

Crittografia e Sicurezza Informatica

Sebastiano Fabio Schifano

University of Ferrara and INFN-Ferrara

February 10, 2016

Talk Outline

1 PEC: Posta Elettronica Certificata

2 Crittografia Informatica

- Steganografia vs Crittografia
- Crittoanalisi
- Storia della crittografia

3 Come Realizzare un Sistema Crittografico

- Crittografia a Chiave Simmetrica
- Crittografia a Chiave Asimmetrica

4 Applicazioni della Crittografia

- Digest
- Firma Digitale
- Certificato Digitale

5 Crittografia Grafica

Posta Elettronica Certificata

Da Wikipedia:

La posta elettronica certificata (PEC) è uno strumento che permette di dare ad un messaggio di posta elettronica lo stesso valore legale di una raccomandata con avviso di ricevimento tradizionale.

*La PEC può certificare il contenuto del messaggio solo se in combinazione con un **certificato digitale**, ovvero una **firma digitale** che permette di identificare il mittente in modo univoco.*

?????

firma digitale ? certificato digitale ?

Steganografia vs Crittografia

steganografia

stèganos (nascosto) + *graphía* (scrittura).

- tecnica risalente all'antica Grecia
- si prefigge di **nascondere** la comunicazione tra due interlocutori
- tecnica utilizzata in passato ma anche dai terroristi "moderni" !
- permette di nascondere un messaggio segreto all'interno di un messaggio pubblico

crittografia

kryptós (nascosto) e *graphía* (scrittura).

- tecnica più recente
- mirata a rendere **incomprensibile** un messaggio per chiunque tranne che per il destinatario.

Esempio di Steganografia

Secondo Erodoto i Greci usarono più volte la steganografia nella guerra contro i Persiani di Serse:

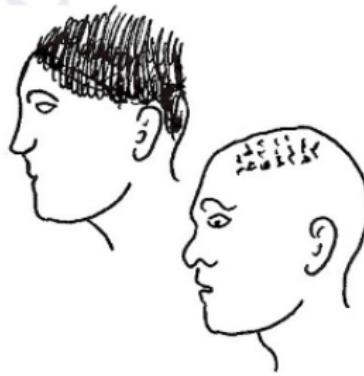
"Infatti, il pericolo di essere scoperti era grande; gli [] venne in mente un solo modo di far giungere in patria l'avviso: grattar via la cera da un paio di tavolette per scrittura, annotare sul legno sottostante le intenzioni di Serse, e ricoprire il messaggio con cera nuova. In tal modo le tavolette, che sembravano vergini, furono recapitate senza insospettire le guardie. Quando il messaggio giunse a destinazione, mi risulta che nessuno immaginò la sua esistenza, finché Gorgo, moglie di Leonida, ebbe una premonizione e disse che, grattando via la cera, sul legno sarebbe apparsa una scritta. Fu fatto così, il messaggio fu trovato e letto, poi riferito agli altri greci."*

[*] a Demarato, esule greco in Persia, ma ancora fedele alla patria natia.

Esempio di Steganografia

Altro aneddoto raccontato da Erodoto:

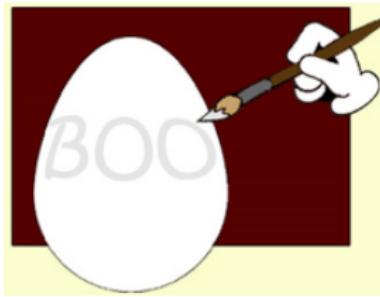
Istieo voleva incoraggiare Aristagora di Mileto a ribellarsi al re persiano. Per far giungere le relative istruzioni in modo sicuro, egli fece rasare il capo a un corriere, gli scrisse il messaggio sulla cute e aspettò che gli ricrescessero i capelli.



NdR: evidentemente Istieo non aveva molta fretta ... erano altri tempi !

Esempio di Steganografia

- Nel XVI secolo il filosofo e alchimista Giovanni Battista Della Porta consigliava di scrivere sul guscio di un uovo sodo usando una soluzione di mezzo litro di aceto e 30 g. di allume
- La soluzione penetra nel guscio senza lasciare traccia, ma tinge l'albuminato solidificato sottostante



[http://www.wonderhowto.com/wonderment/
send-secret-messages-hard-boiled-eggs-0113016/](http://www.wonderhowto.com/wonderment/send-secret-messages-hard-boiled-eggs-0113016/)

Esempio di Steganografia

Alice e Bruno si accordano sull'uso di un sistema steganografico:

il numero di virgole presente in una singola pagina sarà tra 1 e 21, questo numero corrisponderà ad una lettera dell'alfabeto.

Qualora Alice e Bruno dovessero trovarsi in un regime di comunicazione controllata:

- potrebbero scrivere pagine di copertura narrando informazioni prive di senso,
- ma facendo un uso accurato delle virgole, riuscirebbero a nascondere il vero messaggio con questa tecnica steganografica.

Scopo della Crittografia

La crittografia serve a:

- **nascondere** il significato del messaggio rendendolo incomprensibile
- garantire l'**autenticità** del messaggio
- **identificare** l'autore del messaggio
- **firmare** e datare il messaggio

Crittoanalisi

Crittoanalisi

kryptós (nascosto) + *analýein* (scomporre").

Un potenziale avversario si prefigge l'obiettivo di:

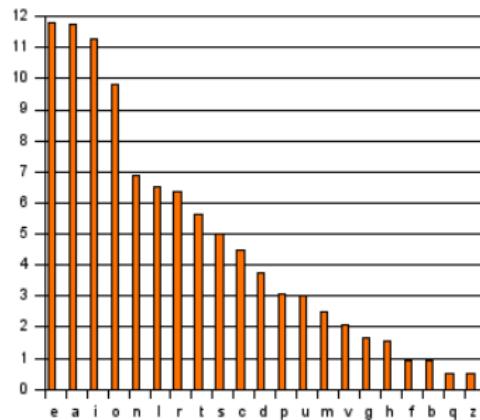
- comprendere il significato del messaggio
- alterare il messaggio
- rimuovere o modificare l'autore
- rimuovere o modificare la firma e/o la data

La *crittoanalisi* studia i metodi per ottenere il significato di informazioni cifrate senza avere accesso all'informazione segreta che è di solito richiesta per effettuare l'operazione.

Analisi delle Frequenze

Nella crittoanalisi, l'analisi delle frequenze è lo studio della frequenza di utilizzo delle lettere o gruppi di lettere in un testo cifrato. Questo metodo è utilizzato per violare i cifrari classici.

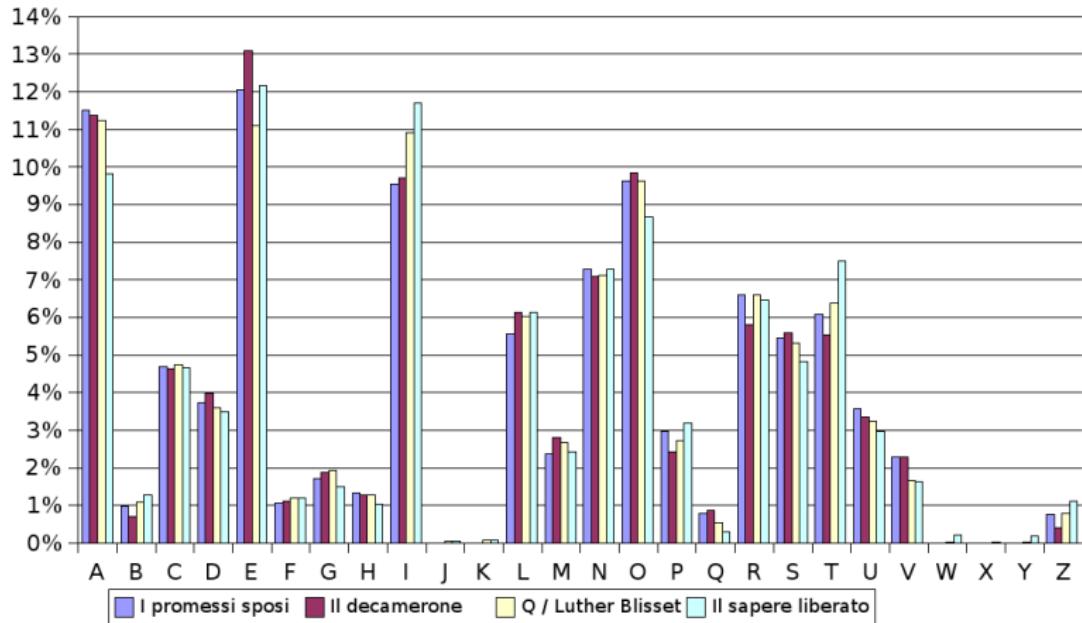
L'analisi può ad esempio essere fatto su un campione rappresentativo della lingua del messaggio da decifrare: es. *Divina Commedia*.



In un testo in cui un certo simbolo appare oltre il 12% delle volte si può intuire che quel simbolo potrebbe corrispondere alla lettera E.

Analisi delle Frequenze

Analisi di frequenza di 4 testi italiani: due classici un romanzo e un saggio.



- **frequenti:** E, A, I, O
- **Comuni:** N, R, T, L, S, C, D
- **Rare:** B, F, H, Q, Z
- **Assenti:** J, K, W, X, Y

Glossario

- **testo in chiaro (plaintext):**
testo o file nella sua forma normalmente utilizzabile
- **testo cifrato (ciphertext) o crittogramma:**
testo o file nella sua forma cifrata
- **cifratura:**
operazione che permette di passare da un testo in chiaro ad un testo cifrato
- **codice:**
regola per sostituire ad un'informazione un altro oggetto
- **decrittazione:**
operazione che permette di passare dal testo cifrato al testo in chiaro ad utente diverso da colui per il quale il messaggio era inteso
- **cifrario (cypher):**
algoritmo utilizzato per eseguire operazioni di cifratura e decifrazione
- **chiave (key):**
parametro che rende variabile la cifratura, se la cifratura non è debole basta tenere segreta la chiave per ottenere l'effetto di tenere segreto l'intero testo
- **coppia di chiave (key pair):**
coppia di parametri usati dalla nuova crittografia asimmetrica: quando una delle due chiavi viene usata per la cifratura serve l'altra per decifrare

Atbash

Atbash

è un semplice cifrario a sostituzione *monoalfabetica* in cui la prima lettera dell'alfabeto è sostituita con l'ultima, la seconda con la penultima, e così via, "invertendo" l'ordine alfabetico delle lettere.

Esempio, nel caso dell'alfabeto italiano:

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

- l'origine di questo cifrario si può trovare nella Bibbia, nel libro di Geremia
- per codificare le parole *Kasdīm* (Caldei) in *Leb Kamai* e
- *Babel* (Babele) in *Sheshakh* (nell'alfabeto ebraico).

Il procedimento da utilizzare per *decifrare* è **identico** a quello per *cifrare*.

Scitala

- dal greco bastone, è una bacchetta *rastremata*
- utilizzata dagli Spartani per trasmettere messaggi segreti
- il messaggio scritto su una striscia di pelle arrotolata attorno alla scitala
- srotolata la striscia di pelle era impossibile capire il messaggio
- la decifrazione richiede una bacchetta identica alla scitala del mittente
- il più antico metodo di crittografia per trasposizione conosciuto.



Cifrario di Cesare

Esempio di cifrario a sostituzione mono-alfabetico

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

- ogni lettera è sostituita dalla lettera K posizione dopo
- nel caso di Cesare $K = 3$

Se I è un letterale del messaggio in chiaro ($(I' = I + 3) \text{ mod } 21$) è il letterale del messaggio cifrato.

Esempio: AVE CAESARE diventa DBE FDHVDUH

Primo esempio di aritmetica dell'orologio o aritmetica in modulo !

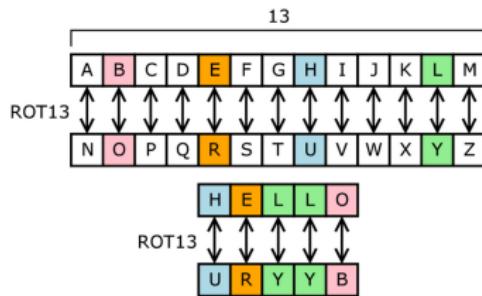
Osservazioni:

- **preserva gli spazi**
- **a lettera uguale corrisponde simbolo uguale!**

OKKIO alla critto-analisi !

ROT13

- *rotate by 13 places* noto in italiano come *eccesso 13*,
- è un semplice e debole cifrario monoalfabetico,
- è una variante del cifrario di Cesare ma con chiave 13: ogni lettera è sostituita con quella posta 13 posizioni più avanti nell'alfabeto.



Utilizzato per *rottare* (offuscare) un testo:

- chiaro: **l'assassino e' Mario Rossi**
- rottato: **y'nnfnvab r' znevb rbffv**

Es: Utilizzato dai giornali per nascondere la soluzione ad un quiz !!

I pizzini di Provenzano

- Un rudimentale sistema di cifratura basato sul cifrario di Cesare è stato usato anche da *Bernardo Provenzano* per proteggere informazioni rilevanti scritte nei suoi famosi **pizzini**,
- i piccoli foglietti di carta con i quali il boss della mafia, durante la sua latitanza, riceveva informazioni e impartiva ordini.
- Il sistema scelto da Provenzano era abbastanza semplice: si trattava di sostituire ad ogni lettera il numero corrispondente alla posizione nell'alfabeto più 3 e di comporre così un singolo, lungo numero.

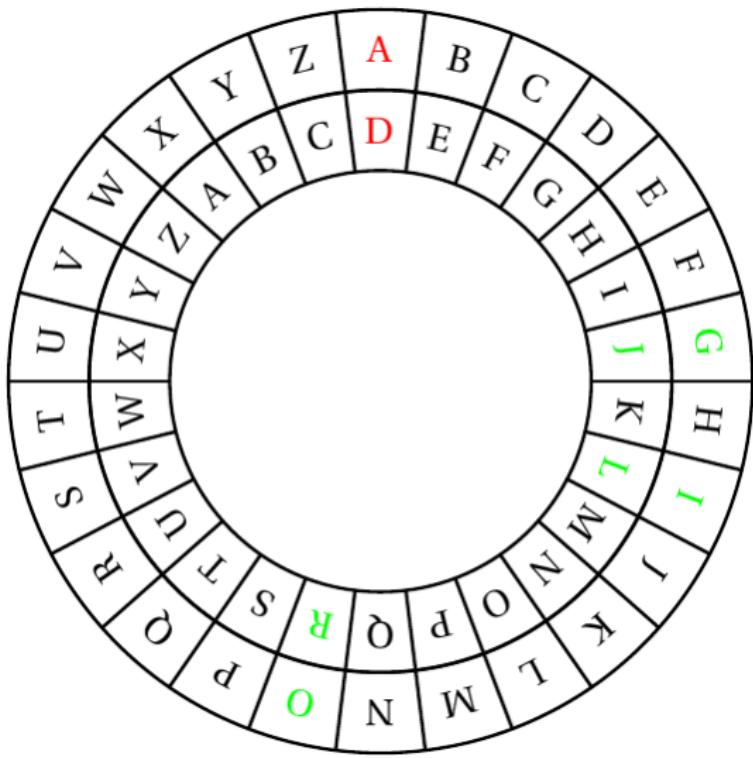
Ad esempio:

- i numeri "512151522 191212154" nascondono il nome di "Binnu Riina"
- infatti, $5 = 2$ (posizione della B) + 3
- $12 = 9$ (posizione della I) + 3, ecc ...

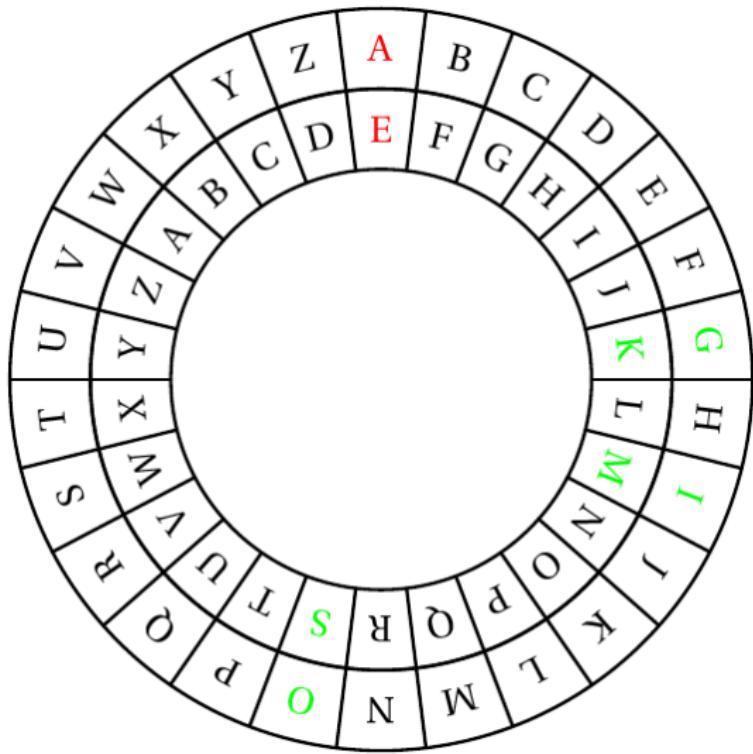
<http://www.anti-phishing.it/news/articoli/news.10052006.php>

Disco Cifrante di Leon Battista Alberti

- chiave D: OGGI \Rightarrow RJJL

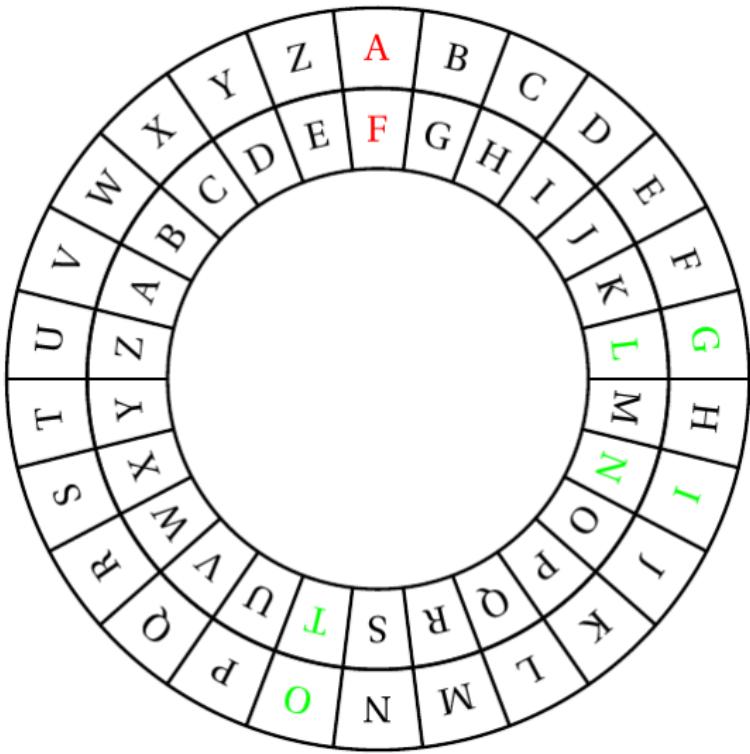


Disco Cifrante di Leon Battista Alberti



- chiave E: OGGI \Rightarrow SKKM

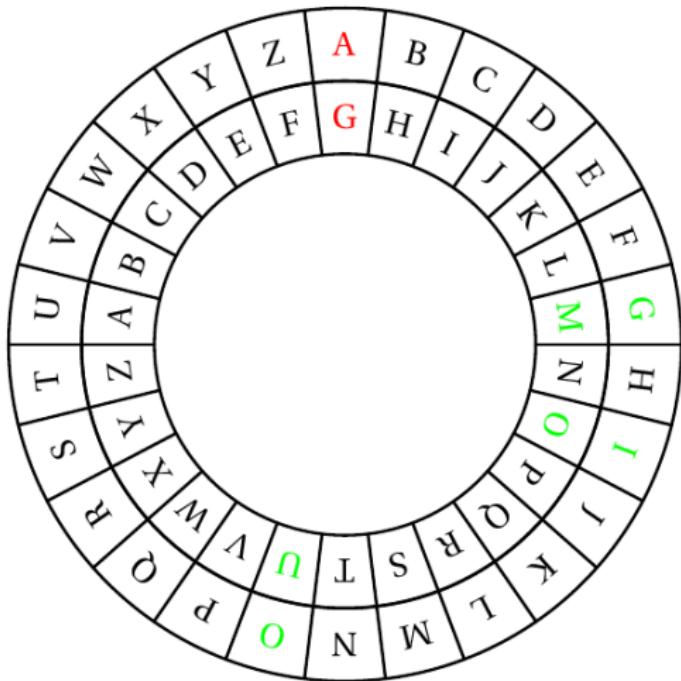
Disco Cifrante di Leon Battista Alberti



- chiave F: OGGI \Rightarrow TLLN

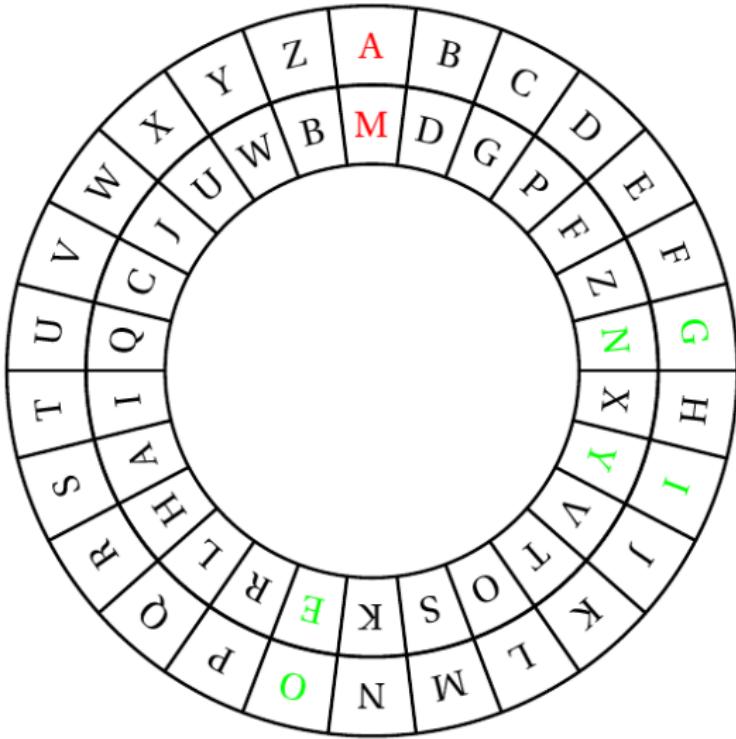
Disco Cifrante di Leon Battista Alberti

- chiave G: OGGI \Rightarrow UMMO



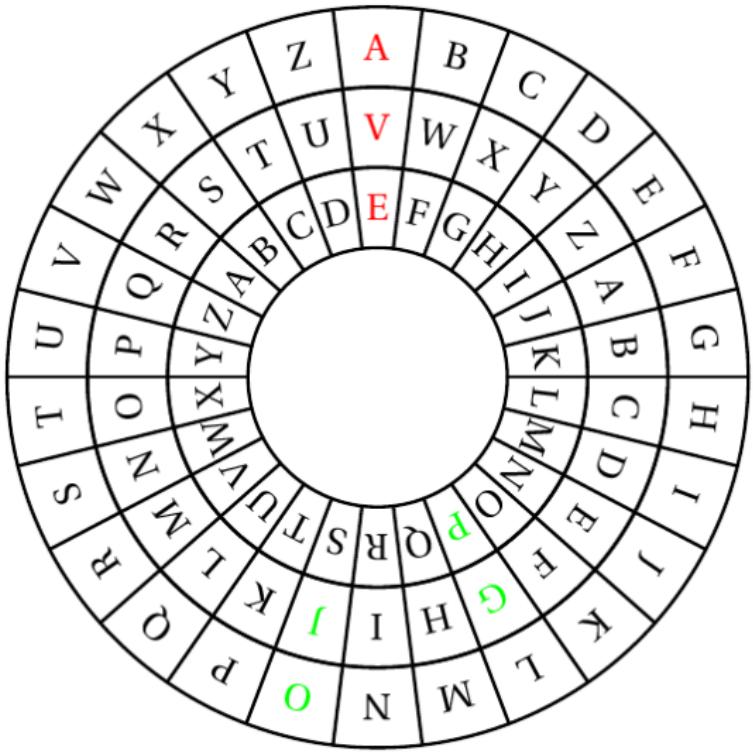
Disco Cifrante di Leon Battista Alberti

- chiave M: OGGI \Rightarrow ENNY
- variante di Cesare
- sostituzione mono-alfabetica



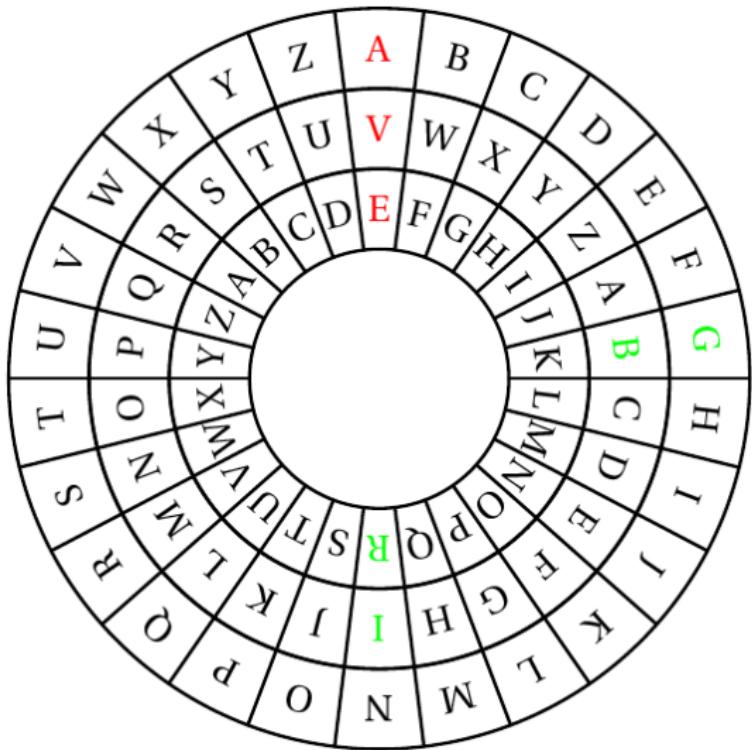
Disco Cifrante di Vigenère

- chiave **VE**: **OG** ⇒ **JP**



Disco Cifrante di Vigenère

- chiave **VE**: **OGGI** ⇒ **JPBR**
- lettere uguali possono essere sostituite con lettere diverse
- sostituzione poli-alfabetica



La macchina Enigma 1920-1945

- macchina per **cifrare** e **decifrare** messaggi in dotazione alle forze armate tedesche.
- sistema elettro-meccanico
- può essere considerata come un'estensione del metodo del cifrario di Vigenère
- **vedi:** [http://it.wikipedia.org/wiki/Enigma_\(crittografia\)](http://it.wikipedia.org/wiki/Enigma_(crittografia))

The Imitation Game, 2015.



One Time Pad: il cifrario perfetto (Vernam)

One Time Pad

Un sistema crittografico in cui la chiave è casuale, lunga quanto il testo in chiaro e non riutilizzabile.

- si dimostra un sistema sicuro
- praticamente impossibile da usare !
- vedi: http://en.wikipedia.org/wiki/One-time_pad

Esempio:

testo in chiaro	Benvenuti
chiavi	HKTRSXCVP
testo cifrato	xxxxxxxxxx

Questo sistema è stato utilizzato per le comunicazioni con le spie, che venivano equipaggiate di taccuini (pad in inglese) contenenti una lunga chiave per ogni pagina, da poter strappare e gettare una volta utilizzata (one time, ovvero "mono-uso").

Come Realizzare un Sistema Crittografico

I metodi di crittografia sono caratterizzati da tre parametri indipendenti:

- algoritmo utilizzato per codificare il messaggio
- il tipo di chiave utilizzata
 - ▶ chiave **unica** o **simmetrica**
 - ▶ chiave multipla o **asimmetrica**
- il modo in cui viene processato il messaggio in chiaro

In un sistema di calcolo le chiavi sono memorizzate come sequenze di **bit**:

1001001110011...

Crittografia

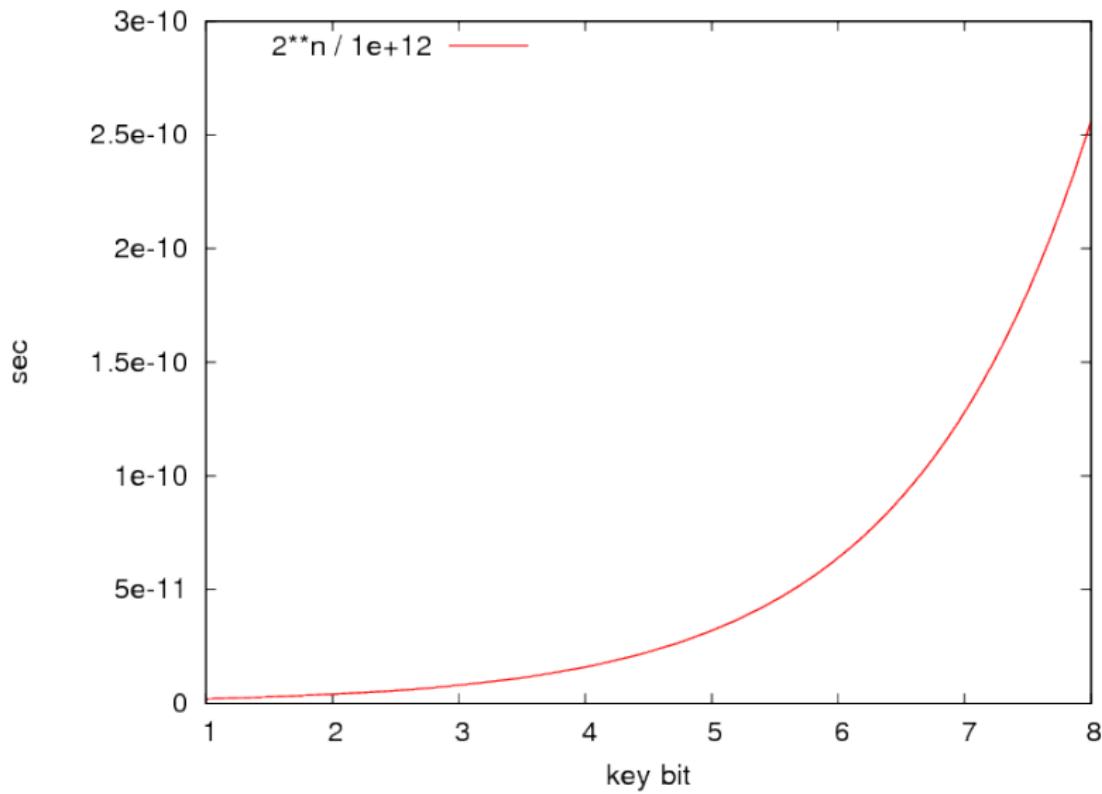
Il grado di sicurezza del sistema deve dipendere dalla segretezza della chiave, non dalla segretezza dell'algoritmo.

- 1 bit \Rightarrow 2 valori 0,1
- 2 bit \Rightarrow 4 valori 0,1,2,3
- 3 bit \Rightarrow 8 valori 0,1,2,3,4,5,6,7
- ... *applico il principio di induzione*
- $k-1$ bit $\Rightarrow 2^{k-1}$ valori $0, \dots, 2^{k-2}$
- k bit $\Rightarrow 2 \times 2^{k-1} = 2^k$ valori $0, \dots, 2^{k-1}$

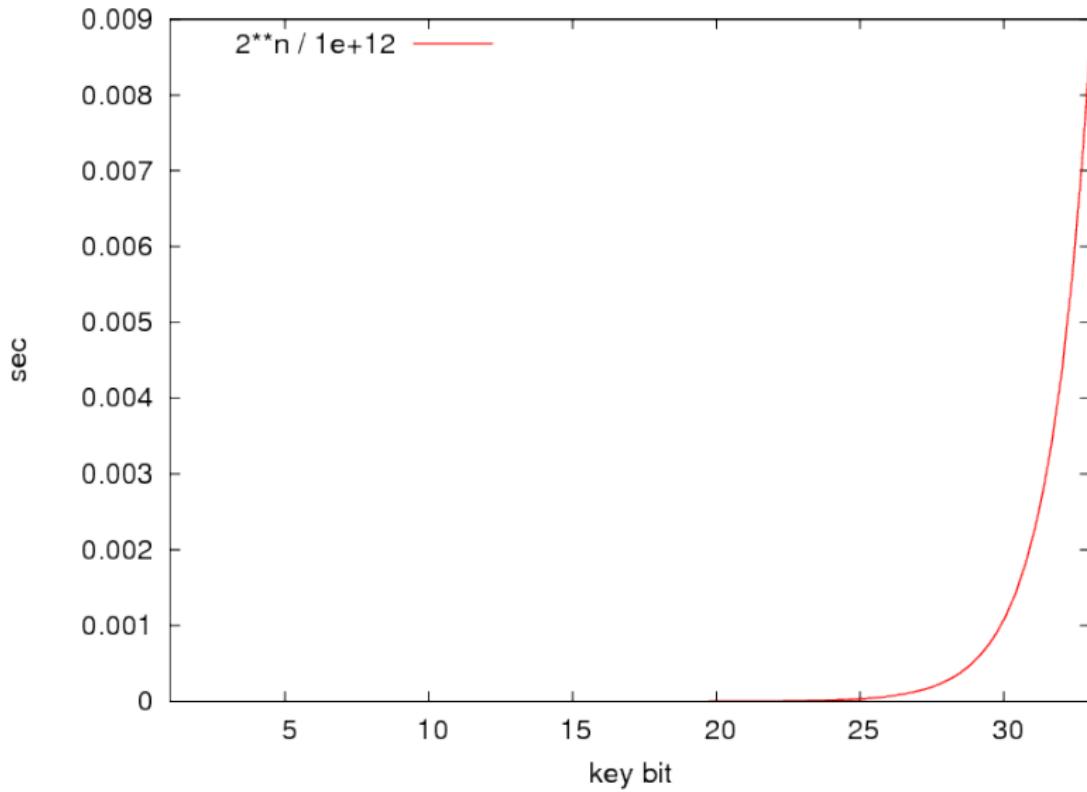
chiave (bit)	Num. di chiave	Tempo (10^{12} decritt./sec)
32	$2^{32} \approx 4.3 \times 10^9$	2.1×10^{-3} sec
56	$2^{56} \approx 7.2 \times 10^{16}$	7.2×10^4 sec = 20 ore
128	$2^{128} \approx 3.4 \times 10^{38}$	3.4×10^{26} sec = 10^{19} anni
256	$2^{256} \approx 1.1 \times 10^{77}$	1.1×10^{65} sec = 3.7×10^{57} anni

Il tempo di decifrazione cresce in modo esponenziale con il numero di bit della chiave!

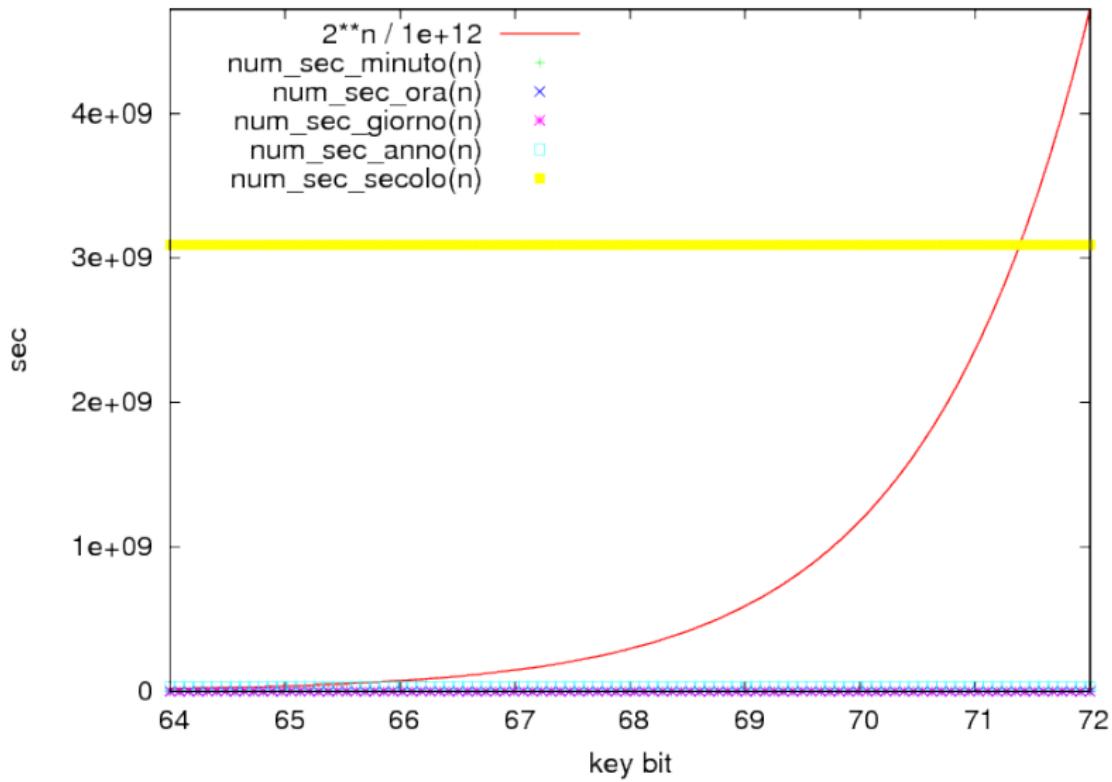
Crittografia (scala lineare)



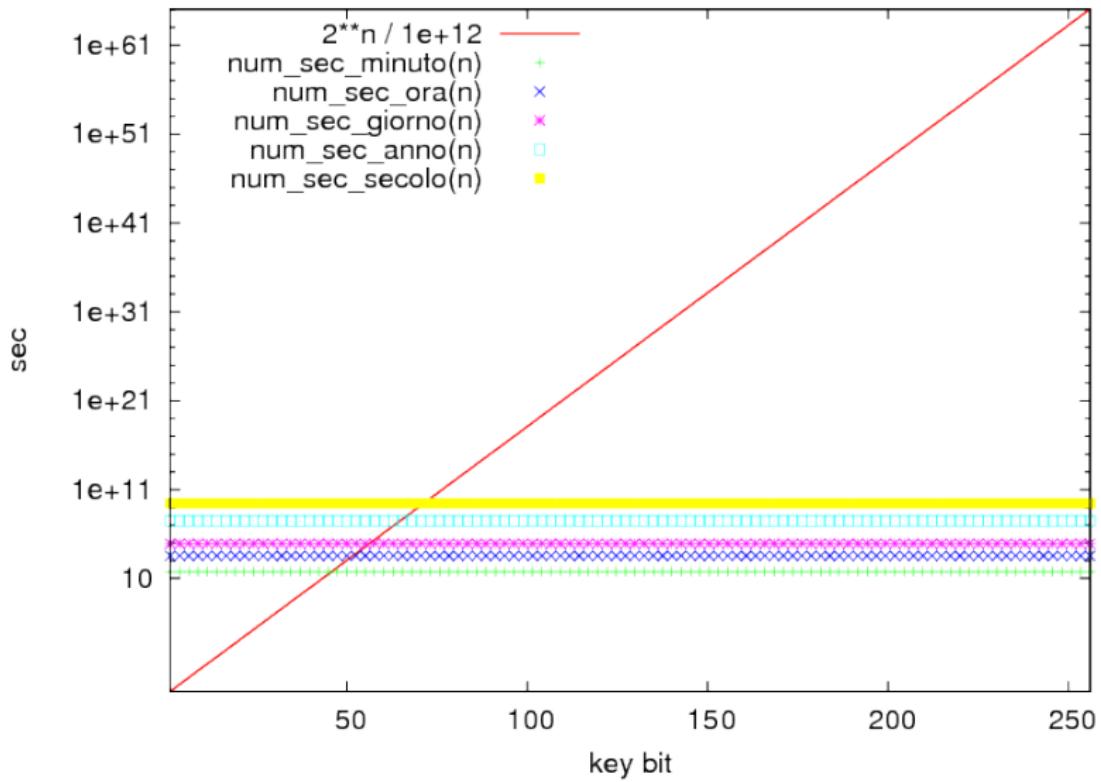
Crittografia (scala lineare)



Crittografia (scala lineare)



Crittografia (scala logaritmica)



Crittografia a chiave simmetrica

Si utilizza una chiave **unica** K per cifrare e decifrare il messaggio.

Sia

- \mathcal{M} il messaggio in chiaro
- \mathcal{C} il messaggio cifrato
- \mathcal{A} l'algoritmo di cifratura
- \mathcal{A}^{-1} l'algoritmo di de-cifratura

Allora valgono le seguenti uguglianze:

$$\mathcal{C} = \mathcal{A}(K, \mathcal{M})$$

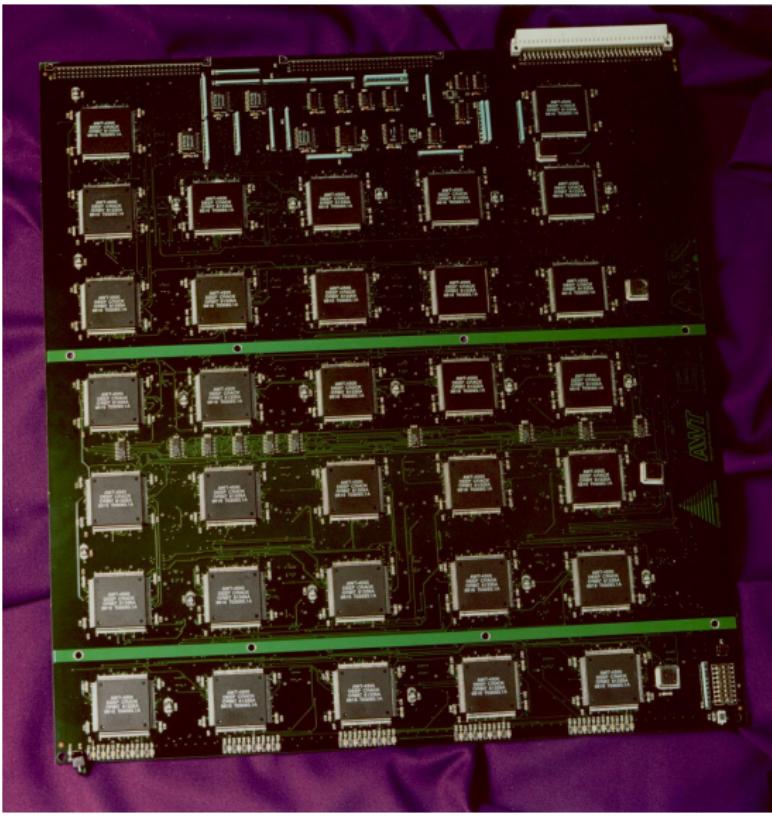
$$\mathcal{M} = \mathcal{A}^{-1}(K, \mathcal{A}(K, \mathcal{M}))$$

Crittografia a chiave simmetrica: DES

- **Data Encryption System** è stato adottato dal governo degli Stati Uniti nel 1976
- è un sistema a chiave simmetrica di 56-bit,
quindi usa solo $2^{56} \approx 7.2 \times 10^{16}$ chiavi !
- è un sistema insicuro oggi: nel gennaio del 1999 distributed.net e
Electronic Frontier Foundation collaborarono per rompere pubblicamente
una chiave di crittazione, e ci riuscirono in 22 ore e 15 minuti.

DES-cracker: Attacco con forza bruta

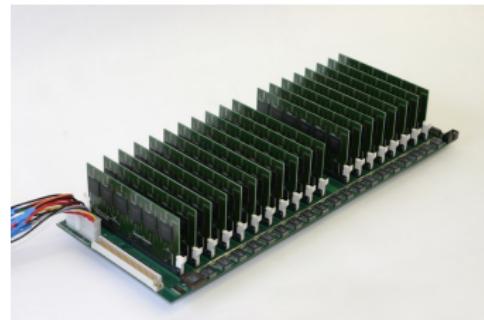
La vulnerabilità del DES fu dimostrata praticamente nel 1998 quando fu costruita appositamente la **DES-cracker** machine dall'Electronic Frontier Foundation (EFF) del costo di circa 250.000 \$.



Copacobana: Attacco con forza bruta

L'unico sistema ufficialmente conosciuto per violare la cifratura DES è il sistema COPACOBANA (abbreviazione in inglese di cost-optimized parallel code breaker) costruito dalle università di Bochum e Kiel (Germania).

- COPACOBANA utilizza dispositivi riconfigurabili (versatilità)
- La versione del marzo 2007 era composta da 120 *Field programmable gate array* (FPGA) di tipo XILINX Spartan3-1000 operanti in parallelo mentre la versione di maggio 2008 è composta da 128 Virtex-4 SX 35 FPGA.
- il costo della macchina del 2007 è di 10000\$ Eur, 25 volte più bassa del costo del DES-cracker, ma 30 volte più potente !



Crittografia a chiave simmetrica

Problema delle chiavi:

- 2 persone usano 1 chiave $\Rightarrow (2 \times 1)/2$
- 3 persone usano 3 chiavi $\Rightarrow (3 \times 2)/2$
- 4 persone usano 6 chiavi $\Rightarrow (4 \times 3)/2$
- ... *applico il principio di induzione*
- $n - 1$ persone che comunicano usano $((n - 1) \times (n - 2))/2$
- n persone che comunicano necessita di $(n \times (n - 1))/2$ chiavi, ovvero $n^2/2 - n/2$

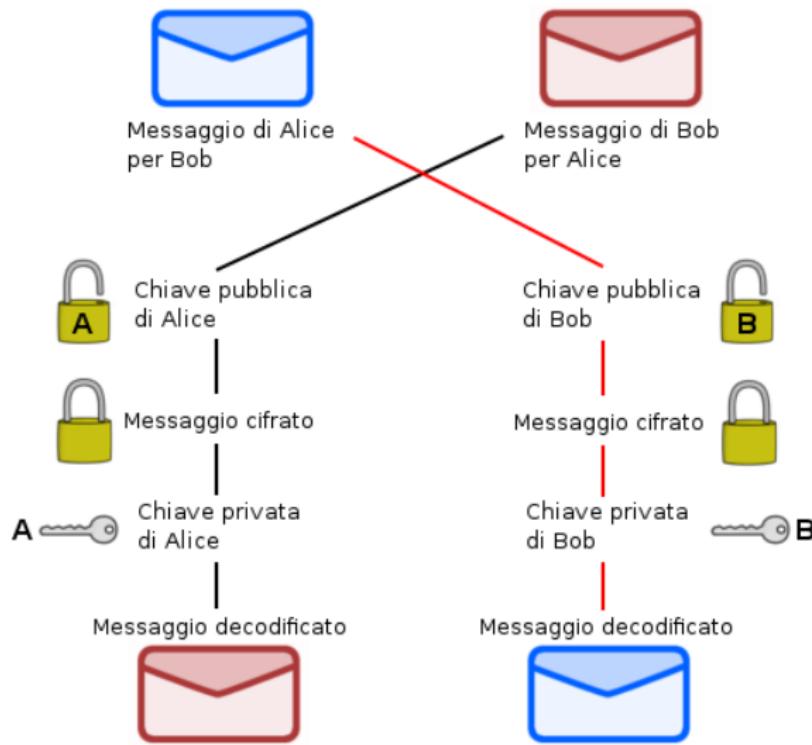
Il numero delle chiavi da utilizzare è $\mathcal{O}(n^2)$.

Esempio:

100 persone che comunicano necessitano di $(100 \times 99)/2 = 4950$ chiavi !

Crittografia a Chiave Asimmetrica

Si utilizza una chiave K_1 **pubblica** per cifrare ed una K_2 **privata** per decifrare.



Crittografia a Chiave Asimmetrica

Sia

- K_1 e K_2 le chiavi
- M il messaggio in chiaro
- C il messaggio cifrato
- \mathcal{C}_C l'algoritmo di cifratura
- \mathcal{C}_D l'algoritmo di de-cifratura

Allora valgono le seguenti uguglianze:

$$M = \mathcal{C}_D(K_1, \mathcal{C}_C(K_2, M))$$

$$M = \mathcal{C}_D(K_2, \mathcal{C}_C(K_1, M))$$

Crittografia a chiave Asimmetrica

Principi di base:

- Da una chiave è impossibile risalire all'altra
- Quello che si cifra con una si decifra con l'altra (si decide una volta la pubblica e la privata)
- Non è necessario lo scambio:
 - ▶ il mittente cifra con la chiave pubblica del destinatario.
 - ▶ il destinatario decifra con la sua chiave privata.
- Per n utenti il numero di chiavi è $2n \in \mathcal{O}(n)$
- Svantaggio: lenta (> 1000 volte più lenta della simmetrica)

Trapdoor Function (funzione botola)

Principio

Trovare i fattori di un numero intero è difficile.

- se $p = 17$ e $q = 29$ calcolare $z = p \times q = 493$ è facile
- dato $z = 493$ calcolare i fattori “non banali” (1 e se stesso) è difficile:
 - ▶ devo trovare tutti i numeri x, y tali che $x \times y = 493$
 - ▶ procedo, ad esempio, per tentativi:
 - ★ $1 \times 2, 1 \times 3, \dots, 1 \times 493$
 - ★ $2 \times 2, 2 \times 3, \dots, 2 \times 493$
 - ★ ...
 - ★ $493 \times 1, \dots, 493 \times 493$
 - ▶ quindi, dato numero z devo calcolare circa z^2 moltiplicazioni
 - ▶ se z è il prodotto di due numeri primi p e q molto grandi, p e q sono unici e trovarli è un problema difficile

Trapdoor Function (funzione botola)

Cifre del numero	sapere se primo	determinare i fattori
50	15 sec	4 ore
75	22 sec	104 giorni
100	40 sec	74 anni
200	10 min	$4 * 10^9$ anni (l'età della terra)
500	3 giorni	$4 * 10^{25}$ anni
1000	1 settimana	ecc.

Osservazioni:

- sapere se un numero è primo è “**facile**”
- determinare i fattori di un numero è **difficile**

Il un numero primo più grande è:

$2^{74,207,281} - 1$ ha 22,338,618 cifre scoperto il 7 Gennaio 2016 ha richiesto 41 giorni di calcoli su un PC.

Aritmetica Modulare

Cos'è ?

Potremmo anche chiamarla aritmetica:

- dell'**orologio**: se adesso sono le ore “una” che ore sono tra 13 ore ?
Le ore 14 ! (orologio da polso classico !)
- della **settimana**: se oggi è il primo giorno (lunedì) della settimana che giorno è fra 8 giorni ?
Il “nono” giorno !
- del **mese**: se oggi è il giorno 2 che giorno è tra 32 giorni ?
Il giorno 34 !

Aritmetica Modulare

Dato un numero intero $n > 1$ ci sono n resti possibili della divisione di un qualsiasi intero per n .

L'insieme di questi resti viene denotato con la scrittura

$$\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}$$

Esempio: $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$.

Denotiamo con

$$r = a \bmod n$$

il resto della divisione di a e n , ovvero $a = kn + r$.

Esempio:

- $14 \bmod 12 = 2$: le due (del pomeriggio o del mattino)!
- $9 \bmod 7 = 2$: martedì della settimana successiva !
- $34 \bmod 31 = 3$: il 3 giorno del mese successivo !

Trapdoor Function (funzione botola)

Per realizzare un sistema a chiave asimmetrica serve:

- una funzione **facile** da calcolare ma **difficile** da invertire
- **facile** da invertire conoscendo alcune informazioni

Esempio: algoritmo RSA (Rivest, Shamir, Adleman, 1977)

- dati n numero intero e g tale $\text{MCD}(g,n)=1$ (quindi sono primi tra loro)
- dato e numero intero è **facile** calcolare

$$g^e \bmod n$$

si può utilizzare l'algoritmo **square and multiply**

- viceversa è **difficile** calcolare “ e ” conoscendo solamente:

$$g, g^e, g^e \bmod n$$

Algoritmo RSA

Per semplificare il funzionamento immaginiamo che A debba spedire un messaggio segreto a B. Occorrono i seguenti passaggi:

- 1 B sceglie due numeri primi molto grandi (per esempio da 300 cifre) e li moltiplica con il suo computer (impiegando meno di un secondo).
- 2 B invia il numero che ha ottenuto ad A. Chiunque può vedere questo numero.
- 3 A usa questo numero per cifrare il messaggio
- 4 A manda il messaggio cifrato a B, chiunque può vederlo ma non decifrarlo
- 5 B riceve il messaggio e utilizzando i due fattori primi che solo lui conosceva lo decifra.

A e B hanno impiegato pochi secondi a cifrare e decifrare, ma chiunque avesse intercettato le loro comunicazioni impiegherebbe troppo tempo per scoprire i due fattori primi, con cui si può decifrare il messaggio.

In pratica, per trasmettere grandi quantità di dati occorre tanto tempo, quindi A e B si scambieranno con questo sistema una **chiave segreta** (che occupa poco spazio), che poi useranno per comunicare tra loro usando un sistema a **crittografia simmetrica**, più semplice e veloce.

Algoritmo RSA

RSA è basato sull'elevata complessità computazionale della fattorizzazione in numeri primi. Il suo funzionamento di base è il seguente:

- ① si scelgono a caso due numeri primi grandi p e q
- ② si calcola $n = pq$ detto **modulo**
- ③ si sceglie un numero primo e detto **esponente pubblico**
- ④ si calcola d **esponente privato** t.c. $e * d \text{ mod } ((p - 1)(q - 1)) = 1$

Allora, la chiave pubblica è (n, e) e la chiave privata è (n, d) .

Un messaggio m viene cifrato mediante la funzione

$$c = m^e \text{ mod } n$$

e decifrato mediante la funzione

$$m = c^d \text{ mod } n$$

Esempio RSA: Generazione delle chiavi

Ecco un esempio di cifratura e decifratura RSA. I numeri scelti sono volutamente primi piccoli, ma nella realtà sono usati numeri dell'ordine di 10^{100} .

Generazione delle chiavi

- ① $p = 3, q = 11$, quindi $(p - 1)(q - 1) = 2 * 10 = 20$
- ② $n = pq = 33$
- ③ scelgo $e = 7$ dato che $e < n$ e coprimo con 20
(non è necessario che sia primo)
- ④ scelgo $d = 3$, dato che $(e * d) \bmod 20 = 1$

Quindi abbiamo che

- $(33, 7)$ è la chiave pubblica
- $(33, 3)$ è la chiave privata

Esempio RSA: Cifratura e Decifratura

Prendiamo in considerazione un messaggio $m = 15$ e cifriamolo con la chiave pubblica:

$$c = m^e \bmod n = 15^7 \bmod 33 = 170859375 \bmod 33 = 27$$

Decifriamo adesso $c = 27$ mediante la chiave privata:

$$m = c^d \bmod n = 27^3 \bmod 33 = 19683 \bmod 33 = 15$$

Esempio RSA

- siano $p = 47$ e $q = 61$ due numeri primi, t.c. $\text{MCD}(47,61)=1$.
- scelgo $E = 1183$
- la funzione di codifica con chiave pubblica è:
 $C = P^E \bmod pq = P^{1183} \bmod 2867$
- la funzione di decodifica con chiave privata è : $P = C^7 \bmod 2867$

Esempio:

- Supponiamo che *Bob* voglia inviare ad *Alice* il messaggio: **Sono uscito.**
- Innanzitutto *Bob* codifica il messaggio in un numero mediante la codifica:

$$a = 00, b = 01, c = 02, \dots, A = 26, B = 27, \dots \text{blank} = 62, \dots$$

ed ottiene un numero $P = 4414131462201802081914$.

Esempio RSA

- Bob fraziona il numero P in blocchi P_i di 3 cifre

$$P_1 = 441, P_2 = 413, P_3 = 146, \dots$$

- Bob cifra i blocchi P_i mediante la funzione

$$C_i = P_i^{1183} \bmod 2867$$

ed ottiene:

$$C_1 = 2515, C_2 = 1572, C_3 = 1426, \dots$$

- Alice ricevuti i blocchi C_i li decodifica mediante la funzione

$$P_i = C_i^7 \bmod 2867$$

ed ottiene:

$$P_1 = 2515^7 \bmod 2867 = 441, \dots$$

Applicazioni della Crittografia: Hash Crittografico

- serve a garantire l'integrità dell'informazione
- associamo ai dati che vogliamo proteggere il **digest** (o Hash o finger-print)
- è un valore di lunghezza **fissa** indipendente dalla lunghezza dell'input
- due messaggi diversi possono avere lo stesso digest, ma ...
- minime modifiche ad un messaggio cambiano radicalmente il suo digest
- la probabilità che due messaggi diversi abbiano senso e che siano simili/correlati producono lo stesso digest è praticamente nulla.

Esempio di digest:

$$\Sigma_c(\text{string}) \bmod 99$$

Nella pratica si usano metodi più complessi come **md5sum**.

<http://md5.online-toolz.com/tools/md5-generator.php>

Applicazioni della Crittografia: Scambio di Chiavi

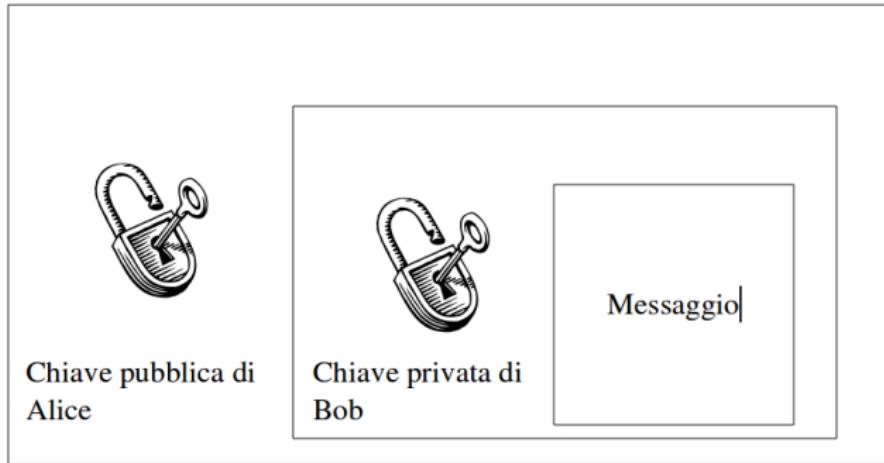
Problema

Bob vuole mandare un messaggio protetto ad Alice, ma Bob non conosce Alice e Alice non conosce Bob.

Due entità necessitano di scambiarsi una chiave crittografica in modo tale che nessuno possa intercettarla.

soluzione: sfruttiamo il fatto che le chiavi sono due, una pubblica ed una privata.

Applicazioni della Crittografia: Scambio di Chiavi



- 1 Bob critpa il messaggio M con la sua chiave privata ed ottiene M'
- 2 Bob usa la chiave pubblica di Alice per criptare il messaggio M'
- 3 Alice usa la sua chiave privata per decrittare il messagio M'
- 4 Alice usa la chiave pubblica di Bob per decrittare il messaggio M

Applicazioni della Crittografia: Firma Digitale

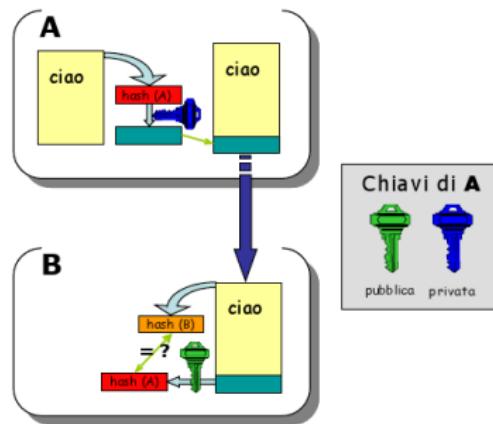
Vogliamo sostituire transazioni **cartacee** con un processo completamente digitale.

- non deve essere **falsificabile**:
se la persona P invia un messaggio M con firma F nessuno può ri-produrre la coppia (M, F)
- deve essere **autenticabile**:
chi riceve deve poter verificare che la firma proviene da P (solo P può averla creata) e che è associata a M.

Anche in questo caso possiamo utilizzare la crittografia asimmetrica, combinata con il digest.

Applicazioni della Crittografia: Firma Digitale

- ① A calcola il digest del messaggio e lo cifra con la sua chiave privata; il digest è la firma digitale
- ② A invia il messaggio e digest a B
- ③ B ricalcola il digest e lo confronta con quello ricevuto da A
- ④ se i due digest sono uguali il messaggio non è stato modificato e A non può ripudiarlo.



Applicazioni della Crittografia: Firma Digitale

Posso aggiungere la segretezza ?

Si, in questo caso utilizzo la crittografia simmetrica:

- ① genero una chiave K per un algoritmo simmetrico
- ② cripto il messaggio
- ③ cripto la chiave K utilizzando la mia chiave privata e la chiave pubblica del destinatario

Posta Elettronica Certificata

Mettiamo tutto insieme:

- 1 A vuole inviare a B un messaggio M mediante PEC
- 2 A genera un chiave K
- 3 A genera una firma digitale F (digest di M) e la critta mediante la propria chiave privata e ottiene F'
- 4 A critta il messaggio M con la chiave K per ottenere M'
- 5 A critta la chiave K con la sua chiave privata e ottiene K'
- 6 A invia (M', F', K') a B criptandolo il tutto con la chiave pubblica di B
- 7 B decripta (M', F', K') con la propria chiave privata
- 8 B decripta F' e K' con la chiave pubblica di A e ottiene F e K
- 9 B decripta M' e ottiene M
- 10 B calcola il digest di M e lo confronta con F

ho **quasi** realizzato la Posta Elettronica Certificata.

Cosa manca ?

Come faccio a sapere qual'è la **vera** chiave pubblica di A e B ?

Applicazioni della Crittografia: Certificati Digitali

Un messaggio dotato di firma digitale è **sicuro** se:

- la chiave di A non è stata compromessa
- B conosce la “vera” chiave pubblica di A

La convalida delle chiavi pubbliche viene effettuata attraverso i certificati: una autorità esterna **Certification Authority (CA)**, garantisce l'autenticità

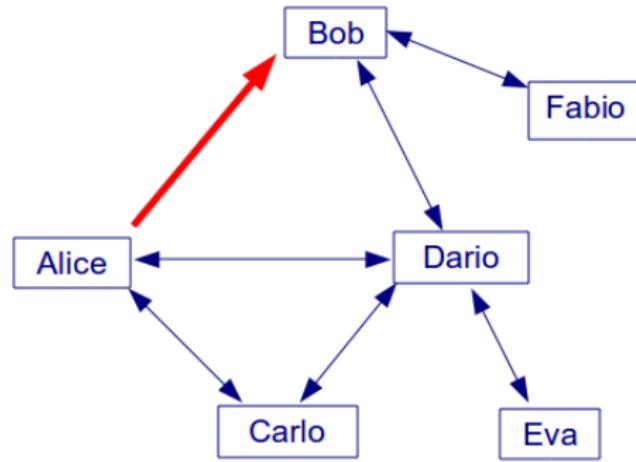
Esistono due modelli principali:

- PGP: **web of trust**
- X.509: organizzazione gerarchica

Applicazioni della Crittografia: Certificati

Web of Trust

- Ideato da Phil Zimmermann per il suo software PGP (primi anni '90)
- Utilizzato dai sistemi che seguono lo standard OpenPGP
- Tutti gli utenti possono essere certificatori
- Ogni chiave può essere certificata da più persone
- Basato sulla fiducia reciproca tra individui (di buon senso! ndr)



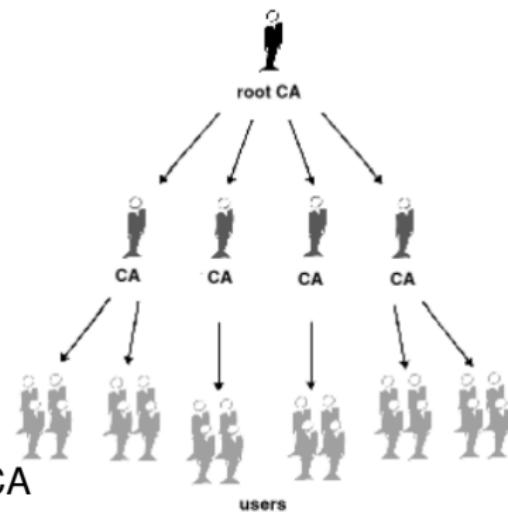
Applicazioni della Crittografia: Certificati

Modello delle *Public Key Infrastructure*

- standard X.509
- struttura gerarchica: tutti si fidano per definizione del vertice *Root Authority* che può delegare altri enti *Certification Authority*
- sistema previsto dalle normative europee ed italiane sulla firma elettronica

Un certificato X.509 contiene:

- informazioni del proprietario
- la data di scadenza
- la chiave pubblica del proprietario
- informazioni sul garante cioè la CA
- il certificato è firmato digitalmente dalla CA

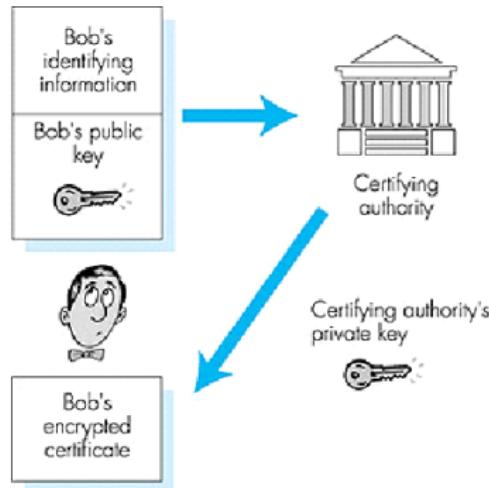


Applicazioni della Crittografia: Certificati

- Autorità di certificazione (CA) garantisce chiavi pubbliche di ogni utente
- un utente registra la sua chiave pubblica presso la CA

A questo punto:

- Alice vuole conoscere la chiave pubblica di Bob
- chiede alla CA il certificato di Bob
- verifica autenticità del certificato, cioè verifica la firma della CA che è pubblica.



Esempio di Crittografia Grafica

Scopo

- ① Cifrare un messaggio M in due messaggi C_1 e C_2
- ② Ricostruire il messaggio M partendo da due messaggi cifrati C_1 e C_2

Rappresentazione grafica del messaggio M :



Esempio di Crittografia Applicata alla Grafica

Rappresentazione testuale del messaggio M:

```
# ImageMagick pixel enumeration: 400,424,255,rgb
0,0: (255,255,255) #FFFFFF white
1,0: (255,255,255) #FFFFFF white
2,0: (255,255,255) #FFFFFF white
3,0: (255,255,255) #FFFFFF white
4,0: (255,255,255) #FFFFFF white
5,0: (255,255,255) #FFFFFF white
6,0: (255,255,255) #FFFFFF white
7,0: (255,255,255) #FFFFFF white
8,0: (255,255,255) #FFFFFF white
9,0: (255,255,255) #FFFFFF white
...
...
```

il messaggio è rappresentato da una matrice di punti $M[i][j]$ detti **pixel**.

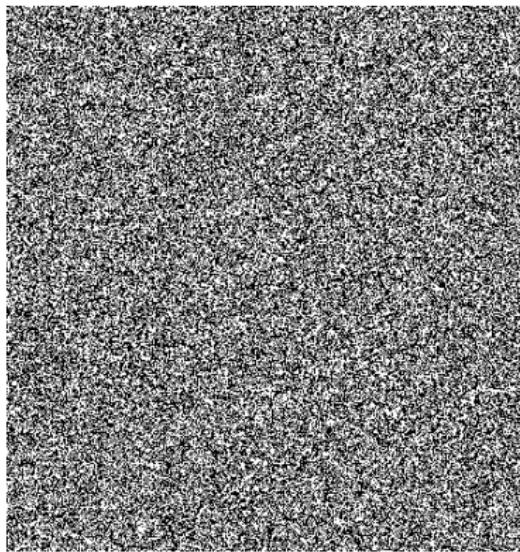
Esempio di Crittografia Applicata alla Grafica

Algoritmo di crittazione:

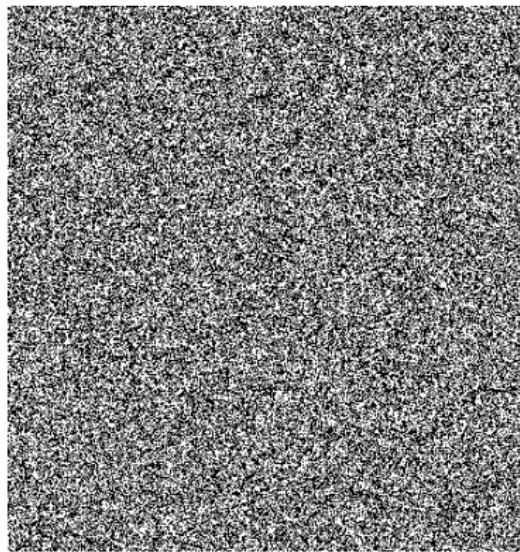
- ① per ogni pixel $M[i][j]$ del messaggio
- ② calcola un numero random $0 < r < 1$
- ③ se $M[i][j] = \text{WHITE}$
 - ① se $r < 0.5$ $C1[i][j] = 0$ e $C2[i][j] = 1$
 - ② altrimenti $C1[i][j] = 1$ e $C2[i][j] = 0$
- ④ altrimenti se $M[i][j] = \text{BLACK}$
 - ① se $r < 0.5$ $C1[i][j] = 0$ e $C2[i][j] = 0$
 - ② altrimenti $C1[i][j] = 1$ e $C2[i][j] = 1$

Esempio di Crittografia Applicata alla Grafica

applicando l'algoritmo precedente alla rappresentazione testuale del messaggio M ottengo due messaggi $C1$ e $C2$ che graficamente rappresentano:



C1



C2

Esempio di Crittografia Applicata alla Grafica

Algoritmo di decriptazione

- 1 per ogni valore di i e j
- 2 $M[i][j] = C1[i][j] \text{ xor } C2[i][j]$



Funzione logica Xor (Or esclusivo)

bit1	bit2	Xor
0	0	0
0	1	1
1	0	1
1	1	0

<http://www.fe.infn.it/u/filimanto/scienza/webkrypto/index.htm>

That's all Folks



References

- Probabilità, numeri e code. La matematica nascosta nella vita quotidiana. Rob Eastaway, Jeremy Wyndham, anteprima su <http://books.google.it/>
- La steganografia da Erodoto a Bin Laden. Nicola Amato, Ed. Italian University Press
- <http://www.mat.unimi.it/users/labls/Crittografia/indexCritt.html>
- <http://mckoss.com/Crypto/Enigma.htm>
- <http://it.wikipedia.org/wiki/Atbash>
- <http://critto.liceofoscarini.it/index.html>
- <http://digilander.libero.it/crittazione/index.htm>
- <http://avires.dimil.uniud.it/claudio/teach/sicurezza2013/lezione-01.pdf>