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* $e_k \in \mathcal{E}$, $e_k : \mathcal{P} \to \mathcal{C}$ *e una funzione di decifratura* $d_k \in \mathcal{D}$, $d_k : \mathcal{C} \to \mathcal{P}$ *tali che, per ogni* $x \in \mathcal{P}$ *si ha*

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

cifrari a trasposizione

$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^m$
abbiamo una m-pla di lettere;
$\mathcal{K}$=\{ permutazioni di $\{1, 2, \ldots m\}$ \} $= S_m$

per ogni $\pi \in \mathcal{K}$, $x = (x_1, x_2, \ldots, x_m) \in \mathcal{P}$,
$y = (y_1, y_2, \ldots, y_m) \in \mathcal{C}$ si ha

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

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

cifrario di Vigenère

- è un cifrario polialfabetico
- m un intero positivo - sarà la lunghezza della chiave
- $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{26})^m$
- se $k = (k_1, k_2, \ldots, k_m)$ si ha
  - $e_k(x_1, x_2, \ldots, x_m) = (x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m)$
  - $d_k(y_1, y_2, \ldots, y_m) = (y_1 - k_1, y_2 - k_2, \ldots, y_m - k_m)$
- tutto modulo 26
- esempio: sia $m = 5$ e $k = (5, 8, 14, 17, 4)$
- se $x = (4, 0, 17, 17, 8)$, allora $e_k(x) = (9, 8, 5, 8, 12)$
- la crittoanalisi è molto più difficile!

cifrario di Hill

- è un cifrario polialfabetico
- m un intero positivo: $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$ pensati come vettori colonna
- $\mathcal{K} = \{$matrici $m \times m$ a coefficienti in $\mathbb{Z}_{26}$ invertibili in $\mathbb{Z}_{26}\}$
- $K \in \mathcal{K}$ è una matrice $m \times m$, $x \in \mathcal{P}$ è una m-pla; la cifratura è il prodotto righe per colonne
  - $e_K(x) = Kx$
  - $d_k(y) = K^{-1}y$
- tutto modulo 26
- la funzioni di cifratura e decifratura sono trasformazioni lineari
- quali sono le matrici invertibili in $\mathbb{Z}_{26}$?

- una matrice A a coefficienti reali è invertibile $\iff$ $\det(A) \neq 0$
- una matrice A a coefficienti in $\mathbb{Z}_n$ è invertibile $\iff$ $\det(A)$ è invertibile in $\mathbb{Z}_n$ $\iff$ $(\det(A), n) = 1$
- esempio: $n = 26$, $K = \begin{pmatrix} 11 & 3 \\ 8 & 7 \end{pmatrix}$, $\det(K) = 53 = 1$
- $K^{-1} = \begin{pmatrix} 7 & -3 \\ -8 & 11 \end{pmatrix} = \begin{pmatrix} 7 & 23 \\ 18 & 11 \end{pmatrix}$
- $e_K \begin{pmatrix} 2 \\ 2 \end{pmatrix} = \begin{pmatrix} 11 & 3 \\ 8 & 7 \end{pmatrix} \begin{pmatrix} 2 \\ 2 \end{pmatrix} = \begin{pmatrix} 28 \\ 30 \end{pmatrix} = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$
- $d_K \begin{pmatrix} 2 \\ 4 \end{pmatrix} = \begin{pmatrix} 7 & 23 \\ 18 & 11 \end{pmatrix} \begin{pmatrix} 2 \\ 4 \end{pmatrix} = \begin{pmatrix} 106 \\ 80 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$

cifrario lineare affine

- generalizza il cifrario di Hill
- m un intero positivo: $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{26})^m$
- $\mathcal{K} = \{(A, b), A \text{ matrice invertibile}, b \in (\mathbb{Z}_{26})^m\}$
- se $k = (A, b)$, si ha
  - $e_k(x) = Ax + b$
  - $d_k(y) = A^{-1}(y - b)$
- tutto modulo 26
- la funzioni di cifratura e decifratura sono trasformazioni affini
- quasi tutti i cifrari visti fino a ora sono di questo tipo!

crittoanalisi: principio di Kerckhoffs

L'attaccante, Eve, può conoscere il crittosistema usato da Alice e Bob.
Non conosce la chiave.
Vantaggi:

- è più facile tenere segreta la chiave
- se la sicurezza si basa sulla chiave, e la chiave viene scoperta, basta cambiare chiave
- si può usare lo stesso crittosistema per far comunicare diverse coppie di persone

- oggi il principio di Kerckhoffs viene inteso in maniera più forte: l'algoritmo deve essere pubblico
- un sistema che viene molto studiato (e attaccato) è più sicuro
- meglio che le debolezze, se ci sono, vengano scoperte e rese pubbliche
- se l'algoritmo è pubblico, non c'è rischio di reverse engineering
- si possono stabilire standard