

Introduzione alla crittografia

Sicurezza informatica

v 2.3 ~ mag 2021



Prof. Marco Farina

marco.farina@its-ictpiemonte.it
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.

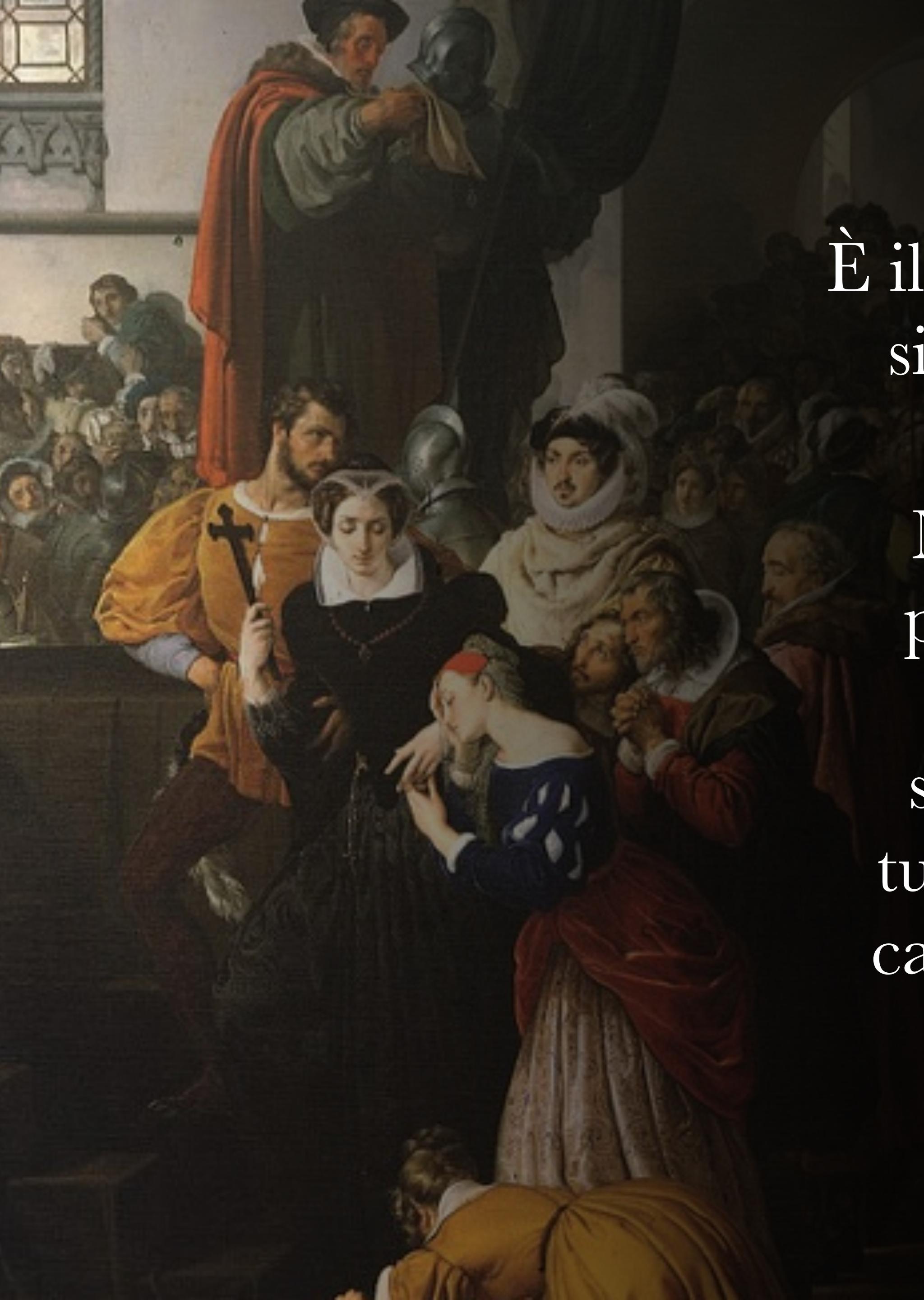
Mary, Regina degli scozzesi, è accusata di tradimento: avrebbe partecipato a un complotto mirante a sopprimere Elisabetta e a porla sul trono d'Inghilterra al posto dell'uccisa.



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.

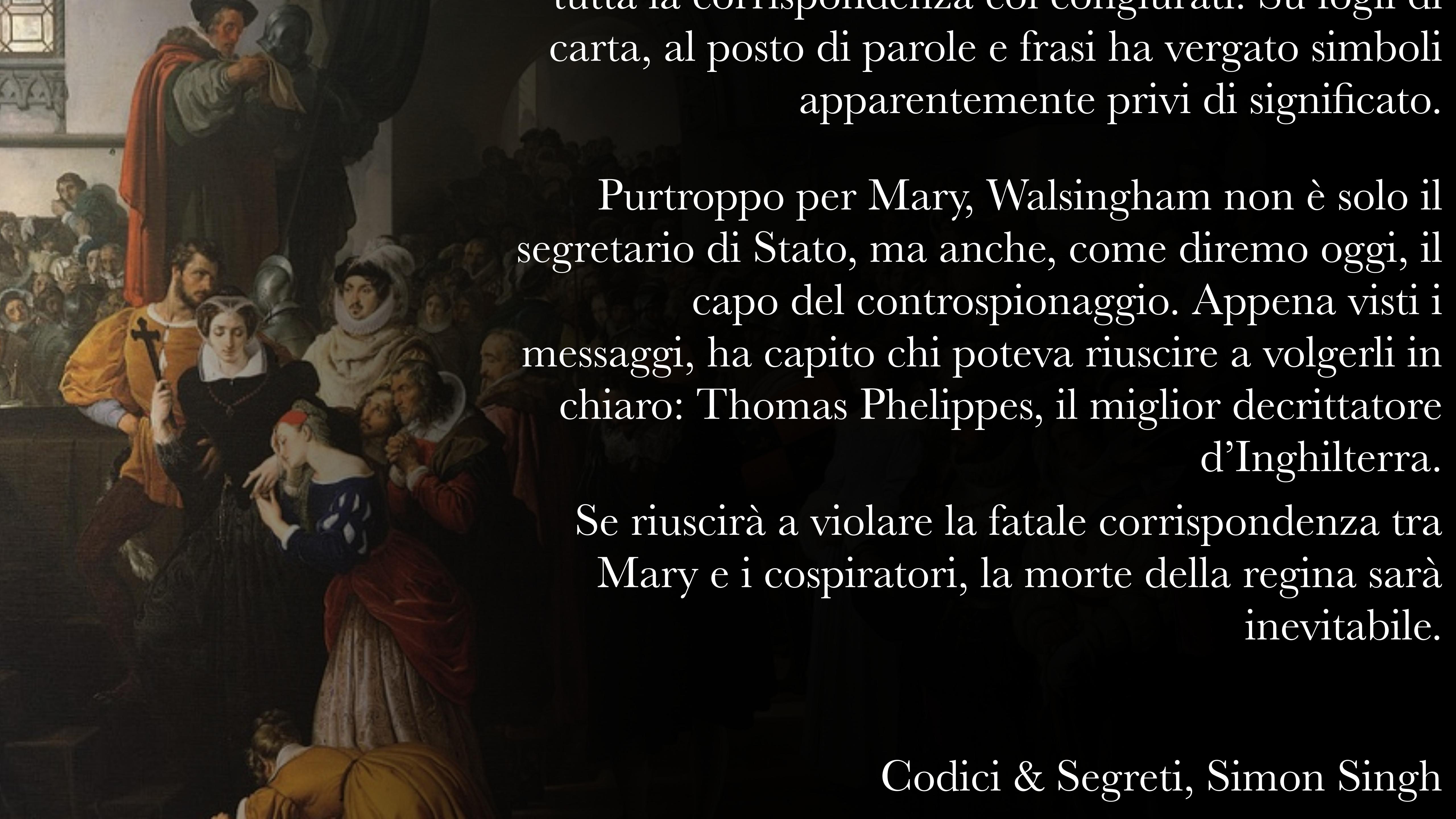
In primo luogo Mary è regina di Scozia, e molti dubitano che mandare a morte il capo di un paese straniero rientri nei poteri di un tribunale inglese. In secondo luogo, l'esecuzione può creare un pericoloso precedente: se uno Stato si arroga il diritto di sopprimere il monarca, i capi di un'eventuale 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

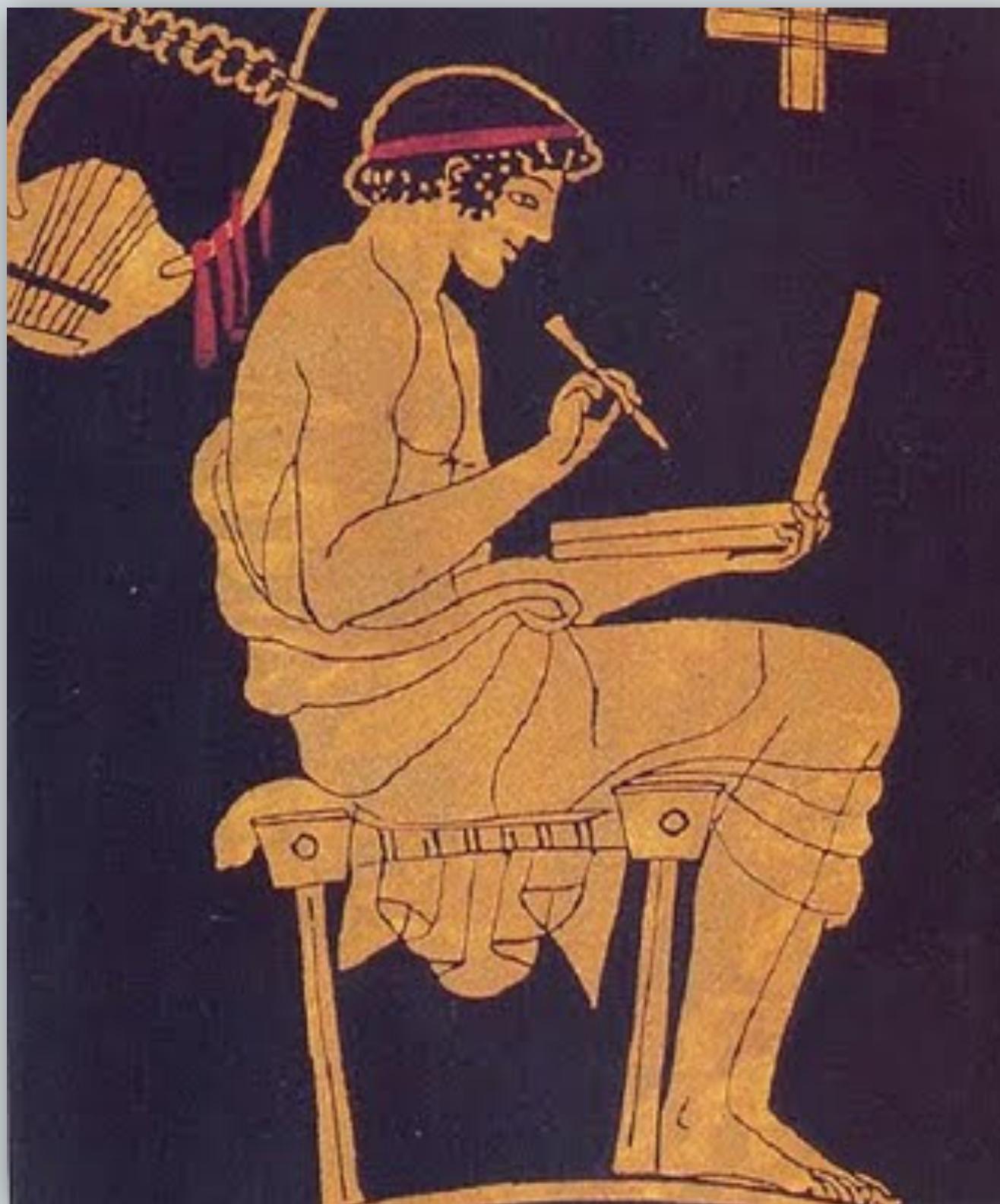
(immaginate di ascoltare l'Aria sulla quarta corda)

Steganografia



Demarato di Sparta
(-480)

Steganografia



Demarato di Sparta
(-480)



Istieo di Mileto
(-499)

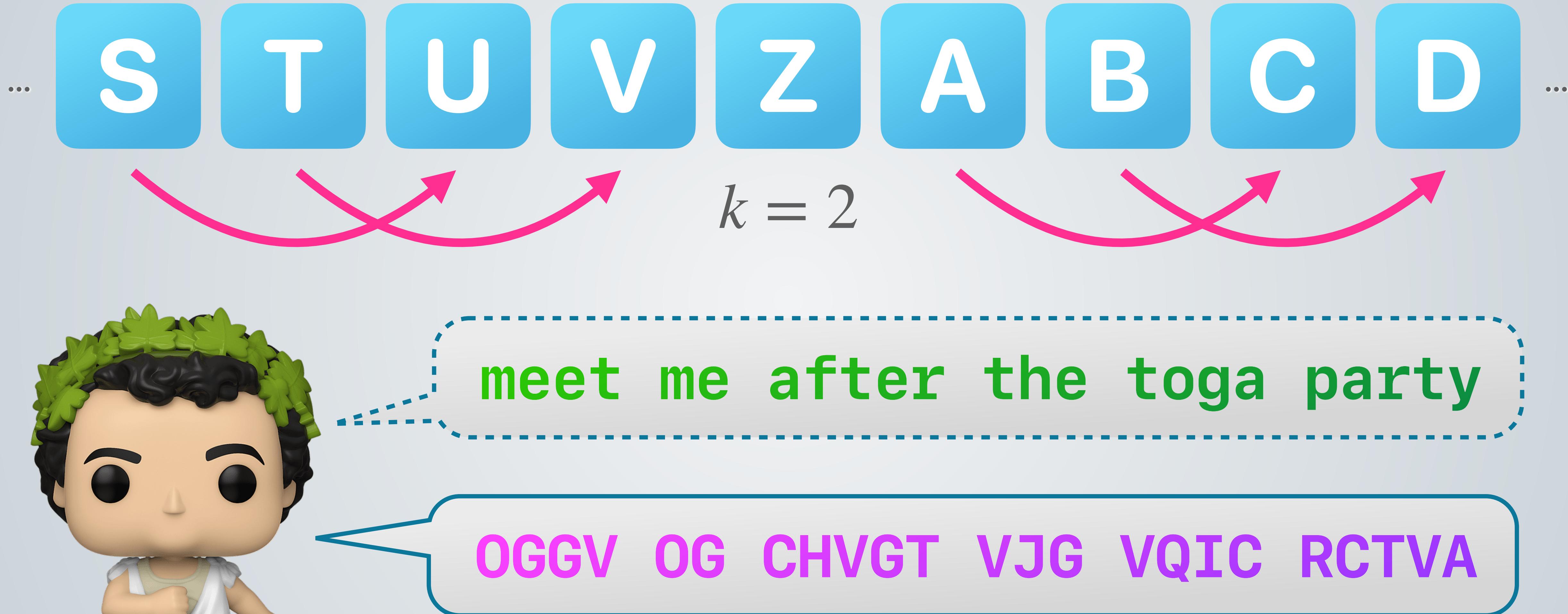
Crittografia



Decrittografia



Il Cifrario di Cesare



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 Σ costituisce la chiave crittografica.

Quanto è grande lo spazio delle chiavi?

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

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

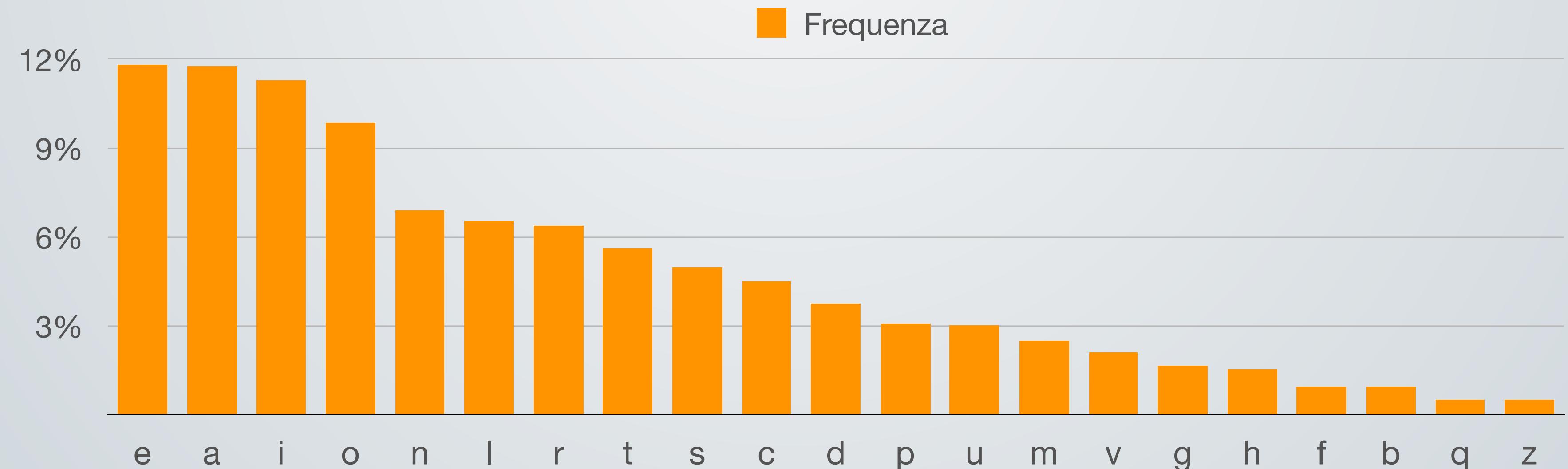
Crittoanalisi



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

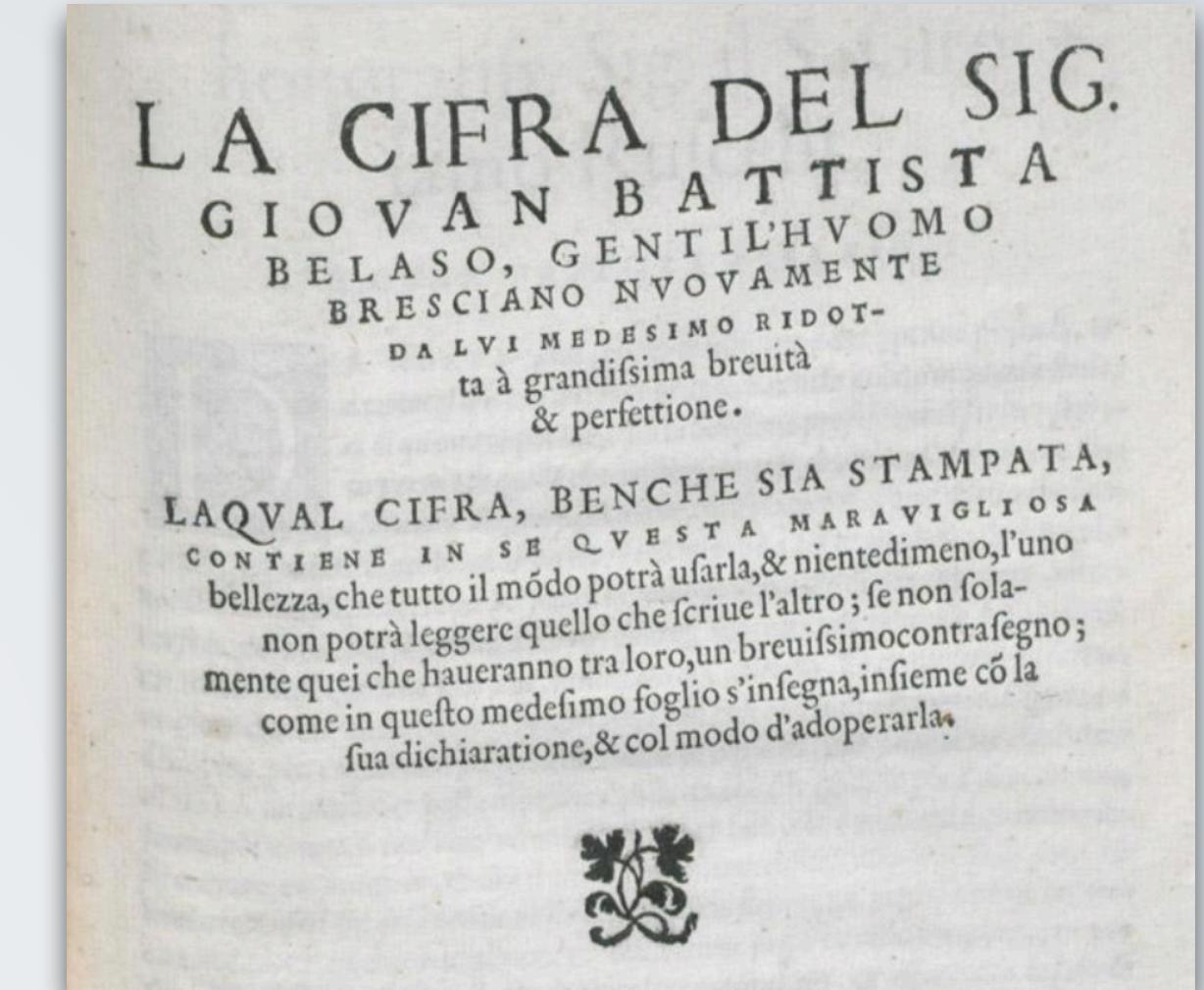


Leon Battista Alberti, 1466

Cifrario polialfabetico



Leon Battista Alberti, 1466



Giovanni Battista Bellaso, 1553

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

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 dective dectivedeceptivede

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

deceptivedeceptivedeceptivede

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"

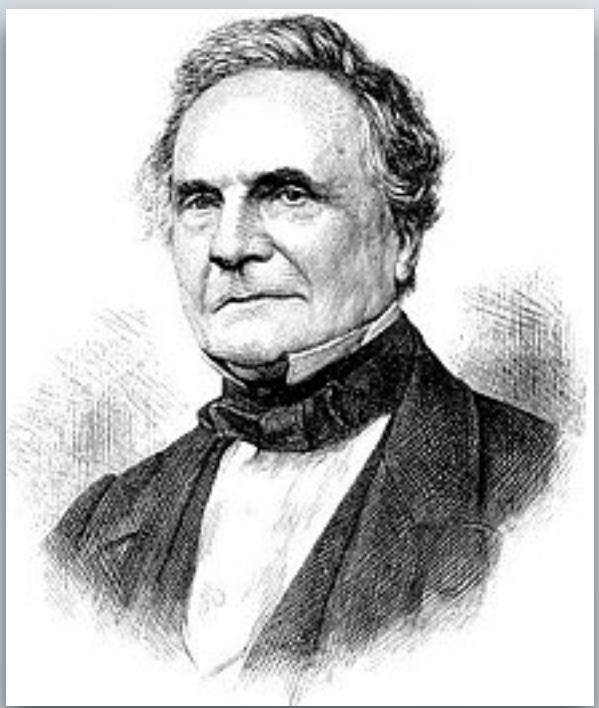
wearediscoveredsaveyourselves
deceptive deceptivedeceptivedeceptivede
ZICVTWQNGRZGVTWAVZH CQYGLMGZHW

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
ZICVTWQNGRZGVTWAVZHCQYGLMGZHW

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

WUMOGIZWYRMHMCESSVLPISCLLGUILLEYMV
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		✓		✓									✓	

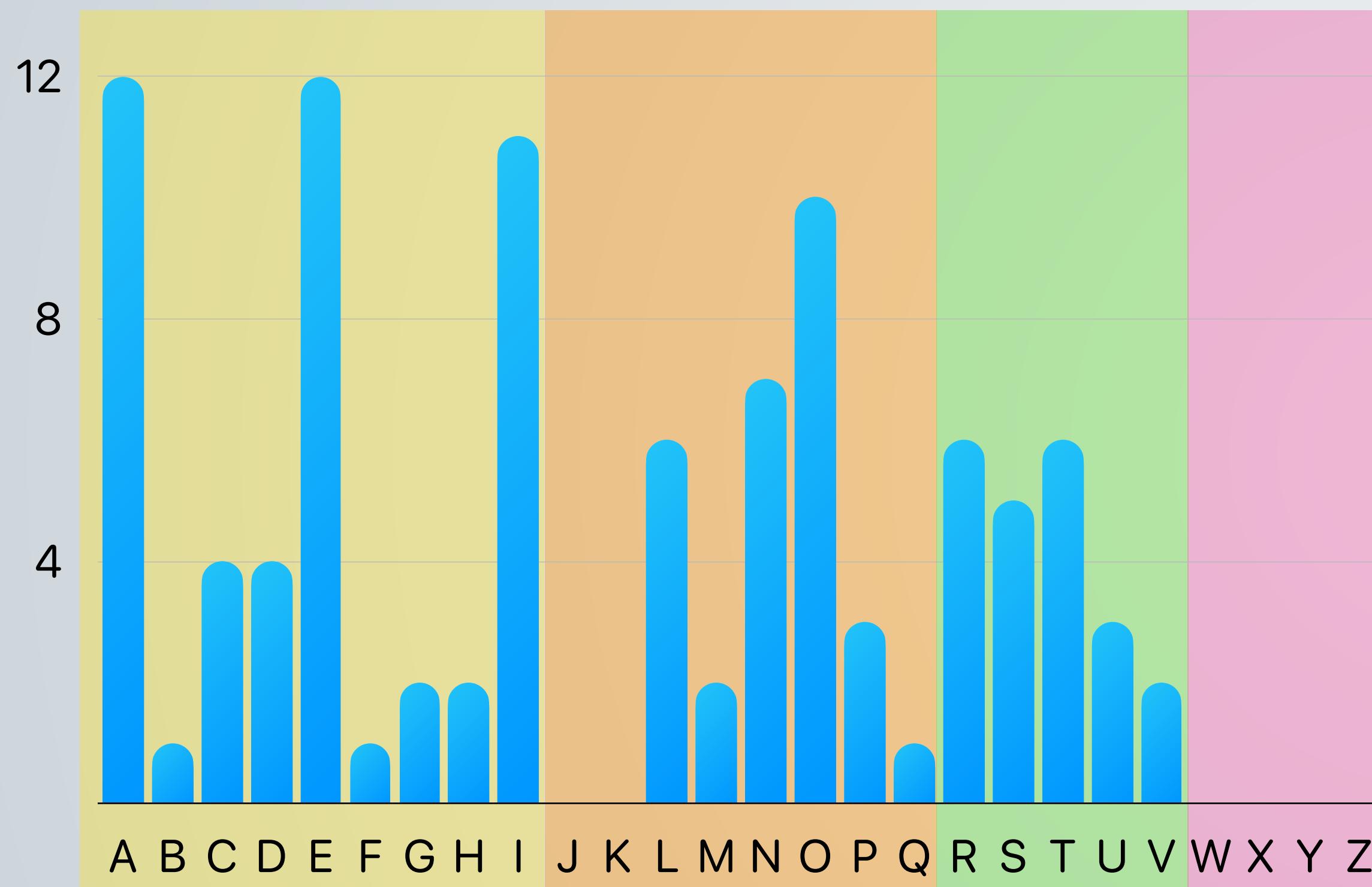
Test di Kasiski

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

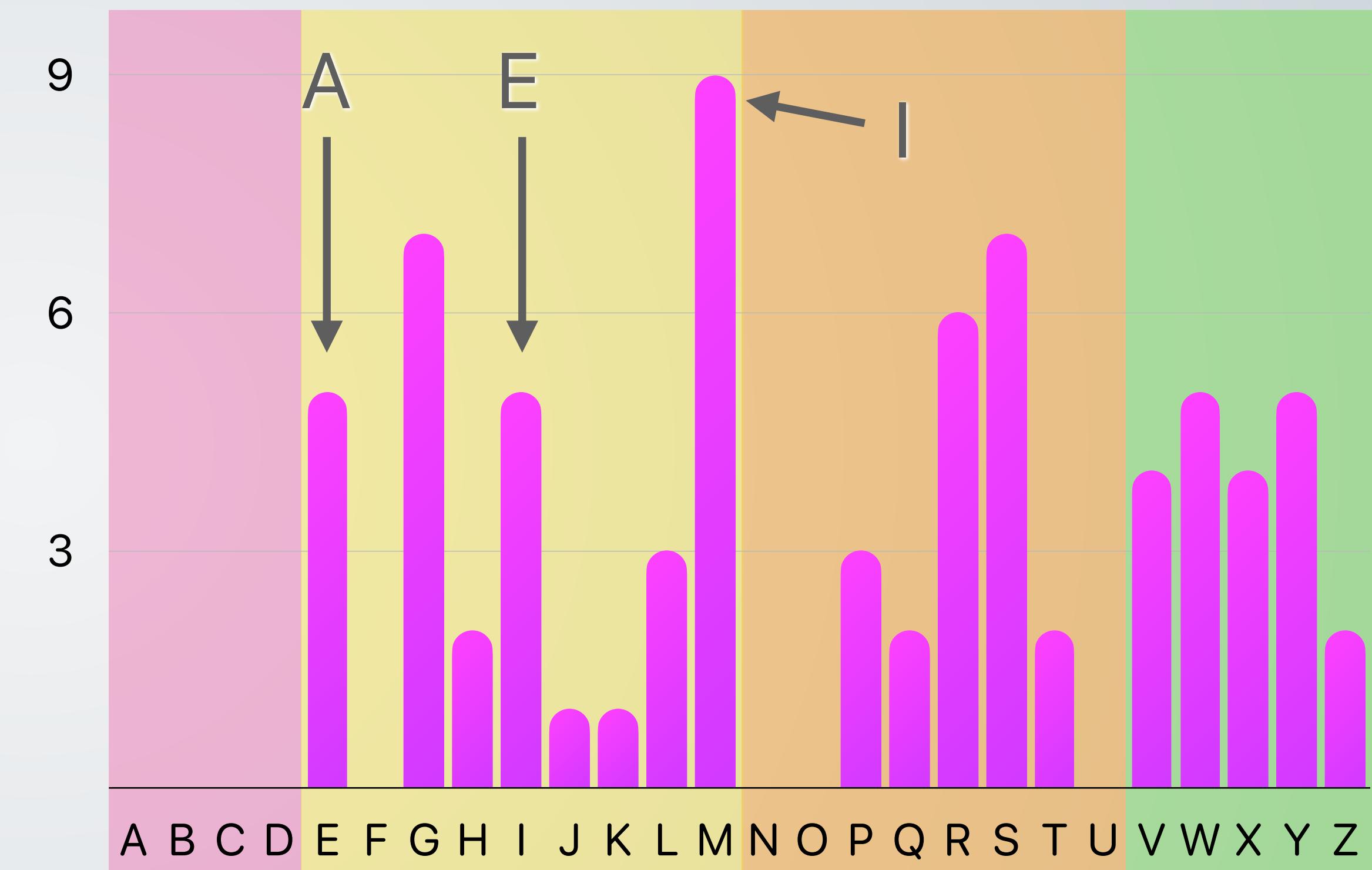
Tutti i multipli della prima lettera della chiave k_1 formano un cifrario monoalfabetico a sé stante, attaccabile con l'analisi statistica.

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.

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 della crittografia

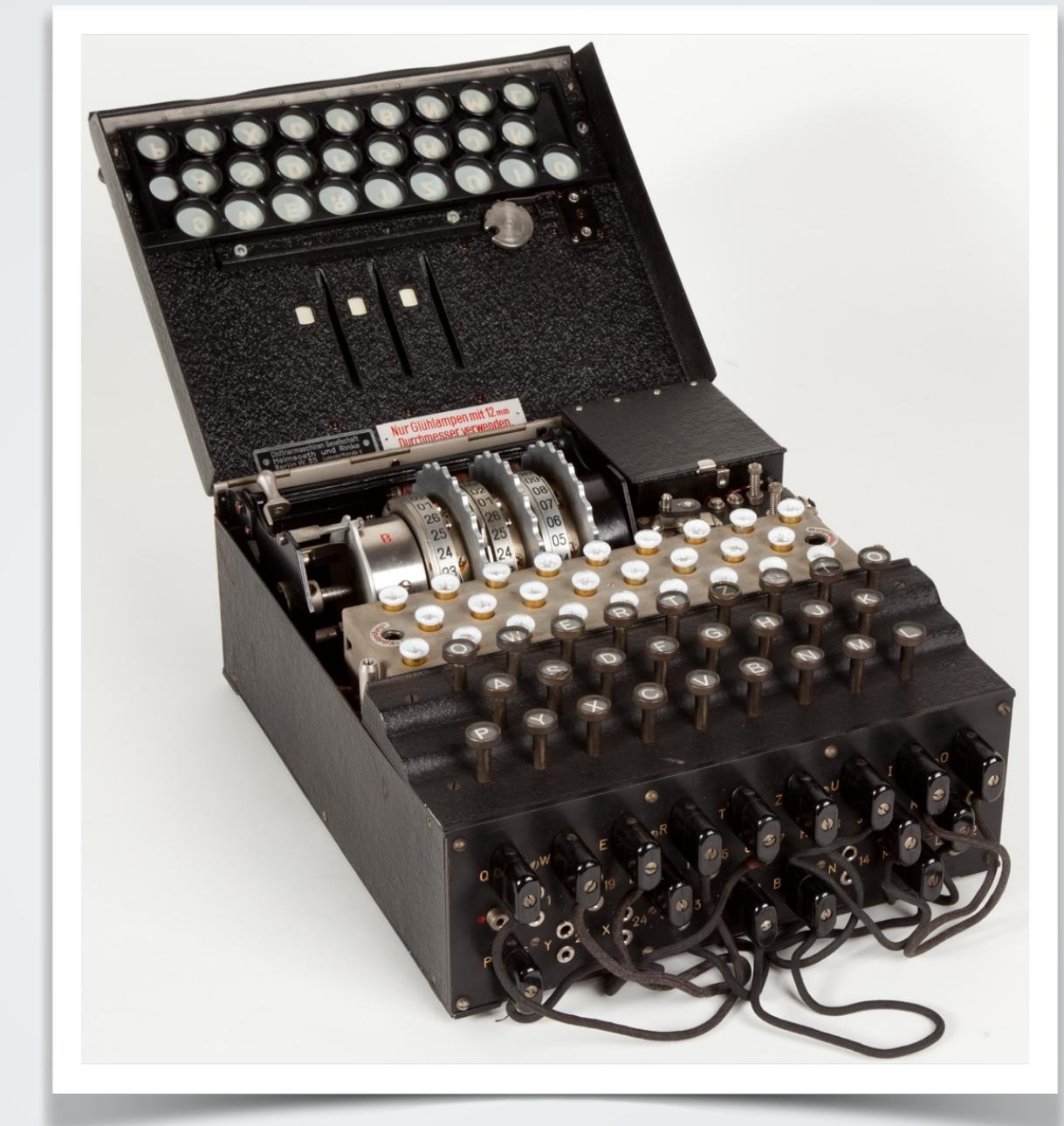


W

Seconda Guerra Mondiale



TypeX



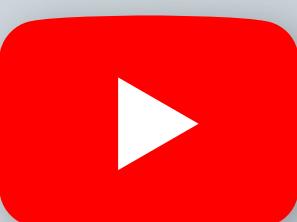
Enigma



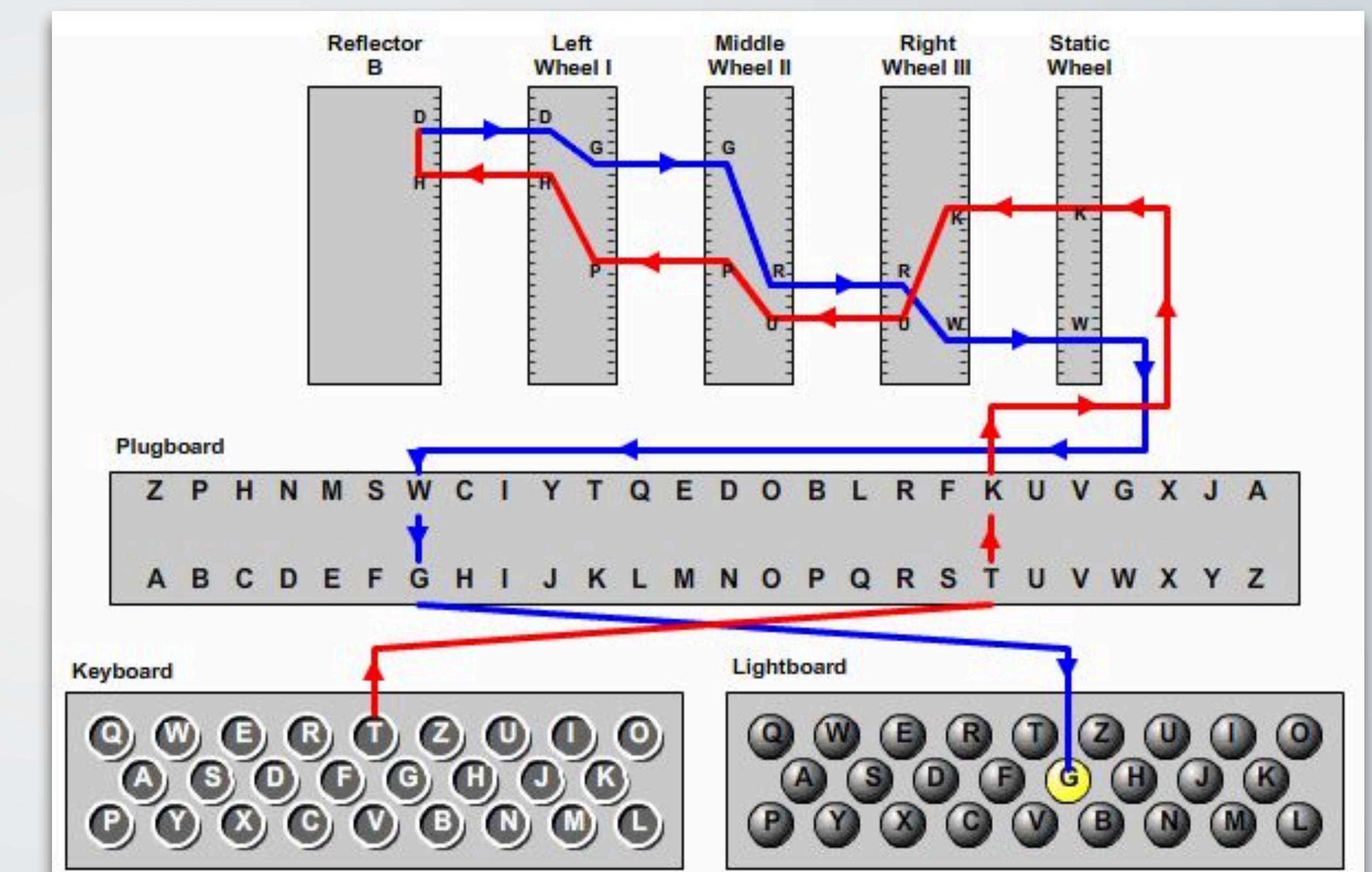
SIGABA



Foto: www.cryptomuseum.com



La macchina Enigma



Le chiavi crittografiche di Enigma

Geheime Kommandosache! Jede einzelne Tageschlüssel ist geheim. Minen & im Flugzeug verboten!				Nr. 00190																					
Luftwaffen-Maschinen-Schlüssel Nr. 649																									
Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.																									
Muttertag	Wellenlage	Ringstellung	Steckerverbindungen am Steckerbrett										Nenngruppen												
			an der Umkehrrolle	1	2	3	4	5	6	7	8	9	10												
649	31	I	V	III	14	09	24	SZ	GT	DV	KU	FO	MY	EW	JN	IX	LQ	wny	dgy	ekb	rzg				
649	30	IV	III	II	05	26	02	IS	EV	MX	RW	DT	UZ	JQ	AO	CH	NY	ktr	acw	zsi	wao				
649	29	III	II	I	12	24	03	KM	AX	PZ	GO	DJ	AT	CV	IO	ER	QS	LW	FZ	FN	BH	ioc	acn		
649	28	II	III	V	06	08	16	DI	CN	BR	PV	CR	FV	AI	DK	OT	MQ	EU	BX	LP	GJ	lrb	cld		
649	27	III	I	IV	11	03	07	LT	EQ	HS	UW	DY	IN	BV	GR	AM	LO	PP	HT	EX	UW	woj	fbh		
649	26	I	IV	V	17	22	19	VZ	AL	RT	KO	CG	EI	BJ	DU	FS	HP	xle	gbo	uev	rxm				
649	25	IV	III	I	08	25	12	OR	PV	AD	IT	PK	HJ	LZ	NS	EQ	CW	ouc	uhq	uew	uit				
649	24	V	I	IV	05	18	14	TY	AS	OW	KV	JM	DR	HX	GL	CZ	NU	kpl	rw1	vci	tlq				
649	23	IV	II	I	24	12	04	QV	FR	AK	EO	DH	CJ	MZ	SX	GN	LT	ebn	rwm	udf	tlo				
649	22	II	IV	V	01	09	21	FJ	ES	IM	RX	LV	AY	OU	BG	WZ	CN	jqc	acx	mwe	wve				
649	21	I	V	II	13	05	19	RU	HL	FY	OS	GZ	DM	AW	CE	TV	NX	jpw	del	mwf	wvf				
649	20	III	IV	V	24	01	10	DF	MO	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh				
649	19	V	III	I	17	25	20	OX	PR	FH	WY	DL	CM	AE	TZ	JS	GI	idr	fpk	jwg	tlg				
649	18	IV	II	V	15	23	26	EJ	OY	IV	AQ	KW	FX	MT	PS	LU	BD	lsa	bw	vcj	rxn				
649	17	I	IV	II	21	10	06	IR	KZ	LS	EM	OV	OY	QX	AP	JP	BU	mae	hzi	sog	ysi				
649	16	V	II	III	08	16	13	HM	JO	DI	NR	BY	XZ	GS	PU	FQ	CT	tdp	dhb	fkb	uiv				
649	15	II	IV	I	01	03	07	DS	HY	MR	GW	LX	AJ	BQ	CO	IP	NT	ldw	hzj	soh	wvg				
649	14	IV	I	V	15	11	05	GM	JR	KS	IY	HZ	PL	AX	BT	CQ	NV	imz	noa	tjv	xtk				
649	13	I	III	II	13	20	03	LY	AG	KM	BR	IQ	JU	HV	SW	ET	CX	zgr	dgz	gjo	ryq				
649	12	V	I	IV	18	10	07	MU	BP	CY	RZ	KX	AN	JT	DG	IL	FW	zdy	rkf	tjw	xtl				
649	11	II	IV	III	02	26	15	KN	UY	HR	PW	FM	BO	EZ	QT	DX	JV	zea	rjy	soi	wvh				
649	10	III	V	IV	23	21	01	LR	IK	MS	QU	HW	PT	GO	VX	FZ	EN	lrc	zbx	vbm	rxo				
649	9	V	I	III	16	04	08	QY	BS	LN	KT	AP	IU	DW	HO	RV	JZ	edj	eyr	vby	tih				
649	8	IV	II	V	13	19	25	FI	NQ	SY	CU	BZ	AH	EL	TX	DO	KP	yiz	dha	ekc	tli				
649	7	I	IV	II	09	03	22	UX	IZ	HN	BK	QQ	CP	FT	JY	MW	AR	lan	dgb	zsj	wbi				
649	6	III	I	V	11	18	14	DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	lao	cft	zsk	wbj				
649	5	V	II	IV	23	02	25	MV	CL	OK	OQ	BI	FU	HS	PX	NW	EY	lju	cdr	iye	waj				
649	4	II	IV	I	04	21	09	QT	WZ	KV	GM	AC	BL	OZ	EK	QW	OP	SU	DH	JM	TX	lsb	zby	vcy	ujb
649	3	V	I	II	19	11	06	BF	NR	DX	CS	KR	MP	CN	BF	EH	DZ	IW	AV	GJ	LO	lap	owd	iwu	wak
649	2	IV	V	I	16	14	02	BN	HU	EG	PY	KQ	CP	OS	JW	AI	VZ	aqd	bdy	iyf	xtd	giq	wuv		
649	1	II	I	III	23	12	10	DP	BM	NZ	CK	GV	HQ	AF	UY	SW	JO	kgl	cdf						

Secret Command

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

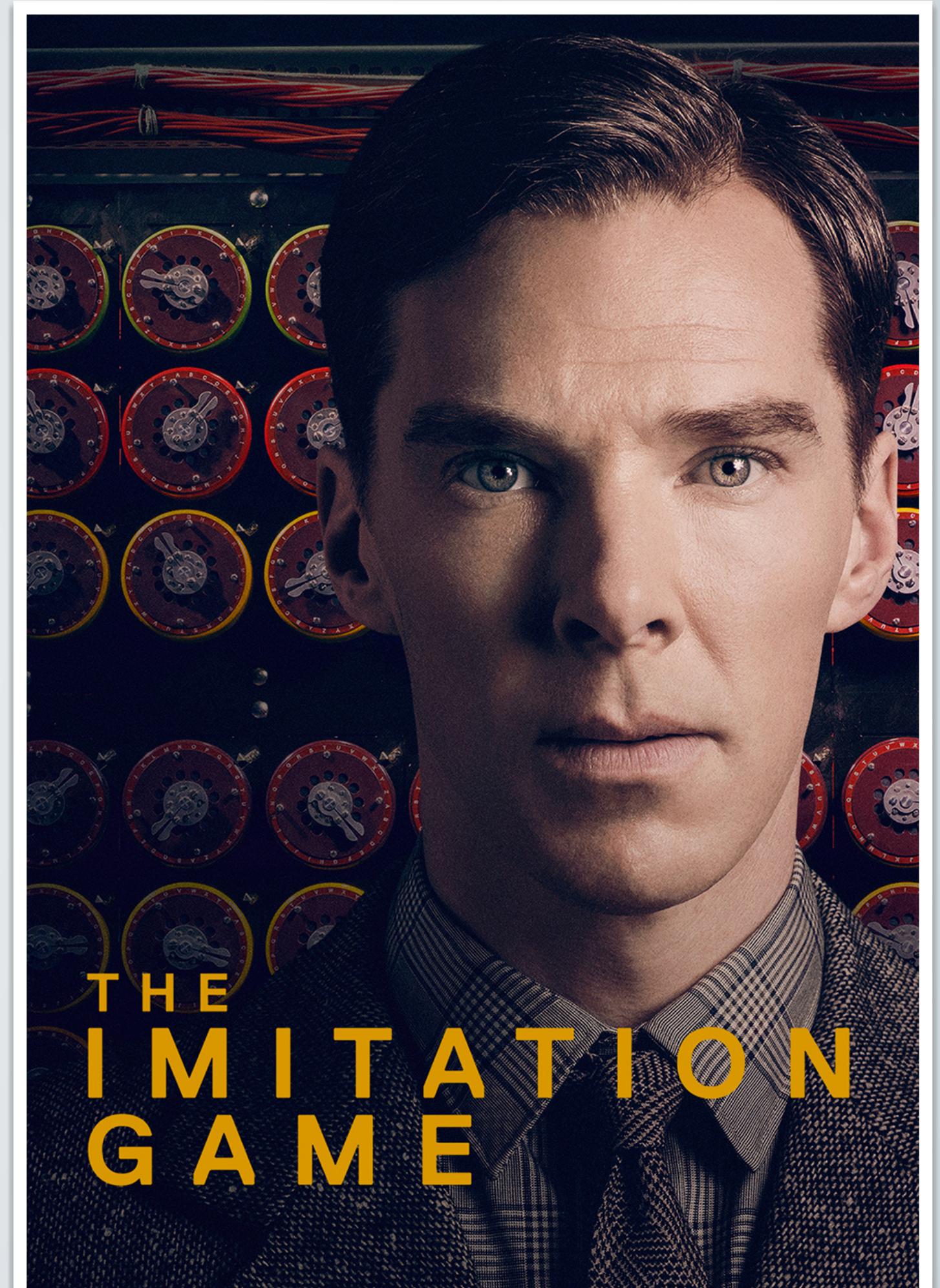
Luftwaffe Machine Key No.649

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

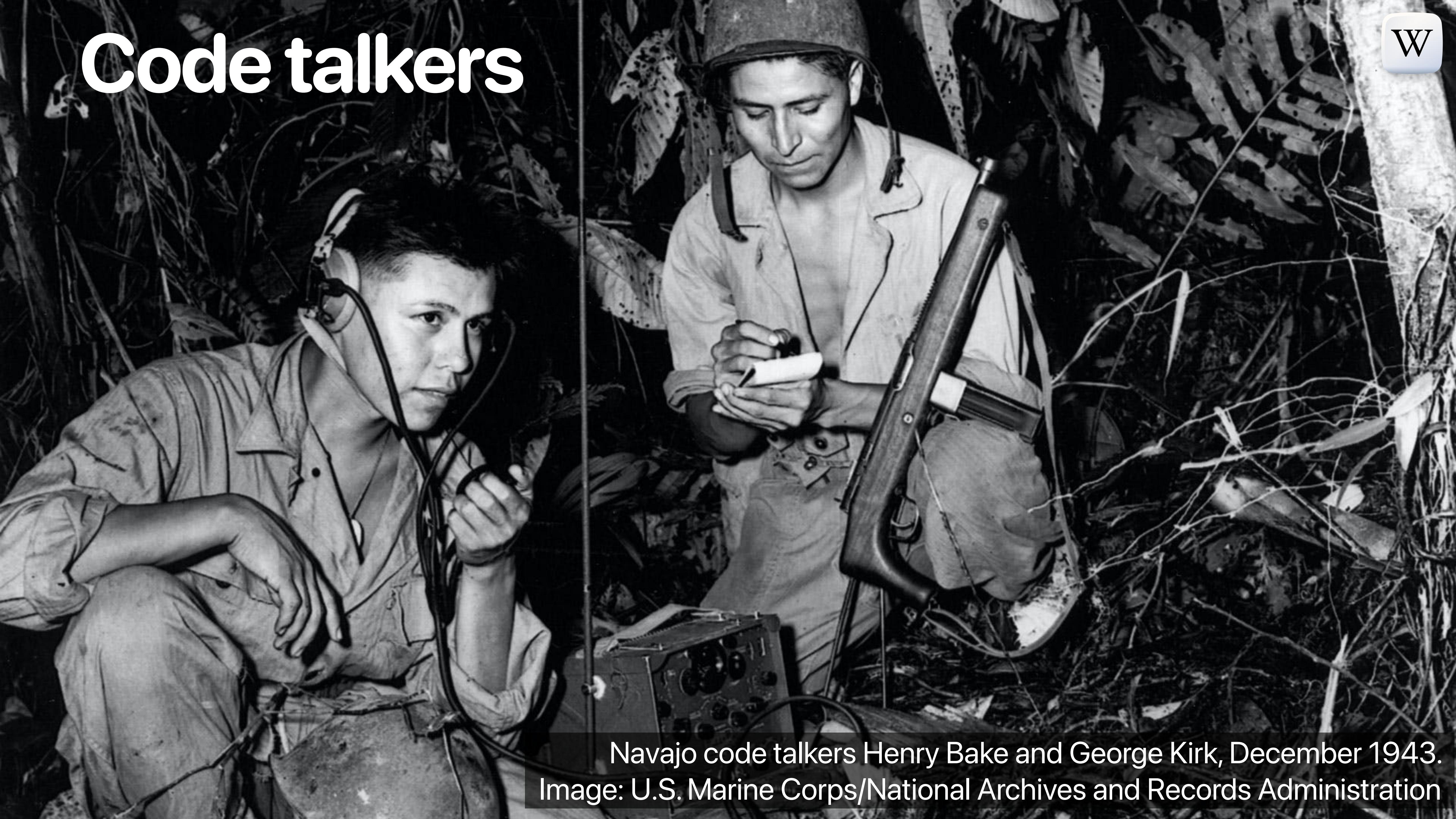
Bletchley Park



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]