Cryptology

Cryptography:
secret writing (κρυπτος hidden)

Cryptanalysis:
breaking codes and ciphers

Codes and Ciphers

Codes and ciphers render a *plaintext* message unintelligible by applying transformations to the plaintext (*encoding*, or *enciphering* the text).

Code: the basic transformation is substitution of words by *codewords*.

Cipher: the basic transformation is substitution of letters/symbols by letters/symbols.

Cipher is often used to denote arbitrary encryption schemes.

Steganography and Cryptography

στεγανος: covered

γραφειν: (to) write

κρυπτος: hidden

Steganography tries to hide the presence of message.

Cryptography tries to obscure the contents of the message.

Technical Steganography

- message on silk in wax balls (ancient China)
- Xerxes
- Histaiaeus (Herodotus)
- invisible inks (at least 100AD)
- Giovanni Porta and the hardboiled egg (15th century)
- hollow heels
- microdots
- IP timing delays (covert channels)

Linguistic Steganography

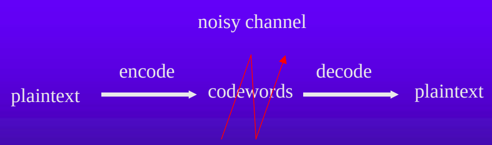
Semagrams (graphical)
- Francis Bacon
- Watermarking

Open Code
- Grilles
- Weather Reports in *Breakfast at Tiffany's*
- Velvalee Dickinson (“The Doll Woman)
- (censorship)

“Aighotkcruiderl Honalulu wgilshaskertavlidahmagesall dapairgedsbyphairedfdstywebkfost Fwebkaofy.February.”

Coding Theory

Error-Correcting Code: guard against noisy channel



Secret Communication

Eve

Keys

Encryption and decryption can depend on a *key* which is kept secret.

The collection of possible keys is called the *key space*.

If we assume that only the key, not the method of encryption is secret, the *combinatorial complexity*, that is, the size of the key space is a first rough measure of how hard it is to break a cipher.

Eve's Goals

- Reading secret messages — Oscar
- Finding key — Oscar
- Corrupting messages (Integrity) — Mallory
- Masquerade as Alice (Authentication) — Mallory

Types of Attack

- Ciphertext only
- Known plaintext (cribs)
- Chosen plaintext
- Chosen ciphertext

Kerckhoff's Principle

> Compromise of the system should not inconvenience the correspondents.
>
> Auguste Kerckhoff
> La Cryptographie Militaire, 1883