

# 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](mailto: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, 1### 9.4-09-01]

## 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, 1### 9.4-08-20; Denning comments are 1### 9.2-01-22, 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

- 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-produced ...The 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, 1### 9.4-0831]
- Bill Sommerfeld notes: "If this is indeed the case, Matt Blaze's results should be particularly devastating to them." [B.S., 1### 9.4-09-01]

## 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, 1### 9.4-03-23]

## 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, 1### 9.4-08-15]

## 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, 1### 9.4-06-29]

## 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](http://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](mailto:alt.security.pgp), 1### 9.4-07-03]

## 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/1### 9.40304)" [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 their 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 countries 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. [1### 9.409-06] (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, 1### 9.4-07-07]

## 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, 1#### 9.4-06-29]

## 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 version:
  - "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 Encryption 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, 1### 9.3-03-23]

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 Chesapeake 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, 4-1594, sci.crypt>
  - possible back doors in the Skipjack 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 Tesseract found by Matt Blaze?"

- Technically, Blaze's work was done on a Tesseract card, which implements the Skipjack 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, 19.4-07-04]
  - "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, 19.4-09-04]

## 9.11. Products, Versions -- Tesseract, 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.nsl.nist.gov](http://csrc.nsl.nist.gov)"--see the file cryptcal.txt [David Koontz, 19.4-08-08].

## 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, 19.4-09-05]

## 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, 19.4-08-03]
- 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 FedX, 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-timesensitive documents via FedX when they could have been sent via first-class mail." [Lew Glendenning, USPS digital signature announcement, sci.crypt, 19.4-08-23] (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 governmentgranted monopolies.
- The USPS proposal may be an opening shot in an attempt to gain control of electronic mail...it never had control of email, 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, 19.4-07-24]

## 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!, 19.3-06-01]

## 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](mailto:usacm_dc@acm.org), USACM Calls for Clipper Withdrawal, press release, 19.4-0630]

## 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, drugrunning, 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, 19.4-0427]

## 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, 19.4-07-17]
- 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, 19.407-19]
- 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., 19.4-06-26, 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, 19.4-07], 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 circumstances, 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](mailto:steve@vesheu.sar.usf.edu), [sci.crypt](http://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](http://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, 19.3-08-02]
  - 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 19.3 21:25:11 GMT Organization: Stratus Computer, Marlboro MA Lines: 28 Message-ID: [23k0nn\\$8gk@transfer.stratus.com](mailto: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](mailto:steve@vesheu.sar.usf.edu), 414-94, [talk.politics.crypto](mailto: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 be 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, 19.4-07-05]

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, 19.4-08-19]
  - 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," 19.4-07-21]

## 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