



Luoghi comuni sulla matematica

- La matematica è arida e mortifica la fantasia.

Sai, per essere un matematico non aveva abbastanza immaginazione; ma ora è diventato un poeta e se la cava davvero bene.

(David Hilbert, parlando di un suo ex studente)

- Un matematico può fare solo l'insegnante di matematica.
- La matematica è inutile.

Un ponte tra università e aziende

De Componendis Cifris Welcome ▾ Associazione ▾ Attività ▾ Collabora con noi ▾

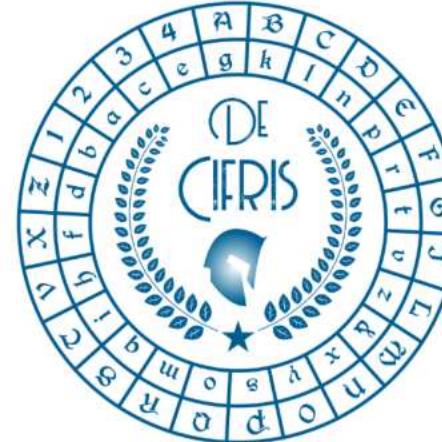
Fai ricerca?

Lavori in azienda?

Insegni a scuola?

Sei studente?

Ti incuriosisce?



L'associazione di promozione sociale De Componendis Cifris o, in forma abbreviata De Cifris, si propone di animare la comunità crittografica italiana, sia nelle sue componenti accademiche, che nelle sue ramificazioni nel mondo del lavoro e dell'impresa.

Tra gli obiettivi, si prefigge di:

- Incentivare in Italia lo studio e la ricerca nell'ambito della crittografia a livello accademico e applicativo, con particolare attenzione alle aree della Matematica, dell'Informatica e dell'Ingegneria.
- Sostenere la realizzazione di qualificati progetti di ricerca che richiedano il coinvolgimento e la collaborazione di numerosi studiosi appartenenti a discipline anche molto diverse.
- Divulgare l'uso responsabile della crittografia, favorendo il formarsi di una cultura propria e autonoma.
- Contribuire al rafforzamento della cooperazione internazionale in questo settore, in ambito scientifico e del suo impiego, anche con principi di solidarietà.

La De Cifris auspica che l'Italia possa sviluppare cifrari robusti e flessibili, adatti all'era moderna, e che emergano talenti dedicati alle scienze crittografiche. L'associazione intende coinvolgere enti del mondo accademico, così come centri di ricerca, aziende, studenti universitari, liberi professionisti, e più in generale tutti coloro che condividono questa visione.

Fra le varie iniziative proposte si evidenziano numerosi seminari, diffusi anche tramite le pagine YouTube e LinkedIn dell'associazione.

Luoghi comuni sulla matematica

- La matematica è arida e mortifica la fantasia.

Sai, per essere un matematico non aveva abbastanza immaginazione; ma ora è diventato un poeta e se la cava davvero bene.

(David Hilbert, parlando di un suo ex studente)

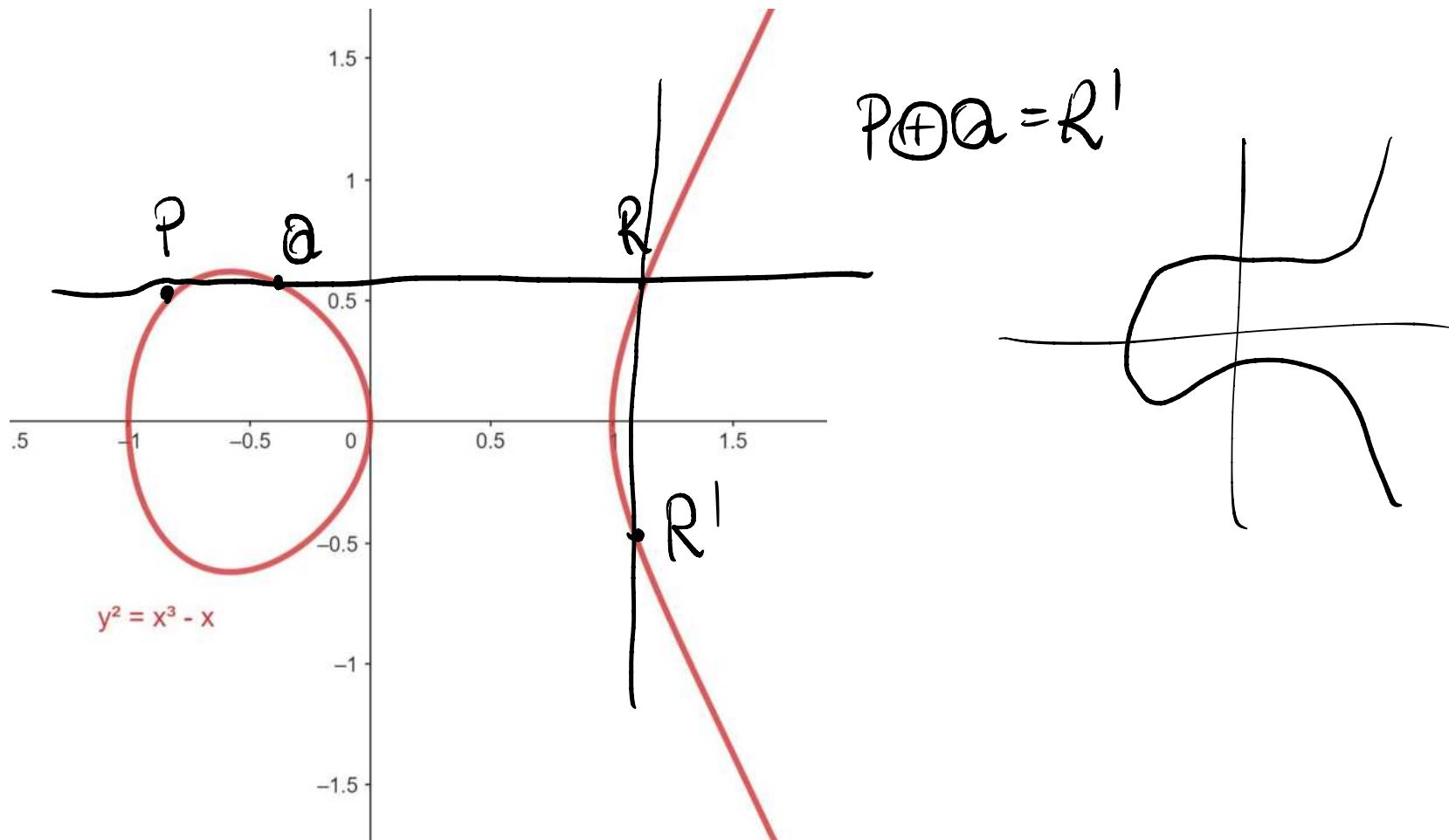
- Un matematico può fare solo l'insegnante di matematica.
- La matematica è inutile.

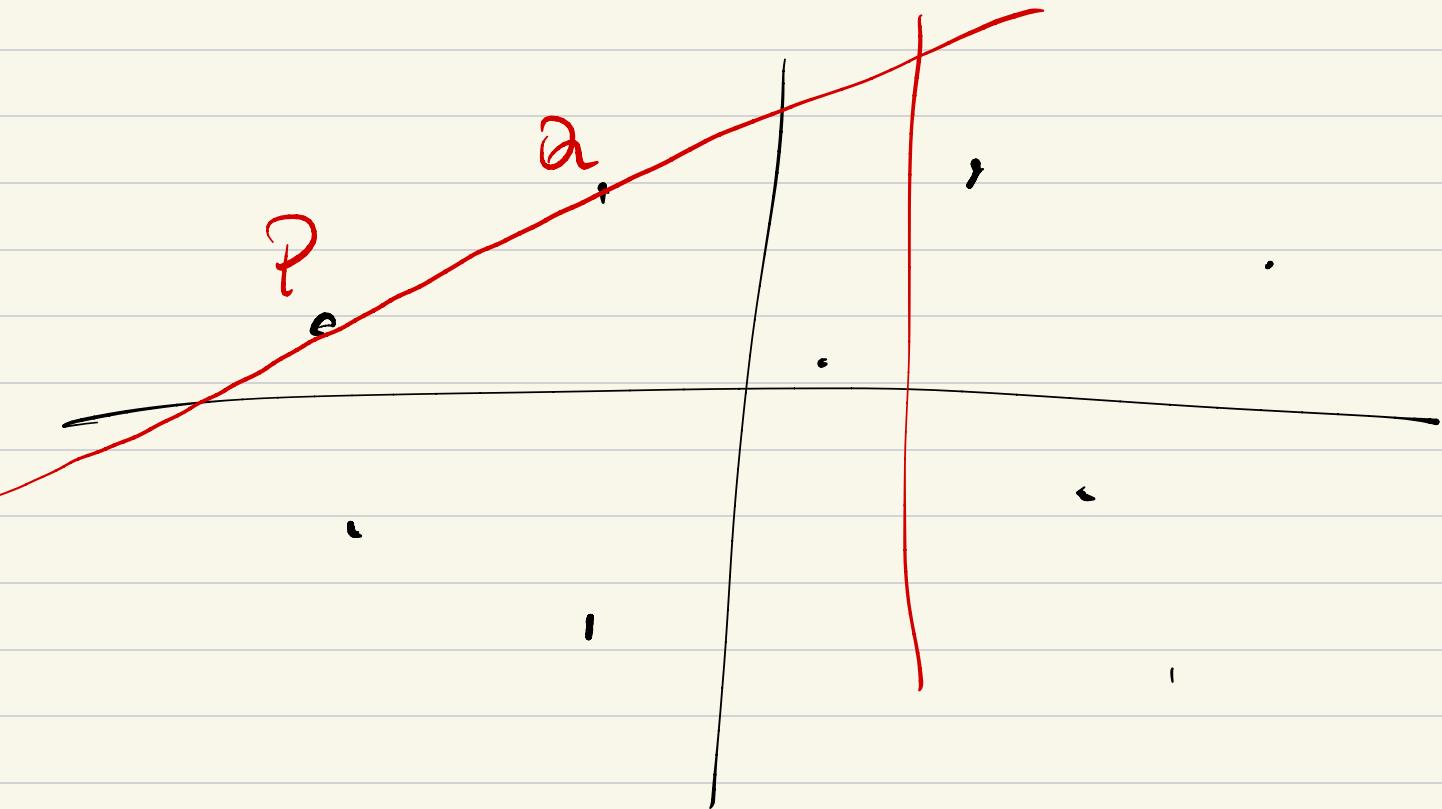
Curve ellittiche

$$ax^3 + by^3 + cx^2y + dx^2y^2$$

$$y^2 = x^3 - x$$

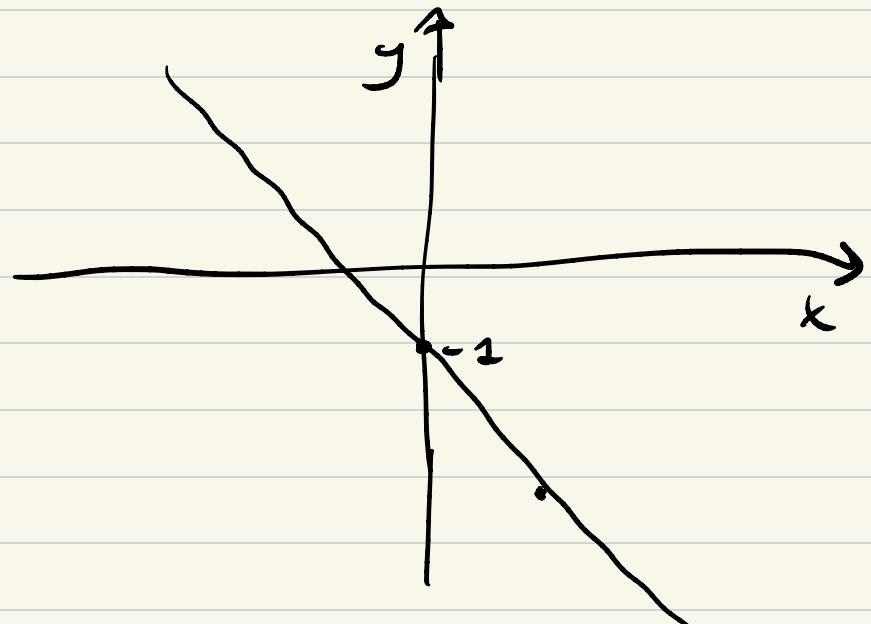
$$y^2 = x^3 + Ax + B$$





CURVE ALGEBRICHE : $F(x, y) = 0$, F polinomio

1) F polinomio di grado 1: $ax + by + c = 0$, $a, b, c \in \mathbb{R}$



$$(x, y) \in \mathbb{R} \times \mathbb{R} \text{ t.c.}$$

$$ax + by + c = 0$$

$$3x + y + 1 = 0$$

$$\begin{aligned} x = 0 &\rightarrow 0 + y + 1 = 0 \\ y &= -1 \end{aligned}$$

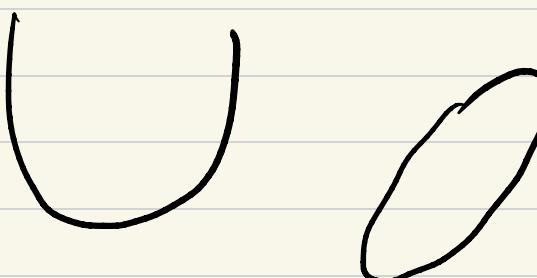
$$\boxed{x = 1} \rightarrow 3 \cdot 1 + y + 1 = 0 \rightarrow \boxed{y = -4}$$

$(1, -4)$

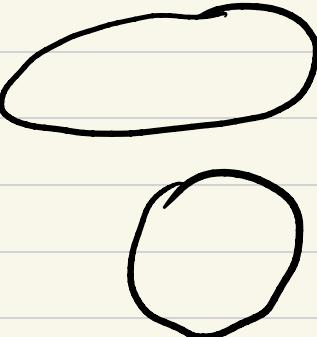
$$(0, -1) \in \text{curve.}$$

2) F grado 2

$$F(x,y) = 0 : ax^2 + by^2 + cxy + dx + ey + f = 0$$
$$a, b, \dots \in \mathbb{R}$$



(x,y) che verificano
l'equazione e
le segnano.



CONICHE

PARABOLE ELLISI (IPERBOLI)

Curve ellittiche

*«It is possible to write endlessly on elliptic curves.
This is not a threat!»*

(Serge Lang)

- Gauss (1777-1855)
- Abel (1802-1829)
- Jacobi (1805-1851)
- Legendre (1752-1833)

$$y^2 = x^3 + Ax + B$$

$$(x, y) \in \mathbb{Q} \times \mathbb{Q}$$

$$(x, y) \in \mathbb{Z} \times \mathbb{Z}$$

$$\mathbb{N} = \{1, 2, 3, 4, \dots\}$$

NATURALI

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

INTERI

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$$

RAZIONALI

R

• π

e

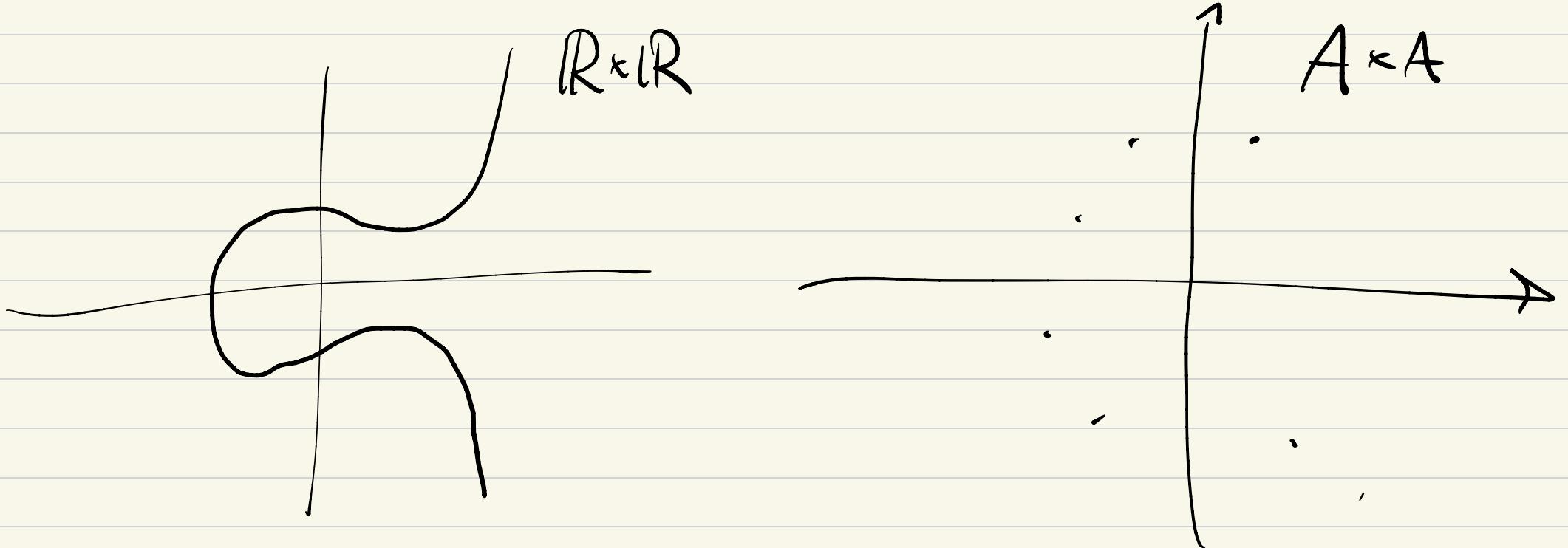
• $\sqrt{2}$

• α

N

Z

• β



(1,3)

$$3, \overline{3} \xrightarrow{\text{EQ}} \frac{10}{3} \quad \begin{array}{c} 13 \\ \hline 10 \end{array} = \frac{26}{20}$$

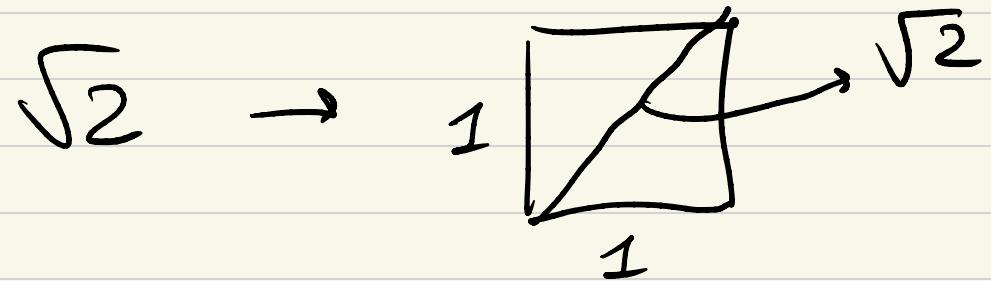
$3, \overline{67} \xrightarrow{\text{EQ}}$

$$\overbrace{\begin{array}{r} 10 \\ 9 \\ \hline 10 \end{array}}^{\widehat{10}} + \begin{array}{r} 3 \\ 3 \\ \hline 33 \end{array}$$
$$\begin{array}{r} 9 \\ 9 \\ \hline 10 \\ 9 \\ \hline \end{array}$$

$\pi \sim 3,1428 \rightsquigarrow$ NO FRAZIONE

$e \sim 2,7 \rightarrow$ NUMERO DI EULERO/NEPERO

$\sqrt{2} \sim 1,4 \dots$



$$\mathbb{R} = \mathbb{Q} \cup \overline{\mathbb{I}} \rightarrow \begin{cases} e, \pi \\ \sqrt{2} \end{cases} \xrightarrow{\text{TRASCENDENTI}}$$

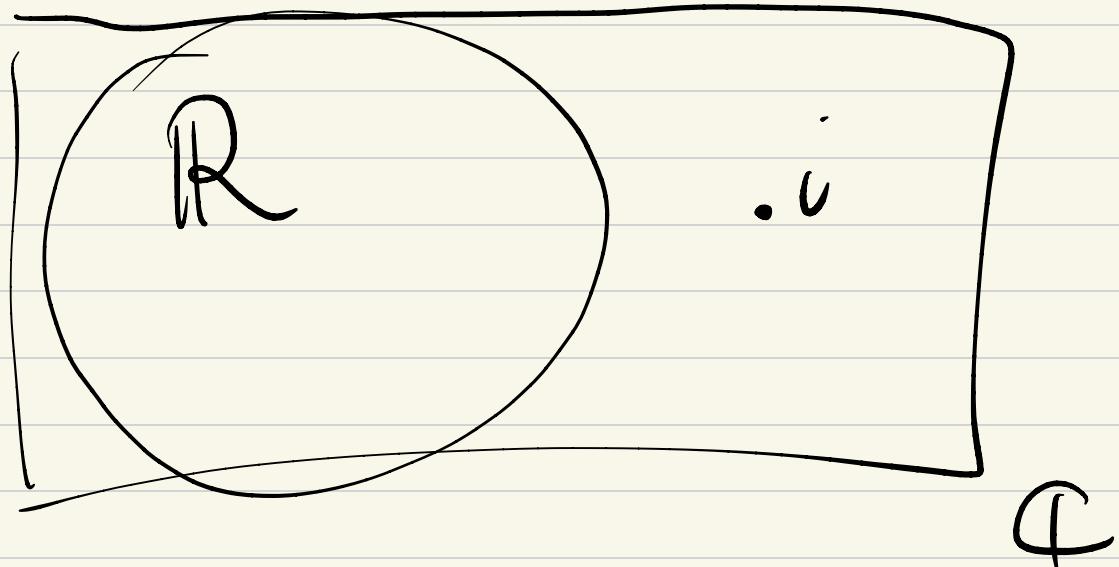
Oss. me: $\sqrt{2} \notin \mathbb{Q}$ ma $\sqrt{2}$ verifica l'equazione

$$x^2 - 2 = 0$$

$\rightarrow \sqrt{2}$ soluzione di equazione polinom.
a coeff. razionali.

$\pi \notin \mathbb{Q}$ ma si può dimostrare che non è RAZ
soluzione di eq. pol. o coeff. razionali.

$$x^2 + 1 = 0 \rightarrow i \text{ tc } \boxed{i^2 = -1} \quad i = \sqrt{-1}$$



$$a+ib, a, b \in \mathbb{R}$$

Curve... in tasca



Curve... in tasca

$$y^2 = x^3 + 486662x^2 + x$$

$$y^2 = x^3 + Ax + B$$

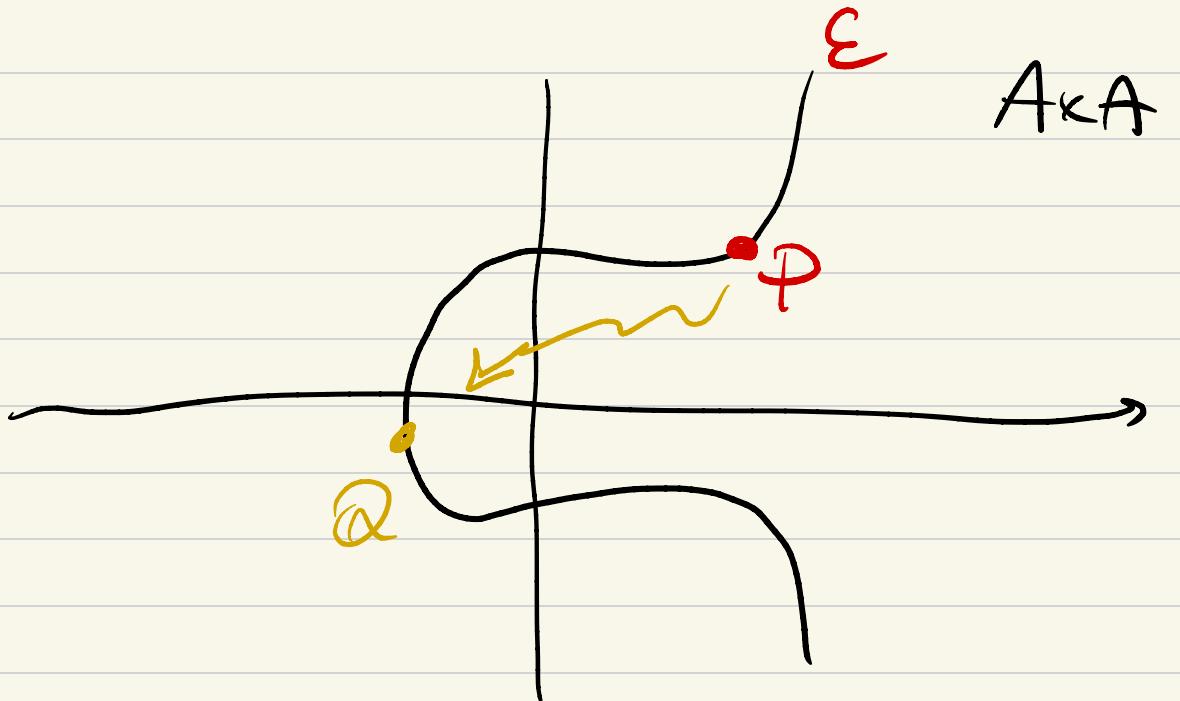
Curva 25519:

The first time a WhatsApp group member sends an Add-on to a Community Announcement Group::

1. The sender generates a random 32-byte Chain Key.
2. The sender generates a random **Curve25519** Signature Key key pair.
3. The sender combines the 32-byte Chain Key and the public key from the Signature Key into into an Add-on Sender Key message.
4. The sender individually encrypts the Add-on Sender Key to each member of the community announcement group, using the pairwise messaging protocol explained previously.

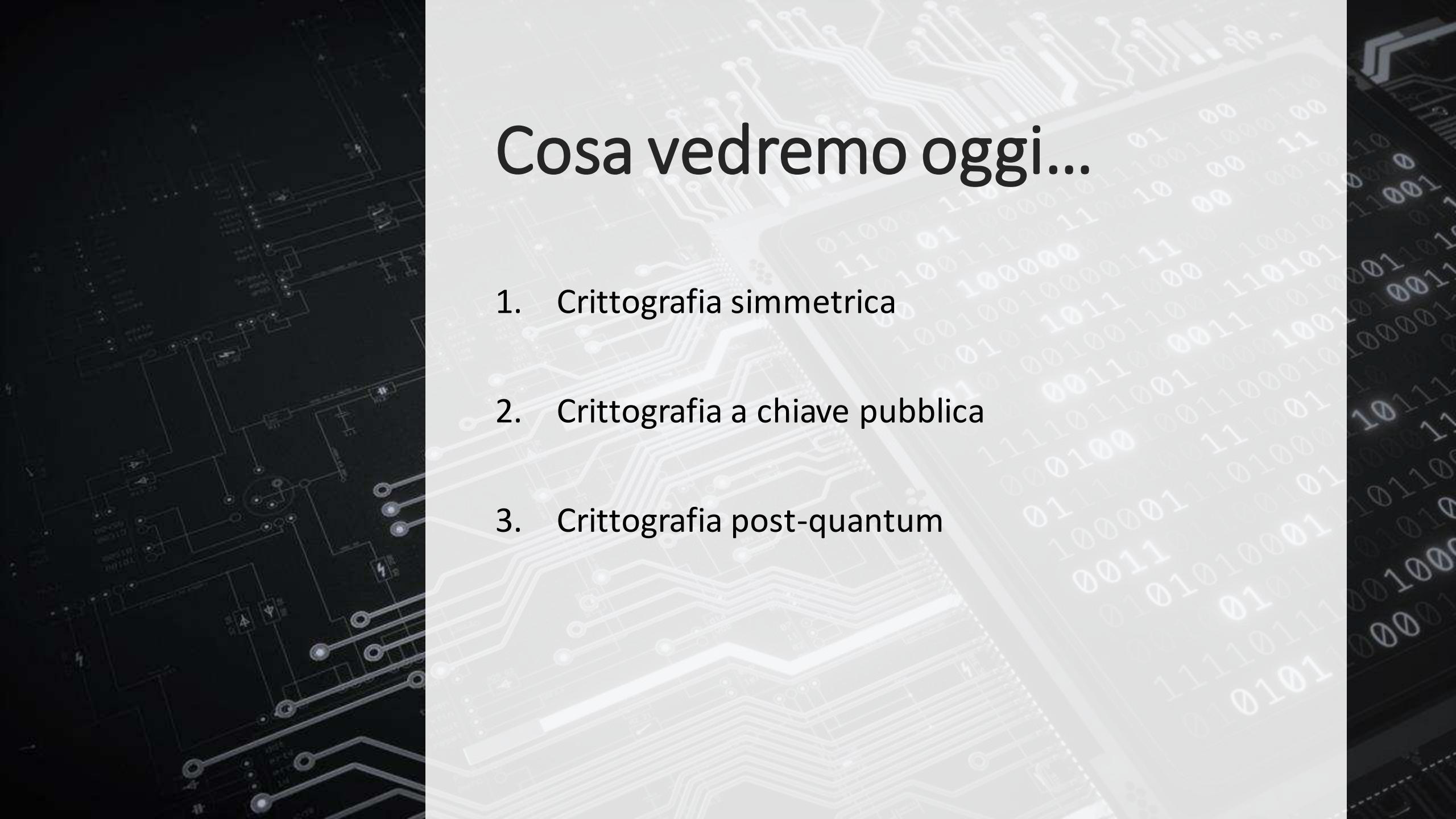
For all Add-ons sent to a community announcement group:

1. The sender derives an encryption key from the target message's Message Secret Add-on Target Key = HKDF(length=32, key=Target Message Secret, info=Target Message Identifier || Target sender Identifier || Add-on Sender Identifier || "Add-on type string").
2. The sender then encrypts the Add-on content with Add-on Target Key using AES-256-GCM to produce inner ciphertext.
3. The sender derives a Message Key from the Chain Key, and updates the Chain Key



A&A

M \rightsquigarrow Pee



Cosa vedremo oggi...

1. Crittografia simmetrica
2. Crittografia a chiave pubblica
3. Crittografia post-quantum



Crittografia simmetrica

Cos'è la Crittografia?

- È la scienza (arte) che studia come rendere **segreta** e **sicura** la comunicazione tra due persone (Alice e Bob) o entità nascondendo il significato del messaggi.
- Crittografia significa letteralmente «scrittura segreta».
- Con questo termine si intende oggi un insieme di tecniche che consentono di trasmettere messaggi mantenendoli segreti a tutti, tranne ad alcune persone che possiedano la chiave per comprenderli.



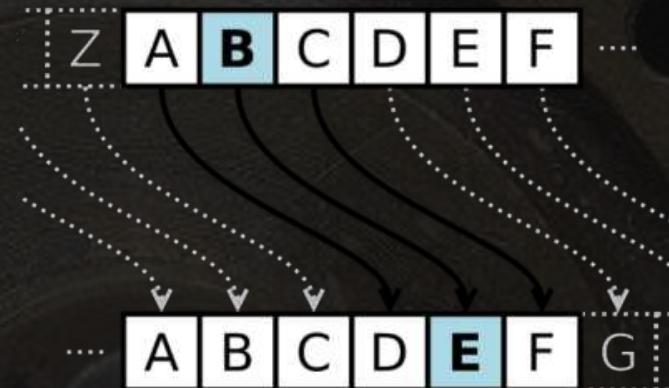
$20 \xrightarrow{+3} 20 + 3 \rightarrow 2$

$2 \xrightarrow{+3} C$

Un metodo molto antico: il CIFRARIO DI CESARE

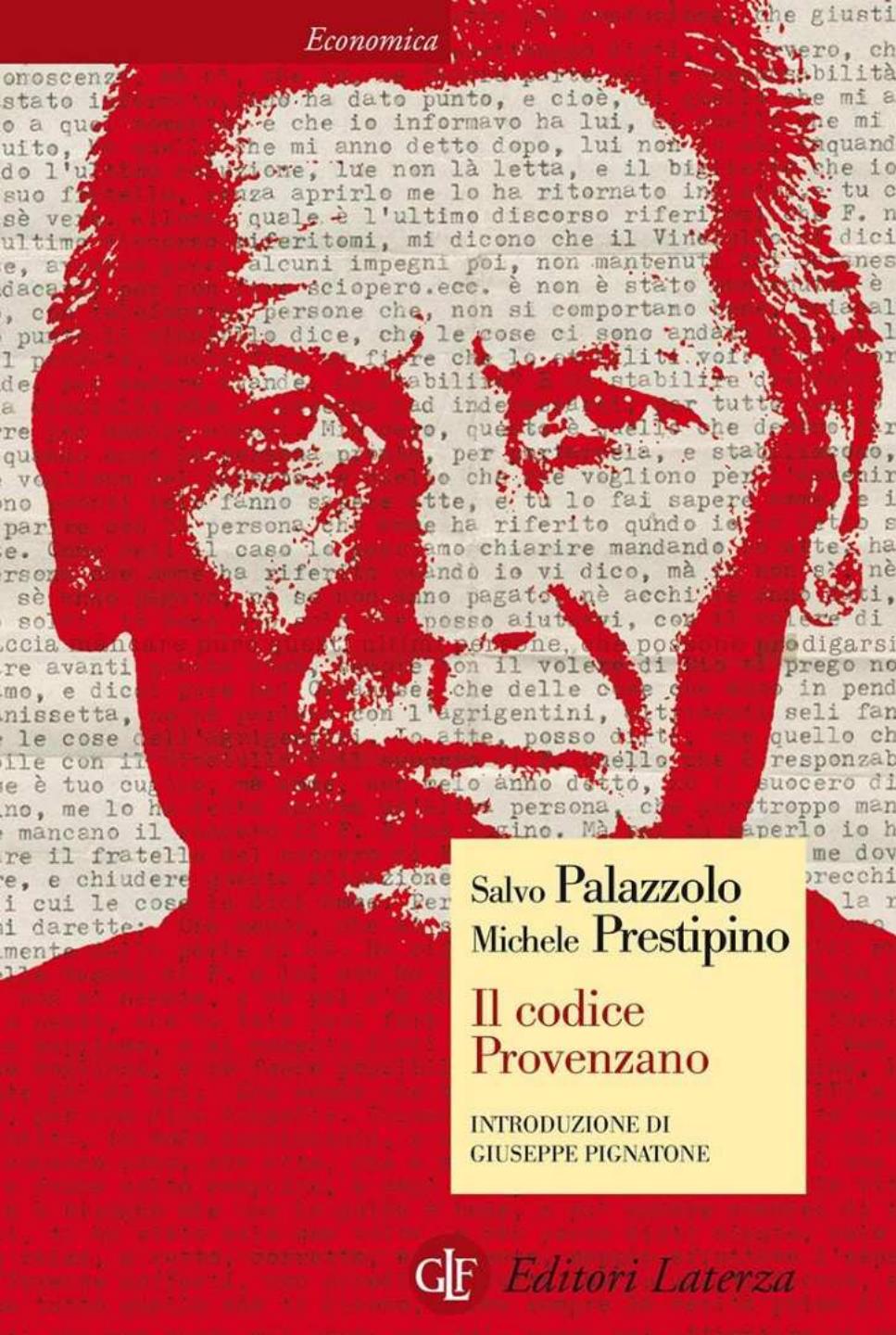
"Extant et ad Ciceronem, item ad familiares domesticis de rebus, in quibus, si qua occultius preferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset: quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet..,

(Svetonio, De Vita Caesarum)



scien~~ze~~ → vfnhq~~ch~~

PRINCIPIO DI RERKHOFF: La sicurezza di un criptosistema
si basa solo sulla segretezza
della chiave



Un metodo molto antico...ma non troppo

«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 sommato a 3 e di comporre così un singolo, lungo numero.»



Un metodo molto antico: il CIFRARIO DI CESARE

Da un punto di vista matematico...

1. Corrispondenza lettere-numeri

A	B	C	D	...	X	Y	Z
0	1	2	3	...	23	24	25

1. Cifratura: X si trasforma in $X + 3 \pmod{26}$
2. Chiave? **3**

La matematica dell'orologio

$$32 = 12 \cdot 2 + 8$$

$$21 = 12 \cdot 1 + 9$$

$$b = q \cdot a + r$$

Divisione

Euclidea

Un'aritmetica inusuale:

- I numeri del nostro ambiente sono: $0, 1, 2, \dots, 11$ e corrispondono alle ore di un nostro orologio
- Le operazioni sono intese in questo modo:
 - **somma:** $a + b$ è l'ora che si ottiene spostando la lancetta dalla posizione a in avanti di b ore;
 - **prodotto:** $a \cdot b$ è l'ora che si ottiene sommando a a sé stessa b volte.

I risultati nella matematica dell'orologio vengono distinti dagli altri mediante l'espressione **(mod 12)**.

Esercizio 1

Calcolare $7 \cdot 3 \pmod{12}$, $8 \cdot 4 \pmod{12}$, $10 \cdot 5 \pmod{12}$.

Esercizio 2

Riflettere sul rapporto che c'è fra i risultati usuali e i risultati $\pmod{12}$.

$50 \text{ mod } 12$

$$\begin{array}{r} 50 \\ 48 \\ \hline 2 \end{array}$$

$$7^{15} = \underbrace{7 \cdot 7}_{15} \cdot 1$$

$1200 \cdot 183 \text{ mod } 10$

La matematica dell'orologio

Problema 1

Provare a dare una definizione matematica di $a + b \text{ (mod } 12)$ e di $a \cdot b \text{ (mod } 12)$ che non faccia uso dell'orologio.

Quindi:

- $a + b \text{ (mod } 12)$ è il resto della divisione di $a + b$ per 12;
- $a \cdot b \text{ (mod } 12)$ è il resto della divisione di $a \cdot b$ per 12.

Gara 1

Calcolare $7^{15} \text{ (mod } 12)$ nel minor tempo possibile **senza calcolatrice**.

Idea chiave: elevare a potenza nella matematica dell'orologio può essere un'operazione molto più veloce di quello che si potrebbe immaginare.

Generalizziamo: ARITMETICA MODULARE

Non c'è niente di speciale nel numero 12. Sostituiamolo con un numero intero n qualsiasi, purché maggiore di 1.

$$\begin{array}{r} 2210 \\ \hline 20 \end{array}$$

- I numeri del nostro ambiente sono: $0, 1, 2, \dots, n - 1$
- Le operazioni sono intese in questo modo:
 - $a + b \pmod{n}$ è il resto della divisione di $a + b$ per n ;
 - $a \cdot b \pmod{n}$ è il resto della divisione di $a \cdot b$ per n .

Questo insieme numerico viene indicato con il simbolo:

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

Quando è chiaro che ci stiamo riferendo ad operazioni in \mathbb{Z}_n possiamo omettere l'espressione $(\text{mod } n)$.

Esercizio 3

Calcolare: $21 + 23 \pmod{14}$, $21 \cdot 23 \pmod{19}$, $2210 \pmod{20}$, senza calcolatrice.

$$2210 \pmod{20} = 0$$

CRITOSISTEMA. \rightarrow Una quintupla (P, C, K, E, D)

P = insieme Testi in chiaro

C = insieme Testi cifrati

K = insieme chiavi

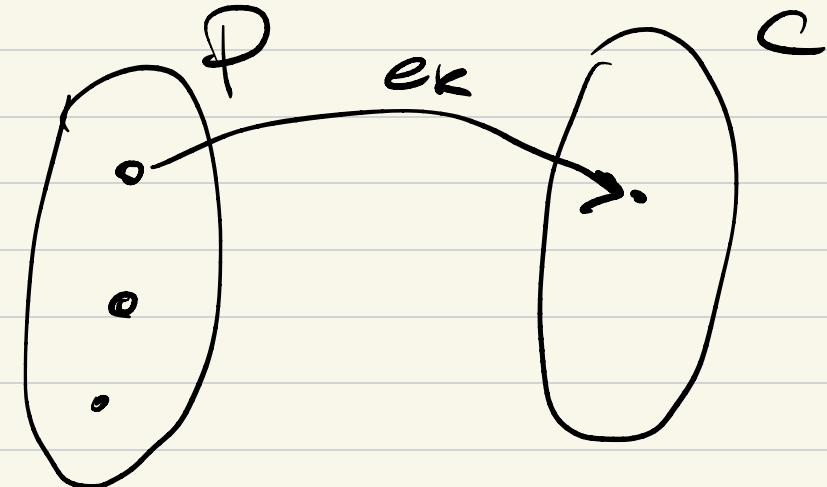
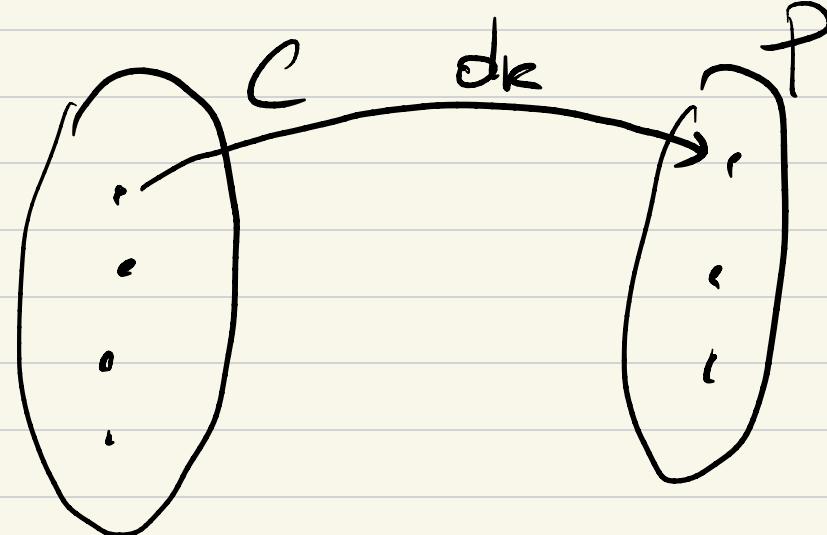
E = funzioni cifratura

D = funzioni di decifrazione.

$$E : \forall k \in K \exists e_k : P \rightarrow C$$

per ogni \downarrow esiste \downarrow
 \uparrow appartiene

$D: \forall k \in \mathbb{K} \exists d_k \in D, d_k: C \rightarrow P$



Proprietà (Correttezza):

Fisso $k \in K$ no e_k, d_k .

Voglio che $\forall m \in P$, $d_k(e_k(m)) = m$

- Proprietà:
- e_k, d_k siano computazionalmente semplici da calcolare. (comodità)
 - Da e_k e d_k deve essere computazionalmente difficile ricavare k . (sicurezza)

CIFRARIO DI CESARE $\rightarrow (\mathcal{P}, \mathcal{C}, k, \mathcal{E}, \mathcal{D})$

$$\mathcal{P} = \{A, B, C, \dots\} = \{0, 1, \dots\} = \mathbb{Z}_{26}$$

$$\mathcal{C} = \mathbb{Z}_{26}$$

$$\mathcal{K} = \mathbb{Z}_{26} \setminus \{0\}$$

$$\mathcal{E} = \{e_k : \mathcal{P} \rightarrow \mathcal{C} \mid k \in \mathcal{K}\}, \quad e_{\mathbb{Z}_{26}}(x) = x + k \pmod{26}$$

$$\mathcal{D} = \{d_k : \mathcal{C} \rightarrow \mathcal{P} \mid k \in \mathcal{K}\}, \quad d_k(y) = y - k \pmod{26}$$

VERIFICO LA CORRETEZZA:

$$\forall x \in P, d_k(e_k(x)) = x$$

$$d_k(e_k(x)) = d_k(x+k) = (x+k) - k = x + k - k = x \quad \checkmark$$

GENERALIZZIAMO: $P = C = \mathbb{Z}_{26} \circ \mathbb{Z}_{21}$

$$x \mapsto x+k = f(x)$$

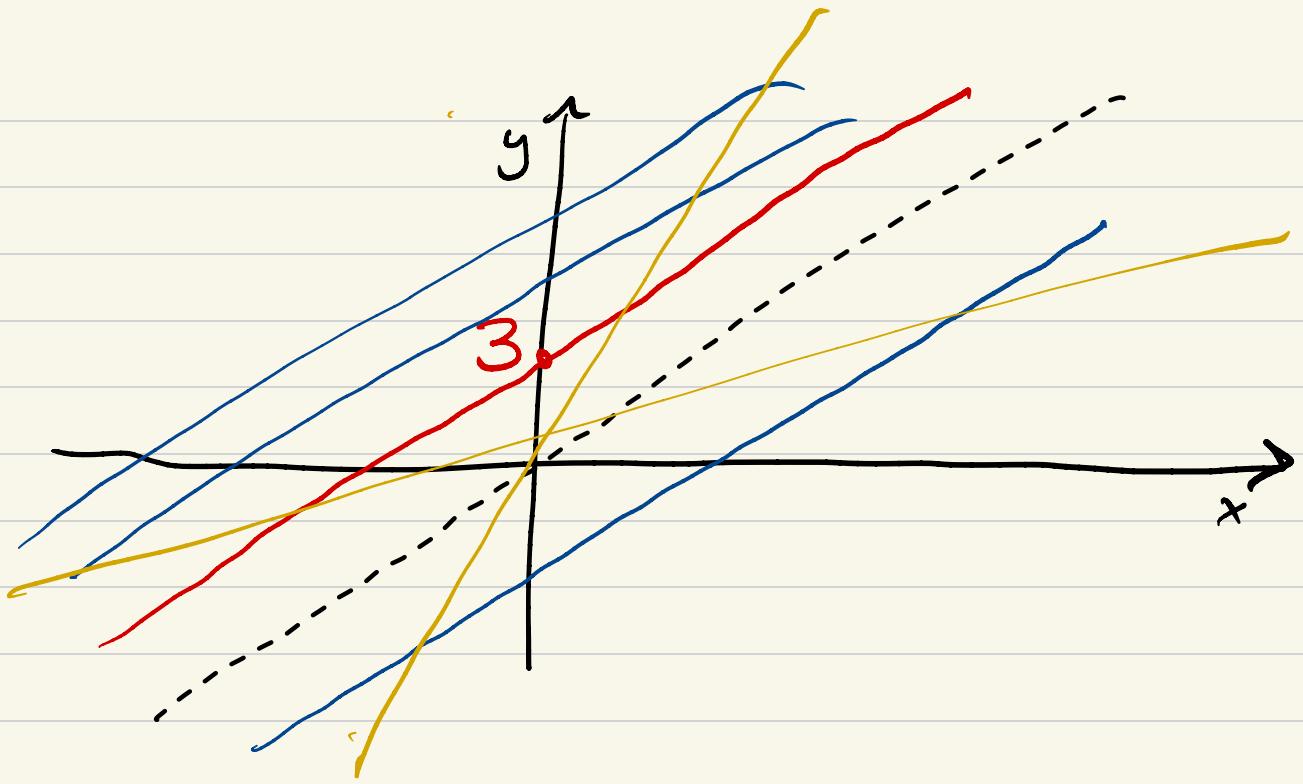
$$f(x) = x+k \quad \text{l'insieme}$$

$$y = mx + q$$

+
PENDENZA

BISETTRICE
 $1^\circ e 3^\circ$

$$y = x$$



Cesare: $y = x + 3$

$y = x + k$

$y = mx + q$

$$E : e_k(x) = ax + b \pmod{26} \quad a, b \in \mathbb{Z}_{26}$$

$$k = (a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}$$

$$(P, C, K, E, D) \text{ have } P = C = \mathbb{Z}_{26}$$

$$K = \mathbb{Z}_{26} \times \mathbb{Z}_{26}$$

$$E : e_{(a,b)}(x) = ax + b \pmod{26}$$

$$D : d_{(a,b)}(y) = \dots$$

Una possibile generalizzazione...

Il cifrario di Cesare:

- Testi in chiaro: \mathbb{Z}_{21}
- Testi cifrati: \mathbb{Z}_{21}
- Chiavi: \mathbb{Z}_{21}
- Codifica: $e_k(x) = x + k \pmod{21}$

Cifrario affine:

- Testi in chiaro: \mathbb{Z}_{21}
- Testi cifrati: \mathbb{Z}_{21}
- Chiavi: $\mathbb{Z}_{21} \times \mathbb{Z}_{21}$
- Codifica: $e_{a,b}(x) = a \cdot x + b \pmod{21}$

$$(a, b) = (3, 1) \leftarrow e_{(3, 2)}(x) = 3x + 1 \pmod{21}$$

0 \longrightarrow

1

2

3

4

5

A \longmapsto B

H \longmapsto B

$a \in \mathbb{Z}_{21}$ t.c $\text{MCD}(a, 21) = 1$

$a \downarrow$
a INVERTIBLE IN \mathbb{Z}_{21}

$$3 \cdot 0 + 1 = 1$$

$$3 \cdot 7 + 1 = 21 + 1 = 1$$

$$ax+b = ay+b \text{ con } x \neq y$$

PROBLEMA

$$ax+b \stackrel{\text{mod } 21}{=} ay+b$$

$$ax = ay \rightarrow ax - ay = 0 \rightarrow a(x-y) = 0 \text{ mod } 21$$

a invertibile $\leftrightarrow \text{MCD}(a, 21) = 1$, $a(x-y) = 0$

$$a^{-1} \cdot a(x-y) = 0 \cdot a^{-1}$$

$$1 \cdot (x - y) = 0$$

$$x - y = 0$$

$$\boxed{x = y}$$

$$K = \cancel{\mathbb{Z}_{26} \times \mathbb{Z}_{26}} = \mathbb{Z}_{26}^* \times \mathbb{Z}_{26}$$

$\underbrace{}$
↑
el. invertibili
di \mathbb{Z}_{26}

Clifratio affine: $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{26} \times \mathbb{Z}_{21}$

$$K = \mathbb{Z}_{26}^* \times \mathbb{Z}_{21}$$

$$e_{(a,b)}(x) = ax + b \pmod{26}$$

$$d_{(a,b)}(y) = \frac{y - b}{a} \pmod{26}$$

$$d_{(a,b)}(e_{(a,b)}(x)) = d_{(a,b)}(ax + b) = \frac{ax + b - b}{a} = \frac{ax}{a} = x$$

THM: $a \in \mathbb{Z}_m$ è invertibile $\Leftrightarrow \text{MCD}(a,m) = 1$

Esperimento 1

Calcolare le funzioni di codifica relative alle seguenti chiavi: $(3, 0)$, $(3, 1)$, $(2, 0)$, $(2, 1)$.

Discutere i risultati ottenuti.

- Perché le chiavi con $a = 3$ non sono adeguate, mentre quelle con $a = 2$ sì?
- Qual è secondo voi la **motivazione** di natura matematica?

$$a \cdot x_1 = a \cdot x_2 \text{ per qualche } x_1 \neq x_2$$

- Quale **congettura** di carattere generale vi sentireste di formulare al riguardo? Come si distinguono le chiavi valide da quelle non valide (se necessario, provate anche altre chiavi!)
- Come provereste a **dimostrare** tale congettura?

Deve esistere x con $ax = 1 \pmod{21} \Rightarrow ax = c \cdot 21 + 1$. Ciò implica $MCD(a, 21) = 1$. Viceversa, se $MCD(a, 21) = 1$ allora $ax_1 = ax_2$ non può mai verificarsi dato che 21 divide $a(x_1 - x_2)$.

$$3! = 3 \cdot 2 \cdot 1 = 6$$

$$4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$$

$$5! = 120$$

$$6! = 720$$

Sostituzioni monoalfabetiche

$$21! = 21 \cdot 20 \cdot 19 \cdot \dots \cdot 2 \cdot 1$$

- In generale il crittosistema di Cesare è un cifrario in cui la stessa lettera è cifrata sempre con la stessa lettera (**Sostituzione monoalfabetica**).
- Più in generale si dice «cifrario di Cesare» un cifrario nel quale la lettera del messaggio chiaro viene spostata di un numero fisso k di posti (k è la **chiave**).
- Il caso più generale è quello in cui l'alfabeto cifrato è una **permutazione** di quello in chiaro.

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
m	n	b	v	c	x	z	a	s	d	f	g	h	j	k	l	p	o	i	u	y	t	r	e	w	q

Sostituzioni monoalfabetiche: la sicurezza

$$\begin{array}{ccc} A & \xrightarrow{\quad} & R \\ 0 & & 15 \end{array}$$

$$\begin{aligned} x &\mapsto x+k \\ 0 &\mapsto 0+k = 15 \\ k &= 15 \end{aligned}$$

- Le possibili permutazioni dell'alfabeto italiano sono $21!$ (circa 51×10^{18}).
- Una ricerca esaustiva per trovare la permutazione giusta è praticamente impossibile, eppure questi cifrari sono tutt'altro che sicuri.



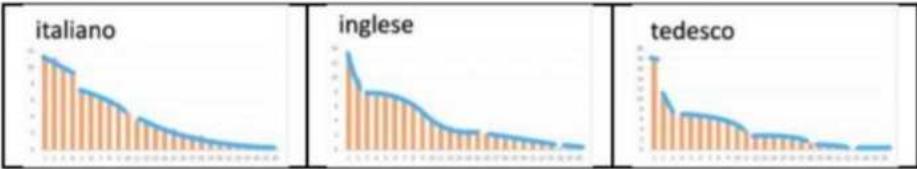
IMPRONTA LINGUISTICA

$$\begin{array}{l} B \mapsto R \\ C \mapsto H \end{array} \quad \begin{array}{l} 1 \mapsto 15 \\ 2 \mapsto 7 \end{array} \quad \left\{ \begin{array}{l} a \cdot 1 + b = 15 \\ a \cdot 2 + b = 7 \end{array} \right.$$

$$\hookrightarrow a =$$

$$b = -$$

Le caratteristiche statistiche delle lingue

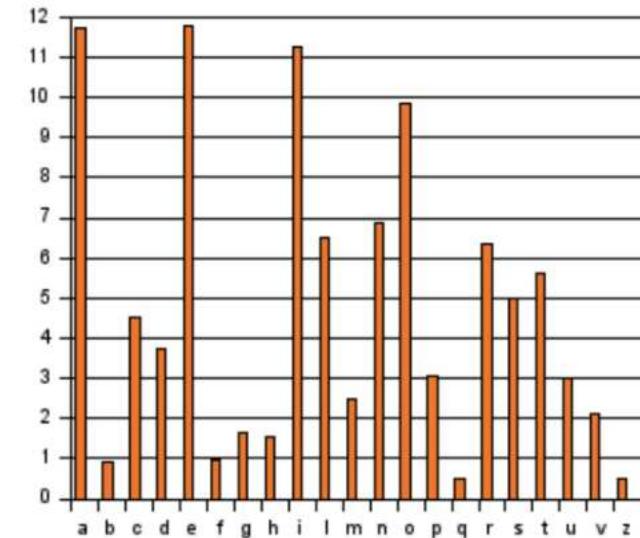


- Ogni lingua si differenzia dalle altre per caratteristiche statistiche quali la frequenza delle singole lettere, dei bigrammi e dei digrammi; nell'insieme queste caratteristiche costituiscono una vera e propria *impronta digitale* della lingua.
- Per esempio, l'italiano è una lingua molto vocalizzata, l'inglese, al contrario, presenta un'alta frequenza di consonanti. Il francese è anch'esso molto vocalizzato anche se è ricco di lettere come la J, che in italiano sono poco frequenti. La lettera E è la più frequente in quasi tutte le lingue europee, in particolare in francese e in tedesco ha una prevalenza nettissima.
- Questa impronta digitale è di grande importanza per la crittanalisi statistica.

Le frequenze della Lingua Italiana

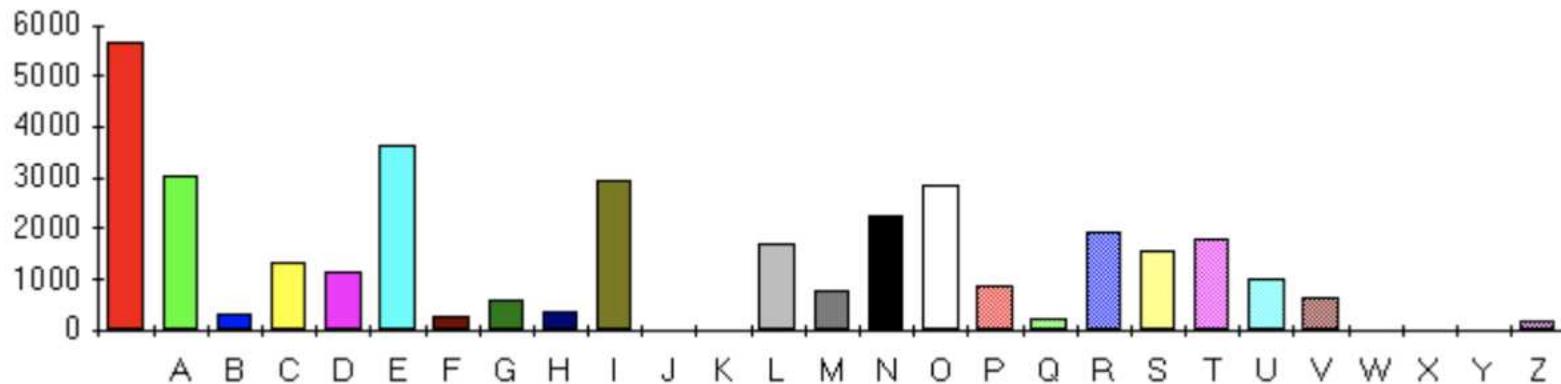
- È detto da tutti che l'italiano è una lingua musicale; infatti analizzando un testo e calcolando la frequenza delle varie lettere , si può notare che le vocali **E, A, I, O** sono le lettere più frequenti, senza che esista una preponderanza netta di una di queste sulle altre, e la loro percentuale, che in media raggiunge il 46,4%, è tra le più alte tra le varie lingue esaminate
- Seguono le consonanti **L, N, R, S, T.**
- Tra i bigrammi più frequenti troviamo **Q-U** sempre seguiti da vocale. La lettera H è spesso preceduta dalla lettera C o G per formare i trigrammi **CHE , CHI , GHE , GHI** . Nella lingua italiana sono quasi assenti le lettere J, K, Y, X, W salvo nei nomi di persone o località straniere.

·Lettera	·%	·Lettera	·%	·Lettera	·%
·a	·11,74	·h	·1,54	·q	·0,51
·b	·0,92	·i	·11,2 8	·r	·6,38
·c	·4,50	·l	·6,51	·s	·4,98
·d	·3,73	·m	·2,52	·t	·5,63
·e	·11,79	·n	·6,88	·u	·3,02
·f	·0,95	·o	·9,83	·v	·2,10
·g	·1,65	·p	·3,05	·z	·0,49



Le frequenze della Lingua Italiana

Il seguente grafico mostra la frequenza delle varie lettere del primo capitolo del celebre romanzo di Alessandro Manzoni, «*I Promessi Sposi*».



Frequenze letterali ne *I PROMESSI SPOSI*

A	11,51
B	0,97
C	4,69
D	3,72
E	12,4
F	1,5
G	1,71
H	1,34
I	9,53

J	0
K	0
L	5,56
M	2,36
N	7,29
O	9,64
P	2,96
Q	0,77
R	6,59

S	5,46
T	6,8
U	3,56
V	2,3
W	0
X	0
Y	0
Z	0,75

Bigrammi e doppie ne *I PROMESSI SPOSI*

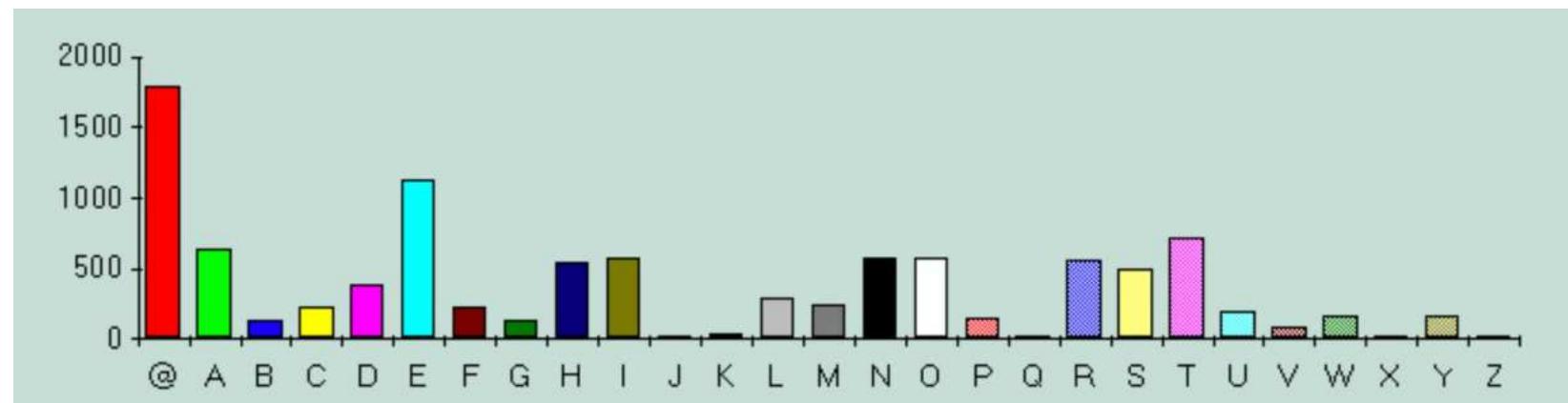
Bigramma	Percentuale
ER	1,91%
ON	1,68%
EN	1,54%
AN	1,52%
RE	1,44%
TO	1,38%
ES	1,36%
DI	1,31%
AR	1,37%

Doppia	Percentuale
LL	0,86%
TT	0,73%
SS	0,64%
CC	0,38%
AA	0,3%
EE	0,3%
BB	0,19%
RR	0,18%
NN	0,18%

Le frequenze della Lingua Inglese

- Anche per questa lingua, la lettera **E** è la più frequente, ma essa ha una frequenza di poco superiore a quella della lettera **T**, che immediatamente la segue. Seguono poi le vocali (in ordine) **O, A, I**, e le consonanti **N, R, S, H**, che non hanno frequenze molto diverse l'una dall'altra.
- Le lettere più frequenti formano la successione mnemonica: ETOANIRSH.
- I seguenti bigrammi sono tra i più frequenti: TH, HE, AN, ER, ON, RE, IN, ED, ND, AT, OF, OR, HA, EN, NT, EA, TO, TI, ST, IT, ecc., con frequenze percentuali che variano tra 35 e 10 per mille lettere di un testo normale. Le lettere J, V, Z sono sempre seguite da vocali.

Questo grafico illustra la frequenza delle lettere presenti nel primo capitolo del «*Frankenstein*» di Mary Shelley.



Un po' di crittanalisi...



Elementi di crittoanalisi: l'analisi delle frequenze

Sfruttare le vulnerabilità rispetto all'**analisi delle frequenze**, di doppie, coppie, triple, di lettere amiche e nemiche e in generale di rapporti fra lettere vicine.

Ad esempio sapendo che il testo è in italiano, è facile che l'ultima lettera di ciascuna parola sia una vocale.

- Si cercano i simboli più frequenti nel testo cifrato
- Si provano a sostituire con le lettere più frequenti in italiano
- Si cerca di vedere se si riesce a “intravedere” delle parti di parole
- Qualche tentativo può portare a parole improbabili, in tal caso si deve rivedere alcune scelte

Elementi di crittoanalisi: l'analisi delle frequenze

Esempio: **TRT QRDIAAR NTMNFZ N GLPRIN**

- Primo tentativo: inizio dalle lettere terminali di una parola e associando loro le vocali, in ordine di frequenza: **R = e, N = a , T = i, Z = o,**
- si ottiene **iei QeDIAe aiMNFZ a GLPeIa**
- Rivediamo alcune scelte (la prima parola non ha senso) **T = n,** (è la seconda consonante per frequenza: la prima è L che non sembra adatta), **R = o, Z = e,**
- Otteniamo **non QoDIAo anMaFe a GLPoIa**
- Ora introduciamo le consonanti più frequenti ancora mancanti (**l, r,t,s,c**) e reintroduciamo la **i.** Proviamo con **I = l, A = i, D = t, F = r, G = s , L=c:**

non Qotlio anMare a scPolia

Posso modificare ancora **D = g** e continuare...

•Lettera	•Occor-	•Lettera	•Occor-	•Lettera	•Occor-
	•renze		•renze		•renze
•A	•1	•H	•0	•Q	•1
•B	•0	•I	•2	•R	•4
•C	•0	•L	•1	•S	•0
•D	•1	•M	•1	•T	•3
•E	•0	•N	•4	•U	•0
•F	•1	•O	•0	•V	•0
•G	•1	•P	•1	•Z	•1

La sostituzione polialfabetica

- Un crittosistema per sostituzione polialfabetica non usa sempre lo stesso simbolo per la stessa lettera.
- Per ogni posizione di una lettera nel messaggio in chiaro viene usato un alfabeto diverso.
- Così si supera (parzialmente...) il problema della debolezza visto per i crittosistemi monoalfabetici.
- Infatti ha “meno” senso contare le frequenze di simboli, non essendoci più corrispondenza tra lettere in chiaro e simboli cifrati.

Il cifrario di Vigenère

Blaise de Vigenère pubblicò nel 1586 un trattato di cifre nel quale ne proponeva tra le altre una che ebbe grande fortuna e che è ricordata con il suo nome. Si tratta della più semplice cifra di sostituzione polialfabetica.



Il metodo si può considerare una generalizzazione del cifrario di Cesare; invece di spostare sempre dello stesso numero di posti la lettera da cifrare, questa viene spostata di un numero di posti variabile, determinato in base ad una **parola chiave**, da concordarsi tra mittente e destinatario, e da scriversi sotto il messaggio, carattere per carattere; la parola è detta verme, per il motivo che, essendo in genere molto più corta del messaggio, deve essere ripetuta molte volte sotto questo, come nel seguente esempio:

- Testo chiaro: **ARRIVANOIRINFORZI**
- Verme: **VERMEVERMEVERMEVE**
- Testo cifrato: **VVIUZVRFUVDRWAVUM**

$(P, C, K, \varepsilon, \delta)$

verrone lungo 2 $\Rightarrow P = \mathbb{Z}_{26} \times \mathbb{Z}_{26}$

verrone lungo 3: $P = \mathbb{Z}_{26} \times \mathbb{Z}_{26} \times \mathbb{Z}_{26}$

⋮
⋮
⋮

verrone lungo n :

$$\boxed{P = \mathbb{Z}_{26}^n}$$

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

$$A \times A = \{(a_1, a_2) \mid a_1 \in A, a_2 \in A\}$$

$$A^3 = A \times A \times A = \{(a_1, a_2, a_3) \mid a_1, a_2, a_3 \in A\}$$

⋮

$$A^M = \underbrace{A \times A \times \dots \times A}_{M \text{ volte}} = \{(a_1, \dots, a_M) \mid a_i \in A\}$$

$$C = \mathbb{Z}_{26}^M$$

$$K = \mathbb{Z}_{26}^m$$

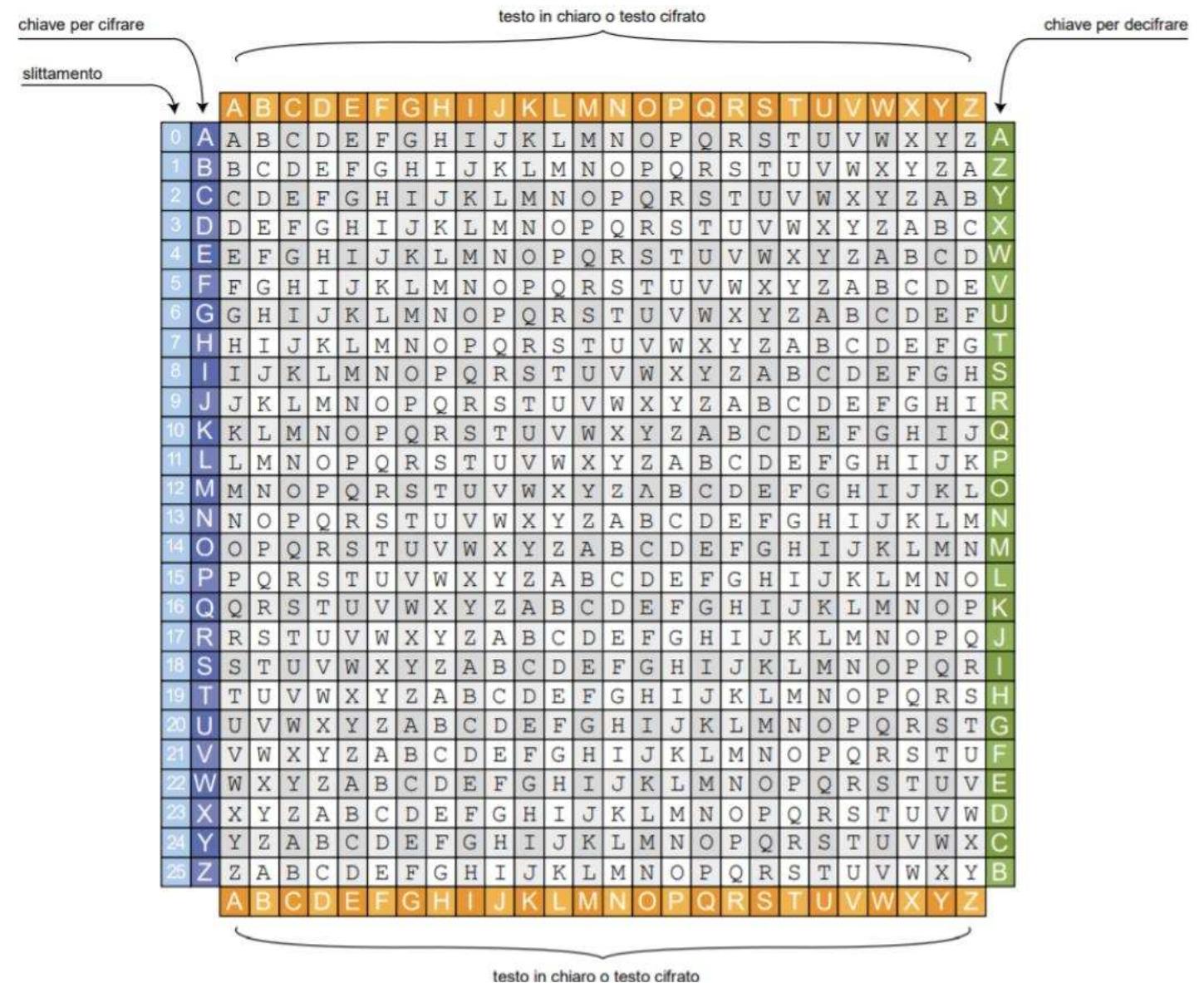
$$E : e_{(k_1, \dots, k_m)} (x_1, \dots, x_m) = (x_1 + k_1, \dots, x_m + k_m)$$

verme
blocco in chiuso
mod 26

$$D : d_{(k_1, \dots, k_m)} (y_1, \dots, y_m) = (y_1 - k_1, \dots, y_m - k_m)$$

verme
blocco C fatto

Il cifrario di Vigenère è un **crittosistema simmetrico**, che usa la stessa chiave sia per la cifratura sia per la decifratura.



Il cifrario di Vigenère: la sicurezza

Come si è detto questo cifrario ha goduto per tre secoli la fama di essere un cifrario inattaccabile; nel 1863 il colonnello prussiano **Friedrich Kasiski** pubblicò un primo metodo di decrittazione. In realtà anche se questa cifratura è molto più sicura di quella di Cesare, è anch'essa facilmente crackabile.

La debolezza del Vigenère sta nell'essere, di fatto, un insieme di n cifrari di Cesare, dove n è la lunghezza della chiave; se il crittoanalista riesce a determinare la lunghezza della chiave (nel nostro caso, n) la decrittazione diventa molto semplice.

Attacchi al cifrario di Vigenère



Attacchi: **Kasiski – Friedman**

- Obiettivo: determinare la lunghezza della parola chiave.
- Decrittare i messaggi implica considerazioni statistiche sulle caratteristiche di ciascuna lingua.
- Il lavoro di decrittazione consiste in successive induzioni e deduzioni in merito al presumibile significato.

Attacco di KASISKI (1863)

Porzioni ripetute di messaggio cifrate con la stessa porzione di chiave risultano in segmenti di testo cifrato identici.

PROV	ADIC	IFRA	TURA
HTML	HTML	HTML	HTML
WKAG	HWUN	PYDL	ANDL

Stessa lettera viene cifrata in modo diverso nelle sue varie occorrenze (**lettera R**).

Se due lettere sono poste ad una distanza pari alla lunghezza della chiave vengano cifrate nello stesso modo (**lettera A**).

Attacco di KASISKI (1863)

- Dobbiamo spostare la nostra attenzione non su lettere ma su sequenze di lettere uguali.
- Si individuano tutte le sequenze ripetute nel testo cifrato.
- Il numero di lettere comprese tra gli intervalli dei poligrammi è multiplo del numero di lettere della chiave
- Il massimo comune divisore tra le distanze tra sequenze identiche è la lunghezza della chiave.

EVFTSIX**RES**CEKHF

XVVGHIBSDZ**SIC**YO

XVVOPLI**RES**IMTNL

SICIN**XVV**ISUDIMT

XVVMIMFIIGVMNFL

Sequenze	Distanze	Scomposizione
RES	30	7×5
SIC	20	4×5
XVV	10, 15	$2 \times 5, 3 \times 5$

→ MCD=5

Attacco di KASISKI (1863)

- Dobbiamo spostare la nostra attenzione non su lettere ma su sequenze di lettere uguali.
- Si individuano tutte le sequenze ripetute nel testo cifrato.
- Il numero di lettere comprese tra gli intervalli dei poligrammi è multiplo del numero di lettere della chiave
- Il massimo comune divisore tra le distanze tra sequenze identiche è la lunghezza della chiave.

EVFTS	IXRES	CEKHF
XVVGH	IBSDZ	SICYO
XVVOP	LIRES	IMTNL
SICIN	XVVIS	UDIMT
XVVMI	MFIIG	VMNFL

Sequenze	Distanze	Scomposizione
RES	30	7×5
SIC	20	4×5
XVV	10, 15	$2 \times 5, 3 \times 5$

→ MCD=5

Attacco di KASISKI (1863)

Riduzione al codice di Cesare

- Determinazione della lunghezza della parola chiave equivale alla determinazione del numero degli alfabeti.
- Il messaggio si riduce a messaggi intercalati, tutti cifrati con un codice di Cesare ed è allora molto facile completarne la decifratura.
- Le risultanti porzioni monoalfabetiche possono essere risolte individualmente.

Considerazioni

- Segmenti ripetuti di testo cifrato di lunghezza 4 o maggiore sono più utili, poiché le ripetizioni accidentali sono meno probabili.
- Il calcolo del MCD deve essere fatto considerando solo le sequenze sospette.
- È possibile che la lunghezza non sia esattamente il MCD ma un suo multiplo.

Mettiamoci alla prova...

DAZFI SFSPA VQLSN PXYSZ WXALC DAFGQ UISMT PHZGA MKTTF TCCFX
KFCRG GLPFE TZMMM ZOZDE ADWVZ WMWKV GQSOH QSVHP WFKLS LEASE
PWHMJ EGKPU RVSXJ XVBWV POSDE TEQTX OBZIK WCXLW NUOVJ MJCLL
OEOF A ZENVM JILOW ZEKAZ EJAQD ILSWW ESGUG KTZGQ ZVRMN WTQSE
OTKTK PBSTA MQVER MJEGL JQRTL GFJYG SPTZP GTACM OECBX SESCI
YGUFP KVILL TWDKS ZODFW FWEAA PQTFS TQIRG MPMEL RYELH QSVWB
AWMOS DELHM UZGPG YEKZU KWTAM ZJMLS EVJQT GLAWV OVvxH KWQIL
IEUYS ZWXAH HUSZO GMUZQ CIMVZ UVWIF JJHPW VXFSE TZEDF

Mettiamoci alla prova...

DAZFI SFSPA VQLSN PXYSZ WXALC DAFGQ UISMT PHZGA MKTTF TCCFX
KFCRG GLPFE TZMMM ZOZDE ADWVZ WMWKV GQSOH QSVHP WFKLS LEASE
PWHMJ EGKPU RVSXJ XVBWV POSDE TEQTX OBZIK WCXLW NUOVJ MJCLL
OEOF A ZENVM JILOW ZEKAZ EJAQD ILSWW ESGUG KTZGQ ZVRMN WTQSE
OTKTK PBSTA MQVER MJEGL JQRTL GFJYG SPTZP GTACM OECBX SESCI
YGUFP KVILL TWDKS ZODFW FWEAA PQTFS TQIRG MPMEL RYELH QSVWB
AWMOS DELHM UZGPG YEKZU KWTAM ZJMLS EVJQT GLAWV OVvxH KWQIL
IEUYS ZWXAH HUSZO GMUZQ CIMVZ UVWIF JJHPW VXFSE TZEDF

Mettiamoci alla prova...

DAZFI SFSPA VQLSN PXYSZ WXALC DAFGQ UISMT PHZGA MKTTF TCCFX
KFCRG GLPFE TZMMM ZOZDE ADWVZ WMWKV GQSOH QSVHP WFKLS LEASE
PWHMJ EGKPU RVSXJ XVBWV POSDE TEQTX OBZIK WCXLW NUOVJ MJCLL
OEOF A ZENVM JILOW ZEKAZ EJAQD ILSWW ESGUG KTZGQ ZVRMN WTQSE
OTKTK PBSTA MQVER MJEGL JQRTL GFJYG SPTZP GTACM OECBX SESCI
YGUFP KVILL TWDKS ZODFW FWEAA PQTFS TQIRG MPMEL RYELH QSWB
AWMOS DELHM UZGPG YEKZU KWTAM ZJMLS EVJQT GLAWV OVvxH KWQIL
IEUYS ZWXAH HUSZO GMUZQ CIMVZ UVWIF JJHPW VXFSE TZEDF

Mettiamoci alla prova...

DAZFI SFSPA VQLSN PXYSZ WXALC DAFGQ UISMT PHZGA MKTTF TCCFX
KFCRG GLPFE TZMMM ZOZDE ADWVZ WMWKV GQSOH QSVHP WFKLS LEASE
PWHMJ EGKPU RVSXJ XVBWV POSDE TEQTX OBZIK WCXLW NUOVJ MJCLL
OEOF A ZENVM JILOW ZEKAZ EJAQD ILSWW ESGUG KTZGQ ZVRMN WTQSE
OTKTK PBSTA MQVER MJEGL JQRTL GFJYG SPTZP GTACM OECBX SESCI
YGUFP KVILL TWDKS ZODFW FWEAA PQTFS TQIRG MPMEL RYELH QSWB
AWMOS DELHM UZGPG YEKZU KWTAM ZJMLS EVJQT GLAWV OVvxH KWQIL
IEUYS ZWXAH HUSZO GMUZQ CIMVZ UVWIF JJHPW VXFSE TZEDF

Mettiamoci alla prova...

DAZFI SFSPA VQLSN PXYSZ WXALC DAFGQ UISMT PHZGA MKTTF TCCFX
KFCRG GLPFE TZMMM ZOZDE ADWVZ WMWKV GQSOH QSVHP WFKLS LEASE
PWHMJ EGKPU RVSXJ XVBWV POSDE TEQTX OBZIK WCXLW NUOVJ MJCLL
OEOF A ZENVM JILOW ZEKAZ EJAQD ILSWW ESGUG KTZGQ ZVRMN WTQSE
OTKTK PBS TA MQVER MJEGL JQRTL GFJYG SPTZP GTACM OECBX SESCI
YGUFP KVILL TWDKS ZODFW FWEAA PQTFS TQIRG MPME L RYELH QSVWB
AWMOS DELHM UZGPG YEKZU KW TAM ZJMLS EVJQT GLAWV OVvxH KWQIL
IEUYS ZWXAH HUSZO GMUZQ CIMVZ UVWIF JJHPW VXFSE TZEDF

Mettiamoci alla prova...

Stringa	Posizioni	Distanza
YSZWXA	17	353
HQSV	84	294
MJEG	103	215
OSDE	121	303
ETZ	59	389
HPW	88	382
AZE	154	168
TAM	208	322
SZO	264	362
ELH	292	306
MUZ	309	366

Mettiamoci alla prova...

Stringa	Posizioni	Distanza
YSZWXA	17	$2^4 \times 3 \times 7$
HQSV	84	$2 \times 3 \times 5 \times 7$
MJEG	103	$2^4 \times 7$
OSDE	121	$2 \times 3 \times 5 \times 7$
ETZ	59	$2 \times 3 \times 5 \times 11$
HPW	88	$2 \times 3 \times 7^2$
AZE	154	2×7
TAM	208	$2 \times 3 \times 19$
SZO	264	2×7^2
ELH	292	2×7
MUZ	309	3×19

I fattori più comuni delle distanza tra le sequenze ripetute sono **2, 3, 7, 14...**

Escluso 2, **14** è quello che compare più spesso.

Mettiamoci alla prova...

DAZFISFSPAVQLS NPXYSZWXALCDAF GQUI SMTPHZGAMK TTFTCCFXKFCRGG
LPFETZMMMZOZDE ADWVZWMWKVGQSO HQSVHPWFKL SLEA SEPWHMJEGLPURV
SXJXVBWVPOSDET EQTXOBZIKWCXLW NUOVJMJC LLOEOF AZENVMJILOWZEK
AZEJAQDILSWWES GUGKTZGQZVRMNW TQSEOTKTPBSTA MQVERMJEGLJQRT
LGFJYGSPTZPGTA CMOECBXSESCIYG UFPKVILLTWDKSZ ODFWFWEAAPQTFS
TQIRGMPMELRYEL HQSVWBAWMOSDEL HMUZGPGYEKZUKW TAMZJMLSEVJQTG
LAWVOVVXHKWQIL IEUYSZWXAHHUSZ OGMUZQCIMVZUVW IFJJHPWVXFSETZ
EDF

INDICE DI CONCERNZA

CALCOLO DELLE PROBABILITÀ

- Definiamo P come la probabilità che presa una coppia di simboli in un **testo in chiaro** questi siano uguali.

$$P = \sum_{i=1}^{26} p_i^2 = 0,075$$

Probabilità relativa alla lettera i-esima
nella lingua italiana

- Definiamo Q come la probabilità che preso una coppia di simboli in un **testo casuale** questi siano uguali.

$$Q = \sum_{i=1}^{26} \left(\frac{1}{26}\right)^2 = 0,038$$

Attacco di
FRIEDMAN
(1925)

Friedman trovò un nuovo metodo più efficiente per risalire alla lunghezza della chiave L , che si basa sulla probabilità che prese due lettere nel testo cifrato queste siano uguali.

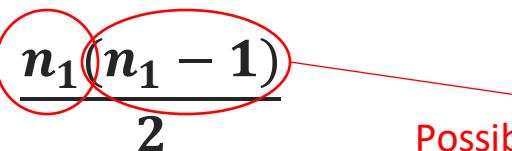
Si calcola L in funzione di tale probabilità denominata **indice di coincidenza**.

Consideriamo una sequenza di n lettere: n_1 è il numero di occorrenze della lettera A ... n_{26} numero di occorrenze della lettera Z.

- Numero di coppie formate dalla lettera A:

$$\frac{n_1(n_1 - 1)}{2}$$

Possibilità che la prima lettera sia A Possibilità che la seconda lettera sia A



- Calcoliamo il numero delle coppie formate dalla stessa lettera e indichiamolo con Z :

$$Z = \sum_{i=1}^{26} \frac{n_i(n_i - 1)}{2}$$

Attacco di FRIEDMAN (1925)

INDICE DI COINCIDENZA

- Abbiamo calcolato il numero dei casi favorevoli.
- Il numero di coppie possibili è $\frac{n(n-1)}{2}$.



La probabilità di prendere una coppia uguale in un messaggio cifrato

$$I = \frac{\sum_{i=1}^{26} \frac{n_i(n_i - 1)}{2}}{\frac{n(n - 1)}{2}}$$

Attacco di
FRIEDMAN
(1925)

ESEMPIO (1)

Frasy sidhx lakahg

Hjhq waapqq svsj a

Adagsiu qyw isbajl

Ajhajsus cqywoeb

ahjkabsswqomjab



L = 1

$$I(c_0, c_1, \dots, c_n) = \begin{cases} 0,075 & \text{se } L = 1 \\ 0,038 & \text{se } L \neq 1 \end{cases}$$

L = 2

$$I(c_1, c_3, \dots) = I(c_0, c_2, \dots) = \begin{cases} 0,075 & \text{se } L = 2 \\ 0,038 & \text{se } L \neq 2 \end{cases}$$

Attacco di
FRIEDMAN
(1925)

ESEMPIO (2)

- $L = 1?$ $I(c_0, c_1, \dots, c_n) = 0,045$
- $L = 2?$ $I(c_0, c_2, \dots) = 0,0463$
 $I(c_1, c_3, \dots) = 0,0468$
- $L = 3?$ $I(c_0, c_3, \dots) = 0,0431$
 $I(c_1, c_4, \dots) = 0,0459$
 $I(c_2, c_5, \dots) = 0,0456$
- $L = 4?$ $I(c_0, c_4, \dots) = 0,0421$
 $I(c_1, c_5, \dots) = 0,0492$
 $I(c_2, c_6, \dots) = 0,0437$
 $I(c_3, c_7, \dots) = 0,0444$
- $L = 5?$ $I(c_0, c_5, \dots) = 0,07221$
 $I(c_1, c_6, \dots) = 0,0715$
 $I(c_2, c_7, \dots) = 0,0810$
 $I(c_3, c_8, \dots) = 0,0684$
 $I(c_4, c_9, \dots) = 0,0759$

Attacco di
FRIEDMAN
(1925)

Tutti vicini a 0,075,
allora $L = 5!!$

Mettiamoci alla prova...

DAZFISFSPAVQLS NPXYSZWXALCDAF GQUI SMTPHZGAMK TTFTCCFXKFCRGG
LPFETZMMMZODZ DE ADWVZWMWKVGQSO HQSVHPWFKLSLEA SEPWHMJEGLPURV
SXJXVBWVPOSDET EQTXOBZIKWCXLW NUOVJMJCLOEOF AZENVMJILOWZEK
AZEJAQDILSWWES GUGKTZGQZVRMNW TQSEOTKTPBSTA MQVERMJEGLJQRT
LGFJYGSPTZPGTA CMOECBXSESCIYG UFPKVILLTWDKSZ ODFWFWEAAPQTFS
TQIRGMPMELRYEL HQSVWBAWMOSDEL HMUZGPGYEKZUKW TAMZJMLSEVJQTG
LAWVOVVXHKWQIL IEUYSZXAHUSZ OGMUZQCIMVZUVW IFJJHPWVXFSETZ
EDF

Indice di coincidenza (medio) : 0,064378

Mettiamoci alla prova...

Esaminando le sequenze di stessa posizione...

Chiave: **AMBROISETHOMAS**

Testo decifrato:

DO YOU KNOW THE LAND WHERE THE ORANGE TREE BLOSSOMS?
THE COUNTRY OF GOLDEN FRUITS AND MARVELOUS ROSES,
WHERE THE BREEZE IS SOFTER AND BIRDS LIGHTER,

WHERE BEES GATHER POLLEN IN EVERY SEASON,
AND WHERE SHINES AND SMILES, LIKE A GIFT FROM GOD,
AN ETERNAL SPRINGTIME UNDER AN EVER-BLUE SKY!

ALAS! BUT I CANNOT FOLLOW YOU
TO THAT HAPPY SHORE FROM WHICH FATE HAS EXILED ME!
THERE! IT IS THERE THAT I SHOULD LIKE TO LIVE,
TO LOVE, TO LOVE, AND TO DIE!

IT IS THERE THAT I SHOULD LIKE TO LIVE, IT IS THERE, YES, THERE!

Il cifrario di Vigenère: la sicurezza

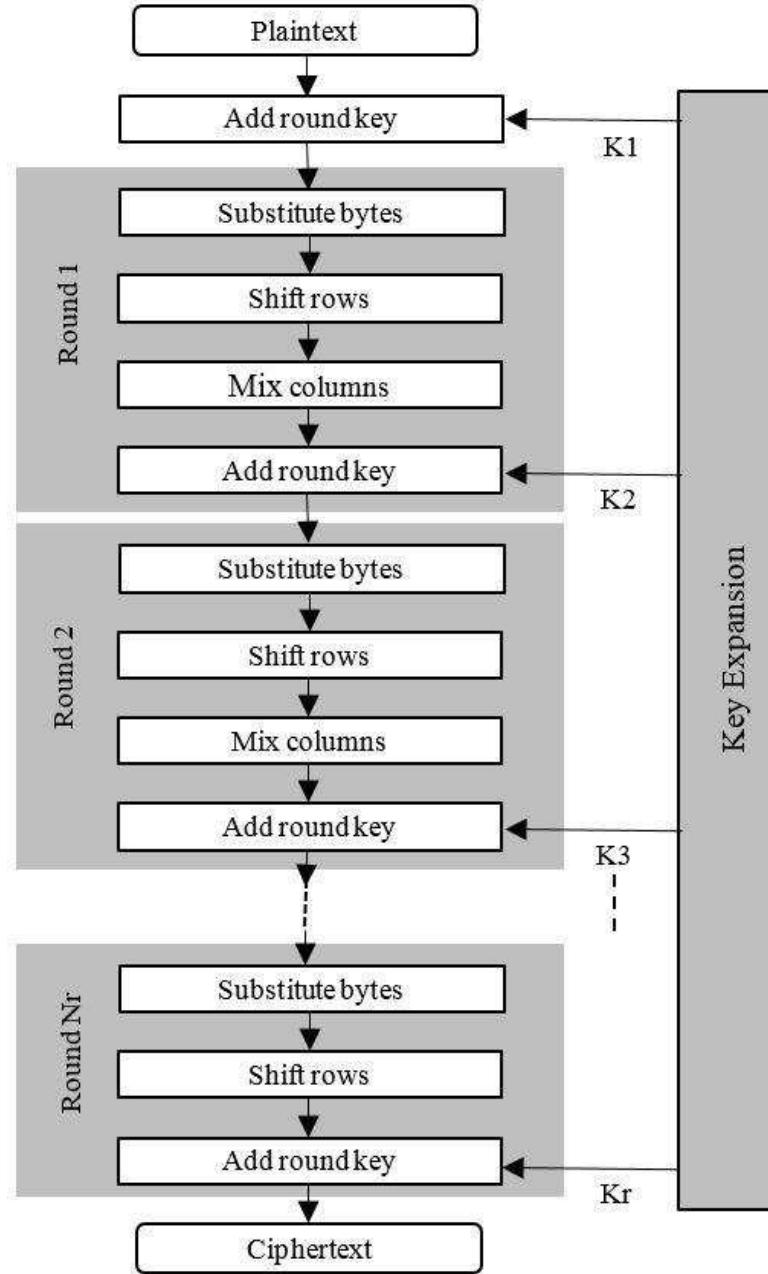
Per evitare questo problema, una soluzione consiste nell'usare una chiave di dimensioni simili a quella del testo per rendere impossibile uno studio statistico del testo criptato.

Questo tipo di sistema di cifratura è detto **SISTEMA A CHIAVE USA E BUTTA**.

Il problema di questo metodo è la lunghezza della chiave di cifratura (più il testo da criptare è lungo, più la chiave deve essere voluminosa), che impedisce la sua memorizzazione e include una probabilità d'errore nella chiave maggiore (un solo errore rende il testo indecifrabile, ecc.).

AES (Advanced Encryption Standard)

MARCO
R Moca



$$(P_1, C_1, K_1, \mathcal{E}_1, D_1) = \text{CRITOSIST. 1}$$

$$\mathcal{E}_1 = \{ e_k : P_1 \rightarrow C_1 \mid k \in K_1 \}$$

$$(P_2, C_2, K_2, \mathcal{E}_2, D_2) = \text{CRITOSIST. 2}$$

CRITOSIST. 3 : combinez. des critosist 1 et poi critosist 2.

"

$$(P_3, C_3, K_3, \mathcal{E}_3, D_3)$$

$$f : A \rightarrow B$$

$$g : B \rightarrow C$$

$$A \xrightarrow{f} B \xrightarrow{g} C$$

$g \circ f$

$$e_{K_1} : P_1 \rightarrow C_1$$

cifr. critt. 1

$$e_{K_2} : P_2 \rightarrow C_2$$

cifr. critt. 2

\rightarrow VORDEI FARE

$$e_{K_2} \circ e_{K_1}$$

$$P_1 \xrightarrow{e_{K_1}} C_1 \xrightarrow{e_{K_2}}$$

\downarrow
PER POTERLO FAR E:

$$C_1 = P_2$$

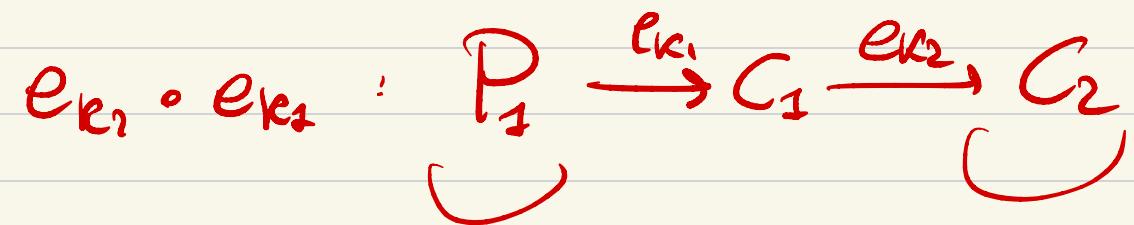
$CRIT. 1 = (P_1, C_1, K_1, E_1, D_1)$

$CRIT. 2 = (C_1, A_1, K_2, E_2, D_2)$

$CRIT. 3 = (P_1, C_2, K_1 \times K_2, E_3, D_3) = CRIT. 1 \times CRIT. 2$

$$e_{K_1} \in E_1$$

$$e_{K_2} \in E_2$$



$$\rightarrow E_3 = \left\{ \underbrace{e_{K_2} \circ e_{K_1}}_{e_{(K_1, K_2)}} \mid (K_1, K_2) \in K_1 \times K_2 \right\}$$

$$D_3 = \{d_{k_1} \circ d_{k_2} \mid (k_1, k_2) \in K_1 \times K_2\}$$

$$d_{k_2} \circ d_{k_1} : C_2 \xrightarrow{d_{k_2}} C_1 \xrightarrow{d_{k_1}} P_1$$

$$\text{CRITI}_1 = C_{\text{core}} = \text{CRITL}_2 = (\mathbb{Z}_{21}, \mathbb{Z}_{21}, \mathbb{Z}_{21}, E_1, D_1)$$

$$e_{k_1} : \mathbb{Z}_{21} \rightarrow \mathbb{Z}_{21}$$

$$a \mapsto a + k_1 \bmod 21$$

$$d_{k_1} : \mathbb{Z}_{21} \rightarrow \mathbb{Z}_2$$

$$b \mapsto b - k_1 \pmod{21}$$

$$\text{Cesare} \times \text{Cesare} = (\mathbb{Z}_{21}, \mathbb{Z}_{21}, \mathbb{Z}_{21} \times \mathbb{Z}_{21}, E_3, D_3)$$

$$e_k \in E_3 \quad , \quad e_k = e_{k_2} \circ e_{k_1} : \mathbb{Z}_{21} \xrightarrow{e_{k_1}} \mathbb{Z}_{21} \xrightarrow{e_{k_2}} \mathbb{Z}_{21}$$

$$k = (k_1, k_2)$$

$\begin{smallmatrix} \cap \\ \mathbb{Z}_{21} \end{smallmatrix} \quad \begin{smallmatrix} \cap \\ \mathbb{Z}_{21} \end{smallmatrix}$

$$a \mapsto a + k_1 \pmod{21} \mapsto (a + k_1) + k_2 \pmod{21}$$

$$a \mapsto a + (k_1 + k_2) \pmod{21}$$

$$d_k = d_{k_1} \circ d_{k_2} : \mathbb{Z}_{21} \longrightarrow \mathbb{Z}_{21}$$

$$b \mapsto b - (k_1 + k_2) \pmod{21}$$

S_1, S_2 due crittosistemi $\rightarrow S_1 \times S_2$ sì forte!

Proprietà: $S_1 \times S_2 \neq S_2 \times S_1$ $\mathbb{Z}_{21} \times \mathbb{Z}_{26} \neq \mathbb{Z}_{26} \times \mathbb{Z}_{21}$

$$S_1 \times (S_2 \times S_3) = (S_1 \times S_2) \times S_3$$

Caso particolare: $S_1 = S_2 = S$ - - - $S_1 \times S_2 = S \times S = S^2$

$$\underbrace{S \times S \times \dots \times S}_{n \text{ volte}} = S^n$$

Definizione: Si dice che un critosistema S è IDEMPOTENTE

$$\text{se } S^2 = S$$

→ Cesare, Vigenère, affine, sostituzione, permutazione sono idempotenti

Come posso trovare un critosistema S tale che $S^2 \neq S$

→ Provo con un $S = S_1 \times S_2$

$$S^2 \neq S ?$$

$$(S_1 \times S_2)^2 \neq S_1 \times S_2$$

THM: $S = S_1 \times S_2$.

Se vale che : ① $S_1^2 = S_1$ e $S_2^2 = S_2$

② $S_1 \times S_2 = S_2 \times S_1$

$$\Rightarrow (S_1 \times S_2)^2 = S_1 \times S_2$$

↪ Il prodotto di 2 crtl. idempotenti che commutano
è ancora idempotente.

$$(S_1 \times S_2)^2 = (S_1 \times S_2) \times (S_1 \times S_2)$$



$$\stackrel{(2)}{=} (S_1 \times S_2) \times (S_2 \times S_1)$$

$$= S_1 \times (S_2 \times S_2) \times S_1$$

$$\stackrel{(1)}{=} S_1 \times S_2 \times S_1$$

$$\stackrel{(2)}{=} S_1 \times S_1 \times S_2$$

$$\stackrel{(1)}{=} S_1 \times S_2$$

S_1 = Vigenere

S_2 = permutazione

} non commutano.

Nella realtà: $S_1 = \text{Vigenere}$

$S_2 = \text{sostituzione}$

$S_3 = \text{permutozione}$

$\left. \begin{array}{l} S_1 \\ S_2 \\ S_3 \end{array} \right\} S = S_1 \times S_2 \times S_3$

↳ Considero il critosistema $S^M = (S_1 \times S_2 \times S_3)^M$

↳ SPN

(substitution - permutation network)

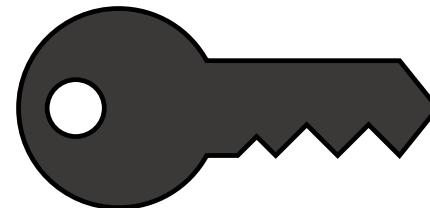


Crittografia a chiave pubblica

Il problema fondamentale

Tutto funziona bene ma...

ALICE e BOB devono condividere una chiave segreta!



COME SCAMBIARSI LA CHIAVE A DISTANZA?

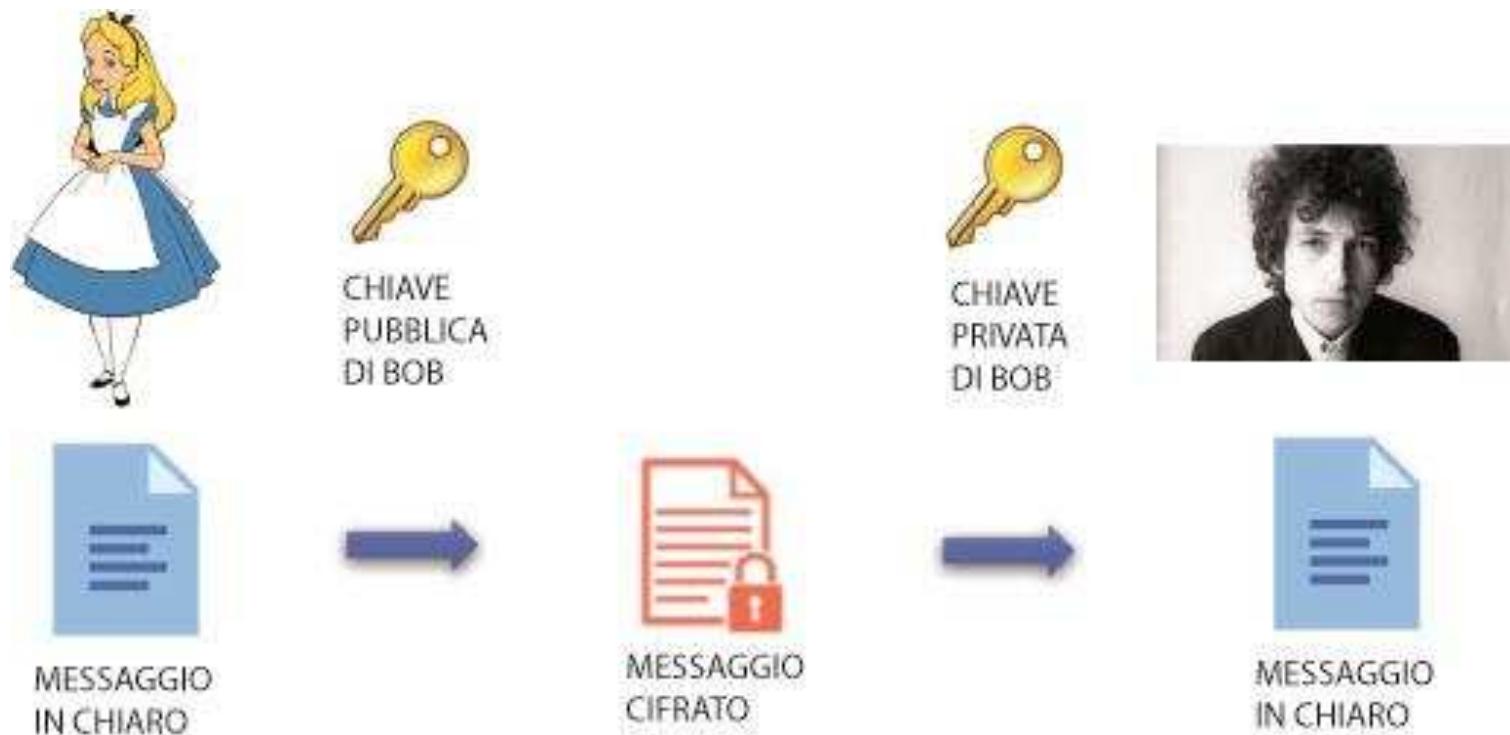
La crittografia di Whatsapp



- I messaggi che ALICE e BOB si scambiano **NON** sono decifrabili neanche da WHATSAPP!
- Ogni utente deve poter comunicare con ogni altro utente.
- Gli utenti sono già più di un miliardo.

Soluzione: la crittografia ASIMMETRICA (a chiave pubblica)

- Metodo di cifratura:
ACCESSIBILE A TUTTI
- Metodo di decifratura:
NOTO SOLO AL DESTINATARIO



IMPOSSIBILE TORNARE INDIETRO

La crittografia a chiave pubblica si basa sull'impossibilità da parte di un attaccante di ricostruire la chiave privata di BOB, conoscendo la sua chiave pubblica.

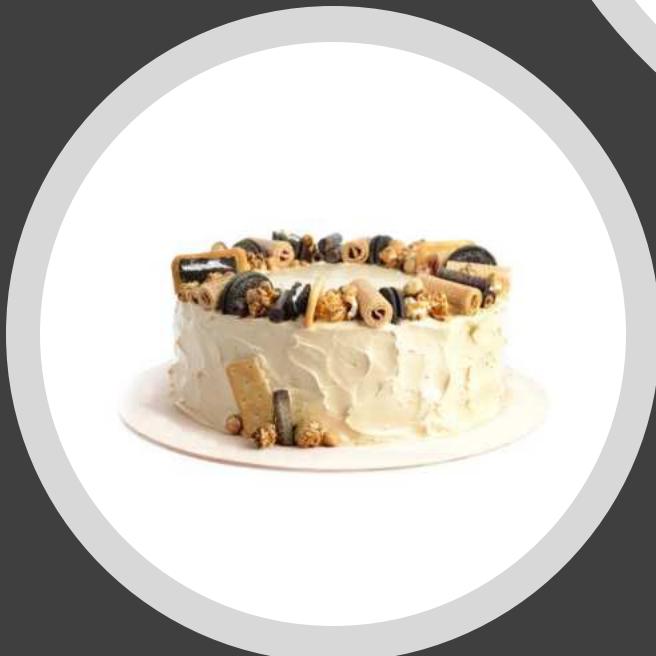
Cosa si intende per **IMPOSSIBILE**?

COMPUTAZIONALMENTE
impossibile, ovvero impossibile in tempi utili!



Esempi di procedimenti non invertibili

- Conoscendo il numero di telefono di una persona, trovare il suo nome utilizzando l'elenco telefonico
- Risalire da un dolce preparato alla sua ricetta
- Qual è il più importante e famoso segreto industriale del mondo?



Coca-Cola

TRAPPOLE MATEMATICHE:

procedimento
matematico che sia
facile da eseguire, ma che
sia troppo dispendioso da
invertire

ELEVAMENTO A POTENZA
MODULARE: **facile** da
eseguire

$$(A, B) \rightarrow A^B \bmod N$$

OPERAZIONE INVERSA:
difficile da eseguire

$$(A, A^B) \rightarrow B \bmod N$$

$$B = \log_A A^B$$

**PROBLEMA DEL
LOGARITMO DISCRETO**

Perché
invertire la
potenza
modulare è
difficile?

$$\log_5 71 \bmod 103 ?$$

Calcolo la sequenza delle potenze di
 $A = 5$ modulo $p = 103$

5, 25, 22, 7, 35, 72, 51, 49, 39, 92, 48,
34, 67, 26, 27, 32, 57, 79, 86, 18, 90,
38, 87, 23, 12, 60, 94, 58, 84, 8, 40, 97,
73, 56, 74, 61, 99, 83, 3, 15, 75, 66, 21,
2, 10, 50, 44, 14, 70, 41, 102, 98, 78,
81, 96, 68, 31, 52, 54, 64, 11, 55, 69,
36, 77, 76, **71**, 46, 24, 17, 85, 13, 65,
16, 80, 91, 43, 9, 45, 19, 95, 63, 6, 30,
47, 29, 42, 4, 20, 100, 88, 28, 37, 82,
101, 93, 53, 59, 89, 33, 62, 1

Alice e Bob vogliono condividere una chiave segreta

PROTOCOLLO DI DIFFIE-HELLMAN



- Sceglie un numero random A
- Sceglie un numero random B
- Calcola A^B
- Pubblica A^B e A
- Tiene segreto B
- Sceglie un numero random C
- Calcola A^C
- Pubblica A^C

Alice e Bob conoscono $A^{BC} = (A^C)^B = (A^B)^C$

Un eventuale **hacker** può conoscere A , A^B , A^C ma non riesce a calcolare A^{BC} !!

$$\begin{matrix} A^B \\ A^C \end{matrix} \quad \left. \begin{matrix} \\ \downarrow \end{matrix} \right\} \rightarrow A^{B+C}$$

$$A^B \cdot A^C = A^{B+C}$$

ALTRA TRAPPOLA MATEMATICA: PROBLEMA DELLA FATTORIZZAZIONE

Siano p, q due numeri primi:

- Calcolare $N = pq$ è **facile**
- Dato $N = pq$, è **difficile** risalire a p, q



R. Rivest
A. Shamir
L. Adleman
(MIT)



Realizzazione pratica di un sistema crittografico basato sulla difficoltà di fattorizzare il prodotto di due numeri primi grandi



CRITTOISTEMA RSA

IL CRITTOSSISTEMA RSA



- Sceglie due numeri primi p, q ;
- Calcola $N = pq$;
- Sceglie un numero e invertibile
 $\mod(p - 1)(q - 1)$
- Calcola
 $d = e^{-1} \mod(p - 1)(q - 1)$
- CHIAVE PUBBLICA (N, e)
- CHIAVE PRIVATA (p, q, d)
- Decodifica di C :
 $C^d \mod(N)$

- Codifica C di un messaggio M :
 $C = M^e \mod(N)$

La decodifica funziona perché,
grazie al Teorema di Eulero, vale
che

$$C^d = (M^e)^d = M \mod(N)$$

Il crittosistema RSA è sicuro?

Nel loro articolo Rivest, Shamir e Adleman proposero a tutti di fattorizzare il numero:

RSA129

114381625757888867669235779976146612010218296721242
362562561842935706935245733897830597123563958705058
989075147599290026879543541

PREVISIONE: migliaia di anni per trovare la soluzione

SOLUZIONE: nel 1994, grazie a 1600 computers connessi a internet, circa 600 volontari

Possibile solo grazie a [miglioramenti teorici matematici!](#)

Chiavi deboli

- Esistono algoritmi di fattorizzazione che risultano veloci se p e q hanno determinate proprietà
- Un esempio di chiave debole è quello in cui p e q sono relativamente vicini
- Un altro esempio di chiave debole è quella in cui $p - 1$ o $q - 1$ si fattorizzano in tanti fattori primi piccoli
- Per questo si tende a scegliere $p = 2p_1 + 1$ e $q = 2q_1 + 1$ con p_1 e q_1 primi
- Pare che una percentuale rilevante delle chiavi RSA sia debole: su 6,4 milioni di chiavi RSA, 12934 sono vulnerabili (**0.2%**)!

Lenstra - Hughes - Augier - Bos - Kleinjung - Watcher (2012)



$$M = pq \quad , \quad p, q \text{ primi} \quad , \quad p, q \sim 2^{2024}, 2^{2048}$$

for $i := 1, \dots$

Calcolo $M + i^2$

Controlla se $M + i^2$ è un quadrato perfetto $\rightarrow M + i^2 = s^2$?

Se Trouvo i tale che $M + i^2 = s^2$ ho un'idea!

$$\underbrace{M}_{\substack{\text{pq} \\ \text{if}}} = s^2 - i^2 = \underbrace{(s-i)}_p \underbrace{(s+i)}_q$$

$$\begin{cases} p = s-i \\ q = s+i \end{cases} \Rightarrow 2^a \text{ equez} - 1^a \text{ equez} : q-p = (s+i) - (s-i)$$
$$q-p = 2i$$
$$i = \frac{q-p}{2}$$

Per non essere ottaccibili

p e q devono essere
molto distanti

La crittografia...al contrario: la FIRMA DIGITALE



Fino ad ora **Alice** può mandare un messaggio a **Bob** senza che un **hacker** possa capire cosa si siano scritti.

Come fa **Bob** ad essere sicuro che sia stata proprio **Alice** a mandare quel messaggio?

Ad **Alice** serve poter **FIRMARE** il messaggio che manda a **Bob**!

La crittografia...al contrario: la FIRMA DIGITALE



Alice ha una sua coppia di chiavi pubblica e privata per la firma digitale (**Pubbl**, **Priv**)

Le due chiavi sono dei **PROCEDIMENTI** che sono l'uno l'inverso dell'altro.

Dalla chiave pubblica **Pubbl** NON è possibile risalire alla chiave privata **Priv**.

$$\text{Pubbl}(\text{Priv}(X))=X \quad \text{Priv}(\text{Pubbl}(X))=X$$

La crittografia...al contrario: la FIRMA DIGITALE



- Prende il documento M che vuole firmare (numero)
- Applica la sua chiave privata **Priv** a M
- Ottiene M'
- Manda M e F a **Bob**
- Riceve M e F da **Alice**
- Applica chiave pubblica **Pubbl** di **Alice** a F
- Ottiene C
- Verifica se M=C

$$\text{Pubbl}(\text{Priv}(X))=X \quad \text{Priv}(\text{Pubbl}(X))=X$$

Esigenza pratica? Matematica più astratta!

- PROBLEMA: trattamento dei numeri enormi che servono per garantire sicurezza in dispositivi che non sono PC (es.: dispositivi medici, passaporto elettronico).
- SOLUZIONE: funzioni trappola matematicamente più complesse.
- NUOVE TRAPPOLE: moltiplicare/sommare oggetti diversi, non necessariamente numeri.

Di cosa abbiamo bisogno...

- Un insieme G
- Un'operazione \star tra gli elementi di G con determinate proprietà

$$G = \mathbb{N}$$
$$\star : a \star b = 2^a + 3^b$$

Problema del logaritmo discreto in (G, \star) :



Dati $g, g^a \in G$, trovare a

$$g \star g \star \dots \star g = b$$

$\underbrace{\star}_{c \text{ volte}}$

Strutture algebriche

(G, \star) si dice **GRUPPO** se l'operazione \star

- **interna:** per ogni $g_1, g_2 \in G$, $g_1 \star g_2 \in G$
- **associativa:** per ogni $g_1, g_2, g_3 \in G$, $(g_1 \star g_2) \star g_3 = g_1 \star (g_2 \star g_3)$
- **esiste identità (elemento neutro):** esiste $1_G \in G$ tale che per ogni $g \in G$, $g \star 1_G = 1_G \star g = g$
- **esistono gli inversi:** per ogni $g_1 \in G$, esiste $g_2 \in G$ tale che
$$g_1 \star g_2 = g_2 \star g_1 = 1_G$$

Proprietà commutativa → GRUPPO COMMUTATIVO

1) $G = \mathbb{R}$, $a * b = a + b + 2$, $a, b \in \mathbb{R}$

2) $G = \mathbb{R} \setminus \{0\}$, $a * b = |ab|$

3) $G = \{8a + 14b \mid a, b \in \mathbb{Z}\}$, $a * b = a + b$

4) $G = \{\text{ensemble symétrique M-diagonale régulière}\}, a * b = a \circ b$

1) $G = \mathbb{R}$, $a * b = a + b + 2$

ASSOCIAZIONE: $a, b, c \in \mathbb{R}$, $(a * b) * c \neq a * (b * c)$

$$\begin{aligned} & (a + b + 2) * c && a * (b + c + 2) \\ & (a + b + 2) + c + 2 && a + (b + c + 2) + 2 \\ & a + b + c + 4 &\equiv& a + b + c + 4 \end{aligned}$$

IDENTITÀ: $\exists q = x$, $a * x = a \rightarrow a + x + 2 = a$

$$x = a - a - 2$$

$$x = -2 \in \mathbb{R} = G$$

INVERSI: Prendo $a \in G$ voglio trovare $x \in G$ tale che

$$\frac{a * x}{\downarrow} = x * a = -2$$

• $a * x = -2$

$$a + x + 2 = -2 \rightarrow x = -a - 2 - 2 = -a - 4 \in \mathbb{R}$$

• $x * a = -2 \rightarrow x + a + 2 = -2 \rightarrow x = -a - 4 \in \mathbb{R}$

Ese: $a = 7$, inverso di $7 = -11$

Verifico: $7 * (-11) = 7 + (-11) + 2 = -2 \checkmark$

$$2) G = \mathbb{R} \setminus \{0\}, \quad a * b = |ab|$$

$$\left. \begin{array}{l} a = 3 \\ b = -2 \\ c = 2 \end{array} \right\} \quad \begin{array}{c} (a * b) * c \neq a * (b * c) \\ \downarrow \\ ((|3| \cdot (-2)) * 2 \end{array} \quad \begin{array}{c} \hookrightarrow \\ 3 * (|-2| \cdot 2) \\ 3 * (4) \\ \downarrow \\ (-6) * 2 \\ \downarrow \\ |-6| \cdot 2 \\ \downarrow \\ 12 \end{array}$$

$$1_G = x \quad a * x = a \quad \forall a \in G$$

$$x * a = a \quad \forall a \in G$$

$$\rightarrow |x| \cdot a = a \rightarrow |x| = 1 \quad \begin{array}{l} x=1 \\ x=-1 \end{array}$$

$$|a|x = a \rightarrow x = \frac{a}{|a|} = \pm 1$$

$$a = 2 \quad a * 1 = |2| \cdot 1 = 2 = a \quad x = 1 \quad \checkmark$$

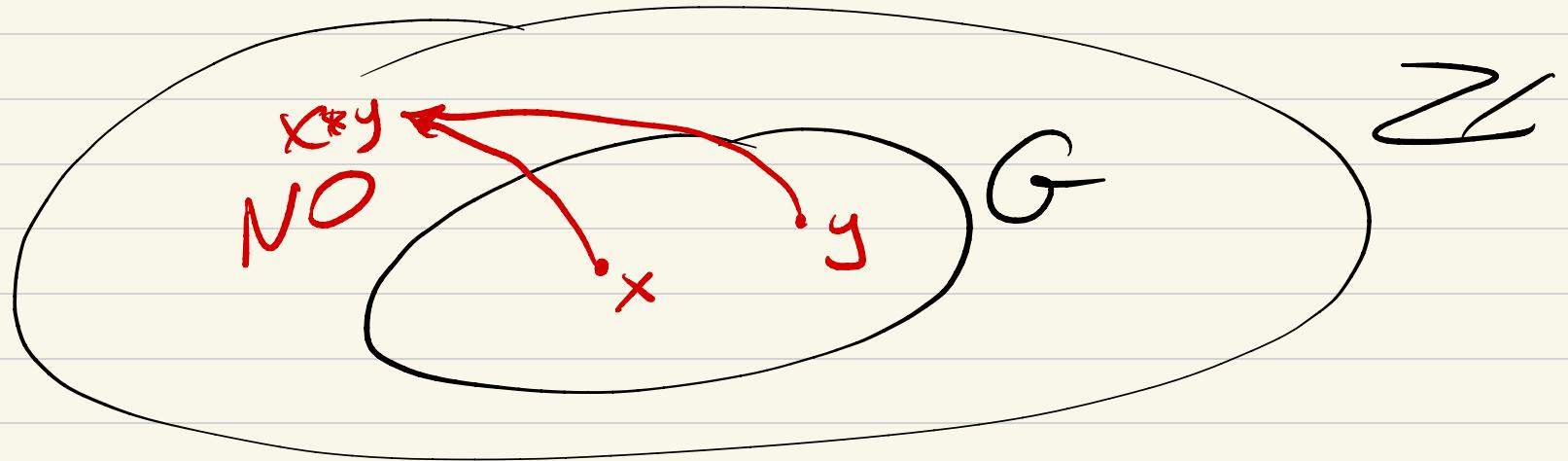
$$1 * a = |1| \cdot a = a \quad \checkmark x = 1$$

$$a = -2 \quad a * 1 = |-2| \cdot 1 = 2 \neq a \rightarrow 1 \text{ non e' id.}$$

Provo con -1

$$\begin{aligned} a &= 2 \\ x &= -1 \end{aligned} \quad a * (-1) = |2| \cdot (-1) = -2 \neq a$$

$$G = \{8a + 14b \mid a, b \in \mathbb{Z}\} \quad a * b = a + b$$



$$x = 8a + 14b, \quad a, b \in \mathbb{Z}$$

$$y = 8c + 14d, \quad c, d \in \mathbb{Z}$$

$$x * y = x + y = (8a + 14b) + (8c + 14d)$$

$$\begin{aligned}
 &= 8a + 8c + 14b + 14d \\
 &= 8(a+c) + 14(\underbrace{b+d}) \in G
 \end{aligned}$$

↗ ↗ ↗ ↗
 2 2 2 2

$$x \in G, \quad x = 8a + 14b$$

$$\begin{aligned}
 \text{l'inverso } \bar{x} - x &\notin G \rightarrow -x = -(8a+14b) \\
 &= 8(-a) + 14(-b) \in G
 \end{aligned}$$

Esempi

L'insieme $\mathbb{N} = \{0, 1, 2, \dots\}$ è un gruppo rispetto all'addizione?

- L'operazione è interna?

Sì!

- L'operazione è associativa?

Sì!

- L'operazione ammette un'identità?

Sì!

- Esistono gli inversi?

No!

$(\mathbb{N}, +)$ NON È UN GRUPPO!

Esempi

L'insieme $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ è un gruppo rispetto all'addizione?
Sì!

L'insieme \mathbb{Z}_p è un gruppo rispetto all'addizione?
Sì!

L'insieme \mathbb{Z} è un gruppo rispetto alla moltiplicazione?
No!

Esempi

L'insieme $\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}$ è un gruppo rispetto alla moltiplicazione?

No!

$(\mathbb{Q} \setminus \{0\}, \cdot)$ è un gruppo rispetto alla moltiplicazione

$$\mathbb{Z}_m = \mathbb{Z}_{15}$$

[5]

L'insieme \mathbb{Z}_p è un gruppo rispetto alla moltiplicazione?

No!

$(\mathbb{Z}_p \setminus \{0\}, \cdot)$ è un gruppo rispetto alla moltiplicazione

$$\text{MCD}(5, 15) = 5 > 1$$

[5] non inverso

Strutture algebriche

(G, \oplus, \star) si dice **CAMPO** se

- (G, \oplus) è un gruppo commutativo con identità 0_G
- $(G \setminus \{0_G\}, \star)$ è un gruppo commutativo con identità 1_G
- valgono le proprietà distributive: per ogni $g_1, g_2, g_3 \in G$
$$(g_1 \oplus g_2) \star g_3 = (g_1 \star g_3) \oplus (g_2 \star g_3)$$

$$(g_1 \star g_2) \oplus g_3 = (g_1 \oplus g_3) \star (g_2 \oplus g_3)$$

Esempi

$(\mathbb{R}, +, \cdot)$ è un campo?

- $(\mathbb{R}, +)$ è un gruppo commutativo con identità 0
- $(\mathbb{R} \setminus \{0\}, \cdot)$ è un gruppo commutativo con identità 1
- Valgono le proprietà distributive

Sì $(\mathbb{R}, +, \cdot)$ è un campo!

$(\mathbb{R}, +, \cdot)$ è un campo INFINITO → poco utile alla crittografia!

$(\mathbb{Z}_p, +, \cdot)$ è un campo FINITO.

Esigenza pratica? Matematica più astratta!

- PROBLEMA: trattamento dei numeri enormi che servono per garantire sicurezza in dispositivi che non sono PC (es.: dispositivi medici, passaporto elettronico).
- SOLUZIONE: funzioni trappola matematicamente più complesse.
- NUOVE TRAPPOLE: moltiplicare/sommare oggetti diversi, non necessariamente numeri.



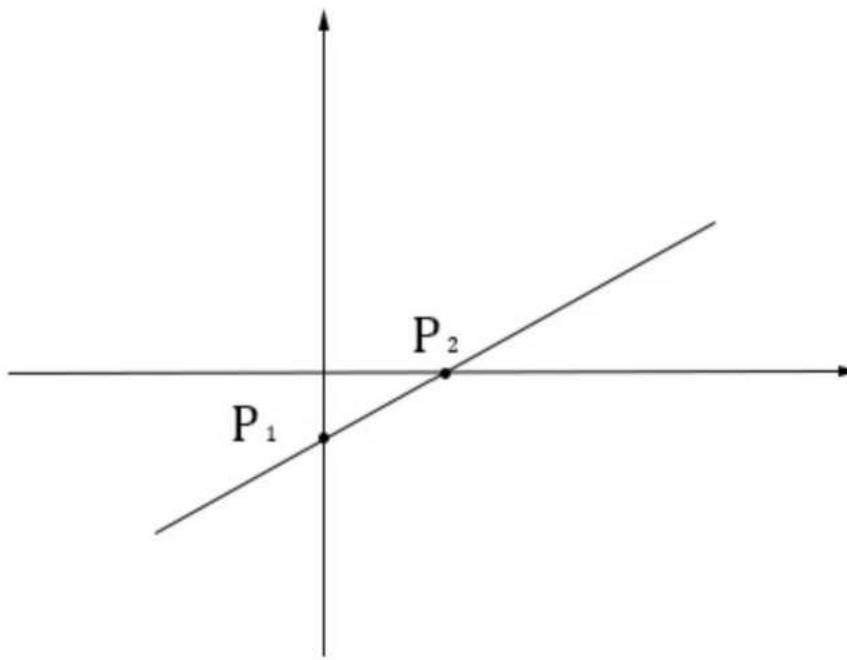
TRAPPOLE GEOMETRICHE:
sommiamo punti e non numeri!

Curve (crittograficamente) noiose

- Curve di grado 1:

$$ax + by + c = 0,$$

$(a, b) \neq (0, 0)$.



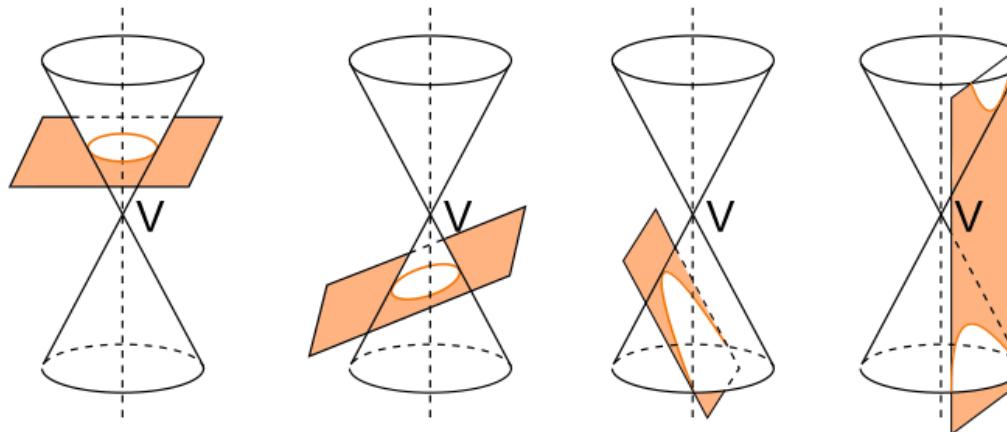
Curve (crittograficamente) noiose

- Curve di grado 2:

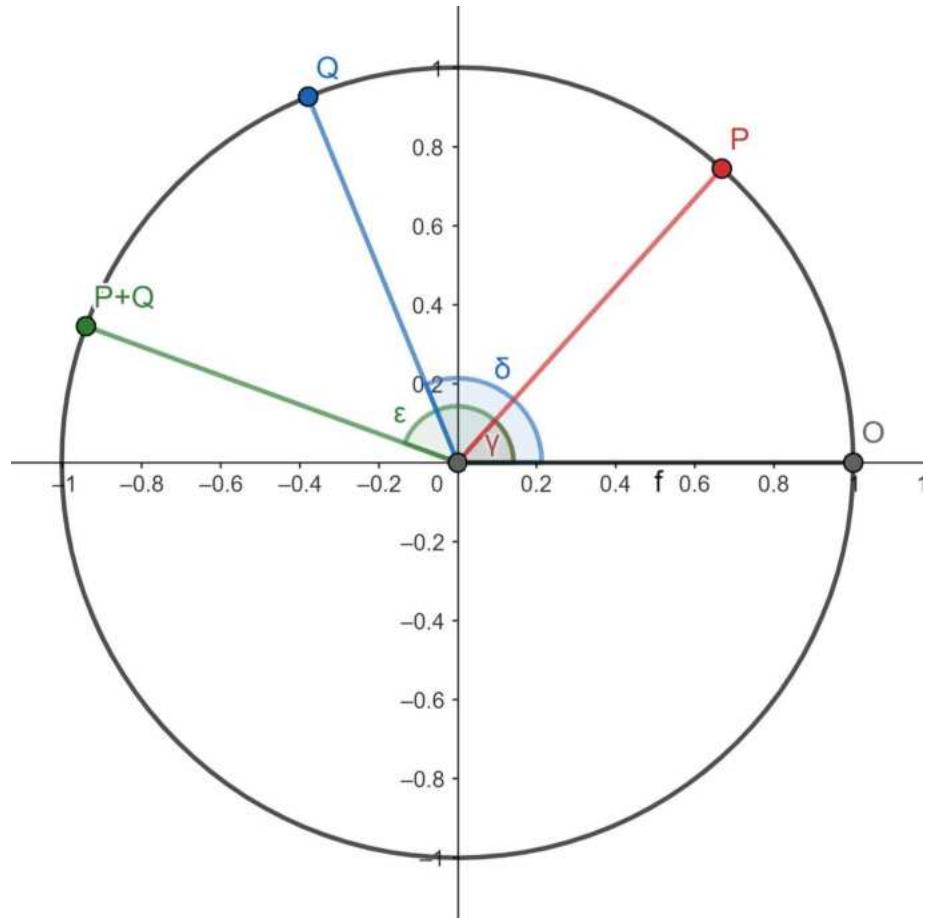
$$ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

$(a, b, c) \neq (0, 0, 0)$.

Circonferenza Ellisse Parabola Iperbole



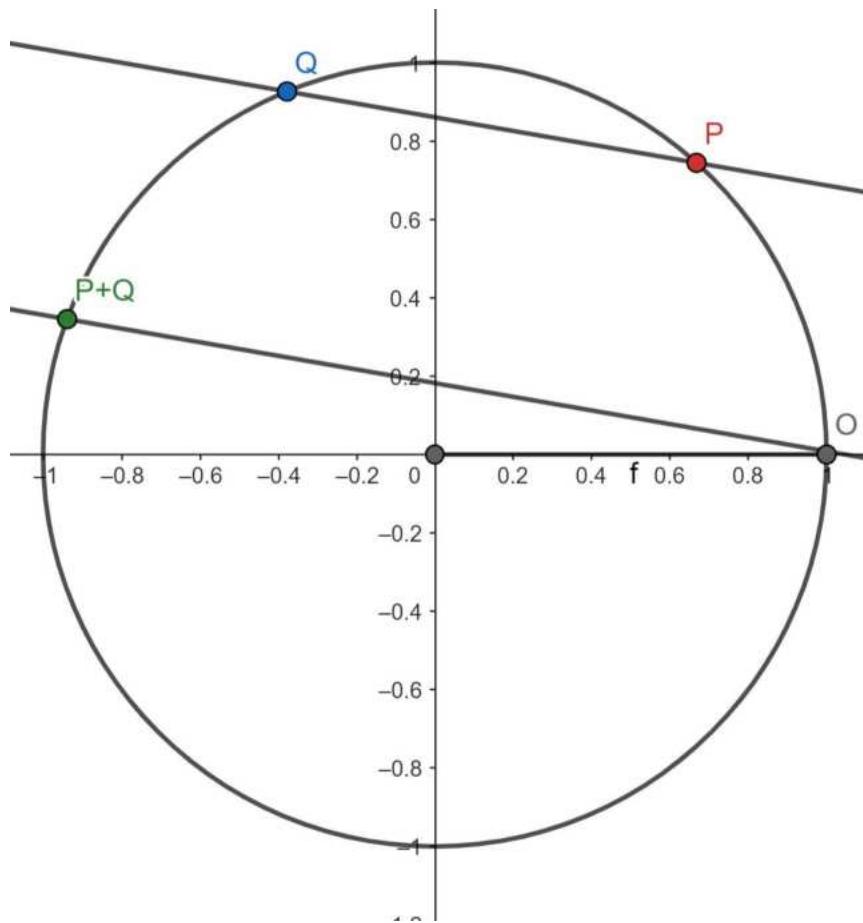
Un primo tentativo...



Come esprimere le coordinate dei punti in funzione degli angoli?
 $P = (\cos \gamma, \sin \gamma)$ e $Q = (\cos \delta, \sin \delta)$, quali sono le coordinate di $P + Q$?

$$P + Q = (\cos(\gamma + \delta), \sin(\gamma + \delta))$$

Un primo tentativo...



Problema: se $P = (x_1, y_1)$ e $Q = (x_2, y_2)$, quali sono le coordinate di $P + Q$?

$$P + Q = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)$$

Operazione associativa, commutativa, che ammette elemento neutro e inversi.

Crittograficamente non abbastanza «sicura».

Inizia il divertimento...

- Curve di grado 3:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0.$$

Dopo una serie di passaggi algebrici si può ridurre questa equazione a

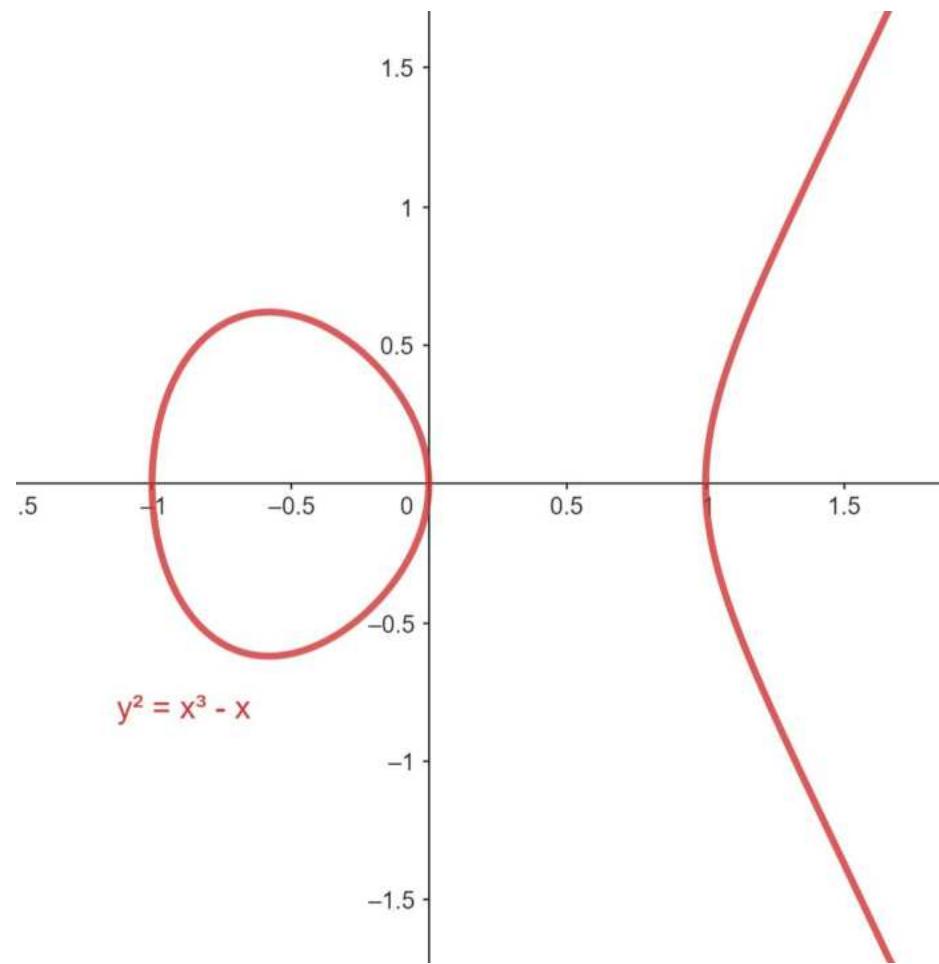
$$y^2 = x^3 + ax + b$$



CURVE ELLITTICHE (se $4a^3 + 27b^2 \neq 0$)

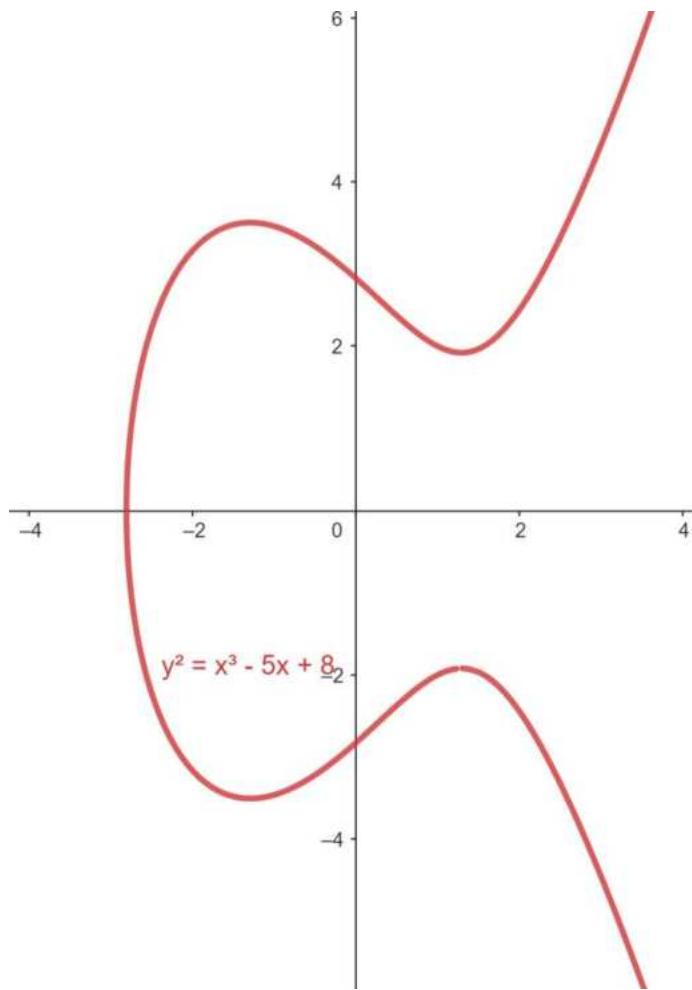
Curve ellittiche

$$y^2 = x^3 - x$$

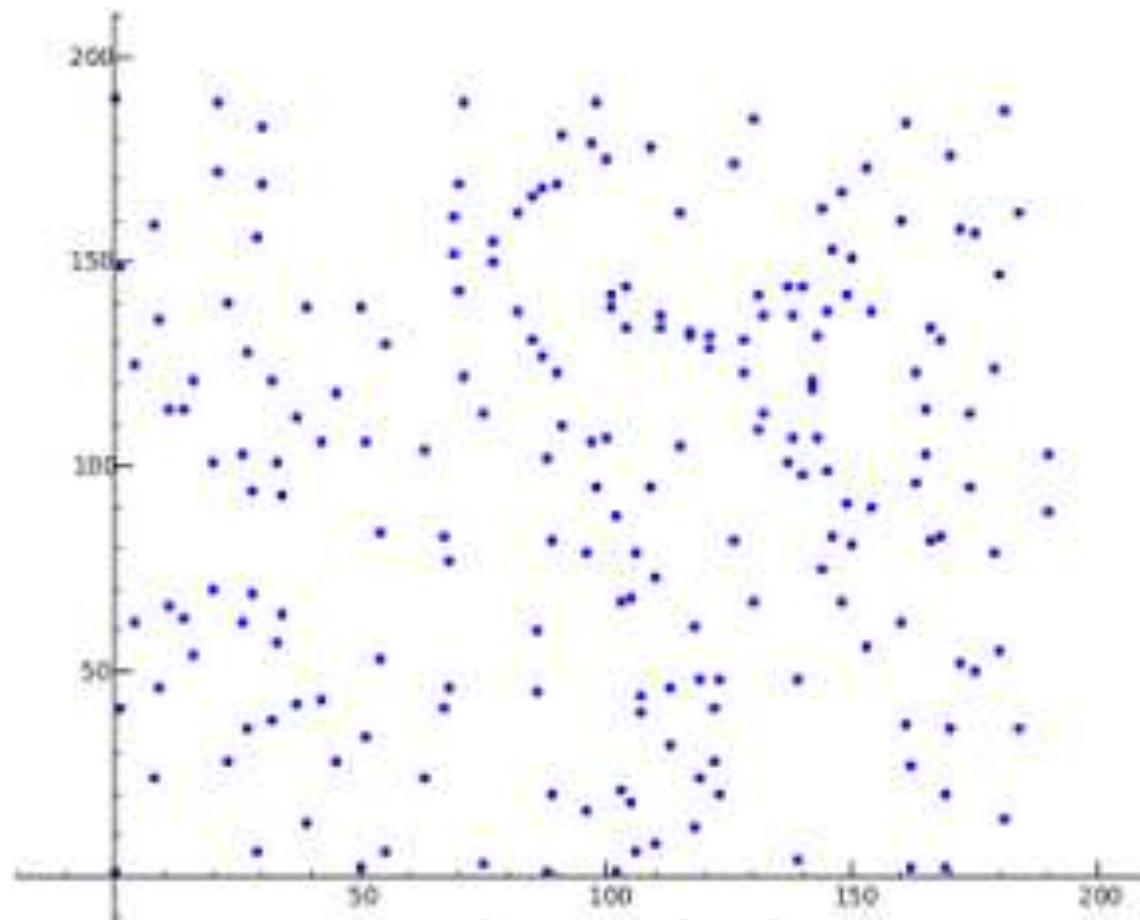


Curve ellittiche

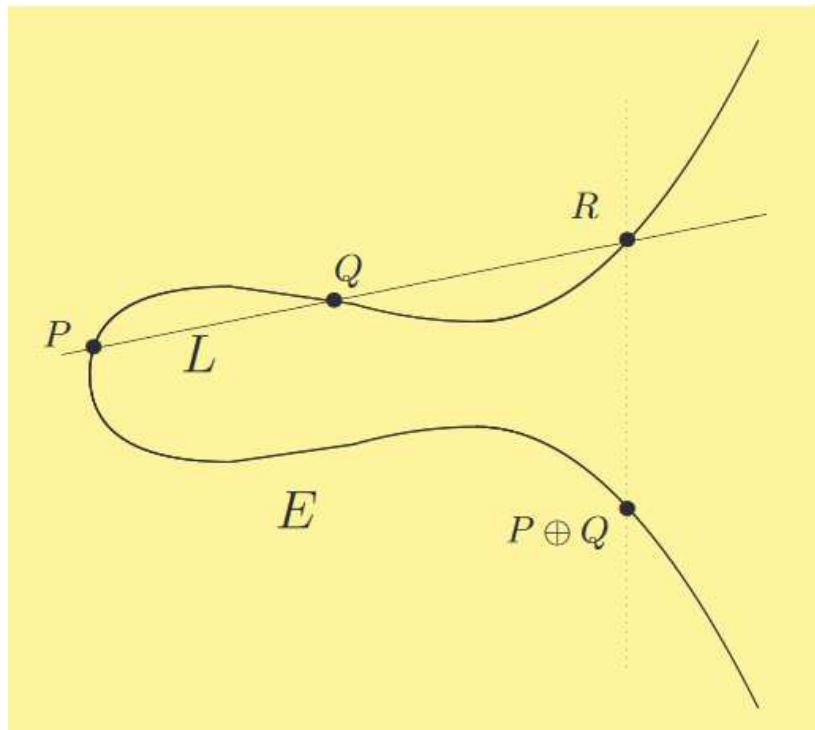
$$y^2 = x^3 - 5x + 8$$



Stessi esempi, ma su un campo finito



Esempio $y^2 = x^3 - 5x + 8$



Fissiamo due punti P e Q di E

Sia L la retta per P e Q

L intersecherà la curva ellittica in un terzo punto R

Consideriamo la retta verticale passante per R

Il punto simmetrico ad R sarà $P \oplus Q$

In formule...

- Sia E : $y^2 = x^3 + ax + b$, con $a, b, c \in \mathbb{Z}_p$ e $4a^3 + 27b^2 \neq 0$
- Siano (x_1, y_1) e (x_2, y_2) due punti di E
- Si ponga m uguale a $\frac{y_2 - y_1}{x_2 - x_1}$ se $x_1 \neq x_2$, altrimenti è uguale a $\frac{3x_1^2 + a}{2y_1}$
- Allora $(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3)$ con
 - $x_3 = m^2 - x_1 - x_2$
 - $y_3 = -m(x_3 - x_1) - y_1$

In formule...

- Con questa operazione $(E(\mathbb{R}), \oplus)$ è un **GRUPPO COMMUTATIVO (INFINITO)**
- In crittografia non si usano curve ellittiche su \mathbb{R} , ma su campi finiti
- In questo caso, il numero di punti della curva è finito
- Curve ellittiche su \mathbb{Z}_p possono essere definite «esattamente» come su \mathbb{R} → le operazioni su \mathbb{R} vengono sostituite con le operazioni su \mathbb{Z}_p .

$(E(\mathbb{Z}_p), \oplus)$ è un **GRUPPO COMMUTATIVO FINITO**

Crittografia su curve ellittiche

Se ciò di cui abbiamo bisogno è un gruppo, perché non usare il gruppo di una curva ellittica?
(Koblitz e Miller, 1985)



Neal Koblitz is a man with short, light-colored hair, wearing a white shirt and a patterned tie. He is looking slightly to his left.

MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 167, JANUARY 1987, pp. 201–209

Elliptic Curve Cryptosystems
By Neal Koblitz

This paper is dedicated to Daniel Shanks on the occasion of his seventieth birthday.

Abstract. We discuss analogs based on elliptic curves over finite fields of public key cryptosystems which use the multiplicative group of a finite field. These elliptic curve cryptosystems have the potential for being more secure than the classical discrete logarithm problem over $GF(2^n)$. We discuss the question of primitive points on an elliptic curve modulo p , and give a theorem on nonexistence of the order of the cyclic subgroup generated by a global point.

1. Introduction. The earliest public key cryptosystems using number theory were based on the structure either of the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^\times$ or the multiplicative group of a finite field $GF(q)$, $q = p^n$. The subsequent construction of analogous systems based on other finite Abelian groups, together with H. W. Lenstra's success in using elliptic curves for factoring integers, has led to interest in the possibility of public key cryptography based on the structure of the group of points of an elliptic curve over a large finite field. We first briefly recall the facts we need about such elliptic curves (for more details, see [4] or [5]). We then describe elliptic curve analogs of the Massey-Omura and ElGamal systems. We give some concrete examples, discuss the question of primitive points, and conclude with a theorem concerning the probability that the order of a cyclic subgroup is nonsmooth.

I would like to thank A. Odlyzko for valuable discussions and correspondence, and for sending me a preprint by V. S. Miller, who independently arrived at some similar ideas about elliptic curves and cryptography.

2. Elliptic Curves. An elliptic curve E_K defined over a field K of characteristic $\neq 2$ or 3 is the set of solutions $(x, y) \in K^2$ to the equation

(1) $y^2 = x^3 + ax + b,$ $a, b \in K$

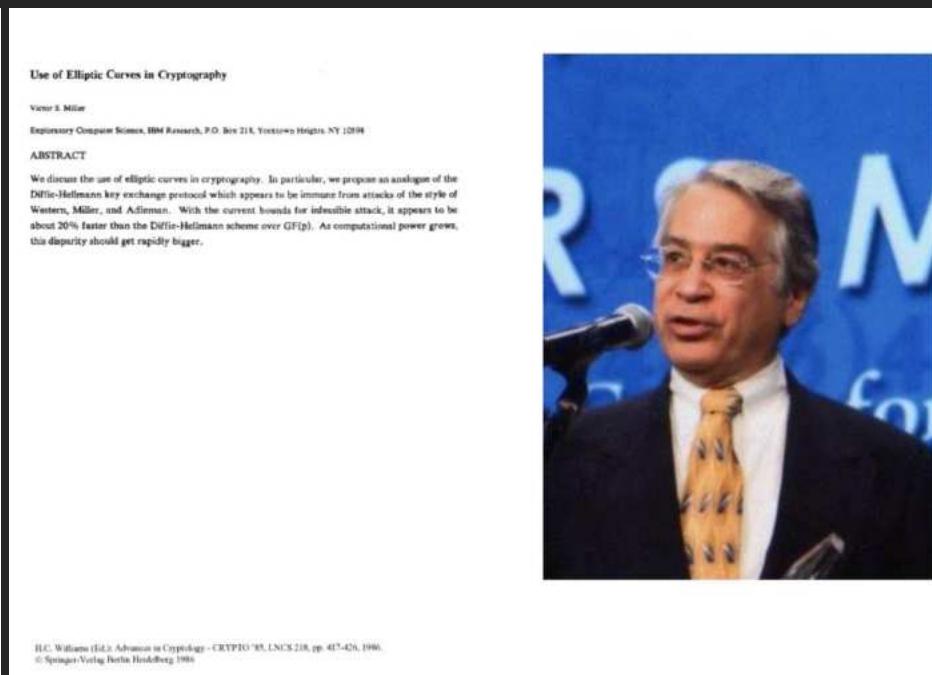
(where the cubic on the right has no multiple roots). More precisely, it is the set of such solutions together with a "point at infinity" (with homogeneous coordinates $(0, 1, 0)$; if K is the real numbers, this corresponds to the vertical direction which the tangent line to E_K approaches as $x \rightarrow \infty$). One can start out with a more complicated general formula for E_K which can easily be reduced to (1) by a linear change of variables whenever $\text{char } K = 2, 3$. If $\text{char } K = 2$ —an important case in

Rational October 29, 1985; revised June 7, 1986.
1986 Mathematics Subject Classification (1985 Revision). Primary 11T71, 94A60; Secondary 14H52, 11Y40.

©1987 American Mathematical Society
0025-5718/87/0101-0201+\$01.25 per page

201

License or copyright restrictions may apply to redistribution; see <http://www.ams.org/journal-terms-of-use>.



Pro e Contro

Pro

- **Stessa sicurezza** di RSA o sistemi basati su DLP classico, ma con **chiavi più corte** (160-256 bit vs 1024-3072 bit)
- L'algoritmo Index Calculus (**sub-esponenziale**) non è applicabile al gruppo di una curva ellittica

«It is extremely unlikely that an index calculus attack on the elliptic curve method will ever be able to work»

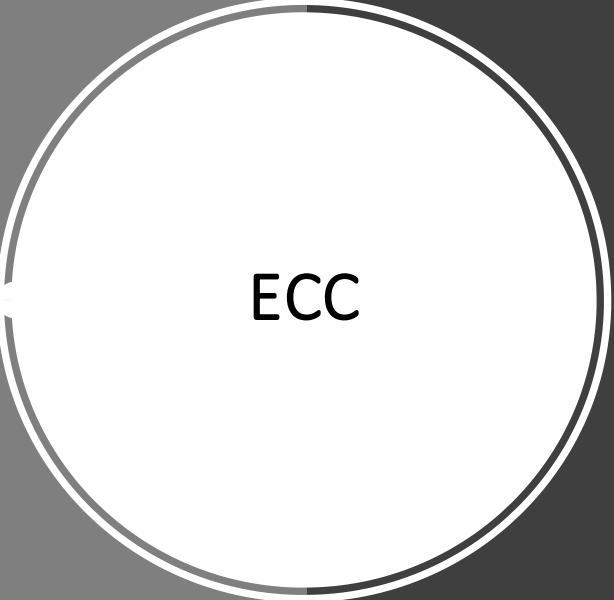
(V.S. Miller)

Contro

- Attacco MOV: bisogna stare attenti alla scelta della curva...

ECDH

- Analogico a DH
- Basta sostituire il gruppo (\mathbb{Z}_p^*, \cdot) con il gruppo (\mathcal{X}, \oplus)
- Logaritmo molto più difficile che in (\mathbb{Z}_p^*, \cdot) ; la stessa sicurezza viene garantita da chiavi più piccole



ECC

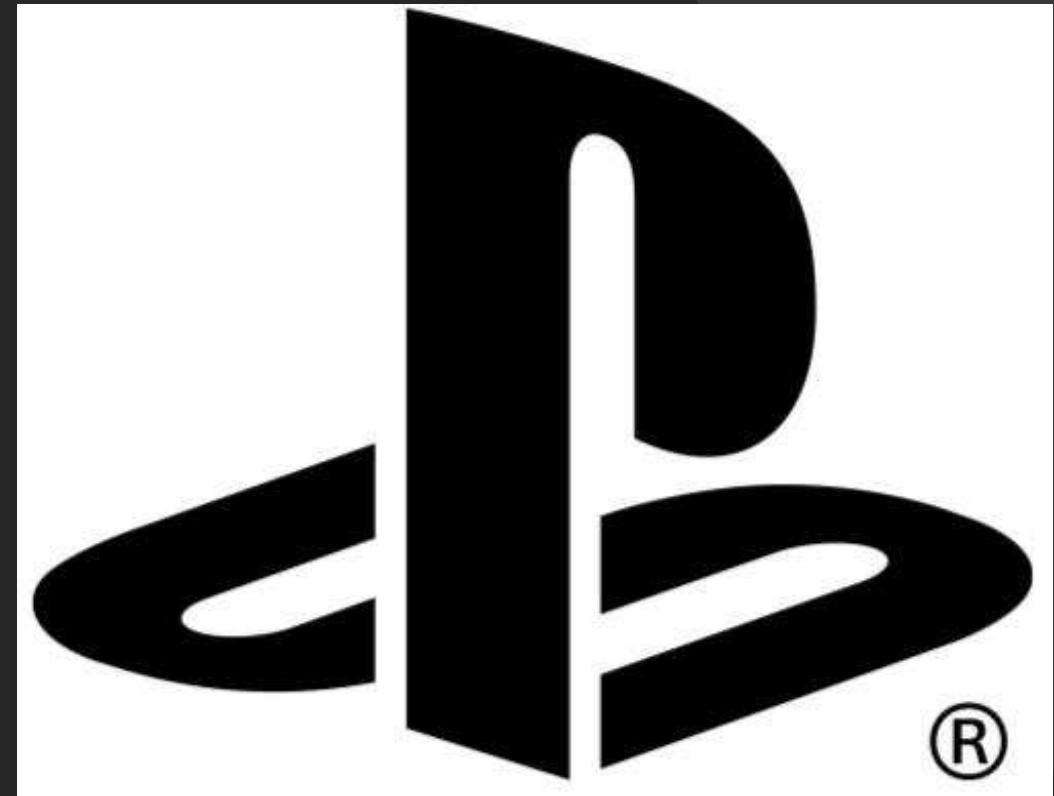
- Sia \mathcal{X} la curva ellittica definita su un campo finito \mathbb{Z}_p , con p primo.
- Sia P un punto di ordine N primo (con N che divide la cardinalità di $\mathcal{X}(\mathbb{Z}_p)$, e tale che il logaritmo discreto non sia fattibile nel sottogruppo generato da P)
- Testi in chiaro: elementi di \mathbb{Z}_p^* . Testi cifrati: elementi di $\mathbb{Z}_p \times \mathbb{Z}_2 \times \mathbb{Z}_p^*$
- **Chiave privata:** a elemento di \mathbb{Z}_N^*
- **Chiave pubblica:** $p, \mathcal{X}, P, N, Q = [a]P$
- **Cifratura di un messaggio x .** Si stabilisce una chiave privata di sessione $k \in \mathbb{Z}_N^*$, si calcola il punto $[k]Q = (x_0, y_0)$ e si invia $(x \cdot x_0 \pmod p, \text{PointCompress}([k]P))$
- **Decifratura di (y_1, y_2) .** Si calcola $\text{PointCompress}(y_2)$ determinando in questo modo $[k]P$. Quindi si determina $[k]Q$ calcolando $[a]([k]P)$. Infine $x = y_1/x_0 \pmod p$.

ECC vs RSA

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Playstation

- SONY crea le proprie chiavi: pubblica e privata
- in ogni console è caricata la chiave pubblica
- in ogni DVD, oltre al gioco, c'è la firma del gioco: il gioco mascherato con la chiave privata
- Ogni volta che il gioco viene caricato, la console controlla l'autenticità della firma applicando alla firma la chiave pubblica, e verificando che il risultato sia ancora il gioco



PS3 e curve ellittiche

- L'algoritmo di firma visto prima utilizza proprio la trappola delle curve ellittiche ECDSA
- Nel dicembre 2010 un gruppo di hacker è riuscito a risalire alla chiave privata di Sony
- Non ci sarebbero mai riusciti se non avessero avuto conoscenze matematiche di livello universitario

GAMING & CULTURE —

PS3 hacked through poor cryptography implementation

A group of hackers named failOverflow revealed in a presentation how they ...

CASEY JOHNSTON - 12/30/2010, 6:25 PM

158



A group of hackers called failOverflow claim they've figured out a way to get better control over a PlayStation 3 than ever before. After they worked through a number of Sony's security measures, they found the keystone to gaining access to the system's innards was the PS3's poor use of public key cryptography.

At the Chaos Communication Conference 27C3, the team gave a 45-minute presentation on the methods they used to work through the PS3's various security levels, which include a chain of trust, a hypervisor, and signed executables. Their primary goal was to restore the capability to run Linux, something that was forcibly removed from the original PS3 and never possible on the PS3 Slim.

After beating several other security measures, the group was able to locate the PS3's ECDSA signature, a private cryptographic key needed to sign off on high-level operations. Normally, these kinds of keys are difficult to figure out, and require running many generations of keys to crack.

But when failOverflow worked backwards from generated keys, they found out that a parameter that should have been randomized for each key generation wasn't being randomized at all. Instead, the PS3 was using the same number for that variable, every single time, making it easy to work out acceptable keys.

PS4

*Crittografia migliore...
forse troppo?*

How ISIS could use video games, messaging apps to evade surveillance

ISIS uses Sony's PlayStation 4 gaming platform to communicate covertly, according to a new report.

PS5

L33TH4XX0RS —

Hacking group says it has found encryption keys needed to unlock the PS5 [Updated]

FailOverflow announcement suggests a private exploit to expose system's secure kernel.

KYLE ORLAND - 11/8/2021, 11:14 PM



Crittografia post-quantum

La minaccia quantistica

- La «supremazia quantistica» o «vantaggio quantistico» è la capacità dei dispositivi di calcolo quantistico di risolvere problemi che i computer classici non riescono a risolvere.
- FINORA, LA SUPREMAZIA QUANTISTICA NON È STATA ANCORA RAGGIUNTA!
- Google aveva annunciato l'intenzione di dimostrare la supremazia quantistica entro la fine del 2017...
- A marzo 2018, Google ha annunciato Bristlecone, un nuovo processore quantistico da **72 qubit**, ma sta ancora cercando di farlo funzionare...



Computer quantistico VS Crittografia classica

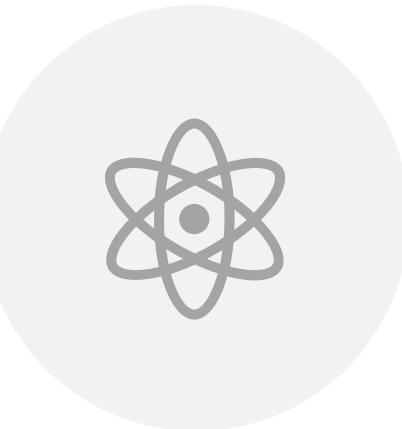
Se esistesse un computer quantistico:
si romperebbe crittografia a chiave pubblica
basata sulle trappole della fattorizzazione
classica e dei log discreti
(a causa dell'algoritmo di Shor)

e
costringerebbe a raddoppiare le dimensioni
delle chiavi della crittografia a chiave
simmetrica

(a causa dell'algoritmo di Grover).

- Non si conoscono molti altri algoritmi quantistici... ancora!
- Allora... quali soluzioni adottare?

Ci sono due
alternative...



I fisici dicono: «*Usa le tecnologie quantistiche per combattere la tecnologia quantistica!*»

CRITTOGRAFIA QUANTISTICA



I matematici dicono: «*Basa la tua crittografia sulla matematica che i computer quantistici non possono risolvere.*»

CRITTOGRAFIA

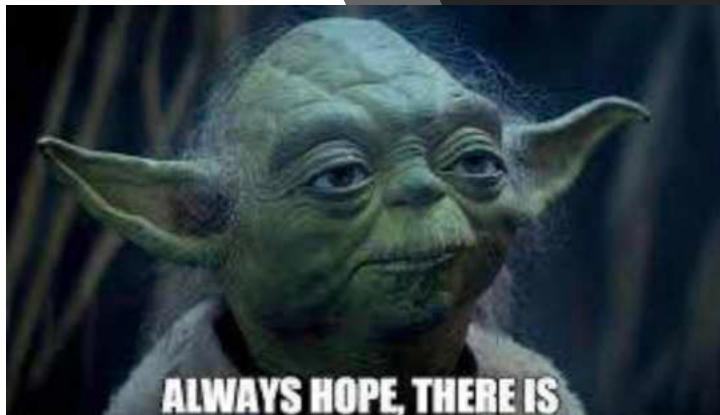
POST-QUANTISTICA

La crittografia quantistica nella pratica...

- principalmente si limita alla distribuzione di chiavi quantistiche,
- richiede una connessione diretta in fibra ottica o una linea di vista,
- ha un problema con le grandi distanze,
- necessita di nuove infrastrutture e nuove tecnologie,
- non funziona con telefoni cellulari, reti di sensori, auto, ecc.
- si basa sulle leggi della fisica e sulla sicurezza teorica dell'informazione, piuttosto che sulla matematica e sulla complessità computazionale.

Post Quantum Cryptography (o PQC)

I computer quantistici non risolvono **TUTTI** i problemi **difficili...**



PQC è costituito da algoritmi **classici** che:

- funzionano in modo efficiente su computer classici in termini di tempo, memoria e comunicazione,
- sono difficili da rompere sia con algoritmi classici che quantistici,
- fanno affidamento su problemi matematici diversi dalla fattorizzazione o dai logaritmi discreti.

Competizione NIST Post-quantum

«*Regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing*»



Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PROJECTS

Post-Quantum Cryptography PQC



Overview

The [Candidates to be Standardized](#) and [Round 4 Submissions](#) were announced July 5, 2022. [NISTIR 8413, Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process](#) is now available.

New Call for Proposals:

[Call for Additional Digital Signature Schemes for the Post-Quantum Cryptography Standardization Process](#)

[Post-Quantum Encryption: A Q&A With NIST's Matt Scholl](#)

[Post-Quantum Cryptography: the Good, the Bad, and the Powerful \(video\)](#)

Competizione NIST Post-quantum

- Feb. 2016 Annuncio a PQCrypto 2016
- Apr. 2016 Il NIST rilascia NISTIR 8105 - Report on Post-Quantum Cryptography
- Dic. 2016 Invito formale a presentare proposte
- Nov. 2017 Scadenza per l'invio
- Workshop inizio 2018 Presentazioni dei partecipanti
- Gen. 2019 2° round
- Lug. 2020 3° round
- Lug. 2022 Vincitori

Candidati NIST

Famiglia	Firma	KEM/PKE	Somma
Reticoli	5	23	28
Codici	3	17	20
Multivariata	7	3	10
Hash	2	0	2
Altro	3	6	9
TOTALE	20	49	69



Crittografia basata su codici

Teoria dei Codici

Branca della Teoria dell'Informazione che si occupa di rilevare e correggere eventuali errori nella comunicazione

Pro e Contro

Vantaggi

- Efficiente
- Molto sicuro (l'algoritmo originale ha superato 40 anni di test)

Svantaggi

- Chiavi di grandi dimensioni



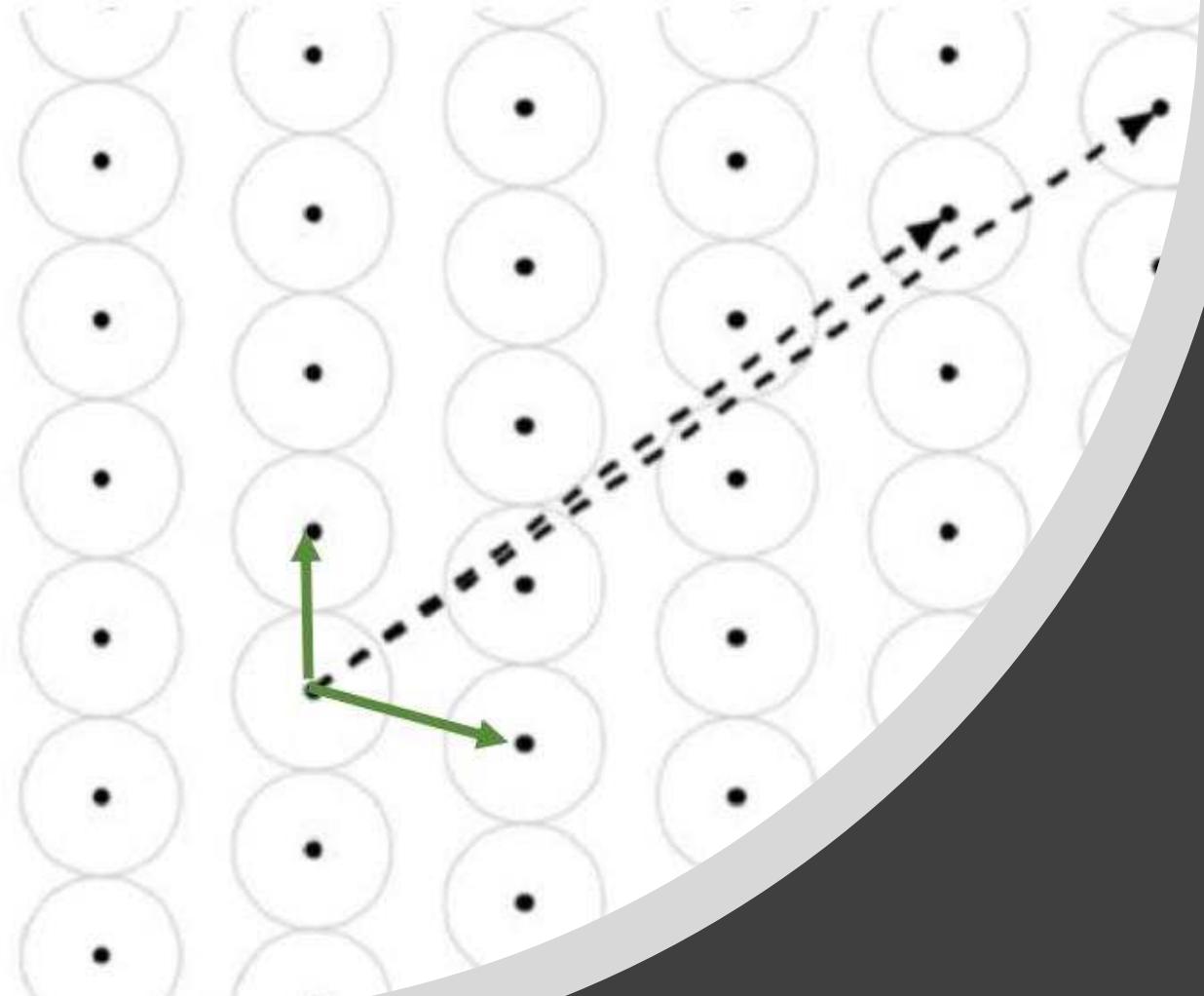
Crittografia basata su reticolati

Reticoli e codici

Le idee sulla crittografia basata su reticoli sono molto simili a quelle sulla crittografia basata su codici.

Un reticolo è un **sottogruppo** del gruppo additivo \mathbb{R}^n che è isomorfo al gruppo additivo \mathbb{Z}^n ... in altre parole, un insieme di punti con n coordinate, una somma, un prodotto scalare e la metrica euclidea...

- È possibile disegnare la "palla" più grande tale che, quando è centrata in ogni punto del reticolo, le palline non si intersecano.
- **Un messaggio è un punto del reticolo.**
- Per crittografare aggiungiamo un errore "piccolo" (all'interno del cerchio) al messaggio iniziale.



Sistemi lineari

Risolvere sistemi lineari è facile!

- Date

$$\begin{aligned}1s_1 + 2s_2 + 5s_3 + 2s_4 &= 9 \text{ mod } 13 \\12s_1 + 1s_2 + 1s_3 + 6s_4 &= 7 \text{ mod } 13 \\6s_1 + 10s_2 + 3s_3 + 6s_4 &= 1 \text{ mod } 13 \\10s_1 + 4s_2 + 12s_3 + 8s_4 &= 0 \text{ mod } 13\end{aligned}$$

- Trovare s_1, s_2, s_3, s_4 .

Sistemi lineari con errori

Risolvere sistemi lineari con errori è difficile!

- Date

$$1s_1 + 2s_2 + 5s_3 + 2s_4 \approx 9 \bmod 13$$

$$12s_1 + 1s_2 + 1s_3 + 6s_4 \approx 7 \bmod 13$$

$$6s_1 + 10s_2 + 3s_3 + 6s_4 \approx 1 \bmod 13$$

$$10s_1 + 4s_2 + 12s_3 + 8s_4 \approx 0 \bmod 13$$

- Trovare s_1, s_2, s_3, s_4 , sapendo che la soluzione ha un errore di circa ± 1 .
- Il problema si chiama **Learning with errors (LWE)**.



Crittografia multivariata

Il problema è...
... risolvere un sistema di m equazioni polinomiali in n variabili.

Tale problema è detto **problema MP** ed è molto complesso anche per un sistema quadratico.

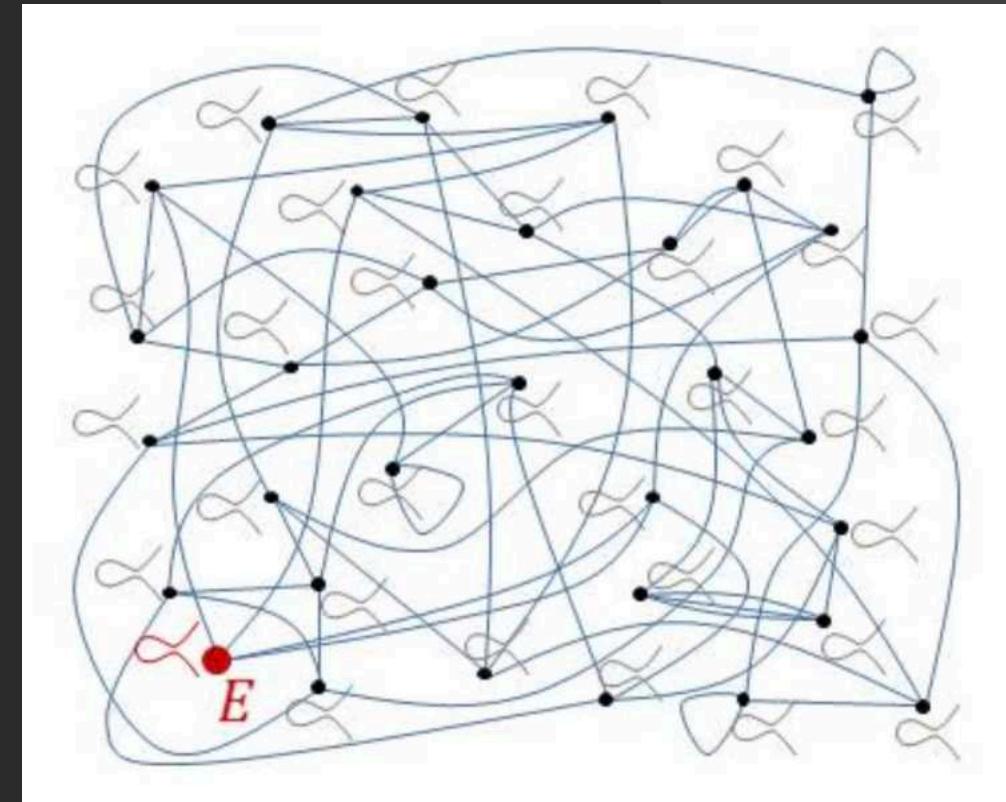
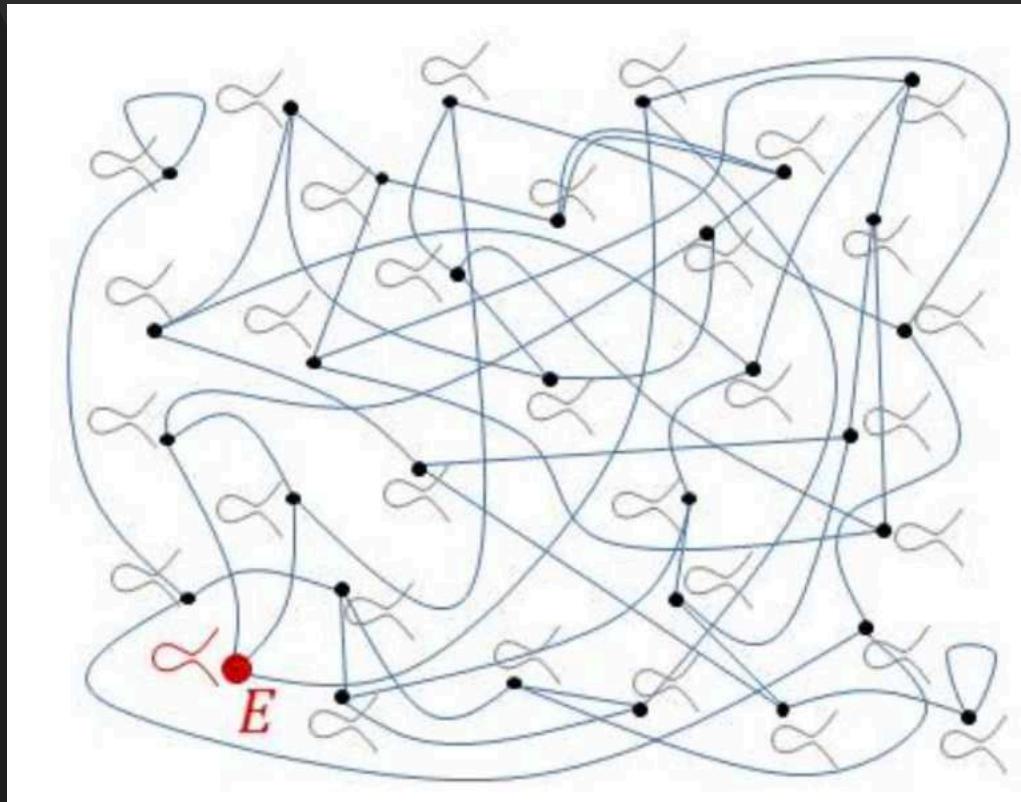
Esempio con $m = 3$ e $n = 3$:

$$5x_1^3x_2x_3^2 + 17x_2^4x_3 + 23x_1^2x_2^4 + 13x_1 + 12x_2 + 5 = 0$$

$$12x_1^3x_2^3x_3 + 15x_1x_3^3 + 25x_2x_3^3 + 5x_1 + 6x_3 + 12 = 0$$

$$28x_1x_2x_3^4 + 14x_2^3x_3^2 + 16x_1x_3 + 32x_2 + 7x_3 + 10 = 0$$

Grafo di curve ellittiche



PROBLEMA: Data una curva ellittica E' ottenuta applicando una sequenza casuale di due o tre isogenie a partire da una curva base E , trovare come arrivare da E a E' utilizzando la stessa mappa.

Classic ECC VS Crittografia basata su isogenie

- **ECC classico:** scopri la relazione nascosta tra due punti P, P' su una data curva ellittica E .
- **Crittografia basata su isogenie:** trova un cammino tra due curve ellittiche E, E' all'interno di un certo grafo di curve ellittiche.

Pro Vs Contro

- Costo di comunicazione basso.
- Chiavi piccole.
- Elevato costo computazionale.
- Proposta molto recente; sicurezza non ancora ben compresa.
- Prima proposta con curve ordinarie rotta da computer quantistici.
- Nuova proposta che utilizza curve supersingolari sotto esame (un attacco è in fase di verifica)

PQC: schema di cifratura e firme a chiave pubblica

Codici	Reticoli	Isogenie	Multivariata
<ul style="list-style-type: none">• Più testato• Veloce• Dimensioni di chiavi più grandi	<ul style="list-style-type: none">• Relativamente «nuovo»• Chiavi abbastanza corte• Più veloce	<ul style="list-style-type: none">• Grafi e curve ellittiche• Dimensioni di chiavi più piccole• Lento	<ul style="list-style-type: none">• Proposte fragili• Chiavi abbastanza corte per la firma• Velocità moderata

Per concludere, dobbiamo preoccuparci?

- Gli schemi post-quantistici esistono già per dispositivi potenti, ma sono molto impegnativi per dispositivi come microprocessori ecc.
- RSA è molto vecchio e facile da implementare in modo non sicuro.
- ECC è molto elegante ed efficiente ma in qualche modo limitato a pochissimi casi d'uso.
- La crittografia ibrida potrebbe essere una buona soluzione temporanea.
- La progettazione di nuovi protocolli per adattarsi meglio alla limitazione degli schemi post quantistici è certamente un must.
- ... e per rispondere alla domanda del titolo... **sì, dovremmo!**

*Grazie per
l'attenzione!*

Marco Timpanella
marco.timpanella@unipg.it