segretezza perfetta

- un crittosistema CS=$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ è a segretezza perfetta se $\forall x \in \mathcal{P}$ e $\forall y \in \mathcal{C}$

$$\mathbf{Pr}(x|y) = \mathbf{Pr}(x)$$

- si può riformulare questa definizione in termini di indistinguibilità
- $\forall x_0, x_1 \in \mathcal{P}$ e $\forall y \in \mathcal{C}$, scelta in modo casuale una chiave $k \in \mathcal{K}$

$$\mathbf{Pr}(e_k(x_0) = y) = \mathbf{Pr}(e_k(x_1) = y)$$

sfida

- possiamo pensare a un sfida fra un avversario $\mathcal{A}$ e l'utente $\mathcal{U}$ di un crittosistema CS=$(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$; definiamo un esperimento EXP come segue:
  1. $\mathcal{A}$ sceglie due messaggi x_0 e x_1 in $\mathcal{P}$
  2. $\mathcal{U}$ sceglie una chiave in modo casuale e genera un CT $y = e_k(x_b)$, $b = 0$ o 1. $\mathcal{U}$ trasmette y a $\mathcal{A}$
  3. $\mathcal{A}$ produce un bit b', $b' = 0$ o 1.
  4. l'output dell'esperimento EXP è 1 se $b = b'$ ($\mathcal{A}$ ha indovinato) e 0 altrimenti
- Un CS ha segretezza perfetta se per ogni avversario $\mathcal{A}$ si ha

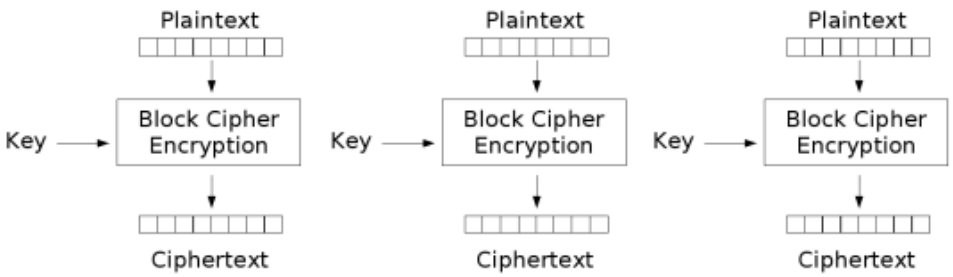
$$\mathbf{Pr}(\ \mathrm{EXP} = 1) = \tfrac{1}{2}$$

definizione concreta di indistinguibilità

- invece che un avversario arbitrario $\mathcal{A}$ si considera un avversario "efficiente" ma computazionalmente limitato (che usa algoritmi polinomiali)
- si concede che la probabilità non sia esattamente $\frac{1}{2}$, ma $\mathbf{Pr}(\text{EXP} = 1) \leq \frac{1}{2} + \varepsilon$
- dove ε è trascurabile (negligible)
- ε dovrebbe essere una funzione dell'input – possiamo pensare a $\varepsilon < \frac{1}{2^{80}}$
- se un CS soddisfa una proprietà di questo tipo si dice che soddisfa IND-EAV (indistinguishable wrt to eavesdropping)
- si parla anche di sicurezza semantica
- vale per una chiave utilizzata per cifrare un solo messaggio (one-time key)

cifrare messaggi lunghi

- Esistono diversi metodi per cifrare messaggi di lunghezza maggiore di un blocco
- Il più semplice è cifrare ogni blocco separatamente con la stessa chiave
- metodo ECB (Electronic CodeBook)

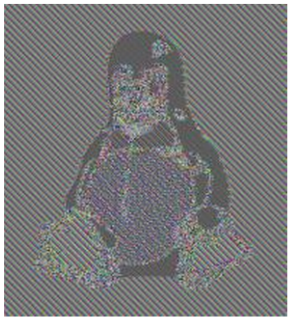


Electronic Codebook (ECB) mode encryption

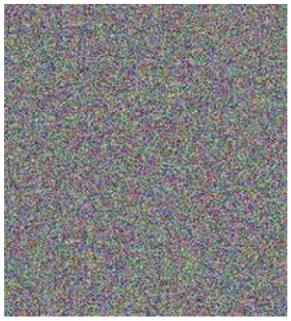
- Problemi?

- Se due plaintext sono uguali, anche i corrispondenti testi cifrati lo sono (possibili analisi di frequenza).

Original



Encrypted using ECB mode



Modes other than ECB result in pseudo-randomness

- Un attaccante può inserirsi e cambiare parte del messaggio senza essere scoperto (man-in-the-middle attack).
- Di fatto l'ECB non va mai utilizzato.
- si usano varie tecniche per ovviare a questo:
  - Cifratura randomizzata (Randomized encryption)

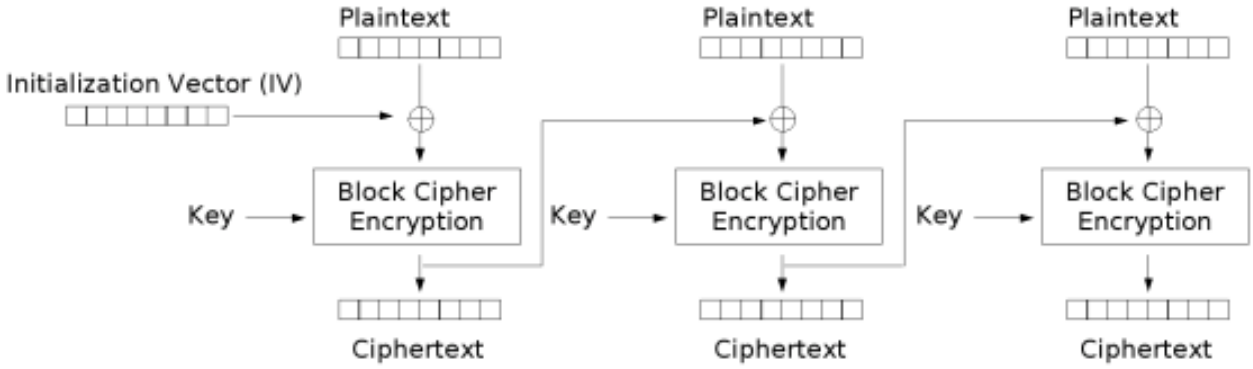
IND-CPA

- per molti messaggi lunghi cifrati con la stessa chiave (many-times key) si richiede che il CS soddisfi una richiesta più forte: IND-CPA (chosen plaintext attack)
- $\mathcal{A}$ avversario computazionalmente limitato - definiamo un esperimento EXP come segue:
  1. $\mathcal{A}$ sceglie due messaggi x_0 e x_1 in $\mathcal{P}$
  2. $\mathcal{U}$ sceglie una chiave in modo casuale e genera un CT $y = e_k(x_b)$, $b = 0$ o 1. $\mathcal{U}$ trasmette y a $\mathcal{A}$
  3. $\mathcal{A}$ ha accesso a una macchina cifrante: può ottenere la cifratura di alcuni messaggi di sua scelta, anche x_0 e x_1
  4. $\mathcal{A}$ produce un bit b', $b' = 0$ o 1.
  5. l'output dell'esperimento EXP è 1 se $b = b'$ ($\mathcal{A}$ ha indovinato) e 0 altrimenti
- Un CS è IND-CPA se per ogni avversario c. l. $\mathcal{A}$ si ha

$$\mathbf{Pr}(\ \mathrm{EXP} = 1) \leq \frac{1}{2} + \varepsilon, \text{ dove } \varepsilon \text{ è trascurabile}$$

Cipher Block Chaining

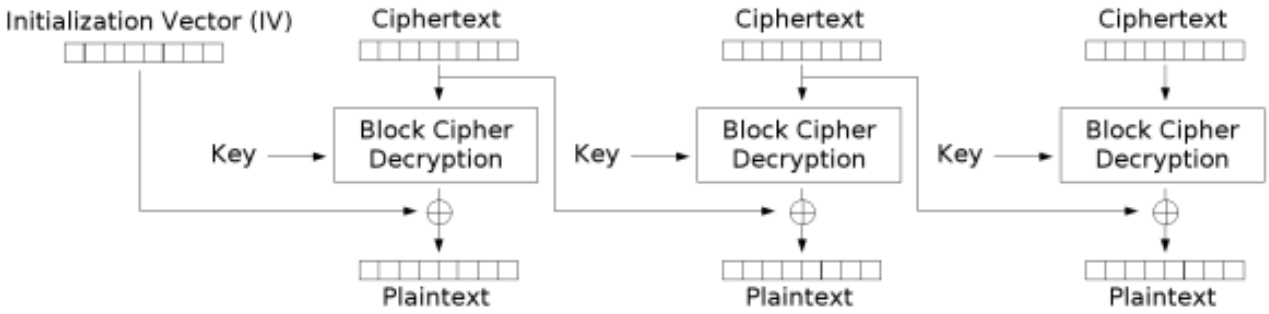
Nel metodo CBC, il plaintext è messo in XOR con il testo cifrato precedente prima di essere cifrato.



Cipher Block Chaining (CBC) mode encryption

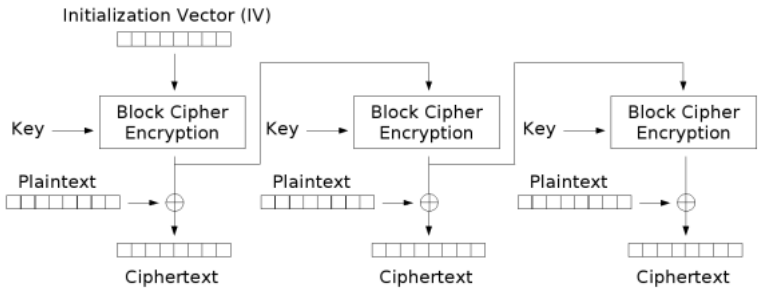
- È una cifratura randomizzata
- Bisogna generare e trasmettere l'IV
- Il CT diventa più lungo del PT: il primo blocco ricevuto saà l'IV
- l'IV non dev'essere segreto, ma deve essere random
- Nasconde eventuali pattern del plaintext
- La lunghezza del PT dev'essere un multiplo della lunghezza di un blocco: si introduce padding

Cipher Block Chaining – decifratura



Cipher Block Chaining (CBC) mode decryption

Output FeedBack



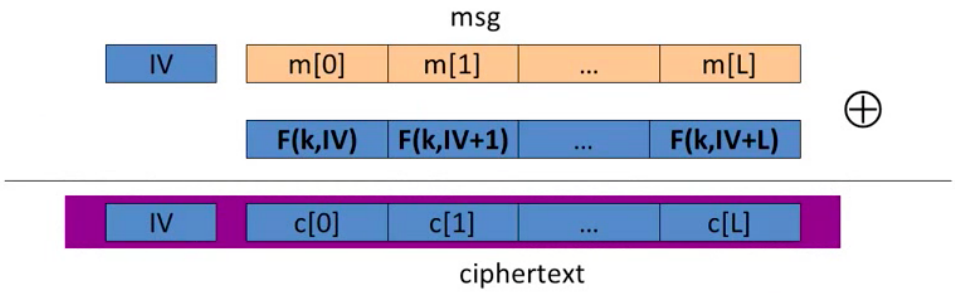
Output Feedback (OFB) mode encryption

- Usa il cifrario a blocchi come un generatore di numeri pseudocasuali.
- Il messaggio è cifrato con uno XOR (OTP)
- la chiave K dell'OTP si ha considerando

$$e_k(IV) = K_0, e_k(e_k(IV)) = e_k(K_0) = K_1, \ldots e_k(K_{i-1}) = K_i$$

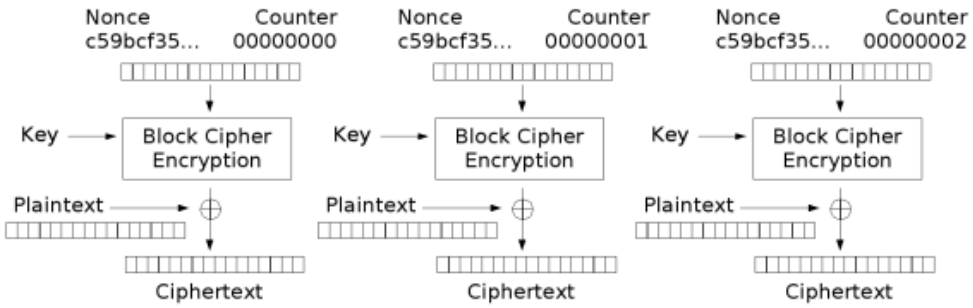
- Posso calcolare questa chiave prima di conoscere il PT da trasmettere

randomized counter mode



- Anche qui si usa il cifrario a blocchi come un generatore di numeri pseudocasuali.
- la chiave K dell'OTP si ha considerando $e_k(IV) = K_0, e_k(IV + 1) = K_1, \ldots, e_k(IV + i) = K_i$
- Posso calcolare questa chiave prima di conoscere il PT da trasmettere e in parallelo.

nonce-based counter mode



Counter (CTR) mode encryption

- invece di un IV random, si considera un nonce concatenato a un counter
- sia nell'OFB che nelle modalità counter, per decifrare si usa solo la cifratura del cifrario a blocchi (per calcolare la chiave OTP)