- Una din schemele generale:

pp. că avem o familie de funcții

$(F_k)_{k \in \mathcal{K}}$ $\quad F_k : \{0,1\}^n \to \{0,1\}^n$

↑ spațiu de chei $\quad n = 64, 128, 192, 256.$

Criptarea unui bloc se face astfel:

→ $\mathcal{G}(1^n)$: $k \xleftarrow{u} \mathcal{K}$ extrage o cheie

→ $\mathcal{E}(k, m)$: se generează random

$r \xleftarrow{u} \{0,1\}^n$ iar criptotext

tul e de forma $c = (r, F_k(r) \oplus m)$

Decriptare: $\mathcal{D}(k, c)$: $c = (r, s)$

$m = s \oplus F_k(r)$

Dacă familia de fct F_k e pseudoroandom (PRF) → nu generează output atât mai aproape de random pur, atunci schema e CPA sigură - (H probabilistă)

$m \to r_1 \quad (r_1, F_k(r_1) \oplus m)$

$r_2 \quad (r_2, F_k(r_2) \oplus m)$

Pt familia de fct F_k, putem avea.

$(DES_k)_{k \in \{0,1\}^{64}}$ - cheia de lungime 64.

$(AES_k)_{k \in \{0,1\}^{128 \text{ sau } 192 \ldots}}$

sau $(3DES_k)_{k \in \{0,1\}^{128}}$ (cu 2 chei)