


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).

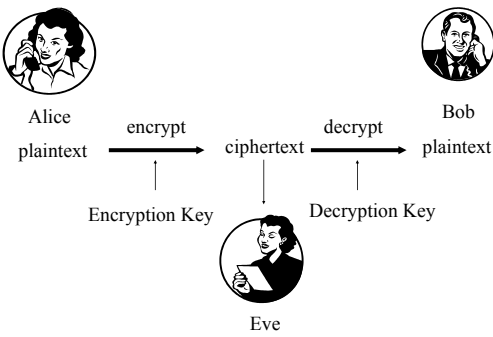
Code: the basic transformation is substitution of words by *codewords*.

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


Cipher is often used to denote arbitrary encryption schemes.



Secret Communication



The diagram illustrates the process of secret communication. On the left, Alice is shown with a telephone receiver to her ear. Below her is the label 'Alice plaintext'. An arrow labeled 'encrypt' points from Alice to a central point labeled 'ciphertext'. Below this arrow is the label 'Encryption Key'. From the 'ciphertext' point, an arrow labeled 'decrypt' points to Bob on the right, who is also shown with a telephone receiver to his ear. Below this arrow is the label 'Decryption Key'. Below Bob is the label 'Bob plaintext'. At the bottom center, Eve is shown with a notepad and pen, looking up at the communication process. Below her is the label '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 size of the key space is a first measure of how hard it is to break a cipher.




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
