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
"DICHIARARE 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	

LE CONGRUENZE E IL CIFRARIO DI CESARE

Ma la matematica dov'è?

Riprendiamo il primo esempio in cui la chiave è 5

La A in posizione 0 va in posizione 0+5=5

La B in posizione 1 va in posizione 1+5= 6

....

La S in posizione 16 va in posizione 16+5 =21 ma le posizioni possibili sono solo da 0 a 20 quindi andrà al posto della A, cioè in posizione 0

La T in posizione 17 va in posizione 17+5=22, andrà al posto della B cioè in pos izione 1

La U _____

La V _____

La Z _____

In matematica questo tipo di calcoli rientrano nell'aritmetica modulare o aritmetica dell'orologio.

Il primo ad ideare questa aritmetica fu Gauss

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

Definizione: Sia n un intero positivo fissato. Due numeri $a, b \in Z$ sono congrui modulo n se e solo se *a*-*b* è multiplo di n.

<u>Espresso in formule</u> $a \equiv b\ (mod\ n) \leftrightarrow (a - b) = n \cdot h\ con\ h \in Z$

Pensiamo all'orologio :

$15 \equiv 3\ (mod\ 12)$; $18 \equiv 6\ (mod\ 12)$; $23 \equiv 11\ (mod\ 12)$

Completa le seguenti congruenze:

$14 \equiv$ $(mod\ 12)$; $16 \equiv$ $(mod\ 12)$; $21 \equiv$ $(mod\ 12)$; $17 \equiv$ $(mod\ 12)$

$26 \equiv$ $(mod\ 12)$; $29 \equiv$ $(mod\ 12)$; $33 \equiv$ $(mod\ 12)$; $27 \equiv$ $(mod\ 12)$

Scrivi 5 numeri che sono congrui a 7 modulo 12:

Possiamo dire che un numero è congruo a 7 modulo 12 quando

Scrivi 5 numeri che sono congrui a 11 modulo 12:

Possiamo dire che un numero è congruo a 11 modulo 12 quando

In generale possiamo dire che tutti i numeri divisi per 12 possono dare come resto 0 oppure 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

Si formano in questo modo degli insiemi i cui elementi sono i numeri che divisi per 12 danno lo stesso resto. Tali insiemi si indicano con classi resto modulo 12 e si indicano con [0]; [1]; [2]; .....

L'insieme delle classi resto modulo 12 si indica con Z_{12}

Operazioni nelle classi resto

Nelle classi resto vengono definite le operazioni di addizione e moltiplicazione. Aiutiamoci con delle tabelle per capire il funzionamento di queste operazioni

Z_3

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

·	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Osserva le particolarità delle tabelle moltiplicative. Lo zero si ottiene in modi diversi. Cosa succede?

Costruisci tabelle analoghe in Z_5