Fondazione CRT | Progetto DIDEROT

[ITADINFO]
CONVEGNO ITALIANO
SULLA DIDATTICA DELL'INFORMATICA

UNIVERSITÀ DI TORINO | Dipartimento di Informatica

La crittografia? è un Gioco!



Copyleft- CC BY-SA

Iniziativa realizzata nell'ambito del Progetto Diderot della Fondazione CRT

LINEA 11

LA CRITTOGRAFIA? È UN GIOCO!

ambito disciplinare:

INFORMATICA, STORIA, MATEMATICA, EDUCAZIONE CIVICA

classi 3°,4°,5°

finalità:

introdurre gli studenti ai principi fondamentali della crittografia attraverso i concetti di algoritmo, codifica e rappresentazione dell'informazione, utilizzando anche esercizi ispirati ai principali cifrari storici. Il percorso ripercorre l'evoluzione delle tecniche di cifratura, dalle civiltà antiche all'era digitale, per comprendere le sfide legate alla protezione dei dati e alla sicurezza delle comunicazioni nel mondo contemporaneo.

numero di studenti: 7.000

- 2 incontri da circa 2 ore per ogni classe
- dalla terza primaria alla terza secondaria di secondo grado
- dai 7000 ai 9000 alunn* ogni anno
- tutte le province di Piemonte e Val D'Aosta

Progettazione didattica

- differenziazione di percorsi per fascia di età
  - 3-4 primaria
  - 5 primaria 1 secondaria di secondo grado
  - 2-3 secondaria di primo grado

- approccio unplugged

Fondazione CRT | Progetto DIDEROT

[ITADINFO]
CONVEGNO ITALIANO
SULLA DIDATTICA DELL'INFORMATICA

UNIVERSITÀ DI TORINO | Dipartimento di Informatica

Che cos'è la crittografia?
Quando è nata?



A.S. 2024/2025
Copyleft- CC BY-SA
Sara Capecchi

La crittografia è antichissima!



1900 a.C.



1500 a.C.



650 a.C.

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

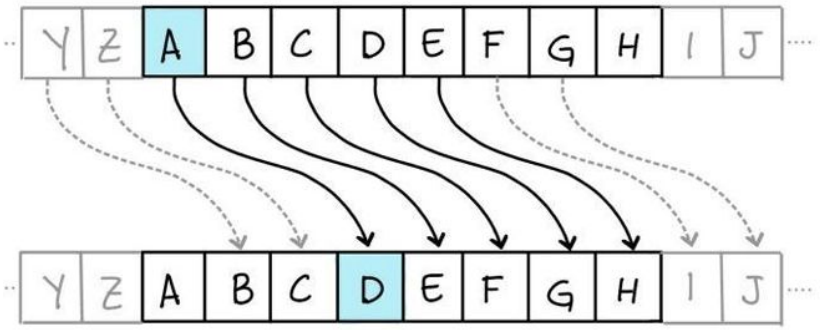
A.S. 2024/2025
Copyleft- CC BY-SA
Sara Capecchi

Fondazione CRT | Progetto DIDEROT

[ITADINFO]
CONVEGNO ITALIANO
SULLA DIDATTICA DELL'INFORMATICA

UNIVERSITÀ DI TORINO | Dipartimento di Informatica

Crittografia con il cifrario di Cesare





A.S. 2024/2025
Copyleft- CC BY-SA
Sara Capecchi

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

(cc) BY-SA **Michael Lodi, Marco Sbaraglia, Simone Martini**, 2021. Creative Commons Attribution-ShareAlike 4.0 International License

Fondazione CRT | Progetto DIDEROT

[ITADINFO]
CONVEGNO ITALIANO
SULLA DIDATTICA DELL'INFORMATICA

UNIVERSITÀ DI TORINO | Dipartimento di Informatica

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

A.S. 2024/2025
Copyleft- CC BY-SA
Sara Capecchi

Siete pronti per un nuovo sistema?

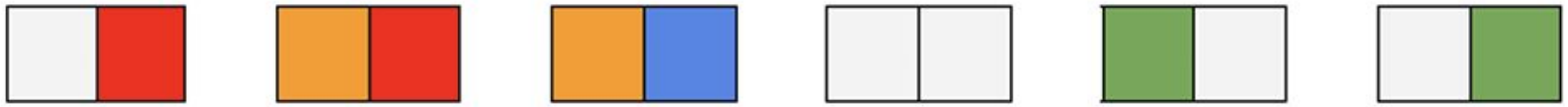
Cifrario di Polibio

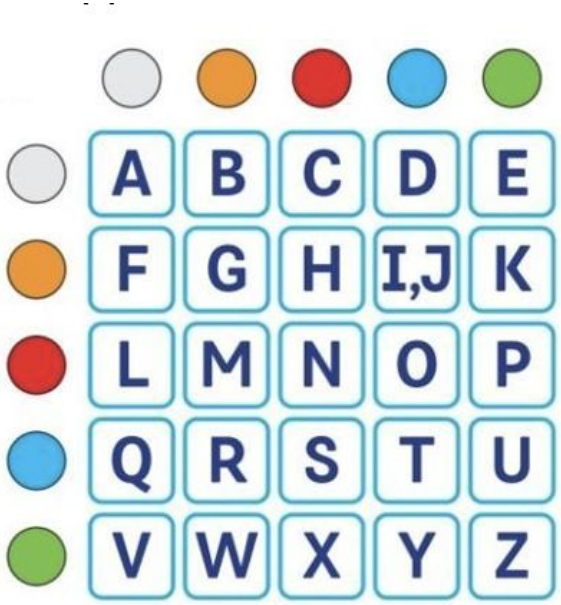
100 a.c: nonostante sia molto vecchio è stato utilizzato più recentemente in Russia (durante il periodo degli zar) e dai prigionieri di guerra durante la guerra del Vietnam.

	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

A.S. 2024/2025
Copyleft- CC BY-SA
Sara Capecchi

Proviamo a decifrare questo messaggio

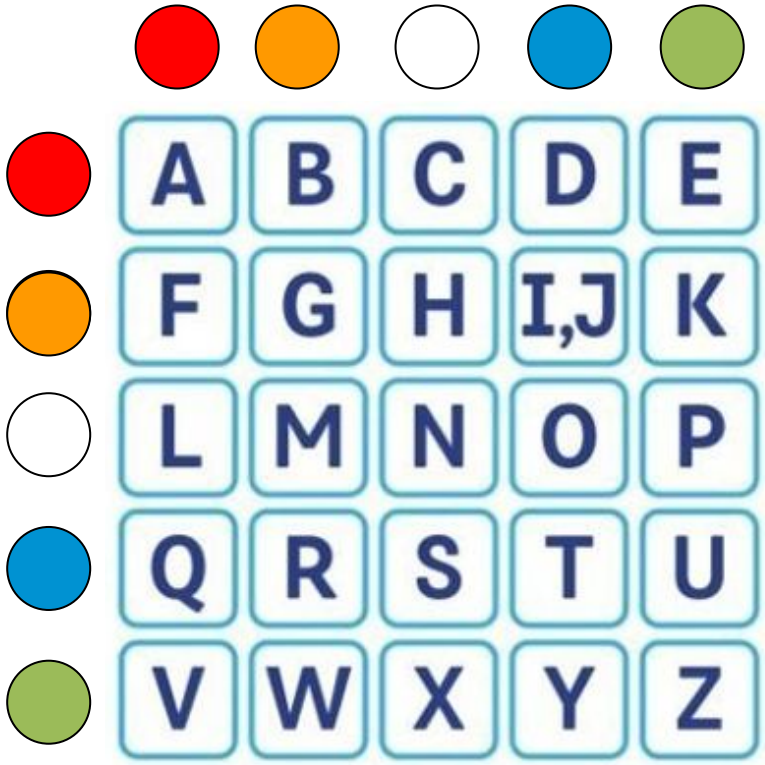




Copyleft- CC BY-SA
Sara Capecchi


Quercetti
Peg
Code
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
DI DEROT

Quante chiavi diverse possiamo creare?



Fondazione CRT | Progetto DIDEROT

[ITADINFO]
CONVEGNO ITALIANO
SULLA DIDATTICA DELL'INFORMATICA

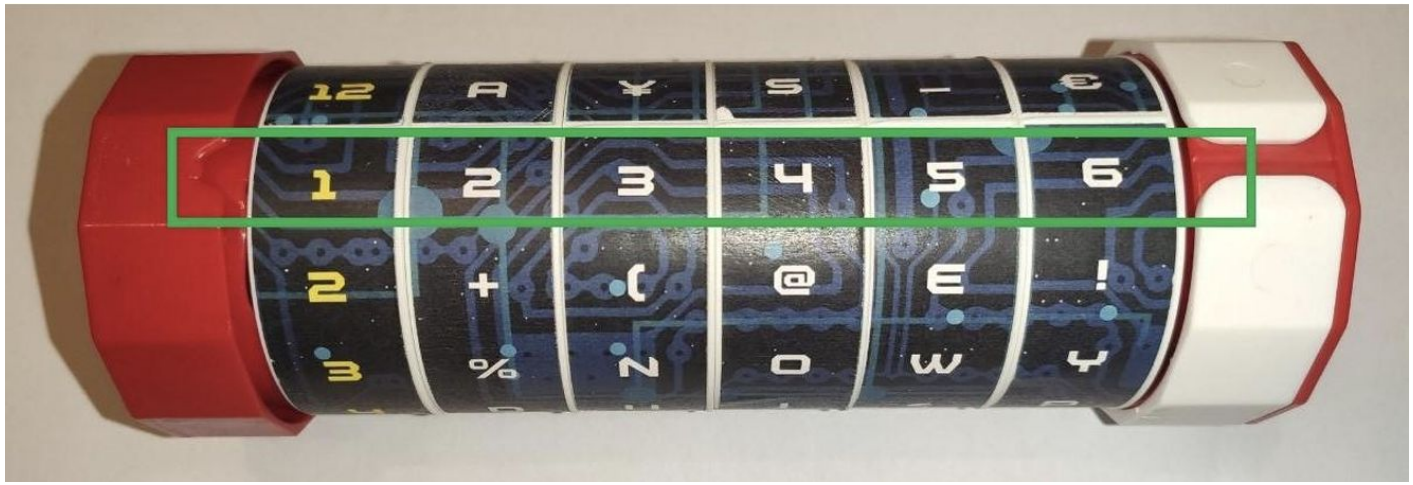
UNIVERSITÀ DI TORINO | Dipartimento di Informatica

La macchina ENIGMA



A.S. 2024/2025
Copyleft- CC BY-SA
Sara Capecchi

E adesso …la nostra enigma!



A.S. 2024/2025
Copyleft- CC BY-SA
Sara Capecchi

Fondazione CRT | Progetto DIDEROT

[ITADINFO]
CONVEGNO ITALIANO
SULLA DIDATTICA DELL'INFORMATICA

UNIVERSITÀ DI TORINO | Dipartimento di Informatica

Adesso create il vostro codice!

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

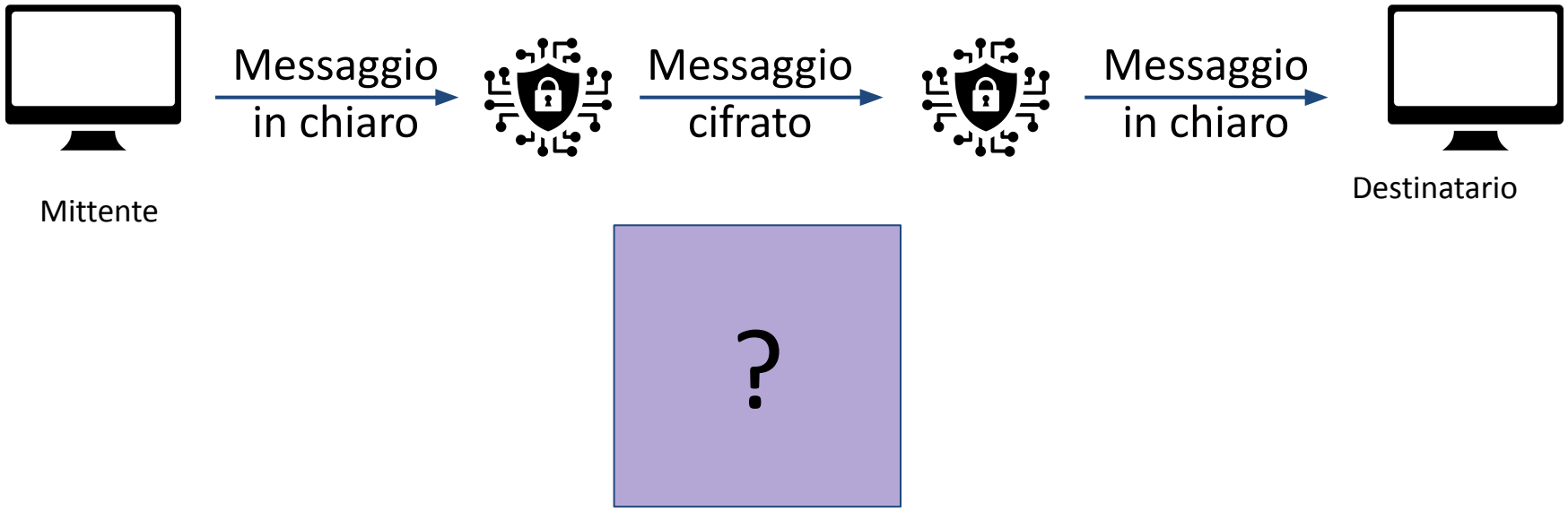


A.S. 2024/2025
Copyleft- CC BY-SA
Sara Capecchi

OK, ma dove sta l'informatica??



Perché la crittografia oggi è così complicata?



Fondazione CRT | Progetto DIDEROT

[ITADINFO]
CONVEGNO ITALIANO
SULLA DIDATTICA DELL'INFORMATICA

UNIVERSITÀ DI TORINO | Dipartimento di Informatica

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.

A.S. 2024/2025
Copyleft- CC BY-SA

Fondazione CRT | Progetto DIDEROT

[ITADINFO]
CONVEGNO ITALIANO
SULLA DIDATTICA DELL'INFORMATICA

UNIVERSITÀ DI TORINO | Dipartimento di Informatica

Appunti sull'inclusione

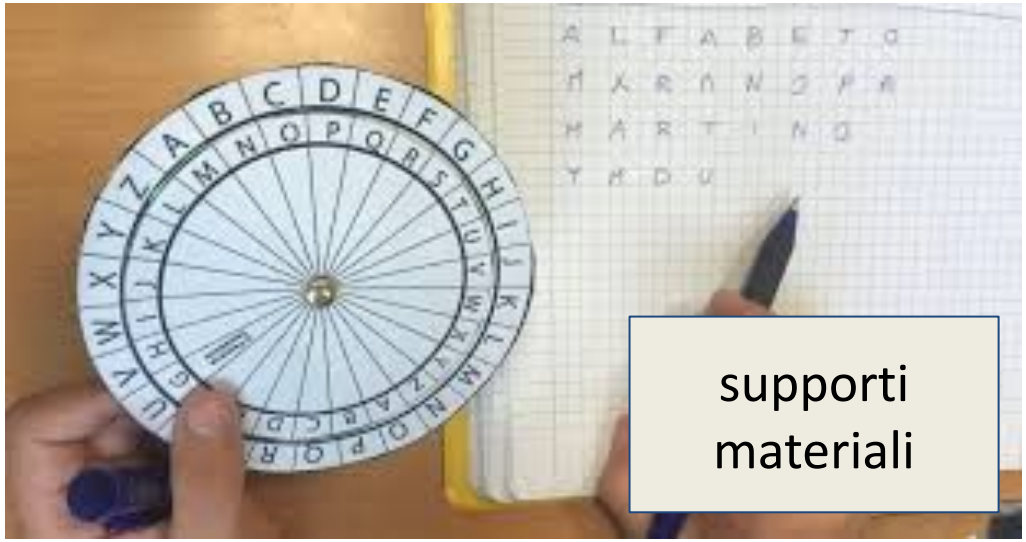


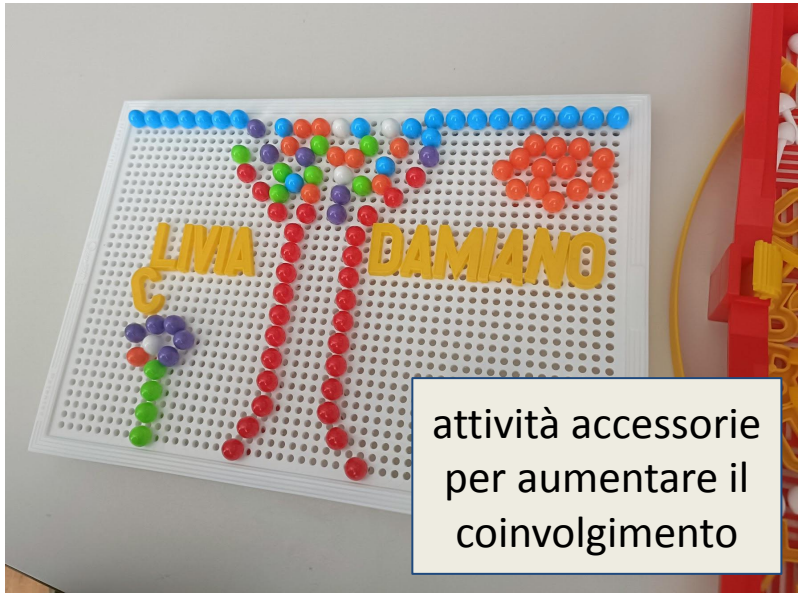
A.S. 2024/2025
Copyleft- CC BY-SA

Fondazione CRT | Progetto DIDEROT

[ITADINFO]
CONVEGNO ITALIANO
SULLA DIDATTICA DELL'INFORMATICA

UNIVERSITÀ DI TORINO | Dipartimento di Informatica









Grazie dell'attenzione!

…domande?



La crittografia si usa anche oggi





Fondazione CRT | Progetto DIDEROT

[ITADINFO]
CONVEGNO ITALIANO
SULLA DIDATTICA DELL'INFORMATICA

Dipartimento di Informatica
UNIVERSITÀ DI TORINO
DIPARTIMENTO DI INFORMATICA

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

A.S. 2024/2025
Copyleft- CC BY-SA
Sara Capecchi

Fondazione CRT | Progetto DIDEROT

[ITADINFO]
CONVEGNO ITALIANO
SULLA DIDATTICA DELL'INFORMATICA

Dipartimento di Informatica
UNIVERSITÀ DI TORINO
DIPARTIMENTO DI INFORMATICA

La crittografia durante la II Guerra Mondiale



Alan Turing



A.S. 2024/2025
Copyleft- CC BY-SA
Sara Capecchi

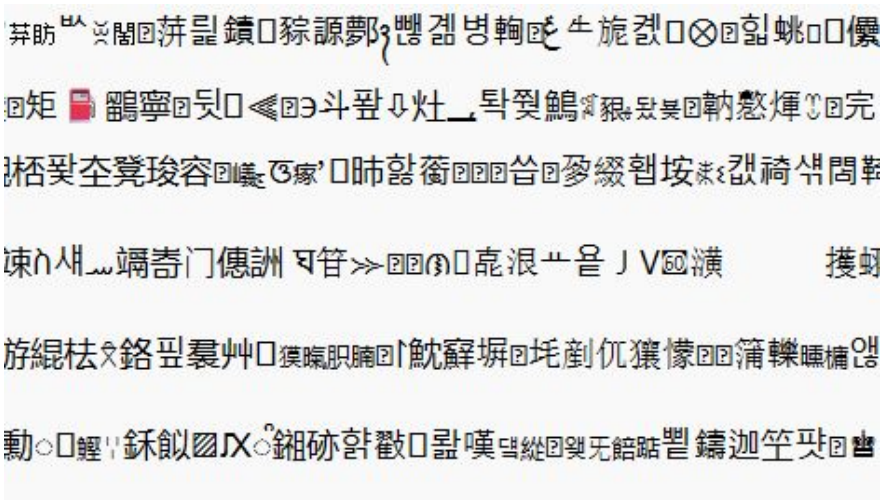
Fondazione CRT | Progetto DIDEROT

[ITADINFO]
CONVEGNO ITALIANO
SULLA DIDATTICA DELL'INFORMATICA

Dipartimento di Informatica
UNIVERSITÀ DI TORINO
DIPARTIMENTO DI INFORMATICA

La crittografia nell'era dei computer e di Internet



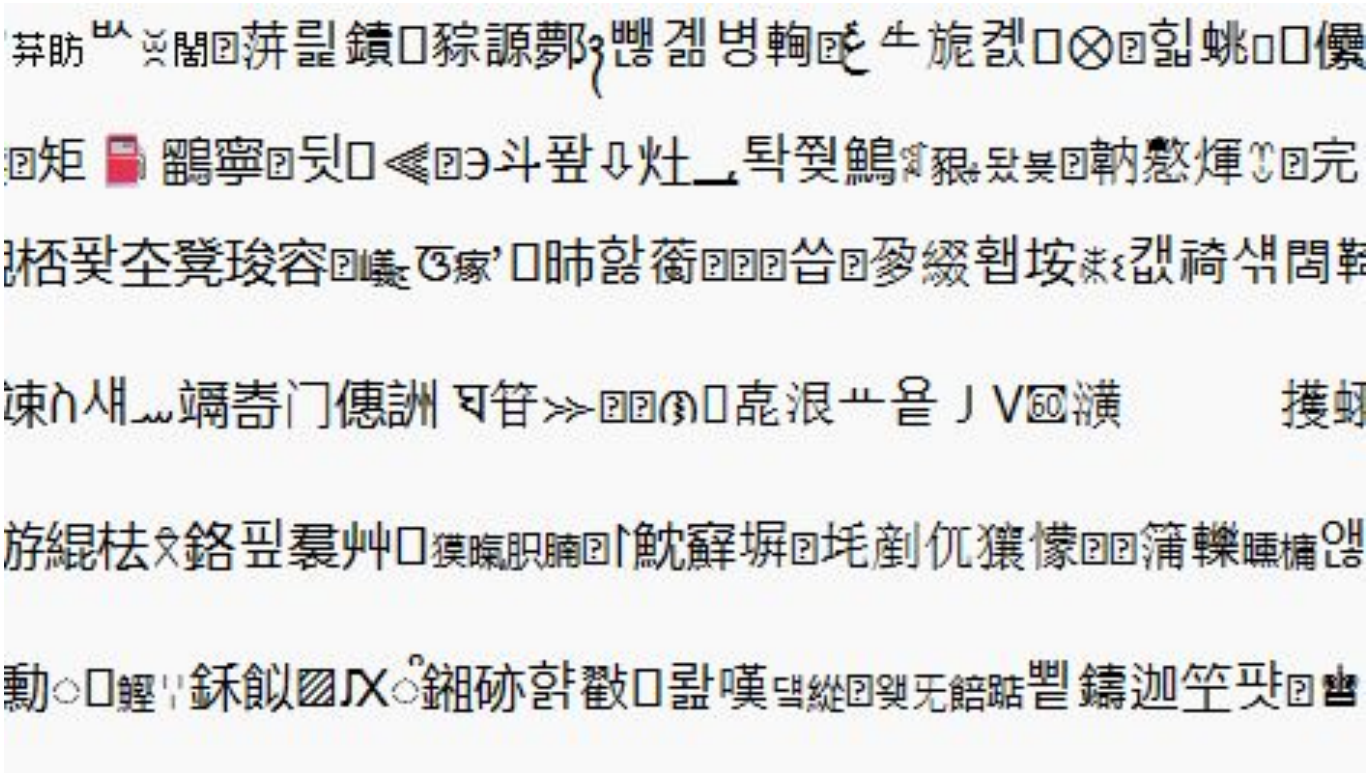




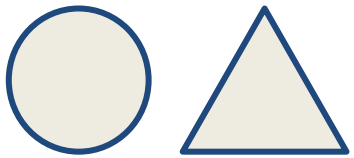


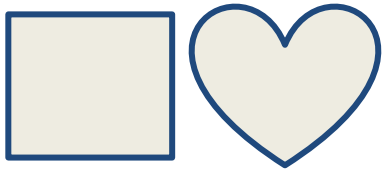
A.S. 2024/2025
Copyleft- CC BY-SA
Sara Capecchi

un file cifrato dal mio PC:



esempio:

A= 

B= 

D= 

E= 

. . .

. . .

. . .

A.S. 2024/2025
Copyleft- CC BY-SA
Sara Capecchi

Fondazione CRT | Progetto DIDEROT

[ITADINFO]
CONVEGNO ITALIANO
SULLA DIDATTICA DELL'INFORMATICA

UNIVERSITÀ DI TORINO
Dipartimento di Informatica
DIPARTIMENTO DI INFORMATICA

E ora… giochiamo con la macchine cifranti!

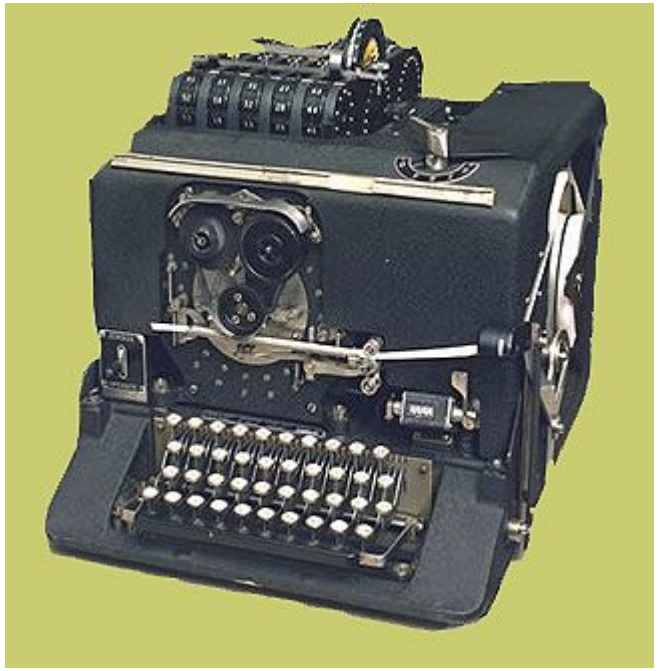


A.S. 2024/2025
Copyleft- CC BY-SA

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.

A.S. 2024/2025
Copyleft- CC BY-SA
Sara Capecchi



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)

A.S. 2024/2025
Copyleft- CC BY-SA
Sara Capecchi

Fondazione CRT | Progetto DIDEROT

[ITADINFO]
CONVEGNO ITALIANO
SULLA DIDATTICA DELL'INFORMATICA

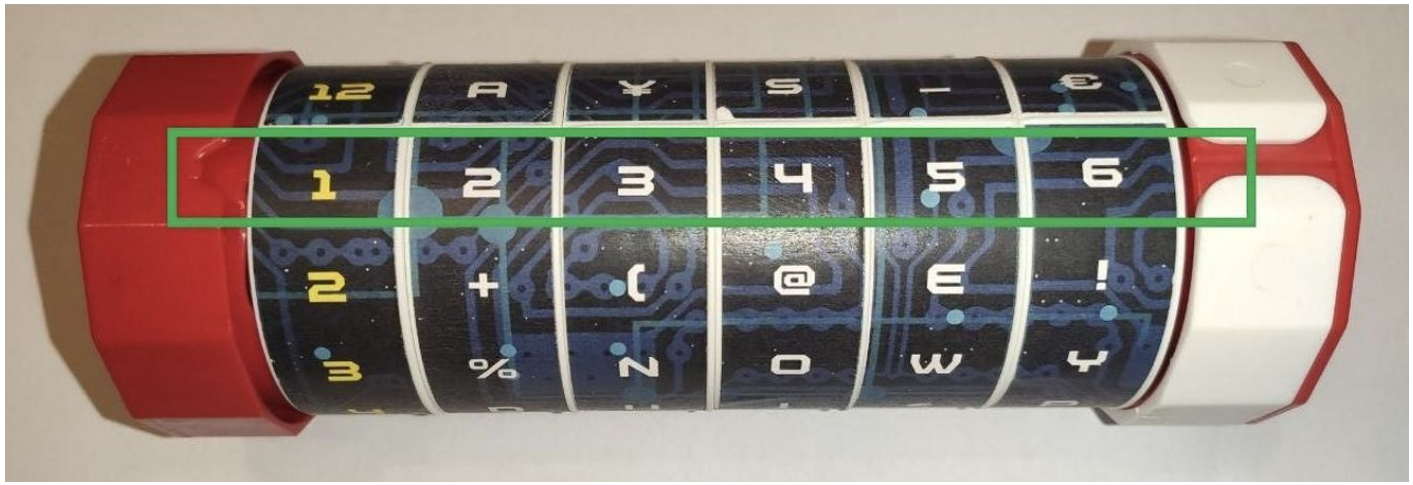
UNIVERSITÀ DI TORINO
DIPARTIMENTO DI INFORMATICA

La macchina ENIGMA



A.S. 2024/2025
Copyleft- CC BY-SA
Sara Capecchi

E adesso …la nostra enigma!



A.S. 2024/2025
Copyleft- CC BY-SA
Sara Capecchi

Cifrare un testo:

1. scegliere una chiave e segnarla 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