

# Block ciphers

---

## Block ciphers

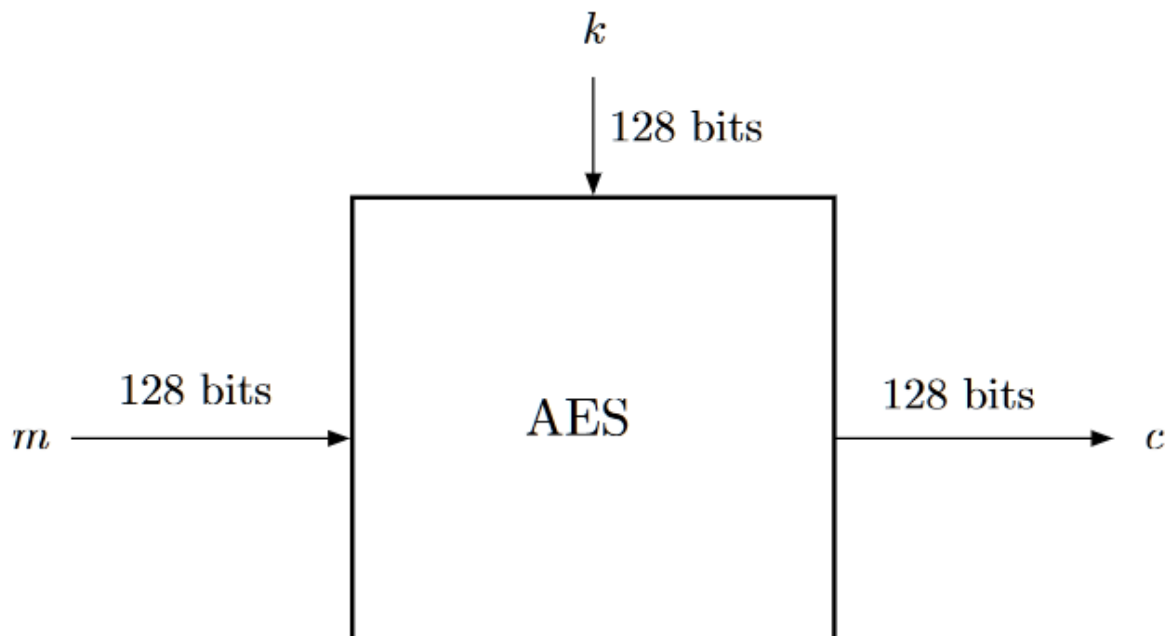
---

### Intro

- <https://www.youtube.com/watch?v=FGhj3CGxl8I>

*Intuition:*

- A block cipher is an encryption method that applies a **deterministic algorithm** along with a **symmetric key** to encrypt a **block of text**, rather than encrypting one bit at a time as in stream ciphers



### Definition - block cipher

- Functionally, a block cipher is a deterministic cipher  $(E, D)$  whose message space and ciphertext space are the same (finite) set  $\mathcal{X}$ .
- If the key space of  $(E, D)$  is  $\mathcal{K}$ , we say that  $(E, D)$  is a block cipher defined over  $(\mathcal{K}, \mathcal{X})$ .
- We call an element  $x \in \mathcal{X}$  a data block, and refer to  $\mathcal{X}$  as the datablock space of  $(E, D)$

### Encryption and decryption

- $\forall k \in \mathcal{K}$  we define  $E(k, \cdot) = f_k : \mathcal{X} \longrightarrow \mathcal{X}$ 
  - We want the function to be one-to-one  $\Rightarrow f_k$  is a permutation on  $\mathcal{X}$
- $D(k, \cdot) = f_k^{-1}$

### Security - black box test

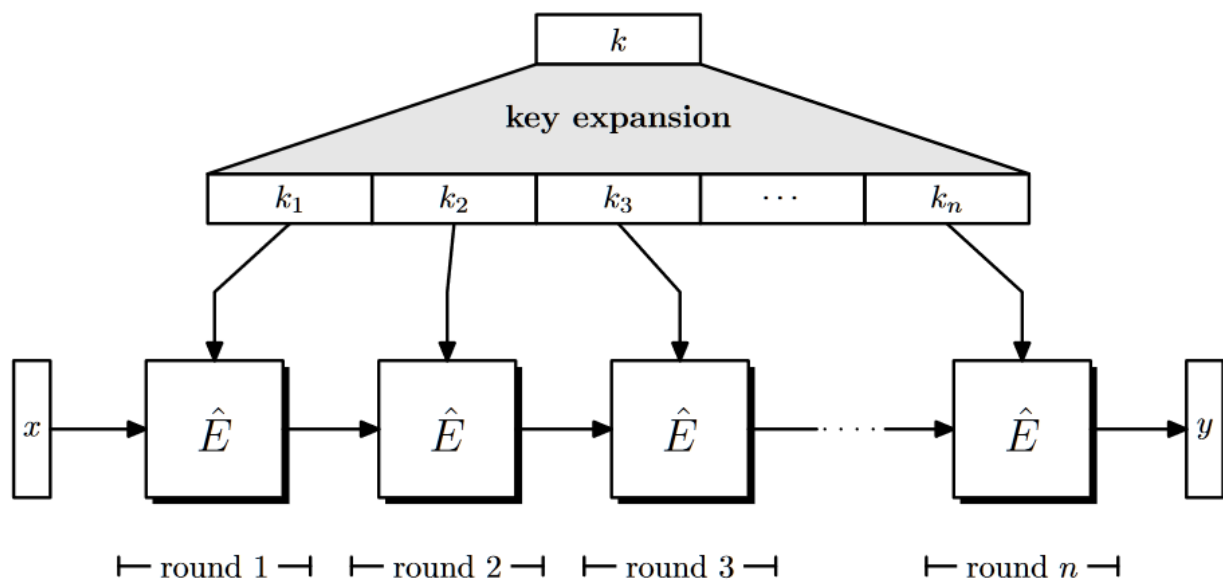
- An adversary can give the challenger a value  $x \in \mathcal{X}$  and receive  $y = f(x)$
- The challenger will respond by applying one of the functions
  - $f_k = E(k, \cdot)$
  - $f$  = truly random function chose uniformly from all permutations on  $\mathcal{X}$
- The adversary mustn't be able to distinguish which function was used => **Computationally indistinguishable**
- The block cipher is secure if any efficient adversary have negligible advantages

### Remarks

- A secure block cipher is unpredictable

### Constructing block ciphers

- Pick a block cipher  $(E, D)$  - **round cipher**
- Pick a PRG to expand the key  $k$  into more keys - **key expansion function**
  - $(k_1, \dots, k_d) \leftarrow G(k)$
- Apply iteratively
  - $c = E(k_d, E(k_{d-1}, \dots E(k_2, E(k_1, x)) \dots))$
- Decrypt by applying the round keys in reverse order



### Remark

- Linear functions never lead to secure block ciphers
- non-linear functions appear to give a secure block after a few iterations