Elementi di crittografia

Francesca Merola

marzo-maggio 2012

informazioni

- orario: lu, (me), gio, 9.45 - 11.15, aula N21
- ricevimento: su appuntamento
  lu, gio, 11.30-12.30
  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
- 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

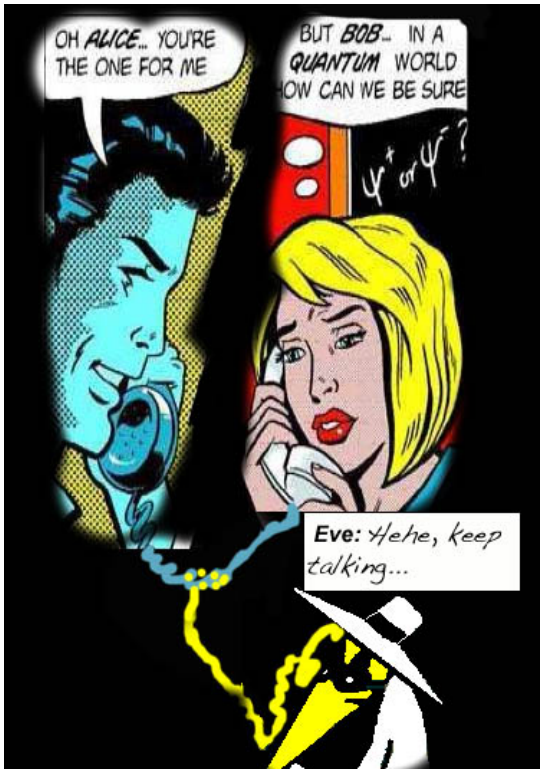
crittoanalisi

- 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!!

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)