CCA - chosen ciphertext attack.
- adversarul are posibilitatea de a afla mesaje originale asociate unor criptotexte (alese de el = adoptiv). → intuitionând oracolul.

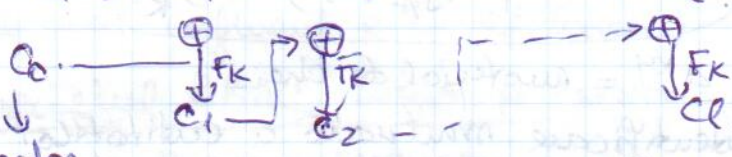
Criptosistemele simetrice (au chei private). { Stream / bloc.

Gr. (RC4) Stream → cheie scurtă de acces lung cu mesajul.
- cheia e generată dintr-una mică și apoi se expandează.
ex: RC4 -
→ vulnerabilitate: al doilea octet din cheia scurtă e 0 cu probab. de 1/128 (↑ mare). [Foarte rapide în practică]
• pt securitate, cheia de criptare trebuie schimbată de la mesaj la mesaj
• Criptosist bloc: mes. e împărțit în blocuri de criptare
se face bloc cu bloc → $k \leftarrow G(1^n)$; $\mathcal{E}(k,m)$; $c = G(k) \oplus m$
$\mathcal{D}(c,k)$, $m = G(k) \oplus c$
• se generează o cheie → avem o familie de fct pseudo-random;
; se criptează mesajul cu cheia k; cu cât generatorul e mai random, schema e CPA sigură.
- de decriptare, se face decr tot cu cheia k → Des - 64 biți, AES - 128 b.
3Des - 128 pt 2 key, 192 pt 3 key

Vulnerabilități: $c_1 = m_1 + G(k)$, $c_2 = m_2 + G(k)$, $m_1 \Rightarrow c_1 \oplus c_2 = (m_1 \oplus m_2)$ vulnerabil. NU!

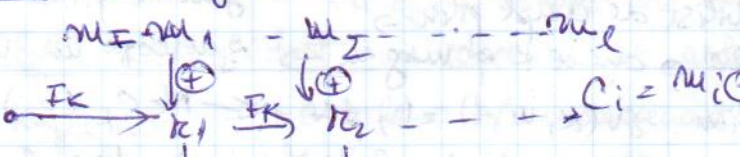
Moduri de criptare: ECB:
electronic code block.
→ $c_1 = F_k(m_1)$, ---$c_l = F_k(m_l)$
$r \leftarrow \{0,1\}^n$ random, $c_1 = F_k(m_1 \oplus r)$ un bloc care apare de mai multe ori e criptat la fel = vulnerab. majoră! → în practică nu se utilizează!

CBC - Cypher block chaining)



vector de inițializare. ; Dacă c_0 = random și metoda de inițializ e random, schema e CPA sigură

OFB = output feedback -



$c_i = m_i \oplus F_k^i(r_0)$ } Ca un criptosistem de tip

CPA sigură dacă r_0 = random și met de inițializ = random
F_k = familie de fct pseudorandom. ex Des, AES, 3DES → 64, 128, 128/192.