




Encryption

Dr. Tim Margush
University of Akron



What is Encryption?

- Information is often stored and transmitted in a file
- A **plaintext** file uses a common encoding format such as ASCII or Unicode to represent the characters of the file.
- Encryption is a translation of a file into a format that hides the content from selected parties; a secret code; **ciphertext**.

Uses of Encryption

- Privacy/Secrecy
 - email messages
 - wireless phones
- Security
 - passwords
 - wireless networks
- Intellectual Property
 - copy protection
- Confidentiality
 - personnel records
 - medical records
 - transaction records
- Authentication
 - digital signatures
 - login

Technology and Risk

- Technological advances created new risks
 - electronic communication makes information more easily available to more parties
 - long-term storage of sensitive data requires stronger encryption techniques
- Some technologies actually reduce risk
 - fiber optic cable
 - strong encryption

Wiretapping (telephone surveillance)

- Banned in 1934 but regularly practiced by government and law-enforcement agencies
- Wiretapping with a court order was authorized in 1968
 - Omnibus Crime Control and Safe Streets Act
 - Limited duration
 - Emergency situations excluded

Email? Wireless Communications?

- Wiretap restrictions were extended to data transmissions via computer in 1986 and 1994
 - Electronic Communications Privacy Act of 1986
 - Does not limit employer access to this information
- Some relaxation of these requirements were introduced in 2001
 - Patriot Act

CALEA

- Communications Assistance for Law Enforcement Act
 - Passed in 1994, intended "to make clear a telecommunications carrier's duty to cooperate in the interception of communications for Law Enforcement purposes, and for other purposes"
 - Required technology to provide wiretapping ability, resulting in increased cost to consumers

Carnivore

- FBI's term for "tapping" email
 - Requires physical access to network to allow sniffing of communications packets
 - Configurable to intercept only information authorized by court order
 - "Carnivore ... does NOT search through the contents of every message and collect those that contain certain key words like "bomb" or "drugs." It selects messages based on criteria expressly set out in the court order..."
 - FBI Director, Donald Kerr

Echelon

- Secret world-wide monitoring network operated by the UKUSA community
 - NSA neither confirms nor denies its existence
 - Monitors radio, satellite, telephone, fax, and email
 - Performs automated analysis

Steganography

- The art of concealing the very existence of a message
 - Invisible inks
 - Microdots
 - Terrorist videos (?)
 - Data hidden in images or audio
 - Digital Invisible Ink Toolkit: <http://diit.sourceforge.net/>

World War II

- Banned international mailing of chess moves, crossword puzzles, children's drawings, knitting instructions, etc.
- Banned international cables for specific flower arrangements to be delivered on a specific date
- Suspicious of classified advertising, arrangement of stamps on letters, radio call-ins requesting a favorite tune
- During the war, Navajo Indians were used to send secret messages hidden in dialog spoken in their native tongue
 - In 1990, the US Government prevented Navajos from transmitting messages in the Navajo language via Armed Forces Radio to family members serving in the Gulf War (however public outcry caused the government to reverse this decision)

Cryptography

- The science of encryption and decryption; converting between plaintext and ciphertext
- Cryptanalysis
 - The science of breaking ciphers
- Key
 - A piece of information that allows decoding of an encrypted message

Private and Public Keys

- A private key is held by sender and recipient
 - The key(s) must be kept secret introducing the problem of getting the key to the recipient
- A public key system uses a private and a public key
 - Only the recipient need hold the private key
 - The public key is used to encrypt the message which can only be decrypted with the private key

Private Key: DES

- Data Encryption Standard
 - Adopted in 1976 as US Government standard encryption technique
 - Utilizes a 56-bit symmetric key
 - Suspected of having "backdoors"
 - Cracked in 1998
 - Replaced in 2002 by AES which utilizes 128 bit (or longer) keys

Public Key: RSA

- Theoretical development published in 1976 by Whitfield Diffie and Martin Hellman
- The RSA Algorithm was invented in 1977 by Ronald Rivest, Adi Shamir and Leonard Adleman
- The British Government had secretly developed the same algorithm in 1973

Exporting Cryptology

- National security
 - Export of cryptographic techniques (even their description) was illegal up until 1996 – considered munitions
 - Some restrictions remain under the control of the Department of Commerce
 - High-security systems require key-recovery abilities

PGP

- Pretty Good Privacy
 - Encryption and authentication system developed by Phil Zimmermann in 1991
 - Commonly used for secure email communication
 - Uses public key and symmetric key technologies
 - Binds public keys to user identities
 - Phil was investigated 1993-1996 for violating the munitions export laws
 - The investigation ended without charges

Zimmermann on Privacy

- *If privacy is outlawed, only outlaws will have privacy. Intelligence agencies have access to good cryptographic technology. So do the big arms and drug traffickers. So do defense contractors, oil companies, and other corporate giants. But ordinary people and grassroots political organizations mostly have not had access to affordable military grade public-key cryptographic technology. Until now.*
 - Why Do You Need PGP?, Phil Zimmermann
 - <http://www.pgpi.org/doc/whypgp/en/>

Bernstein vs. United States

- Daniel Bernstein wanted to publish an encryption algorithm named Snuffle
 - Bernstein sued the government over the constitutionality of ITAR (International Traffic in Arms Regulations)
 - In 1997 (affirmed 1999) it was ruled that software was speech, and therefore protected by the 1st Amendment
 - Case was dismissed in 2002