The Clipper Chip Controversy
It Satisfies The FBI, the CIA, and the NSA. Does It Satisfy You?
Secret Drawers and Backdoors

“Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court.”

Supreme Court Justice Louis Brandeis - c1920
What is Encryption?

Encryption is a way of coding messages, whether it be text, voice or data communications, so that it is recognizable only between the sender and the receiver.
Securing Voice and Data Transmission

Cryptography

- Caesar ciphers (substitution ciphers)
  - Used simple algorithms
  - A becomes F, B becomes G (equal distant)
- Advanced forms of mathematics
  - Graph isomorphism
  - Multiplexers
  - One-way hash functions.
The military has used this type of encryption method for years to safeguard the nation’s most sensitive documents, such as the launch sequence codes for America’s nuclear arsenal.
Encryption has been used by business and industry to protect confidential communication transmissions.

With the growth of computers, business is interested in finding a secure, **data encryption standard** that can be used by everyone, especially over the internet.
Since 1977, the standard has been DES (Digital Encryption System) which provides powerful data security.

However, supercomputers can easily crack the DES codes.

In this age of global competition and industrial espionage, the stakes are high.

Improved protection can be obtained with double- and triple-DES.
National Security Agency

- Has done most of U.S. research in encryption.
- Wrestled control from Nation Science Foundation (NSF)
- Dictates
  - Which encryption algorithms to produce.
  - How strong they could be.
  - IBM (1974)
    - The Lucifer Chip
    - 128 bit to 56 bit
    - Reduced strength by factor of several million
So what’s the problem?

❖ The U.S. government worries that law enforcement officials, (FBI, NSA and the CIA) will not be able to decipher data communications

❖ In January of 1994, computer makers were ready to adopt encryption standards so robust, that NSA supercomputers could not crack it
Encryption Development

- Lucifer becomes DES (Data Encryption Standard)
- Strength of DES falters as computers become faster
NSA secretly developed a stronger algorithm called “Skipjack”

- 80-bit key, 16 million times stronger than DES
- No risk of being broken for 30 to 40 years with the fastest supercomputer today and a “shortcut” insight into breaking it
- The Skipjack algorithm embedded in a chip is called the Clipper Chip
- Telecommunications systems use Skipjack in the Tessara card
The session key is constructed from information from both devices.

Facilitates *decryption* but does not automatically approve *interception*.
A Matter of Privacy

Clipper Chip to be installed in:
- telephones
- faxes
- modems
Implemented using Skipjack via Escrowed Encryption Standard (EES); two in each device: one each for sending and receiving
- Sending Clipper encodes
- Receiving Clipper decodes
One of codes are escrowed to Depts. of Justice and Commerce
Clipper Chip keys held by government
- National Institute of Standards and Technology (NIST)
- Automated Systems Division of Department of Treasury (ASD)
- Resistant to reengineering

Has gone through several proposals with Clipper 4 including escrow by a company, with divulgence only on court order
“These procedures do not create, and are not intended to create, any substantive rights for individuals intercepted through electronic surveillance, and noncompliance with these procedures shall not provide the basis for any motion to suppress or any other objection to the introduction of electronic surveillance lawfully acquired.”

i.e., FBI can play by its own rules
If you were a senator which position would you vote for?

- Criminals and terrorists should not have access to encryption technologies to hide their activities even though this requires a restriction on law abiding citizens.

or

- All persons have a right to unfettered access to encryption technologies that protect their communications.
Opposing Forces

NSA, CIA, FBI
Clinton Administration

Computer Firms
Civil libertarians
Cypherpunks
Terrorists
Criminals
Spies
EFF
What are three arguments for and three arguments against the use of the Clipper Chip?
Support for Clipper

Law Enforcement and Government Agencies want to counteract terrorism and criminal behavior.

Wiretapping is difficult enough

- call forwarding
- cellular lines
- Lesser encryptions thwart law enforcement
  - child pronographer encrypted diaries, hindering investigation.
“without Clipper, the FBI would be unable to protect against foreign threats, terrorism, espionage, violent crime, kidnapping or other violent crimes.”
James Kallstrom, FBI.
It provides a very secure standard for data communication.

The escrow agents, the National Standard Institute of Technology and the Department of Treasury, may only release the keys under court order. The key release system is similar to that used for the atomic weapon codes - very complex, and virtually foolproof.
No evidence of misuse of wiretapping/DES

Wire taps are constitutional. So would Clipper and taps

US security interests are protected

There is a need to protect against the export of dangerous technologies to foreign powers
Law enforcement may still use wire tapping and surveillance to obtain evidence

- 22,000 felons have been convicted in the past decade due to evidence produced through wiretaps
- 1991 - government listened to 1.35 million conversations and made 3,000 arrests

Some criminals are stupid
Best algorithm for the law-abiding citizen to use

Clipper is voluntary. Companies can use other key-escrows

Government will use it itself.

Government should be involved in standard setting
Arguments Against Clipper

- Does not increase government’s ability to wiretap
  - Wiretapping involves fewer than 800 cases a year
  - 15 of these cases involve murder
- Potential to go mandatory
- Escrow system can be compromised
- Potential misuse for traffic analysis
Currently over 200 non-Clipper alternatives.
  - More expensive
  - Not as strong
  - No government access

If voluntary, will criminals “really use it”

Distrust of the NSA
  - Built in “trap door”
Clipper Chip devices will only be used by law abiding citizens. No criminal would. Therefore, the Feds can use the system only to spy on law abiding citizens.

Adoption hurts overseas sales of communications technology since no foreign government or corporation would use a device where the only key holder is the US Government.

Potential to ban other forms of cryptography.
Some knowledgeable observers indicate the algorithm is actually very weak
Why would foreign customers (or crooks) use this technology when powerful, uncompromised encryption is available overseas?

Citizens have a right to privacy - the government does not have the right to put a cap on how much privacy individuals can have.

Newer, more powerful future computers will quickly antiquate the Clipper Chip.
Summary

- Government develops Clipper Chip
- Government wants chip placed into all communications devices
- Government to hold internal key to encryption
- Where is our privacy?
Drop the escrow key concept
No law should bar use of encryption
Crypto-policy should be developed in the open
56-bit encryption techniques should be exportable
Government should encourage encryption in business and personal communications: computer and telephone
Assumes a business will assist in criminal investigations
Communications Assistance for Law Enforcement Act (CA-LEA)

.requires telecommunications and common carriers to:
  - Isolate and enable interception of communications and call identification data
  - Deliver the intercepted communications to the government
  - Facilitate authorized interception

dration at carrier expense

hydration for up to 10K calls simultaneously
Other Important Encryption-Related Developments

- RSA (Rivest, Shamir, and Adleman) set up a commercial public key company (1978)
- PGP released by Phil Zimmerman (1990)
- Professor Daniel Bernstein (1999) was allowed by Federal 9th Circuit Court, to post “Snuffle” source code on a web site
- Digital Signature Standard (2000)
Cyberspace Electronic Security Act (proposed 2000)

Would allow investigators to:
- Break into homes and offices
- Crack security codes of suspects on home and office computers
- Search computers for passwords, encryption keys
- Install keystroke recorders and forward results
- “Patch” encryption software so the session key is always the same
- Eliminates the need for law enforcement to reveal the techniques they used
“Everything on the I-net should be encrypted all the time.”
Bob Metcalf, PC Week

Pros?
Cons?