

Elementi di crittografia

Francesca Merola

lezione 2

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

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

in un crittosistema, bisogna che
 $x, y \in \mathcal{P}, x \neq y, \Rightarrow e_k(x) \neq e_k(y)$; le funzioni di cifratura devono essere iniettive.

\mathcal{P} e \mathcal{C} sono insiemi *finiti*

se in un crittosistema si ha $\mathcal{P} = \mathcal{C}$,

una funzione $f : \mathcal{P} \rightarrow \mathcal{C} = \mathcal{P}$

è iniettiva \Leftrightarrow è suriettiva \Leftrightarrow è biiettiva

dunque in questo caso le funzioni di cifratura sono
permutazioni di \mathcal{P}

permutazioni

Se X è un insieme finito con n elementi
un'applicazione **biiettiva** $\pi : X \rightarrow X$ si dice **permutazione** di X .

Ci sono $n! = n \cdot (n - 1) \dots 3 \cdot 2 \cdot 1$ permutazioni di X .

L'insieme delle permutazioni di un insieme con n elementi
è un gruppo rispetto al prodotto operatorio fra applicazioni; per
 $n \geq 3$ è un gruppo non commutativo.

Si chiama il **gruppo simmetrico**, e si denota con S_n .

cifrari a sostituzione

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

$$\mathcal{K} = \{ \text{permutazioni di } \mathbb{Z}_{26} \} = S_{26}$$

per ogni $\pi \in \mathcal{K}$, si ha

$$e_{\pi}(x) = \pi(x), \quad e \quad d_{\pi}(y) = \pi^{-1}(y).$$

identificheremo \mathbb{Z}_{26} con l'alfabeto

esempio

sia π la permutazione

a	b	c	d	e	f	g	h	i	j	k	l	m
F	X	H	G	N	O	K	A	U	P	S	V	T
n	o	p	q	r	s	t	u	v	w	x	y	z
Q	L	M	D	I	R	Y	C	J	E	Z	B	W

allora π^{-1} è

A	B	C	D	E	F	G	H	I	J	K	L	M
h	y	u	q	w	a	d	c	r	v	g	o	p
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
e	f	j	n	s	k	m	i	l	z	b	t	x

c i v e d i a m o p o i
H U J N G U F T L M L U

Proprietà di un buon crittosistema:

- Dev'essere possibile calcolare ogni e_k e d_k in modo "efficiente";
- Eve non deve essere in grado di risalire alla chiave (o al testo in chiaro) dal testo cifrato.

Per i cifrari additivi, si hanno solamente 26 possibili chiavi!

Nel caso di una sostituzione generica, il numero di chiavi è molto alto

$$|\mathcal{K}| = 26! \approx 4 \cdot 10^{26}.$$

questo non basta a garantire la sicurezza!

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

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

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