UNIVERSITÀ DEGLI STUDI FIRENZE | OpenLAB EDUCAZIONE E DIVULGAZIONE SCIENTIFICA

Il cifrario di Cesare e di Vigenere (14 anni in su)

Giulio Cesare era solito comunicare con i suoi generali tramite messaggi cifrati, in modo tale che né i suoi nemici né tanto meno le spie del senato di Roma, potessero prevedere le sue mosse.

Il metodo era molto semplice: ad ogni lettera sostituiva quella che nell'alfabeto si trova tre posizioni dopo (consideriamo l'alfabeto esteso di 26 lettere, quindi con anche le lettere J,K,W,X,Y), ad esempio la lettera A diventa la lettera D, B diventa E, e così via. Per le lettere in fondo all'alfabeto ricominciava a contare da capo, quindi alla lettera X corrisponde la lettera A, a Y corrisponde B e a Z corrisponde C.

Sai decifrare il messaggio di Cesare al suo generale?
DWWDFFDUH JOL LUULGYFLELOL JDOOL DOOD RUD VHVWD

In termini tecnici, Cesare usava la chiave "3", che corrisponde appunto al numero di lettere da saltare.

Un generale distratto però, nel rispondere al suo condottiero, ha sbagliato chiave, e il messaggio arrivato a Cesare è il seguente:

FNZYT HN XJWATST N WNSKTWEN

Cesare non si lascia abbattere, e riesce a capire che la lettera N corrisponde alla lettera I.
Cosa gli ha risposto il generale?

Questo metodo di cifratura è stato arricchito nei secoli, anche perchè piuttosto vulnerabile se si sa quale metodo viene usato, ma può essere impiegato per crittografie più complesse, come il ***Cifrario di Vigenere***.

Questo cifrario si basa su una parola (addirittura a volte una frase o un testo) chiave, che viene usata per rappresentare un cifrario di Cesare che si alterna.

Ad esempio, se la chiave è ROSE, prova a cifrare
INCONTRIAMOCI

Suggerimento prova a visualizzare il problema così

R	**O**	**S**	**E**	**R**	**O**	**S**	**E**	**R**	**O**	**S**	**E**	**R**
I	**N**	**C**	**O**	**N**	**T**	**R**	**I**	**A**	**M**	**O**	**C**	**I**

Se ti diverte cifrare, puoi stampare i due dischetti in allegato, fissando uno nel centro dell'altro tramire un fermacampione. Sarà molto più veloce cifare e decifare messaggi!

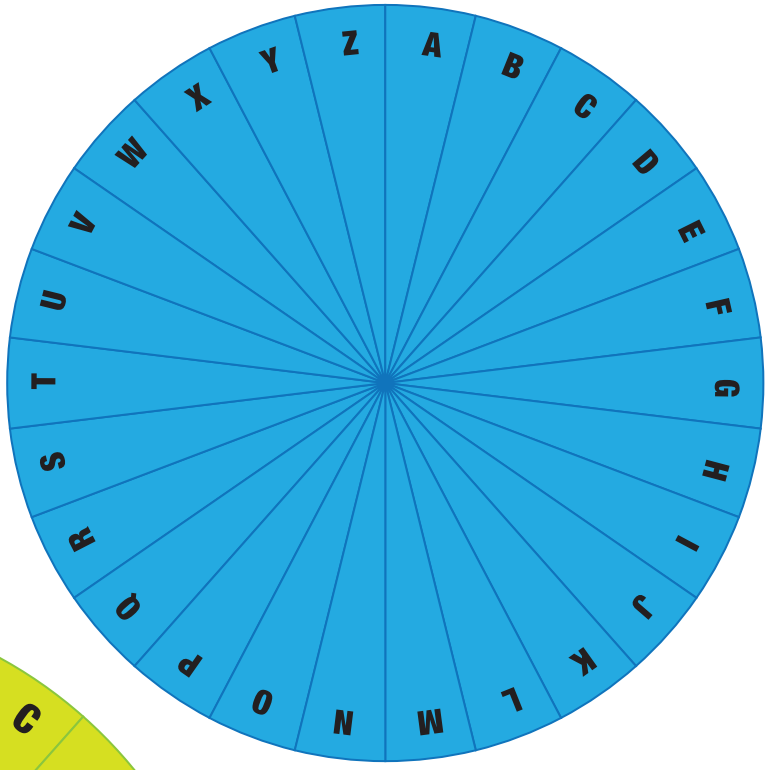
giochi

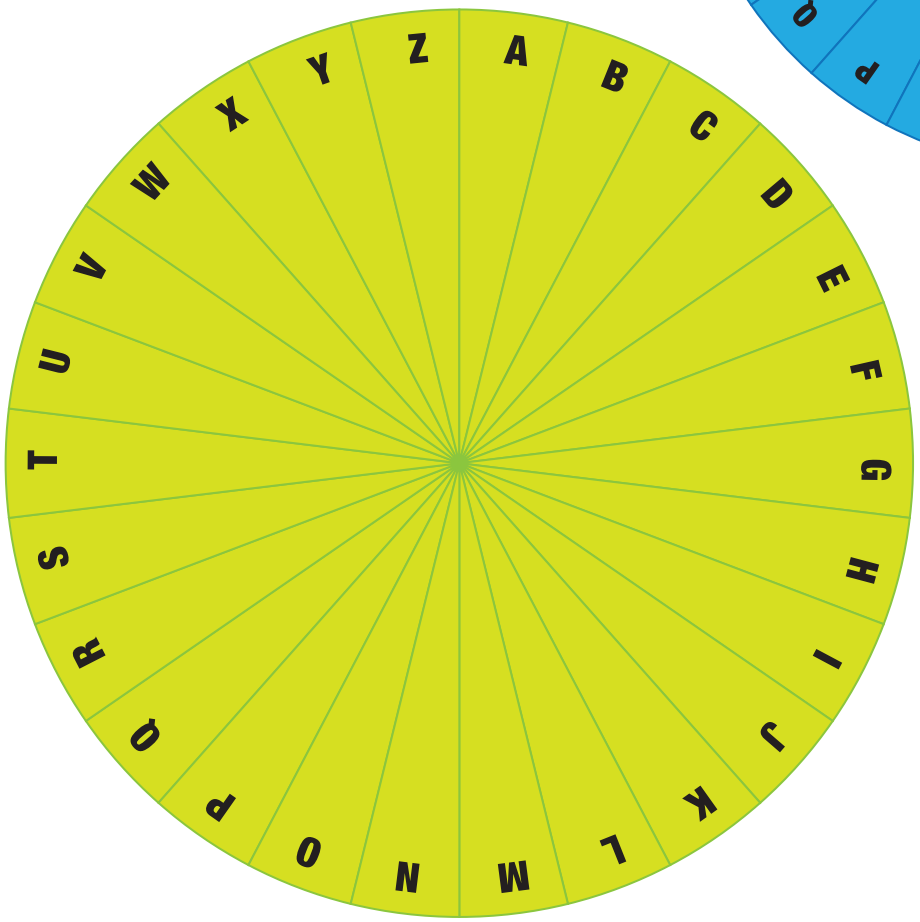
SCIENZESTATE 2020
www.openlab.unifi.it
OpenLab_Firenze
#scienzestate

UNIVERSITÀ DEGLI STUDI FIRENZE

OpenLAB
EDUCAZIONE E DIVULGAZIONE SCIENTIFICA

1. Ritaglia il disco blu **BLU** e foralo nel centro.
2. Ritaglia il disco **VERDE** e foralo nel centro.
3. Sovrapponi i due dischi e fermali nel centro con l'aiuto di un fermacampioni.





giochi

SCIENZESTATE 2020

www.openlab.unifi.it
OpenLab_Firenze
#scienzestate

SOLUZIONE

Nel primo messaggio Cesare dice al suo generale: **ATTACCARE GLI IRRIDUCIBILI GALLI ALLA ORA SESTA**

Basta infatti considerare la seguente tabella dove a ogni lettera quella sotto corrisponde alla sua codifica (da leggere quindi dal basso verso l'alto se si vuole decodificare).

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
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

Nel messaggio del generale, se la lettera N corrisponde alla lettera I, vuol dire che per leggere il messaggio bisogna saltare 5 lettere: ...H **I** J K L M **N** O...
Quindi la chiave è 5 ed il messaggio è: **AIUTO CI SERVONO I RINFORZI**

Più in generale, questo metodo si basa sulle così dette *classi di resto*.

Infatti, assegnando ad ogni lettera dell'alfabeto il numero della posizione corrispondente (quindi A=1, B=2,...,Z=26), per ottenere la cifratura basta sommare la chiave e poi prendere il resto della divisione per 26.

esempio
con la chiave 3 la lettera X diventa A.
Infatti X=24, e (24+3):7 da come resto 1=A.

ATTENZIONE
la chiave D corrisponde al numero 3, perché appunto alla lettera A=1, 1+3=4=D.

Quindi quando la chiave è data in forma di lettera, la forma numerica sarà data dalla sua posizione meno uno.

Raggruppiamo le lettere corrispondenti allo stesso elemento della chiave, ad esempio per la R avremo la prima, la quinta, la nona e la tredicesima lettera, ovvero INAI. A questo punto basta cifrare la parola tramite il cifrario di Cesare corrispondente alla lettera R, ottenendo ZERZ. Ripetendo lo stesso procedimento con le lettere corrispondente agli altri elementi della chiave, otteniamo ZBUTEHJNRAGHZ.