

LABORATORIO DI CRITTOGRAFIA

Il 26 marzo 2010 la classe 2C_L ha partecipato al “Laboratorio di crittografia”, inserito nell’ambito della settimana “L’avventura della scienza” presso il Dipartimento di Matematica in via Saldini a Milano. Il ricercatore Ottavio Rizzo ha tenuto il laboratorio, coinvolgendoci in modo attivo.

La parola crittografia deriva dall'unione di due parole greche: kryptos = nascosto e graphein = scrivere ed è un linguaggio segreto che permette di comunicare in presenza degli avversari.

Il suo primo utilizzo risale ai tempi di Giulio Cesare, che la adoperava per comunicare con i suoi generali.

Per cifrare intendiamo scrivere il messaggio in codice, per decifrare invece, intendiamo “tradurre” il messaggio come testo in chiaro.

Il metodo utilizzato da **Giulio Cesare** consisteva nel sostituire ciascuna lettera del messaggio con un'altra lettera che si trovasse tre posti più avanti nell’alfabeto. (**Chiave D**)

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

Ad esempio AVE diventa DYH.

In questo modo era garantita la piena sicurezza del messaggio poiché, anche nel caso in cui gli avversari lo avessero intercettato, sarebbe risultato loro privo di significato.

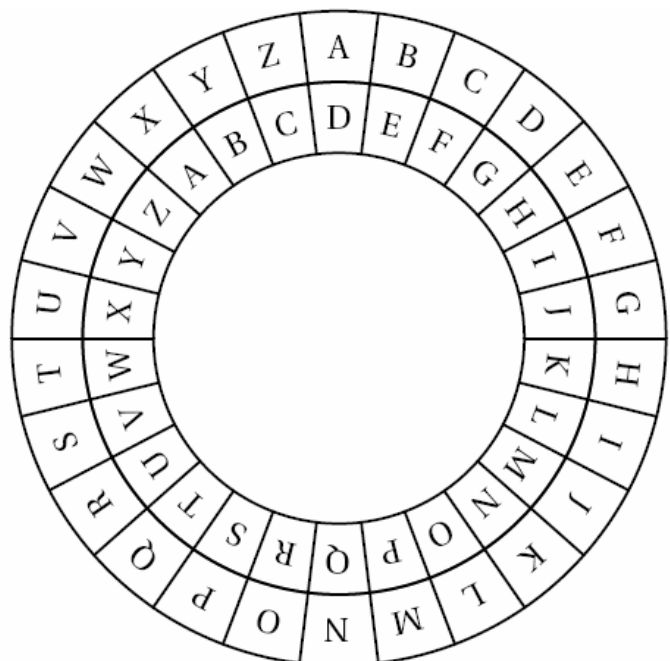
Ma a questo punto, come poteva il destinatario decifrare il messaggio? Ecco che abbiamo bisogno della chiave; essa indica la lettera a cui corrisponde la A e ci dice quindi di quante lettere più avanti è stato spostato l'alfabeto. Nel caso in cui non fosse nota la chiave, basta provare con le 25 chiavi diverse e scoprire il messaggio inviato.

Per decifrare più facilmente un messaggio in codice possiamo utilizzare il **disco cifrante** di Leon Battista Alberti composto da due dischi fissati al centro (che ruotano), sulle estremità dei quali viene scritto l'alfabeto, ruotando la ruota interna in modo da posizionare la chiave sotto la A, abbiamo la corrispondenza tra tutte le lettere.

Così il messaggio DYH decifrato diventa AVE

Il Cifrario di Cesare poteva però essere facilmente rotto poiché, una volta appreso il metodo di cifrazione, era possibile risalire al messaggio provando a decifrarlo con tutte le 25 chiavi (la ventiseiesima avrebbe dato un cifrato uguale al messaggio iniziale); per questo motivo si iniziò a cifrare il messaggio con più chiavi in modo tale da rendere impossibile la decifrazione.

E' possibile quindi utilizzare due chiavi diverse: ad esempio posizione dispari chiave D, posizione pari chiave C.



A V E C testo in chiaro

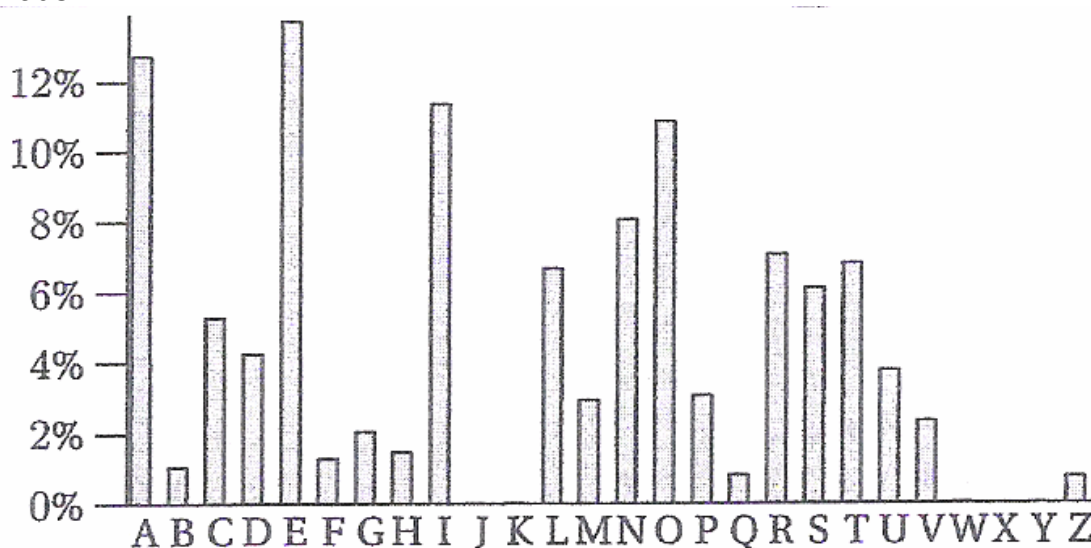
D C D C chiave

D X H E testo cifrato

A questo punto a tutti noi alunni è stato consegnato un messaggio da decifrare con il cifrario rotante, ma non era nota la chiave. Ci siamo divisi in gruppi in modo da poter provare tutte le chiavi possibili.

Il messaggio da decifrare era HUFPGYEFD. Dopo alcune prove, un gruppo ha capito che era W Juventus.

Un metodo utile per riuscire a decifrare un messaggio è quello di osservare la frequenza delle lettere cifrate nell'istogramma, ottenuto analizzando il Decamerone, I Promessi Sposi e Faust



Ci è stato consegnato il seguente messaggio

LOF	LIU	DUL	RGL	FHV	DUH	SXR	HVV	HUH	URW	WRP	ROW	RID	FLO	PHQ	WH
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	----

e utilizzando l'istogramma siamo riusciti a decifrarlo senza conoscerne la chiave.

La chiave era la lettera I e il messaggio era il seguente :

il cifrario di Cesare può essere rotto molto facilmente.

Ha fatto anche notare che decifrare un messaggio con la lettera F o cifrare con la lettera V si ottiene lo stesso messaggio, in quanto spostarsi di 21 lettere a destra è equivalente a spostarsi di 5 a sinistra, cioè $-5 \equiv 21$ in quanto $-5 \equiv 26-5$. Questo è un argomento di aritmetica modulare.

H J X F W J decifrando con F o cifrando con V diventa

C E S A R E

Abbiamo trovato quest'esperienza molto interessante: abbiamo appreso il modo in cui venivano trasmessi messaggi segretamente nell'antica Roma e successivamente.

Ci è sembrato strano assistere ad una lezione all'Università Statale però è stata anche una lezione particolarmente piacevole perchè abbiamo avuto un professore che è stato capace di interessarci e di coinvolgerci anche con attività di traduzione, dall' alfabeto originale a quello crittografato e viceversa.

Sarebbe bello poter ripetere l'esperienza in modo di approfondire ulteriormente l'argomento.

Una lezione di questo tipo sarebbe da consigliare anche ad altri ragazzi, può sempre servire !