Computers and Society
Issues in Encryption

Chris Brooks

Department of Computer Science
University of San Francisco

Uses a system known as key escrow.

A copy of your private keys are kept with a third party.

These keys could be accessed with a court order.

Intended government standard for computer and telephone communications.
Actual algorithm kept secret.
  ▶ No one could use it without providing keys to escrow agents.

Dropped due to technical flaws and political opposition.

Replaced with key recovery schemes
  ▶ Also useful if keys are lost.

Mostly voluntary.
Secrecy

△ As a government tool
△ Evaluating algorithms
   - Public vetting has proved quite helpful at testing security schemes.
△ Potential “back doors”
△ Violation of constitutional rights.
3-3: Issues

- Policies for new technology
- Legal standards were in place for tapping phones and reading mail.
- Law enforcement can also get a list of phone numbers that are called.
  - Is this the same as an email header?
- Is email the same as a phone conversation?
- Rapid change in technology changes what is considered “secure”
The essential tension is between providing government with the tools to protect us and keeping them from the tools to oppress us.

One’s view of government affects where you stand in this debate.
Consider the following scenario:

△ In response to both security concerns and outcry from the entertainment industry over piracy/illegal downloading, the U.S. government proposes Clipper Chip II.

△ This is a ‘chip’ that will be incorporated into all computer hardware sold in the United States.

△ It will keep a record of all encrypted/watermarked messages that are sent or received on this computer.
Federal law enforcement agents will be able to get a record of what messages/files were sent or received (but not their contents) with the same requirements currently needed to get a list of phone numbers called.

- “person of interest” in an investigation

Law enforcement agents will be able to use a “back door” in the chip to decrypt any message sent or received on this computer if a court order is granted.

- Similar to current wiretapping laws - persons indicted or under investigation may be monitored if a court order is granted.
Case Study: Clipper Chip II

Interest groups:
- U.S. Attorney General’s office
- Association of Semiconductor Chip Manufacturers
- American Civil Liberties Union
- Representatives of entertainment industry.
3-8: Case Study: Clipper Chip II

6 Consider the effect of the proposed system from your clients’ perspective.
   △ How will it help? What potential benefits does it have?
   △ How will it cause harm?
   △ Will it have an economic impact?
   △ What are the arguments for/against adoption?

6 Represent your clients’ point of view fairly.