

# Introduzione alla crittografia

## Sicurezza informatica

v 2.5 ~ mag 2022



Prof. Marco Farina

[marco.farina@its-ictpiemonte.it](mailto:marco.farina@its-ictpiemonte.it)

[t.me/marcofarina](https://t.me/marcofarina)

in collaborazione con:



Mercoledì 15 Ottobre 1586. È mattina, Mary Stuart entra nell'affollata aula di giustizia del castello di Fotheringhay. Anni di prigione e l'insorgere di una malattia reumatica hanno lasciato il segno, ma la regina è dignitosa, composta e incontestabilmente regale.

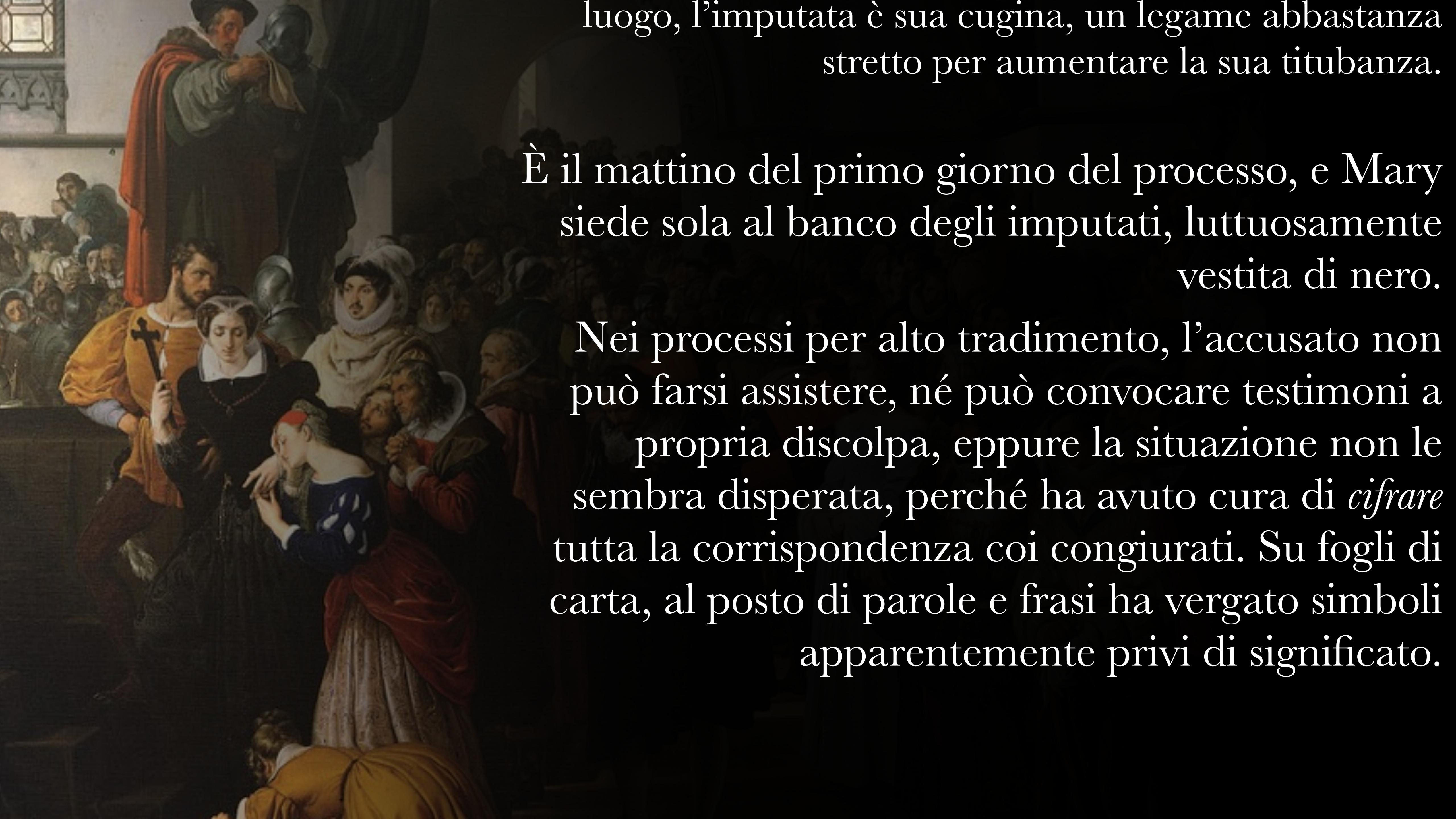
Mary, Regina degli scozzesi, è accusata di tradimento: avrebbe partecipato a un complotto mirante a sopprimere Elisabetta e a porla sul trono d'Inghilterra al posto dell'uccisa.



Il segretario di stato Sir Francis Walsingham, ha arrestato gli altri cospiratori, e dopo averli costretti a confessare, li ha consegnati al boia. Ora intende dimostrare che Mary

Stuart merita la morte, perché era al corrente della congiura e vi ha partecipato attivamente. Walsingham sa bene che Elisabetta non firmerà la condanna se non sarà certa della colpevolezza della Stuart.

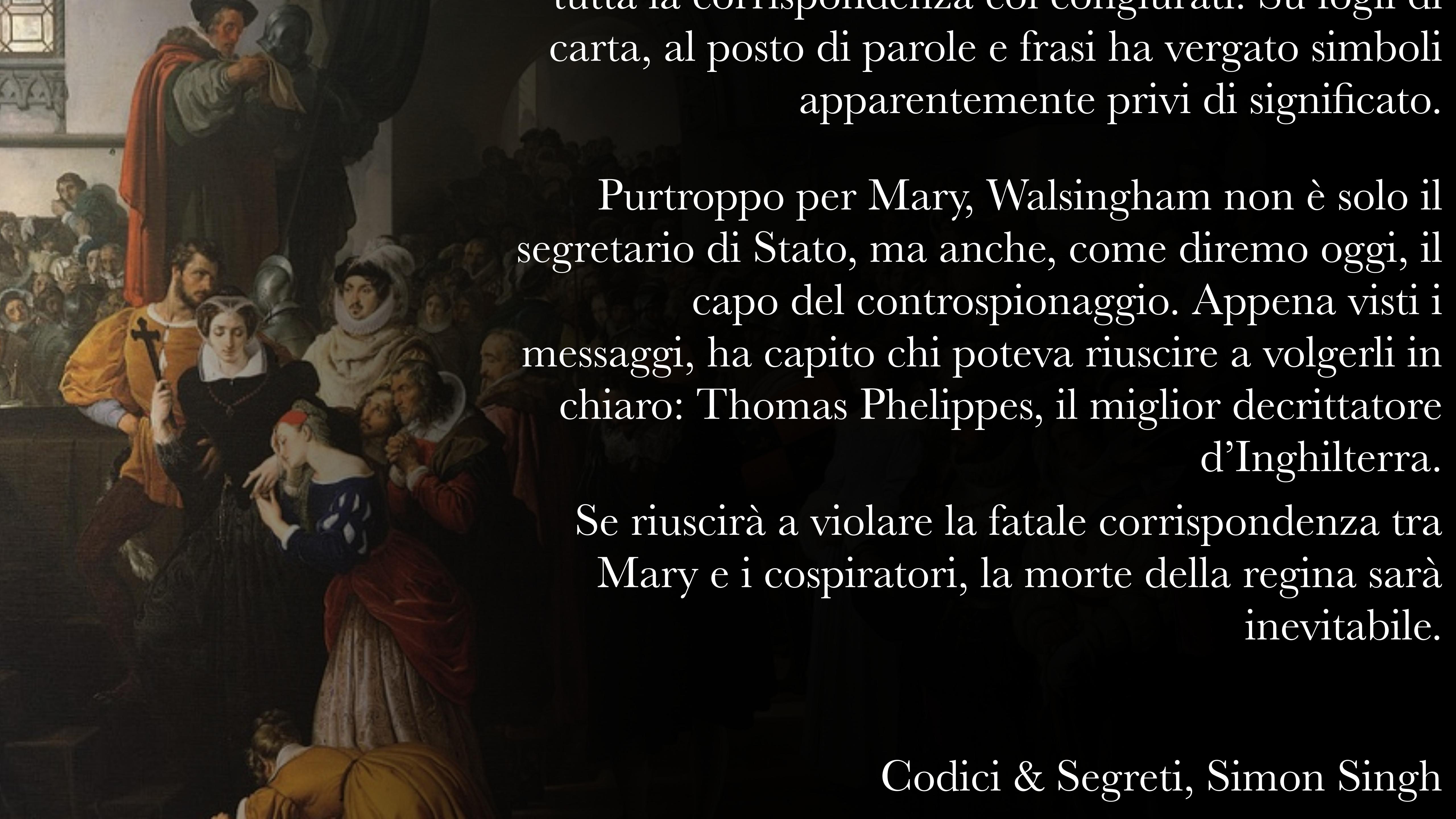
In primo luogo Mary è regina di Scozia, e molti dubitano che mandare a morte il capo di un paese straniero rientri nei poteri di un tribunale inglese. In secondo luogo, l'esecuzione può creare un pericoloso precedente: se uno Stato si arroga il diritto di sopprimere il monarca, i capi di un'eventuale rivolta non avranno scrupoli a fare lo stesso, ed Elisabetta ha ancora molti nemici. In terzo luogo, l'imputata è sua cugina, un legame abbastanza stretto per aumentare la sua titubanza.



luogo, l'imputata è sua cugina, un legame abbastanza stretto per aumentare la sua titubanza.

È il mattino del primo giorno del processo, e Mary siede sola al banco degli imputati, luttuosamente vestita di nero.

Nei processi per alto tradimento, l'accusato non può farsi assistere, né può convocare testimoni a propria discolpa, eppure la situazione non le sembra disperata, perché ha avuto cura di *cifrare* tutta la corrispondenza coi congiurati. Su fogli di carta, al posto di parole e frasi ha vergato simboli apparentemente privi di significato.



tutta la corrispondenza coi congiurati. Su fogli di carta, al posto di parole e frasi ha vergato simboli apparentemente privi di significato.

Purtroppo per Mary, Walsingham non è solo il segretario di Stato, ma anche, come diremo oggi, il capo del controspionaggio. Appena visti i messaggi, ha capito chi poteva riuscire a volgerli in chiaro: Thomas Phelippes, il miglior decrittatore d'Inghilterra.

Se riuscirà a violare la fatale corrispondenza tra Mary e i cospiratori, la morte della regina sarà inevitabile.

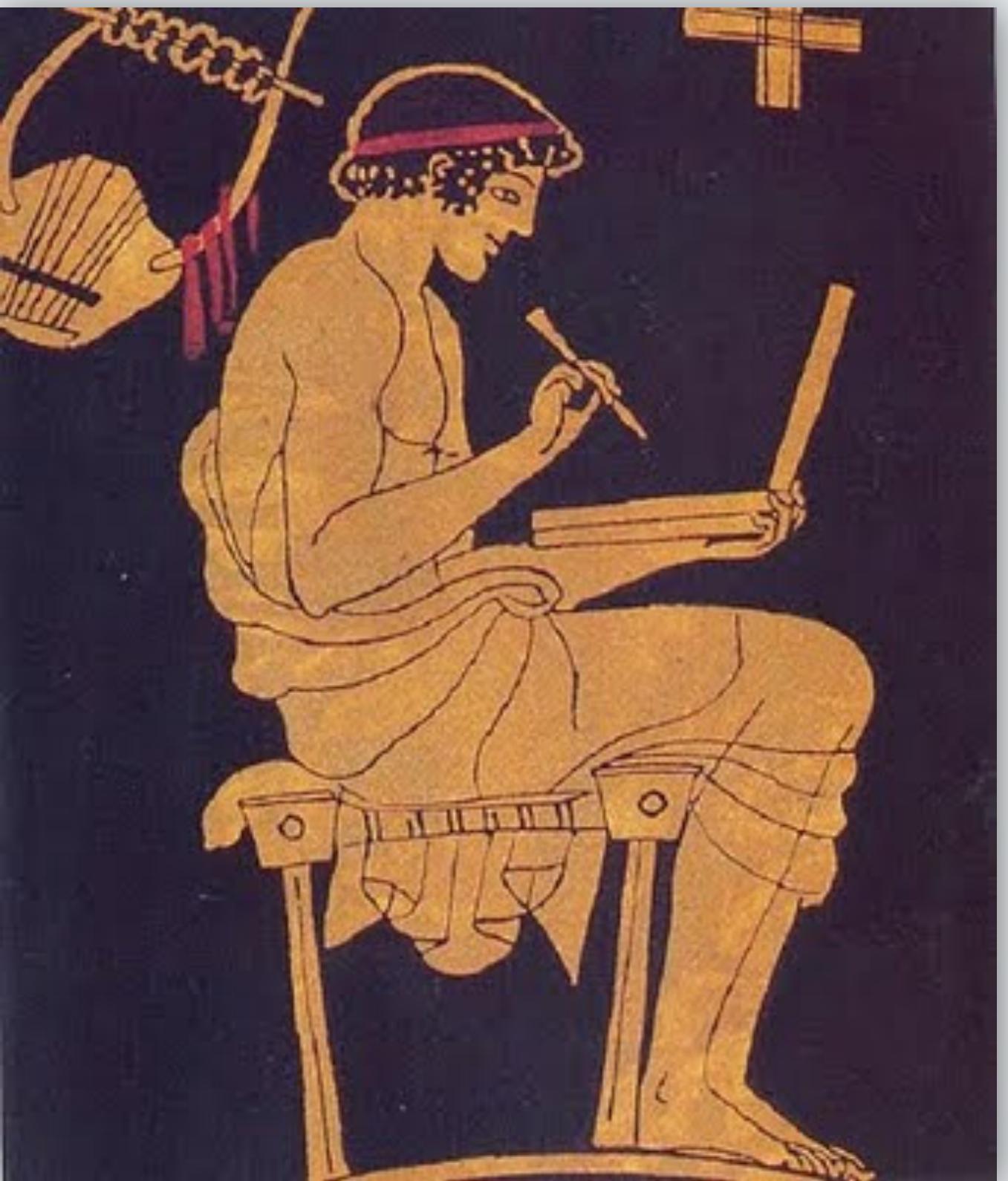
Codici & Segreti, Simon Singh



# La nascita della crittografia

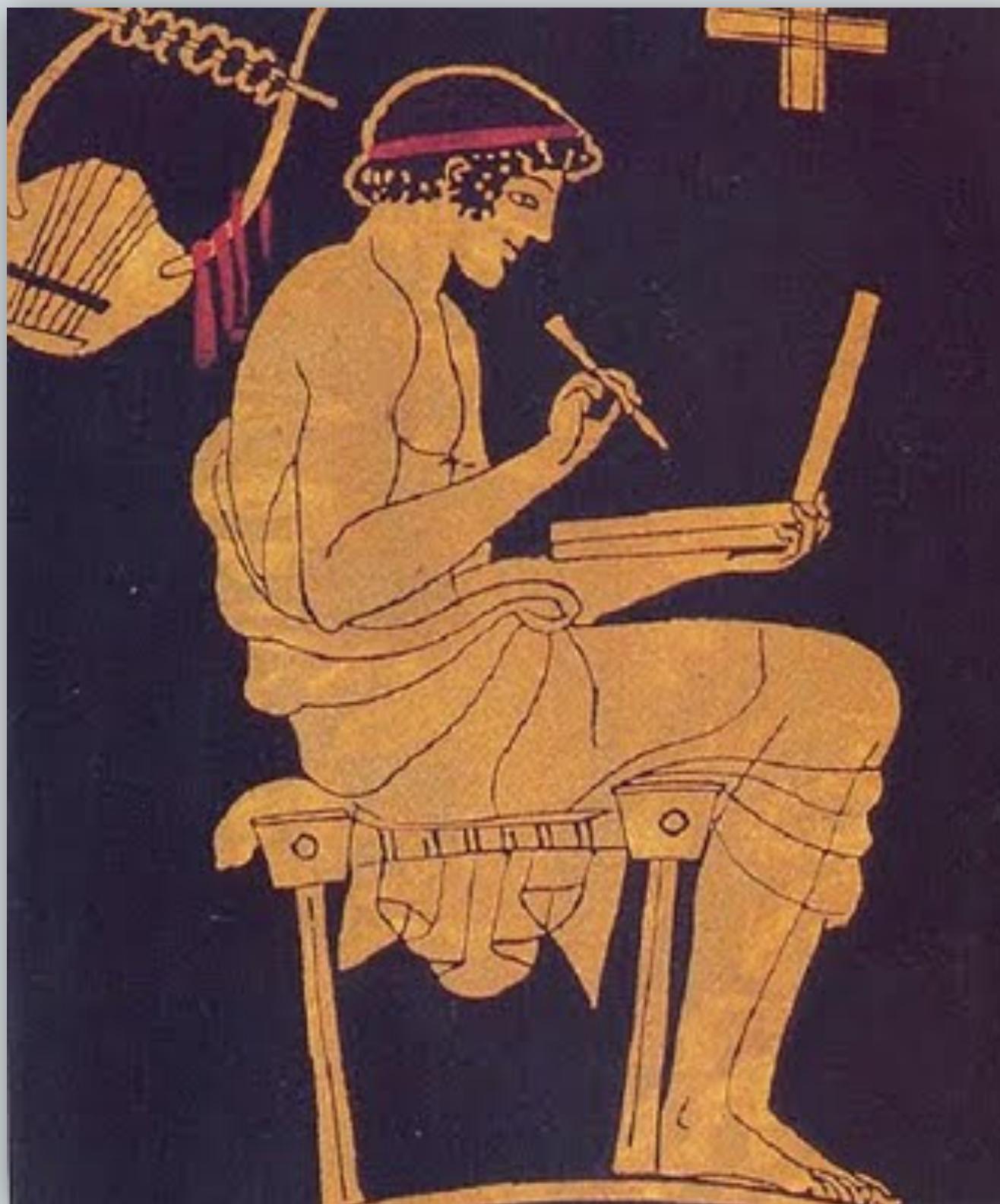
(immaginate di ascoltare l'Aria sulla quarta corda)

# Steganografia



Demarato di Sparta  
(-480)

# Steganografia



Demarato di Sparta  
(-480)



Istieo di Mileto  
(-499)

# Crittografia



# Decrittografia



# Il Cifrario di Cesare



$$k = 2$$



meet me after the toga party

OGGV OG CHVGT VJG VQIC RCTVA

# Crittoanalisi

## Quanto è grande lo spazio delle chiavi?

$$K^{\star} = |\Sigma| = 26$$

**Problema:** spazio delle chiavi troppo piccolo.

**Conseguenza:** attacco brute force.

**Soluzione?** aumentare lo spazio delle chiavi.

# Cifratura monoalfabetica

A B C D E F G H I J K L M N O P Q R S T ...

A B C D E F G H I J K L M N O P Q R S T ...

# Cifratura monoalfabetica

A B C D E F G H I J K L M N O P Q R S T ...

D G N R C S F O A M P B Q J H E I T L K ...

La permutazione di  $\Sigma$  costituisce la chiave crittografica.

## Quanto è grande lo spazio delle chiavi?

$$K^\star = 26! \approx 4 \cdot 10^{26}$$

$$n! := \prod_{k=1}^n k = 1 \cdot 2 \cdot 3 \cdots n$$

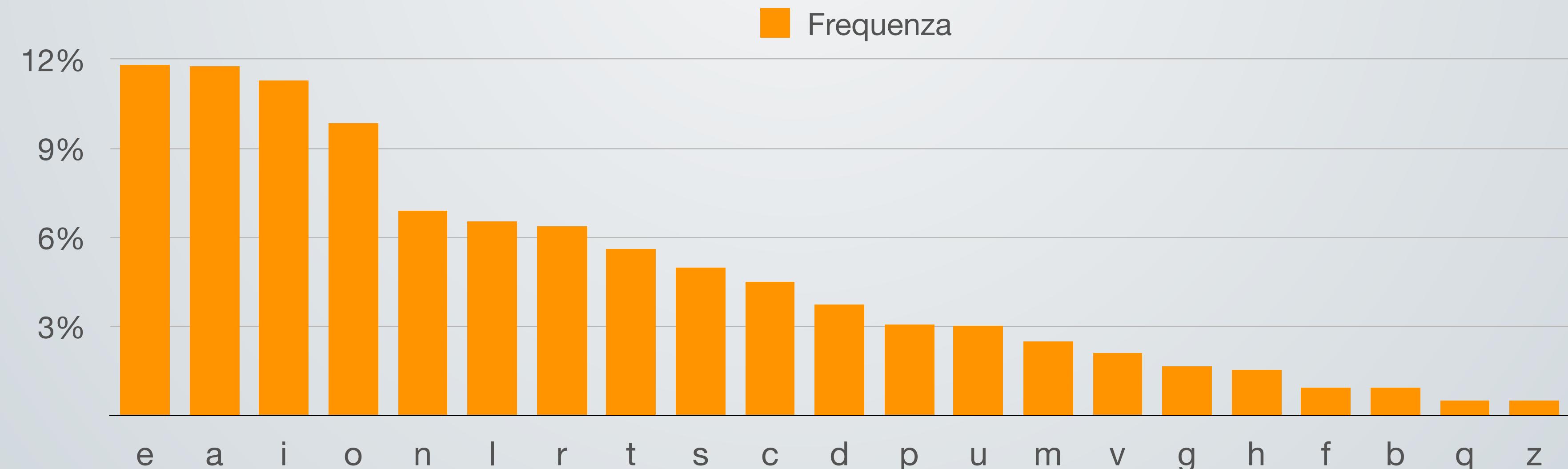
# Crittoanalisi



the cake is a lie

KOC NDPC AL D BAC

- Frequenza?
- C 3 volte
- D 2 volte
- A 2 volte



# Crittoanalisi



the cake is a lie

KOC NDPC AL D BAC

Frequenza?

C 3 volte

D 2 volte

A 2 volte

**Problema:** dipendenze statistiche nel testo.

**Conseguenza:** attacco statistico.

**Soluzione?** aumentare entropia testo cifrato.

# Cifrario polialfabetico



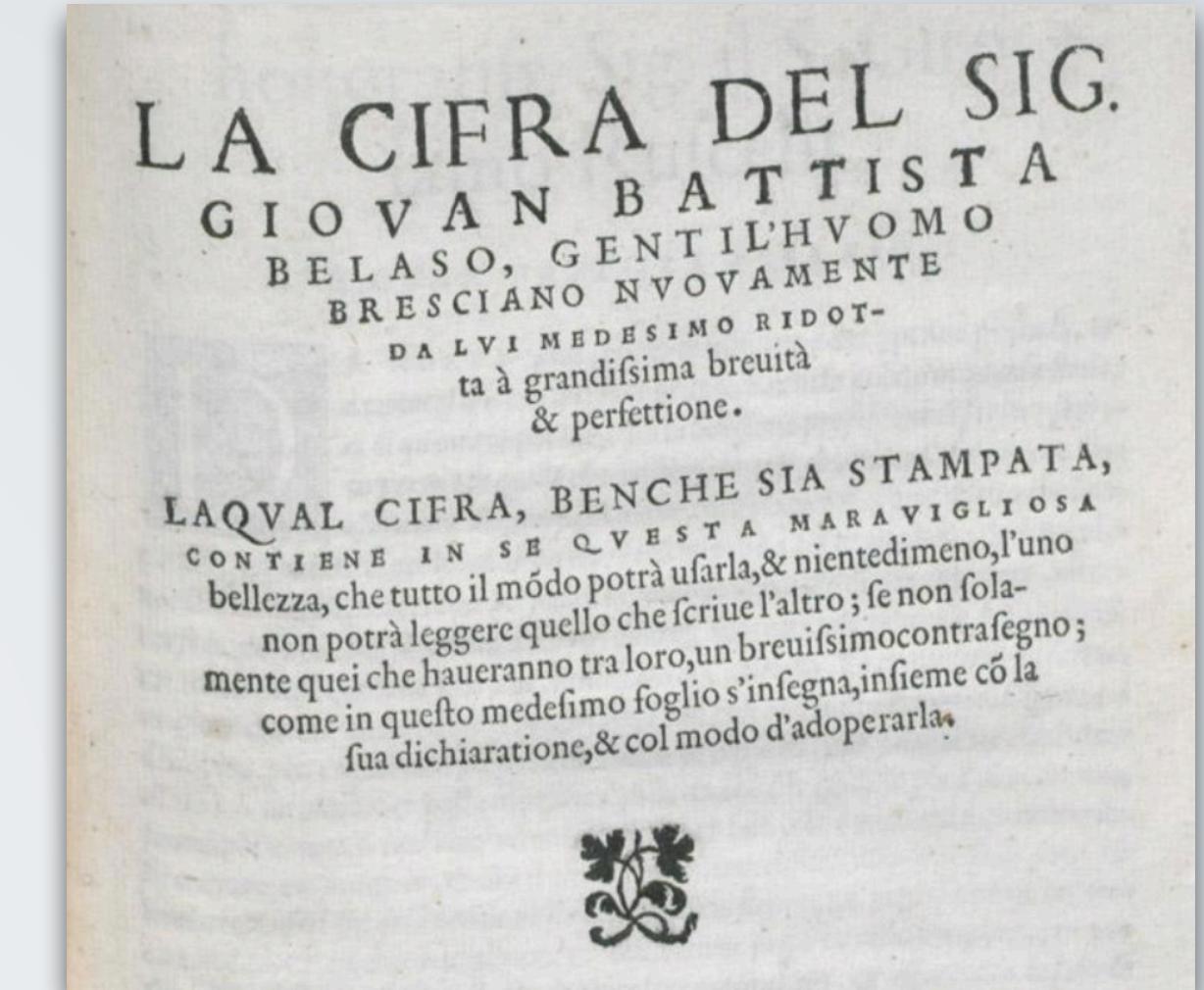
Leon Battista Alberti, 1466

# Cifrario polialfabetico



Leon Battista Alberti, 1466

- La forma definitiva del cifrario fu pubblicata da Blaise de Vigenère nel 1585 nel libro *Traicté des Chiffres* (*Trattato sulle scritture segrete*).
- Mary Stuart venne messa sotto accusa nel 1586, ma nelle sue comunicazioni usò il Cifrario di Cesare e non Vigenère.



Giovanni Battista Belaso, 1553



# Cifrario di Vigenère

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

Password: "deceptive"

Messaggio: "we are discovered, save yourselves"

wearediscoveredsaveyourselves  
deceptive deceptive deceptive de

# Cifrario di Vigenère

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

Password: "deceptive"

Messaggio: "we are discovered, save yourselves"

wearediscoveredsaveyourselves  
deceptive deceptive deceptive de  
Z

# Cifrario di Vigenère

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

Password: "deceptive"

Messaggio: "we are discovered, save yourselves"

wearediscoveredsaveyourselves  
deceptivedeceptivedeceptivede  
ZI

# Cifrario di Vigenère

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

Password: "deceptive"

Messaggio: "we are discovered, save yourselves"

wearediscoveredsaveyourselves  
deceptivedeceptivedeceptivedeceptivede  
ZIC

# Cifrario di Vigenère

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

Password: "deceptive"

Messaggio: "we are discovered, save yourselves"

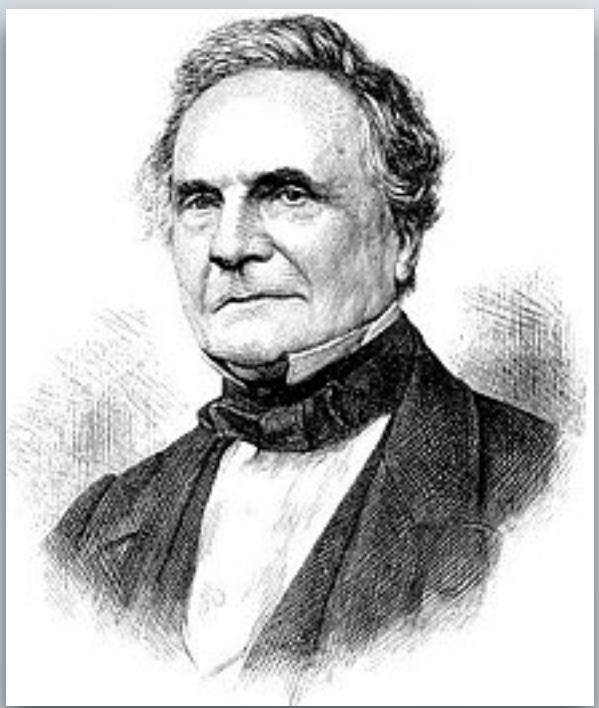
wearediscoveredsaveyourselves  
deceptive deceptivedeceptivedeceptivede  
ZICVTWQNGRZGVTWAVZH CQYGLMGZHW

La stessa lettera in punti diversi del messaggio viene cifrata con lettere diverse, a seconda della corrispondente lettera della password.

# Crittoanalisi

wearediscoveredsaveyourselves  
deceptive deceptive deceptive de  
ZICVTWQNGRZGVTAVZHCQYGLMGZHW

La ripetizione abbassa l'entropia ed è quasi sempre un punto di debolezza. A partire da questa considerazione si sviluppò un metodo sicuro di crittoanalisi.



- La crittoanalisi completa fu probabilmente effettuata da Charles Babbage nel 1854. Non fu mai pubblicata.
- Il metodo di crittoanalisi fu riscoperto in modo indipendente da Friedrich Kasiski nel 1863 (Test di Kasiski) e pubblicato nel libro *Die Geheimschriften und die Dechiffrier-Kunst* (Le scritture segrete e l'arte di decifrare).

# Test di Kasiski

WUMOGIZWYRMHMCESSVLPISCLGUILEYMV  
NGERQLLGAIQGEZKZALQUTKTAZEYHUWRLM  
ZXCHUWRMSZLBSQWCBMZIXCRFWWYWQQL  
ALQATYYZXZGRPQDAVQBZALQBTMJRZLSRB  
WOGZUVZEEYJLOYQAHEYGTQLKIDMDRMEKLP  
RMMAGYXIESEATLKMMTZNVQVZLXUALIJZQ  
ZLLRABCMTBQDMRAQESSIONUXPAGMBTRAVANF  
MEKLZVUMCYQUAPAGTQGSSFQDNEGZLAGTQ  
TMIFMNMPYIWYGUWEMPMMNMPYIWYXMHKYW  
HMRJMMCQMKSCWUIRGSDVZMKZQTQXMVEC  
YZCZKSYCZPIAOYGMEBLLXQCYSYWWYWM

**Cerchiamo nel crittogramma stringhe che si ripetono.**

# Test di Kasiski

WUMOGIZWYRMHMCESSVLPISCLLGUILLEYMV  
NGERQLLGAIQGEZKZALQUTKTAZEY**HUWR LM**  
ZWXC**HUWR LM**MSZLBSQWCBMZIXCRFWWYWQQL  
ALQATYYZXZGRPQDAVQBZALQBTMJRZLSRB  
WOGZUVZEEYJLOYQAHEYGTQLKIDMDRMEKLP  
RMMAGYXIESEATLKMMTZNVQVZLXUALIJZQ  
ZLLRABCMTBQDMRAQESSIONUXPAGMBTRAVANF  
MEKLZVUMCYQUAP**AGTQ**GSSFQDNEGZL**AGTQ**  
TMIF**MNMPYI**WYGUWEMPMM**MNMPYI**WYXMHKYW  
HMRJMMCGQMKSCHUIRGSDVZMKZQTQXMVEC  
YZCZKSYCZPIAOYGMEBLLXQCYSYWWYWM

Cerchiamo nel crittogramma stringhe che si ripetono.

# Test di Kasiski

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

**HUWRLM**



1. chiave di 1 lettera che compie 10 cicli tra le ripetizioni;
2. chiave di 2 lettere che compie 5 cicli tra le ripetizioni;
3. chiave di 5 lettere che compie 2 cicli tra le ripetizioni;
4. chiave di 10 lettere che compie 1 ciclo tra le ripetizioni.

# Test di Kasiski

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

Stringa	Distanza	Possibile lunghezza della chiave													
		2	3	4	5	6	7	8	9	10	11	12	13	14	15
HUWRLM	10	✓			✓					✓					
AGTQ	15		✓		✓									✓	
MNMPYI	15		✓		✓									✓	

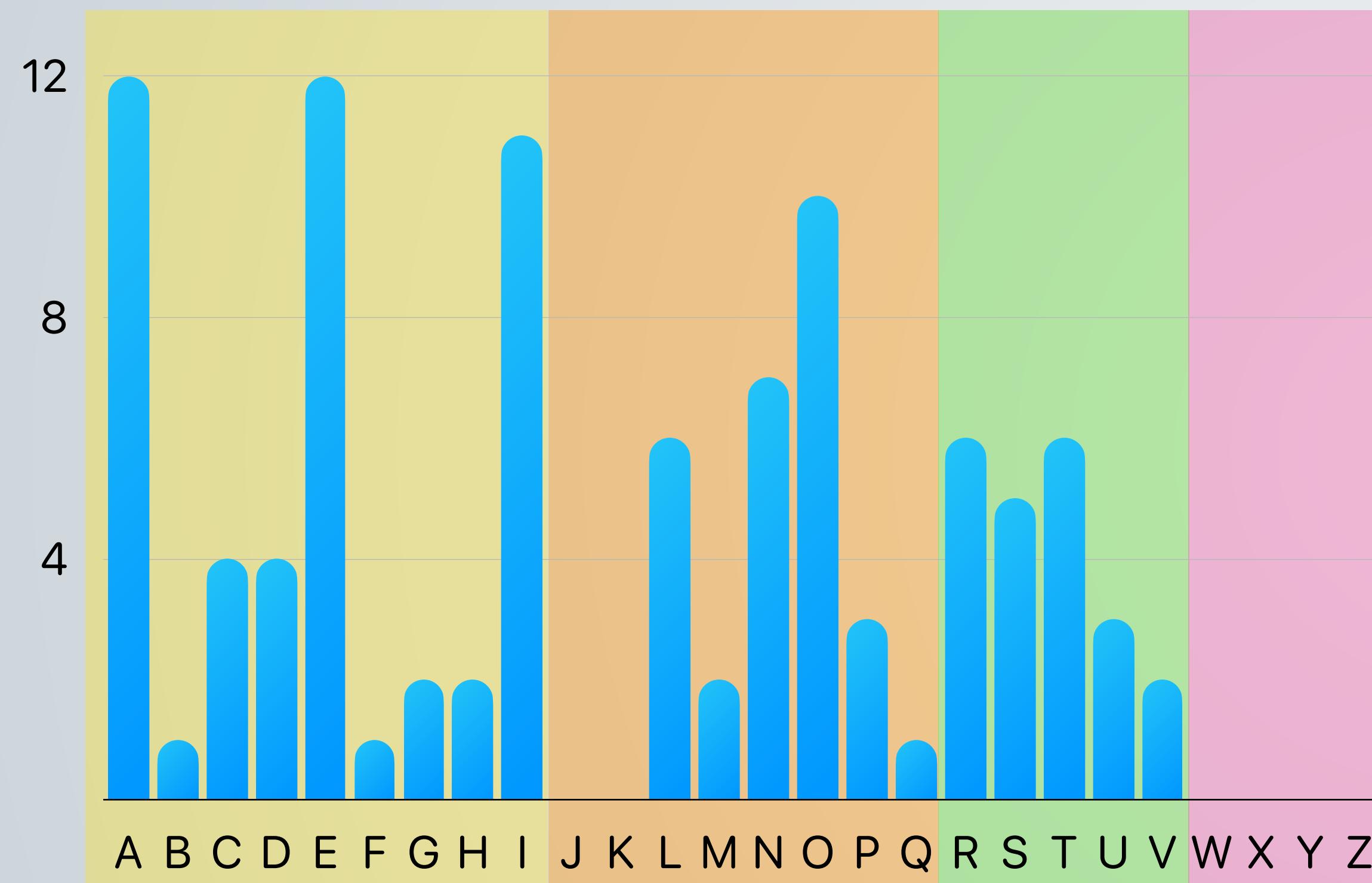
# Test di Kasiski

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

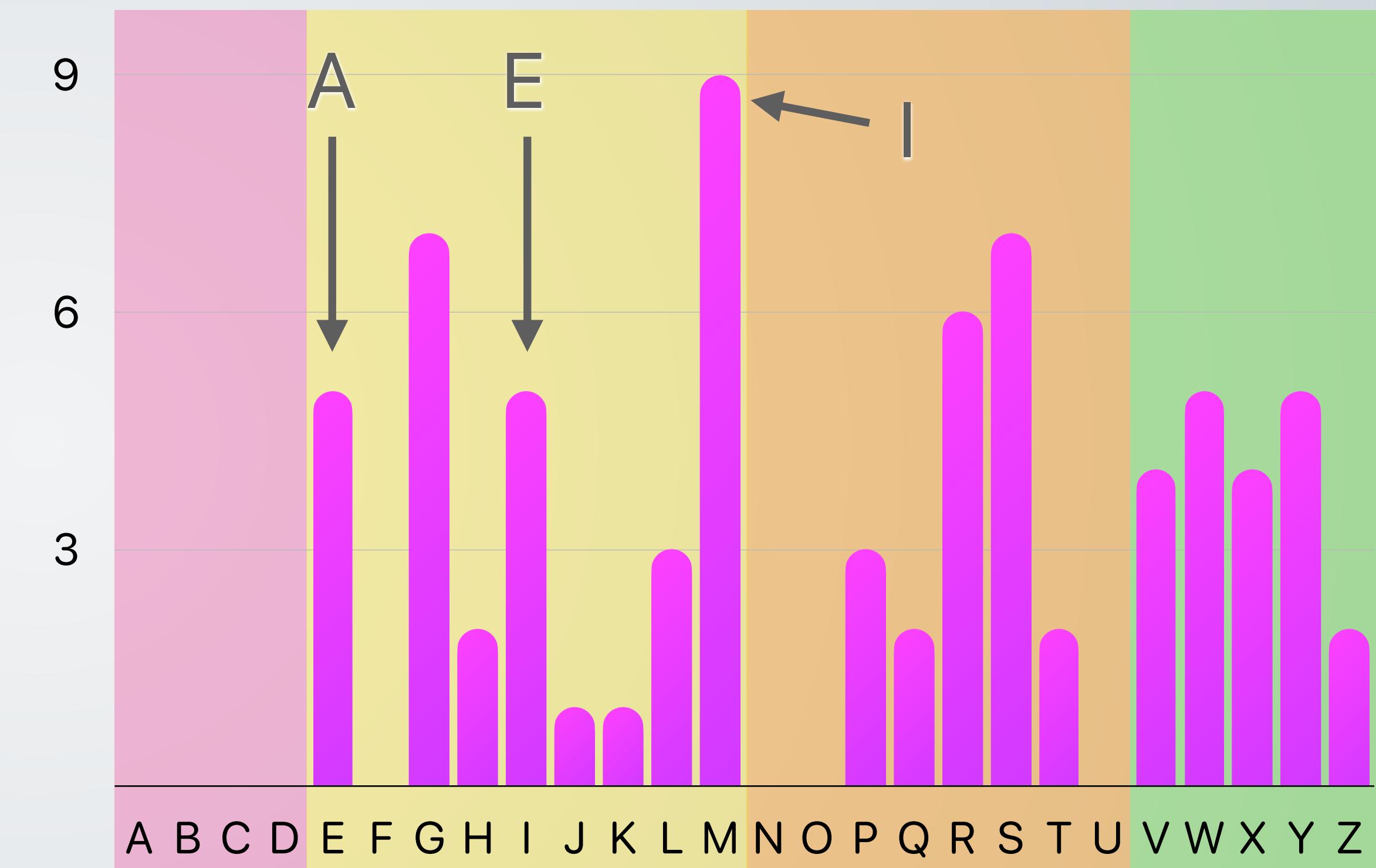
Tutti i multipli della prima lettera della chiave  $k_1$  formano un cifrario monoalfabetico a sé stante, attaccabile con l'analisi statistica.

# Test di Kasiski

Istogramma lingua italiana



Istogramma del crittogramma



Sequenza di 4 lettere poco probabili

Possiamo ipotizzare che  $k_1 = 4$  e dunque che la prima lettera della password sia E.

# Test di Kasiski

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

I multipli della seconda lettera della chiave  $k_2$  formano un secondo cifrario monoalfabetico.  
Il procedimento di analisi è il medesimo del precedente e si può facilmente giungere alla  
conclusione che  $k_2 = 12$  e dunque che la seconda lettera della password è **M**.

# Test di Kasiski

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

Proseguendo l'analisi con tutti gli altri gruppi di lettere otterremo la password **EMILY**, che decifra correttamente il testo.

# Test di Kasiski

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

Proseguendo l'analisi con tutti gli altri gruppi di lettere otterremo la password **EMILY**, che decifra correttamente il testo.

# Test di Kasiski

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

Proseguendo l'analisi con tutti gli altri gruppi di lettere otterremo la password **EMILY**, che decifra correttamente il testo.

Siedi e non ti vergognare  
guancia a guancia, fianco a fianco  
che m importa di ogni nome  
di ogni grado e ordinamento?  
lascia che sia un po indiscreto  
che ti offra un po di vino  
gamba questa chiameresti?  
scarna e piu la tua o la mia?  
l'opre non ti salveranno  
troppi sono i tuoi peccati  
tronchi scabri e rami secchi  
vuoti spaurocchi, io e te!  
colma la ciotola e colma la tazza  
sveglia, prima che sia giorno  
ogni istante un uomo muore  
ogni istante un uomo nasce.



Alfred Tennyson, *Vision of sin*, 1842

# Ottocento: la crittografia militare

1800

1831 Telegrafo

1835 Codice Morse

1854 Playfair cipher

1855 Babbage decifra Vigenère

1883 Principi di Kerckhoffs

1885 Cifrario Beale

- Il sistema deve essere praticamente, se non matematicamente, **indecifrabile**.
- Il sistema **non deve essere segreto**, dev'essere in grado di cadere nelle mani del nemico senza inconvenienti.
- La sua **chiave deve essere comunicabile** senza l'aiuto di note scritte, e modificabile o modificabili a piacimento dei corrispondenti.
- Deve essere applicabile alla corrispondenza **telegrafica**.
- Deve essere portatile e il suo utilizzo e uso non deve richiedere il concorso di più persone.
- È necessario che la sua applicazione sia **facile da usare** e che non richieda la conoscenza e l'uso di una lunga serie di regole.



# La meccanizzazione dei cifrari

# l mécanicien

---

Descartes  
(1662)

La Mettrie  
(1784)



René Descartes  
*De Hominem* (1662)



Julien de La Mettrie  
*L'homo machine* (1748)

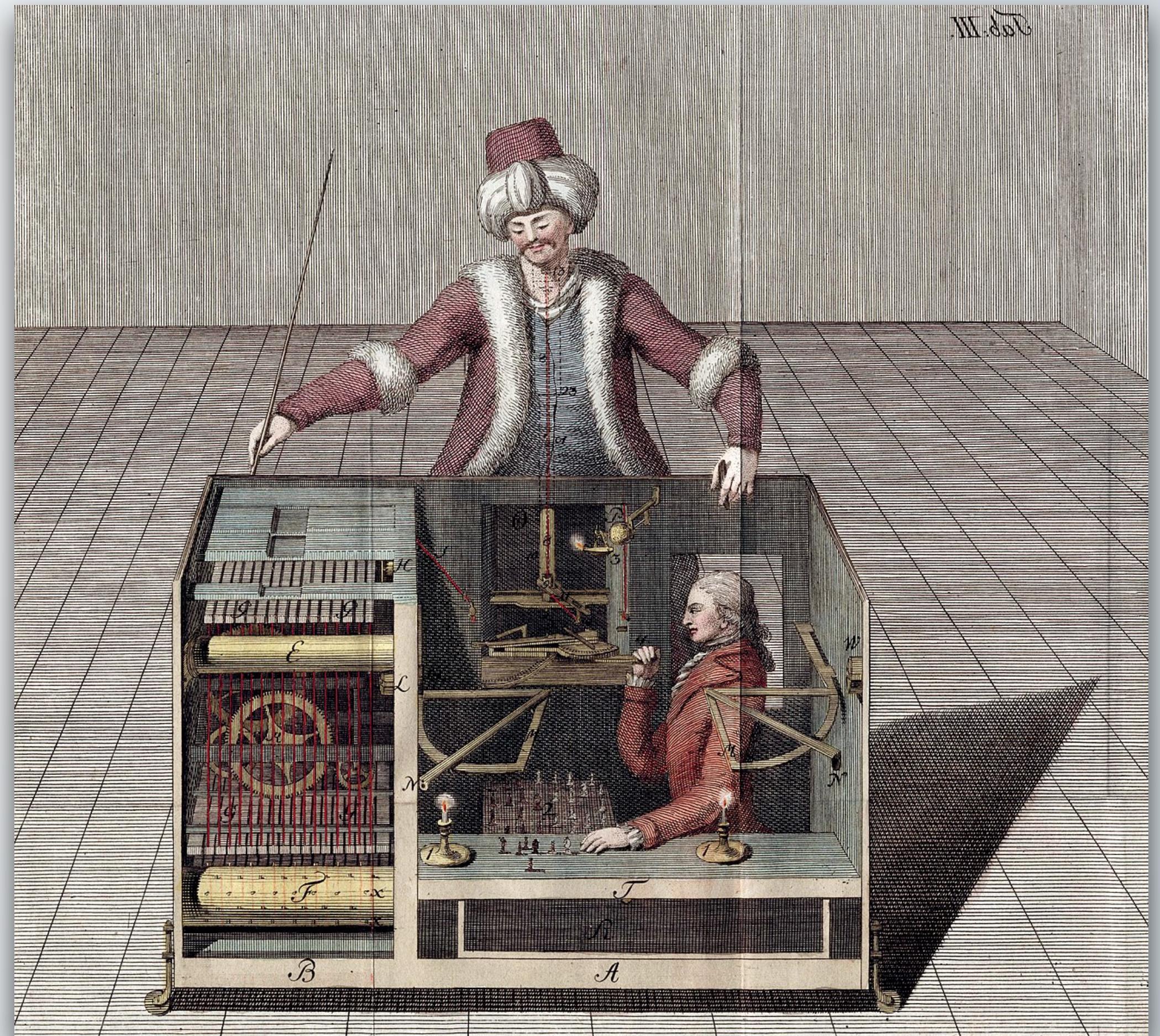
# l mécanicien

Descartes  
(1662)

La Mettrie  
(1784)

von Kempelen  
(1769)

Wolfgang von Kempelen  
*// Turco* (1769)



# l mécanicien

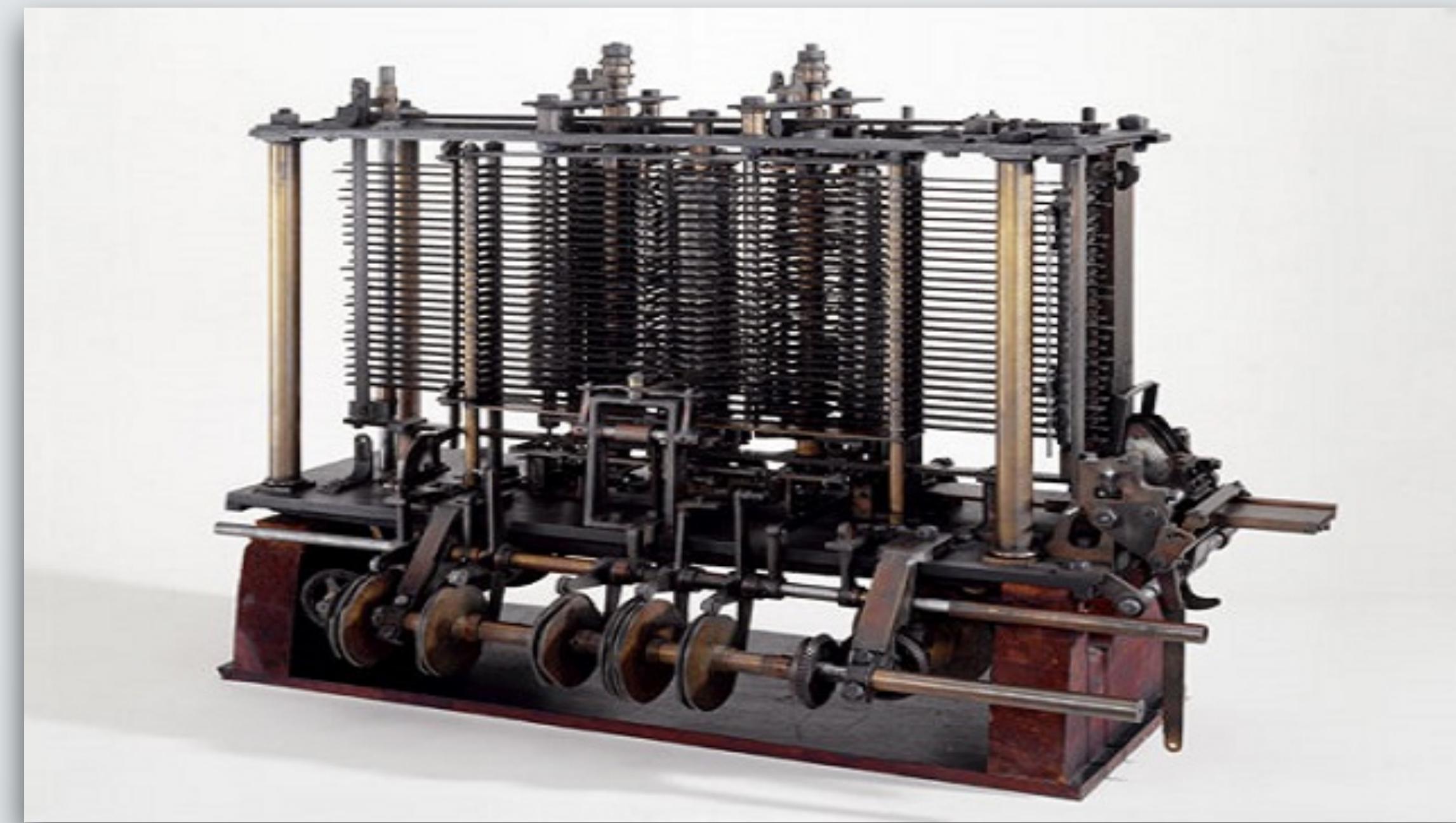


Descartes  
(1662)

La Mettrie  
(1784)

von Kempelen  
(1769)

Babbage  
(1837)



Charles Babbage  
*Macchina Analitica* (1837)

# I mécanicien



Descartes  
(1662)

La Mettrie  
(1784)

von Kemplen  
(1769)

Babbage  
(1837)

Sholes e Glidden  
(1874)



Sholes e Glidden  
*Remington n°1 (1874)*

# Le macchine cifranti



Discret, 1899

Dr. Friedrich Rehmann, Karlsruhe (Germania)

Foto: [www.cryptomuseum.com](http://www.cryptomuseum.com)

# Novecento: le Guerre Mondiali



TypeX



SIGABA



Enigma





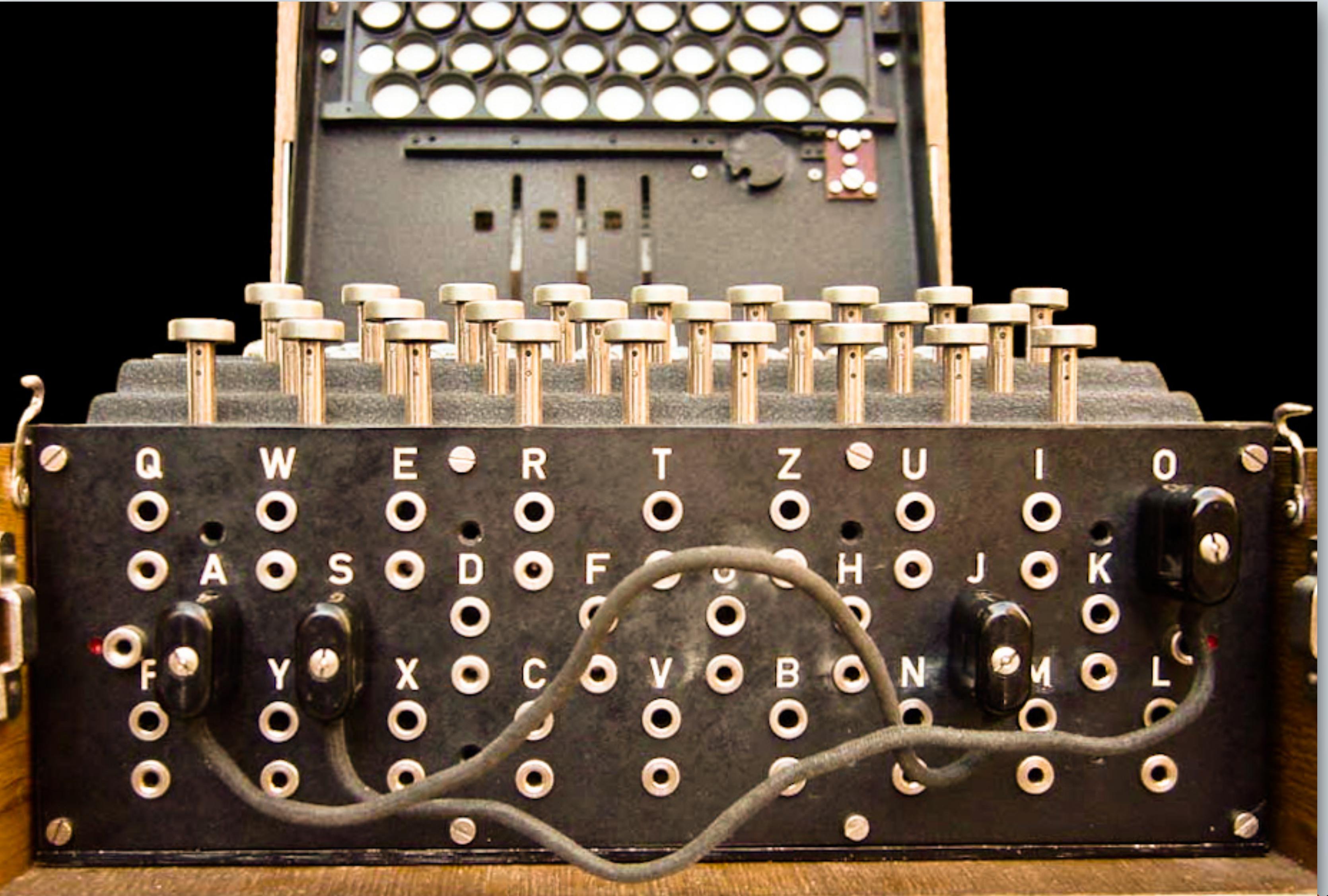
# La macchina Enigma



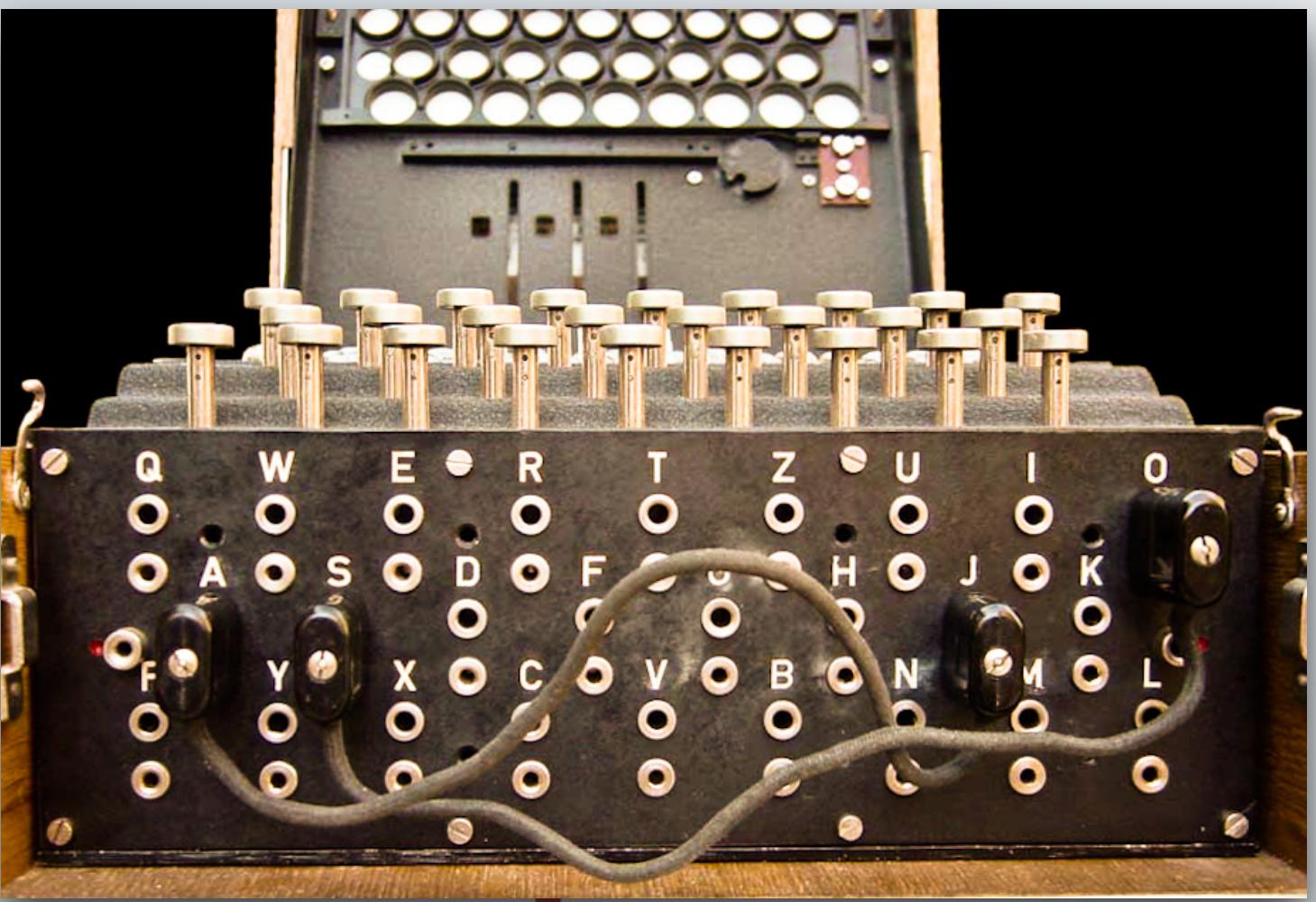
# La macchina Enigma



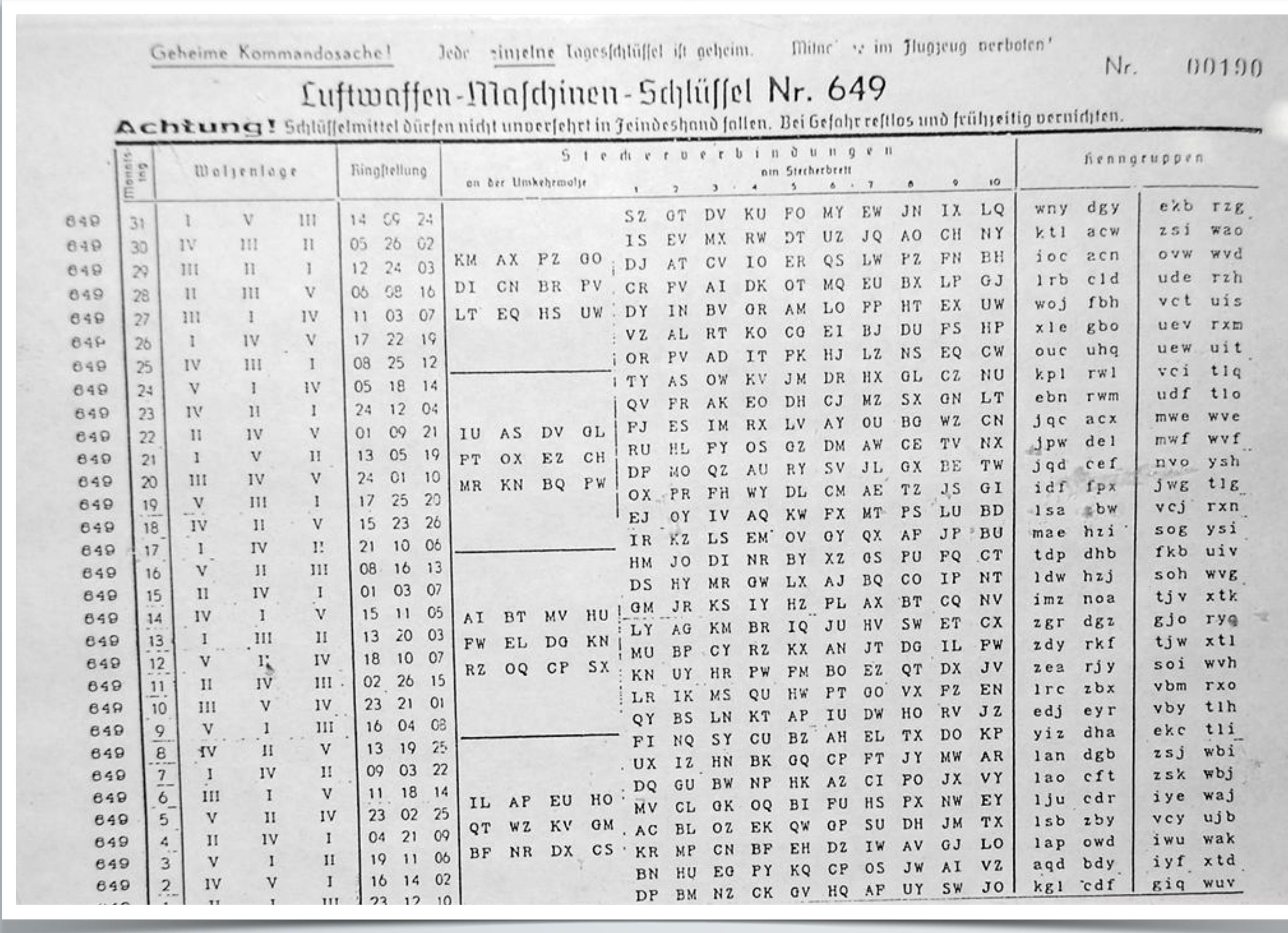
# La macchina Enigma



# La macchina Enigma



# Le chiavi crittografiche di Enigma



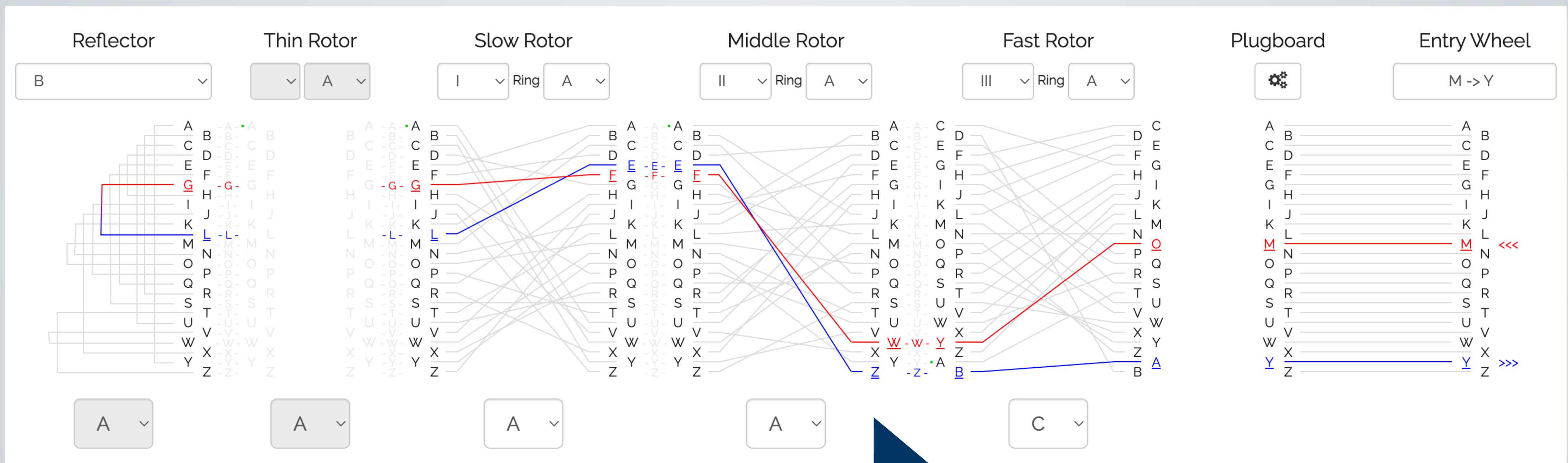
# Secret Command Document!

Every individual daily key is secret.  
Forbidden to bring on aircraft.

# Luftwaffe Machine Key Nr.649

Attention! Key material must not fall into enemy hands intact. In case of danger destroy thoroughly and early.

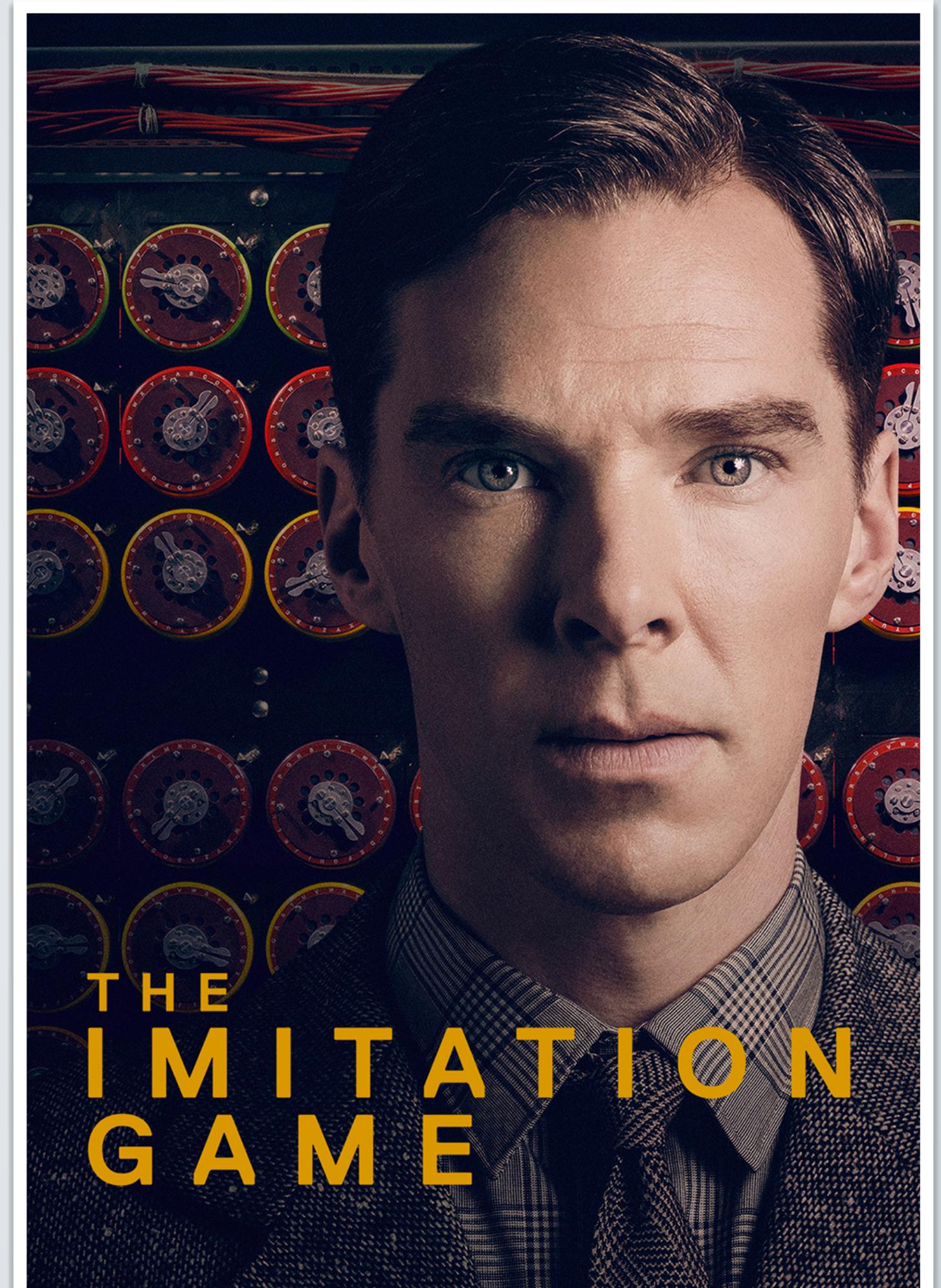
# Live demo



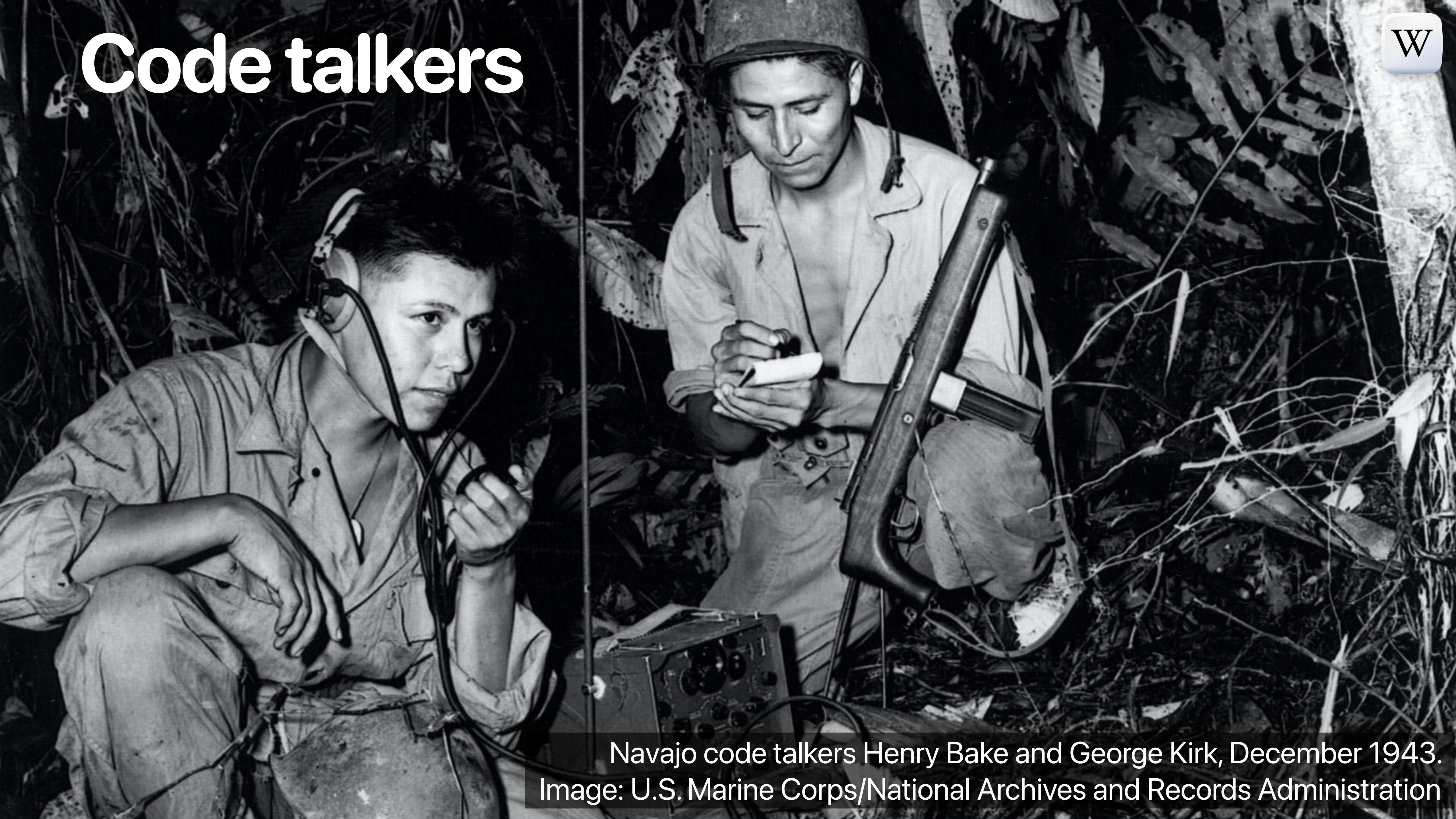
# Bletchley Park



The only known picture of the gathering known as Captain Ridley's shooting party. Photograph: Bletchley Park Trust



# Code talkers



Navajo code talkers Henry Bake and George Kirk, December 1943.  
Image: U.S. Marine Corps/National Archives and Records Administration

ÁLA'IH, DO'NEH'LINI,  
DO'NEH'LINI, ÁLA'IH,  
ÁLA'IH, DO'NEH'LINI,  
DO'NEH'LINI, DO'NEH'LINI,  
ÁLA'IH, ÁLA'IH,  
DO'NEH'LINI, ÁLA'IH,  
DO'NEH'LINI, DO'NEH'LINI,  
DO'NEH'LINI . . .

FOR ADDED SECURITY, AFTER  
WE ENCRYPT THE DATA STREAM,  
WE SEND IT THROUGH OUR  
NAVAJO CODE TALKER.

| ... IS HE JUST USING  
| NAVAJO WORDS FOR  
| "ZERO" AND "ONE"?

| WHOA, HEY, KEEP  
| YOUR VOICE DOWN!



[originale]

[spiegazione]