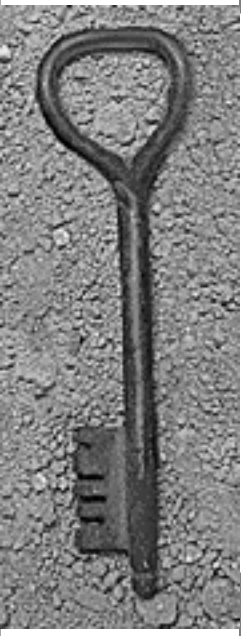
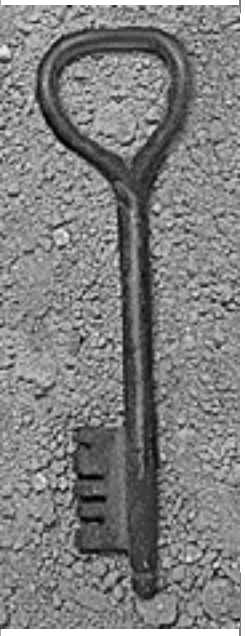


Cryptology

Cryptography: secret writing (κρυπτος hidden)

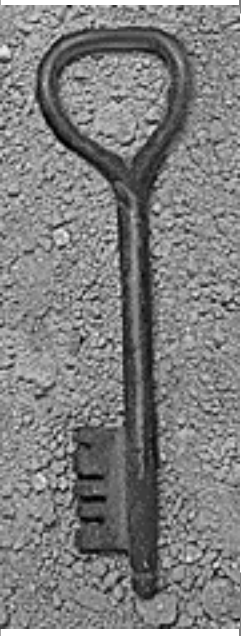
Cryptanalysis: breaking codes and ciphers



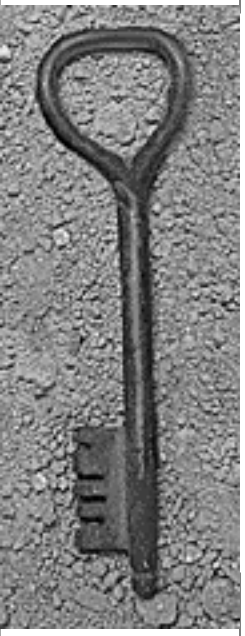
Steganography (covert writing)

Steganography tries to hide the presence of message.

- Technical
  - invisible inks (at least 100AD)
  - hollow heels
  - frequency subband permutation
  - microdots
- Linguistic
  - Semagrams
    - Herodotus, Francis Bacon
    - Watermarking (protection against removal)
  - Open Code
    - (Weather Reports, Breakfast at Tiffany's)



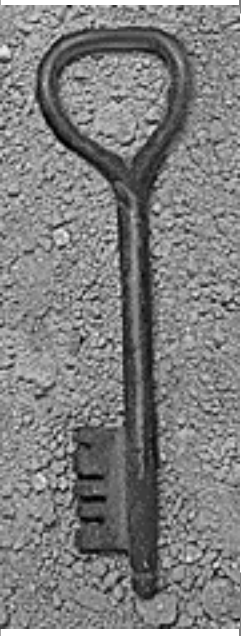
Watermarking



Codes and Ciphers

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

In a code the basic transformation is the substitution of words by codewords.



Cryptology

Alice

plaintext

encrypt

ciphertext

decrypt

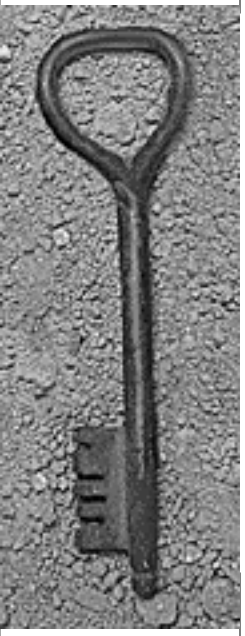
Bob

plaintext

Encryption Key

Decryption Key

Eve

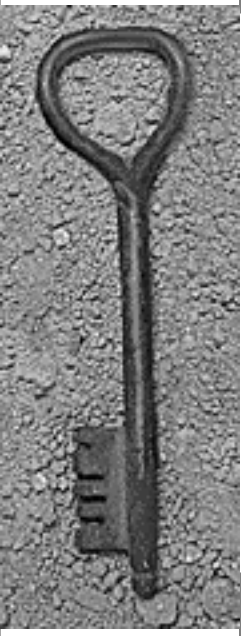


Eve's Goals

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

Oscar

Mallory



Types of Attack

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

Kerckhoff's Principle

Assume that enemy knows encryption method (but not key).

Auguste Kerckhoff,
La Cryptographie Militaire, 1883