Elementi di crittografia

Francesca Merola

informazioni

- orario: ma-me 9.15 - 11, aula N2
- ricevimento: su appuntamento
  martedì 11.00 – 12.30
  studio 300 dipartimento di matematica
- pagina web:
  http://ricerca.mat.uniroma3.it/users/merola/
- email: `merola@mat.uniroma3.it`

Testi consigliati

- D. Stinson: Cryptography - theory and practice
- Languasco, Zaccagnini: Introduzione alla crittografia
- Baldoni, Ciliberto, Piacentini: Aritmetica, crittografia e codici
- Katz, Lindell: An introduction to modern cryptography
- W. Stallings: Crittografia e sicurezza delle reti.
- B. Schneier: Applied Cryptography

schema del corso

- crittografia classica
- cifrari a blocchi e cifrari a flusso
- SPN, cifrario di Feistel, DES, AES
- crittografia a chiave pubblica
  - cifrari basati su fattorizzazione: RSA
  - cifrari basati sul logaritmo discreto: El Gamal
  - firma digitale
- alcuni protocolli crittografici

crittografia

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

crittografia

crittologia

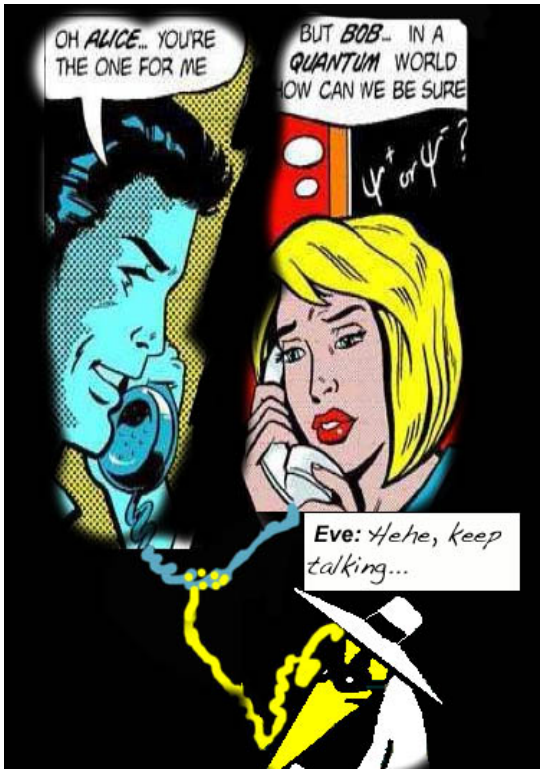
crittoanalisi

- 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

⇓

Bob



Alice

⇓

← Eve

Bob

la scitala - un cifrario a trasposizione

atbash - un cifrario a sostituzione

ABCDEFGHIJKLM
ZXYWVUTSRQPON
ciao $\rightarrow$ YRZL

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

esercizio

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
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

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

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!