costs of entry (e.g., a private citizen could launch a "bankruptcy filings" data base, using public records, with no expiration-they're just reporting the truth, e.g., that Joe Blow filed for personal bankruptcy in 1987
 - this gets into some of the strange ideas involving mandatory rewriting of the truth, as when "credit records are expunged" (expunged from what? from my personal data bases? from records that were public and that I am now selling access to?)
 - + there may be arguments that the "public records" are copyrighted or otherwise owned by someone and hence cannot be sold
 - telephone book case (however, the Supremes held that the "creative act" was the specific arrangement)
 - one ploy may be a Habitat-like system, where some of the records are "historical"
 - to offshore data bases
 - + Book Reviews, Music Reviews
 - sometimes with pseudonyms to protect the authors from retaliation or even lawsuits
 - + "What should I buy?" services, a la Consumer Reports
 - again, protection from lawsuits
- 16.17.5. Crypto Banks and the "Shell Game" as a Central Metaphor
- + Central metaphor: the Shell Game
 - description of conventional shell game (and some allusions to con artists on a street corner-the hand is quicker than the eye)
 - + like entering a room filled with safe deposit boxes, with no surveillance and no way to monitor activity in the boxes....and user can buy new boxes anonymously, transferring contents amongst the boxes
 - only shutting down the entire system and forcing all the boxes open would do anything-and this would "pool"

- all of the contents (unless a law was passed saying people could "declare" the contents before some day....)
 - + the shell game system can be "tested"-by testing services, by suspicious individuals, whatever-at very low cost by dividing some sum amongst many accounts and verifying that the money is still there (by retrieving or cashing them in)
 - and remember that the accounts are anonymous and are indistinguishable, so that the money cannot be seized without repercussions
 - + this is of course the way banks and similar reputation-based institutions have always (or mostly) worked
 - people trusted the banks not to steal their money by verifying over some period of time that their money was not vanishing
 - and by relying upon some common sense ideas of what the bank's basic business was (the notion that a bank exists to continue in business and will make more money over some long run period by being trustworthy than it would make in a one-shot ripoff)
 - + Numbered accounts
 - recall that Switzerland has bowed to international pressure and is now limiting (or eliminating) numbered accounts (though other countries are still allowing some form of such accounts, especially Lichtenstein and Luxembourg)
 - + with crypto numbers, even more security
 - "you lose your number, tough"
 - but the money must exist in some form at some time?
 - + options for the physical form of the money
 - + accounts are shares in a fund that is publicly invested
 - shares act as "votes" for the distribution of proceeds
 - dividends are paid to the account (and sent wherever)
 - an abstract, unformed idea: multiple tiers of money, like unequal voting rights of stock...
 - + could even be physical deposits
 - perhaps even manipulated by automatic handling systems (though this is very insecure)
 - the Bennett-Ross proposal for Global Data Services is essentially the early form of this
- 16.17.6. cryonicists will seek "crypto-trusts" to protect their assets
- + again, the "crypto" part is not really necessary, given trustworthy lawyers and similar systems
 - but the crypto part-digital money-further automates the system, allowing smaller and more secure transactions (overhead is lower, allowing more dispersions and diffusion)
 - and eliminates the human link
 - thus protecting better against subpoenas, threats, etc.
 - + and to help fund "persistent institutions" that will fund research and protect them in suspension
 - they may also place their funds in "politically correct" longterm funds-which may or may not exert a positive influence in the direction they wish, what with the law of unintended consequences and all

opl

- + many avenues for laundering money for persistent institutions
 - + dummy corporations (or even real corporations)
 - with longterm consulting arrangements
 - "shell game" voting
- + as people begin to believe that they may just possibly be revived at some future time, they will begin to worry about protecting their current assets
- + recollections of "Why Call Them Back from Heaven?"
 - worries about financial stability, about confiscation of wealth, etc.
 - no longer will ersatz forms of immortality-endowments for museums, universities, etc.-be as acceptable...people will want the real thing
- + Investments that may outlive current institutions
 - purchases of art works (a la Bill Gates, who is in fact a possible model for this kind of behavior)
 - rights to famous works, with provision for the copyright expirations, etc. (which is why physical possession is preferable)
 - shell games, of course (networks of reputation-based accounts)
 - Jim Bennett reports that Saul Kent is setting up such things in Lichtenstein for Alcor (which is what I suggested to Keith Henson several years ago)

16.18. Organized Crime: Triads, Yakuza, Mafia, etc.

16.18.1. "The New Underworld Order"

- + Claire Sterling's "Thieve's World"
 - (Sterling is well-known for her conservative views on political matters, having written the controversial "The Terror Connection," which basically dismissed the role of the CIA and other U.S. agencies in promoting terrorism. "Thieve's World" continues the alarmist stance, but has some juicy details anyway.)
 - she argues for more law enforcement
- + but it was the corrupt police states of Nazi Germany, Soviet Russia, etc., that gave so many opportunities for modern corruption
 - and the CIA-etc. drug trade, Cold War excuses, and national security state waivers
- + in the FSU, the Russian Mafia is the chief beneficiary of privatization...only they had the cash and the connections to make the purchases (by threatening non-Mob bidders, by killing them, etc.)
 - as someone put in, the world's first complete criminal state

16.18.2. "Is the criminal world interested in crypto? Could they be early adopters of these advanced techniques?"

- early use: BBS/Compuserve messages, digital flash paper, codes
- money-laundering, anstalts, banks
- Triads, chop marks
- Even though this use seem inevitable, we should probably be careful here. Both because the clientele for our advice may be violent, and ditto for law enforcement. The conspiracy

- and RICO laws may be enough to get anyone who advises such folks into major trouble. (Of course, advice and consulting may happen through the very same untraceable technology!)
- 16.18.3. crypto provides some schemes for more secure drug distribution
- cells, dead drops, secure transfers to foreign accounts
 - communication via pools, or remailers
 - too much cash is usually the problem...
 - "follow the money" (FinCEN)
 - no moral qualms...nearly all drugs are less dangerous than alcohol is...that drug was just too popular to outlaw
 - this drug scenario is consistent with the Triad/Mob scenario
- 16.19. Privately Produced Law, Polycentric Law, Anarcho-Capitalism
- 16.19.1. "my house, my rules"
- 16.19.2. a la David Friedman
- 16.19.3. markets for laws, Law Merchant
- corporations, other organizations have their own local legal rules
 - Extropians had much debate on this, and various competing legal codes (as an experiment...not very successful, for various reasons)
 - "Snow Crash"
- 16.19.4. the Cypherpunks group is itself a good example:
- a few local rules (local to the group)
 - a few constraints by the host machine environment (toad, soda)
 - + but is the list run on "United States law"?
 - with members in dozens of countries?
 - only when the external laws are involved (if one of us threatened another, and even then this is iffy) could the external laws....
 - benign neglect, by necessity
- 16.19.5. I have absolutely no faith in the law when it comes to cyberspatial matters (other matters, too).
- especially vis-a-vis things like remote access to files, a la the AA BBS case
 - "the law is an ass"
 - patch one area, another breaks
 - What then? Technology. Remailers, encryption
- 16.19.6. Contracts and Cryptography
- + "How can contracts be enforced in crypto anarchy situations?"
 - A key question, and one which causes many people to question whether crypto anarchy can work at all.
 - + First, think of how many situations are already essentially outside the scope of the law...and yet in which something akin to "contracts" are enforceable, albeit not via the legal process.
 - friends, relationships
 - + personal preferences in food, books, movies, etc.
 - what "recourse" does one have in cases where a meal is unsatisfactory? Not going back to the restaurant is usually the best recourse (this is also a hint about the importance of "future expectation of business" as a means of dealing with such things).

- In these cases, the law is not directly involved. In fact, the law is not involved in most human (and nonhuman!) interactions.
 - + The Main Approaches:
 - + Reputations.
 - reputations are important, are not lightly to be regarded
 - Repeat Business.
 - Escrow Services.
 - + The "right of contract" (and the duty to adhere to them, to not try to change the contract after the facts) is a crucial building block.
 - Imagine a society in which contracts are valid. This allows those willing to sign contracts setting limits on malpractice to get cheaper health care, while those who won't sign such contracts are free to sue--but will of course have to pay more for health care. Nothing is free, and frivolous malpractice lawsuits have increased operating costs. (Recall the "psychic" who alleged that her psychic powers were lost after a CAT scan. A jury awarded her millions of dollars. Cf. Peter Huber's books on liability laws.)
 - Now imagine a society in which it is never clear if a contract is valid, or whether courts will overturn or amend a contract. This distorts the above analysis, and so hospitals, for example, have to build in safety margins and cushions.
 - + Crypto can help by creating escrow or bonding accounts held by third parties--untraceable to the other parties--which act as bonding agents for completion of contracts.
 - Such arrangements may not be allowed. For example, a hospital which attempted to deal with such a bonding agency, and which asked customers to also deal with them, could face sanctions.
 - "Secured credit cards" are a current example: a person pays a reserve amount greater than the card limits (maybe 110%). The reason for doing this is not to obtain "credit," obviously, but to be able to order items over the phone, or to avoid carrying cash. (The benefit is thus in the channel of commerce).
- 16.19.7. Ostracism, Banishment in Privately Produced Law
- + Voluntary and discretionary electronic communities also admit the easy possibility of banishment or ostracism (group-selected kill files). Of course, enforcement is generally difficult, e.g., there is nothing to stop individuals from continuing to communicate with the ostracized individual using secure methods.
 - I can imagine schemes in which software key escrow is used, but these seem overly complicated and intrusive.
 - The ability of individuals, and even subgroups, to thwart the ostracism is not at all a bad thing.
 -
 - "In an on-line world it would be much easier to enforce banishment or selective ostracism than in real life. Filtering agents could look for certificates from accepted enforcement agencies before letting messages through. Each user could have a set of agencies which were compatible

with his principles, and another set of "outlaws". You could even end up with the effect of multiple "logical subnets" of people who communicate with each other but not outside their subnet. Some nets might respect intellectual property, others not, and so on." [Hal Finney, 1994-08-21]

16.19.8. Governments, Cyberspaces, PPLs

- Debate periodically flares up on the List about this topic.
- Can't be covered here in sufficient detail.
- Friedman, Benson, Stephenson's "Snow Crash," etc.

16.19.9. No recourse in the courts with crypto-mediated systems

- insulated from the courts
- PPLs are essential
- reputations, escrow, mediation (crypto-mediated mediation?)

16.19.10. Fraud

- not exactly rare in the non-crypto world!
- new flavors of cons will likely arise
- anonymous escrow accounts, debate with Hal Finney on this issue, etc.

16.19.11. PPLs, polycentric law

16.20. Libertaria in Cyberspace

16.20.1. what it is

16.20.2. parallels to Oceania, Galt's Gulch

16.20.3. Privacy in communications alters the nature of connectivity

- virtual communities, invisible to outsiders
- truly a crypto cabal
- this is what frightens the lawmakers the most...people can opt out of the mainstream governmental system, at least partly (and probably increasingly)

16.21. Cyberspace, private spaces, enforcement of rules, and technology

16.21.1. Consider the "law" based approach

- a discussion group that wants no men involved ("a protected space for womyn")
- so they demand the civil law system enforce their rules
- practical example: sysadmins yank accounts when "inappropriate posts" are made
- the C&S case of spamming is an example
- Note: The Net as currently constituted is fraught with confusion about who owns what, about what are public and what are private resources, and about what things are allowed. If Joe Blow sends Suzy Creamcheese an "unwanted" letter, is this "abuse" or "harassment"? Is it stealing Suzy's resources? (In my opinion, of course not, but I agree that things are confusing.)

16.21.2. The technological approach:

- spaces created by crypto...unbreachable walls
- + example: a mailing list with controls on membership
- could require nomination and vouching for by others
- presentation of some credential (signed by someone), e.g. of femaleness
- pay as you go stops spamming

16.21.3. This is a concrete example of how crypto acts as a kind of building material

- and why government limitations on crypto hurt those who wish to protect their own spaces
- a private mailing list is a private space, inaccessible to

- those outside
- "There are good engineering approaches which can force data to behave itself. Many of them involve cryptography. Our government's restrictions on crypto limit our ability to build reliable computer systems. We need strong crypto for basic engineering reasons." [Kent Borg, "Arguing Crypto: The Engineering Approach," 1994-06-29]
- 16.21.4. Virtual Communities-the Use of Virtual Networks to Avoid Government
 - that is, alternatives to creating new countries (like the Minerva project)
 - the Assassin cult/sect in the mountains of Syria, Iraq, Afghanistan, etc. had a network of couriers in the mountain fastnesses
 - pirate communities, networks of trading posts and watering holes, exempt-if only for a few years-from the laws of the imperial powers
- 16.21.5. These private spaces will, as technology makes them more "livable" (I don't mean in a full sense, so don't send me notes about how "you can't eat cyberspace"), become full-functioned "spaces" that are outside the reach of governments. A new frontier, untouchable by outside, coercive governments.
 - Vinge's "True Names" made real
- 16.21.6. "Can things really develop in this "cyberspace" that so many of us talk about?"
 - "You can't eat cyberspace!" is the usual point made. I argue, however, that abstract worlds have always been with us, in the forms of commerce, reputations, friends, etc. And this will continue.
 - Some people have objected to the sometimes over-enthusiastic claims that economies and societies will flourish in computer-mediated cyberspaces. The short form of the objection is: "You can't eat cyberspace." Meaning, that profits and gains made in cyberspace must be converted to real world profits and gains.
 - In "Snow Crash," this was made out to be difficult...Hiro Protagonist was vastly wealthy in the Multiverse, but lived in a cargo container at LAX in the "real world." A fine novel, but this idea is screwy.
- + There are many ways to transfer wealth into the "real" world:
 - + all the various money-laundering schemes
 - money in offshore accounts, accessible for vacations, visits, etc.
 - phony purchase orders
 - my favorite: Cyberspace, Inc. hires one as a "consultant" (IRS cannot and does not demand proof of work being done, the nature of the work, one's qualifications to perform the work, etc....In fact, many consultants are hired "on retainer," merely to be available should a need arise.)
 - information-selling
 - investments
 -
- 16.21.7. Protocols for this are far from complete
 - money, identity, walls, structures

- a lot of basic work is needed (though people will pursue it locally, not after the work is done...so solutions will likely be emergent)

16.22. Data Havens

16.22.1. "What are data havens?"

- + Places where data can be hidden or protected against legal action.
 - Sterling, "Islands in the Net," 1988
- + Medical experiments, legal advice, pornography, weapons
 - reputations, lists of doctors, lawyers, rent deadbeats, credit records, private eyes
- What to do about the mounting pressure to ban certain kinds of research?
- One of the powerful uses of strong crypto is the creation of journals, web sites, mailing lists, etc., that are "untraceable." These are sometimes called "data havens," though that term, as used by Bruce Sterling in "Islands in the Net" (1988), tends to suggest specific places like the Cayman Islands that corporations might use to store data. I prefer the emphasis on "cypherspace."
- "It is worth noting that private "data havens" of all sorts abound, especially for financial matters, and most are not subject to governmental regulation....Some banks have research departments that are older and more comprehensive than credit reporting agencies. Favored customers can use them for evaluation of private deals....Large law firms maintain data banks that approach those of banks, and they grow with each case, through additions of private investigators paid for by successive clients....Security professionals, like Wackenhut and Kroll, also market the fruits of substantial data collections....To these add those of insurance, bonding, investment, financial firms and the like which help make or break business deals." [John Young, 1994-09-07]

16.22.2. "Can there be laws about what can be done with data?"

- Normative laws ("they shouldn't keep such records and hence we'll outlaw them") won't work in an era of strong crypto and privacy. In fact, some of us support data havens precisely to have records of, say, terminal diseases so we'll not lend money to Joe-who-has-AIDS. It may not be "fair" to Joe, but it's my money. (Same idea as in using offshore or cryptospacial data havens to bypass the nonsense in the "Fair Credit Reporting Act" that outlaws the keeping of certain kinds of facts about credit applicants, such as that they declared bankruptcy 10 years ago or that they left a string of bad debts in Germany in the 1970s, etc.)

16.22.3. Underground Networks, Bootleg Research, and Information Smuggling

- + The Sharing of Forbidden Knowledge
 - even if the knowledge is not actually forbidden, many people relish the idea of trafficking in the forbidden
- + Some modern examples
 - + drugs and marijuana cultivation
 - drugs for life extension, AIDS treatments
 - illegal drugs for recreational use

- + bootleg medical research, AIDS and cancer treatments, etc.
 - for example, self-help user groups that advise on treatments, alternatives, etc.
- + lockpicking and similar security circumvention techniques
 - recall that possession of lockpicks may be illegal
 - what about manuals? (note that most catalogs have a disclaimer: "These materials are for educational purposes only, ...")
- defense-related issues: limitations on debate on national security matters may result in "anonymous forums"
- + BTW, recent work on crab shells and other hard shells has produced even stronger armor!
 - this might be some of the genetic research that is highly classified and is sold on the anonymous nets
- + Alchemists and the search for immortality
 - + theory that the "Grandfather of all cults" (my term) started around 4500 B.C.
 - in both Egypt and Babylonia/Sumeria
 - + ancestor of Gnostics, Sufis, Illuminati, etc.
 - The Sufi mystic Gurdjieff claimed he was a member of a mystical cult formed in Babylon about 4500 B.C.
 - spider venom?
- + Speculation: a group or cult oriented toward life extension, toward the search for immortality-perhaps a link to The Epic of Gilgamesh.
 - + The Gilgamesh legend
 - Gilgamesh, Akkadian language stone tablets in Nineveh
 - made a journey to find Utnapishtim, survivor of Babylonian flood and possessor of secret of immortality (a plant that would renew youth)
 - but Gilgamesh lost the plant to a serpent
 - + Egyptians
 - obviously the Egyptians had a major interest in life extension and/or immortality
 - + Osiris, God of Resurrection and Eternal Life
 - also the Dark Companion of Sirius (believed to be a neutron star?)
 - they devoted huge fraction of wealth to pyramids, embalming, etc. (myrrh or frankincense from desert city in modern Oman, discovered with shuttle imaging radar)
 - + "pyramid power": role on Great Seal, as sign of Illuminati, and of theories about cosmic energy, geometrical shapes, etc.
 - and recall work on numerological significance of Great Pyramid dimensions
-
- + Early Christianity
 - focus on resurrection of Jesus Christ
- + Quest for immortality is a major character motivation or theme
 - + arguably for all people: via children,

- themselves, to create networks (thus creating de facto allies of the libertarian-oriented users)
- + Organ Banks
 - + establishing a profit motive for organ donors
 - may be the only way to generate enough donations, even from the dead
 - some plans are being made for such motives, especially to motivate the families of dying patients
 - ethical issues
 - + what about harvesting from the still-living?
 - libertarians would say: OK, if informed consent was given
 - the rich can go to overseas clinics
- + AIDS patients uniting via bulletin boards to share treatment ideas, self-help, etc.
 - with buying trips to Mexico and elsewhere
 - authorities will try to halt such BBSs (on what grounds, if no money is changing hands?)
- + Doctors may participate in underground research networks to protect their own reputations and professional status
 - to evade AMA or other professional organizations and their restrictive codes of ethics
 - + or lawsuits and bad publicity
 - some groups, the "Guardian Angels" of the future, seek to expose those who they think are committing crimes: abortionists (even though legal), etc.
 - "politically incorrect" research, such as vitamin therapy, longevity research, cryonics
 - breast implant surgery may be forced into black markets (and perhaps doctors who later discover evidence of such operations may be forced to report such operations)
- + Back Issues of Tests and Libraries of Term Papers
 - already extant, but imagine with an AMIX-like frontend?
- + Different kinds of networks will emerge, not all of them equally accessible
 - + the equivalent of the arms and drug networks-one does not gain entree merely by asking around a bit
 - credibility, reputation, "making your bones"
 - these networks are not open to the casual person
- + Some Networks May Be For the Support of Overseas Researchers
 - + who face restrictions on their research
 - e.g., countries that ban birth control may forbid researchers from communication with other researchers
 - + suppose U.S. researchers are threatened with sanctions-loss of their licenses, censure, even prosecution-if they participate in RU-486 experiments?
 - recall the AIDS drug bootleg trials in SF, c. 1990
 - or to bypass export restrictions
 - scenario: several anonymous bulletin boards are set up-and then closed down by the authorities-to facilitate anonymous hookups (much like "anonymous FTP")
- + Groups faced with debilitating lawsuits will "go underground"
 - Act Up! and Earth First! have no identifiable central office that can be sued, shut down, etc.

- and Operation Rescue has done the same thing

16.22.4. Illegal Data

- credit histories that violate some current law about records
- bootleg medical research
- stolen data (e.g., from competitors....a GDS system could allow remote queries of a database, almost "oracular," without the stolen data being in a U.S. jurisdiction)
- customers in the U.K or Sweden that are forbidden to compile data bases on individuals may choose to store the data offshore and then access it discreetly (another reason encryption and ZKIPS must be offered)

16.22.5. "the Switzerland of data"

- Brussels supposedly raises fewer eyebrows than Lichtenstein, Luxembourg, Switzerland, etc.
- Cayman Islands, other small nations see possibilities

16.22.6. Information markets may have to move offshore, due to licensing and other restrictions

- just as stock brokers and insurance brokers are licensed, the government may insist that information resellers be licensed (pass exams, be subject to audits and regulations)

16.23. Undermining Governments--Collapse of the State

16.23.1. "Is it legal to advocate the overthrow of governments or the breaking of laws?"

- Although many Cypherpunks are not radicals, many others of us are, and we often advocate "collapse of governments" and other such things as money laundering schemes, tax evasion, new methods for espionage, information markets, data havens, etc. This raises obvious concerns about legality.
- First off, I have to speak mainly of U.S. issues...the laws of Russia or Japan or whatever may be completely different. Sorry for the U.S.-centric focus of this FAQ, but that's the way it is. The Net started here, and still is dominantly here, and the laws of the U.S. are being propagated around the world as part of the New World Order and the collapse of the other superpower.
- Is it legal to advocate the replacement of a government? In the U.S., it's the basic political process (though cynics might argue that both parties represent the same governing philosophy). Advocating the *violent overthrow* of the U.S. government is apparently illegal, though I lack a cite on this.

+ Is it legal to advocate illegal acts in general? Certainly much of free speech is precisely this: arguing for drug use, for boycotts, etc.

+ The EFF gopher site has this on "Advocating Lawbreaking, Brandenburg v. Ohio. ":

- "In the 1969 case of Brandenburg v. Ohio, the Supreme Court struck down the conviction of a Ku Klux Klan member under a criminal syndicalism law and established a new standard: Speech may not be suppressed or punished unless it is intended to produce 'imminent lawless action' and it is 'likely to produce such action.' Otherwise, the First Amendment protects even speech that advocates violence. The Brandenburg test is the law today. "

16.23.2. Espionage and Subversion of Governments Will be Revolutionized by Strong Crypto

- (I think they see what we see, too, and this is a motivation for the attempts to limit the use of strong crypto. Besides some of the more conventional reasons.)
- + Digital dead drops will revolutionize espionage
 - + spies and their controllers can communicate securely, relatively quickly, without fear of being watched, their drops compromised, etc.
 - no more nooks of trees, no more chalk marks on mailboxes to signal a drop to be made
- + this must be freaking out the intelligence community!
 - more insights into why the opposition to crypto is so strong
- + Cell-Based Systems and Conventional Protection Systems
 - + Cells are a standard way to limit the damage of exposure
 - the standard is the 3-person cell so common in the early days of Soviet espionage in the U.S.
 - but computer systems may allow new kinds of cells, with more complicated protocols and more security
- + Keeping files for protection is another standard protection method
 - + and with strong crypto, these files can be kept encrypted and in locations not apparent (e.g., posted on bulletin boards or other such places, with only the key needed at a later time to open them)
 - a la the "binary files" idea, wherein encrypted files are widely available for some time before the key is distributed (thus making it very hard for governments to halt the distribution of the raw files)

16.23.3. "Xth Column" (X = encrypted)

- The possible need to use strong cryptography as a tool to fight the state.
- + helping to undermine the state by using whistleblowers and anonymous information markets to leak information
 - the 63,451 people given false identities in the WitSec program...leak their names, watch them be zapped by vengeful enemies, and watch the government squirm
 - auction off the details of the 1967 Inspector General's report on CIA assassinations

16.23.4. use of clandestine, cell-based systems may allow a small group to use "termite" methods to undermine a society, to destroy a state that has become too repressive (sounds like the U.S. to me)

- encrypted systems, anonymous pools, etc., allow truly secure cell-based systems (this is, by the way, one of the concerns many countries have about "allowing" cryptography to be used...and they're right about the danger!)
- subversion of fascist or socialist governments, undermining the so-called democratic governments

16.23.5. "Why won't government simply ban such encryption methods?"

- + This has always been the Number One Issue!
 - raised by Stiegler, Drexler, Salin, and several others (and in fact raised by some as an objection to my even discussing these issues, namely, that action may then be taken to head off the world I describe)
- + Types of Bans on Encryption and Secrecy

- Ban on Private Use of Encryption
- Ban on Store-and-Forward Nodes
- Ban on Tokens and ZKIPS Authentication
- Requirement for public disclosure of all transactions
- + Recent news (3-6-92, same day as Michaelangelo and Lawnmower Man) that government is proposing a surcharge on telcos and long distance services to pay for new equipment needed to tap phones!
 - S.266 and related bills
 - this was argued in terms of stopping drug dealers and other criminals
 - but how does the government intend to deal with the various forms of end-user encryption or "confusion" (the confusion that will come from compression, packetizing, simple file encryption, etc.)
- + Types of Arguments Against Such Bans
 - The "Constitutional Rights" Arguments
 - + The "It's Too Late" Arguments
 - PCs are already widely scattered, running dozens of compression and encryption programs...it is far too late to insist on "in the clear" broadcasts, whatever those may be (is program code distinguishable from encrypted messages? No.)
 - encrypted faxes, modem scramblers (albeit with some restrictions)
 - wireless LANs, packets, radio, IR, compressed text and images, etc....all will defeat any efforts short of police state intervention (which may still happen)
 - + The "Feud Within the NSA" Arguments
 - COMSEC vs. PROD
 - + Will affect the privacy rights of corporations
 - and there is much evidence that corporations are in fact being spied upon, by foreign governments, by the NSA, etc.
 - + They Will Try to Ban Such Encryption Techniques
 - + Stings (perhaps using viruses and logic bombs)
 - or "barium," to trace the code
 - + Legal liability for companies that allow employees to use such methods
 - perhaps even in their own time, via the assumption that employees who use illegal software methods in their own time are perhaps couriers or agents for their corporations (a tenuous point)
- 16.23.6. "How will the masses be converted?"
 - Probably they won't. Things will just happen, just as the masses were not converted on issues of world financial markets, derivative instruments, and a lot of similar things.
 - Crypto anarchy is largely a personal approach of withdrawal, of avoidance. Mass consensus is not needed (unless the police state option is tried).
 - Don't think in terms of selling crypto anarchy to Joe Average. Just use it.
- 16.23.7. As things seem to be getting worse, vis-a-vis the creation of a police state in the U.S.--it may be a good thing that anonymous assassination markets will be possible. It may help to level the playing field, as the Feds have had their

hit teams for many years (along with their safe houses, forged credentials, accommodation addresses, cut-outs, and other accouterments of the intelligence state).

- (I won't get into conspiracies here, but the following terms may trigger some memories: Gehlen Org, Wackenhut, McKee Team, Danny Casolaro, Cabazon Indians, Gander crash, Iraq arms deals, Pan Am 103, Bridegrooms of Death, French Connection, Fascist Third Position, Phoenix Program, Bebe Rebozo, Marex, Otto Skorzeny, Nixon, P-2, Klaus Barbie, etc.)
- Plenty of evidence of misbehavior on a massive scales by the intelligence agencies, the police forces, and states in general. Absolute power has corrupted absolutely.
- I'm certainly not advocating the killing of Congressrodents and other bureaucrats, just noting that this cloud may have a silver lining.

16.24. Escrow Agents and Reputations

16.24.1. Escrow Agents as a way to deal with contract renegeing

- On-line clearing has the possible danger implicit in all trades that Alice will hand over the money, Bob will verify that it has cleared into his account (in older terms, Bob would await word that his Swiss bank account has just been credited), and then Bob will fail to complete his end of the bargain. If the transaction is truly anonymous, over computer lines, then of course Bob just hangs up his modem and the connection is broken. This situation is as old as time, and has always involved protocols in which trust, repeat business, etc., are factors. Or escrow agents.
- Long before the "key escrow" of Clipper, true escrow was planned. Escrow as in escrow agents. Or bonding agents.
- Alice and Bob want to conduct a transaction. Neither trusts the other; indeed, they are unknown to each other. In steps "Esther's Escrow Service." She is also utraceable, but has established a digitally-signed presence and a good reputation for fairness. Her business is in being an escrow agent, like a bonding agency, not in "burning" either party. (The math of this is interesting: as long as the profits to be gained from any small set of transactions is less than her "reputation capital," it is in her interest to forego the profits from burning and be honest. It is also possible to arrange that Esther cannot profit from burning either Alice or Bob or both of them, e.g., by suitably encrypting the escrowed stuff.)
- Alice can put her part of the transaction into escrow with Esther, Bob can do the same, and then Esther can release the items to the parties when conditions are met, when both parties agree, when adjudication of some sort occurs, etc. (There a dozen issues here, of course, about how disputes are settled, about how parties satisfy themselves that Esther has the items she says she has, etc.)

16.24.2. Use of escrow services as a substute for government

- + as in underworld deals, international deals, etc.
 - "Machinery of Freedom" (Friedman), "The Enterprise of Law" (Benson)
- "It is important to note in any case that the use of third-

party escrow as a substitute for Government regulation was a feature of the Northern European semi-anarchies of Iceland and Ireland that have informed modern libertarian thought." [Duncan Frissell, 1994-08-30]

- 16.24.3. Several people have raised the issue of someone in an anonymous transaction simply taking the money and not performing the service (or the flip side). This is where intermediaries come into the picture, just as in the real world (bonds, escrow agents, etc.).
- 16.24.4. Alice and Bob wish to conduct an anonymous transaction; each is unknown to the other (no physical knowledge, no pseudonym reputation knowledge). These "mutually suspicious agents," in 1960s- and 70s-era computer science lingo, must arrange methods to conduct business while not trusting the other.
- 16.24.5. Various cryptographic protocols have been developed for such things as "bit commitment" (useful in playing poker over the phone, for example). I don't know of progress made at the granularity of anonymous transactions, though. (Though the cryptographic protocol building blocks at lower levels--such as bit commitment and blobs--will presumably be used eventually at higher levels, in markets.)
- 16.24.6. I believe there is evidence we can shorten the cycle by borrowing noncryptographic protocols (heresy to purists!) and adapting them. Reputations, for example. And escrow agents (a form of reputation, in that the "value" of a bonding entity or escrow agent lies in reputation capital).
- 16.24.7. if a single escrow agent is suspected of being untrustworthy (in a reputation capital sense), then can use multiple escrows
 - with various protocols, caveat emptor
 - n-out-of-m voting schemes, where n escrow agents out of m are required to complete a transaction
 - hard to compromise them all, especially if they have no idea whether they are being "legitimately bribed" or merely pinged by a reputation-rating service
 - Hunch: the work of Chaum, Bos, and the Pfaltzmanns on DC-nets may be directly applicable here...issues of collusion, sets of colluders, detection of collusion, etc.

16.25. Predictions vs. Implications

- 16.25.1. "How do we know that crypto anarchy will 'work,' that the right institutions will emerge, that wrongs will be righted, etc.?"
 - We don't know. Few things are certain. Only time will tell. These are emergent situations, where evolution will determine the outcome. As in other areas, the forms of solutions will take time to evolve.
 - (The Founders could not have predicted the form corporate law would take, as but one example.)
- 16.25.2. My thinking on crypto anarchy is not so much prediction as examination of trends and the implications of certain things. Just as steel girders mean certain things for the design of buildings, so too does unbreakable crypto mean certain things for the design of social and economic systems.
- 16.25.3. Several technologies are involved:
 - Unbreakable crypto
 - Untraceable communication

- Unforgeable signatures
- 16.25.4. (Note: Yes, it's sometimes dangerous to say "unbreakable," "untraceable," and "unforgeable." Purists eschew such terms. All crypto is economics, even information-theoretically secure crypto (e.g., bribe someone to give you the key, break in and steal it, etc.). And computationally-secure crypto--such as RSA, IDEA, etc.--can in **principle** be brute-forced. In reality, the costs may well be exorbitantly high...perhaps more energy than is available in the entire universe would be needed. Essentially, these things are about as unbreakable, untraceable, and unforgeable as one can imagine.)
- 16.25.5. "Strong building materials" implies certain things. Highways, bridges, jet engines, etc. Likewise for strong crypto, though the exact form of the things that get built is still unknown. But pretty clearly some amazing new structures will be built this way.
- 16.25.6. Cyberspace, walls, bricks and mortar...
- 16.25.7. "Will strong crypto have the main effect of securing current freedoms, or will it create new freedoms and new situations?"
 - There's a camp that believe mainly that strong crypto will ensure that current freedoms are preserved, but that this will not change things materially, Communications can be private, diaries can be secured, computer security will be enhanced, etc.
 - Another camp--of which I am a vocal spokesman--believes that qualitatively different types of transactions will be made possible. In addition, of course, to the securing of liberties that the first camp things is the main effect.
 - + These effects are speculative, but probably include:
 - increased hiding of assets through untraceable banking systems
 - markets in illegal services
 - increased espionage
 - data havens
- 16.25.8. "Will all crypto-anarchic transactions be anonymous?"
 - No, various parties will negotiate different arrangements. All a matter of economics, of enforcement of terms, etc. Some will, some won't. The key thing is that the decision to reveal identity will be just another mutually negotiated matter. (Think of spending cash in a store. The store owner may want to know who his customers are, but he'll still take cash and remain ignorant in most cases. Unless a government steps in and distorts the market by requiring approvals for purchases and records of identities--think of guns here.)
 - For example, the local Mob may not lend me money if I am anonymous to them, but they have a "hook" in me if they know who I am. (Aspects of anonymity may still be used, such as systems that leave no paper or computer trail pointing to them or to me, to avoid stings.)
 - "Enforcement" in underground markets, for which the conventional legal remedies are impossible, is often by means of physical force: breaking legs and even killing welschers.
 - (Personally, I have no problems with this. The Mob cannot turn to the local police, so it has to enforce deals its

own way. If you can't pay, don't play.)

16.26. How Crypto Anarchy Will Be Fought

16.26.1. The Direct Attack: Restrictions on Encryption

- + "Why won't government simply ban such encryption methods?"
- + This has always been the Number One Issue!
 - raised by Stiegler, Drexler, Salin, and several others (and in fact raised by some as an objection to my even discussing these issues, namely, that action may then be taken to head off the world I describe)
- + Types of Bans on Encryption and Secrecy
 - Ban on Private Use of Encryption
 - Ban on Store-and-Forward Nodes
 - Ban on Tokens and ZKIPS Authentication
 - Requirement for public disclosure of all transactions
- + Recent news (3-6-92, same day as Michaelangelo and Lawnmower Man) that government is proposing a surcharge on telcos and long distance services to pay for new equipment needed to tap phones!
 - S.266 and related bills
 - this was argued in terms of stopping drug dealers and other criminals
 - but how does the government intend to deal with the various forms of end-user encryption or "confusion" (the confusion that will come from compression, packetizing, simple file encryption, etc.)
- + Types of Arguments Against Such Bans
 - The "Constitutional Rights" Arguments
 - + The "It's Too Late" Arguments
 - PCs are already widely scattered, running dozens of compression and encryption programs...it is far too late to insist on "in the clear" broadcasts, whatever those may be (is program code distinguishable from encrypted messages? No.)
 - encrypted faxes, modem scramblers (albeit with some restrictions)
 - wireless LANs, packets, radio, IR, compressed text and images, etc....all will defeat any efforts short of police state intervention (which may still happen)
 - + The "Feud Within the NSA" Arguments
 - COMSEC vs. PROD
 - + Will affect the privacy rights of corporations
 - and there is much evidence that corporations are in fact being spied upon, by foreign governments, by the NSA, etc.
- + They Will Try to Ban Such Encryption Techniques
- + Stings (perhaps using viruses and logic bombs)
 - or "barium," to trace the code
- + Legal liability for companies that allow employees to use such methods
 - perhaps even in their own time, via the assumption that employees who use illegal software methods in their own time are perhaps couriers or agents for their corporations (a tenuous point)
- restrictions on: use of codes and ciphers
- + there have long been certain restrictions on the use of encryption

- encryption over radio waves is illegal (unless the key is provided to the government, as with Morse code)
- + in war time, many restrictions (by all governments)
 - those who encrypt are ipso facto guilty and are shot summarily, in many places
 - even today, use of encryption near a military base or within a defense contractor could violate laws
- + S.266 and similar bills to mandate "trapdoors"
- + except that this will be difficult to police and even to detect
 - so many ways to hide messages
 - so much ordinary compression, checksumming, etc.
- + Key Registration Trail Balloon
 - cite Denning's proposal, and my own postings
- 16.26.2. Another Direct Attack: Elimination of Cash
 - + the idea being that elimination of cash, with credit cards replacing cash, will reduce black markets
 - "one person, one ID" (goal of many international standards organizations)
 - this elimination of cash may ultimately be tied in to the key registration ideas...government becomes a third party in all transactions
 - + a favorite of conspiracy theorists
 - in extreme form: the number of the Beast tattooed on us (credit numbers, etc.)
 - currency exchanges (rumors on the Nets about the imminent recall of banknotes, ostensibly to flush out ill-gotten gains and make counterfeiting easier)
 - + but also something governments like to do at times, sort of to remind us who's really in charge
 - Germany, a couple of times
 - France, in the late 1950s
 - various other devaluations and currency reforms
 - + Partial steps have already been made
 - cash transactions greater than some value-\$10,000 at this time, though "suspicious" sub-\$10K transactions must be reported-are banned
 - + large denomination bills have been withdrawn from circulation
 - used in drug deals, the argument goes
 - Massachusetts has demanded that banks turn over all account records, SS numbers, balances, etc.
 - + "If what you're doing is legal, why do you need cash for it?"
 - part of the old American dichotomy: privacy versus "What have you got to hide?"
 - + But why the outlawing of cash won't work
 - + if a need exists, black markets will arise
 - i.e., the normal tradeoff between risk and reward: there may be some "discounts" on the value, but cash will still circulate
 - + too many other channels exist: securities, secrets, goods
 - + from trading in gold or silver, neither of which are outlawed any longer, to trading in secrets, how can the government stop this?
 - art being used to transfer money across international borders (avoids Customs)

- "consideration" given, a la the scam to hide income
- + total surveillance?
- it doesn't even work in Russia
- on the other hand, Russia lacks the "point of sale" infrastructure to enforce a cashless system

16.26.3. Another Direct Attack: Government Control of Encryption, Networks, and Net Access

- a la the old Bell System monopoly, which limited what could be hooked up to a phone line
- + the government may take control of the networks in several ways:
 - + FCC-type restrictions, though it is hard to see how a private network, on private property, could be restricted
 - as it is not using part of the "public spectrum"
 - but it is hard to build a very interesting network that stays on private property....and as soon as it crosses public property, BINGO!
 - + "National Data Highway" could be so heavily subsidized that alternatives will languish (for a while)
 - the Al Gore proposals for a federally funded system (and his wife, Tipper, is of course a leader of the censorship wing)
 - and then the government can claim the right and duty to set the "traffic" laws: protocols, types of encryption allowed, etc.
 - key patents, a la RSA (if in fact gov't. is a silent partner in RSA Data Security)

16.26.4. An Indirect Attack: Insisting that all economic transactions be "disclosed" (the "Full Disclosure Society" scenario)

- + this sounds Orwellian, but the obvious precedent is that businesses must keep records of all financial transactions (and even some other records, to see if they're colluding or manipulating something)
 - for income and sales tax reasons
 - and OSHA inspections, INS raids, etc.
- + there is currently no requirement that all transactions be fully documented with the identities of all parties, except in some cases like firearms purchases, but this could change
 - especially as electronic transactions become more common: the IRS may someday insist on such records, perhaps even insisting on escrowing of such records, or time-stamping
- + this will hurt small businesses, due to the entry cost and overhead of such systems, but big businesses will probably support it (after some grumbling)
 - big business always sees bureaucracy as one of their competitive advantages
- + and individuals have not been hassled by the IRS on minor personal transactions, though the web is tightening:
 - 1099s are often required (when payments exceed some amount, such as \$500)
 - small scale barter transactions
- + but the nature of CA is that many transactions can be financial while appearing to be something else (like the transfer of music or images, or even the writing of letters)

- which is why a cusp is coming: full disclosure is one route, protection of privacy is another
 - + the government may cite the dangers of a "good old boy network" (literally) that promulgates racist, sexist, and ableist discrimination via computer networks
 - i.e., that the new networks are "under-representing people of color"
 - and how can quotas be enforced in an anonymous system?
 - proposals in California (7-92) that consultants file monthly tax statements, have tax withheld, etc.
 - a strategy for the IRS: require all computer network users to have a "taxpayer ID number" for all transactions, so that tax evasion can be checked
- 16.26.5. Attempts to discredit reputation-based systems by deceit, fraud, nonpayment, etc.
- deliberate attacks on the reputation of services the government doesn't want to see
 - there may be government operations to sabotage businesses, to undermine such efforts before they get started
 - analogous to "mail-bombing" an anonymous remailer
- 16.26.6. Licensing of software developers may be one method used to try to control the spread of anonymous systems and information markets
- by requiring a "business license" attached to any and all chunks of code
 - + implemented via digital signatures, a la the code signing protocols mentioned by Bob Baldwin as a means of reducing trapdoors, sabotage, and other modifications by spies, hackers, etc.
 - proposals to require all chunks of code to be signed, after the Silicon Valley case in mid-80s, where spy/saboteur went to several s/w companies and meddled with code
 - "seals" from some group such as "Software Writers Laboratories," with formal specs required, source code provided to a trusted keeper, etc.
 - + such licensing and inspection will also serve to lock-in the current players (Microsoft will love it) and make foreign competition in software more difficult
 - unless the foreign competition is "sanctioned," e.g., Microsoft opens a code facility in India
- 16.26.7. RICO-like seizures of computers and bulletin board systems
- sting operations and setups
 - Steve Jackson Games is obvious example
 - for illegal material (porno, drug advocacy, electronic money, etc.) flowing through their systems
 - even when sysop can prove he did not know illegal acts were being committed on his system (precedents are the yachts seized because a roach was found)
 - + these seizures can occur even when a trial is never held
 - e.g., the "administrative seizure" of cars in Portland in prostitution cases
 - and the seizures are on civil penalties, where the standards of proof are much lower
 - + in some cases a mere FBI investigation is enough to get employees fired, renters kicked out, IRS audits started
 - + reports that a woman in Georgia who posted some "ULs"

(unlisted numbers?) was fired by her company after the FBI got involved, told by her landlord that her lease was not being extended, and so forth

- "We don't truck with no spies"

- the IRS audit would not ostensibly be for harassment, but for "probable cause" (or whatever term they use) that tax avoidance, under-reporting, even money-laundering might be involved

16.26.8. Outlawing of Digital Pseudonyms and Credentialling

+ may echoe the misguided controversy over Caller ID

- misguided because the free market solution is clear: let those who wish to hide their numbers-rape and battering support numbers, police, detectives, or even just citizens requesting services or whatever-do so

- and let those who refuse to deal with these anonymous callers also do so (a simple enough programming of answering machines and telephones)

- for example, to prevent minors and felons from using the systems, "true names" may be required, with heavy fines and forfeitures of equipment and assets for anybody that fails to comply (or is caught in stings and setups)

+ minors may get screened out of parts of cyberspace by mandatory "age credentialing" ("carding")

- this could be a major threat to such free and open systems, as with the various flaps over minors logging on to the Internet and seeing X-rated images (however poorly rendered) or reading salacious material in alt.sex

- there may be some government mood to insist that only "true names" be used, to facillitate such age screening (Fiat-Shamir passports, papers, number of the Beast?)

+ the government may argue that digital pseudonyms are presumptively considered to be part of a conspiracy, a criminal enterprise, tax evasion, etc.

- the old "what have you got to hide" theory

- closely related to the issue of whether false IDs can be used even when no crimes are being committed (that is, can Joe Average represent himself by other than his True Name?)

- civil libertarians may fight this ban, arguing that Americans are not required to present "papers" to authorities unless under direct suspicion for a crime (never mind the loitering laws, which take the other view)

16.26.9. Anonymous systems may be restricted on the grounds that they constitute a public nuisance

- or that they promote crime, espionage, etc.

+ especially after a few well-publicized abuses

- possibly instigated by the government?

- operators may have to post bonds that effectively drive them out of business

16.26.10. Corporations may be effectively forbidden to hire consultants or subcontractors as individuals

+ the practical issue: the welter of tax and benefit laws make individuals unable to cope with the mountains of forms that have to be filed

- thus effectively pricing individuals out of this market

+ the tax law side: recall the change in status of

consultants a few years back...this may be extended further

- a strategy for the IRS: require all computer network users to have a "taxpayer ID number" for all transactions, so that tax evasion can be checked
 - not clear how this differs from the point above, but I feel certain more such pressures will be applied (after all, most corporations tend to see independent contractors as more of a negative than a positive)
 - this may be an agenda of the already established companies: they see consultants and free lancers as thieves and knaves, stealing their secrets and disseminating the crown jewels (to punningly mix some metaphors)
 - and since the networks discussed here facilitate the use of consultants, more grounds to limit them
- 16.26.11. There may be calls for U.N. control of the world banking system in the wake of the BCCI and similar scandals
- to "peirce the veil" on transnationals
 - calls for an end to banking secrecy
 - talk about denying access to the money centers of New York (but will this push the business offshore, in parallel to the Eurodollar market?)
- + motivations and methods
- recall the UNESCO attempt a few years back to credential reporters, ostensibly to prevent chaos and "unfair" reporting...well, the BCCI and nuclear arms deals surfacing may reinvigorate the efforts of "credentiallers"
- + the USSR and other countries entering the world community may sense an opportunity to get in on the formation of "boards of directors" of these kinds of banks and corporations and so may push the idea in the U.N.
- sort of like a World Bank or IMF with even more power to step in and take control of other banks, and with the East Bloc and USSR having seats!
- 16.26.12. "National security"
- if the situation gets serious enough, a la a full-blown crypto anarchy system, mightn't the government take the step of declaring a kind of national emergency?
 - provisions exist: "401 Emergency" and FEMA plans
 - of course, the USSR tried to intitiate emergency measures and failed
 - recall that a major goal of crypto anarchy is that the systems described here will be so widely deployed as to be essential or critical to the overall economy...any attempt to "pull the plug" will also kill the economy
- 16.26.13. Can authorities force the disclosure of a key?
- + on the "Yes" side:
- + is same, some say, as forcing combination to a safe containing information or stolen goods
 - but some say-and a court may have ruled on this-that the safe can always be cut open and so the issue is mostly moot
 - while forcing key disclosure is compelled testimony
 - and one can always claim to have forgotten the key
 - i.e., what happens when a suspect simply clams up?
 - but authorities can routinely demand cooperation in investigations, can seize records, etc.
- + on the "No" side:

- can't force a suspect to talk, whether about where he hid the loot or where his kidnap victim is hidden
- practically speaking, someone under indictment cannot be forced to reveal Swiss bank accounts....this would seem to be directly analogous to a cryptographic key
- thus, the key to open an account would seem to be the same thing
- a memorized key cannot be forced, says someone with EFF or CPSPR
- on balance, it seems clear that the disclosure of cryptographic keys cannot be forced (though the practical penalty for nondisclosure could be severe)
- but this has not really been tested, so far as I know
- and many people say that such cooperation can be demanded...

16.27. How Crypto Anarchy Advocates Will Fight Back

16.27.1. Bypassing restrictions on commercial encryption packages by not making them "commercial"

- public domain
- freely distributed
- after all, the basic algorithms are simple and don't really deserve patent protection: money will not be made by the originators of the code, but by the actual providers of services (for transmission and storage of packets)

16.27.2. Noise and signals are often indistinguishable

- as with the LSB audio signal approach...unless the government outlaws live recordings or dubs on digital systems...

16.27.3. Timed-release files (using encryption) will be used to hide files, to ensure that governments cannot remove material they don't like

- easier said than done

16.27.4. Legal approaches will also be taken: fundamental constitutional issues

- privacy, free speech, free association

16.27.5. The Master Plan to Fight Restrictions on Encryption

- + "Genie out of the bottle" strategy: deploy crypto widely
 - intertwined with religions, games, whistleblower groups, and other uses that cannot easily just be shut down
 - scattered in amongst many other activities
- Media attention: get media to report on value of encryption, privacy, etc.
- + Diffusion, confusion, and refusion
 - Diffuse the use by scattering it around
 - Confuse the issue by fake religions, games, other uses
 - Refuse to cooperate with the government
- Free speech arguments: calling the discussions free speech and forcing the government to prove that the free speech is actually an economic transaction
- + links with religions, corporations, etc.
 - private meetings protected
 - voting systems

16.28. Things that May Hide the Existence of Crypto Anarchy

16.28.1. first and foremost, the incredible bandwidth, the bits sloshing around the world's networks...tapes being exchanged,

PCs calling other PCs, a variety of data and compression formats, ISDN, wireless transmission, etc.

16.28.2. in the coming years, network traffic will jump a thousand-fold, what with digital fax, cellular phones and computers, ISDN, fiber optics, and higher-speed modems

- and these links will be of all kinds: local, private, corporate, business, commercial, bootleg (unrecorded), cellular radio, etc.

16.28.3. corporations and small groups will have their own private LANs and networks, with massive bandwidth, and with little prospects that the government can police them--there can be no law requiring that internal communications be readable by the government!

- and the revelations that Ultra Black has been used to read messages and use the information will be further proof to corporations that they need to adopt very strong security measures
- + and "partnerships" can be scattered across the country, and even internationally, and have great latitude in setting up their own communication and encryption systems
 - recall Cargill case
 - and also remember that the government may crack down on these systems

16.28.4. AMIX-like services, new services, virtual reality (for games, entertainment, or just as a place of doing business) etc.

- + many users will encrypt their links to VR servers, with a decryption agent at the other end, so that their activities (characters, fantasies, purchases, etc.) cannot be monitored and logged
- + this will further increase the bandwidth of encrypted data and will complicate further the work of the NSA and similar agencies
 - attempts to force "in the clear" links will be doomed by the welter of PC standards, compression utilities, cellular modems, and the like...there will be no "cleartext" that can be mandated

16.28.5. steganography

- + in general, impossible to know that a message contains other encrypted messages
 - except in stings and setups, which may be ruled illegal
- + the LSB method, and variants
 - + LSB of DAT, DCC, MD, etc., or even sound bites (chunks of sampled sounds traded on bulletin boards)
 - especially of live or analog-dubbed copies (the noise floor of a typical consumer-grade mike is much higher than the LSB of DAT)
 - + of images, Adobe Photoshop images, artwork, etc.
 - + imagine an "Online Art Gallery" that is used to store messages, or a "Photo Gallery" that participants post their best photos to, offering them for sale
 - Sturges case
 - LSB method
- + gets into some theoretical nitpicking about the true nature of noise, especially if the entire LSB channel is uncharacteristic of "real noise"
 - but by reducing the bandwidth somewhat, the noise profile can be made essentially undistinguishable from

- real noise
 - and a 2 GB DAT produces 130 MB of LSB, which is a lot of margin!
- + what could the government do?
 - stings and setups to catch and scare off potential users
 - an attempt to limit the wide use of digital data-hopeless!
- + a requirement for government-approved "dithering"?
 - this would be an enforcement nightmare
 - + and would only cause the system to be moved into higher bits
 - and with enough error correction, even audible dithering of the signal would not wipe out the encrypted signal
- + variants: text justification, word selection
 - bandwidth tends to be low
 - but used in Three Days of the Condor
- + virtual reality art may further enable private communications
 - think of what can be encrypted into such digital images!
 - and user has total privacy and is able to manipulate the images and databases locally
- 16.28.6. in the sense that these other things, such as the governments own networks of safe houses, false identities, and bootleg payoffs, will tend to hide any other such systems that emerge
 - + because investigators may think they've stumbled onto yet another intelligence operation, or sting, or whatever
 - this routinely cripples undercover investigations
 - scenario: criminals even float rumors that another agency is doing an operation....?
- 16.28.7. Government Operations that Resemble Cryptoanarchy will Confuse the Issues
 - various confidential networks already exist, operated by State, DoD, the services, etc.
 - + Witness Protection Program (or Witness Relocation Program)
 - false IDs, papers, transcripts
 - even money given to them (and the amounts seem to be downplayed in the press and on t.v., with a sudden spate of shows about how poorly they do in the middle of middle America-sounds like a planted story to me)
 - cooperation with certain companies and schools to assist in this aspect
 - + Payoffs of informants, unofficial agents
 - like agents in place inside defense contractors
 - vast amount of tips from freelancers, foreign citizens, etc.
 - operators of safe houses (like Mrs. Furbershaw)
 - + Networks of CIA-funded banks, for various purposes
 - a la the Nugan-Hand Bank, BCCI, etc.
 - First American, Bank of Atlanta, Centrust Savings, etc.
 - these banks and S&Ls act as conduits for controversial or secret operations, for temporary parking of funds, for the banking of profits, and even for the private retirement funds of agents (a winked-at practice)
 - + Confidential networks over computer lines
 - e.g., encrypted teleconferencing of Jasons, PFIAB, etc.

- + these will increase, for many reasons
 - concerns over terrorism
 - demands on time will limit travel (especially for groups of non-fulltime committee members)
- these suspected government operations will deter investigation
- 16.28.8. Encrypted Traffic Will Increase Dramatically
 - of all kinds
 - mail, images, proposals, faxes, etc.
 - acceptance of a P-K mail system will make wide use of encryption nearly automatic (though some fraction, perhaps the majority, will not even bother)
 - + there may even be legal reasons for encryption to increase:
 - requirements that employee records be protected, that medical records be protected, etc.
 - "prudent man" rules about the theft of information (could mean that files are to be encrypted except when being worked on)
 - digital signatures
 - echoes of the COMSEC vs. SIGINT (or PROD) debate, where COMSEC wants to see more encryption (to protect American industry against Soviet and commercial espionage)
 - + Selling of "Anonymous Mailers"?
 - using RSA
 - + avoiding RSA and the P-K patent morass
 - could sell packets of one-time pads
 - + no effective guarantee of security, but adequate for many simple purposes
 - + especially if buyers swap them with others
 - but how to ensure that copies are not kept?
 - idea is to enable a kind of "Democracy Wall"
 - + prepaid "coins," purchased anonymously
 - as with the Japanese phone cards
 - or the various toll booth electronic tokens being developed
- 16.28.9. Games, Religions, Legal Consultation, and Other "Covers" for the Introduction and Proliferation of Crypto Anarchy
 - won't be clear what is real encryption and what is game-playing
 - imagine a game called "Cryptoanarchy"!
 - + Comment on these "Covers"
 - some of these will be quite legitimate, others will be deliberately set up as covers for the spread of CA methods
 - perhaps subsidized just to increase traffic (and encrypted traffic is already expected to increase for a variety of reasons)
 - people will have various reasons for wanting anonymity
 - + Games
 - + "Habitat"-style games and systems
 - with "handles" that are much more secure than at present (recall Chip's comments)
 - + behaviors that are closely akin to real-world illegal behaviors:
 - a thieves area
 - an espionage game
 - a "democracy wall" in which anything can be posted

- anonymously, and read by all
- + MUDs (Multi-user Domains, Multi-User Dungeons)
 - lots of interest here
 - topic of discussion at a special Cypherpunks meeting, early 1994.
- + interactive role-playing games will provide cover for the spread of systems: pseudonyms will have much more protection than they now have
 - though various methods may exist to "tag" a transaction (a la barium), especially when lots of bandwidth is involved, for analysis (e.g., "Dark Dante" is identified by attaching specific bits to stream)
- + Dealing with Barium Tracers
 - code is allowed to simmer in an offsite machine for some time (and with twiddling of system clock)
 - mutations added
- + Shared Worlds
 - authors, artists, game-players, etc. may add to these worlds
 - hypertext links, reputation-based systems
- + hypothesize a "True Names" game on the nets, based explicitly on Vinge's work
 - perhaps from an outfit like Steve Jackson Games, maker of similar role-playing games
 - with variable-resolution graphics (a la Habitat)
 - virtual reality capabilities
- + a game like "Habitat" can be used as a virtual Labyrinth, further confusing the line between reality and fantasy
 - and this could provide a lot of bandwidth for cover
 - the Smalltalk "Cryptoids" idea is related to this...it looks like a simulation or a game, but can be used by "outsiders"
- + Religions
 - + a nearly ironclad system of liberties, though some limits exist
 - e.g., a church that uses its organization to transport drugs or run a gambling operation would be shut down quickly (recall the drug church?)
 - and calls for tax-break limitations (which Bill of Rights says nothing about)
 - still, it will be very difficult for the U.S. government to interfere with the communications of a "religion."
- + "ConfessionNet"
 - + a hypothetical anonymous system that allows confessions to be heard, with all of the privileges of privacy that normal confessions have
 - successors to 900 numbers?
 - + virtually ironclad protections against government interference
 - "Congress shall make no law..."
 - + but governments may try to restrict who can do this, a la the restrictions in the 70s and 80s on "instant Reverends"
 - Kirby J. Hensley's Universal Life Church
 - various IRS restrictions, effectively establishing two classes of religions: those grandfathered in and

- given tax breaks and the like, and those that were deemed invalid in some way
- + Scenario: A Scientology-like cult using CA as its chief communications system?
 - levels of initiation same as a cell system
 - "clearing"
 - New Age garbage: Ascended Masters, cells, money flowing back and forth
 - blackballing
- + Digital Personals
 - the "personals" section of newspapers currently requires the newspaper to provide the anonymity (until the parties mutually agree to meet)
 - what about on AMIX or similar services?
 - a fully digital system could allow self-arranging systems
- + here's how it could work:
 - Alice wants to meet a man. She writes up a typical ad, "SWF seeks SWM for fun and walks on the beach..."
 - Alice encloses her specially-selected public key, which is effectively her only name. This is probably a one-time deal, unlinkable to her in any way.
 - She encrypts the entire package and sends it through a remailing chain (or DC-Net) for eventual posting in a public place.
 - Everyone can download the relevant area (messages can be sorted by type, or organized in interest groups), with nobody else knowing which messages they're reading.
 - Bob reads her message and decides to repond. He digitizes a photo of himself and includes some other info, but not his real name. He also picks a public key for Alice to communicate with him.
 - Bob encrypts all of this with the public key of Alice (though remember that he has no way of knowing who she really is).
 - Bob sends this message through a remailing chain and it gets posted as an encrypted message addressed to the public key of Alice. Again, some organization can reduce the total bandwidth (e.g., an area for "Replies").
 - Alice scans the replies and downloads a group of messages that includes the one she can see-and only she can see!-is addressed to her.
 - This has established a two-way communication path between Alice and Bob without either of them knowing who the other one is or where they live. (The business about the photos is of course not conducive to anonymity, but is consistent with the "Personals" mode.)
 - If Alice and Bob wish to meet in person it is then easy for them to communicate real phone numbers and the like.
- + Why is this interesting?
 - it establishes a role for anonymous systems
 - it could increase the bandwidth of such messages
- + Legal Services (Legitimate, i.e., not even the bootleg stuff)

- + protected by attorney-client privileges, but various Bar Associations may place limits on the use of networks
 - but if viewed the way phones are, seems unlikely that Bars could do much to limit the use of computer networks
 - and suppose a Nolo Press-type publishing venture started up on the Nets? (publishing self-help info under pseudonyms)
 - or the scam to avoid taxes by incorporating as a corporation or nonprofit?
- + Voting Systems
 - with and without anonymity
 - + Board of Directors-type voting
 - with credentials, passwords, and (maybe) anonymity (under certain conditions)
 - + Blackballing and Memberships
 - generally anonymous
 - blackballing may be illegal these days (concerns about racism, sexism, etc.)
 - cf. Salomaa for discussion of indistinguishability of blackballing from majority voting
 - + Consumer Ratings and Evaluations
 - e.g., there may be "guaranteed anonymous" evaluation systems for software and other high-tech items (Joe Bluecollar won't mess with computers and complicated voting systems)
 - + Politically Active Groups May Have Anonymous Voting
 - to vote on group policies, procedures, leadership
 - or on boycott lists (recall the idea of the PC-Card that doesn't allow politically incorrect purchases)
 - + this may be to protect themselves from lawsuits (SLAPP) and government harassment
 - they fear government infiltrators will get the names of voters and how they voted
- + Official Elections
 - though this is unlikely for the barely-literate majority
 - the inevitable fraud cases will get wide exposure and scare people and politicians off even more
 - unlikely in next decade
- + Journal Refereeing
 - some journals, such as Journal of Cryptology, appropriately enough, are already using paper-based versions of this
 - + Xanadu-like systems may be early adopters
 - there are of course reasons for just the opposite: enhanced used of reputations
 - but in some cases anonymity may be preferred
- + Groupware
 - anonymous comment systems (picture a digital blackboard with anonymous remarks showing up)
 - these systems are promoted to encourage the quiet to have an equal voice
 - but they also provide another path to anonymous and/or reputation-based systems
- + Psychological Consultations
 - will require the licensing of counselors, of course

- (under U.S. laws)
- what if people call offshore counselors?
- + and various limitations on privacy of records exist
 - Tavisoff [spelling?]
 - subpoenas
 - record-keeping required
- + may be used by various "politically correct" groups
 - battered women
 - abused children
 - perhaps in conjunction with the RU-486-type issues, some common ground can be established (a new kind of Underground Railroad)
- + Advice on Medicine (a la AIDS, RU 486)
 - anonymity needed to protect against lawsuits and seizure
 - NOW and other feminist groups could use crypto anarchy methods to reduce the risks to their organizations
- + Anonymous Tip Lines, Whistleblower Services
 - + for example, a newspaper might set up a reward system, using the crypto equivalent of the "torn paper" key
 - where informant holds onto the torn off "key"
 - even something like the James Randi/Yuri Geller case reveals that "anonymous critics" may become more common
- + corporate and defense contractor whistleblowers may seek protection through crypto methods
 - a "Deep Throat" who uses bulletin boards to communicate with DS?
- + this presumes much wider use of computers and modems by "average" people...and I doubt "Prodigy"-type systems will support these activities!
 - but there may be cheap systems based on video game machines, a la the proposed Nintendo computers
- environmentalists set up these whistleblower lines, for people to report illegal logging, spraying, etc.
- + Online, "Instant" Corporations
 - + shell companies, duly incorporated in Delaware or wherever (perhaps even foreign sites) are "sold" to participants who wish to create a corporate cover for their activities
 - so that AMIX-like fees are part of the "internal accounting"
- + Anonymous collaborative writing and criticism
 - similar to anonymous voting
- 16.28.10. Compressed traffic will similarly increase
 - and many compression algorithms will offer some form of encryption as a freebie
 - and will be difficult to decypher, based just on sheer volume
 - files will have to at least be decompressed before key word searches can be done (though there may be shortcuts)
- 16.29. The Coming Phase Change
 - 16.29.1. "We'd better hope that strong cypto, cheap telecoms and free markets can provide the organizing basis for a workable society because it is clear that coercion as an organizing principle ain't what it used to be." [Duncan Frissell, in his sig, 4-13-94]
 - 16.29.2. "What is the "inevitability" argument?"

- Often made by me (Tim May), Duncan Frissell, Sandy Sandfort, and Perry Metzger (with some twists). And Hal Finney takes issue with certain aspects and contributes incisive critiques.
- + Reasons:
 - borders becoming more transparent to data flow
 - encryption is not detectable/stoppable
 - derivative financial instruments, money sloshing across borders
 - transnationalism
 - cash machines, wire transfers
 - "permanent tourists"
- Borders are becoming utterly transparent to massive data flows. The rapid export of crypto is but an ironic example of this. Mosaid, ftp, gopher, lynx...all cross borders fluidly and nearly untraceably. It is probably too late to stop these systems, short of "pulling the plug" on the Net, and this pulling the plug is simply too expensive to consider. (If the Feds ever really figure out the long-range implications of this stuff, they may try it...but probably not.)

16.29.3. "What is the "crypto phase change"?"

- I'm normally skeptical of claims that a "singularity" is coming (nanotechnology being the usual place this is claimed, a la Vinge), but "phase changes" are more plausible. The effect of cheap printing was one such phase change, altering the connectivity of society and the dispersion of knowledge in a way that can best be described as a phase change. The effects of strong crypto, and the related ideas of digital cash, anonymous markets, etc., are likely to be similar.
- transition
- tipping factors, disgust by populace, runaway taxation
- + "leverage effect"
 - what Kelly called "the fax effect"
 - crypto use spreads, made more popular by common use
- can nucleate in a small group...doesn't need mass acceptance

16.29.4. "Can crypto anarchy be stopped?"

- + A goal is to get crypto widely enough deployed that it cannot then be stopped
 - to the point of no return, where the cost of withdrawing or banning a technology is simply too high (not always a guarantee)
- The only recourse is a police state in which homes and businesses are randomly entered and searched, in which cryptography is outlawed and vigorously prosecuted, in which wiretaps, video surveillance, and other forms of surveillance are used aggressively, and in which perhaps the very possession of computers and modems is restricted.
- Anything short of these police state tactics will allow the development of the ideas discussed here. To some extent. But enough to trigger the transition to a mostly crypto anarchic situation.
- (This doesn't mean everyone, or even most, will use crypto anarchy.)

16.29.5. Need not be a universal or even popular trend

- even if restricted to a minority, can be very influential
 - George Soros, Quantum fund, central banks, Spain, Britain, Germany
 - and a minority trend can affect others
- 16.29.6. "National borders are just speedbumps on the digital superhighway."
- 16.29.7. "Does crypto anarchy have to be a mass movement to succeed?"
- Given that only a tiny fraction is now aware of the implications....
 - + Precedents for "vanguard" movements
 - + high finance in general is an elite thing
 - Eurodollars, interest rate swaps, etc....not exactly Joe Average...and yet of incredible importance (George Soros has affected European central bank policy)
 - smuggling is in general not a mass thing
 - etc.
 - + Thus, the users of crypto anarchic tools and instruments can have an effect out of proportion to their numbers
 - others will start to use
 - resentment by the "suckers" will build
 - the services themselves--the data havens, the credit registries, the espionage markets--will of course have a real effect
- 16.29.8. Strong crypto does not mean the end to law enforcement
- "...cryptography is not by any means a magic shield for criminals. It eliminates, perhaps, one avenue by which crimes might be discovered. However, it is most certainly not the case that someone who places an open anonymous contract for a murder in an open forum is doing so "risk free". There are *plenty* of ways she might be found out. Likewise, big secret societies that nefariously undermine the free world via cryptography are as vulnerable as ever to the motivations of their own members to expose the groups in a double-cross." [Mike McNally, 1994-09-09]
- 16.30. Loose Ends
- 16.30.1. governments may try to ban the use of encryption in any broadcast system, no matter how low the power, because of a realization that all of them can be used for crypto anarchy and espionage
- a losing battle, of course, what with wireless LANs of several flavors, cellular modems, the ability to hide information, and just the huge increase in bandwidth
- 16.30.2. "tontines"
- Eric Hughes wrote up some stuff on this in 1992 [try to get it]
 - Italian pseudo-insurance arrangements
 - "digital tontines"?
- 16.30.3. Even in market anarchies, there are times when a top-down, enforced set of behaviors is desirable. However, instead of being enforced by threat of violence, the market itself enforces a standard.
- For example, the Macintosh OS, with standardized commands that program developers are "encouraged" to use. Deviations are obviously allowed, but the market tends to punish such deviations. (This has been useful in avoiding modal software, where the same keystroke sequence might save a

file in one program and erase it in another. Sadly, the complexity of modern software has outpaced the Mac OS system, so that Command-Option Y often does different things in different programs.)

- Market standards are a noncoercive counter to total chaos.
- 16.30.4. Of course, nothing stops people from hiring financial advisors, lawyers, and even "Protectors" to shield them from the predations of others. Widows and orphans could choose conservative conservators, while young turks could choose to go it alone.
- 16.30.5. on who can tolerate crypto anarchy
 - Not much different here from how things have been in the past. Caveat emptor. Look out for Number One. Beware of snake oil.
- 16.30.6. Local enforcement of rules rather than global rules
 - + e.g., flooding of Usenet with advertising and chain letters
 - + two main approaches
 - ban such things, or set quotas, global acceptable use policies, etc. (or use tort law to prosecute & collect damages)
 - local carriers decide what they will and will not carry, and how much they'll charge
 - it's the old rationing vs. market pricing argument
- 16.30.7. Locality is a powerful concept
 - self-responsibility
 - who better to make decisions than those affected?
 - tighter feedback loops
 - avoids large-scale governments
 - + Nonlocally-arranged systems often result in calls to stop "hogging" of resources, and general rancor and envy
 - + water consumption is the best example: anybody seen "wasting" water, regardless of their conservations elsewhere or there priorities, is chastised and rebuked. Sometimes the water police are called.
 - the costs involved (perhaps a few pennies worth of water, to wash a car or water some roses) are often trivial...meanwhile, billions of acre-feet of water are sold far below cost to farmers who grow monsoon crops like rice in the California desert
 - this hypocrisy is high on my list of reasons why free markets are morally preferable to rationing-based systems

17. The Future

17.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

17.2. SUMMARY: The Future

17.2.1. Main Points

- where things are probably going

17.2.2. Connections to Other Sections

17.2.3. Where to Find Additional Information

17.2.4. Miscellaneous Comments

17.3. Progress Needed

17.3.1. "Why have most of the things Cypherpunks talk about *not* happened?"

- + Except for remailers and basic crypto, few of the main ideas talked about for so long have actually seen any kind of realization. There are many reasons:
 - A. Difficult to achieve. Both Karl Kleinpaste and Eric Hughes implemented simple first-generation remailers in a matter of days, but "digital cash" and "aptical foddering," for example, are not quite so straightforward. (I am of course not taking anything away from Kleinpaste, Hughes, Helsingius, Finney, etc., just noting that redirecting mail messages--and even implementing PGP and things like delay, batching, etc., into remailers--is a lot easier conceptually than DC-Nets and the like.
 - B. Protocols are confusing, tough to implement. Only a tiny fraction of the "crypto primitives" discussed at Crypto Conferences, or in the various crypto books, have been realized as runnable code. Building blocks like "bit commitment" have not even--to my knowledge--been adequately realized as reusable code. (Certainly various groups, such as Chaum's, have cobbled-together things like bit commitment....I just don't think there's a consensus as to the form, and this has limited the ability of nonspecialists to use these "objects.")
 - C. Semantic confusion as well. While it's fairly clear what "encrypting" or "remailing" means, just what is a "digital bank"? Or a "reputation server"?
 - D. Interoperability is problematic. Many platforms, many operating systems, many languages. Again, remailers and encryption work because there is a de facto lowest common denominator for them: the simple text block, used in e-mail, editors, input and output from programs, etc. That is, we all mostly know exactly what an ASCII text block is, and crypto programs are expected to know how to access and manipulate such blocks. This largely explains the success of PGP across many platforms--text blocks are the basic element. Ditto for Cypherpunks remailers, which operate on the text blocks found in most mail systems. The situation becomes much murkier for things like digital money, which are not standalone objects and are often multi-party protocols involving time delays, offline processing, etc.
 - E. Lack of an economic motive. We on this list are not being paid to develop anything, are not assisted by anyone, and don't have the financial backing of corporations to assist us. Since much of today's "software development" is actually deal-making and standards negotiation, we are left out of lots of things.

17.4. Future Directions

17.4.1. "What are some future directions?"

17.4.2. The Future of the List

- + "What can be done about these situations?"

- That is, given that the Cypherpunks list often contains sensitive material (see above), and given that the current membership list can be accessed by..... what can be done?
 - Move central server to non-U.S. locale
 - Or to "cyberspace" (distributed network, with no central server...like FidoNet)
 - subscribers can use pseudonyms, cutouts, remailers
- 17.4.3. What if encryption is outlawed?
- can uuencode (and similar), to at least slow down the filter programs a bit (this is barely security through obscurity, but....)
 - underground movements?
 - will Cypherpunks be rounded up?
- 17.4.4. "Should Cypherpunks be more organized, more like the CPSR, EFF, and EPIC?"
- Those groups largely are lobbying groups, with a staff in Washington supported by the membership donations of thousands or tens of thousands of dues-paying members. They perform a valuable service, of course.
 - But that is not our model, nor can it plausibly be. We were formed as an ad hoc group to explore crypto, were dubbed "Cypherpunks," and have since acted as a techno-grassroots anarchy. No staff, no dues, no elections, no official rules and regulations, and no leadership beyond what is provided by the power of speech (and a slight amount of "final say" provided by the list maintainer Eric Hughes and the machine owner, John Gilmore, with support from Hugh Daniel).
 - If folks want a lobbying group, with lawyers in Washington, they should join the EFF and/or CPSR.
 - And we fill a niche they don't try to fill.
- 17.4.5. Difficult to Set Directions
- an anarchy...no centralized control
 - emergent interests
 - everyone has some axe to grind, some temporary set of priorities
 - little economic motivation (and most have other jobs)
- 17.4.6. The Heart and Soul of Cypherpunks?
- + Competing Goals:
 - + Personal Privacy
 - PGP, integration with mailers
 - education
 - + Reducing the Power of Institutions
 - whistleblower group
 -
 - Crypto Anarchy
 - + Common Purposes
 - + Spreading strong crypto tools and knowledge
 - PGP
 - + Fighting government restrictions and regulations
 - Clipper/Skipjack fight was a unifying experience
 - + Exploring new directions in cryptology
 - digital mixes, digital cash, voting
- 17.4.7. Possible Directions
- + Crypto Tools...make them ubiquitous "enough" so that the genie cannot be put back in the bottle
 - can worry about the politics later (socialists vs.

anarchocapitalists, etc.) (Although socialists would do well to carefully think about the implications of untraceable communications, digital cash, and world-wide networks of consultants and workers--and what this does to tax collection and social spending programs--before they work with the libertarians and anarchocapitalists to bring on the Crypto Millenium.)

- + Education
 - educating the masses about crypto
 - public forums
 - this was picked by the Cambridge/MIT group as their special interest
- + Lobbying
 - talking to Congressional aides and committee staffers, attending hearings, submitting briefs on proposed legislation
 - coordinating with EFF, CPSR, ACLU, etc.
 - this was picked by the Washington group as their special interest, which is compellingly appropriate (Calif. group is simply too far away)
- Legal Challenges
- + mixture of legal and illegal
 - use legal tools, and illegal tools
 - fallback positions
 - enlist illegal users as customers...help it spread in these channels (shown to be almost uncontrollable)

17.4.8. Goals (as I see them)

- + Get strong crypto deployed in such a way as to be unstoppable, unrecallable
 - "fire and forget" crypto
 - genie out of the bottle
 - Note that this does not necessarily that crypto be widely deployed, though that's generally a good idea. It may mean seeding key sites outside the U.S. with strong crypto tools, with remailers, and with the other acouterments.
- + Monkeywrench threats to crypto freedom.
 - economic sabotage of those who use statist contracts to thwart freedom (e.g., parts of AT&T)
- + direct sabotage
 - someday, viruses, HERF, etc.

17.4.9. A Vision of the Future

- encrypted, secure, untraceable communications
- hundreds of remailers, in many countries
- interwoven with ordinary traffic, ensuring that any attempt to quash crypto would also have a dramatic effect on business
- data havens, credit, renters, etc.
- information markets
- ability to fight wars is hindered
- U.S. is frantic, as its grip on the world loosens...Pax Americana dies

17.4.10. Key concepts are the way to handle the complexity of crypto

- The morass of protocols, systems, and results is best analyzed, I think, by not losing sight of the basic "primitives," the things about identity, security, authentication, etc. that make crypto systems work the way

they do.

- + Axiom systems, with theorems and lemmas derivable from the axioms
 - with alternate axioms giving the equivalent of "non-Euclidean geometries" (in a sense, removing the physical identity postulate and replacing it with the "the key is the identity" postulate gives a new landscape of interactions, implications, and structures).
 - (Markets, local references, voluntary transactions, etc.)
 - (ecologies, predators, defenders, etc.)
 - (game theory, economics, etc..)

17.5. Net of the Future

17.5.1. "What role, if any, will MUDs, MOOs, and Virtual Realities play?"

- "True Names," "Snow Crash," "Shockwave Rider"
- Habitat, online services
- + the interaction is far beyond just the canonical "text messages" that systems like Digital Telephony are designed to cope with
 - where is the nexus of the message?
 - what about conferences scattered around the world, in multiple jurisdictions?
- crypto = glue, mortar, building blocks
- "rooms" = private places; issues of access control
- Unless cops are put into these various "rooms," via a technology we can barely imagine today (agents?), it will be essentially impossible to control what happens in these rooms and places. Too many degrees of freedom, too many avenues for exchange.
- cyberspaces, MUDs, virtual communities, private law, untouchable by physical governments

17.5.2. keyword-based

- can be spoofed by including dictionaries

17.5.3. dig sig based (reputation-based)

17.5.4. pools and anonymous areas may be explicitly supported

17.5.5. better newsreaders, screens, filters

17.5.6. Switches

- "switching fabrics"
- ATM
- Intel's flexible mesh interconnects, iWARP, etc.
- all of these will make for an exponential increase in degrees of freedom for remailer networks (labyrinths). On-chip remailing is essentially what is needed for Chaum's mixes. ATM quanta (packets) are the next likely target for remailers.

17.5.7. "What limits on the Net are being proposed?"

- NII
- + Holding carriers liable for content
 - e.g., suing CompuServe or Netcom
 - often done with bulletin boards
- "We have to do something!"
- + Newspapers are complaining about the Four Horsemen of the Infocalypse:
 - terrorists, pedophiles, drug dealers, and money launderers
- + The "L.A. Times" opines:

- "Designers of the new Information Age were inspired by noble dreams of free-flowing data as a global liberating force, a true democratizing agent. Sadly, the crooks and creeps have also climbed aboard. The time has come for much tighter computer security. After all, banks learned to put locks on their vaults." ["L.A. Times," editorial, 1994-07-13]

17.6. The Effects of Strong Crypto on Society

17.6.1. "What will be the effects of strong crypto, ultimately, on the social fabric?"

- It's hard to know for sure.
- + These effects seem likely:
 - Starvation of government tax revenues, with concomitant effects on welfare, spending, etc.
 - increases in espionage
 - trust issues

17.6.2. The revelations of surveillance and monitoring of citizens and corporations will serve to increase the use of encryption, at first by people with something to hide, and then by others. Cypherpunks are already helping by spreading the word of these situations.

- a snowballing effect
- and various government agencies will themselves use encryption to protect their files and their privacy

17.6.3. People making individual moral choices

- people will make their own choices as to what to reveal, what they think will help world peace, or the future, or the dolphins, or whatever
- and this will be a liquid market, not just souls shouting in the desert
- of course, not everything will be revealed, but the "mosaic effect" ensures that mostly the truth will emerge
- every government's worst fear, that it's subjects will decide for themselves what is secret, what is not, what can be told to foreigners, etc.

17.7. New Software Tools and Programming Frameworks

17.7.1. Needed software

- Drop-in crypto modules are a needed development. As V. Bontchev says, "it would be nice if disk encryption software allowed the user to plug in their own modules. This way everybody could use whatever they trust - MDC/SHA, MDC/MD5, DES, IDEA, whatever." [V.B., sci.crypt, 1994-07-01]
- + Robustness
 - Security and robustness are often at odds
 - Files that are wiped at the first hint of intrusion (digital flash paper), remailer sites that go down at the first signs of trouble, and file transmission systems that split files into multiple pieces--any one of which can be lost, thus destroying the whole transmission--are not exactly models of robustness.
 - Error correction usually works by decreasing entropy through redundancy, which is bad for crypto.
 - The military uses elaborate (and expensive) systems to ensure that systems do not go down, keys are not lost,

- etc. Most casual users of crypto are unwilling to take these steps.
 - And so keys are lost, passphrases are forgotten (or are written down on Post-It Notes and taped to terminals), and remailers are taken down when operators go on vacation. All very flaky and non-robust.
 - Look at how flaky mail delivery is!
 - + A challenge is to create systems which are:
 - robust
 - not too complicated and labor-intensive to use
 - where redundancy does not compromise security
 - + Crypto workbench
 - An overused term, perhaps, but one that captures the metaphor of a large set of tools, templates, programming aids, etc.
 - + QKS and "Agents Construction Kit" (under development)
 - along with Dylan, DylanAgents, Telescript, and probably several other attempts to develop agent toolkits
 - Henry Strickland is using "tcl" (sort of a scripting language, like "perl") as a basis.
 - + Software crisis
 - tools, languages, frameworks, environments, objects, class libraries, methods, agents, correctness, robustness, evolution, prototyping
 - + Connections between the software crisis and cryptography
 - complex systems, complicated protocols
 - price of being "wrong" can be very high, whether it's an airport that can't open on time (Denver) or a digital bank that has its assets drained in seconds
 - agents, objects are hoped to be the "silver bullets"
 - + The need for better software methodologies
 - "silver bullets"
 - failures, errors, flaws, methods
 - provably correct designs? (a la Viper)
 - It is often said that much better methodologies are needed for real time programming, due to the time-criticality and (probably) the difficulty of doing realistic testing. But surely the same should be said of financial programming, a la the banking and digicash schemes that interest us so much.
 - "the one aspect of software that most makes it the flaky industry it is is that it is unusual for practitioners to study the work of others. Programmers don't read great programs. Designers don't study outstanding designs. The consequences ... no, just look for yourself. [Cameron Laird, comp.software-eng, 1994-08-30]"
 - + Large Software Constructs
 - The software crisis becomes particularly acute when large systems are built, such as--to apply this to Cypherpunks issues--when digital money systems and economies are built.
- 17.7.2. Object-oriented tools
- + While tres trendy, some very real gains are being reported; more than just a buzzword, especially when combined with other tools:
 - frameworks, toolkits

- + dynamic languages
 - greater flexibility than with static, strongly-typed languages (but also less safety, usually)
 - OpenStep, Visual Age, Visual Basic, Dylan, Telescript (more agent-oriented), Lisp, Smalltalk, etc
- 17.7.3. Protocol Ecologies
- Behavioral simulations of agents, digital money, spoofing, etc.
 - the world in which Alice and Bob and their crypto friends live
 - defense, attack, spoofing, impersonation, theft
 - elements that are cryptographically strong (like D-H key exchanges), but combined in complex ways that almost have to be simulated to find weaknesses
 - "middle-out" instead of "top-down" (conventional, formal) or "bottom-up" (emergent, A-LIFE)
 - like Eurisko (Lenat), except oriented toward the domain of financial agents
- 17.7.4. Use of autonomous agents (slaves?)
- "An advanced telecommunications environment offers a number of ways to protect yourself against the problems involved in dealing with anonymous entities in a situation in which there is no monopoly Government.....When one's PBX finds that one's call is not going through via a particular long distance carrier, it automatically switches to another one. It is easy to imagine one's intelligent agents testing various sorts of transaction completions and switching vendors when one fails. Professional checkers can supply information on vendor status for a fee. After all, we don't care if a company we are dealing with changes if its service is unaffected." [Duncan Frissell, 1994-08-30]
- 17.7.5. Tools
- + "Languages within languages" is a standard way to go to implement abstractions
 - "Intermediate Design Languages" (IDLs)
 - abstract concepts: such as "engines" and "futures"
 - Lisp and Scheme have been favored languages for this
 - other languages as well: Smalltalk, Dylan
 - + For crypto, this seems to be the case: abstractions represented as classes or objects
 - with programming then the selective subclassing
 - and sometimes gener
 - + "type checking" of crypto objects is needed
 - to ensure compliance with protocols, with forms expected, etc.
 - check messages for form, removal of sigs, etc. (analogous to checking a letter before mailing for proper addressing, for stamp, sealing, etc.)
 - much of the nonrobustness of mail and crypto comes from the problems with exception handling--things that a human involved might be able to resolve, in conventional mail systems
 - "dead letter department"?
 - Note: In the "Crypto Anarchy Game" we played in September, 1992, many sealed messages were discarded for being in the wrong form, lacking the remailer fee that the remailer required, etc. Granted, human beings make

fairly poor maintainers of complex constraints....a lot of people just kept forgetting to do what was needed. A great time was had by all.

17.7.6. "What programming framework features are needed?"

- What follows are definitely my opinions, even more my own opinions than most of what I've written. Many people will disagree.
- + Needed:
 - Flexibility over speed
 - Rapid prototyping, to add new features
 - Evolutionary approaches
 - Robustness (provably correct would be nice, but...)

17.7.7. Frameworks, Tools, Capabilities

- Nearly all the cutting-edge work in operating systems, from "mutually suspicious cooperating processes" to "deadlock" to "persistence," show up in the crypto areas we are considering.
- + Software of the Net vs. Software to Access the Net
 - The Net--is current form adequate?
 - Software for Accessing the Net
- + OpenDoc and OLE
 - components working together, on top of various operating systems, on top of various hardware platforms
- + Persistent Object Stores
 - likely to be needed for the systems we envision
 - robust, so that one's "money" doesn't evaporate when a system is rebooted!
 - interesting issues here...
 - CORBA. OpenDoc, OLE II, SOM, DOE, Gemstone, etc.
- + Programming Frameworks
 - Dynamic languages may be very useful when details are fuzzy, when the ideas need exploration (this is not a call for nondeterminism, for random futzing around, but a recognition that the precise, strongly-typed approach of some languages may be less useful than a rich, exploratory environment. This fits with the "ecology" point of view.
 -
- + Connectivity
 - needs to be more robust, not flaky the way current e-mail is
 - handshakes, agents, robust connections
 - ATM, SONET, agents, etc....the "Net of the Future"

17.8. Complexity

17.8.1. The shifting sands of modern, complex systems

- lots of cruft, detail...changing..related to the "software crisis"...the very flexibility of modern software systems promotes the frequent changing of features and behaviors, thus playing hob with attempts of others to understand the structure...evolution in action
- humans who use these systems forget how the commands work, where things are stored, how to unsubscribe from lists, etc. (This is just one reason the various sub-lists of our list have seldom gotten much traffic: people use what they are most used to using, and forget the rest.)
- computer agents (scripts, programs) which use these systems

often "break" when the underlying system changes. A good example of this are the remailer sites, and scripts to use them. As remailer sites go up and down, as keys change, as other things change, the scripts must change to keep pace.

- This very document is another example. Scattered throughout are references to sites, programs, sources, etc. As time goes by, more and more of them will (inevitably) become obsolete. (My hope is that enough of the pointers will point to still-extant things so as to make the pointers remain useful. And I'll try to update/correct the bad pointers.)

17.8.2. "Out of Control"

- Kevin Kelly's book
- inability to have precise control, and how this is consistent with evolution, emergent properties, limits of formal models
- crypto, degrees of freedom
- + imagine nets of the near future
 - ten-fold increase in sites, users, domains
 - ATM switching fabrics..granularity of transactions changes...convergence of computing and communications...
- + distributed computation (which, by the way, surely needs crypto security!)
 - Joule, Digital Silk Road
 - agents, etc.
- + can't control the distribution of information
- + As with the Amateur Action BBS case, access can't be controlled.
 - "The existence of gateways and proxy servers means that there is no effective way to determine where any information you make accessible will eventually end up. Somebody in, say, Tennessee can easily get at an FTP site in California through a proxy in Switzerland. Even detailed information about what kind of information is considered contraband in every jurisdiction in the world won't help, unless every *gateway* in the world has it and uses it as well."
[Stephen R. Savitzky, comp.org.eff.talk, 1994-08-08]

17.8.3. A fertile union of cryptology, game theory, economics, and ecology

- + crypto has long ignored economics, except peripherally, as an engineering issue (how long encryption takes, etc.)
 - in particular, areas of reputation, risk, etc. have not been treated as central idea...perhaps proper for mathematical algorithm work
 - but economics is clearly central to the systems being planned...digital cash, data havens, remailers, etc.
- + why cash works so well...locality of reference, immediate clearing of transactions, forces computations down to relevant units
 - reduces complaints, "he made me do it" arguments...that is, increases self-responsibility...caveat emptor
- + game theory
 - + ripe for treatment of "Alice and Bob" sorts of situations, in which agents with different agendas are interacting and competing
 - "defecting" as in Prisoner's Dilemma

- payoff matrices for various behaviors
- evolutionary game theory
- evolutionary learning, genetic algorithms/programming
- protocol ecologies

17.9. Crypto Standards

17.9.1. The importance of standards

- a critical role
- + Part of standards is validation, test suites, etc.
 - validating the features and security of a remailer, through pings, tests, performance tests, reliability, etc.
 - thus imposing a negative hit on those who fail
- + There are many ways to do this standards testing
 - market reports (as with commercial chips, software)
 - "seals of approval" (especially convenient with digital sigs)

17.10. Crypto Research

17.10.1. Academic research continues to increase

17.10.2. "What's the future of crypto?"

- Predicting the future is notoriously difficult. IBM didn't think many computers would ever be sold, Western Union passed on the chance to buy Bell's telephone patents. And so on. The future is always cloudy, the past is always clear and obvious.
- We'll know in 30 years which of our cypherpunkish and cryptoanarchist predictions came to pass--and which didn't.

17.10.3. Ciphers are somewhat like knots...the right sequence of moves unties them, the wrong sequence only makes them more tangled. ("Knot theory" is becoming a hot topic in math and physics (work of Vaughn Jones, string theory, etc.) and I suspect there are some links between knot theory and crypto.)

17.10.4. Game theory, reputations, crypto -- a lot to be done here

- a missing link, an area not covered in academic cryptology research
- distributed trust models, collusion, cooperation, evolutionary game theory, ecologies, systems

17.10.5. More advanced areas, newer approaches

- + some have suggested quasigroups, Latin squares, finite automata, etc. Quasigroups are important in the IDEA cipher, and in some DES work. (I won't speculate further about an area I know almost nothing about....I'd heard of semigroups, but not quasigroups.)
- "The "Block Mixing Transform" technology which I have been promoting on sci.crypt for much of this spring and summer is a Latin square technology. (This was part of my "Large Block DES" project, which eventually produced the "Fenced DES" cipher as a possible DES upgrade.)....Each of the equations in a Block Mixing Transform is the equation for a Latin square. The multiple equations in such a transform together represent orthogonal Latin squares. [Terry Ritter, sci.crypt, 1994-08-15]
- + But what about for public key uses? Here's something Perry Metzger ran across:
 - "'Finite Automata, Latin arrays, and Cryptography" by Tao

Renji, Institute of Software, Academia Sinica, Beijing.
This (as yet unpublished) paper covers several
fascinating topics, including some very fast public key
methods -- unfortunately in too little detail. Hopefully
a published version will appear soon..." [P.M.,
sci.crypt, 1994-08-14]

17.10.6. Comments on crypto state of the art today vs. what is likely
to be coming

- Perry Metzger comments on today's practical difficulties:
"...can the difference between "crypto can be transforming
when the technology matures" and "crypto is mature now" be
that unobvious?....One of the reasons I'm involved with the
IETF IPSP effort is because the crypto stuff has to be
transparent and ubiquitous before it is going to be truly
useful -- in its current form its just junk. Hopefully,
later versions of PGP will also interface well with the new
standards being developed for an integrated secure message
body type in MIME. (PGP also requires some sort of scalable
and reverse mapable keyid system -- the current keyids are
not going to allow key servers to scale in a distributed
manner.) Yes, I've seen the shell scripts and the rest, and
they really require too much effort for most people -- and
at best, once you have things set up, you can now securely
read some email at some sites. I know that for myself,
given that I read a large fraction of my mail while working
at clients, where I emphatically do not trust the hardware,
every encrypted message means great inconvenience,
regardless." [Perry Metzger, 1994-08-25]

17.11. Crypto Armageddon? Cryptageddon?

17.11.1. "Will there be a "Waco in cyberspace"?"

- while some of us are very vocal here, and are probably
known to the authorities, this is not generally the case.
Many of the users of strong crypto will be discreet and
will not give outward appearances of being code-using
crypto anarchist cultists.

17.11.2. Attacks to come

- "You'll see these folks attacking anonymous remailers,
cryptography, psuedonymous accounts, and other tools of
coercion-free expression and information interchange on
the net, ironically often in the name of promoting
"commerce". You'll hear them rant and rave about
"criminals" and "terrorists", as if they even had a good
clue about the laws of the thousands of jurisdictions
criss-crossed by the Internet, and as if their own attempts
to enable coercion bear no resemblance to the practice of
terrorism. The scary thing is, they really think they
have a good idea about what all those laws should be, and
they're perfectly willing to shove it down our throats,
regardless of the vast diversity of culture, intellectual,
political, and legal opinion on the planet."
[<an50@desert.hacktic.nl> (Nobody), libtech-1@netcom.com,
1994-06-08]

+ why I'm not sanguine about Feds

- killing Randy Weaver's wife and son from a distance,
after trumped-up weapons charges
- burning alive the Koresh compound, on trumped-up charges

- of Satanism, child abuse, and wife-insulting
- seizures of boats, cars, etc., on "suspicion" of involvement with drugs

17.12. "The Future's So Bright, I Gotta Wear Shades"

17.12.1. Despite the occasionally gloomy predictions, things look pretty good. No guarantees, of course, but trends that are favorable. No reason for us to rest, though.

17.12.2. Duncan Frissell puts it this way:

- "Trade is way up. Wealth is way up. International travel is way up. Migration is way up. Resource prices are the lowest in human history. Communications costs are way down. Electronics costs are way down. We are in a zero or negative inflation environment. The quantity and quality of goods and services offered on the markets is at an all-time high. The percentage of the world's countries headed by dictators is the lowest it's ever been.

"What all this means is that political philosophies that depend on force of arms to push people into line, will increasingly fail to work. Rich people with choices will, when coerced, tend to change their investments and business affairs into a friendlier form or to move to a friendlier environment. Choice is real. If choices exist, they will be made. An ever higher proportion of the world's people will be "rich" in wealth and choice as the years go on.

"Only a political philosophy that depends on the uncoerced cooperation of very different people has a chance of functioning in the future." [Duncan Frissell, 1994-09-09]

17.13. "Will cryptography really bring on the Millenium?"

17.13.1. Yes. And cats will move in with dogs, Snapple will rain from the sky, and P will be shown unequal to NP.

17.13.2. Seriously, the implications of strong privacy, of cyberspatial economies, and of borders becoming transparent are enormous. The way governments do business is already changing, and this will change things even more dramatically. The precise form may be unpredictable, but certain end states are fairly easy to predict in broad brush strokes.

17.13.3. "How do we know the implications of crypto are what I've claimed?"

- We can't know the future.
- Printing, railroads, electrification

17.13.4. "When will it all happen? When will strong crypto really begin to have a major effect on the economy?"

+ Stages:

- The Prehistoric Era. Prior to 1975. NSA and other intelligence agencies controlled most crypto work. Cryptography seen as a hobby. DES just starting to be deployed by banks and financial institutions.
- The Research Era. 1975-1992. Intense interest in public key discovery, in various protocols. Start of several "Crypto" conferences. Work on digital money, DC-Nets, timestamping, etc.
- The Activism Era. 1992--?? (probably 1998). PGP 2.0

released. Cypherpunks formed. Clipper announced--meets firestorm of protest. EFF, CPSR, EPIC, other groups. "Wired" starts publication. Digital Telephony, other bills. Several attempts to start crypto businesses are made...most founder.

- The Transition Era. After about 1999. Businesses start. Digital cash needed for Net transactions. Networks and computers fast enough to allow more robust protocols. Tax havens flourish. "New Underworld Order" (credit to Claire Sterling) flourishes.
 - It is premature to expect that the current environment-- technological and regulatory--will be beneficial to the type of strong crypto we favor. Too many pieces are missing. Several more advances are needed. A few more failures are also needed (gulp!) to show better how not to proceed.
- 17.13.5. "But will crypto anarchy actually happen?"
- To a growing extent, it already is happening. Look at the so-called illegal markets, the flows of drug money around the world, the transfer of billions of dollars a day on mere "chop marks," and the thriving trade in banned items.
 - "Grey and black capitalism is already a major component of international cash flows....Once adequate user friendly software is available, the internet will accelerate this already existing trend....Crypto anarchy is merely the application of modern tools to assist covert capitalism." [James Donald, 1994-08-29]
 - There are arguments that a Great Crackdown is coming, that governments will shut down illegal markets, will stop strong crypto, will force underground economies aboveground. This is doubtful--it's been tried for the past several decades (or more). Prohibition merely made crime more organized; ditto for the War on (Some) Drugs.
- 17.13.6. "Has the point of no return been passed on strong crypto?"
- Actually, I think that in the U.S. at least, the point was passed decades ago, possibly a century or more ago, and that any hope of controlling strong crypto and private communication evaporated long ago. Abuses by the FBI in wiretapping Americans, and reports of NSA monitoring of domestic communications notwithstanding, it is essentially.....

17.14. Loose Ends

17.14.1. firewalls, virtual perimeters, swIPe-type encrypted tunnels, an end to break-ins,

17.14.2. "What kind of encryption will be used with ATM?"

- (ATM = Asynchronous Transfer Mode, not Automated Teller Machine)

- some reports that NSA is developing standards for ATM

17.14.3. Shapes of things to come, maybe....(laws of other countries)

- + India has a fee schedule for BBS operators, e.g., they have to pay \$50,000 a year to operate a bulletin board! (This sounds like the urban legend about the FCC planning a modem tax, but maybe it's true.)

- "The Forum for Rights to Electronic Expression (FREE) has been formed in India as a body dedicated to extending fundamental rights to the electronic domain....FREE owes

its creation to an attack on Indian datacom by the Indian government, in the form of exorbitant licence fees (a minimum Rs. 1.5 million = US\$50,000 each year for a BBS, much higher for e-mail)." [amehta@doe.ernet.in (Dr. Arun Mehta), forwarded by Phil Agre, comp.org.cpsr.talk, 1994-08-31]

- for more info: ftp.eff.org
/pub/EFF/Policy/World/India/FREE

17.14.4. Cyberspace will need better protection

- to ensure spoofing and counterfeiting is reduced (recall Habitat's problems with people figuring out the loopholes)

18. Loose Ends and Miscellaneous Topics

18.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

18.2. SUMMARY: Loose Ends and Miscellaneous Topics

18.2.1. Main Points

18.2.2. Connections to Other Sections

18.2.3. Where to Find Additional Information

18.2.4. Miscellaneous Comments

- I hate to have a section like this, but there are just some things that don't seem to fit neatly elsewhere
- hopefully you found this topics with your editor search tools

18.3. Quantum Cryptography

18.3.1. "What is quantum cryptography?"

- + Two main flavors:
 - + secure channels exploiting the Uncertainty Principle
 - + Brassard, Bennett, fiber optic lines, short distances, detects tapping
 - + Quantum cryptography
 - bits can be exchanged-albeit at fairly low efficiencies-over a channel
 - with detection of taps, via the change of polarizations
 - + Stephen Wiesner wrote a 1970 paper, half a decade before the P-K work, which outlined this-not published until much later
 - speculate that the NSA knew about this and quashed the publication
 - + factoring of numbers using a strange Many World interpretation
 - Shor
 - + hearkens to my spoof about Russians
 - I never knew I hit so close to the mark!

18.3.2. "What about quantum cryptography?"

- + Exploiting Uncertainty Principle to make untappable communication lines. (More precisely, tapped lines give indication of having been tapped.)
 - Bennett and Brassard

- faint flashes of light in a fiber optic cable used; polarized photons
- Alice and Bob go through a protocol that involves them picking Linear or Circular Polarization (LP or CP); can't be simultaneously measured...
-
- Not likely to be important for a long time.
- An additional tool, or crypto primitive building block.

18.4. Chaotic Cryptography

18.4.1. the oscillator scheme was broken at Crypto '94

18.5. Neural Nets and AI in Crypto

18.5.1. "What about neural nets and AI in crypto?"

- Of limited use, at least in breaking modern ciphers. Marvin Minsky once said that if you don't understand how to solve a problem, adding randomness usually doesn't help.
- The shape of the solution space is very spiky, very poorly-suited to hill-climbing or divide-and-conquer methods
- + Neural nets are not likely to do well with modern ciphers (e.g., RSA, IDEA, DES, etc.), mainly because of the shape of the solution space. Instead of the "rolling hills and valleys" that neural nets (and related methods, such as genetic algorithms, simulated annealing, etc.) do well in, the solution space for modern ciphers offers very little in the way of "learning" opportunities: you either have the solution (the key), or you don't.

Think of a needle standing up from a flat plain...a NN or any other hill-climber could wander for years and never find it. Well-designed modern ciphers like RSA and IDEA appear to admit no analysis based on "nonrandom" properties. If anybody has found shortcuts to factoring the modulus in RSA, for example, they haven't let on.

I suspect there are uses in peripheral aspects, such as guessing passwords (when people have not picked high-entropy passwords, but have instead used familiar names). Or in traffic analysis. Those who munch on lots of traffic may well be using neural nets, custom signal processing, etc. to "prepare" the captured traffic for further analysis. A safe bet, in fact.

But the move in modern cryptology is definitely away from using anything with "structure" that can be learned. Put another way, neural nets and such work well in structured environments, where there's something to learn, but not in the high-entropy, seemingly random world of encrypted data.

- + AI may be useful in other areas
 - protocol generation
 - SIGINT

18.5.2. Evolutionary or Genetic Programming

- a la Holland, Koza
- RNGs

18.6. Miscellaneous Advanced Crypto Ideas

18.6.1. "Why have provably "NP-complete" problems not found uses in crypto?"

- One of the great Unresolved Mysteries! Or the Holy Grail, if you will.
- The issue is why have provably hard (or NP-complete, to be more accurate) problems not been used? (Factoring is not known to NP-complete...experts can correct my phrasing here if I'm misstating things.)
- It would be nice if a provably hard problem, such as the domino tiling problem, or 3SAT, or other such things out of Garey and Johnson's book on NP-Completeness could be used. This would increase confidence in ciphers still further.

18.6.2. "Can cellular automata, like Conway's "Game of Life," be used for cryptography?"

- Stephen Wolfram proposed use of cellular automata for cryptography some years back; his collection of essays on cellular automata contains at least one such mention. Many people suspected that 1D CAs were no stronger than linear feedback shift registers (LFSRs), and I recall hearing a couple of years ago that someone proved 1D CAs (and maybe all CAs?) are equivalent to LFSRs, which have been used in crypto for many years.
- Wolfram's book is "Theory and Applications of Cellular Automata," 1986, World Scientific. Several papers on using CAs for random sequence generation. P. Bardell showed in 1990 that CAs produce the outputs of LFSRs.) Wolfram also has a paper, "Cryptography with cellular automata," in Proc. CRYPTO 85.
- Intuitively, the idea of a CA looks attractive for "one-way functions," for the reasons mentioned. But what's the "trapdoor" that gives the key holder a shortcut to reverse the process? (Public key crypto needs a trapdoor 1-way function that is easy to reverse if one has the right information).

18.7. Viruses and Crypto

18.7.1. "What's the connection between Cypherpunks and viruses?"

- Like, dewd, it's so kool.
- Beavis 'n Butthead use PGP (actually, Eric Hughes proposed at one point that we suggest a crypto tie-in to the writers)
- There's only peripheral connection.
- Viruses can be spread with anonymous remailers, but digital signatures can be used to safeguard software. Signed software, no mods allowed.

18.7.2. "What about the "encryption viruses," like KOH?"

- (A little far afield, but the issue does come up.)
- Somebody asked about this on sci.crypt and Vesselin Bontchev said: "This topic has been debated to death in alt.security.pgp, when somebody posted KOH, without even a warning that it is a virus.....Both viruses indeed use the IDEA cipher - the same that is used both by SecureDevice and SecureDrive. However, the viruses pose some significant threats to the integrity of your data, exactly because of their viral replication means.....Also, if you acquire it by viral means, you do not get the documentation and one utility, both of which are essential for the proper usage

of the product - thus proving one more time that its viral capabilities are unnecessary and harmful. Also, the virus does not come in source, which means that it could have some hidden backdoors or simply security flaws, and you have no way to check this or to fix them. At last, in some cases the virus could destroy valuable information during its replication process."

- "In short - don't use them. You will gain nothing over using stand-alone encryption programs, and you'll expose your data's integrity to significant risks. Those viruses are completely useless and even harmful; they have been created with the only reason to condone the illicit activities of the virus writers, by claiming that computer viruses can be "useful"." [Vesselin Bontchev, sci.crypt, 1994-08-31]

18.7.3. "What about viruses? Are there any ties to crypto and Cypherpunks themes?"

- No direct link that any of us see clearly. Occasionally a virus fan sees the "punks" name and thinks we're involved in writing viruses. (Actually, a few folks on the list have virus expertise.)
- Crypto may protect against viruses, by having code signed. And the reliance on self-responsibility and self-protection is in contrast to the legal approach, which tends not to work too well for virus protection (by the covert nature of many viruses).

18.7.4. "What interests do Cypherpunks have in viruses?"

- Not much, though the topic comes up periodically.
- Some overlap in the communities involved.
- And there are some virus methods which use forms of encryption.
- Also, digital signatures on code can be used to ensure that code has not been modified since being released by the original author.

18.8. Making Money in Crypto

18.8.1. "How can I make money in crypto?"

- crypto experts are hired by software companies
- + start up companies
 - a tough road
 - not clear that even Phil Zimmermann has made money
 - and even RSADSI is facing a challenge (hasn't gone public, not a cash cow, etc.)
- There may be an explosive growth--the phase change I often talk about--and many opportunities will emerge. But, having said this, I still don't see obvious opportunities right now. And starting a company based on hope and ideology, rather than supplying a real market or pushing real technology (market pull vs. technology push argument) seem misguided.

18.9. The Net

18.9.1. Limitations of the current net

- interoperability
- + subsidized, not pay as you go
 - makes spamming inevitable, doesn't allocate resources to those who want them the most
 - this will require digicash in a better form than most users now have access to
- sysadmins get worried
- encryption sometimes banned
- common carrier status not clear
- general cruftiness of Net ("imminent death of Usenet predicted")

18.10. Duress Switches, Dead Man Switches

18.10.1. "What about "duress" codes for additional security?"

- Where a harmless decryption can be done, or an alarm sent.
- + Examples
 - sending alarm, like an under the counter alarm button
 - decrypting a bank card number for a lesser-value account
 - two sets of books (not strictly a "duress" code, unless you view the IRS as causing duress)
 - alarms to associates, as in cells
- " Having a separate authentication mechanism that is used under duress is a very good idea that some existing systems already employ.... From a systems point of view, it is hard to figure out exactly how the system should respond when it recognizes a duress authentication....The safe inside the ATM machines used by BayBanks (Boston Mass) can be opened with two combinations. One combination sends an alarm to the bank via a separate phone line (not the one used to perform the ATM transaction). The alarm phone line is also connected to a conventional panic switch." [Bob Baldwin, Duress Passwords/PINs/Combinations, 1993-11-18]

18.10.2. Duress switches, dead man switches, etc.

- + "Digital flash paper," can be triggered to erase files, etc.
 - (BATF and DEA raiders may have sophisticated means of disabling computers)
- + Duress codes..."erase my files," ways of not giving esrowed information unless proper code is given, etc.
- + "Don't release if I am under indictment"
 - interesting issues about secret indictments, about publicity of such cases, access to court records by offshore computers, etc.

18.10.3. Personal security for disks, dead man switches

- + I have heard that some BBS operators install dead man switches near the doors to rooms containing their systems...entering the room without flipping the switch causes some action to be taken
 - erasing a disk, dumping a RAM disk (a dangerous way to store data, given power failures, soft errors, restarts, etc.)

18.11. Can Encryption be Detected?

18.11.1. "Can messages be scanned and checked for encryption?"

- If the encryption produces markers or other indications, then of course. "BEGIN PGP" is a pretty clear beacon. (Such

markers assists in decryption by the recipient, but are not essential. "Stealth" versions of PGP and other encryption programs--such as S-Tools for DOS--don't have such markers.)

- If the encryption produces "random-looking" stuff, then entropy measures and other statistical tests may or may not be able to detect such messages reliably. Depends on what non-encrypted messages look like, and how the algorithm works.
- + Steganography:
 - making messages look like normal ones
 - tucking the bits in with other random-like bits, such as in the low-order bits of images or sound files
- The practical concern depends on one's local political environment. In many countries, mere suspicion of using crypto could put one in real danger.

18.12. Personal Digital Assistants, Newtons, etc.

18.12.1. "Are there cryptographic uses for things like Newtons?"

- Probably. Eventually. Digital wallets, portable key holders, local agents for access, etc.
- + Meanwhile, a few encryption programs exist. Here's one:
 - -> nCrypt, the strong cryptography application for Newton:
 - > ftp.sumex-aim.stanford.edu/info-mac/nwt/utills/n-crypt-lite.hqx

18.13. Physical Security

18.13.1. "Can fiber optical cables be tapped?"

- + Yes. Light can escape from the fiber in bends, and "near-field" tapping is theoretically possible, at least under lab conditions. Active measures for puncturing cable shields and tapping fibers are also possible.
- "The Fed's want a cost effective F/O tap. My company was approached to develop such a system, can be done but not cheap like copper wire tapping." [
domonkos@access.digex.net (andy domonkos),
comp.org.eff.talk, 1994-06-29]
- Los Alamos technology? 1990?

18.14. Attacking Governments

18.14.1. "termites" (rumors, psy-ops) that can undermine governments, followed by "torpedoes" (direct attack)

18.14.2. WASTE (War Against Strong, Tamper-resistant Encryption).

18.15. Cypherpunks List Issues

18.15.1. too much noise on the list?

- "Of all the lists I'm subscribed to, this is the only one that I read *every* article in. Even the "noise" articles. Humans being what they are, the noise is needed to help decide the direction of the group. Besides, for those of us who are just starting on our journey through crypto-underworld need the noise to help familiarize ourselves with how crypto works. I've learned more from

the informal
ramblings than I've gathered out of all the formal and/or
mathematical
postings to date." [Patrick E. Hykkonen, 5-25-93]

18.16. Tamper-Resistant Modules

18.16.1. TRMs--claims that "Picbuster" processor can be locally
overwritten with focussed or directed UV (OTP)

18.16.2. tamper-resistant modules have some downsides as well
- cash registers for ensuring compliance with all relevant
sales tax, value-added tax (VAT), and rationing rules; a
tamper-resistant module cash register could be the
enforcement mechanism for a national security state.
- "observers"

18.17. Deeper Connections

18.17.1. In several places I've referred to "deep connections" between
things like crypto, money, game theory, evolutionary
ecologies, human motivations, and the nature of law. By this
I mean that there are deeper, unifying principles. Principles
involving locality, identity, and disclosure of knowledge. A
good example: the deep fairness of "cut-and-choose" protocols--
I've seen mention of this in game theory texts, but not
much discussion of other, similar protocols.

18.17.2. For example, below the level of number theory and algorithms
in cryptology lies a level dealing with "identity," "proof,"
"collusion," and other such core concepts, concepts that can
almost be dealt with independent of the actual algorithms
(though the concrete realization of public key methods took
this out of the abstract realm of philosophy and made it
important to analyze). And these abstract concepts are linked
to other fields, such as economics, human psychology, law,
and evolutionary game theory (the study of evolved strategies
in multi-agent systems, e.g., human beings interacting and
trading with each other).

18.17.3. I believe there are important questions about why things work
the way they do at this level. To be concrete, why do threats
of physical coercion create market distortions and what
effects does this have? Or, what is the nature of emergent
behavior in reputation-based systems? (The combination of
crypto and economics is a fertile area, barely touched upon
by the academic cryptology community.) Why is locality is
important, and what does this mean for digital cash? Why does
regulation often produce more crime?

18.17.4. Crypto and the related ideas of reputation, identity, and
webs of trust has introduced a new angle into economic
matters. I suspect there are a couple of Nobel Prizes in
Economics for those who integrate these important concepts.

18.18. Loose End Loose Ends

18.18.1. What the core issues are...a tough thing to analyze

- untraceability as a basic construct has major implications
- + can often ask what the implications would be if, say:
 - invisibility existed
 - untraceability existed
- By "tough to analyze" I mean that things are often
coflated, mixed together. Is it the "reputations" that

matter, or the "anonymity"? The "untraceability" or the "digital money"?

18.18.2. Price signalling in posts...for further information

- + When an article is posted, and there is more complete information available elsewhere by ftp, gopher, mosaic, etc., then how is this to be signalled without actually advertising prominently?
- why not a code, like the "Geek code" so many people put in their sigs? The code could be parsed by a reader and used to automatically fetch the information, pay for it, etc. (Agents that can be built in to newsreaders.)

18.18.3. "What should Cypherpunks support for "cable" or "set-top box" standards?

- Caveats: My opinions, offered only to help frame the debate. And many of us reject the idea of government-mandated "standards," so my phrasing here is not meant to imply support of such standards.
- + Major alternatives:
 - + Set-top box, with t.v. as core of access to "information superhighway."
 - + Problems:
 - limited number of channels, even if "500 channels"
 - makes t.v. the focus, loses some other capabilities
 - few consumers will have television sets with the resolution capabilities that even current computer monitors have (there are reasons for this: size of monitors (related to viewing distance), NTSC constraints, age of televisions, etc.)
 - + Switched-packet cable, as in ATM or even SONET (Synchronous Optical Network) access
 - + Advantages:
 - Television is just one more switched-packet transmission, not using up the bandwidth
 - + Radical Proposal: Complete deregulation
 - + let cable suppliers--especially of optical fibers, which are small and unobtrusive--lay fibers to any home they can negotiate access to
 - e.g., by piggybacking on telephone lines, electrical cables, etc. (to remove the objection about unsightly new poles or cables being strung...should not be an issue with fiber optics)
 - let the market decide...let customers decide
- + In my view, government standards are a terrible idea here. Sure, NTSC was an effective standard, but it likely would have emerged without government involvement. Ditto for Ethernet and a zillion other standards. No need for government involvement.
- Of course, when industry groups meet to discuss standards, one hopes that antitrust laws will not be invoked.

18.18.4. minor point: the importance of "But does it scale?" is often exaggerated

- in many cases, it's much more important to simply get something deployed than it is to worry in advance about how it will break if too many people use it (e.g., MacDonald's worrying in 1955 about scalability of their business).
- Remailer networks, for example, may not scale especially

well in their current form...but who cares? Getting them used will allow further refinement.

19. Appendices

19.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

19.2. SUMMARY: Appendices

19.2.1. Main Points

19.2.2. Connections to Other Sections

19.2.3. Where to Find Additional Information

19.2.4. Miscellaneous Comments

- This is still under construction
- Disorganized!!!
- URLs need to be checked

19.3. Appendix -- Sites, Addresses, URL/Web Sites, Etc.

19.3.1. be sure to get soda address straight!!! [use clones]

- I received mine from soda.csua.berkeley.edu
the menus are: </pub/cypherpunks/pgp/pgp26>

19.3.2. How to use this section

- + comment on URLs being only a snapshot...
 - use reply to Sherry Mayo here

19.3.3. General Crypto and Cypherpunks Sites

- [sci.crypt](ftp://sci.crypt) archive: anon ftp to [ftp.wimsey.bc.ca:/pub/crypto](ftp://ftp.wimsey.bc.ca:/pub/crypto)
[Mark Henderson]
- + <ftp://soda.berkeley.edu/pub/cypherpunks/Home.html> [has probably been changed to soda.csua.edu site]
- <ftp://ftp.u.washington.edu/public/phantom/cpunk/README.html>
- <ftp://furmint.nectar.cs.cmu.edu/security/cypheressay/what-is-cypherpunk.html> [Vincent Cate, 1994-07-03]
- <ftp://wiretap.spies.com/Gov/World/usa.con>
- <http://www.quadralay.com/www/Crypt/Crypt.html>
- <http://cs.indiana.edu/ripem/dir.html>
- misc. article on crypto:
<http://www.quadralay.com/www/Crypt/Crypt.html>
- [ftp.wimsey.bc.ca:/pub/crypto](ftp://ftp.wimsey.bc.ca:/pub/crypto) has REDOC III, Loki91, SHS and HAVAL (Mark Henderson, markh@vanbc.wimsey.com, 4-17-94, sci.crypt)
- + Some misc. ftp sites to check:
 - soda.berkeley.edu
 - [ftp.informatik.uni-hamburg.de](ftp://informatik.uni-hamburg.de)
 - ripem.msu.edu
 - garbo.uwasa.fi
 - [wimsey.bc.ca](ftp://wimsey.bc.ca)
 - ghost.dsi.unimi.it
- <http://rsa.com>
- PC Expo disk package to [ftp.wimsey.bc.ca](ftp://ftp.wimsey.bc.ca) [Arsen Ray Arachelian, 1994-07-05]
- + PC Expo disk

- ftp.wimsey.bc.ca
 - /pub/crypto/software/dist/US_or_Canada_only_XXXXXXXX/pcxpo/pcxpo.zip
- "The FTP site ripem.msu.edu has a bunch of crypto stuff."
 - [Mark Riordan, 1994-07-08]
- + URL for "Applied Cryptography"-related files
 - http://www.openmarket.com/info/cryptography/applied_cryptography.html
- 19.3.4. PGP Information and Sites
 - + <http://www.mantis.co.uk/pgp/pgp.html>
 - information on where to find PGP
 - + pgpinfo@mantis.co.uk
 - send any mail to this site and receive a list back of PGP sites
 - PGP info: [ftp.netcom.com](ftp://ftp.netcom.com), in /pub/gbe and in /pub/qwerty
 - more PGP:
 - ftp://csn.org//mpj/I_will_not_export/crypto_???????/pgp
 - <Michael Paul Johnson, mpj@csn.org, Colorado Catacombs, 4-8-94>
 - For non-U.S. sources of PGP: send blank mail to pgpinfo@mantis.co.uk
 - + Sherry Mayo, a crypto researcher in Australia, is also making versions available:
 - "PGP2.6ui is available (I hope!) on my experimental WWW server, aim your browser at <http://rschp2.anu.edu.au:8080/crypt.html> I am new to this WWW thing so let me know if you have any probs downloading. Available on the server is: PGP2.6ui source for unix machines Executable for the PC version of PGP 2.6ui Executable for MacPGP 2.3" [Sherry Mayo, talk.politics.crypto, 1994-09-06]
- 19.3.5. Key Servers
 - + pgp-public-keys@demon.co.uk
 - HELP in the subject line for more information about how to use
 - pgp-public-keys@jpunix.com
 - + pgp-public-keys@pgp.iastate.edu
 - ``help'' as the subject, to get a list of key servers [Michael Graff <explorer@iastate.edu>, alt.security.pgp, 1994-07-04]
- 19.3.6. Remailer Sites
 - To show active remailers: finger_remailer@soda.berkeley.edu
- 19.3.7. Mail-to-Usenet gateways:
 - + group.name@paris.ics.uci.edu
 - group.name@cs.dal.ca
 - group.name@ug.cs.dal.ca
 - <compiled by Matthew J. Ghio, 4-18-94>
- 19.3.8. Government Information
 - + California Legislative Information
 - "You are invited to browse the new edition of my list of Internet and direct dial sources of California government information at URL: www.cpsr.org/cpsr/states/california/cal_gov_info_FAQ.html " [Chris Mays, comp.org.cpsr.talk, 1994-07-01]
 - + NSA Information

- Can get on NSA/NCSC/NIST mailing list by sending to:
 - csrc.nist.gov:/pub/nistpubs
- 19.3.9. Clipper Info
 - + <http://www.mantis.co.uk/~mathew/>
 - some good Clipper articles and testimony
- 19.3.10. Other
 - + <ftp://furmint.nectar.cs.cmu.edu/security/README.html#taxes>
 - Vincent Cate
 - <http://www.acns.nwu.edu/surfpunk/>
 - + Export Laws
 - "EFF Board member and Cygnus Support co-founder John Gilmore has set up a World Wide Web page on cryptography export issues, including information on how to apply for export clearance, exchanges with Commerce Dept. on export licensing, legal documents on networking issues in relation to export of technology and crypto, and more. The URL is: <http://www.cygnus.com/~gnu/export.html>" [Stanton McCandlish, mech@eff.org, 1994-04-21]
 - + Large integer math libraries
 - [ripem.msu.edu](mailto:mrr@scss3.cl.msu.edu) <Mark Riordan, mrr@scss3.cl.msu.edu, 4-8-94, sci.crypt>
 - [ftp:csn.org//mpj](mailto:mpj@csn.org) <Michael Paul Johnson, 4-8-94, sci.crypt>
 - + Phrack
 - archived at [ftp.netsys.com](ftp://netsys.com)
 - + Bruce Sterling's comments at CFP
 - + Bruce Sterling's remarks delivered at the "Computers, Freedom and Privacy IV"
 - conference , Mar. 26 1994 in Chicago, are now online at EFF:
 - ftp://ftp.eff.org/pub/Publications/Bruce_Sterling/cfp_94_sterling.speech
 - http://www.eff.org/pub/Publications/Bruce_Sterling/cfp_94_sterling.speech
 - gopher://gopher.eff.org/11/Publications/Bruce_Sterling/cfp_94_sterling.speech
 - [gopher.eff.org, 1/Publications/Bruce_Sterling, cfp_94_sterling.speech](gopher.eff.org,1/Publications/Bruce_Sterling,cfp_94_sterling.speech)
 - (source: Stanton McCandlish * mech@eff.org, 3-31-94)
- 19.3.11. Crypto papers
 - [ftp.cs.uow.edu.au](ftp://cs.uow.edu.au/pub/papers)
 - (quantum, other, Siberry, etc.)
- 19.3.12. CPSR URL
 - CPSR URL: <http://www.cpsr.org/home>
- 19.4. Appendix -- Glossary
 - 19.4.1. ****Comments****
 - Release Note: I regret that I haven't had time to add many new entries here. There are a lot of specialized terms, and I probably could have doubled the number of entries here.
 - Much more work is needed here. In fact, I debated at one point making the FAQ instead into a kind of "Encyclopedia Cypherpunkia," with a mix of short and long articles on each of hundreds of topics. Such an organization would suffer the disadvantages found in nearly all lexicographically-organized works: confusion of the

- concepts.
- Many of these entries were compiled for a long handout at the first Cypherpunks meeting, September, 1992. Errors are obviously present. I'll try to keep correcting them when I can.
 - Schneier's "Applied Cryptography" is of course an excellent place to browse for terms, special uses, etc.
- 19.4.2. agoric systems -- open, free market systems in which voluntary transactions are central.
 - 19.4.3. Alice and Bob -- cryptographic protocols are often made clearer by considering parties A and B, or Alice and Bob, performing some protocol. Eve the eavesdropper, Paul the prover, and Vic the verifier are other common stand-in names.
 - 19.4.4. ANDOS -- all or nothing disclosure of secrets.
 - 19.4.5. anonymous credential -- a credential which asserts some right or privilege or fact without revealing the identity of the holder. This is unlike CA driver's licenses.
 - 19.4.6. asymmetric cipher -- same as public key cryptosystem.
 - 19.4.7. authentication -- the process of verifying an identity or credential, to ensure you are who you said you were.
 - 19.4.8. biometric security -- a type of authentication using fingerprints, retinal scans, palm prints, or other physical/biological signatures of an individual.
 - 19.4.9. bit commitment -- e.g., tossing a coin and then committing to the value without being able to change the outcome. The blob is a cryptographic primitive for this.
 - 19.4.10. BlackNet -- an experimental scheme devised by T. May to underscore the nature of anonymous information markets. "Any and all" secrets can be offered for sale via anonymous mailers and message pools. The experiment was leaked via remailer to the Cypherpunks list (not by May) and thence to several dozen Usenet groups by Detweiler. The authorities are said to be investigating it.
 - 19.4.11. blinding, blinded signatures -- A signature that the signer does not remember having made. A blind signature is always a cooperative protocol and the receiver of the signature provides the signer with the blinding information.
 - 19.4.12. blob -- the crypto equivalent of a locked box. A cryptographic primitive for bit commitment, with the properties that a blob can represent a 0 or a 1, that others cannot tell whether it's a 0 or a 1, that the creator of the blob can "open" the blob to reveal the contents, and that no blob can be both a 1 and a 0. An example of this is a flipped coin covered by a hand.
 - 19.4.13. BnD --
 - 19.4.14. Capstone --
 - 19.4.15. channel -- the path over which messages are transmitted. Channels may be secure or insecure, and may have eavesdroppers (or enemies, or disrupters, etc.) who alter messages, insert and delete messages, etc. Cryptography is the means by which communications over insecure channels are protected.
 - 19.4.16. chosen plaintext attack -- an attack where the cryptanalyst gets to choose the plaintext to be enciphered, e.g., when possession of an enciphering machine or algorithm is in the possession of the cryptanalyst.
 - 19.4.17. cipher -- a secret form of writing, using substitution or

- transposition of characters or symbols. (From Arabic "sifr," meaning "nothing.")
- 19.4.18. ciphertext -- the plaintext after it has been encrypted.
 - 19.4.19. Clipper -- the infamous Clipper chip
 - 19.4.20. code -- a restricted cryptosystem where words or letters of a message are replaced by other words chosen from a codebook. Not part of modern cryptology, but still useful.
 - 19.4.21. coin flipping -- an important crypto primitive, or protocol, in which the equivalent of flipping a fair coin is possible. Implemented with blobs.
 - 19.4.22. collusion -- wherein several participants cooperate to deduce the identity of a sender or receiver, or to break a cipher. Most cryptosystems are sensitive to some forms of collusion. Much of the work on implementing DC Nets, for example, involves ensuring that colluders cannot isolate message senders and thereby trace origins and destinations of mail.
 - 19.4.23. COMINT --
 - 19.4.24. computationally secure -- where a cipher cannot be broken with available computer resources, but in theory can be broken with enough computer resources. Contrast with unconditionally secure.
 - 19.4.25. countermeasure -- something you do to thwart an attacker
 - 19.4.26. credential -- facts or assertions about some entity. For example, credit ratings, passports, reputations, tax status, insurance records, etc. Under the current system, these credentials are increasingly being cross-linked. Blind signatures may be used to create anonymous credentials.
 - 19.4.27. credential clearinghouse -- banks, credit agencies, insurance companies, police departments, etc., that correlate records and decide the status of records.
 - 19.4.28. cryptanalysis -- methods for attacking and breaking ciphers and related cryptographic systems. Ciphers may be broken, traffic may be analyzed, and passwords may be cracked. Computers are of course essential.
 - 19.4.29. crypto anarchy -- the economic and political system after the deployment of encryption, untraceable e-mail, digital pseudonyms, cryptographic voting, and digital cash. A pun on "crypto," meaning "hidden," and as when Gore Vidal called William F. Buckley a "crypto fascist."
 - 19.4.30. cryptography -- another name for cryptology.
 - 19.4.31. cryptology -- the science and study of writing, sending, receiving, and deciphering secret messages. Includes authentication, digital signatures, the hiding of messages (steganography), cryptanalysis, and several other fields.
 - 19.4.32. cyberspace -- the electronic domain, the Nets, and computer-generated spaces. Some say it is the "consensual reality" described in "Neuromancer." Others say it is the phone system. Others have work to do.
 - 19.4.33. DC protocol, or DC-Net -- the dining cryptographers protocol. DC-Nets use multiple participants communicating with the DC protocol.
 - 19.4.34. DES -- the Data Encryption Standard, proposed in 1977 by the National Bureau of Standards (now NIST), with assistance from the National Security Agency. Based on the "Lucifer" cipher developed by Horst Feistel at IBM, DES is a secret key cryptosystem that cycles 64-bit blocks of data through multiple permutations with a 56-bit key controlling the

routing. "Diffusion" and "confusion" are combined to form a cipher that has not yet been cryptanalyzed (see "DES, Security of"). DES is in use for interbank transfers, as a cipher inside of several RSA-based systems, and is available for PCs.

- 19.4.35. DES, Security of -- many have speculated that the NSA placed a trapdoor (or backdoor) in DES to allow it to read DES-encrypted messages. This has not been proved. It is known that the original Lucifer algorithm used a 128-bit key and that this key length was shortened to 64 bits (56 bits plus 8 parity bits), this making exhaustive search much easier (so far as is known, brute-force search has not been done, though it should be feasible today). Shamir and Biham have used a technique called "differential cryptanalysis" to reduce the exhaustive search needed for chosen plaintext attacks (but with no import for ordinary DES).
- 19.4.36. differential cryptanalysis -- the Shamir-Biham technique for cryptanalyzing DES. With a chosen plaintext attack, they've reduced the number of DES keys that must be tried from about 2^{56} to about 2^{47} or less. Note, however, that rarely can an attacker mount a chosen plaintext attack on DES systems.
- 19.4.37. digital cash, digital money -- Protocols for transferring value, monetary or otherwise, electronically. Digital cash usually refers to systems that are anonymous. Digital money systems can be used to implement any quantity that is conserved, such as points, mass, dollars, etc. There are many variations of digital money systems, ranging from VISA numbers to blinded signed digital coins. A topic too large for a single glossary entry.
- 19.4.38. digital pseudonym -- basically, a "crypto identity." A way for individuals to set up accounts with various organizations without revealing more information than they wish. Users may have several digital pseudonyms, some used only once, some used over the course of many years. Ideally, the pseudonyms can be linked only at the will of the holder. In the simplest form, a public key can serve as a digital pseudonym and need not be linked to a physical identity.
- 19.4.39. digital signature -- Analogous to a written signature on a document. A modification to a message that only the signer can make but that everyone can recognize. Can be used legally to contract at a distance.
- 19.4.40. digital timestamping -- one function of a digital notary public, in which some message (a song, screenplay, lab notebook, contract, etc.) is stamped with a time that cannot (easily) be forged.
- 19.4.41. dining cryptographers protocol (aka DC protocol, DC nets) -- the untraceable message sending system invented by David Chaum. Named after the "dining philosophers" problem in computer science, participants form circuits and pass messages in such a way that the origin cannot be deduced, barring collusion. At the simplest level, two participants share a key between them. One of them sends some actual message by bitwise exclusive-ORing the message with the key, while the other one just sends the key itself. The actual message from this pair of participants is obtained by XORing the two outputs. However, since nobody but the pair knows the original key, the actual message cannot be traced to either

- one of the participants.
- 19.4.42. discrete logarithm problem -- given integers a , n , and x , find some integer m such that $a^m \bmod n = x$, if m exists. Modular exponentiation, the $a^m \bmod n$ part, is straightforward (and special purpose chips are available), but the inverse problem is believed to be very hard, in general. Thus it is conjectured that modular exponentiation is a one-way function.
 - 19.4.43. DSS, Digital Signature Standard -- the latest NIST (National Institute of Standards and Technology, successor to NBS) standard for digital signatures. Based on the El Gamal cipher, some consider it weak and poor substitute for RSA-based signature schemes.
 - 19.4.44. eavesdropping, or passive wiretapping -- intercepting messages without detection. Radio waves may be intercepted, phone lines may be tapped, and computers may have RF emissions detected. Even fiber optic lines can be tapped.
 - 19.4.45. Escrowed Encryption Standard (EES) -- current name for the key escrow system known variously as Clipper, Capstone, Skipjack, etc.
 - 19.4.46. factoring -- Some large numbers are difficult to factor. It is conjectured that there are no feasible--i.e."easy," less than exponential in size of number-- factoring methods. It is also an open problem whether RSA may be broken more easily than by factoring the modulus (e.g., the public key might reveal information which simplifies the problem). Interestingly, though factoring is believed to be "hard", it is not known to be in the class of NP-hard problems. Professor Janek invented a factoring device, but he is believed to be fictional.
 - 19.4.47. HUMINT --
 - 19.4.48. information-theoretic security -- "unbreakable" security, in which no amount of cryptanalysis can break a cipher or system. One time pads are an example (providing the pads are not lost nor stolen nor used more than once, of course). Same as unconditionally secure.
 - 19.4.49. key -- a piece of information needed to encipher or decipher a message. Keys may be stolen, bought, lost, etc., just as with physical keys.
 - 19.4.50. key exchange, or key distribution -- the process of sharing a key with some other party, in the case of symmetric ciphers, or of distributing a public key in an asymmetric cipher. A major issue is that the keys be exchanged reliably and without compromise. Diffie and Hellman devised one such scheme, based on the discrete logarithm problem.
 - 19.4.51. known-plaintext attack -- a cryptanalysis of a cipher where plaintext-ciphertext pairs are known. This attack searches for an unknown key. Contrast with the chosen plaintext attack, where the cryptanalyst can also choose the plaintext to be enciphered.
 - 19.4.52. listening posts -- the NSA and other intelligence agencies maintain sites for the interception of radio, telephone, and satellite communications. And so on. Many sites have been identified (cf. Bamford), and many more sites are suspected.
 - 19.4.53. mail, untraceable -- a system for sending and receiving mail without traceability or observability. Receiving mail anonymously can be done with broadcast of the mail in

encrypted form. Only the intended recipient (whose identity, or true name, may be unknown to the sender) may be able to decipher the message. Sending mail anonymously apparently requires mixes or use of the dining cryptographers (DC) protocol.

- 19.4.54. Message Pool
- 19.4.55. minimum disclosure proofs -- another name for zero knowledge proofs, favored by Chaum.
- 19.4.56. mixes -- David Chaum's term for a box which performs the function of mixing, or decorrelating, incoming and outgoing electronic mail messages. The box also strips off the outer envelope (i.e., decrypts with its private key) and remails the message to the address on the inner envelope. Tamper-resistant modules may be used to prevent cheating and forced disclosure of the mapping between incoming and outgoing mail. A sequence of many remailings effectively makes tracing sending and receiving impossible. Contrast this with the software version, the DC protocol. The "remailers" developed by Cypherpunks are an approximation of a Chaumian mix.
- 19.4.57. modular exponentiation -- raising an integer to the power of another integer, modulo some integer. For integers a , n , and m , $a^m \bmod n$. For example, $5^3 \bmod 100 = 25$. Modular exponentiation can be done fairly quickly with a sequence of bit shifts and adds, and special purpose chips have been designed. See also discrete logarithm.
- 19.4.58. National Security Agency (NSA) -- the largest intelligence agency, responsible for making and breaking ciphers, for intercepting communications, and for ensuring the security of U.S. computers. Headquartered in Fort Meade, Maryland, with many listening posts around the world. The NSA funds cryptographic research and advises other agencies about cryptographic matters. The NSA once obviously had the world's leading cryptologists, but this may no longer be the case.
- 19.4.59. negative credential -- a credential that you possess that you don't want any one else to know, for example, a bankruptcy filing. A formal version of a negative reputation.
- 19.4.60. NP-complete -- a large class of difficult problems. "NP" stands for nondeterministic polynomial time, a class of problems thought in general not to have feasible algorithms for their solution. A problem is "complete" if any other NP problem may be reduced to that problem. Many important combinatorial and algebraic problems are NP-complete: the travelling salesman problem, the Hamiltonian cycle problem, the graph isomorphism problem, the word problem, and on and on.
- 19.4.61. oblivious transfer -- a cryptographic primitive that involves the probabilistic transmission of bits. The sender does not know if the bits were received.
- 19.4.62. one-time pad -- a string of randomly-selected bits or symbols which is combined with a plaintext message to produce the ciphertext. This combination may be shifting letters some amount, bitwise exclusive-ORed, etc.). The recipient, who also has a copy of the one time pad, can easily recover the plaintext. Provided the pad is only used once and then destroyed, and is not available to an eavesdropper, the system is perfectly secure, i.e., it is information-theoretically secure. Key distribution (the pad) is

- obviously a practical concern, but consider CD-ROM's.
- 19.4.63. one-way function -- a function which is easy to compute in one direction but hard to find any inverse for, e.g. modular exponentiation, where the inverse problem is known as the discrete logarithm problem. Compare the special case of trap door one-way functions. An example of a one-way operation is multiplication: it is easy to multiply two prime numbers of 100 digits to produce a 200-digit number, but hard to factor that 200-digit number.
 - 19.4.64. P ==? NP -- Certainly the most important unsolved problem in complexity theory. If $P = NP$, then cryptography as we know it today does not exist. If $P \neq NP$, all NP problems are "easy."
 - 19.4.65. padding -- sending extra messages to confuse eavesdroppers and to defeat traffic analysis. Also adding random bits to a message to be enciphered.
 - 19.4.66. PGP
 - 19.4.67. plaintext -- also called cleartext, the text that is to be enciphered.
 - 19.4.68. Pool
 - 19.4.69. Pretty Good Privacy (PGP) -- Phillip Zimmerman's implementation of RSA, recently upgraded to version 2.0, with more robust components and several new features. RSA Data Security has threatened PZ so he no longer works on it. Version 2.0 was written by a consortium of non-U.S. hackers.
 - 19.4.70. prime numbers -- integers with no factors other than themselves and 1. The number of primes is unbounded. About 1% of the 100 decimal digit numbers are prime. Since there are about 10^{70} particles in the universe, there are about 10^{23} 100 digit primes for each and every particle in the universe!
 - 19.4.71. probabilistic encryption -- a scheme by Goldwasser, Micali, and Blum that allows multiple ciphertexts for the same plaintext, i.e., any given plaintext may have many ciphertexts if the ciphering is repeated. This protects against certain types of known ciphertext attacks on RSA.
 - 19.4.72. proofs of identity -- proving who you are, either your true name, or your digital identity. Generally, possession of the right key is sufficient proof (guard your key!). Some work has been done on "is-a-person" credentialling agencies, using the so-called Fiat-Shamir protocol...think of this as a way to issue unforgeable digital passports. Physical proof of identity may be done with biometric security methods. Zero knowledge proofs of identity reveal nothing beyond the fact that the identity is as claimed. This has obvious uses for computer access, passwords, etc.
 - 19.4.73. protocol -- a formal procedure for solving some problem. Modern cryptology is mostly about the study of protocols for many problems, such as coin-flipping, bit commitment (blobs), zero knowledge proofs, dining cryptographers, and so on.
 - 19.4.74. public key -- the key distributed publicly to potential message-senders. It may be published in a phonebook-like directory or otherwise sent. A major concern is the validity of this public key to guard against spoofing or impersonation.
 - 19.4.75. public key cryptosystem -- the modern breakthrough in cryptology, designed by Diffie and Hellman, with

contributions from several others. Uses trap door one-way functions so that encryption may be done by anyone with access to the "public key" but decryption may be done only by the holder of the "private key." Encompasses public key encryption, digital signatures, digital cash, and many other protocols and applications.

- 19.4.76. public key encryption -- the use of modern cryptologic methods to provided message security and authentication. The RSA algorithm is the most widely used form of public key encryption, although other systems exist. A public key may be freely published, e.g., in phonebook-like directories, while the corresponding private key is closely guarded.
- 19.4.77. public key patents -- M.I.T. and Stanford, due to the work of Rivest, Shamir, Adleman, Diffie, Hellman, and Merkle, formed Public Key Partners to license the various public key, digital signature, and RSA patents. These patents, granted in the early 1980s, expire in the between 1998 and 2002. PKP has licensed RSA Data Security Inc., of Redwood City, CA, which handles the sales, etc.
- 19.4.78. quantum cryptography -- a system based on quantum-mechanical principles. Eavesdroppers alter the quantum state of the system and so are detected. Developed by Brassard and Bennett, only small laboratory demonstrations have been made.
- 19.4.79. remailers -- software versions of Chaum's "mixes," for the sending of untraceable mail. Various features are needed to do this: randomized order of resending, encryption at each stage (picked in advance by the sender, knowing the chain of remailers), padding of message sizes. The first remailer was written by E. Hughes in perl, and about a dozen or so are active now, with varying feature sets.
- 19.4.80. reputations -- the trail of positive and negative associations and judgments that some entity accrues. Credit ratings, academic credentials, and trustworthiness are all examples. A digital pseudonym will accrue these reputation credentials based on actions, opinions of others, etc. In crypto anarchy, reputations and agoric systems will be of paramount importance. There are many fascinating issues of how reputation-based systems work, how credentials can be bought and sold, and so forth.
- 19.4.81. RSA -- the main public key encryption algorithm, developed by Ron Rivest, Adi Shamir, and Kenneth Adleman. It exploits the difficulty of factoring large numbers to create a private key and public key. First invented in 1978, it remains the core of modern public key systems. It is usually much slower than DES, but special-purpose modular exponentiation chips will likely speed it up. A popular scheme for speed is to use RSA to transmit session keys and then a high-speed cipher like DES for the actual message text.
 - Description -- Let p and q be large primes, typically with more than 100 digits. Let $n = pq$ and find some e such that e is relatively prime to $(p - 1)(q - 1)$. The set of numbers p , q , and e is the private key for RSA. The set of numbers n and e forms the public key (recall that knowing n is not sufficient to easily find p and q ...the factoring problem). A message M is encrypted by computing $M^e \bmod n$. The owner of the private key can decrypt the encrypted message by exploiting number theory results, as follows. An integer d

is computed such that $ed \equiv 1 \pmod{(p-1)(q-1)}$. Euler proved a theorem that $M^{ed} \equiv M \pmod{n}$ and so $M^{ed} \pmod{n} = M$. This means that in some sense the integers e and d are "inverses" of each other. [If this is unclear, please see one of the many texts and articles on public key encryption.]

- 19.4.82. secret key cryptosystem -- A system which uses the same key to encrypt and decrypt traffic at each end of a communication link. Also called a symmetric or one-key system. Contrast with public key cryptosystem.
- 19.4.83. SIGINT --
- 19.4.84. smart cards -- a computer chip embedded in credit card. They can hold cash, credentials, cryptographic keys, etc. Usually these are built with some degree of tamper-resistance. Smart cards may perform part of a crypto transaction, or all of it. Performing part of it may mean checking the computations of a more powerful computer, e.g., one in an ATM.
- 19.4.85. spoofing, or masquerading -- posing as another user. Used for stealing passwords, modifying files, and stealing cash. Digital signatures and other authentication methods are useful to prevent this. Public keys must be validated and protected to ensure that others don't substitute their own public keys which users may then unwittingly use.
- 19.4.86. steganography -- a part of cryptology dealing with hiding messages and obscuring who is sending and receiving messages. Message traffic is often padded to reduce the signals that would otherwise come from a sudden beginning of messages. "Covered writing."
- 19.4.87. symmetric cipher -- same as private key cryptosystem.
- 19.4.88. tamper-responding modules, tamper-resistant modules (TRMs) -- sealed boxes or modules which are hard to open, requiring extensive probing and usually leaving ample evidence that the tampering has occurred. Various protective techniques are used, such as special metal or oxide layers on chips, armored coatings, embedded optical fibers, and other measures to thwart analysis. Popularly called "tamper-proof boxes." Uses include: smart cards, nuclear weapon initiators, cryptographic key holders, ATMs, etc.
- 19.4.89. tampering, or active wiretapping -- interfering with messages and possibly modifying them. This may compromise data security, help to break ciphers, etc. See also spoofing.
- 19.4.90. Tessera
- 19.4.91. token -- some representation, such as ID cards, subway tokens, money, etc., that indicates possession of some property or value.
- 19.4.92. traffic analysis -- determining who is sending or receiving messages by analyzing packets, frequency of packets, etc. A part of steganography. Usually handled with traffic padding.
- 19.4.93. traffic analysis -- identifying characteristics of a message (such as sender, or destination) by watching traffic. Remailers and encryption help to foil traffic analysis.
- 19.4.94. transmission rules -- the protocols for determining who can send messages in a DC protocol, and when. These rules are needed to prevent collision and deliberate jamming of the channels.
- 19.4.95. trap messages -- dummy messages in DC Nets which are used to catch jammers and disrupters. The messages contain no private

information and are published in a blob beforehand so that the trap message can later be opened to reveal the disrupter. (There are many strategies to explore here.)

- 19.4.96. trap-door -- In cryptography, a piece of secret information that allows the holder of a private key to invert a normally hard to invert function.
- 19.4.97. trap-door one way functions -- functions which are easy to compute in both the forward and reverse direction but for which the disclosure of an algorithm to compute the function in the forward direction does not provide information on how to compute the function in the reverse direction. More simply put, trap-door one way functions are one way for all but the holder of the secret information. The RSA algorithm is the best-known example of such a function.
- 19.4.98. unconditional security -- same as information-theoretic security, that is, unbreakable except by loss or theft of the key.
- 19.4.99. unconditionally secure -- where no amount of intercepted ciphertext is enough to allow the cipher to be broken, as with the use of a one-time pad cipher. Contrast with computationally secure.
- 19.4.100. URLs
- 19.4.101. voting, cryptographic -- Various schemes have been devised for anonymous, untraceable voting. Voting schemes should have several properties: privacy of the vote, security of the vote (no multiple votes), robustness against disruption by jammers or disrupters, verifiability (voter has confidence in the results), and efficiency.
- 19.4.102. Whistleblowers
- 19.4.103. zero knowledge proofs -- proofs in which no knowledge of the actual proof is conveyed. Peggy the Prover demonstrates to Sid the Skeptic that she is indeed in possession of some piece of knowledge without actually revealing any of that knowledge. This is useful for access to computers, because eavesdroppers or dishonest sysops cannot steal the knowledge given. Also called minimum disclosure proofs. Useful for proving possession of some property, or credential, such as age or voting status, without revealing personal information.

19.5. Appendix -- Summary of Crypto Versions

19.5.1. DOS and Windows

- SecureDevice
- + SecureDrive
 - "Secdrv13d is the latest version. There was an unupdated .exe file in the package that had to be fixed. From the readme file: If you found this file inside FPART13D.ZIP, this is an update and bug fix for the FPART utility of SecureDrive Release 1.3d,
 - Edgar Swank involved?
- + SecureDevice
 - Major Versions:
 - Functions:
 - Principal Authors:
 - Major Platforms:
- + Where to Find:
 - ftp://ftp.csn.org/mpj/I_will_not_export/crypto_???????/secdrv/secdev.arj

- See ftp://ftp.csn.org/mpj/README.MPJ for the ????????
- Strengths:
 - Weaknesses:
 - + Notes:
 - By the way, I'm not the only one who gets SecureDrive and SecureDevice confused. Watch out for this.
 - + SFS
 - "A MS-DOS-based package for hard disk encryption. It is implemented as a device driver and encrypts a whole partition (i.e., not a file or a directory). It uses the MDC/SHA cipher. ... It is available from Garbo (garbo.uwasa.fi:/pc/encrypt/sfs110.zip, I think), and also from our ftp site: ftp.informatik.uni-hamburg.de:/pub/virus/encrypt/disk/sfs110.zip I would recommend the Garbo site, because ours is a bit slow." [Vesselin Bontchev, alt.security.pgp, 1994-09-05]
 - Compared to SecureDrive, users report it to be faster, better-featured, has a Windows interface, is a device driver, and is robust. The disadvantages are that it currently does not ship with source code and uses a more obscure cipher.
 - "SFS (Secure FileSystem) is a set of programs which create and manage a number of encrypted disk volumes, and runs under both DOS and Windows. Each volume appears as a normal DOS drive, but all data stored on it is encrypted at the individual-sector level....SFS 1.1 is a maintenance release which fixes a few minor problems in 1.0, and adds a number of features suggested by users. More details on changes are given in in the README file." [Peter Gutmann, sci.crypt, 1994-08-25]
 - "from garbo.uwasa.fi and all its mirror sites worldwide as /pc/encrypt/sfs110.zip."
 - + WinCrypt.
 - "WinCrypt is pretty good IF you keep your encrypted text to less than the length of your password, AND IF you generate your password randomly, AND IF you only use each password ONCE. :-)" [Michael Paul Johnson, sci.crypt, 1994-07-08]
 - + Win PGP
 - + there seem to be two identically-named programs:
 - WinPGP, by Christopher w. Geib
 - + WinPGP, by Timothy M. Janke and Geoffrey C. Grabow
 - ftp WinPGP 1.0 from oak.oakland.edu:/pub/msdos/windows3/WinPGP10.ZIP
 - Until this is clarified...
 - + PGPShell
 - "PGPShell v3.2 has been released and is available at these sites: (U.S.) oak.oakland.edu:/pub/msdos/security/pgpshe32.zip (Euro) ftp.demon.co.uk:/sintel20/msdos/security/pgpshe32.zip [still@rintintin.Colorado.EDU (Johannes Kepler), 1994-07-07]
 - + PGS
 - ftp.informatik.uni-hamburg.de:/pub/virus/encrypt/pgp/shells/pgs099b.zip
 - "I just uploaded the bug fix of PGS (v0.99b) on some FTP-

sites:

wuarchive.wustl.edu:/pub/msdos_uploads/pgs/pgs099b.zip
rzsun2.informatik.uni-hamburg.de:/pub/virus/crypt/pgp/...
(Just uploaded it, should be on in a few days)
oak.oakland.edu:/SimTel/msdos/security/pgs099b.zip (Just
uploaded it, should be on in a few days)

[Eelco Cramer <crame001@hio.tem.nhl.nl>, 1994-06-27]

- + DOS disk encryption utilities
- + Several free or nearly free utilities are available:
 - ftp.informatik.uni-hamburg.de:/pub/virus/crypt/disk/
[Vesselin Vladimirov Bontchev, as of 1994-08]
- + Norton's "Diskreet" is weak and essentially useless
 - uses DES in weak (ECB) mode...is probably the "snake
oil" that Zimmermann writes about in his docs. SFS docs
say it is even worse than that.
- + PGS
 - "PGS v0.99c is out there!

This new version of PGS supports 8 bytes keyid's.
This version will be able to run in a OS/2 DOS box.

PGS v0.99c is available on the following site:
wuarchive.wustl.edu:/pub/msdos_uploads/pgs/pgs099c.zip"
[ER CRAMER <crame001@hio.tem.nhl.nl>, 1994-07-08]

- + Program:
 - Major Versions:
 - Functions:
 - Principal Authors:
 - Major Platforms:
 - Where to Find:
 - Strengths:
 - Weaknesses:
 - Notes:

19.5.2. OS/2

19.5.3. Amiga

- + Program: PGPAmiga, Amiga PGP
- + Major Versions: 2.3a.4, PGP 2.6
 - "The Amiga equivalent of PGP 2.6ui is called PGP
2.3a.3" [unknown commenter]
- Functions:
- Principal Authors:
- Major Platforms:
- Where to Find:
- Strengths:
- Weaknesses:
- Notes: Situation is confusing. 2.3a.3 is not equivalent
to PGP 2.6ui.

19.5.4. Unix

- NeXTStep
- Sun 4.3
- Solaris
- HP
- SGI
- + swIPE

- Metzger: It was John Ioannidis' swIPE package, and it was not merely announced but released. Phil has done a similar package for KA9Q and was one of

19.5.5. SFS ?

- "A MS-DOS-based package for hard disk encryption. It is implemented as a device driver and encrypts a whole partition (i.e., not a file or a directory). It uses the MDC/SHA cipher. ... It is available from Garbo (garbo.uwasa.fi:/pc/crypt/sfs110.zip, I think), and also from our ftp site: ftp.informatik.uni-hamburg.de:/pub/virus/crypt/disk/sfs110.zip I would recommend the Garbo site, because ours is a bit slow." [Vesselin Bontchev, alt.security.pgp, 1994-09-05]

19.5.6. Macintosh

+ more on MacPGP

- From: phinely@uhunix.uhcc.Hawaii.Edu (Peter Hinely)
Subject: Re: MacPGP 2.6ui doesn't actually work
Message-ID: <CsI3wr.I3B@news.Hawaii.Edu>
Sender: news@news.Hawaii.Edu
Organization: University of Hawaii
References: <m0qJqLD-001JKsC@sunforest.mantis.co.uk>
Date: Wed, 6 Jul 1994 04:17:15 GMT
Lines: 9

In article <m0qJqLD-001JKsC@sunforest.mantis.co.uk> mathew@stallman.mantis.co.uk (mathew at home) writes:
>Well, I downloaded the rumoured MacPGP 2.6ui, but sadly it bombs out
>immediately with an address error when I try to run it.

MacPGP 2.6ui works on my Quadra 605.
The MacBinary process cannot handle pathnames >63 characters, but as long as you encrypt files on the desktop, it's not too much of a problem.

- From: warlord@MIT.EDU (Derek Atkins)
Newsgroups: alt.security.pgp
Subject: Re: When will there be a bug fix for MacPGP?
Followup-To: alt.security.pgp
Date: 6 Jul 1994 10:19:13 GMT
Organization: Massachusetts Institute of Technology
Lines: 19
Message-ID: <WARLORD.94Jul6061917@toxicwaste.mit.edu>
References: <AWILSON-020794082446@ts7-57.upenn.edu>
NNTP-Posting-Host: toxicwaste.media.mit.edu
In-reply-to: AWILSON@DRUNIVAC.DREW.EDU's message of 2 Jul 1994 12:25:14 GMT

In article <AWILSON-020794082446@ts7-57.upenn.edu> AWILSON@DRUNIVAC.DREW.EDU (AL WILSON) writes:

When will there be a bug fix for MacPGP (1.1.1)? I am not complaining, I know that the software is free. I just want to start utilizing it for communications at the earliest possible time.

There are still a number of outstanding bugs that need to be fixed, but the hope is to make a bugfix release in the near future. I don't know when that is going to be, but hopefully it will be Real Soon Now (TM).

- Date: Wed, 6 Jul 1994 10:42:08 -0700
From: tcmay (Timothy C. May)
To: tcmay
Subject: (fwd) Re: What is the difference between 2.6 & 2.6ui?
Newsgroups: alt.security.pgp
Organization: NETCOM On-line Communication Services (408 261-4700 guest)
Status: 0

Xref: netcom.com alt.security.pgp:16979
Path: netcom.com!netcomsv!decwrl!lll-winken.llnl.gov!sol.ctr.columbia.edu!howland.reston.ans.net!pipex!lyra.csx.cam.ac.uk!iwj10
From: iwj10@cus.cam.ac.uk (Ian Jackson)
Newsgroups: alt.security.pgp
Subject: Re: What is the difference between 2.6 & 2.6ui?
Date: Wed, 6 Jul 1994 10:14:24 GMT
Organization: Linux Unlimited
Lines: 55
Message-ID:
<1994Jul6.101424.9203.chiark.ijackson@nyx.cs.du.edu>
References: <CsE3CC.Gqz@crash.cts.com>
<RATINOX.94Jul3221136@delphi.ccs.neu.edu>
NNTP-Posting-Host: bootes.cus.cam.ac.uk
Summary: Use 2.6ui :-).
Originator: iwj10@bootes.cus.cam.ac.uk

-----BEGIN PGP SIGNED MESSAGE-----

In article <RATINOX.94Jul3221136@delphi.ccs.neu.edu>, Stainless Steel Rat <ratinox@ccs.neu.edu> wrote:
>Ed Dantes <edantes@crash.cts.com> writes [quoting normalised - iwj]:
>> subject line says it all.
>
>PGP 2.6 is distributed from MIT and is legally available to US and Canadian residents. It uses the RSAREF library. It has code that will prevent interoperation with earlier versions of PGP.
>
>PGP 2.6ui is a modified version of PGP 2.3a which functions almost identically to MIT PGP 2.6, without the "cripple code" of MIT PGP 2.6. It is legally available outside the US and Canada only.

This is false. PGP 2.6ui is available to US and Canadian

residents.

It is definitely legal for such people to download PGP 2.6ui and study it.

However, RSADSI claim that *using* PGP 2.6ui in the US and Canada violates their patents on the RSA algorithm and on public key cryptography in general. Other people (like myself) believe that these patents wouldn't stand up if tested in court, and that in any case the damages recoverable would be zero.

You might also like to know that the output formats generated by 2.6ui and MIT-2.6 are identical, so that if you choose to use 2.6ui in North America noone will be able to tell the difference anyway.

Unfortunately these patent problems have caused many North American FTP sites to stop carrying 2.3a and 2.6ui, for fear of committing contributory infringement.

If you would like to examine PGP 2.3a or 2.6ui, they are available on many FTP sites. Try
black.ox.ac.uk:/src/security
ftp.demon.co.uk:/pub/pgp
ftp.dsi.unimi.it:/pub/security/crypt/PGP
ftp.funet.fi:/pub/crypt
for starters. Look out for the regular postings here in alt.security.pgp for other sites.

-----BEGIN PGP SIGNATURE-----

Version: 2.6

iQCVAgUBLhqD48MWjroj9a3bAQH9VgQAqOvCVXqJLhnFvsKfr82M5808h
6GKY5RW
SZ1/YLmshlDEMgeab4pSLSz+lDvsox2KFxQkP7O3oWYnswXcdr4FdLBu/
TXU+IQw
E4r/jY/IXSupP97Lxj9BB73TkJIHVmrqgoPQG2Nszj60cbE/LsiGs5uMn
CSESypH
c0Y8FnR64gc=
=Pejo

-----END PGP SIGNATURE-----

--

Ian Jackson, at home <ijackson@nyx.cs.du.edu> or
<iwj10@cus.cam.ac.uk>
+44 223 575512 Escoerea on IRC.
<http://www.cl.cam.ac.uk/users/iwj10/>
2 Lexington Close, Cambridge, CB4 3LS, England. Urgent:
<iwj@cam-orl.co.uk>

--

.....
.....
Timothy C. May | Crypto Anarchy: encryption,
digital money,
tcmay@netcom.com | anonymous networks, digital
pseudonyms, zero
408-688-5409 | knowledge, reputations,
information markets,
W.A.S.T.E.: Aptos, CA | black markets, collapse of
governments.
Higher Power: 2^859433 | Public Key: PGP and MailSafe
available.
"National borders are just speed bumps on the information
superhighway."

+ CurveEncrypt, for Mac

- "Curve Encrypt 1.1, IDEA encryption for the Macintosh is now available.....Curve Encrypt is a freeware drag-and-drop encryption application for the Macintosh. It uses IDEA cipher-feedback mode with a 255 character pass phrase, encrypts both the data and resource forks of files, and will encrypt the contents of a folder or volume in a single operation. Source code is provided, natch. CE is System 7 only....(Note that this program has nothing whatsoever to do with elliptic curve encryption methods, just so nobody gets confused...)" ["W. Kinney" <kinney@bogart.Colorado.EDU>, 1994-07-08]
- "Ftp Sites:

ripem.msu.edu:pub/crypt/other/curve-encrypt-idea-for-mac/
This is an export controlled ftp site: read
pub/crypt/GETTING_ACCESS for
information.

ftp.csn.org:/mpj/I_will_not_export/crypto_??????/curve_e
ncrypt/
csn.org is also export-controlled: read /mpj/README for
the characters
to replace ??????." ["W. Kinney"
<kinney@bogart.Colorado.EDU>, 1994-07-08]

+ RIPEM on Macintosh

- Carl Ellison says "I've only used RIPEM on AOL -- but it should be the same....I run on a Mac, generating the armored file, and then use AOL's "paste from file" option in the File menu to include the encrypted file in the body of my message.....In the other direction, I have to use Select All and Copy to get it out of AOL mail, Paste to get it into an editor. From there I can file it and give that file to PGP or RIPEM.....BBEDIT on the Mac has good support for RIPEM. I wish I knew how to write BBEDIT extensions for Mac PGP as well." [C.E., 1994-07-06]

+ URL for Stego (Macintosh)

- <http://www.nitv.net/~mech/Romana/stego.html>
- 19.5.7. Newton
- 19.5.8. Atari
- 19.5.9. VMS
- 19.5.10. IBM VM/etc.
- 19.5.11. Miscellaneous
- 19.5.12. File-splitting utilities
 - + Several exist.
 - XSPLIT
 - cryptosplit, Ray Cromwell
 - shade
- 19.6. Appendix -- References
- 19.6.1. the importance of libraries
 - "Use a library. That's a place with lots of paper periodicals and paper books. Library materials not online, mostly, but it is still where most of the world's encoded knowledge is stored. If you don't like paper, tough. That's the way the world is right now." [Eric Hughes, 1994-04-07]
- 19.6.2. Books
 - Bamford, James, "The Puzzle Palace," 1982. The seminal reference on the NSA.
 - N. Koblitz, "A course in number theory and cryptography", QA3.G7N0.114. Very technical, with an emphasis on elliptic functions.
 - + D. Welsh, "Codes and Cryptography", Oxford Science Publications, 1988, Eric Hughes especially recommends this.
 - Z103.W461988
 - D.E. Denning, "Cryptography and Data Security", 1982, Addison-Wesley, 1982, QA76.9.A25D46. A classic, if a bit dated, introduction by the woman who later became the chief supporter of Clipper.
 - + G. Brassard, "Modern Cryptology: a tutorial", Lecture Notes in Computer
 - Science 325, Springer 1988, QA76.L4V.325 A slim little book that's a gem. Sections by David Chaum.
 - Vinge, V., "True Names," 1981. A novel about digital pseudonyms and cyberspace.
 - Card, Orson Scott, "Ender's Game," 1985-6. Novel about kids who adopt digital pseudonyms for political debate.
 - G.J. Simmons, "Contemporary Cryptology", IEEE Press, 1992, QA76.9.A25C6678. A collection of articles by well-known experts. Surprisingly, no discussion of digital money. Gus Simmons designed "Permissive Action Links" for nukes, at Sandia.
- 19.6.3. sci.crypt
 - archived at ripem.msu.edu and rpub.cl.msu.edu
 -
 - + The cryptography anon ftp archive at
 - wimsey.bc.ca:/pub/crypto
 - has been moved to ftp.wimsey.bc.ca
- 19.6.4. cryptography-faq
 - in about 10 parts, put out by Crypt Cabal (several Cypherpunks on it)
 - rtfm.mit.edu, in /pub/usenet/news.answers/cryptography-

- faq/part[xx]
- + posted every 21 days to sci.crypt, talk.politics.crypto,
 - sci.answers, news.answers
- 19.6.5. RSA FAQ
 - Paul Fahn, RSA Laboratories
 - anonymous FTP to rsa.com:/pub/faq
 - rtfm.mit.edu, /pub/usenet/news.answers/cryptography-faq/rsa
- 19.6.6. Computers, Freedom and Privacy Conference
 - next Computers, Freedom and Privacy Conference will be March 1995, San Francisco
- 19.6.7. Various computer security papers, publications, and programs can be found at cert.org.
 - anonymous ftp to it and look in /pub. /pub/info even has the NSA "Orange Book." (Not a secret, obviously. Anyone can get on the NSA/NCSC's mailing list and get a huge pile of documents sent to them, with new ones arriving every several weeks.)
 - or try ftp.win.tue.nl /pub/security
- 19.6.8. Clipper information by Internet
 - ftp.cpsr.org
 - ftp.eff.org
- 19.7. Glossary Items
 - 19.7.1. message pools --
 - 19.7.2. pools -- see "message pools."
 - 19.7.3. cover traffic --
 - 19.7.4. padding -- see "message padding."
 - 19.7.5. message padding --
 - 19.7.6. latency --
 - 19.7.7. BlackNet -- an experiment in information markets, using anonymous message pools for exchange of instructions and items. Tim May's experiment in guerilla ontology.
 - 19.7.8. ILF -- Information Liberation Front. Distributes copyrighted material via remailers, anonymously. Another experiment in guerilla ontology.
 - 19.7.9. digital mix --
 - 19.7.10. FinCEN -- Financial Crimes Enforcement Network.
 - 19.7.11. true name -- one's actual, physical name. Taken from Vernor Vinge's novel of the same name.
 - 19.7.12. mix --
 - 19.7.13. TEMPEST --
 - 19.7.14. OTP --
 - 19.7.15. Vernam cipher --
 - 19.7.16. detweiler -- verb, to rant and rave about tentacles that are destroying one's sanity through crypto anarchist thought control. Named after L. Detweiler. "He's just detweilering."
 - 19.7.17. remailer --
 - 19.7.18. Stego --
 - 19.7.19. incipits -- message indicators or tags (relates to stego)
 - 19.7.20. duress code -- a second key which can decrypt a message to something harmless. Could be useful for bank cards, as well as for avoiding incrimination. A form of security through obscurity, and not widely used.
- 19.8. A comment on software versions, ftp sites, instructions, etc.
 - 19.8.1. I regret that I can't be complete in all versions, platforms supported, sites for obtaining, instructions,

incompatibilities, etc. Frankly, I'm drowning in reports of new versions, questions about use, etc. Most of these versions I have no direct knowledge of, have no experience with, and no appreciation of subtle incompatibilities involved.

19.8.2. There are others who have concentrated on providing up-to-date reports on what is available. Some of them are"

- site

19.8.3. Reading sci.crypt, alt.security.pgp, and related groups for a few weeks and looking for programs of interest to one's own situation should give the most recent and current results. Things are moving quickly, so if one is interested in "AmigaPGP," for example, then the right place to look for the latest versions is in the groups just mentioned, or in groups and ftp sites specific to the Amiga. (Be careful that sabotaged or spoofed versions are not used, as in all crypto. "Joe's AmigaPGP" might need a closer look.)

20. README

20.1. copyright

THE CYPHERNOMICON: Cypherpunks FAQ and More, Version 0.666, 1994-09-10, Copyright Timothy C. May. All rights reserved. See the detailed disclaimer. Use short sections under "fair use" provisions, with appropriate credit, but don't put your name on my words.

20.2. README--BRIEF VERSION

20.2.1. Copyright Timothy C. May. All rights reserved. For what it's worth.

20.2.2. Apologies in advance for the mix of styles (outline, bullet, text, essays), for fragments and incomplete sections. This FAQ is already much too long and detailed, and writing suitable connective material, introductions, summaries, etc. is not in the cards anytime soon. Go with the flow, use your text searching tools, and deal with it.

20.2.3. Substantive corrections welcome, quibbles less welcome, and ideological debate even less welcome. Corrections to outdated information, especially on pointers to information, will be most appreciated.

20.3. Copyright Comments

20.3.1. It may seem illogical for a Cypherpunk to assert some kind of copyright. Perhaps. But my main concern is the ease with which people can relabel documents as their own, sometimes after only adding a few words here and there.

20.3.2. Yes, I used the words of others in places, to make points better than I felt my own words would, to save time, and to give readers a different voice speaking on issues. I have credited quotes with a "[Joe Foofoo, place, date] attribution, usually at the end of the quote. If a place is not listed, it is the Cypherpunks list itself. The author and date should be sufficient to (someday) retrieve the source text. By the way, I used quotes as they seemed appropriate, and make no claims that the quoted points are necessarily original to the author--who may have remembered them from somewhere else--or that the date listed is the origination

date for the point. I have something like 80 megabytes of Cypherpunks posts, so I couldn't do an archaeological dig for the earliest mention of an idea.

- 20.3.3. People can quote this FAQ under the "fair use" provisions, e.g., a paragraph or two, with credits. Anything more than a few paragraphs constitutes copyright infringement, as I understand it.
- 20.3.4. Should I give up the maintaining of this FAQ and/or should others get involved, then the normal co-authorship and inheritance arrangements will be possible.
- 20.3.5. The Web. WWW and Mosaic offer amazing new opportunities for on-line documents. It is in fact likely that this FAQ will be available as a Web document. My concern, however, is that the integrity and authorship be maintained. Thus, splitting the document in a hundred or more little pieces, with no authorship attached, would not be cool. Also, I intend to maintain this document with my powerful outlining tools (Symantec's "MORE," on a Macintosh) and thus anyone who "freezes" the document and uses it as a base for links, pointers, etc., will be left behind as mods are made.

20.4. A Few Words on the Style

20.4.1. Some sections are in outline form

- like this
- with fragments of ideas and points
- with incomplete sentences
- and with lists of points that are obviously only starting points for more complete analyses

20.4.2. Other sections are written in more complete essay form, as reasonably self-contained analyses of some point or topic. Like this. Some of these essays were taken directly out of posts I did for the list, or for sci.crypt, and no attribution H (since I wrote the stuff...quotes from others are credited).

20.4.3. The styles may clash, but I just don't have the hundreds of hours to go through and "regularize" everything to a consistent style. The outline style allows additional points, wrinkles, rebuttals, and elaborations to be grafted on easily (if not always elegantly). I hope most readers can understand this and learn to deal with it.

20.4.4. Of course, there are places where the points made are just too fragmentary, too outlinish, for people to make sense of. I've tried to clean these up as much as I can, but there will always be some places where an idea seemed clear to me at the time (maybe not) but which is not presented clearly to others. I'll keep trying to iron these kinks out in future versions.

20.4.5. Comment on style

- In many cases I merged two or more chunks of ideas into one section, resulting in many cases in mismatching writing styles, tenses, etc. I apologize, but I just don't have the many dozens of hours it might take to go through and "regularize" things, to write more graceful transition paragraphs, etc. I felt it was more important to get the ideas and idea fragments out than to polish the writing. (Essays written from scratch, and in order, are generally more graceful than are concatenations of ideas, facts,

- pointers, and the like.)
- Readers should also not assume that a "fleshed-out" section, made up of relatively complete paragraphs, is any more important than a section that is still mostly made up of short one-liners.
 - References to Crypto Journals, Books. Nearly every section in this document could have one or more references to articles and papers in the Crypto Proceedings, in Schneier's book, or whatever. Sorry, but I can't do this. Maybe someday--when true hypertext arrives and is readily usable (don't send me e-mail about HTML, or Xanadu, etc.) this kind of cross-referencing will be done. Footnotes would work today, but are distracting in on-line documents. And too much work, given that this is not meant to be a scholarly thesis.
 - I also have resisted the impulse to included quotes or sections from other FAQs, notably the sci.crypt and rsadsi FAQs. No point in copying their stuff, even with appropriate credit. Readers should already have these docs, of course.

20.4.6. quibbling

- Any time you say something to 500-700 people, expect to have a bunch of quibbles. People will take issue with phrasings, with choices of definitions, with facts, etc. Correctness is important, but sometimes the quibbling sets off a chain reaction of corrections, counter corrections, rebuttals, and "I would have put it differently"s. It's all a bit overwhelming at times. My hope for this FAQ is that serious errors are (of course) corrected, but that the List not get bogged down in endless quibbling about such minor issues as style and phrasing.

20.5. How to Find Information

20.5.1. This FAQ is very long, which makes finding specific questions problematic. Such is life--shorter FAQ are of course easier to navigate, but may not address important issues.

20.5.2. A full version of this FAQ is available, as well as chapter-by-chapter versions (to reduce the downloading efforts for some people). Search tools within text editors are one way to find topics. Future versions of this FAQ may be paginated and then indexed (but maybe not).

20.5.3. I advise using search tools in editors and word processors to find sections of interest. This is likely faster anyway than consulting an index generated by me (which I haven't generated, and probably never will).

20.6. My Views

20.6.1. This FAQ, or whatever one calls it, is more than just a simple listing of frequently asked questions and the lowest-common-denominator answers. This should be clear just by the size alone. I make no apologies for writing the document I wanted to write. Others are free to write the FAQ they would prefer to read. You're getting what you paid for.

20.6.2. My views are rather strong in some areas. I've tried to present some dissenting arguments in cases where I think Cypherpunks are really somewhat divided, such as in remailer strategies and the like. In cases where I think there's no

credible dissent, such as in the wisdom of Clipper, I've made no attempt to be fair. My libertarian, even anarchist, views surely come through. Either deal with it, or don't read the document. I have to be honest about this.

20.7. More detailed disclaimer

20.7.1. This detailed disclaimer is probably not good in most courts in the U.S., contracts having been thrown out in favor of nominalism, but here it is anyway. At least nobody can claim they were misled into thinking I was giving them warranted, guaranteed advice.

20.7.2. Timothy C. May hereby disclaims all warranties relating to this document, whether express or implied, including without limitation any implied warranties of merchantability or fitness for a particular purpose. Tim May will not be liable for any special, incidental, consequential, indirect or similar damages due to loss of business, indictment for any crime, imprisonment, torture, or any other reason, even if Tim May or an agent of his has been advised of the possibility of such damages. In no event shall Tim May be liable for any damages, regardless of the form of the claim. The person reading or using the document bears all risk as to the quality and suitability of the document. Legality of reading or possessing this document in a jurisdiction is not the responsibility of Tim May.

20.7.3. The points expressed may or may not represent the views of Tim May, and certainly may not represent the views of other Cypherpunks. Certain ideas are explored which, if implemented, would be illegal to various extents in most countries in the world. Think of these explorations of ideas as just that.

20.8. I've decided to release this before the RSA patents run out...