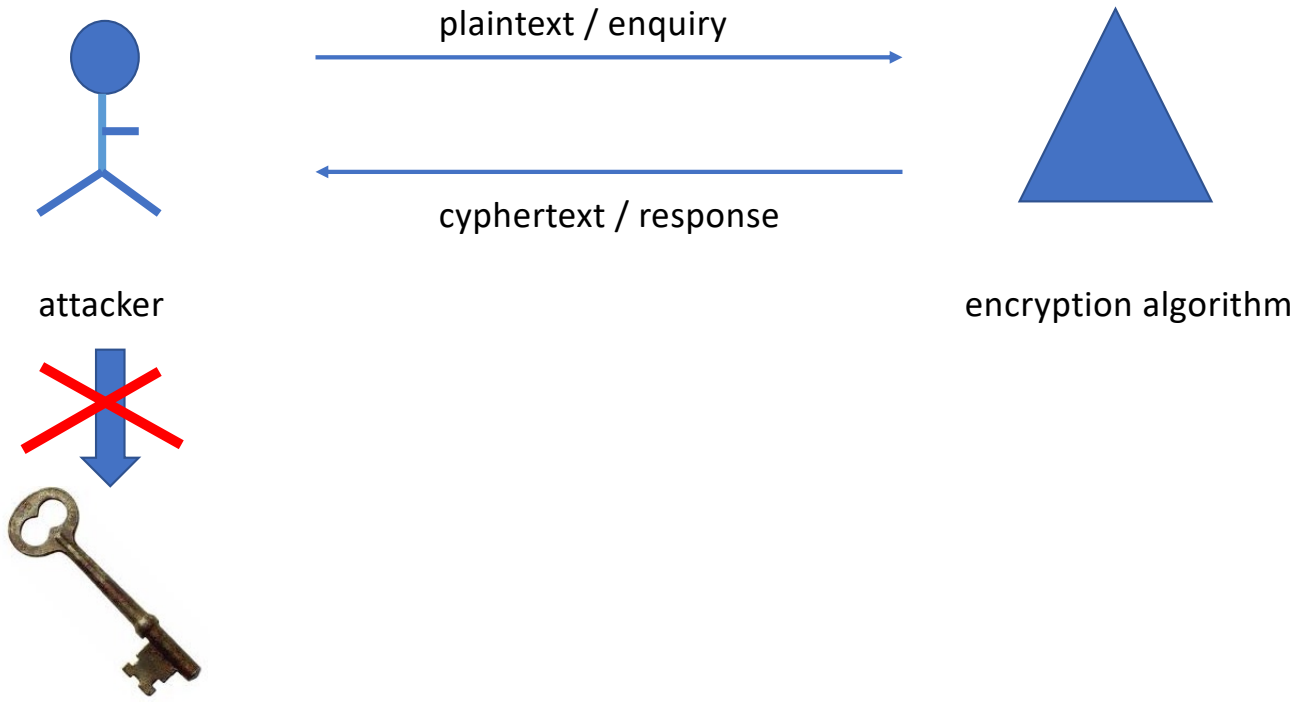
A strong encryption algorithm



Secure Encryption Scheme

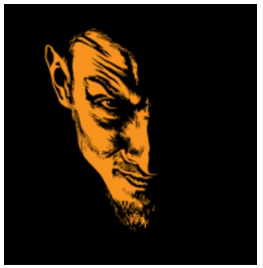
- **Unconditional security**
  - no matter how much computer power is available, the cipher cannot be broken since the ciphertext provides insufficient information to uniquely determine the corresponding plaintext
- **Computational security**
  - the cost of breaking the cipher exceeds the value of the encrypted information;
  - or the time required to break the cipher exceeds the useful lifetime of the information

Desired characteristics

- Cipher needs to completely obscure statistical properties of original message
- more practically Shannon suggested combining elements to obtain:
  - Confusion – how does changing a bit of the key affect the ciphertext?
  - Diffusion – how does changing one bit of the plaintext affect the ciphertext?

confusion

ciphertext



diffusion

plaintext

Ways to achieve

- Symmetric Encryption:
  - substitution / transposition / hybrid
- Asymmetric Encryption:
  - Mathematical hardness - problems that are efficient to compute in one direction, but inefficient to reverse by the attacker
    - Examples: Modular arithmetic, factoring, discrete logarithm problem, Elliptic Logs over Elliptic Curves

Two basic types

- Block Ciphers
  - Typically 64, 128 bit blocks
  - A k-bit plaintext block maps to a k-bit ciphertext block
  - Usually employ Feistel structure
- Stream Ciphers
  - A key is used to generate a stream of pseudo-random bits – key stream
  - Just XOR plaintext bits with the key stream for encryption
  - For decryption generate the key stream and XOR with the ciphertext!

Symmetric Block Encryption

Block cipher

- the most commonly used symmetric encryption algorithms
- input: fixed-size blocks (Typically 64, 128 bit blocks), output: equal size blocks
- provide secrecy and/or authentication services
- Data Encryption Standard (DES), triple DES (3DES), and the Advanced Encryption Standard (AES)s
- Usually employ Feistel structure

Feistel Cipher Structure

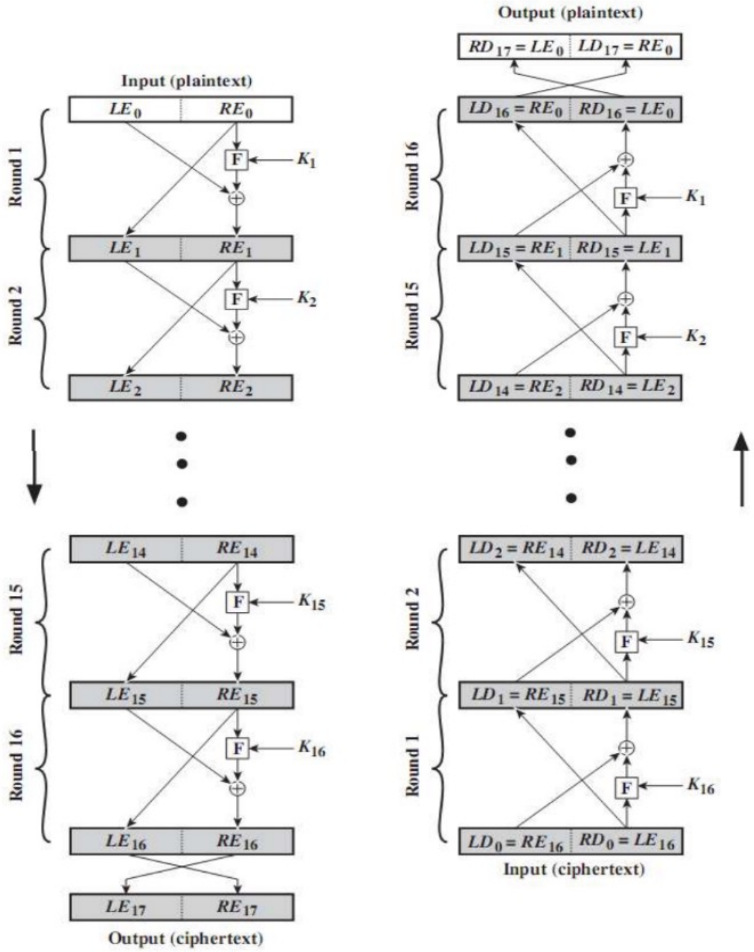
Feistel Cipher Structure

- most symmetric block ciphers are based on a **Feistel Cipher Structure**
- based on the two primitive cryptographic operations
  - *substitution* (S-box)
  - *permutation* (P-box)
- provide *confusion* and *diffusion* of message

Feistel Cipher Structure

- Horst Feistel devised the **feistel cipher** in the 1973
  - based on concept of invertible product cipher
- partitions input block into two halves
  - process through multiple rounds which
    - perform a substitution on left data half
    - based on round function of right half & subkey
    - then have permutation swapping halves
- implements Shannon's substitution-permutation network concept

Feistel Encryption and Decryption



Encryption

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$