Crittografia a chiave pubblica - CR410

Francesca Merola

informazioni

- orario:
  lunedì 16:00-18:00 aula M2
  mercoledì 14:00-16:00 aula M3
  venerdì 14:00-16:00 aula M4 (più o meno a settimane alterne)
- ricevimento: su appuntamento email
  studio 204
- pagina web:
  http://ricerca.mat.uniroma3.it/users/merola/
- email: `merola@mat.uniroma3.it`

Testi consigliati

- Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici
- D. Stinson: Cryptography - theory and practice
- Languasco, Zaccagnini: Manuale di crittografia
- Katz, Lindell: An introduction to modern cryptography
- B. Schneier: Applied Cryptography

schema del corso

- Introduzione alla crittografia. Cenni storici. Definizione di crittosistema. Cifrari classici. Introduzione alla crittoanalisi.
- Introduzione alla crittografia a chiave pubblica. Cenni di teoria della complessità. Problema dello zaino. Cifrario di Merkle-Hellman.
- Il crittosistema RSA. Test di primalità. Algoritmi di fattorizzazione. Alcuni attacchi all'RSA. Cifrario di Rabin.
- Il problema del logaritmo discreto. Scambio della chiave di Diffie-Hellman. Il crittosistema di Elgamal.
- Firma digitale. Schemi di firma. Lo schema RSA. Lo schema di Elgamal.
- Possibili varie: cenni su alcuni protocolli crittografici, cenni di crittografia post quantum.

crittografia

Crittografia - dal greco
$\kappa\rho\upsilon\pi\tau o\varsigma$, nascosto
$\gamma\rho\alpha\phi\epsilon\iota\nu$, scrivere

crittografia

crittologia

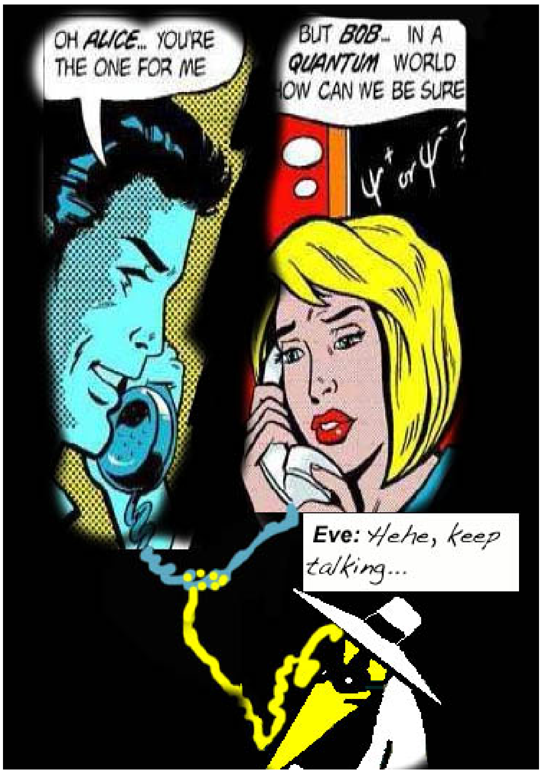
crittoanalisi

- classicamente, crittografia = nascondere il contenuto di un messaggio
- più di recente, molti altri usi:
  - autenticazione di un messaggio/interlocutore
  - scambio di una chiave segreta
  - firma digitale
  - condivisione di un segreto
  - e molto altro

Alice

$\Downarrow$

Bob



Alice

$\Downarrow$ $\leftarrow$ Eve

Bob

atbash - un cifrario a sostituzione


```
ABCDEFGHIJKLM
ZXYWVUTSRQPON
ciao → YRZL
```

la scitala - un cifrario a trasposizione

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*

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

se si ha $x, y \in \mathcal{P}$ con $x \neq y$,
allora dev'essere anche, per ogni chiave k, $e_k(x) \neq e_k(y)$;
le funzioni di cifratura devono essere iniettive.

cifrario additivo (shift cipher)

- $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$;
- fissiamo $0 \leq k \leq 25$; allora
  - $e_k(x) = (x + k) \bmod 26$,
  - $d_k(y) = (y - k) \bmod 26$.

Nota: quando $k = 3$, si ha il cifrario di Cesare.

Identifichiamo $\mathbb{Z}_{26}$ con l'alfabeto:

A 0	B 1	C 2	D 3	E 4	F 5	G 6	H 7	I 8
J 9	K 10	L 11	M 12	N 13	O 14	P 15	Q 16	R 17
S 18	T 19	U 20	V 21	W 22	X 23	Y 24	Z 25	

esempio

la chiave è $k = 9$

s	a	l	u	t	i	d	a	l	m	a	r	e
18	0	11	20	19	8	3	0	11	12	0	17	4
1	9	20	3	2	17	12	9	20	21	9	0	13
B	J	U	D	C	R	M	J	U	V	J	A	N

Nota: spesso si pensa la chiave come una lettera, non come un numero (in questo esempio la chiave è J).

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 al testo in chiaro (o peggio, alla chiave) dal testo cifrato.

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

Provare a decrittare il messaggio

L	E	E	P	Y	E	T	L	W	N	L	Y	P
a	t	t	e	n	t	i	a	l	c	a	n	e

la chiave è 11 (oppure L)

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 $f : \mathcal{P} \longrightarrow \mathcal{C} = \mathcal{P}$
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 $\pi : X \to X$ si dice permutazione di X.

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

L'iniseme delle permutazioni di un insieme con n elementi;
si denota con S_n.

cifrari a sostituzione

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

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

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

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

$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26}^m$
abbiamo una m-pla di lettere;
$\mathcal{K}$={ 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

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

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

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 $k = (k_1, k_2, \dots, k_m)$ si ha
  - $e_k(x_1, x_2, \dots, x_m) = (x_1 + k_1, x_2 + k_2, \dots, x_m + k_m)$
  - $d_k(y_1, y_2, \dots, y_m) = (y_1 - k_1, y_2 - k_2, \dots, y_m - k_m)$
- 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!