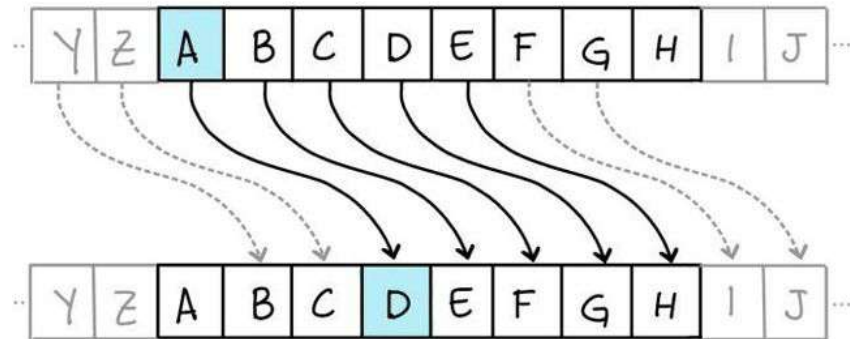


La crittografia? è un Gioco!



Ci conosciamo!

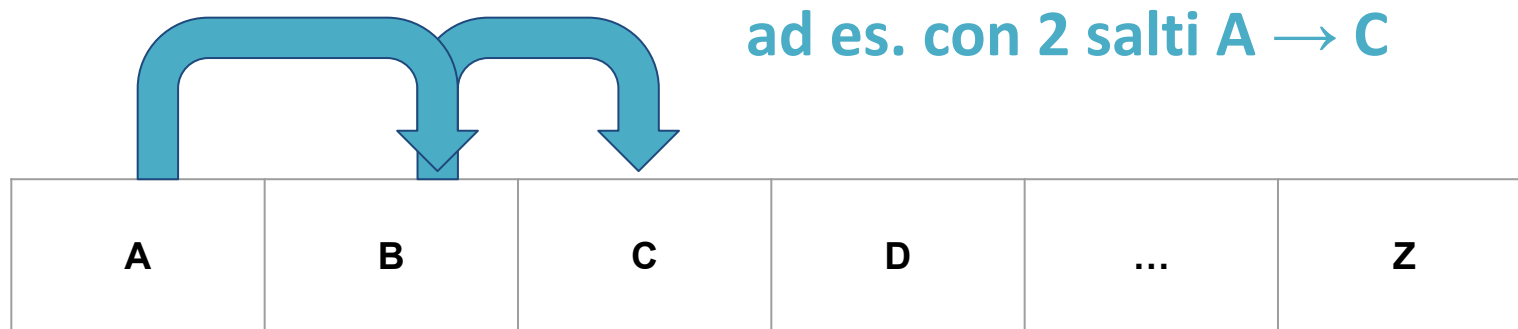
con un nome in codice, come gli agenti segreti
(o i rapper)



YARI → **BDUL** (con tre spostamenti *in avanti*)

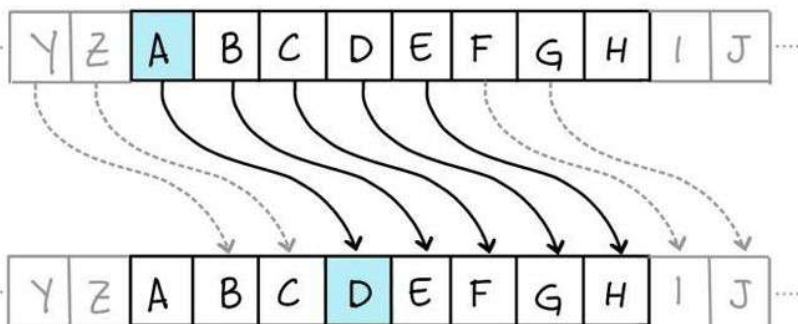
Per il vostro **nome in codice**, scegliete voi il numero di “salti”, le uniche due regole sono:

- stesso numero di spostamenti per ogni lettera
- andare sempre in avanti (da sx a dx)



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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Crittografia con il cifrario di Cesare



Che cos'è la crittografia?

1. Un modo per nascondere i messaggi in modo che solo alcune persone possano capirli.
2. Un tipo di codice segreto che usano solo gli scienziati.
3. Un linguaggio speciale usato per programmare i computer.
4. Un sistema per disegnare figure geometriche.



Che cos'è la crittografia?

1. **Un modo per nascondere i messaggi in modo che solo alcune persone possano capirli.**
2. Un tipo di codice segreto che usano solo gli scienziati.
3. Un linguaggio speciale usato per programmare i computer.
4. Un sistema per disegnare figure geometriche.



Quando è nata la crittografia?

1. Già in tempi antichi, tra i soldati romani e greci, per proteggere le comunicazioni
2. Nel Rinascimento, per proteggere le lettere segrete tra i re, principi, ecc.
3. Durante la seconda guerra mondiale, per proteggere le comunicazioni.
4. Quando è nato internet, per proteggere i dati nel computer dagli attacchi degli hacker



Quando è nata la crittografia?

1. **Già in tempi antichi, tra i soldati romani e greci, per proteggere le comunicazioni**
2. Nel Rinascimento, per proteggere le lettere segrete tra i re, principi, ecc.
3. Durante la seconda guerra mondiale, per proteggere le comunicazioni.
4. Quando è nato internet, per proteggere i dati nel computer dagli attacchi degli hacker

La crittografia è antichissima!



1900 a.C.



1500 a.C.



650 a.C.

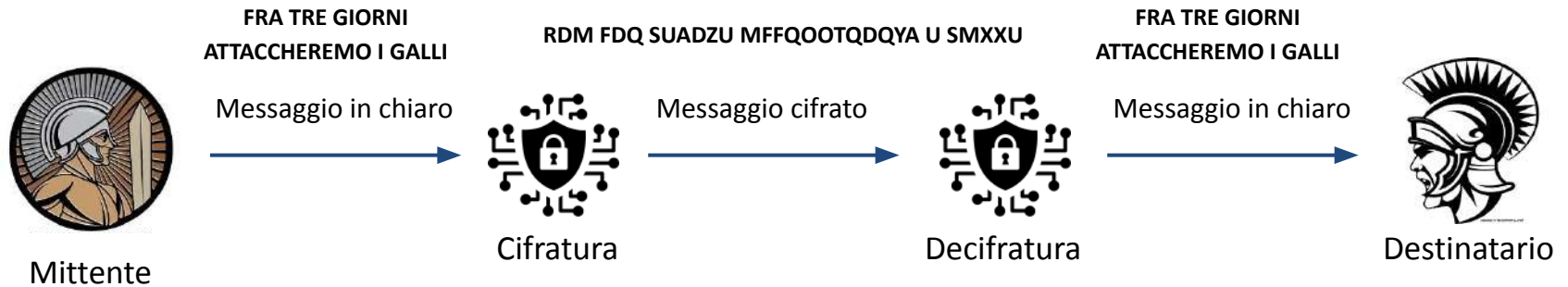
può essere l'occasione per una
ricerca multi-disciplinare!

un'altra tecnica: la **steganografia** ovvero nascondere
l'esistenza della comunicazione

noi ci occuperemo di **crittografia!**



Il cifrario di Cesare ha tutti gli elementi di un *crittosistema*



La stessa chiave è usata sia per cifrare che per decifrare



Chiave segreta condivisa = spostamento 12

Proviamo!

WSPI

con spostamento 4 lettere

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
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

ATTENZIONE!
per DEcifrare mi sposto verso...

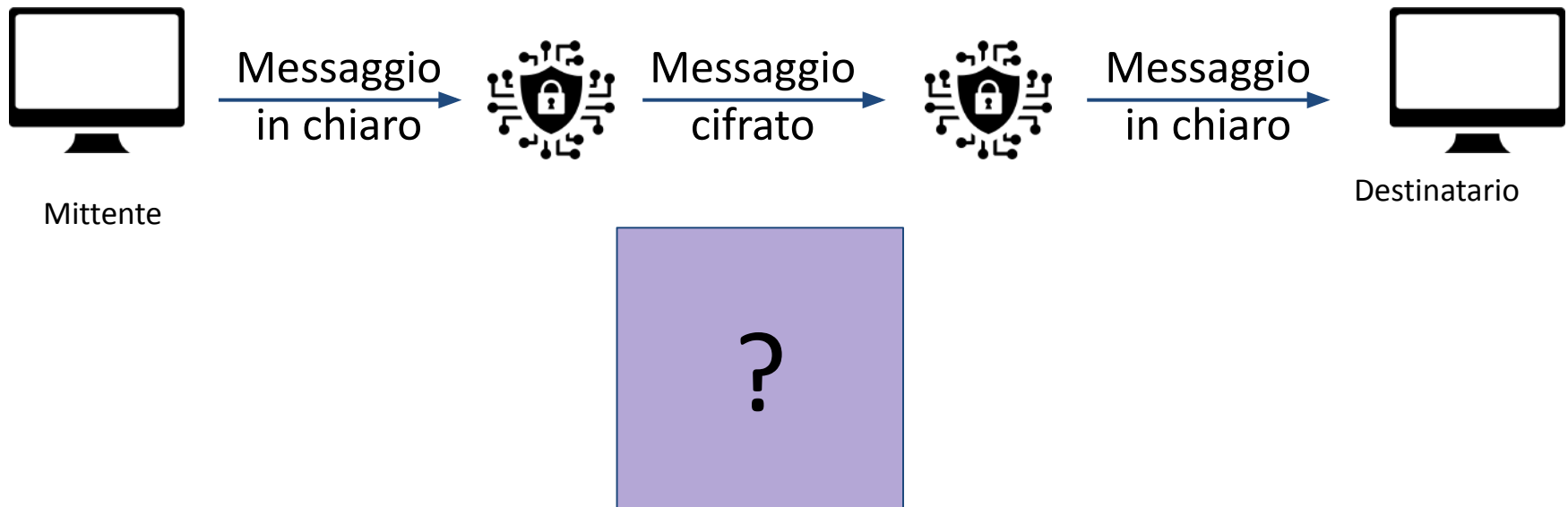
OK, ma dove sta l'informatica??



Che cosa succede se non conosciamo il numero di spostamenti di un messaggio?



Lo stesso principio rimane anche oggi:



La crittografia si usa anche oggi



MFFMOOTQDQYA U ZQYUOU
CGQEFM ZAFFQ



<http://www.crittologia.eu/critto/caesar.html>

Crittoanalisi

l'arte della "rottura" dei codici dei cifrari.
La crittoanalisi studia come decifrare un
messaggio senza esserne “autorizzati”

NB: la chiave deve essere protetta altrimenti i nostri
messaggi segreti potranno essere decifrati

Tornando al nostro viaggio nella Storia...

Quando è nata la crittografia?

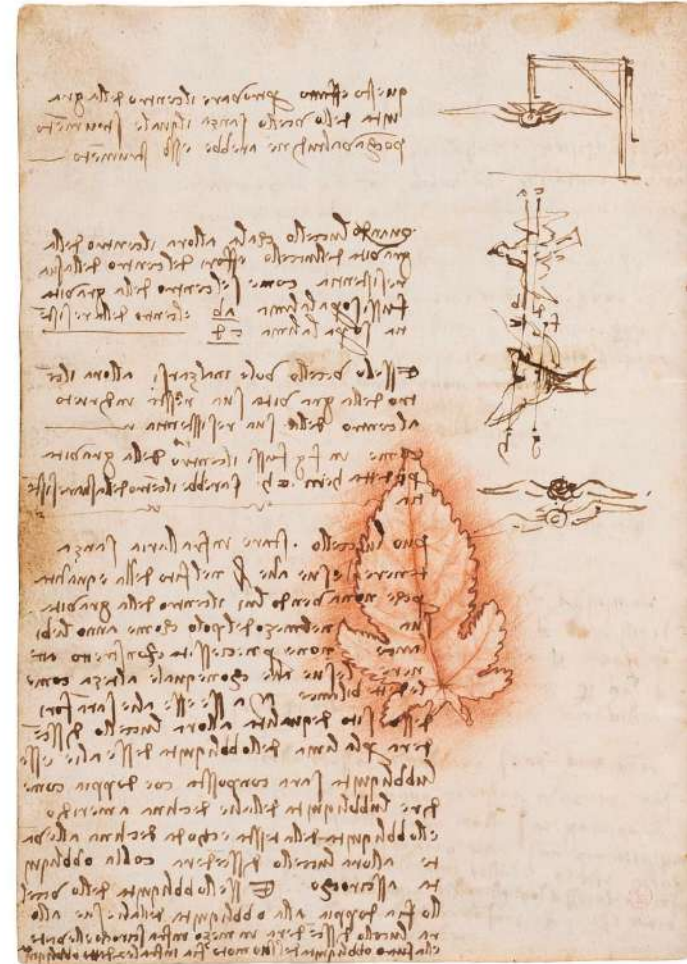
1. Già in tempi antichi, tra i soldati romani e greci, per proteggere le comunicazioni
2. Nel **Rinascimento**, per proteggere le lettere segrete tra i re, principi, ecc.
3. Durante la **seconda guerra mondiale**, per proteggere le comunicazioni.
4. **Quando è nato internet**, per proteggere i dati nel computer dagli attacchi degli hacker

La crittografia nel Rinascimento?

Fuori tema, ma spesso
richiesto dalla classe:



<https://www.leonardodigitale.com/sfoglia/codice-arundel/0002-v/>

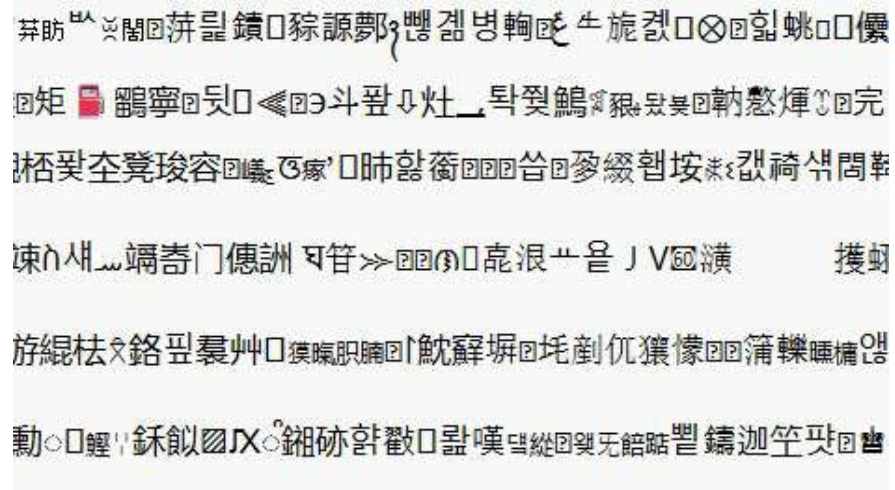


La crittografia durante la II Guerra Mondiale

Alan Turing



La crittografia nell'era dei computer e di Internet



un file cifrato dal mio PC:

[illegible]

Perché la crittografia oggi è così complicata?

1. Perché abbiamo molte più password da ricordare, e spesso sono anche molto lunghe.
2. Perché i programmatori informatici per non annoiarsi hanno inventato sfide sempre più difficili.
3. Perché oggi dobbiamo proteggere molte più informazioni, come messaggi, soldi e dati online e i computer sono in grado di provare molto più velocemente di noi a rompere i segreti.



password & crittografia: non sono la stessa cosa!

possiamo usare la metafora del
diario segreto:

lucchetto = password

scrittura segreta = crittografia



EXTRA!

Esempio del pin a 4 cifre:

- Quanti tentativi devo fare?
- Quanto tempo ci metto per ciascun tentativo?

Which passwords have you ever cracked? (*crittoanalisi*)



Inventa una password sicura e provala su <https://nordpass.com/it/secur-e-password/>

Quale password è più difficile da indovinare?

- c0Mpl!c@t4
- password-molto-facile

possibile collegamento con
educazione civica (cittadinanza digitale)



Secret Code di Quercetti

Altri giochi di crittografia...



Siete pronti per un nuovo sistema?

Cifrario di Polibio

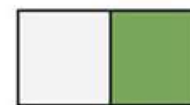
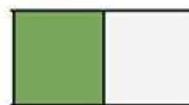
100 a.c: nonostante sia molto vecchio è stato utilizzato più recentemente in Russia (durante il periodo degli zar) e dai prigionieri di guerra durante la guerra del Vietnam.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Noi proveremo una variante di Polibio con i colori....

	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					

Proviamo a decifrare questo messaggio

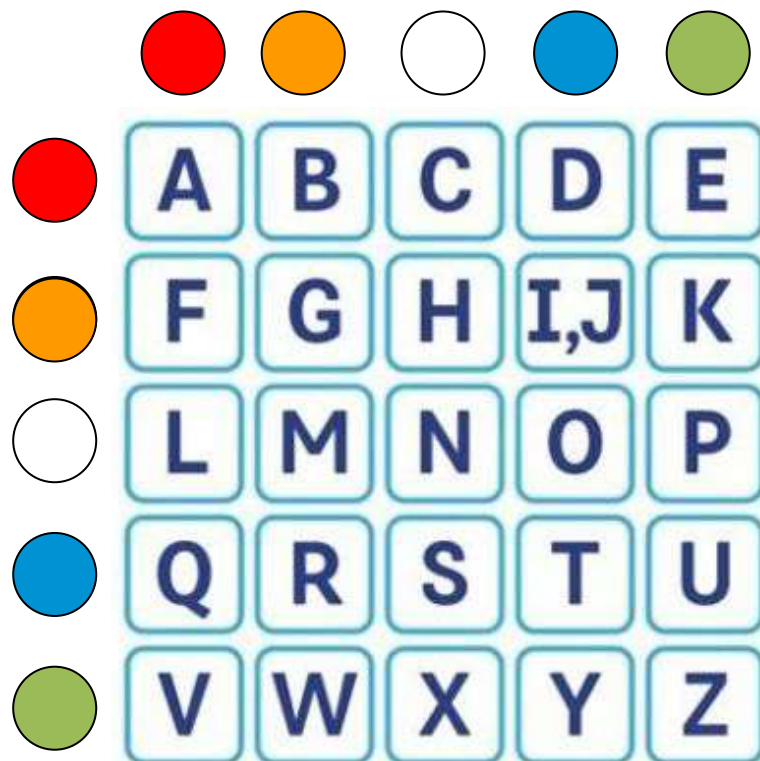


	○	●	●	●	●
○	A	B	C	D	E
●	F	G	H	I,J	K
●	L	M	N	O	P
●	Q	R	S	T	U
●	V	W	X	Y	Z

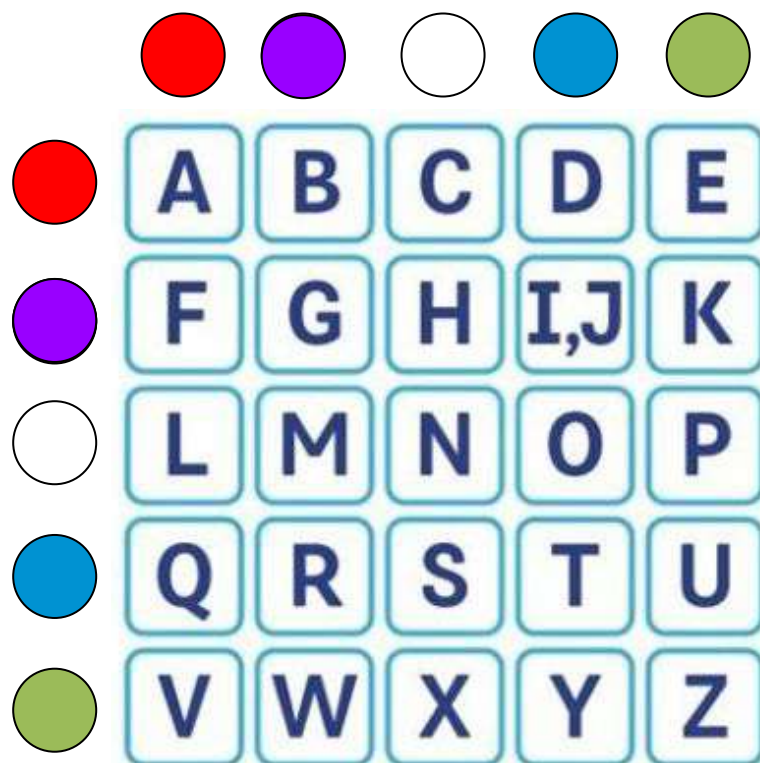




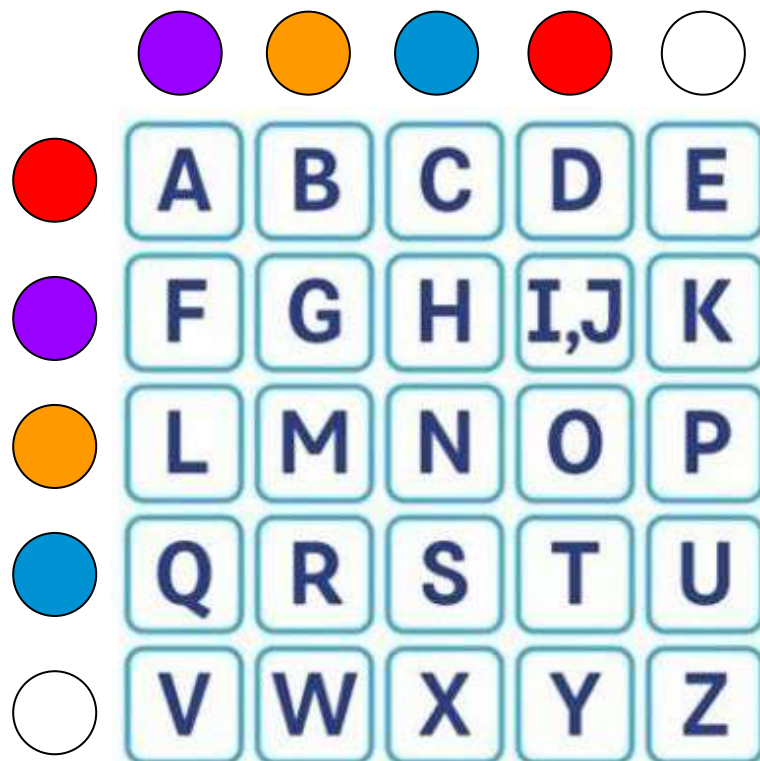
Quante chiavi diverse possiamo creare?



Quante chiavi diverse possiamo creare?



Quante chiavi diverse possiamo creare?



Giochiamo col cifrario di Polibio sperimentando chiavi diverse

EXTRA: l'analisi delle frequenze

cifrario

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

messaggio in chiaro

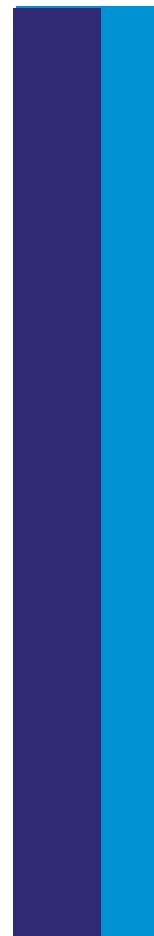
la partenza è prevista alle otto in punto

messaggio cifrato

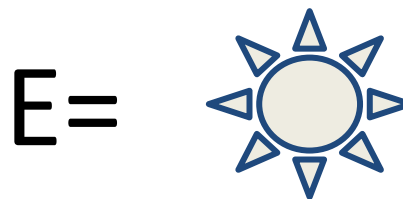
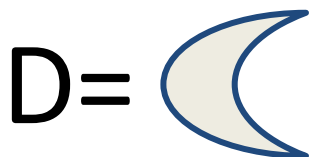
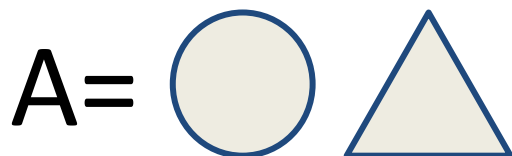
BP TPXDCKYP C TXCNOZDP PBBC QDDQ OK TJKDQ

Adesso create il vostro codice!

**Regola: dovete usare questi simboli per
codificare le lettere dell'alfabeto**



esempio:



...

...

...



E ora... giochiamo con la macchine cifranti!



Il lavoro necessario per **cifrare** e **decifrare** un messaggio segreto è inevitabilmente lungo e noioso; abbondano quindi nella storia della crittografia i progetti più o meno fortunati di **macchine cifranti automatiche**.

L'idea di fondo è in genere quella di uno o più **dischi o cilindri rotanti** che permettono di trasformare automaticamente le lettere del testo chiaro in quelle del testo cifrato e viceversa.

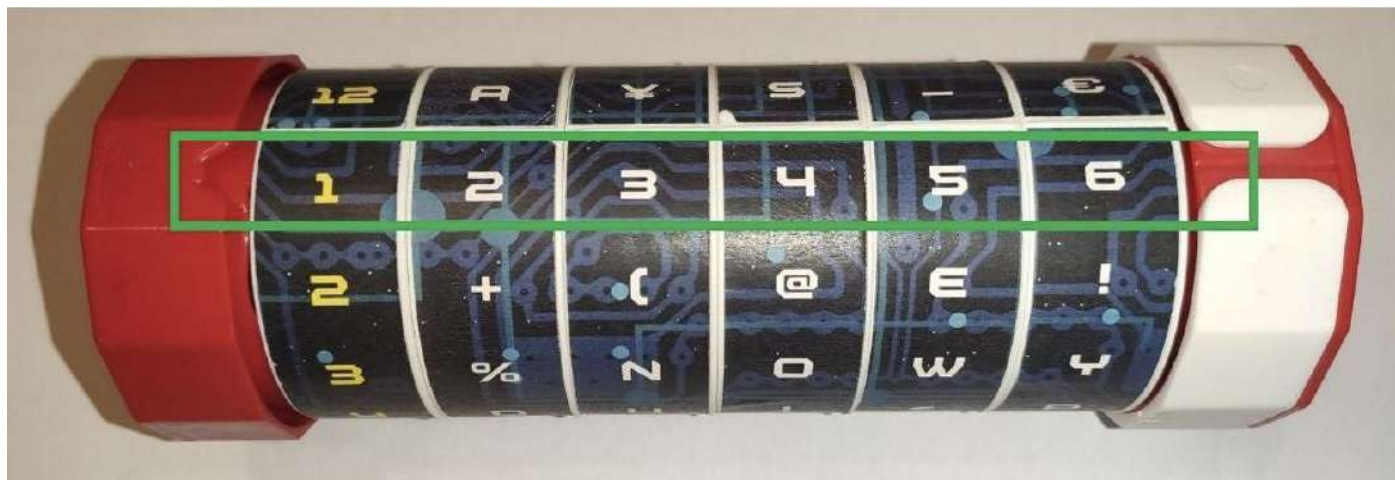


La **macchina Sigaba**, usata dagli Stati Uniti nella II guerra mondiale è l'unica macchina cifrante a non essere mai stata forzata. (dal sito del National Cryptologic Museum)

La macchina ENIGMA



E adesso ...la nostra enigma!



Passo 1 Scelta della chiave: per prima cosa è necessario decidere la chiave;

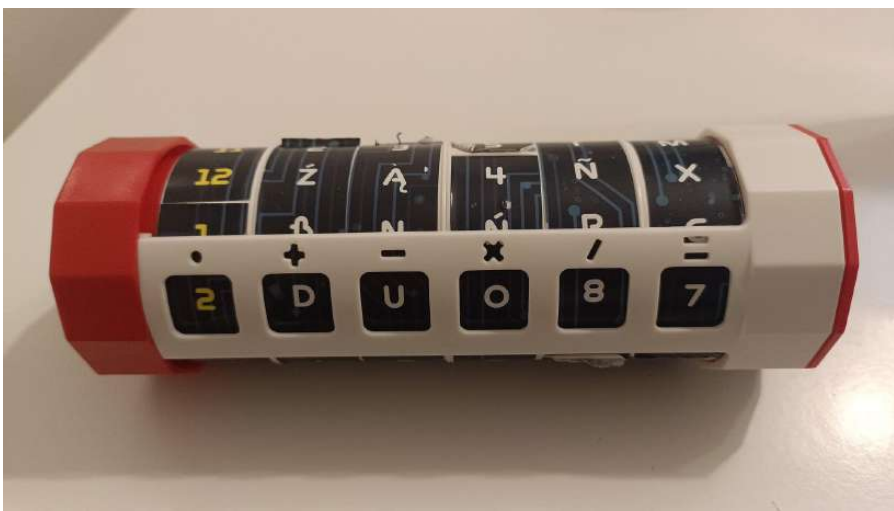
La scelta della chiave consiste nella rotazione dei dischi: si girano i dischi fino a che nel selettore bianco non comparirà la chiave scelta.

Si può scegliere una chiave in modo casuale, l'importante è **scriversi da qualche parte la chiave utilizzata e non perderla.**



Cifrare un testo:

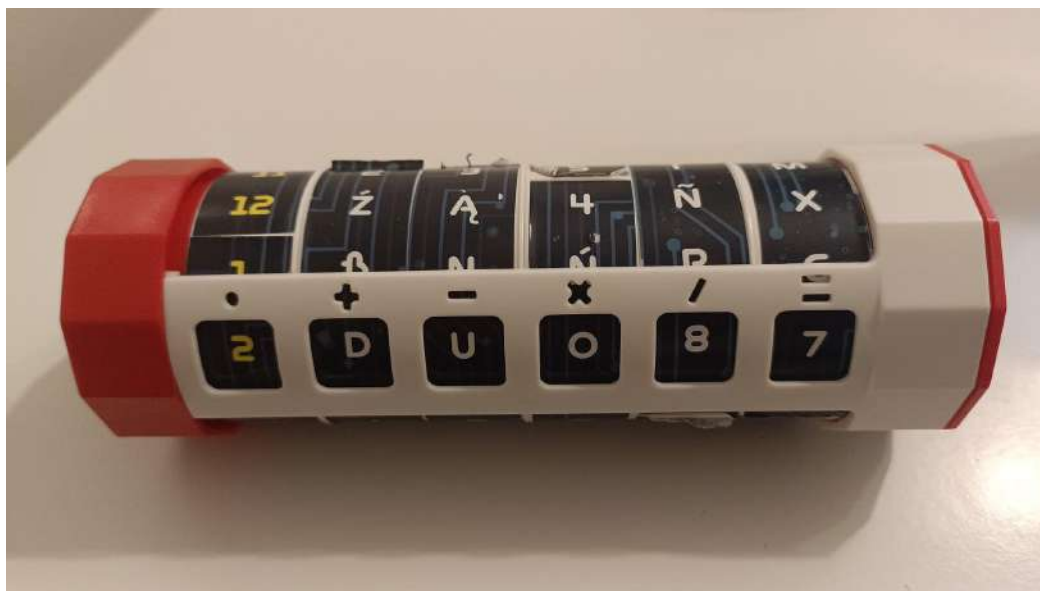
1. scegliere una chiave e segnlarla su un foglio*
2. ora **non bisognerà più ruotare i dischi** ma solo il selettore bianco
3. inquadrare la lettera che vogliamo cifrare con il selettore bianco
4. la lettera cifrata sarà la coppia **numero giallo** della riga & **simbolo (+, -, x, /, =)** corrispondente sul selettore



*chiave:

2 D U O 8 7

chiave 2 D U O 8 7



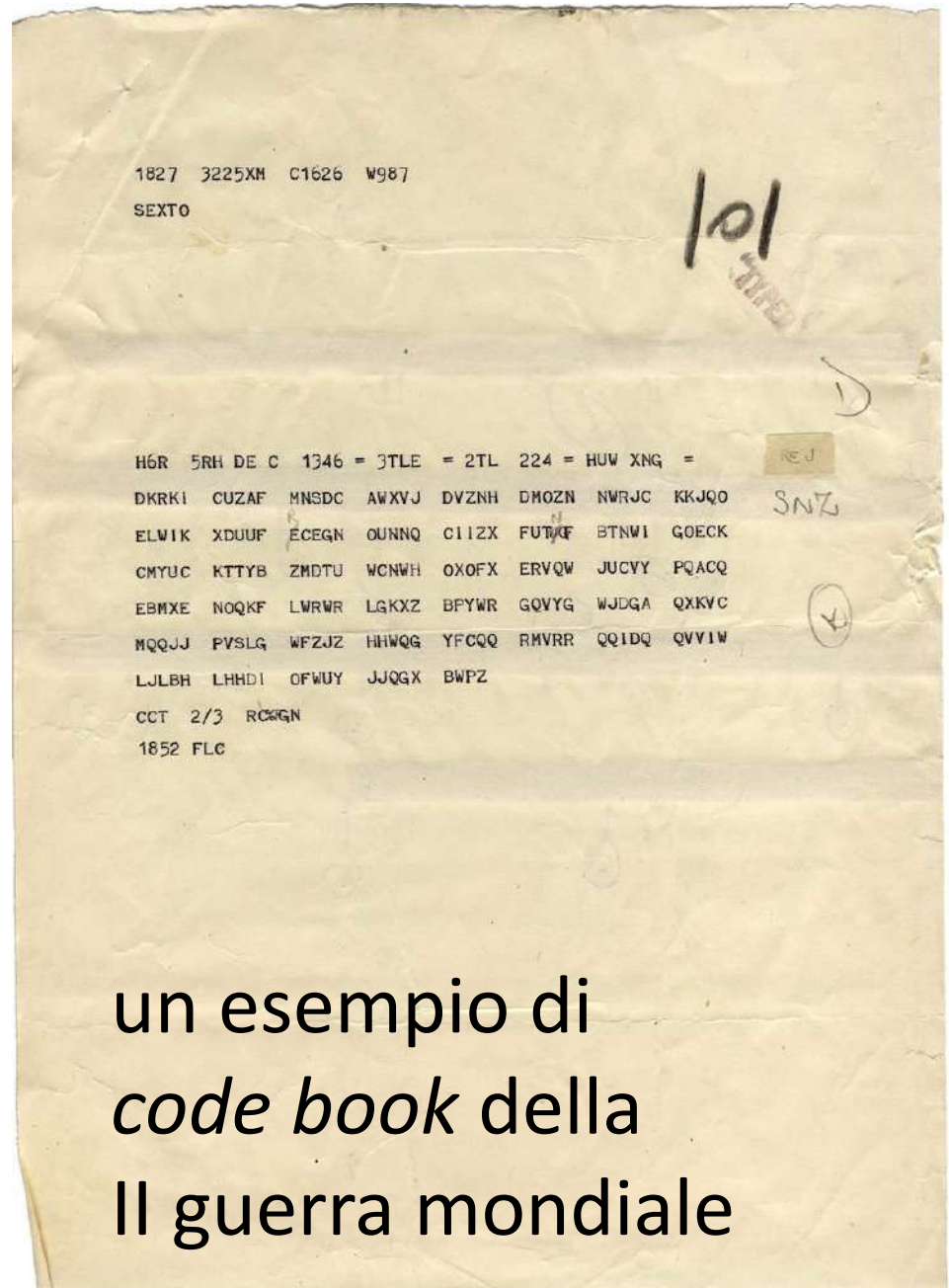
Decifriamo:

11x 3+ 4+ 5/



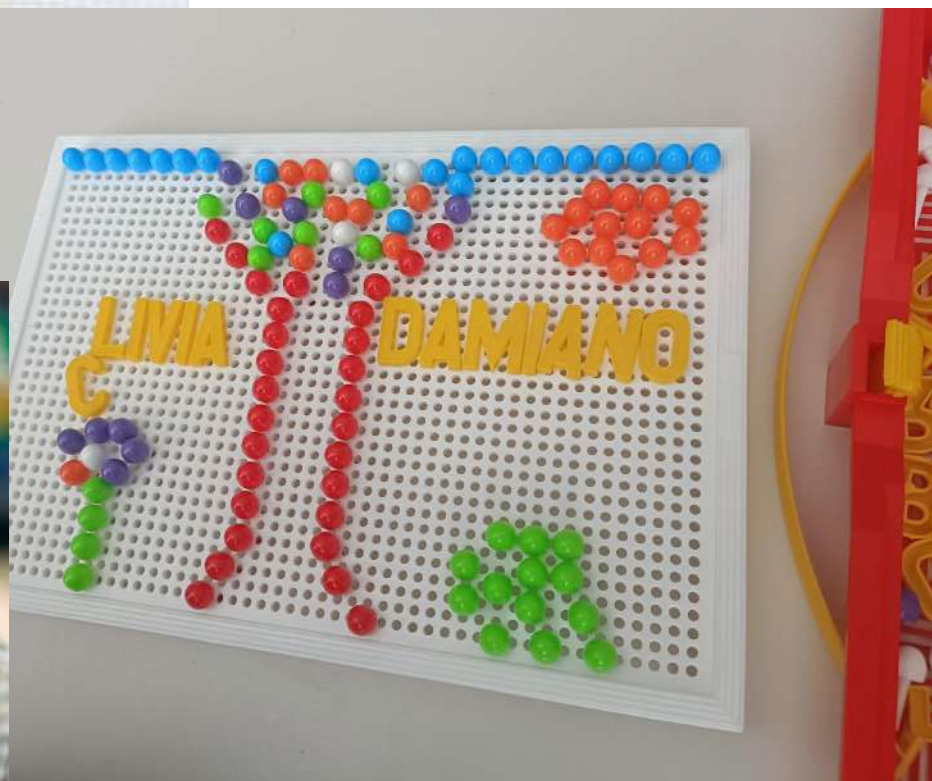
Scambiamoci messaggi in codice!

1. 1DV9CG
2. 3LBSWX
3. 5OVO56
4. 7ZHIC6
5. 9QHÆ56



Appunti sull'inclusione





Dalle nuove indicazioni nazionali

OBIETTIVI SPECIFICI DI APPRENDIMENTO AL TERMINE DELLA CLASSE TERZA

Scegliere ed utilizzare oggetti o simboli per rappresentare informazioni.

Descrivere a parole attività della vita quotidiana tramite sequenze di passi precisi e non ambigui e saperle eseguire.



CONVEGNO ITALIANO
SULLA DIDATTICA DELL'INFORMATICA