crittosistema: definizione

Definizione

Un crittosistema è una quintupla $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, dove

- ① $\mathcal{P}$ è un insieme finito di testi in chiaro (plaintext)
- ② $\mathcal{C}$ è un insieme finito di testi cifrati (ciphertext)
- ③ $\mathcal{K}$ è un insieme finito di chiavi. ($\mathcal{K}$ è detto spazio delle chiavi)
- ④ per ogni $k \in \mathcal{K}$ c'è una funzione di cifratura $e_k \in \mathcal{E}$,
 $e_k : \mathcal{P} \rightarrow \mathcal{C}$ e una funzione di decifratura $d_k \in \mathcal{D}$, $d_k : \mathcal{C} \rightarrow \mathcal{P}$
tali che, per ogni $x \in \mathcal{P}$ si ha

$$d_k(e_k(x)) = x$$

cifrari affini

$$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}$$

$$\mathcal{K} = \{(a, b) \mid a, b \in \mathbb{Z}_{26}, (a, 26) = 1\};$$

per ogni $(a, b) \in \mathcal{K}$, si ha

$$e_{(a,b)}(x) = ax + b, \quad \text{e} \quad d_{(a,b)}(y) = a^{-1}(y - b).$$

Esempio: sia $k = (5, 12)$,

allora si ha $e_{(5,12)}(x) = 5x + 12$,

e $d_{(5,12)}(y) = 21(y - 12) = 21y + 8$.

se $x = 3$, si ha $e_{(5,12)}(3) = 15 + 12 = 27 = 1$

e $d_{(5,12)}(1) = 21 + 8 = 29 = 3$

cifrari a trasposizione

$$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^m$$

abbiamo una m -pla di lettere;

$$\mathcal{K} = \{ \text{permutazioni di } \{1, 2, \dots, m\} \} = S_m$$

per ogni $\pi \in \mathcal{K}$, $x = (x_1, x_2, \dots, x_m) \in \mathcal{P}$,

$y = (y_1, y_2, \dots, y_m) \in \mathcal{C}$ si ha

$$e_\pi(x) = (x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(m)});$$

$$d_\pi(y) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \dots, y_{\pi^{-1}(m)});$$