CPA

→ for constructing a CPA secure encryption, first we define a ~~finite key~~ private-key encryption scheme of length n.

Gen: Input $= 1^n$, Choose $k \leftarrow \{0,1\}^n$ uniformly at random and output it as the key.

Encryption: On Input key $k \in \{0,1\}^n$ and message $m \in \{0,1\}^n$

Choose some $r \leftarrow \{0,1\}^n$ uniformly at random and output the cipher text.

$$C := \langle r, F_k(r) \oplus m \rangle .$$

Decryption: Input a key $k \in \{0,1\}^n$ and a cipher text $c = \langle r, s \rangle$ output the plaintext message.

$$m := F_k(r) \oplus s.$$

We can write an CPA encryption for any given PRF.