

# INTRODUZIONE ALLA CRITTOGRAFIA

Sicurezza informatica

Elena Maria Dal Santo

[elenamaria.dalsanto@its-ictpiemonte.it](mailto:elenamaria.dalsanto@its-ictpiemonte.it)

# Crittografia

Insieme di tutte quelle tecniche che garantiscono l'accesso a un testo soltanto a coloro che ne hanno il permesso.

Garantisce la **C**onfidenzialità di un messaggio.

# Crittografia



A

$$F(M) = C$$



B



E

Alice “nasconde” il messaggio per il Bianconiglio

Non manda il messaggio, ma un certo codice C

# Crittografia



# Crittografia

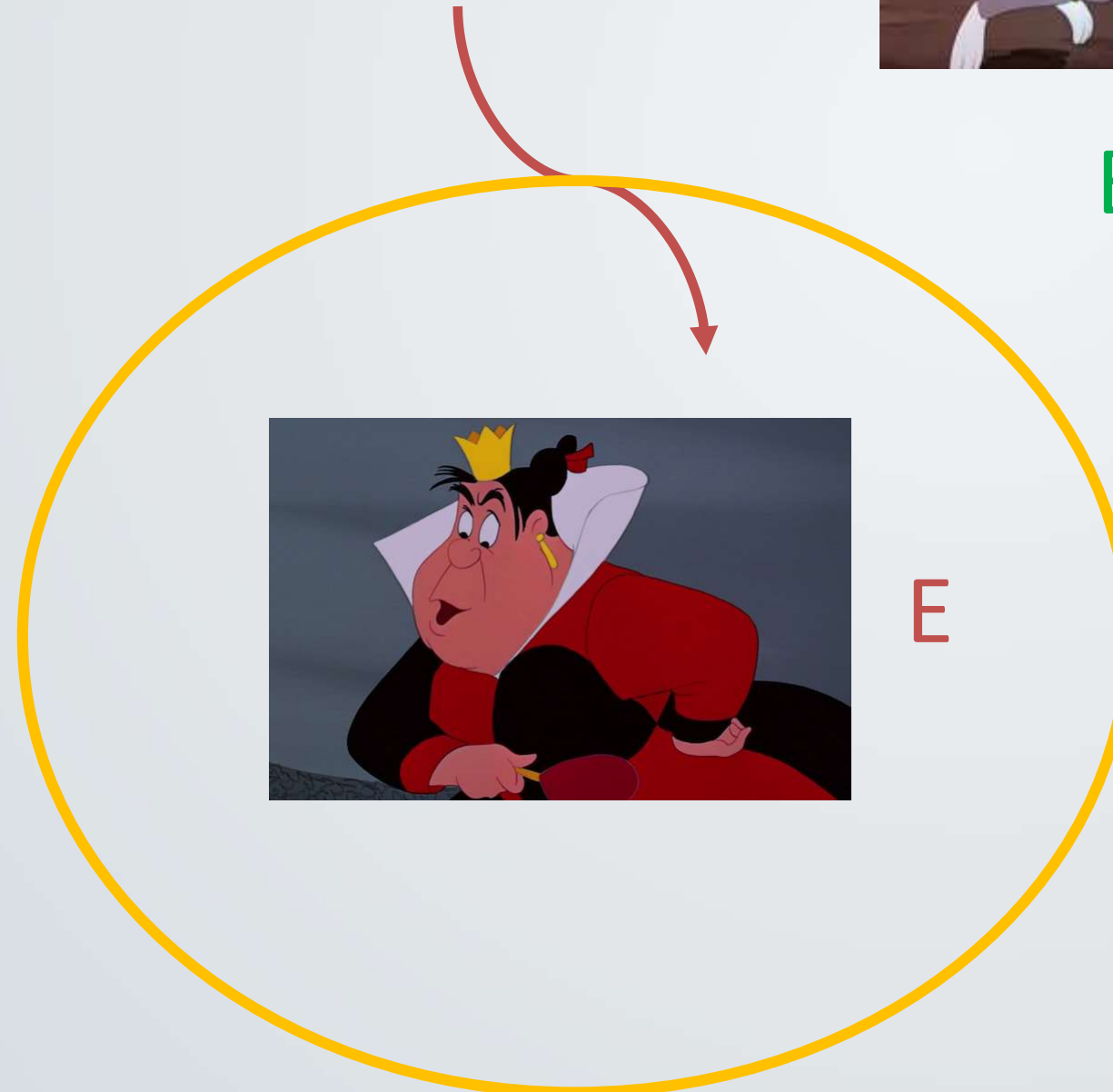


A



B

Solo B sa **decifrare**  
(=comprendere) il  
messaggio!



E



Riceve C ma  
**NON SA LEGGERLO!**



# Decrittografia





È **SEMPRE** possibile decifrare il messaggio!

(Ma non è detto che E sappia farlo in un tempo ragionevole)



# La nascita della crittografia

«Buonasera e benvenuti a Superquark»



# La crittografia "classica"

L'utilizzo più antico della crittografia è stato rinvenuto in alcuni geroglifici, risalenti a più di 4500 anni fa, e su alcune tavolette mesopotamiche.

VI secolo a.C. → **CIFRARI MONOALFABETICI**



Algoritmo (o serie di passaggi) utilizzato per rendere semanticamente non leggibile un messaggio, oppure per ripristinare un messaggio precedentemente cifrato.



Utilizzano un alfabeto per il testo in chiaro, e lo stesso alfabeto "mischiato" (permutato) per il testo cifrato.

# Cosa cambia tra “cifrario” e “codice”?

Convenzionalmente niente, però, volendo essere precisi...

**Codice** → lavora a livello di significato. C'è una convenzione sotto (es A=1000, B=1001, C=1002, ...)

**Cifrario** → lavora a livello più basso, di singole lettere. C'è una formula sotto (es. trasposizione delle lettere di 3 step a destra)

# La crittografia "classica"

Un esempio è il **CIFRARIO DI ATBASH**

Testo in chiaro:	a b c d e f g h i l m n o p q r s t u v z
Testo cifrato:	Z V U T S R Q P O N M L I H G F E D C B A



Usato anche nella Bibbia, per nascondere il vero significato della parola "Sheshach" (→ Babel)

# La crittografia "classica"

La crittografia era molto utilizzata nelle scritture o nei contesti religiosi

Un esempio?

**666**

(Numero della Bestia)



Era probabilmente un modo per indicare l'Imperatore Nerone ai tempi delle persecuzioni



# Steganografia

Istieo di Mileto (VI secolo a.C.) mandò un messaggio al suo vassallo, Aristagora, rasando la testa del suo servo più affidato, "scrivendo" il messaggio sul suo cuoio capelluto, poi mandandolo in viaggio una volta che i suoi capelli erano ricresciuti, con l'istruzione "quando arriverai a Mileto, di' ad Aristagora di rasarti i capelli e di guardarti la testa."



# Steganografia

Quali le differenze con la crittografia?

## STEGANOGRAFIA



Vuole mantenere nascosta **l'esistenza** di un messaggio a chi non conosce il sistema di occultamento.

→ Il messaggio è "in chiaro"

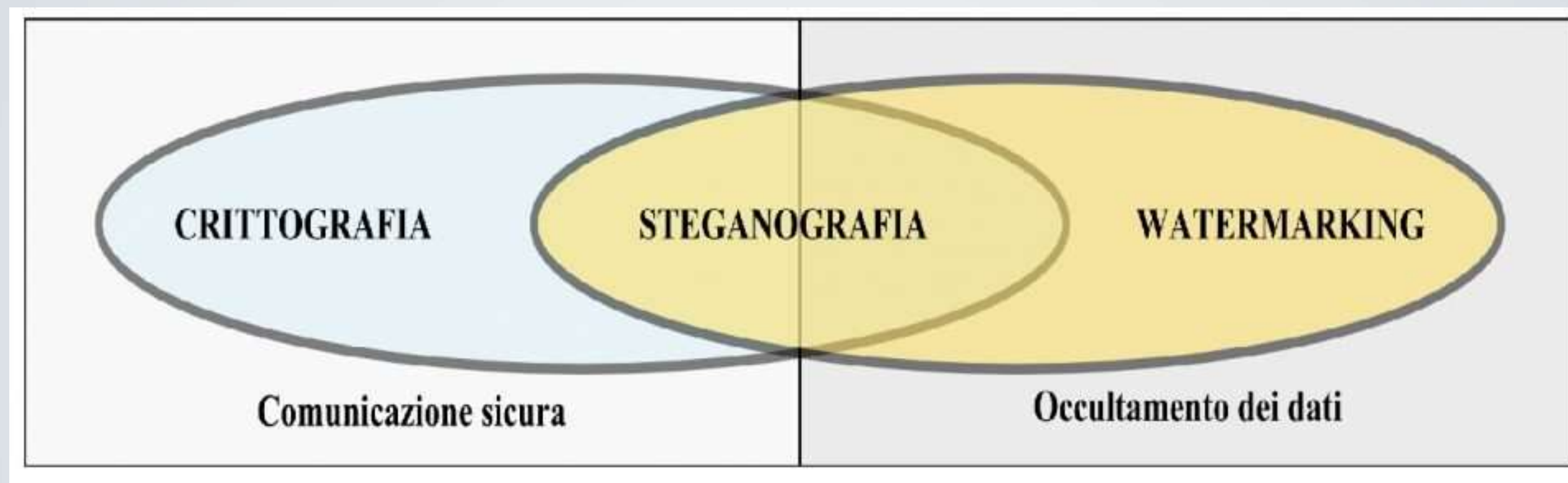
## CRITTOGRAFIA



Vuole mantenere nascosto il **contenuto** del messaggio, anche a chi ne conosce il sistema di occultamento.

→ Il messaggio è "in codice"

# Steganografia



Il **watermarking** è l'inclusione di informazioni all'interno di un file. Queste informazioni possono poi essere estratte per trarre informazioni sul file stesso (es. origine, proprietario), e lasciano il file contrassegnato in modo permanente.

Idea: non nascondo il sistema di occultamento (algoritmo di cifratura), nascondo solo la **chiave**.



Informazione usata come  
parametro in un algoritmo  
crittografico

$$C = \text{nascondiMessaggio}(M, \text{chiave})$$



## PRINCIPIO DI KERCHOFF :

La sicurezza di un crittosistema non deve dipendere dal tenere celato l'algoritmo crittografico, ma solo dal tenere celata la chiave.



Alice usa un cifrario monoalfabetico, ora che lo so potrò leggere tutti i suoi segreti!



No, se non conosci la chiave!

# PERCHÉ, ALLORA, NON USIAMO PIÙ CIFRARI COME QUELLO DI ATBASH?

Il vero problema è diventato  
quante chiavi ho a disposizione,  
ovvero quanto è grande il mio  
**SPAZIO DELLE CHIAVI**



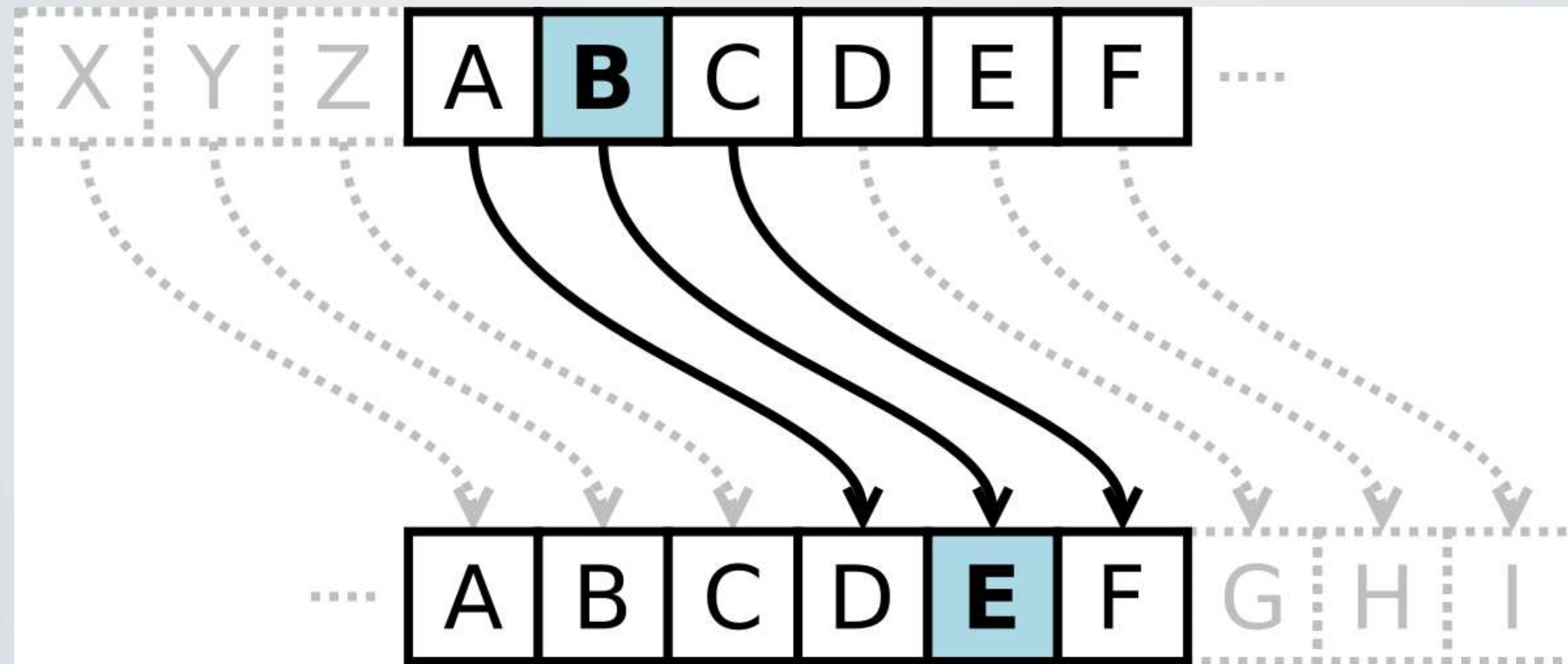
Nei cifrari monoalfabetici, una chiave è una permutazione (“mescolamento”) che possiamo dare alle lettere dell’alfabeto

Per il cifrario di Atbash avremo quindi:

$$K^{\star} = |\Sigma| = 1$$



Poco meglio fa il **cifrario di Cesare**, che si basa su uno “shift” dell’alfabeto verso destra.





“Tu quoque, Brute, fili mi!”



Wx txrtxh, Euxwh, ilol pl


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



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

**Conseguenza:** attacco di forza bruta

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



Tentativo di decifrare un messaggio “andando per tentativi”, utilizzando l’approccio della prova e dell’errore, sperando, alla fine, di indovinare.

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 ...

Mescolo (permuto) “a caso” all’interno dell’alfabeto, abbandonando i  
semplici shift visti finora

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



I miei segreti  
sono finalmente  
al sicuro!

# Crittoanalisi



the cake is a lie

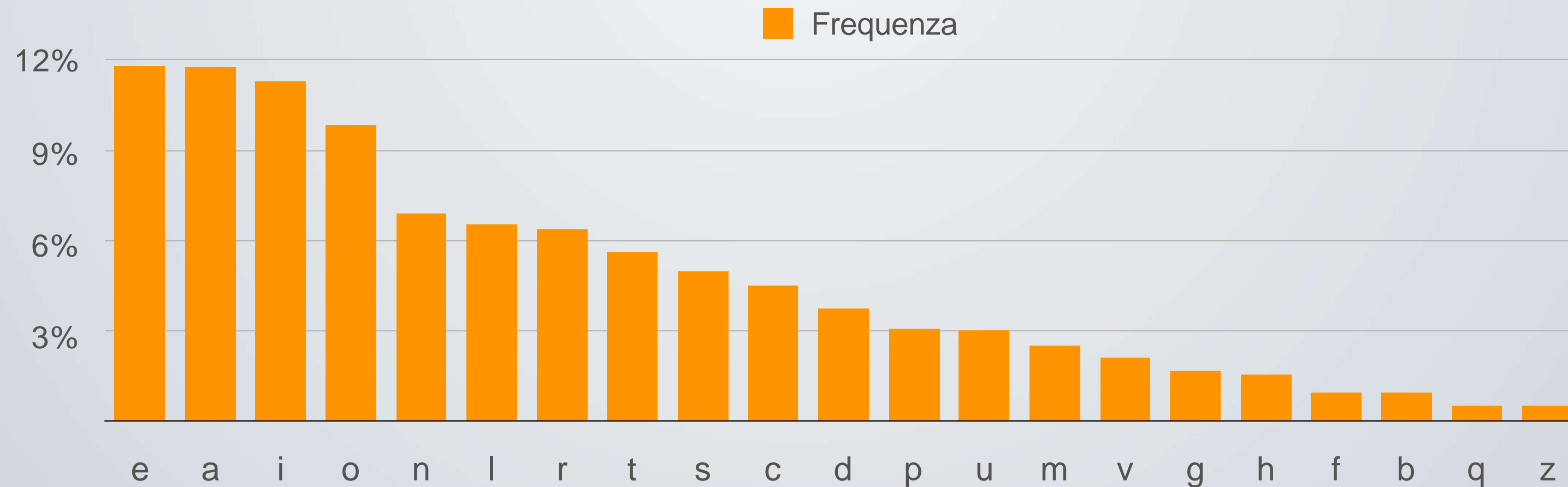
KOC NDPC AL D BAC

Frequenza?

**C** 3 volte

**D** 2 volte

**A** 2 volte





**Problema:** dipendenze statistiche nel testo.

**Conseguenza:** attacco statistico.

**Soluzione?** aumentare entropia testo cifrato.



Attacco che sfrutta le debolezze statistiche di un certo sistema crittografico (es ripetizioni,

# Cifrario polialfabetico

Fa uso di un numero più o meno grande di alfabeti per sostituire le lettere di un messaggio, usando un determinato ordine che costituisce la chiave.

# Cifrario polialfabetico



Leon Battista Alberti, 1466





# 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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Chiave: *"deceptive"*

Messaggio: *"we are discovered, save yourselves"*

wearediscoveredsaveyourselves  
deceptivedeceptivedeceptivede

# 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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Chiave: "deceptive"

Messaggio: "we are discovered, save yourselves"

w e a r e d i s c o v e r e d s a v e y o u r s e l v e s  
d e c e p t i v e d e c e p t i v e d e c e p t i v e d e  
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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Chiave: “*deceptive*”

Messaggio: “*we are discovered, save yourselves*”

wearediscoveredsaveyourselves  
deceptivedeceptivedeceptivede  
Z I

# 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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Chiave: “*deceptive*”

Messaggio: “*we are discovered, save yourselves*”

wearediscoveredsaveyourselves

deceptivedeceptivedeceptivede

ZIC



# Cifrario di Vigenère

w e a r e d i s c o v e r e d s a v e y o u r s e l v e s  
d e c e p t i v e d e c e p t i v e d e c e p t i v e d e  
Z I C V T W Q N G R Z G V T W A V Z H C Q Y G L M G Z H W

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

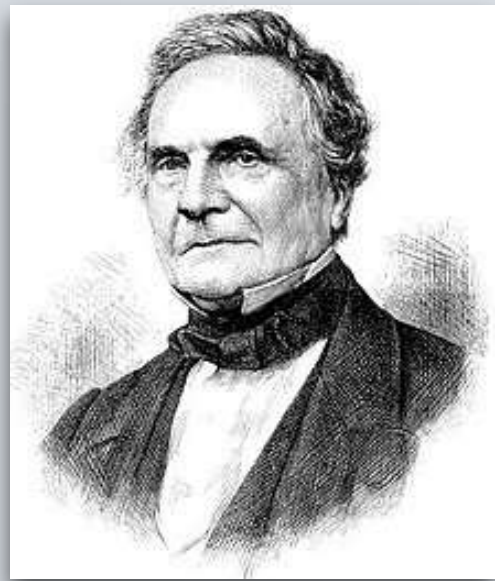


ORA nessuno  
potrà più leggere i  
miei segreti!

# Crittoanalisi

we are discovered save yourselves  
deceptive deceptive deceptive  
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).

# Test di Kasiski

WUMOGI ZWYRMHMCES S VLP I SCLLGUI LEYMV NGE  
RQL LGAI QGEZKZAL QUTKTAZEYHUWRL MZWXCHUWR  
LMSZLBS QWCBMZI XCRFWWYWOQL ALQATYYZXZGR  
PQDAVQBZALQBTMJ RZLSRB WOGZUVZEEYJLOYQA  
EYGTQLKI DMDRMEKLP RMMAGYXI ES EATLKMMTZ  
NVQVZLXUALI JZQZLLRABCMTBQDMRAQESSUXP  
AGMBTRAVANF MEKLZVUMCYQUAPAGTQGS SFQDNEG  
ZLAGTQ TMI FMNMPYI WYGUWE MPMMNMPYI WYXMHKY  
WHMRJ MMC GQMKSCWUI RGS DVZMKZQTQX MVE CYZC  
ZKS YCZPI AOYGMEBL LXQCYSS YWY WOM

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



WU MOGI Z WY 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

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

Proviamo a ragionare sulle possibili lunghezze delle chiavi...

Ricordiamo:

wearediscoveredsaveourselves  
deceptivedeceptivedeceptivede

La chiave dopo un po' "si ripete"

Proprio grazie al fatto che si ripete la chiave, avevamo notato delle ripetizioni nel codice...

wearediscoveredsaveyourselves  
deceptivedeceptivedeceptivede  
ZICVTWQNGRZGVTWAVZHCQYGLMGZHW

Cerchiamo, con la prima ripetizione dell'esempio, di capire quanto potrebbe essere lunga una chiave per ripetersi "bene" da H a H

H U W R L M Z W X C | H U W R L M  
C H I A V E N U N O | C H I A V E

Non conosciamo la chiave, ma una parola lunga 10 lettere è una possibilità! Inizia a ripetersi quando la stringa HUWRLM si ripete!

Ci sono altre possibilità?

H U W R L M Z W X C H U W R L M  
C H I A V C H I A V C H I A V C

Una chiave lunga 5 lettere, oppure...

H U W R L M Z W X C H U W R L M  
C H C H C H C H C H C H C H C H



Abbiamo ottenuto tre possibilità.

Diamo per scontato che la chiave possa anche essere lunga solo 1 lettera (non sarebbe molto furbo, però è una possibilità!)

→ 4 possibili lunghezze per la nostra chiave

HUWRLM



1. chiave di 1 lettera che si ripete 10 volte da H a H
2. chiave di 2 lettere che si ripete 5 volte da H a H
3. chiave di 5 lettere che si ripete 2 volte da H a H
4. chiave di 10 lettere che si ripete 1 volta da H a H

1, 2, 5 e 10 sono anche i  
**divisori** di 10 (cioè i  
numeri che dividono 10)!

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		✓		✓										✓

H U W R L M Z W X C H U W R L M  
C H I A V C H I A V C H I A V C

Questa è la lunghezza che abbiamo scelto, guardiamo ora un'altra cosa...



		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
0	A	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
1	B	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
2	C	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
3	D	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
4	E	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
5	F	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
6	G	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Ogni riga della tabella è  
un cifrario  
monoalfabetico!

→ Ogni riga rappresenta  
uno shift dell'alfabeto

I numeri accanto alle  
righe indicano quanti shift  
abbiamo effettuato

Iniziamo allora a fare dei ragionamenti, limitando il numero di lettere che prendiamo in considerazione

La chiave ha lunghezza 5, si ripete perciò dopo 5 lettere

→ Prendiamo 1 lettera ogni 5

H	U	W	R	L	M	Z	W	X	C	H	U	W	R	L	M	S	Z	L	B
C	H	I	A	V	C	H	I	A	V	C	H	I	A	V	C	H	I	A	V



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

Tutte queste lettere “avranno sotto” (nella riga della chiave) la prima lettera della chiave.

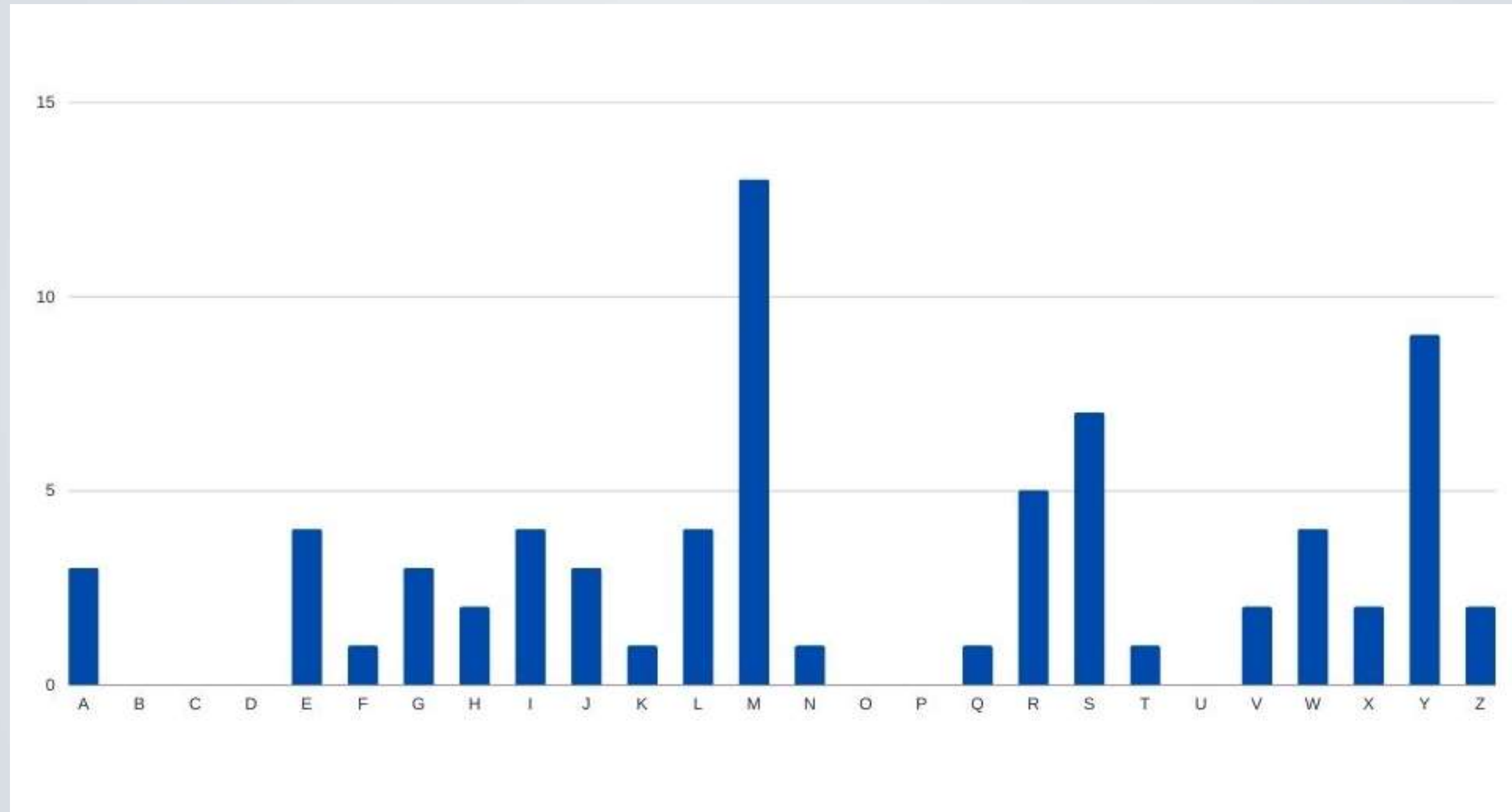
Noi per ora abbiamo messo una C ma NON è CHIAV la nostra chiave! Come troviamo la chiave (e, soprattutto, la prima lettera)?

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

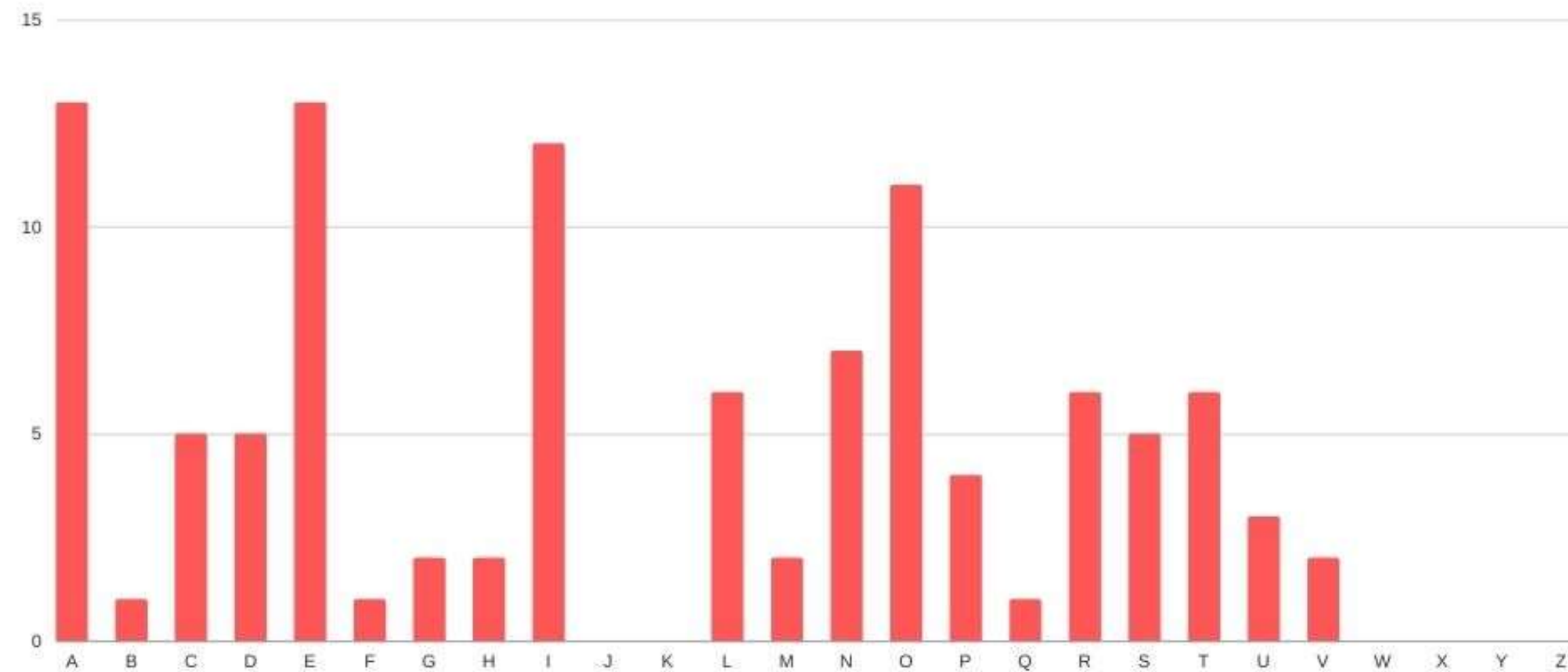
Guardiamo solo le lettere rosa e trattiamole come se formassero  
un messaggio solo loro

WIMSIGYEGELTHMHMSMRQLYRVLJRZEYGIMRYEMVXJLM  
MSARFZYASNAMMYMMYYJQWSKXYSIMXSW

# ISTOGRAMMA DEL CRITTOGRAMMA

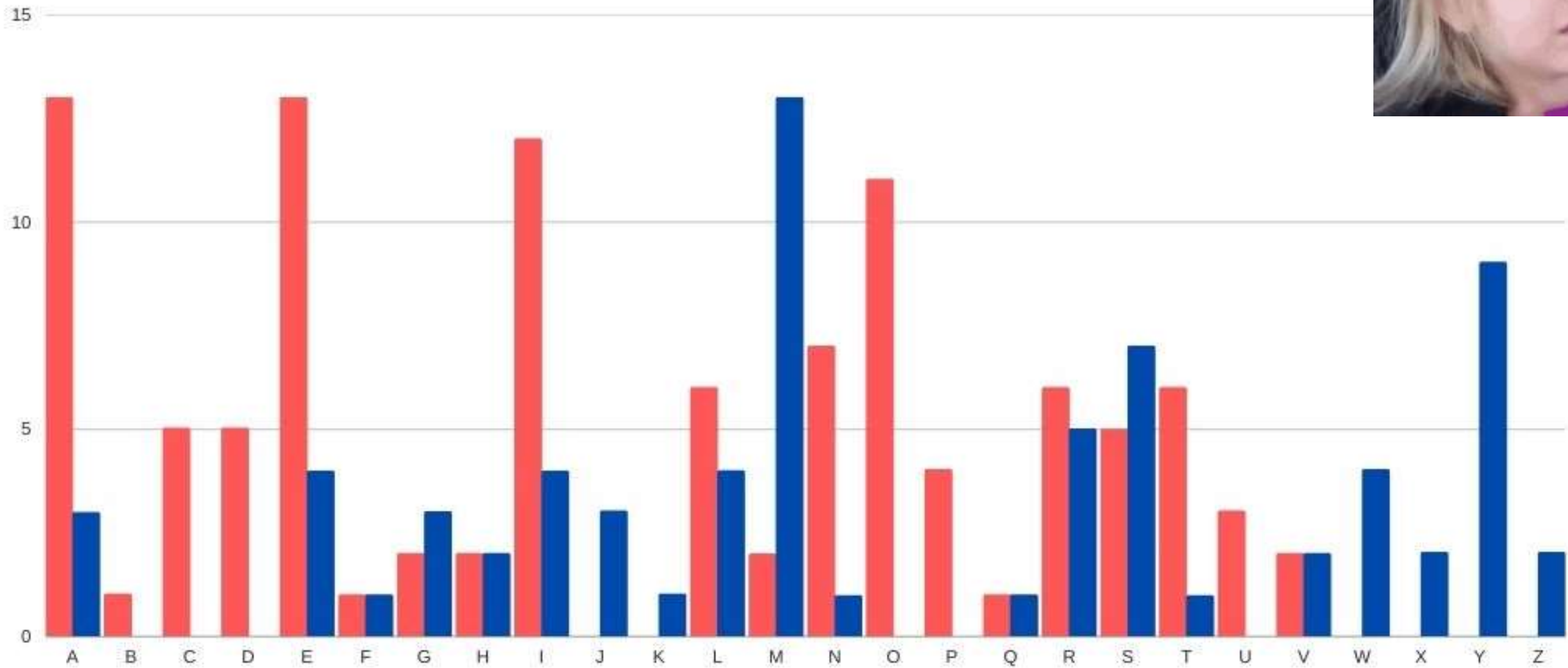
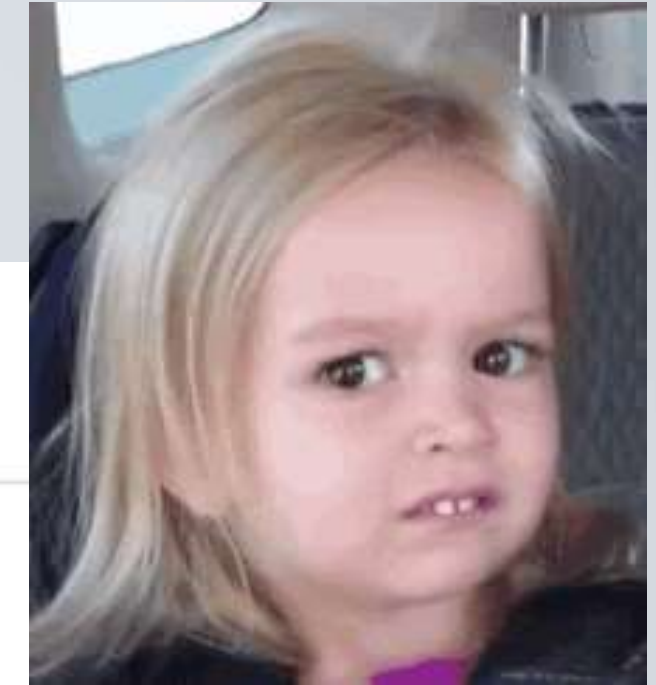


# ISTOGRAMMA DELLA LINGUA ITALIANA

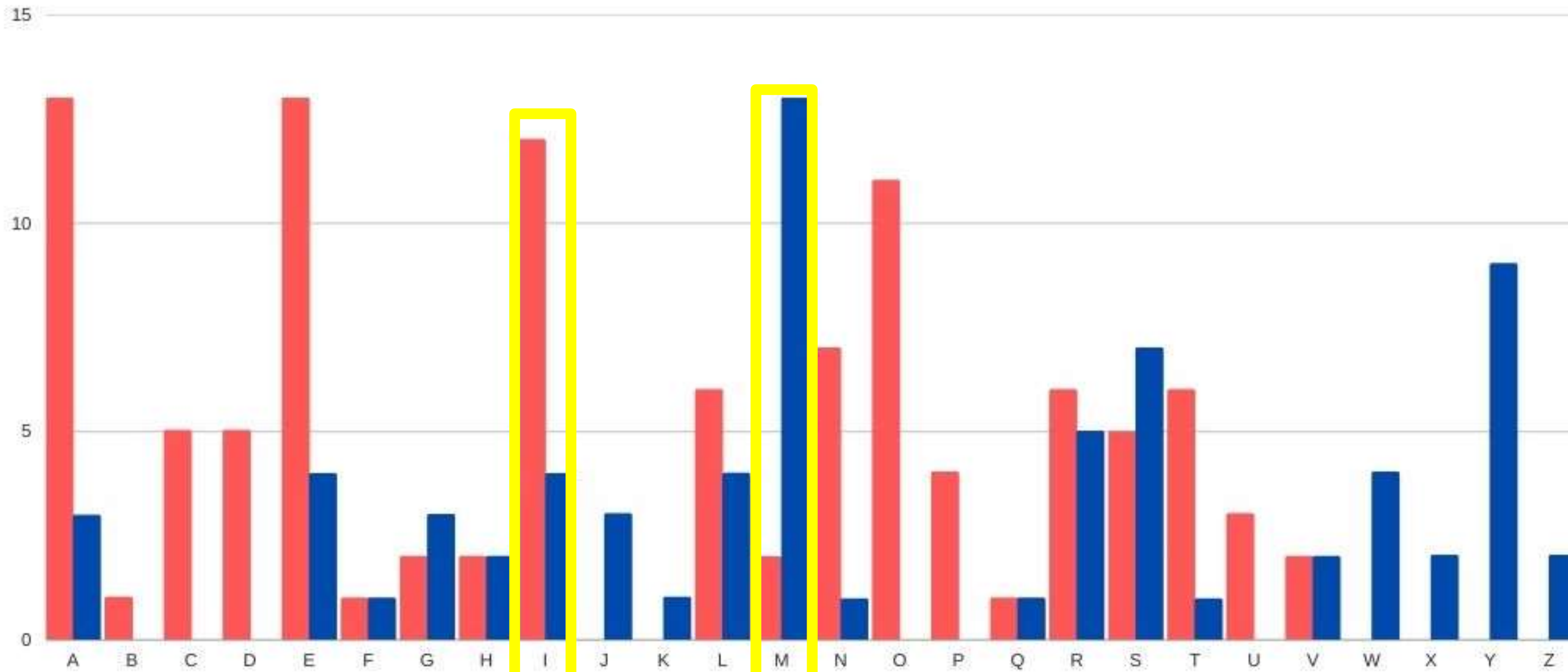


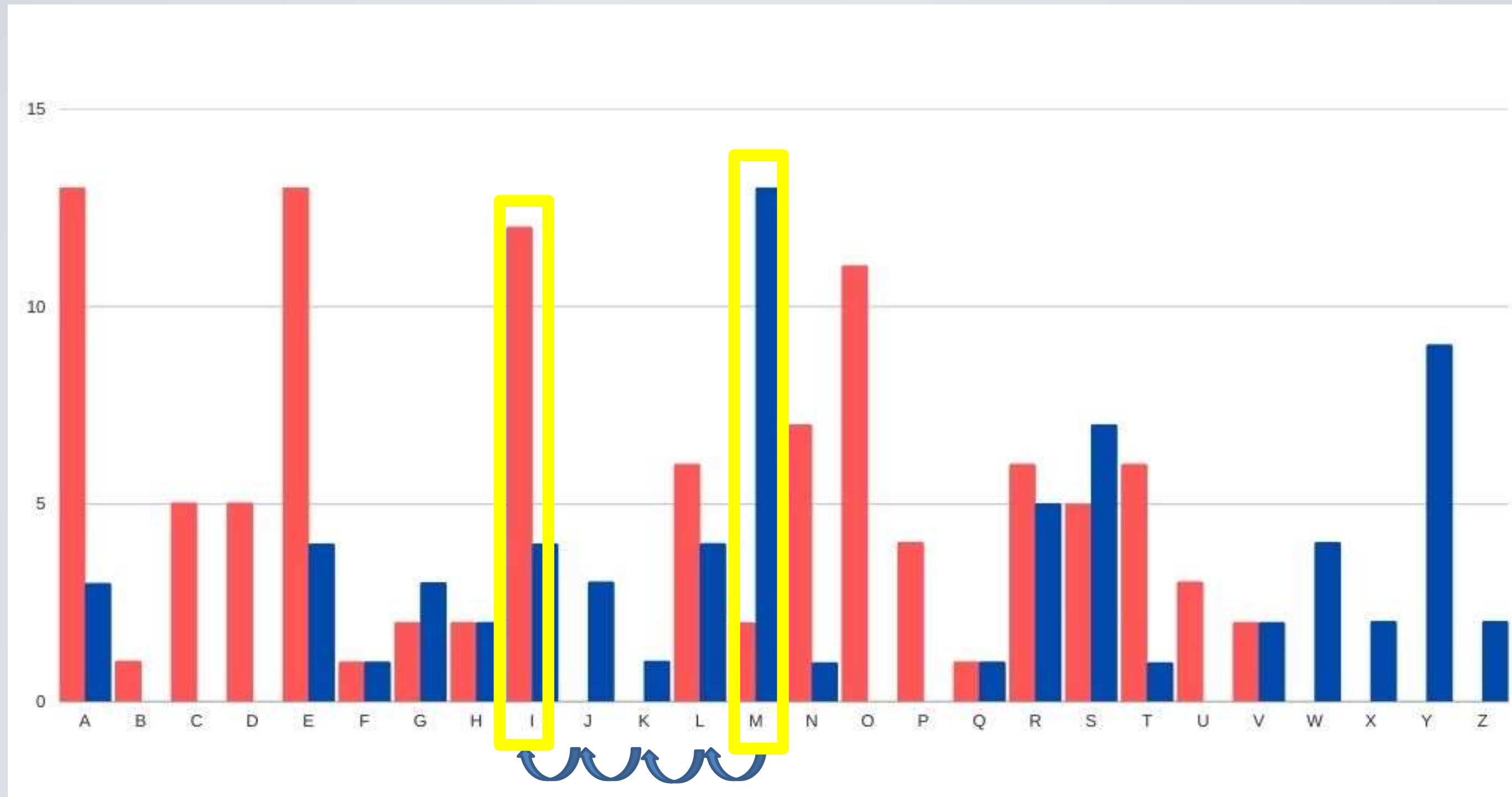


Uniamo le due cose...



Non è perfetto ma...





Dal mio alfabeto "normale" (0 shift), mi sono spostato di 4 passettini  
→ Ho fatto 4 shift!



		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
0	A	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
1	B	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
2	C	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
3	D	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
4	E	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
5	F	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
6	G	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Ma allora la prima lettera della mia chiave è la **E**!



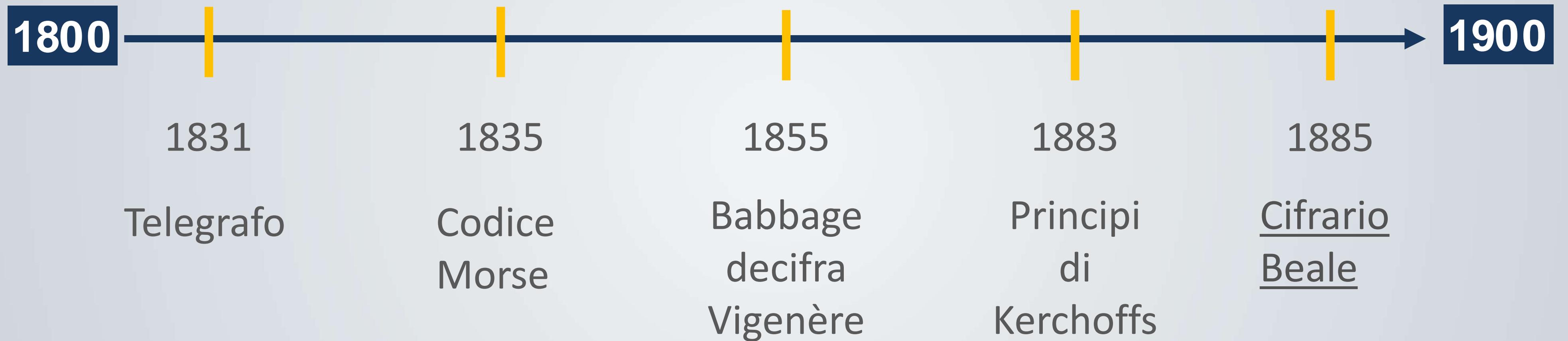
W U M O G I   Z W Y R M H M C E S S V L P I   S C L L G U I   L E Y M V N G E  
R Q L L G A I   Q G E Z K Z A L Q U T K T A Z E Y H U W R L M Z W X C H U W R  
L M S Z L B S Q W C B M Z I   X C R F W W Y W O Q L A L Q A T Y Y Z X Z G R  
P Q D A V Q B Z A L Q B T M J R Z L S R B W O G Z U V Z E E Y J 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 la lunghezza dello shift è 12 e dunque che la seconda lettera della chiave è M.

WUMOGI Z WYRMHMCES S VLP I S C L L GUI 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 chiave **EMILY**, che decifra correttamente il testo.

# Ottocento: la crittografia militare







# La meccanizzazione della crittografia



# Seconda Guerra Mondiale



TypeX



Enigma

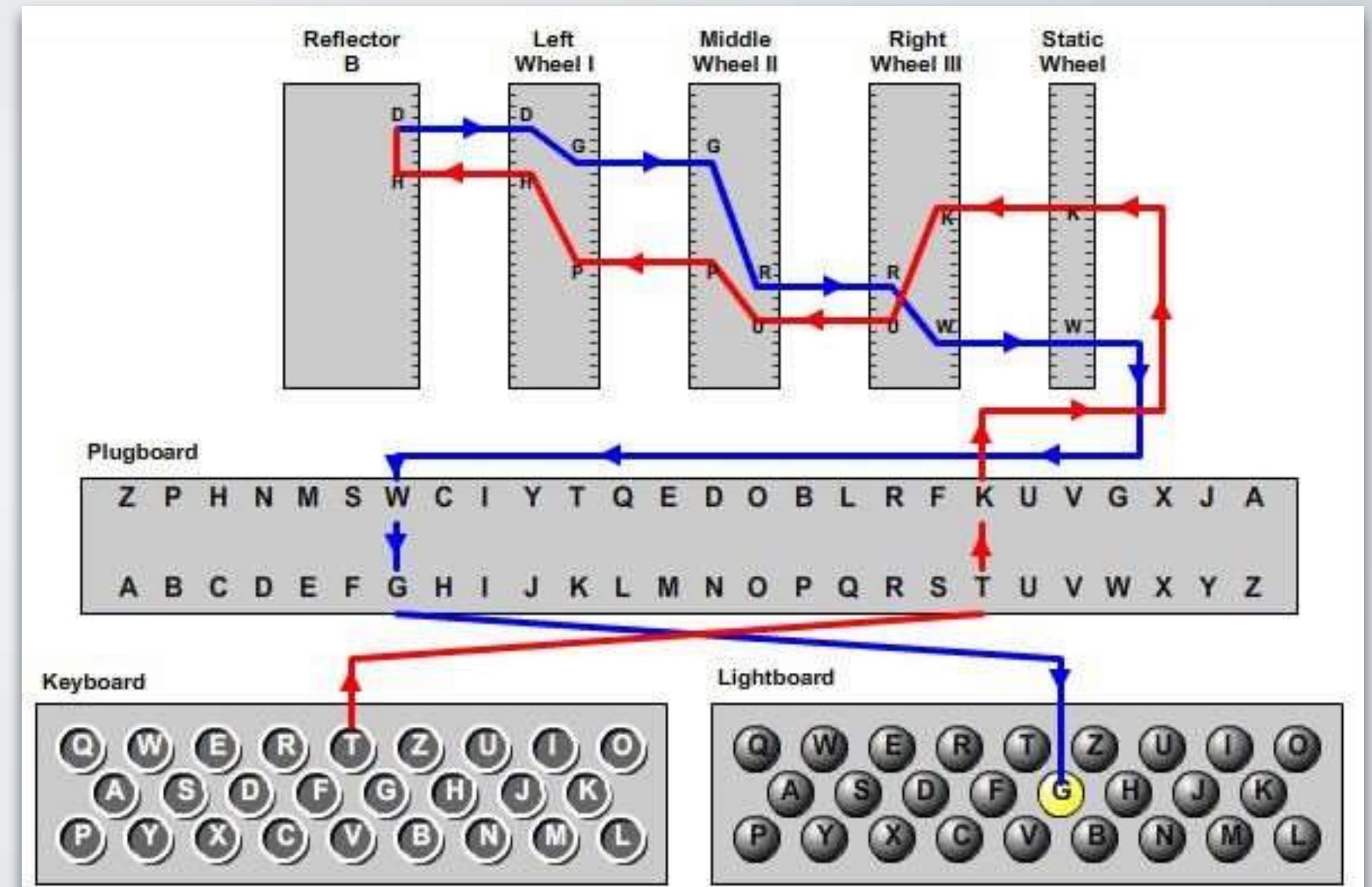


SIGABA





# La macchina Enigma





# Le chiavi crittografiche di Enigma

Geheime Kommandosache! Jede einzelne Tageschlüssel ist geheim. Mitnahme im Flugzeug verboten!

Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

Manöver- tag	Wellenlage			Ringstellung	S i e h e v e r b i n d u n g e n										Benutzungsgruppen					
					an der Umkehrrolle	1	2	3	4	5	6	7	8	9	10					
649	31	I	V	III	14 09 24		SZ	OT	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	kti	acw	zsi	wao
649	29	III	II	I	12 24 03	KM AX PZ GO	DJ	AT	CV	IO	ER	QS	LW	PZ	FN	BH	ioc	acn	ovw	wvd
649	28	II	III	V	06 08 16	DI CN BR PV	CR	FV	AI	DK	OT	MQ	EU	BX	LP	GJ	lrb	cld	ude	rzh
649	27	III	I	IV	11 03 07	LT EQ HS UW	DY	IN	BV	OR	AM	LO	PP	HT	EX	UW	woj	fbh	vct	uis
649	26	I	IV	V	17 22 19		VZ	AL	RT	KO	CO	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	rwl	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	IU AS DV OL	FJ	ES	IM	RX	LV	AY	OU	BO	WZ	CN	jqc	acx	mwe	wve
649	21	I	V	II	13 05 19	PT OX EZ CH	RU	HL	PY	OS	GZ	DM	AW	CE	TV	NX	jpw	del	mwf	wvf
649	20	III	IV	V	24 01 10	MR KN BQ PW	DP	MO	QZ	AU	RY	SV	JL	GX	BE	TW	jqd	cef	nvo	ysh
649	19	V	III	I	17 25 20		OX	PR	PH	WY	DL	CM	AE	TZ	JS	GI	idf	fpx	jwg	tlg
649	18	IV	II	V	15 23 26		EJ	OY	IV	AQ	KW	PX	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	OS	PU	FQ	CT	tdp	dhb	fkf	uiv
649	15	II	IV	I	01 03 07		DS	HY	MR	OW	LX	AJ	BQ	CO	IP	NT	ldw	hzj	soh	wvg
649	14	IV	I	V	15 11 05	AI BT MV HU	GM	JR	KS	IY	HZ	PL	AX	BT	CQ	NV	imz	noa	tjv	xtk
649	13	I	III	II	13 20 03	FW EL DG KN	LY	AG	KM	BR	IQ	JU	HV	SW	ET	CX	zgr	dgz	gjo	rye
649	12	V	I	IV	18 10 07	RZ OQ CP SX	MU	BP	CY	RZ	KX	AN	JT	DG	IL	PW	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	OO	VX	PZ	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	tlh
649	8	IV	II	V	13 19 25		PI	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	GQ	CP	FT	JY	MW	AR	lan	dgb	zsj	wbi
649	6	III	I	V	11 18 14	IL AP EU HO	DQ	GU	BW	NP	HK	AZ	CI	PO	JX	VY	lao	cft	zsk	wbj
649	5	V	II	IV	23 02 25	QT WZ KV GM	MV	CL	GK	OQ	BI	FU	HS	PX	NW	EY	lju	cdr	iye	waj
649	4	II	IV	I	04 21 09	BF NR DX CS	AC	BL	OZ	EK	QW	OP	SU	DH	JM	TX	lsb	zby	vcy	ujb
649	3	V	I	II	19 11 06		KR	MP	CN	BP	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
649	1	III	I	III	23 12 10		DP	BM	NZ	CK	GV	HQ	AF	UY	SW	JO	kgl	cdf	giq	wuv

## Secret Command

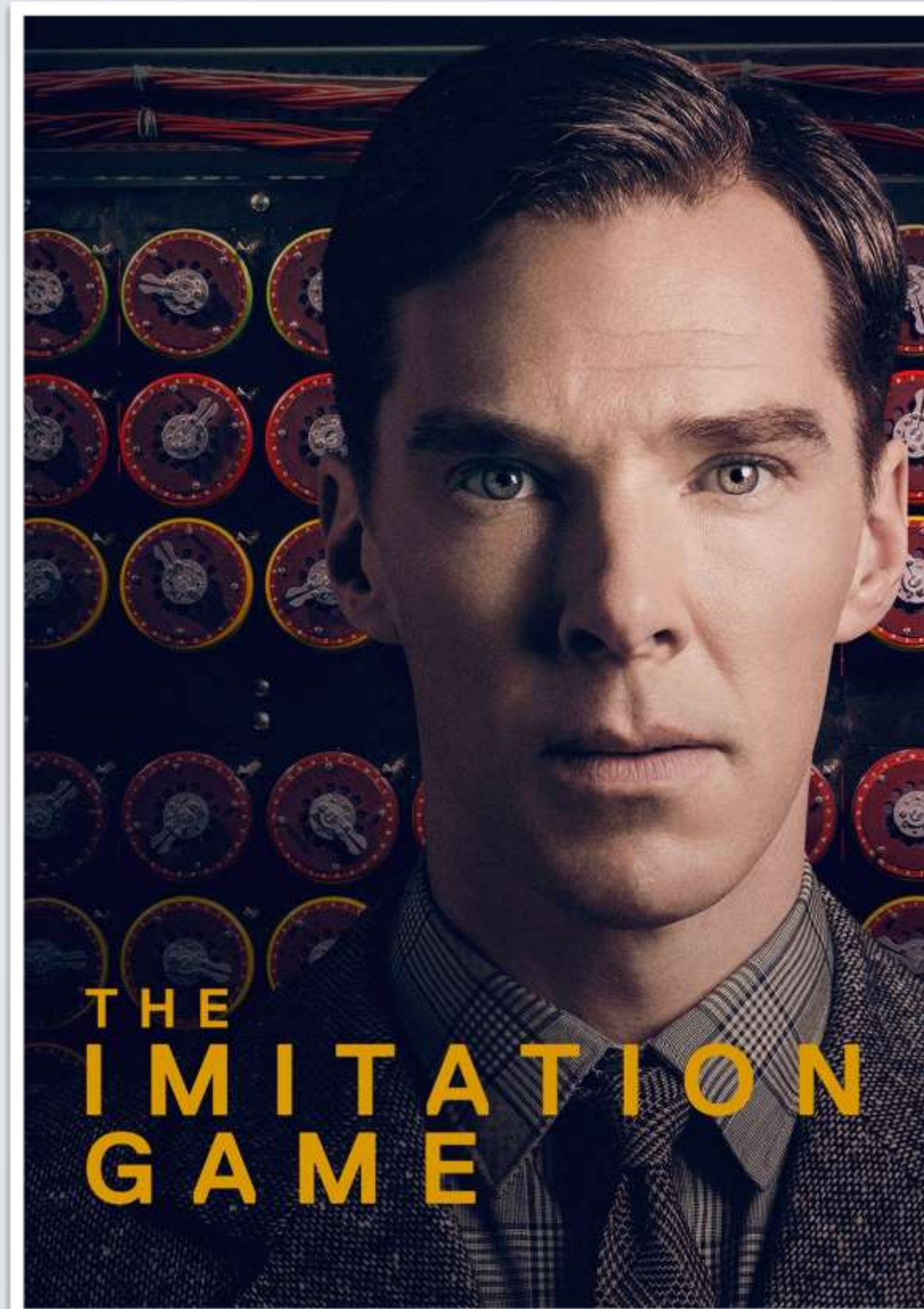
Document! Every individual daily key is secret. Forbidden to bring on aircraft.

Luftwaffe Machine Key No.649

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



# Bletchley Park





# Link utili

- Kryptos (libreria di codici e cifrari), <https://kryptos.altervista.org/>
- Cifrario di Beale <https://www.youtube.com/watch?v=aZRUhS4JHp4>
- The imitation game: Alan Turing cracked the Enigma code - <https://youtu.be/mwFWMM9APLs>

