$3DES_{(k_1,k_2)}(x) = DES_{k_2}(DES^{-1}_{k_1}(DES_{k_2}(x)))$

(e în temă) → temo 2.

- Moduri de criptare:

- ECB: $m = m_1 \dots m_\ell$

(electronic code block)

k ↓

$c_1 = F_k(m_1)$ ... $c_\ell = F_k(m_\ell)$

$r \leftarrow \{0,1\}^w$ random, $c_1 = F_k(m_1 \oplus r)$ un bloc ca

$c_\ell = F_k(m_\ell \oplus r)$

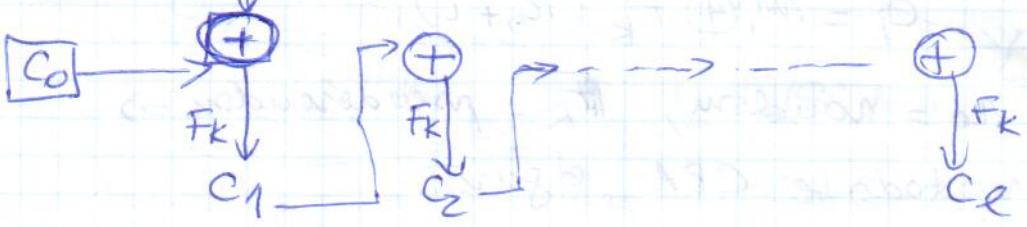
apare de mai multe ori e criptat la fel => vulnerabilitate mojoră.

În practică, acest mod nu trebuie utilizat.

CBC (cipher block chaining).

$m = m_1 \; m_2 \dots m_\ell$

c_0 = random uniform



$c_1 = F_k(m_1 \oplus c_0)$

$c_2 = F_k(m_2 \oplus c_1)$

$c = (c_0, c_1 c_2 \dots c_\ell)$

c_0 = vector de inițializare, (IV)

Dacă c_0 = random și metoda de inițializ e random, atunci ⇒ (CPA — sigur)