CRITTOGRAFIA

Traccia: Dato un messaggio cifrato cercare di trovare il testo in chiaro.
Messaggio cifrato: "HSNFRGH"

Come spiegato oggi in classe, andremo a decifrare il messaggio crittografato che è stato fornito in traccia.
Per andare a “tradurre” tale messaggio, prima di tutto dobbiamo fare un salto indietro nel tempo all’epoca dell’Antica Roma, periodo in cui nasce un primo e rudimentale concetto di messaggio crittografato: il cifrario di Cesare.
L’idea del cifrario di Cesare nasce dall’esigenza di inviare e ricevere messaggi senza dare la possibilità all’esercito nemico di riuscire ad interpretarli, se intercettati.
Quindi l’imperatore Giulio Cesare ideò un sistema di cifrazione, noto solo ai generali dell’esercito, che consisteva in uno spostamento di 3 lettere all’interno dell’alfabeto, in maniera tale da rendere il messaggio incomprensibile.
In seguito è illustrata la tabella di cifrazione utilizzata, in cui la prima riga corrisponde al messaggio in chiaro, la seconda le corrispondenze nel messaggio cifrato:

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

Avendo trovato la chiave di lettura, possiamo andare a decifrare il messaggio crittografato.

H = E
S = P
N = I
F = C
R = O
G = D
H = E

Il messaggio, una volta decifrato, sarà la parola “EPICODE”.