Storia ed Evoluzione della CRITTOGRAFIA

L'evoluzione storica delle tecniche per crittografare i dati e le comunicazioni

Fabio GESARIN

Università degli Studi di Napoli "Federico II"
SICSI VIII Ciclo – Indirizzo Tecnologico - Classe A042
"Storia dell'Informatica e del Calcolo Automatico"
Prof. Aniello MURANO

Innanzitutto diciamo cosa significa CRITTOGRAFIA

La parola CRITTOGRAFIA deriva dall'unione di due parole greche: kryptós che significa nascosto, e gráphein che significa scrivere.

Dunque la crittografia tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile a persone non autorizzate a leggerlo. Un tale messaggio si chiama comunemente crittogramma.

NOTA: lo studio della Crittografia e della Crittanalisi si chiama comunemente Crittologia.

PRIME FORME e applicazioni della Crittografia nelle guerre antiche

Perché nasce la necessità di offuscare un messaggio?

Semplice… per comunicare in guerra evitando di far scoprire al nemico le proprie mosse!

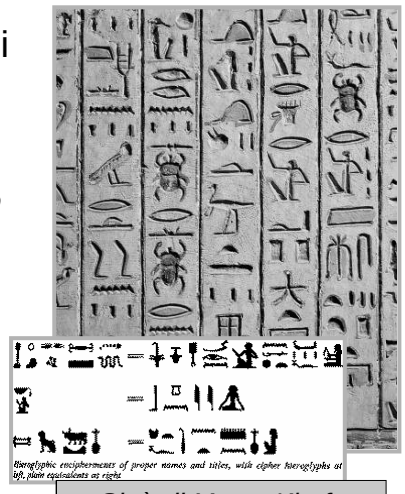
Scitala Spartana 404 a.C.

Infatti la Scitala degli Spartani era un sistema semplice di crittografia per trasposizione (o permutazione) in quanto basato su una striscia di stoffa contenente un messaggio leggibile se avvolta ad una bacchetta (detta appunto "Scitala") di diametro uguale a quello con cui la striscia di stoffa veniva scritta inizialmente.

PRIME FORME e applicazioni della Crittografia nelle civiltà antiche

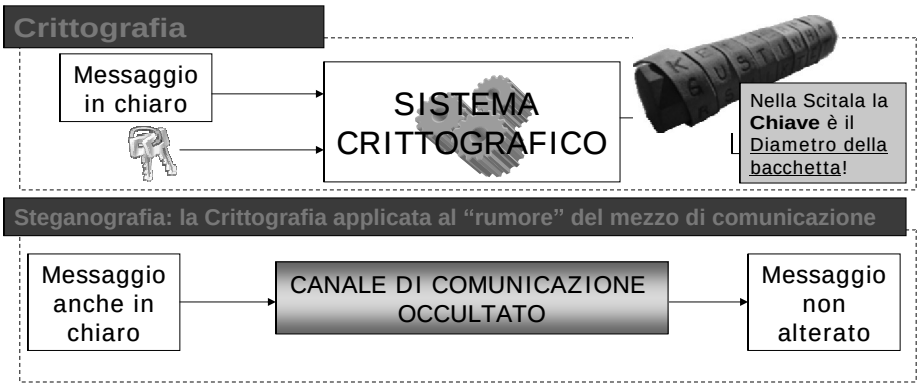
In realtà le tecniche crittografiche sono ancora più antiche di quanto si pensi:

- nel 480 a.c. i greci usarono la *Steganografia* nelle guerre raccontate da Erotodo contro i Persiani
- sono stati ritrovati *Geroglifici Non Standard o parzialmente riprodotti*
- già gli Ebrei usavano un cifrario chiamato *Atbash* di cui si parla anche nella Bibbia



Città di Menet Khufu (Nilo), 4000 anni fa: incisione funebre con parole trasformate per conferire dignità e onorificenza al defunto.

Qualche precisazione doverosa…



NOTA: la differenza principale fra Crittografia e Steganografia sta, in termini sintetici, nel fatto che ad essere crittato non è il contenuto ma il canale di comunicazione.

5

Un esempio di … Steganografia

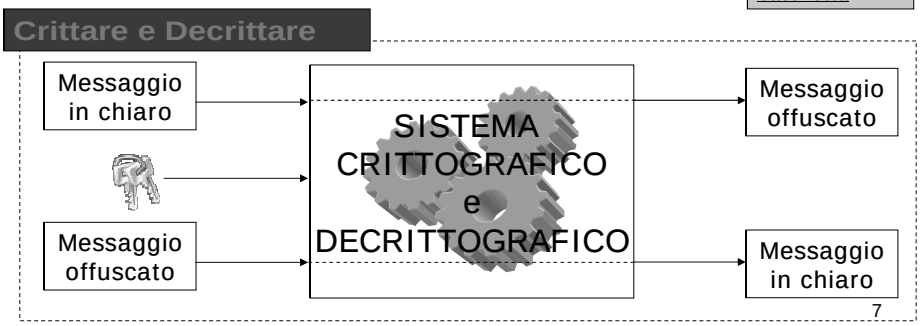
Filmato "la pelata" tratto dalla presentazione "Crittografia" di Gabriele Barni.

6

Torniamo alla Crittografia e parliamo anche di decrittare …

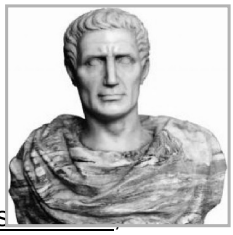
- Nell'uso della Scitala, le bacchette per scrivere il messaggio su essa (crittare) e per leggerlo (decrittare) devono essere dello stesso spessore (la chiave).

Nella Scitala la **Chiave** è il Diametro della bacchetta!



7

Torniamo alla Storia … Cifrari MonoAlfabetici



- Cifrario di Cesare

  Il primo *Cifrario Monoalfabetico*, detto anche a Sos… ogni lettera del messaggio in chiaro viene sostituita con una o più lettere dell'alfabeto secondo una regola prefissata. Tramite gli scritti di Svetonio sappiamo che Cesare cifrava tutta la sua corrispondenza con Augusto e perfino alcune parti del De Bellum Gallico.

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z	A	B	C

METODO: *sostituzione dopo 4 lettere nella sequenza alfabetica (la chiave è il numero "4").*

8

Tecniche dei Metodi Crittografici sinora visti

- Permutazione
  delle stesse lettere del messaggio come nella Scitala Spartana

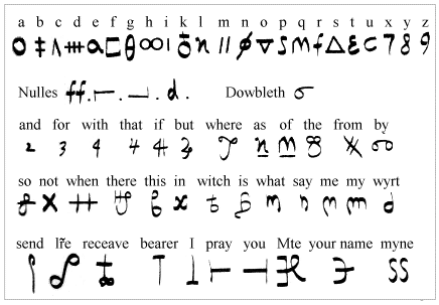
- Sostituzione
  mediante "shift" costante con altre lettere dell'alfabeto come nel Cifrario di Cesare

9

… il Nomenclatore, anno 1000 d.c. …

- Intorno all'anno mille, e alla nascita delle prime ambasciate, vi è un forte ritorno all'utilizzo della crittografia.
  Il metodo usato è noto come Nomenclatore, un elenco di parole che si usano frequentemente e che venivano cifrati utilizzando una serie di simboli o parole convenzionali.

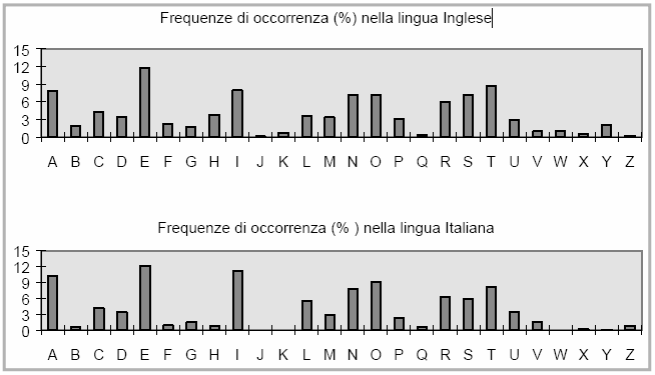
La regina Maria Stuarda è stata condannata a morte nel 1586 perché di fronte a una forte Crittoanalisi il metodo di cifratura usato nelle sue corrispondenze crollò!



METODO: ***sostituzione simbolica (la chiave è …).***

… la Crittanalisi, come, dove, quando

- La Crittanalisi è l'anti-crittografia!



La prima tecnica di analisi è quella basata sulle frequenza con cui si ripetono

lettere_o_simboli/loro_sequenze

nel messaggio cifrato, è nasce dalla semplice considerazione che in ogni messaggio in chiaro (e quindi nella lingua con cui è scritto) si usano con maggiore frequenza certe

lettere/parole!

11

Un Primo Confronto tra ieri e oggi …

- Fino all'anno 1000 è ancora una crittografia debole (anche basata sull'analfabetismo) che l'uomo riesce da solo a decifrare e senza troppi sforzi nonostante la Chiave e il Sistema adoperato non fossero noti!
- Ai nostri giorni i Sistemi Standard di Crittografia sono noti ma tuttavia le capacità di calcolo umane non sono più sufficienti!!

12

1550 circa, qualcosa di nuovo sotto al sol … o meglio, in segreto

- Sino ad allora la Crittanalisi delle frequenze letterali sfondava qualunque Sistema MonoAlfabetico (Cifrario di Cesare e affini)!

Blaise de Vigenère, ripredendo le idee:

- dell'italiano Leon Battista Alberti (architetto-crittologo, scrisse "De Cifris" nel 1466 e propose un *Cifrario MonoAlfabetico a Chiave variabile per singola parola*);
- altri Crittologi dell'epoca come l'abate Johannes Tritemius;

sviluppò un Cifrario PoliAlfabetico, il cosiddetto "Cifrario Indecifrabile"…

13

… "le chiffre indéchiffrable" di *de Viger*

- Cifrario PoliAlfabetico
- A partire dalla Tabella degli Alfabeti, si consideravano quelli corrispondenti alle lettere di una parola prefissata
- Tale parola diveniva la Chiave

Esempio da cifrare:	"attaccare da ovest all'alba"
Chiave:	"alb"
Algoritmo:	ATTACCARE DA OVEST ALL'ALBA ALBALBALB AL ALBAL ALB'ALBA
Crittografato:	AEU…

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Considerazioni Crittoanalitiche sul Cifrario Indecifrabile

- Per quasi 300 anni il Cifrario di *de Vigenère* rimase inviolato a causa del numero enorme di chiavi possibili
- Nel 1861 Friederich Kasiski ci riuscì facendo una semplice constatazione: nei messaggi crittografati con cifrari polialfabetici si osservano delle ripetizioni quando la stessa lettera di un testo in chiaro si trova ad una distanza pari alla lunghezza della chiave, o al più un suo multiplo!!

Esempio da cifrare:	"attaccare da ovest all'alba"
Chiave:	"alb"
Algoritmo:	ATTACCARE DA OVEST ALL'ALBA ALBALBALB AL ALBAL ALB'ALBA
Crittografato:	AEUA…

Il Problema è la lunghezza della chiave: a questo punto più è lunga e più è difficile osservare ripetizioni!!

15

La Crittografia e la Crittanalisi si rincorrono…

- Siamo nel 1917 e l'ingegnere **Vernam** dei Bell Labs inventò un cifrario con chiave lunga quanto il messaggio da cifrare e da adoperare una sola volta (One Time Pad):
  - sotto queste condizioni, esso è il primo cifrario di cui è stata dimostrata l'inviolabilità;
  - tale Cifrario è stato perfezionato in diversi modi, adoperato nella guerra fredda
    e, attualmente, un suo perfezionamento è alla base dell'algoritmo RC4 diffuso su Internet e nei protocolli delle Reti Wireless;
  - è comunque un sistema tutt'altro che semplice da automatizzare per quegli anni.

16

II Guerra Mondiale: Enigma

- Siamo negli anni successivi al Cifrario di Vernam che vedono la fioritura di diversi dispositivi elettro-meccanici di cifratura indispensabili per adoperare sistemi crittografici più complessi e quindi non più banali e immediati per le capacità di calcolo dell'uomo.
- Enigma è il più famoso dispositivo di Cifratura adoperato dai Nazisti brillantemente attaccato dal matematico Rejewsky tanto che il suo lavoro servi a Turing e altri per decifrare molti messaggi in favore degli Alleati.

17

Enigma: il video …

Filmato "Enigma Demo" tratto dalla presentazione "Crittografia" di Gabriele Barni.

18

Il Dopoguerra: la Crittografia e il Computer

- Vengono sviluppati Algoritmi particolarmente adatti ad essere implementati tramite Computer.
- Il più famoso Algoritmo di Cifratura è il Data Encryption Standard (DES) realizzato dalla IBM intorno al 1970 e usato dal Governo Statunitense fino al 2001 per documenti non classificati!!
- Ebbene, già nel 1998 un messaggio crittografato in DES con chiave a 56 bit venne forzato in poco più di 60 ore!!!

19

Una rivoluzione: la Crittografia a Chiave Pubblica (o Asimmetrica)

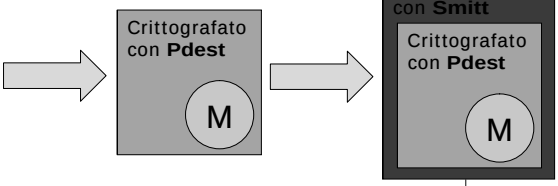
- L'algoritmo **RSA**,
  brevettato da tre ricercatori del MIT, si basa sulla possibilità di creare dei cifrari a chiave asimmetrica. Oggi l'algoritmo RSA è ritenuto di massima affidabilità anche se in realtà non è sicuro in termini puramente matematici:
  - un documento cifrato con una chiave può essere decifrato con l'altra e viceversa;
  - la chiave che cifra non può decifrare lo stesso file;
  - la chiave privata è posseduta dal destinatario ed è segreta;
  - la chiave pubblica è accessibile a tutti i mittenti.

20

La figlia della Crittografia a Chiave Pubblica: la Firma Digitale

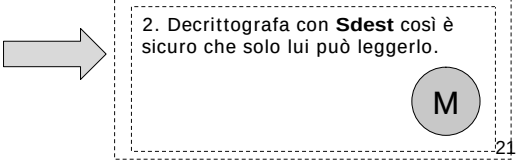
Il Mittente di un Messaggio **M** caccia la lingua agli spioni!
Egli possiede:

1. una sua Chiave Segreta **Smitt**
2. la Chiave Pubblica del Destinatario **Pdest**



Il Destinatario del Messaggio **M** è pensieroso per i possibili spioni?!
Egli possiede:

1. una sua Chiave Segreta **Sdest**
2. la Chiave Pubblica del Mittente **Pmitt**



21

Il futuro: la Crittografia a Quanti e i Computer Quantici

- La **Crittografia Quantistica**

  nella trasmissione dei messaggi è basata sulle proprietà di polarizzazione dei Fotoni
  e, per il "Principio di Indeterminazione di Heisenberg", un attacco del tipo "Man In The Middle" altererebbe irrimediabilmente il messaggio trasmesso invalidandolo e avendo la certezza di un terzo in ascolto.

  Ma se anche la Crittanalisi adoperasse informazioni Quantistiche...
  magari basate sulle possibili interferenze di un campo gravitazionale per avere informazioni sui fotoni di passaggio
  … ma questa per ora è fantascienza!

- Dal suo canto la Crittanalisi, grazie alle illimitate potenze di calcolo dei **Computer a Quanti**, potrebbe decifrare in brevissimo tempo messaggi crittografati con i più attuali algoritmi.

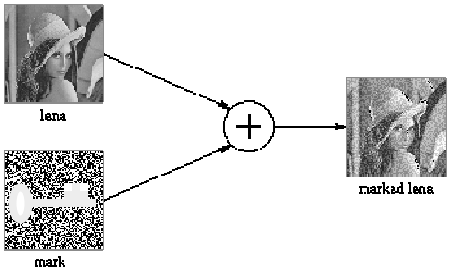
22

La Crittanalisi Quantistica al Cinema…

23

Altre applicazioni …

- Il WaterMarking pensato per proteggere l'autenticità delle opere digitali mediante una firma/messaggio anche crittografato (è cmq un esempio di Steganografia):



24

NOTE CURIOSE … la Crittografia nel quotidiano

Il sistema ROT13 che traspone di 13 lettere ognuna delle 26 lettere dell'alfabeto, è uno dei metodi crittografici largamente diffusi per il grande pubblico:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ
NOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLM
```

- In alcune riviste (generalmente di enigmistica) le soluzioni o i suggerimenti agli enigmi vengono presentati nella stessa pagina ma "debolmente criptati" per non consentire una rapida lettura a vista.
- In alcune riviste di intrattenimento, un commento sul finale di un film viene criptato in modo da rispettare la volontà del lettore che non vuole conoscere subito il commento.

25

Bibliografia e Webografia

"Codici e Segreti" di Simon Sigh, RIZZOLI

Supplemento a PC Professionale n. 122 del di maggio 2001
"*i Quaderni n. 2 – Sicurezza"*, MONDADORI INFORMATICA

"Segreti, Spie, Codici Cifrati" di Giustozzi, Monti e Zimuel, APOGEO

Presentazione "Introduzione alla Crittografia" di Enrico Zimuel
http://www.sikurezza.org/wiki/Risorse/Webbit02

Articolo su Internet intitolato "A scuola di crittografia quantistica"
http://www.mentelocale.it/festivaldellascienza/contenuti/index_html/id_contenuti_varint_16562

Presentazione di Crittografia Classica – Università di Salerno
http://www.dia.unisa.it/~ads/corso-security/www/CORSO-0102/crittografia-classica.pdf

Presentazione di Crittografia Classica – Università di Bologna
http://edenti.deis.unibo.it/LabICT/2003-2004/slide-x6/Sicurezza2.pdf

Articolo e Presentazione di Crittografia con video di Gabriele Barni
http://www.gabry.eu/blog/e-book-gratis-crittologia/

Articoli di WikiPedia.it

26