Dall'Alberti all'Enigma e oltre

Fabrizio Luccio

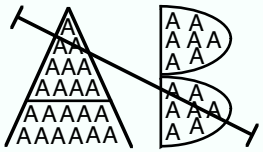
Museo del Calcolo, Pisa 2015

Crittografia

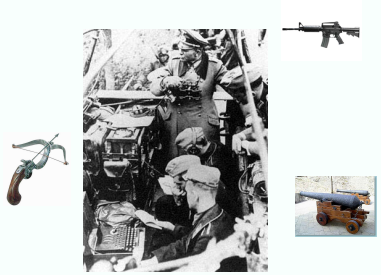
κρυπτος = nascosto γραφειον = scrittura

La crittografia è una "scienza applicata"

. . . . in ambienti diversi



REBUS



ENIGMA

Finché nel 1977 . . .

€ $

¥ £

Per aprire un lucchetto a combinazione (o scoprire un *PIN*) di 4 cifre occorrono fino a 10.000 prove.

Aumentando di 1 il numero di cifre si moltiplica per 10 il numero di prove.

In termini matematici il numero di prove cresce in modo esponenziale rispetto al numero di cifre del lucchetto: per 4 cifre occorrono 10^4 prove.

Il concetto di crescita esponenziale
- di cui è di gran moda parlare a sproposito –
è cruciale in crittografia:

le operazioni permesse (impostare le cifre del lucchetto) devono essere compiute in tempo ragionevole

le operazioni vietate (cercare di aprire il lucchetto senza conoscerne la chiave) devono richiedere tempo esponenziale

Ma riprendiamo questa scienza dall'inizio . . . . .

Erodoto: Storie (V secolo a. C.)

Narra di un messaggio segreto scritto sulla testa di un servo cui erano stati rasati i capelli

Ricresciuti i capelli il servo fu inviato a destinazione ove i capelli gli furono rasati di nuovo per leggere il messaggio

Enea Tattico
Πολιορκετικα' (IV secolo a. C.)

Δ / :: / :·: / N / ::: / Σ / :: / :·: / Σ Κ / · / Λ / :·: / Σ

Διονγσιος Καλος

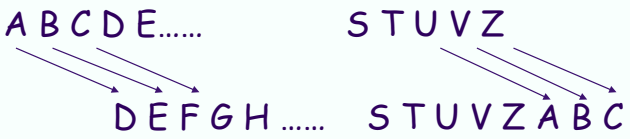
Il numero di puntini corrisponde alla posizione della vocale nell'alfabeto !

Ovidio: Ars Amatoria (1 d. C.)

illa sit in vestris
qui fuit ille notis

Svetonio
Le vite di dodici Cesari

Cesare scriveva "per notas" sostituendo ogni lettera con quella tre posizioni più avanti nell'alfabeto:



CAIUS IULIUS CAESAR
FDLAV LAOLAV FDHVDU

Crittare e decrittare sono operazioni sostanzialmente equivalenti

Solo dal 1977 può non esser più così

Il codice di Cesare era debolissimo.

Infatti:

Ogni codice segreto non può essere mantenuto tale troppo a lungo

Una comunicazione segreta deve essere basata su un'informazione addizionale, la chiave, che sia mantenuta segreta e possa essere modificata facilmente

Le regole devono essere pubbliche e solo la chiave deve essere segreta

Kama Sutra (V secolo d. C.):

"le donne devono imparare sessantaquattro arti tra cui cucina, preparazione dei profumi, massaggio, rilegatura, congiura, falegnameria…e la n. 45: mlecchita-vitalpa ovvero l'arte della scrittura segreta".

Suggerisce di sostituire le lettere basandosi su corrispondenze casuali di coppie di lettere dell'alfabeto.

Possiamo considerare una permutazione arbitraria dell'alfabeto come chiave e variarla a piacere:

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

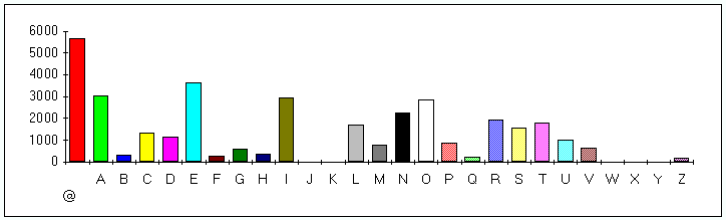
testo: CAIUSIULIUSCAESAR
messaggio cifrato: TSRAFRAURAFTSBFSV

Il numero di chiavi possibili è $> 10^{26}$
un numero enorme, tuttavia . . . . .

…. il sistema è attaccabile facilmente con una analisi statistica sulla frequenza delle lettere

testo: CAIUSIULIUSCAESAR
messaggio cifrato: TSRAFRAURAFTSBFSV

Frequenze delle lettere in italiano
rilevate su "I Promessi Sposi"



Nascita dei cifrari polialfabetici:

il disco di Leon Battista
Alberti (XV secolo)

Chiave: **B-k**

C A E 2 S A R
L g p a y b x

qui la chiave diventa **B-a**

E visto che siamo in un museo:

Sull'idea di Alberti lavorò Blaise de Vigenère
più di un secolo dopo

La chiave è una parola breve ripetuta quanto occorre
BAGDADBAGDADBAGDAD . . . .

Ogni lettera della chiave indica una traslazione
della corrispondente lettera del testo.

chiave: **B A G D A D**
traslazione: **2 1 7 4 1 4**

2 1 7 4 1 4 2 1 7 4 1 4 2 1 7 4 1

Il metodo di de Vigenère ebbe un grande successo perché era di pubblico dominio e semplice da utilizzare.

Fu usato fino a tutto il 1800, quando fu attaccato con successo con metodi statistici sofisticati basati sulla ripetizione della chiave.

Ma molte applicazioni rimasero in uso impiegando chiavi molto lunghe

Così nel 1918 nacque Enigma, basato anch'esso sul metodo polialfabetico e dichiaratamente inspirato al disco di Alberti.

Su Enigma ormai sapete tutto . . .

tranne forse che potete comprare un kit per costruirne un simulatore elettronico

Mark 4: bastano 300 $ e un saldatore

Con una chiave lunga le cose funzionano bene

Bolivia 1967

Se poi si impiega una chiave lunga come il messaggio, casuale e non riutilizzabile, il cifrario diviene inattaccabile.

Un'elegantissima dimostrazione matematica fu proposta da Claude Shannon durante la seconda guerra mondiale.

Un simile cifrario fu proposto a fine '800.
Fu brevettato nel 1917 in forma digitale
(One-Time Pad) . . . .

e fu adottato nella Hot Line per le comunicazioni tra la Casa Bianca e il Cremlino, istituita nel 1967 dopo la crisi dei missili a Cuba.

Nel 2010, incontrando a Washington il presidente russo Medvedev, Obama ha detto che sarebbe tempo di buttare via i telefoni rossi e usare Twitter.

Ma ormai stiamo entrando nell'era digitale (o meglio, binaria)

Nel 1969 Internet muove i primi passi

Nel 1972 nasce un codice standard a chiave segreta. Si chiama

Data Encryption Standard (DES)

DES

- Pubblicamente noto e realizzabile in un circuito su computer di ogni tipo
- Chiave di 8 caratteri rappresentati con 64 bit
- Certificato dal NBS e da NSA

Le chiavi DES non sono sicure con i computer di oggi

Nel 2000 è nato il nuovo standard:
Advaced Encription Standard (AES)

Ma come si può scambiare una chiave segreta con facilità e sicurezza?

Qui entra in gioco la Teoria dei numeri

Hardy (sulla teoria dei numeri, 1940):

" Gauss e tutti i matematici possono rallegrarsi perché la loro scienza si mantiene amabile e incorrotta per la sua lontananza dalle comuni attività umane. "

La frase è comunemente citata come esempio di affermazione incauta . . . .

Una clamorosa smentita a Hardy venne dalla invenzione della Crittografia a chiave pubblica, nata ufficialmente nel 1976 ma preceduta dal lavoro segreto degli agenti britannici del Government Communications Headquarters (GCHQ).

Ellis, Cock e Williamson

1970 – 75. Rapporti TOP SECRET al GCHQ sulla trasmissione cifrata non preceduta dall'accordo su una chiave, con un metodo matematico basato sui numeri primi.

Merkle Diffie Hellman

La crittografia asimmetrica (1976)

Propongono nuovi metodi per lo scambio sicuro di chiavi e messaggi (crittografia a chiave pubblica), destinati a mutare profondamente il mondo della crittografia.

Crittografia a chiave pubblica

L'idea di base è semplice:

Ogni utente U ha una chiave pubblica e una chiave segreta. La cifratura impiega la prima chiave e la decifratura la seconda (dunque i due procedimenti sono diversi)

Chi invia un messaggio a U lo cifra con la chiave pubblica di U; solo U può decifrarlo con la sua chiave segreta

facile da calcolare …

e difficile da invertire …

a meno che non si conosca una chiave segreta !

Shamir Rivest Adleman

R S A (1977)

Propongono il primo sistema a chiave pubblica basato su una funzione matematica "facile" da calcolare e "difficile" da invertire

… era la stessa funzione che Williamson aveva proposto segretamente al GCHQ !

È davvero troppo complicato entrare in qualche dettaglio su questi metodi, su cui tra l'altro è basata la firma elettronica.

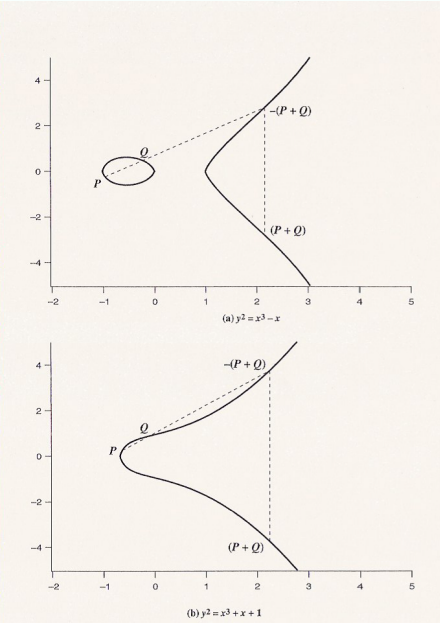
Diamo solo un accenno su una tecnica fondamentale in questo momento:

lo scambio sicuro di chiavi basato su curve ellittiche.

Le curve ellittiche

$y^2 = x^3 + ax + b$

Si considerano solo i punti a coordinate intere (e si opera "in modulo")



Un punto P può essere sommato a sé stesso mediante la tangente in P alla curva

Moltiplicazione di P per una un numero intero k:

$$P + P + \ldots + P = k\,P$$

La moltiplicazione è eseguita con raddoppi e addizioni. Per esempio se k = 13:

$$13\,P = P + 4P + 8P = P + (2(2P)) + (2(4P))$$

Per $R = k\,P$

dati k e P, si calcola R in tempo "breve"

dati R e P, si sa calcolare k solo in tempo esponenziale

Costruzione di una chiave tra Alice e Bob

- I due concordano su una curva da usare e su un suo punto P (che possono essere noti a tutti)
- Alice sceglie un intero segreto α, calcola αP e lo invia a Bob
- Bob sceglie un intero segreto β, calcola βP e lo invia ad Alice
- Alice calcola la chiave comune $k = \alpha\beta P$
  Bob calcola la chiave comune $k = \beta\alpha P$