

CIFRARIO DI CESARE

I più semplici cifrari, e anche i più antichi, sono i cifrari cosiddetti a *sostituzione*: essi consistono nella sostituzione di ciascuna delle 21 lettere che costituiscono l'alfabeto con un'altra lettera dello stesso alfabeto. In *termini matematici* si tratta dunque di operare una *permutazione* dell'alfabeto, dove per permutazione s'intende una *funzione* che trasforma l'alfabeto in se stesso facendo corrispondere a ogni lettera un'altra lettera (in generale diversa) e viceversa.

Numeriamo le lettere da 0 a 20

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z

Decidiamo che la nostra chiave sia 5

Scrivi quale posto occuperanno le singole lettere dopo lo spostamento e completa la tabella

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

Cifrare il seguente messaggio

"Nel mezzo del cammin di nostra vita"

Decritta il seguente messaggio

"HTIPHP L ALNZLBP"

Con chiave 15 cifrare il seguente messaggio

"DICHARARE LA PACE TRA I POPOLI"

Decritta il seguente messaggio

DR AOVLLR V ZCFCNR

ANALISI DELLE FREQUENZE

I cifrari per sostituzione non sono molto sicuri se si dispone di un messaggio cifrato abbastanza lungo, infatti si può fare l'analisi delle frequenze e individuare le lettere più frequenti confrontandoli con quelli della lingua del messaggio in chiaro.

Tavola delle frequenze della lingua italiana:

%	Lettera	%	Lettera	%	Lettera
11,79	e	5,63	t	2,10	v
11,74	a	4,98	s	1,65	g
11,28	i	4,50	c	1,54	h
9,83	o	3,73	d	0,95	f
6,88	n	3,05	p	0,92	b
6,51	l	3,02	u	0,51	q
6,38	r	2,52	m	0,49	z

Tavola delle frequenze lingua italiana

Hai intercettato il seguente messaggio cifrato

T	H		I	N	U		Z	B	N	C	D	V		D	E	D	D	R		R		C	V	P	U	R	

H	U	U	V		R	U	F	H	C	V		S	H		T	R	H		C	D	H	U	G	H			

Riporta nella tabella il numero di volte in cui ciascuna lettera compare nel messaggio cifrato:

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

Aiutandoti con la tavola delle frequenze della lingua italiana, prova a sostituire le lettere terminali di una parola con una vocale dell'alfabeto in chiaro, in ordine di frequenza. Controlla quanto hai ottenuto e, se lo ritieni opportuno, prova a cambiare alcune scelte utilizzando le consonanti più frequenti. Ora prova a sostituire le consonanti più frequenti non ancora utilizzate, rivedendo le scelte se trovi parole prive di significato.

Aiutati con l'alfabeto per decifrare:

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

Qual è il messaggio in chiaro?