


Cryptography

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).

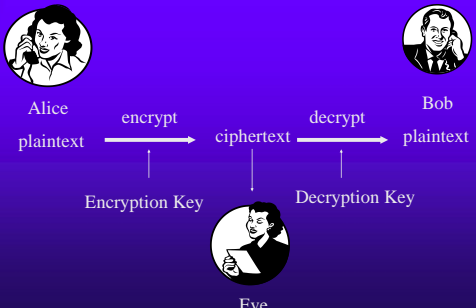
Code: basic transformation is substitution of words by *codewords*.

Cipher: 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 flow of secret communication. On the left, Alice is shown with a telephone receiver to her ear. An arrow labeled 'encrypt' points from Alice to a central point labeled 'ciphertext'. Below this arrow is an upward-pointing arrow labeled 'Encryption Key'. From the 'ciphertext' point, an arrow labeled 'decrypt' points to Bob on the right, who is also shown with a telephone receiver. Below this arrow is a downward-pointing arrow labeled 'Decryption Key'. At the bottom center, Eve is shown with a telephone receiver to her ear, with a vertical line connecting her to the 'ciphertext' point, indicating she is intercepting the message. The labels 'Alice plaintext', 'ciphertext', and 'Bob plaintext' are positioned below their respective points in the flow.



Keys

Encryption and decryption depends 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 called the *combinatorial complexity* of the 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(s)

- 1° Le système doit être matériellement, si non mathématiquement, indéchiffrable ;
- 2° Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;
- 3° La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;
- 4° Il faut qu'il soit applicable à la correspondance télégraphique ;
- 5° Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;
- 6° Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Auguste Kerckhoff,
La Cryptographie Militaire, 1883



Kerckhoff's Principle(s)

1. The system must be practically, if not mathematically, indecipherable;
2. The system must not require secrecy and may fall into the hands of the enemy without causing inconvenience;
3. The key can be communicated and retained without the help of written notes, and be changed or modified at the will of the correspondent;
4. It must be compatible with telegraphic correspondence;
5. It must be portable, and its handling and operation should not require the assistance of several people;
6. Finally, it is necessary, given the circumstances in which the system is applied, that it is easy to use, requiring neither intense brainwork, nor the knowledge of a long series of rules to follow.

Auguste Kerckhoff,
La Cryptographie Militaire, 1883
