Numeri Primi e Crittografia

Linda Pagli

San Pellegrino, Settembre 2014

Numeri primi

Dagli *Elementi* di Euclide (circa 300 a.C.):

πρωτος αριτμος = numero primo,
"misurato" solo dall'unità.

Crittografia

κρυπτος = nascosto, γραφειον = scrittura

EUCLIDE

19

11

3

5

7

EUCLIDE

19

11

3

5

7

EUCLIDE

ENIGMA

19

11

3

7

5

EUCLIDE

ENIGMA

19

11

3

7

5

EUCLIDE

ENIGMA

Finché nel 1977…

19

11

3

7

5

EUCLIDE

ENIGMA

Finché nel 1977...

€

¥

$

£

I numeri primi sono quelli che si possono dividere solo per 1 e per sé stessi.

Per Euclide, e per tutti i matematici che seguirono, questi sono i numeri di base, perché con essi si costruiscono tutti gli altri numeri per moltiplicazione. Per esempio:

$60 = 2 \cdot 2 \cdot 3 \cdot 5$ è formato da 2, 3 e 5 che sono i fattori primi di 60

2 3 5 7 11 13 17 . . . . . sono primi

2 

3 Moschettieri

5 Poliedri regolari

7 Peccati capitali

11 Giorni 11 notti

13 Porta bene

17 Porta male

. . . . . .

Euclide dimostrò che esistono infiniti numeri primi osservando che, partendo da un gruppo qualsiasi di numeri primi noti, se ne può costruire sempre uno nuovo; questo si aggiunge al gruppo precedente e si prosegue all'infinito.

La dimostrazione di Euclide è uno dei gioielli della matematica.

Eratostene, bibliotecario di Alessandria, definì il crivello attorno al 240 A.C.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

dal XVII al XIX secolo

rinacque una grande attenzione per i numeri primi: in particolare si speculò sulla loro distribuzione nell'elenco di tutti i numeri e se essa seguisse una semplice legge. I matematici cercavano una formula per generare tutti i numeri primi.

A oggi il problema è essenzialmente irrisolto.

Eulero (1751) :
"Ci sono misteri che mai potremo comprendere. Per convincerci di ciò basta guardare le tavole dei numeri primi ove non regna ordine né legge."

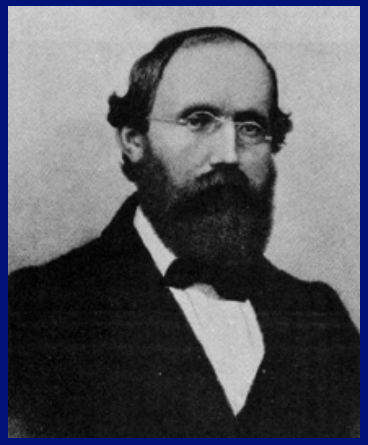
In effetti la distribuzione dei numeri primi ha molte caratteristiche matematiche in comune con una distribuzione casuale, ma ovviamente non lo è perché possiamo decidere quale numero sia primo nell'elenco di tutti i numeri.

Gauss (appunti da adolescente, 1792):

" Primzahlen unter *a* (= ∞) *a* / la "

I numeri primi minori di *a*, per *a* che tende all' infinito, sono *a* diviso il logaritmo naturale di *a*.

La congettura fu dimostrata nel 1896 da Hadamard e de le Valleé-Poussin (che vissero poi entrambi fino quasi a cent'anni). È nota oggi come Teorema dei numeri primi.



Riemann (1859):

" Naturalmente sarebbe bello avere una dimostrazione rigorosa di ciò …"

L'ipotesi di Riemann è legata alla distribuzione dei numeri primi.

Dimostrarla è uno dei problemi principali aperti della matematica del nuovo millennio. E ne varrebbe la pena ....

Cosa dice la formula di Gauss: $n / \ln n$?

n :	10	100	1000	10.000	100.000	1.000.000
di cui sono primi :	4	25	168	1229	9592	78.498

Se Euclide aveva dimostrato che tra tutti gli interi esistono infiniti numeri primi, Gauss comprese che molti interi sono primi: un'ottima notizia per la crittografia, anche se Gauss non poteva immaginarlo...

Motivo di tanta abbondanza è che n ha una crescita esponenziale rispetto a $\ln$.

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

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

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

Il concetto di crescita esponenziale è sempre stato una delle basi della segretezza.

Ecco un esempio importante:

presi due numeri primi p, q

Calcolare $n = p \times q$ " è facile "

Calcolare p, q da n " è difficile "

perché si devono provare tutti i divisori di n che, come per il lucchetto, sono in numero esponenziale rispetto al numero di cifre di n

Dunque le proprietà dei numeri primi e la crescita esponenziale sono oggi ingredienti di base della crittografia

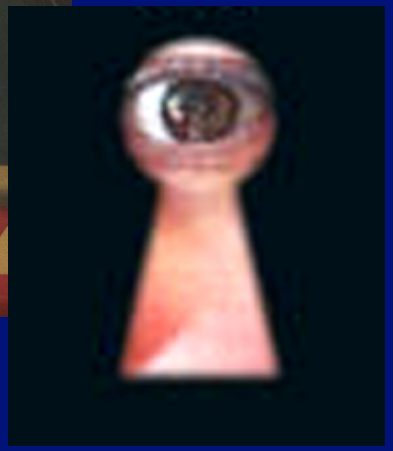
Ma riprendiamo questa scienza sin dall'inizio.....

Alice

Alice

Bob

Alice



Bob

Antichi esempi

Erodoto: Storie (V secolo a. C.)

Aeneas Tacticus
Poliorketika (IV secolo a. C.)

Διονγσιος Καλος

Δ / :: / ⁘ / Ν / ⁙ / Σ / :: / ⁘ / Σ Κ / · / Λ / ⁘ / Σ

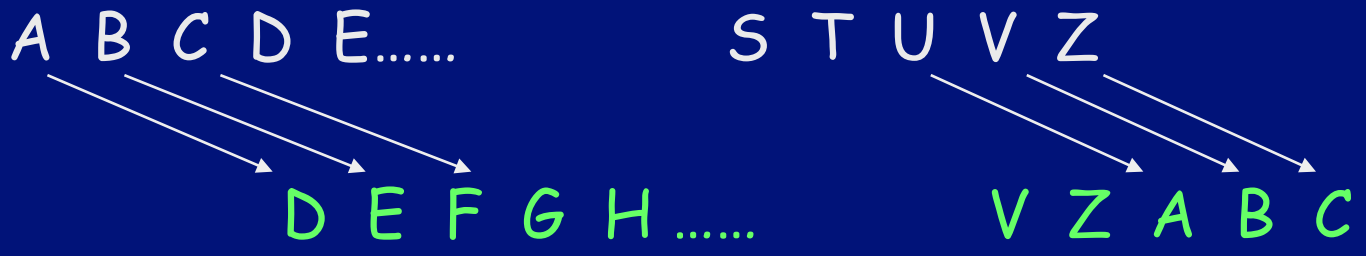
Il numero di puntini corrisponde alla posizione della vocale nell'alfabeto !

Svetonio

Le vite di dodici Cesari

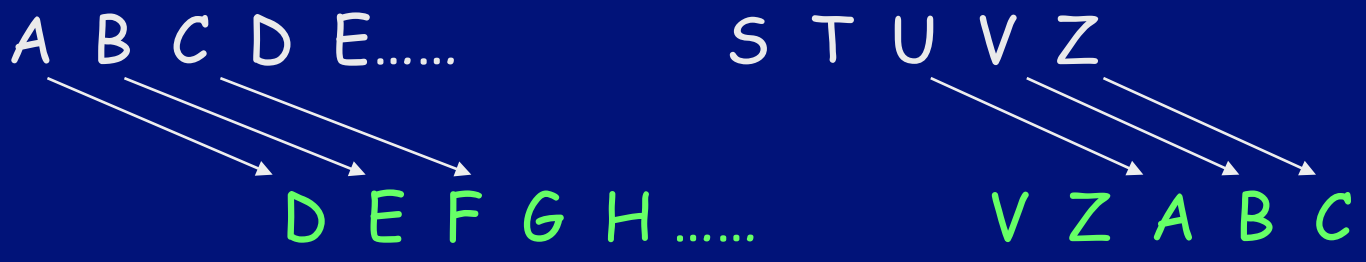
Svetonio
Le vite di dodici Cesari

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



Svetonio
Le vite di dodici Cesari

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



C A I U S I U L I U S C A E S A R
F D L X V L X O L X V F D H V D U

Ogni codice segreto non può essere mantenuto tale troppo a lungo

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 (il codice di Cesare non aveva chiave)

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".

La chiave suggerita è la corrispondenza casuale di coppie di lettere.

Si può prendere una permutazione arbitraria dell'alfabeto come chiave:

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

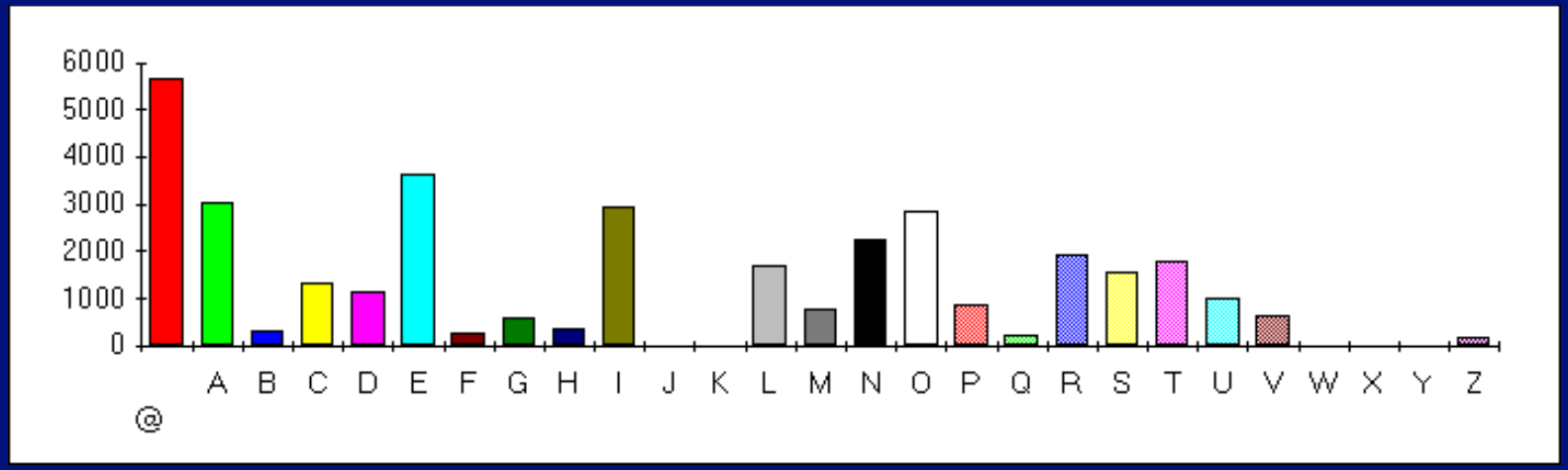
messaggio cifrato: TSRAFRAURAFTSBFSV

vi sono 26! chiavi possibili, un numero enorme. Non è possibile attaccare il cifrario provandole una a una, tuttavia .....

.... il cifrario è attaccabile facilmente con un' analisi statistica sulla frequenza delle lettere

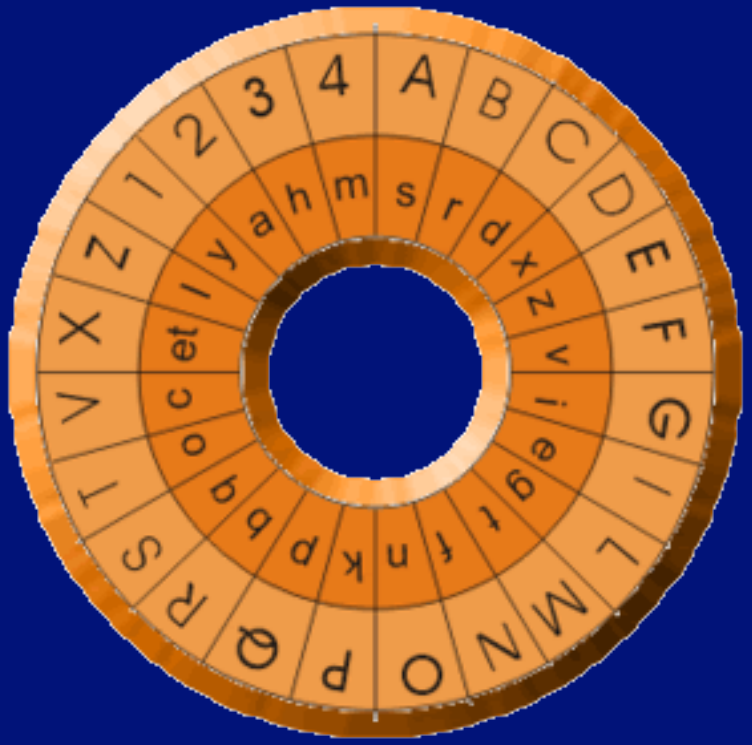
.... il sistema è attaccabile facilmente con un' analisi statistica sulla frequenza dei caratteri

Frequenze dei caratteri in italiano rilevate su "I Promessi Sposi"



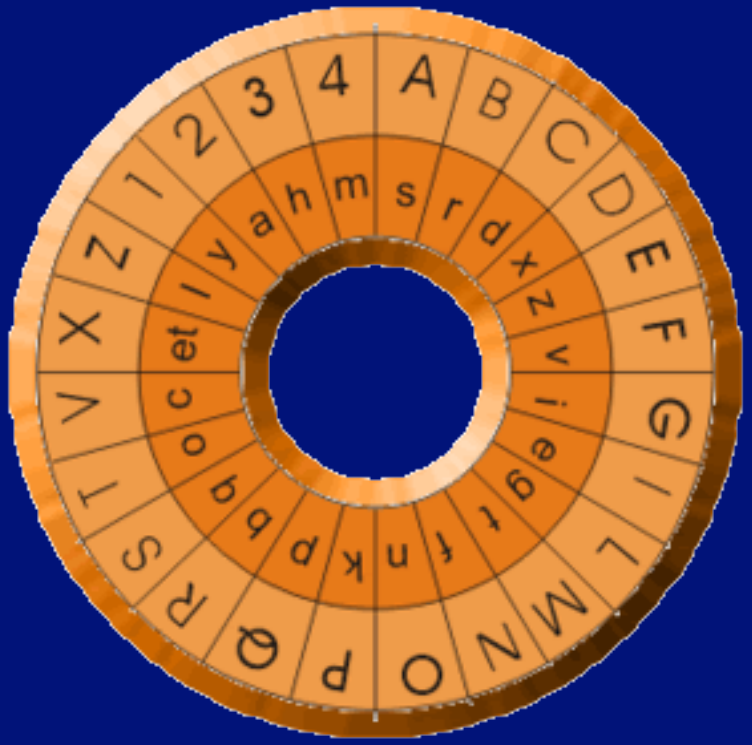
Nascita dei cifrari polialfabetici:

il disco di Leon Battista Alberti (XV secolo)



Nascita dei cifrari polialfabetici:

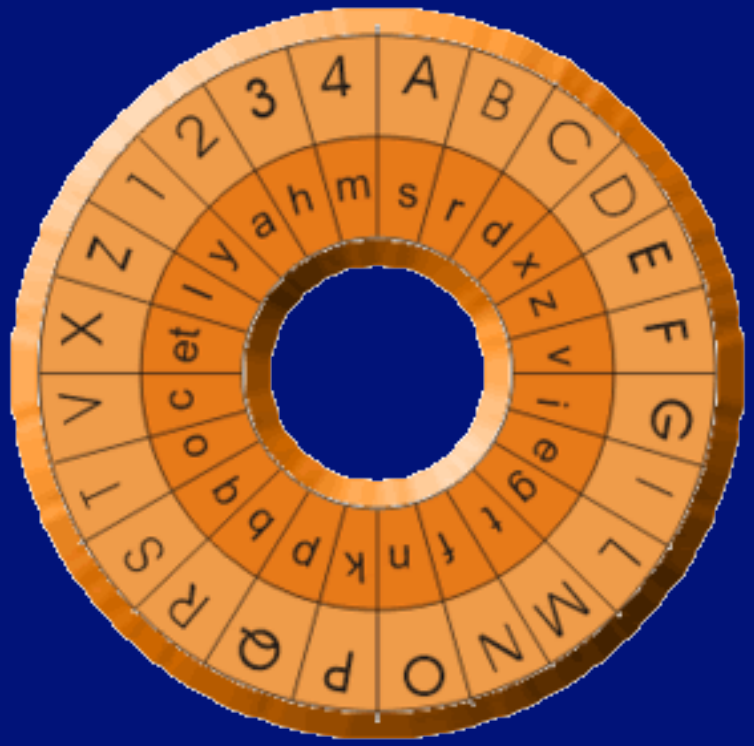
il disco di Leon Battista Alberti (XV secolo)



Chiave: **B-r**

Nascita dei cifrari polialfabetici:

il disco di Leon Battista Alberti (XV secolo)



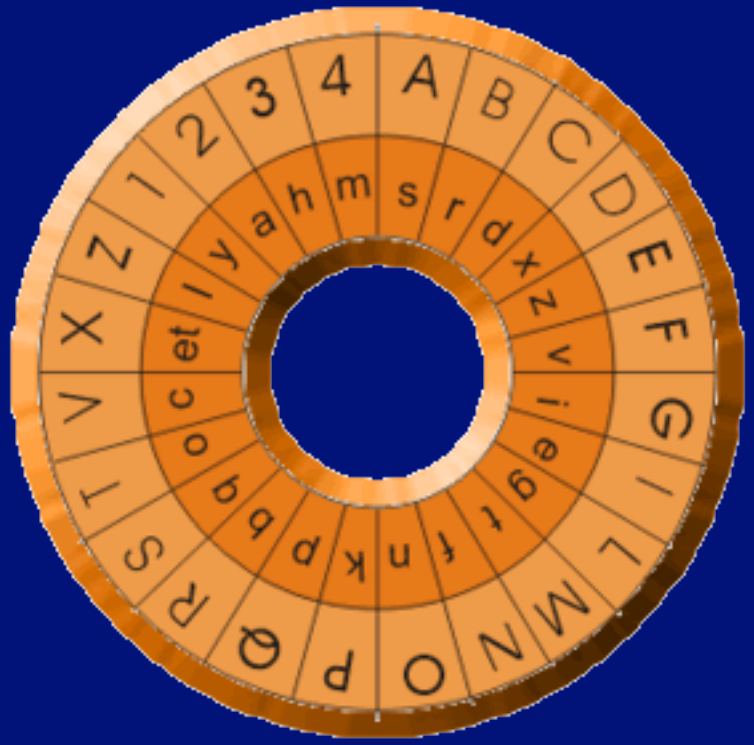
Chiave: **B-r**

C A E 2 S A R

d s z a n y f

Nascita dei cifrari polialfabetici:

il disco di Leon Battista Alberti (XV secolo)



Chiave: **B-r**

C A E 2 S A R
d s z a n y f

qui la chiave diventa **B-a**

Sull'idea di Alberti lavorò de Vigenère (1586)

La chiave è corta e ripetuta ciclicamente.

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

C A I U S I U L I U S C A E S A R

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

E B R B T O Z M R B T G C F C E S

Se estendiamo il metodo di Vigenère impiegando una chiave lunga come il testo, casuale e non riutilizzabile, il cifrario diviene inattaccabile!

È il caso di One-Time Pad (1917) che impiega un codice binario per messaggi e chiavi

Fu usato nella Hot Line per le comunicazioni tra la Casa Bianca e il Cremlino a partire dal 1967

Nel 1972 nasce un codice standard a chiave segreta:

Data Encryption Standard (DES)

- Pubblicamente noto e realizzabile in hardware su computer di ogni tipo
- Chiave di 8 caratteri
- Ogni carattere del crittogramma dipende da tutti i caratteri della chiave

Il DES è tuttora il cifrario più usato, ma le chiavi originali non sono sicure con i computer di oggi. In genere si usa il 3DES con chiavi di doppia lunghezza.

Su Internet si costruisce una nuova chiave per ogni "sessione".

Nel 2000 è nato il nuovo standard:

Advaced Encription Standard (AES)

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

Qui entrano in gioco i numeri primi !

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 oggi comunemente citata come esempio di affermazione clamorosamente smentita dai fatti, ma ci ricorda che ogni scienza di base può giocare un ruolo fondamentale nel progresso tecnologico.

La smentita a Hardy venne dall'invenzione della crittografia a chiave pubblica, nata ufficialmente nel 1976 ma preceduta dal lavoro, coperto da segreto, degli agenti britannici del 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.

Diffie

Merkle

Hellman

1976
Public Key Cryptography

Viene proposta alla comunità scientifica la definizione di crittografia a chiave pubblica, destinata a mutare profondamente le transazioni commerciali su Internet

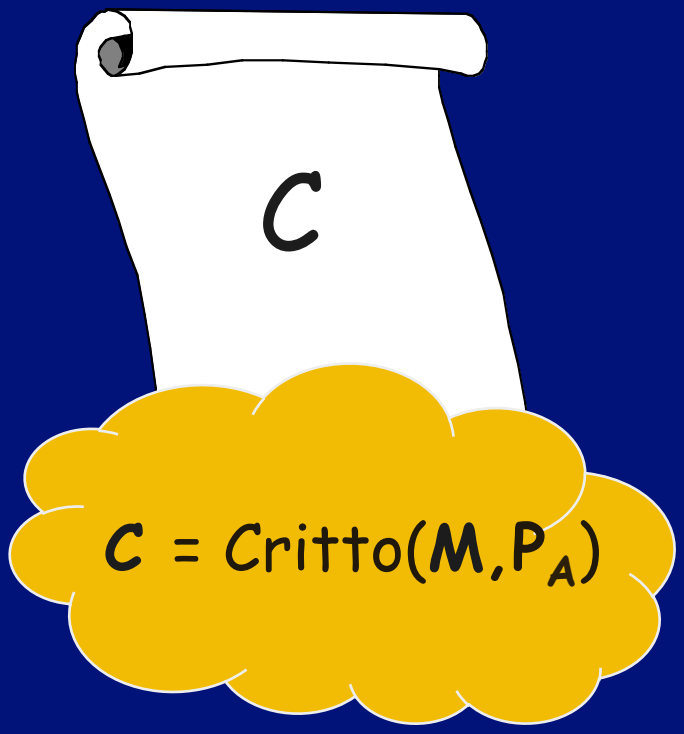
Alice sceglie due chiavi: una segreta e una pubblica

Chiave segreta S_A

Pubblico Registro

Utente	Chiave publica
.....	.....
A	P_A

Bob vuole spedire un messaggio M ad Alice in modo segreto

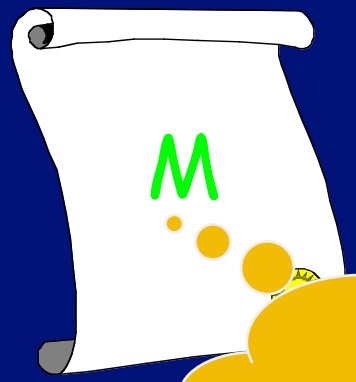


Pubblico Registro

Utente	Chiave publica
.....	.....
A	P_A

Alice traduce il crittogramma C di Bob

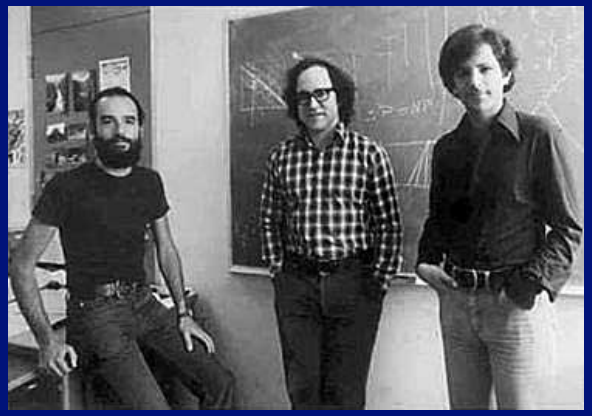
Nessun altro può farlo senza conoscere S_A



$M = Decritto(C, S_A)$

C ?

R S A (1977)



Shamir

Adleman

Rivest

propongono un sistema a chiave pubblica basato su una funzione "facile" da calcolare e "difficile" da invertire

facile da calcolare …

e difficile da invertire …

a meno che non si conosca
una chiave segreta !

RSA si basa sulla moltiplicazione di due numeri primi p, q che abbiamo già incontrato:

RSA si basa sulla moltiplicazione di due numeri primi p, q che abbiamo già incontrato:

Calcolare $n = p \times q$ è facile

Calcolare p, q da n è difficile
a meno che non si conosca uno dei due

RSA si basa sulla moltiplicazione di due numeri primi p, q che abbiamo già incontrato:

Calcolare $n = p \times q$ è facile

Calcolare p, q da n è difficile
a meno che non si conosca
uno dei due

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

Esempio: p = 5 q = 7

A calcola n = 55, $\Phi(n) = (p-1)x(q-1) = 40$

sceglie e < 40 e primo con 40, e = 7

determina d inverso di e, modulo 40.

d=23 (7x23=1 mod 40)

pubblica P_A = <7, 55> e tiene segreta S_A=23

B per spedire M<55

calcola $C = M^e \bmod n = M^7 \bmod 55$

A per decifrare

calcola $M = C^d \bmod n = C^{23} \bmod 55$

LA CARTA DI CREDITO SU INTERNET

Se un cliente C desidera comprare da una ditta D, i computer di C e D devono essere in grado di eseguire gli stessi algoritmi crittografici (per esempio RSA e DES), cioè in questi computer devono essere istallati programmi compatibili tra loro.

RSA per scambio di chiave segreta

DES per scambio dei messaggi

UN PROTOCOLLO RSA - DES

1. D spedisce a C un messaggio detto certificato digitale contenente la chiave pubblica P_D di RSA;

2. C costruisce una chiave segreta random K da impiegare nel DES, cifra K con la chiave P_D con RSA e la invia a D;

3. D ricostruisce K usando la sua chiave RSA segreta S_D; ora C e D hanno la chiave comune K per il DES;

4. C e D si scambiano messaggi in DES; tra questi, i dati sensibili di C.

Perché D deve mandare un certificato ?

Il passo 1 del protocollo precedente (D manda a C la sua chiave pubblica) è molto pericoloso!

Uno spione S potrebbe inviare la sua chiave pubblica P_S a C facendo finta di essere D e decifrare poi i dati di di C con la sua chiave segreta S_S!

Firma Digitale

- A ha due chiavi, una pubblica P_A e una segreta S_A.
  - Per firmare un messaggio M (non necessariamente cifrato), A cifra M con la sua chiave segreta S_A e ottiene F (la firma digitale) e manda a B sia M che F.
  - B decifra F con la chiave pubblica P_A di A.e se ottiene M la firma è autentica.
- F può essere generato solo da A poiché è l'unico a conoscere S_A.

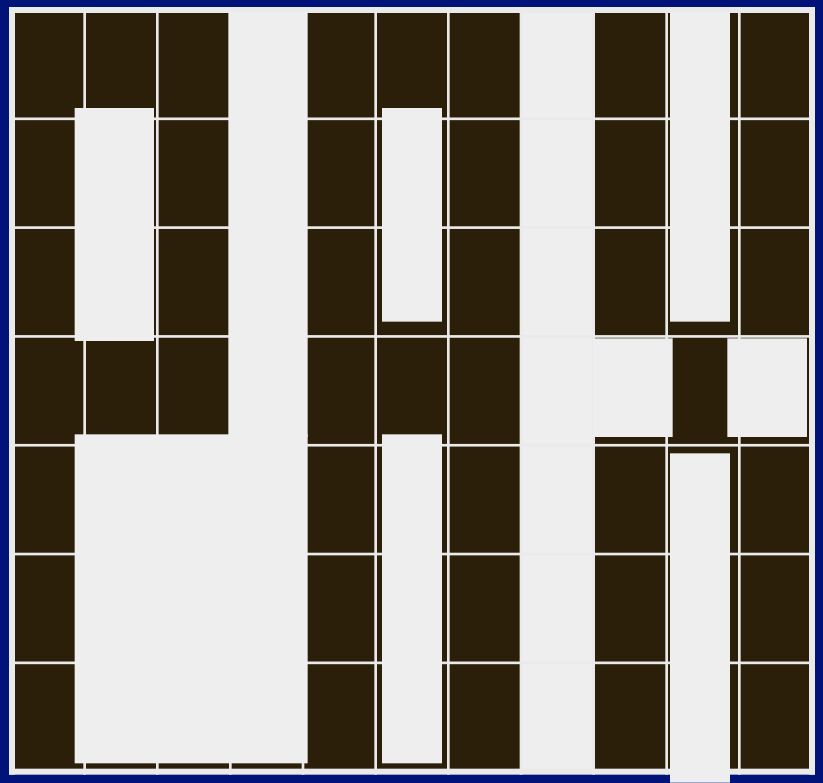
Certification Authority (CA)

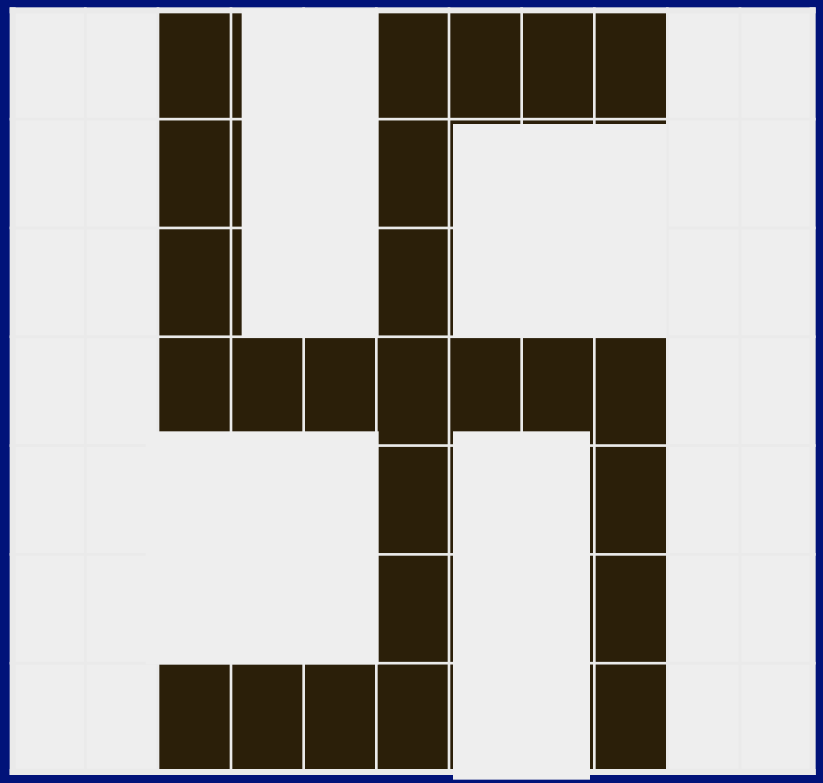
- assegna a ogni utente un file (certificato digitale).
- Il certificato è firmato dalla CA con la sua chiave segreta.
- L' authenticità di un certificato può essere verificato controllando la firma digitale della CA che l'ha emesso.

Steganografia

- L'immagine sullo schermo è formata da un insieme di punti: pixel;
- Ciascun pixel può assumere 256 diversi colori (1 byte color).
- Esempio con solo 4 livelli di grigio numerati da 0 (bianco) a 3 (nero) . O con 8 livelli da 0 (bianco) to 7 (nero) .

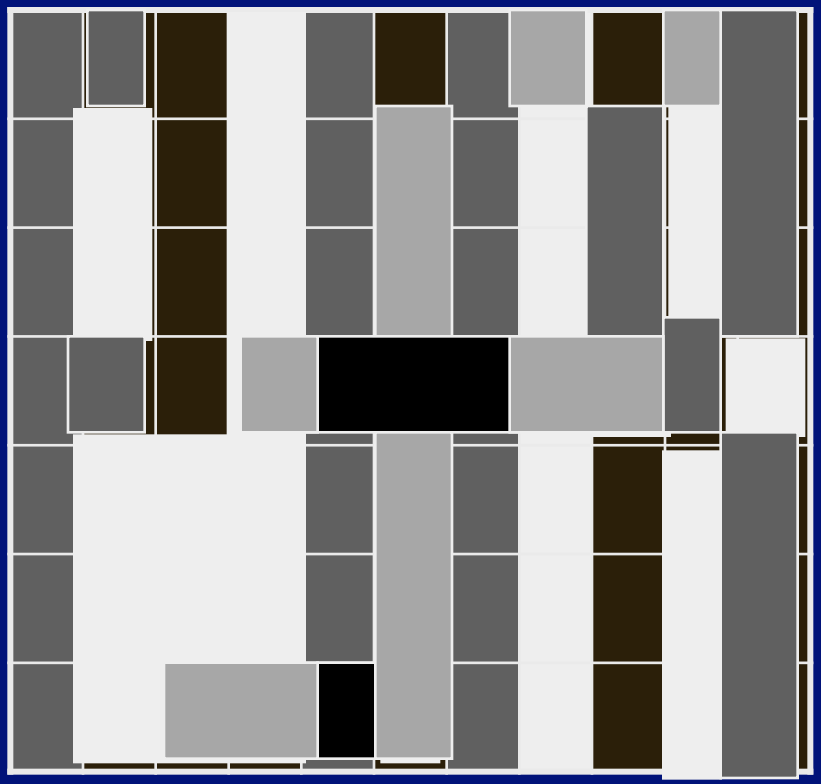
Nascondi un'immagine in un'altra

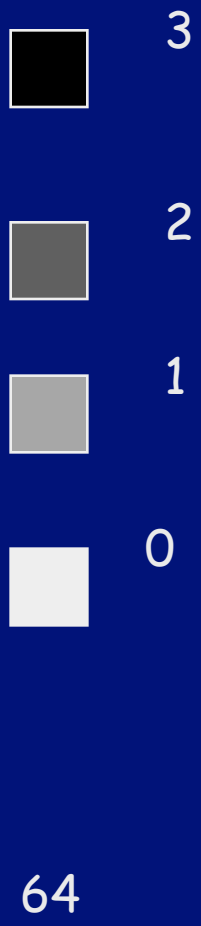




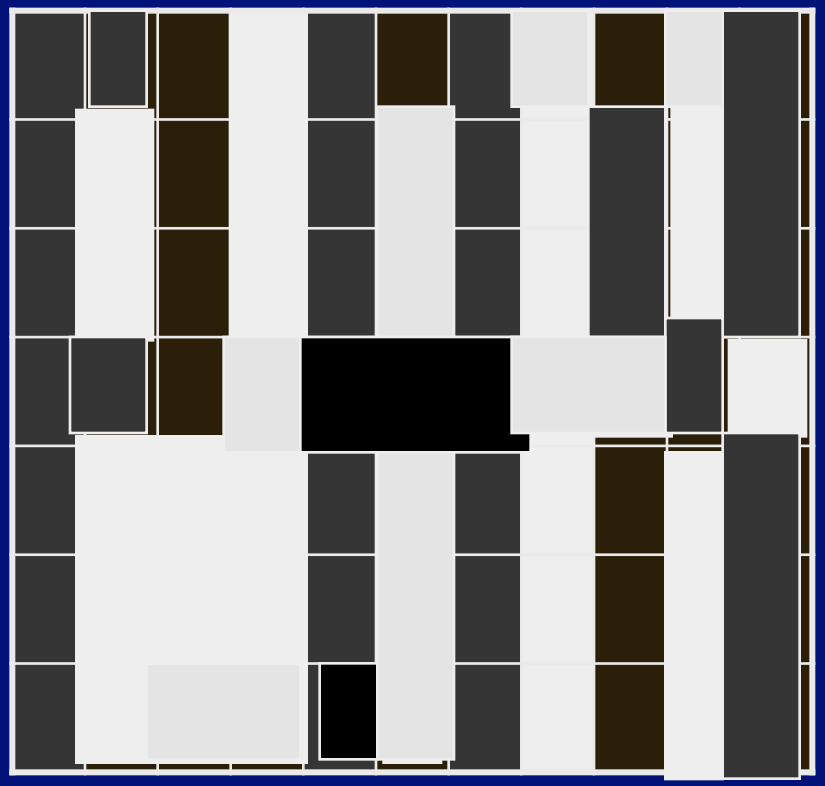
- Mischia le immagini lasciando invariati i pixels uguali in pax e svastica;
- Poni i pixels neri in pax e quelli bianchi in svastica a 2
- Poni i pixels bianchi in pax e neri in svastica a 1

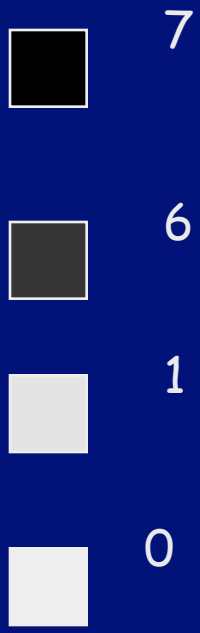
.





Aumentando i livelli di grigio a 8:





Per ricostruire la svastica assegna bianco ai pixel pari e nero a quelli dispari

Bibliografia per cominciare

Marcus du Sautoy. L'Enigma dei numeri primi.
BUR Saggi, Milano 2005.

Simon Singh. Codici e Segreti.
Rizzoli, Milano 1999.

Paolo Ferragina, Fabrizio Luccio.
Crittografia: principi, algoritmi, applicazioni.
Bollati Boringhieri 2001.