CIFRARIO AFFINE

Con le operazioni imparate sulle congruenze è possibile generalizzare il cifrario di Cesare e costruire il cifrario affine.

Nel CIFRARIO DI CESARE la chiave è definita da un solo numero k e per codificare il testo basta eseguire uno spostamento di k di tutte le lettere.

E se una lettera occupa nell'alfabeto in chiaro la posizione n

dopo la codifica occuperà la posizione

$$(n + k\ )(mod 21)$$

Nel CIFRARIO AFFINE la chiave è costituita da una coppia di numeri (a, b).

Se una lettera occupa nell'alfabeto in chiaro la posizione n dopo la codifica occuperà la posizione

$$(an + b\ )(mod 21)$$

Dunque l'operazione matematica alla base di questo cifrario è la precedente

Consideriamo il nostro alfabeto

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

e costruiamo il cifrario affine con chiave (5; 4) ovvero costruiamo il nuovo alfabeto con la procedura (algoritmo) indicata nel CIFRARIO DI CESARE

LEGGO LA POSIZIONE DI OGNI LETTERA n

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

eseguo UN'OPERAZIONE MATEMATICA $an + b$

trovo la NUOVA POSIZIONE $an + b$

costruisco il NUOVO ALFABETO sotto a questa riga

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

Creo la CORRISPONDENZA TRA L'ALFABETO IN CHIARO E IL NUOVO ALFABETO sotto a questa riga

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

LETTERA	POSIZIONE IN CHIARO n	NUOVA POSIZIONE Dopo la cifratura 5n+4	Divido per 21 e prendo il resto Mod 21	NUOVO ALFABETO		LETTERA	POSIZIONE IN CHIARO n	NUOVA POSIZIONE Dopo la cifratura 5n+4	Divido per 21 e prendo il resto Mod 21	NUOVO ALFABETO		LETTERA	POSIZIONE IN CHIARO n	NUOVA POSIZIONE Dopo la cifratura 5n+4	Divido per 21 e prendo il resto Mod 21	NUOVO ALFABETO
A	0	4	4	Scrivo a sotto 4		H	7			Scrivo h sotto		Q	14			Scrivo q sotto
B	1	9	9	Scrivo b sotto 9		I	8					R	15			
C	2	14	14	Scrivo c sotto 14		L	9					S	16			
D	3	19	19	Scrivo d sotto 19		M	10					T	17			
E	4	24	3	Scrivo e sotto 3		N	11					U	18			
F	5					O	12					V	19			
G	6					P	13					Z	20			

NUOVO ALFABETO

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

CORRISPONDENZA TRA LETTERE E LETTERE

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

Dunque un messaggio DELQV viene cifrato con eabcd

E UN MESSAGGIO debac viene decifrato con VDLEQ

ESERCIZIO

Finisci di costruire la corrispondenza suddetta e cifra la frase

La sovranità appartiene al popolo, che la esercita nelle forme e nei limiti della Costituzione