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.

Se una lettera occupa nell'alfabeto in chiaro la posizione n dopo la codifica occuperà la posizione n+k (mod21)

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 (mod21)

Consideriamo il nostro alfabeto in Z_{21}

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)

Posizione e lettera in chiaro	Posizione e lettera dopo la cifratura 5N+4	Posizione e lettera in chiaro	Posizione e lettera dopo la cifratura 5N+4	Posizione e lettera in chiaro	Posizione e lettera dopo la cifratura 5N+4
0 A	4 A	7 H		14 Q	
1 B	9 B	8 I		15 R	
2 C	14 C	9 L		16 S	
3 D	19 D	10 M		17 T	
4 E	24≡3 (mod21) 3 E	11 N		18 U	
5 F	29≡8 (mod21) 8 F	12 O		19 V	
6 G	34≡13 (mod21) 13 G	13 P		20 Z	

Verifica che l'alfabeto cifrato in Z_{21} sia:

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

Decifra il seguente messaggio con questo cifrario:

B FNSBFS T HQS VAGHOOBFIS TMQESNS RHB BSDMVM

Consideriamo il nostro alfabeto in Z_{21}

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 (3; 4)

Posizione e lettera in chiaro	Posizione e lettera dopo la cifratura 3N+4	Posizione e lettera in chiaro	Posizione e lettera dopo la cifratura 3N+4	Posizione e lettera in chiaro	Posizione e lettera dopo la cifratura 5N+4
0 A	**4 A**	7 H	25≡4 (mod21) **4 H**	14 Q	
1 B	7 B	8 I		15 R	
2 C	10 C	9 L		16 S	
3 D	13 D	10 M		17 T	
4 E	16 E	11 N		18 U	
5 F	19 F	12 O		19 V	
6 G	22≡1 (mod21) 1 A	13 P		20 Z	

Completa la tabella e spiega quali problemi incontri

_____

Certamente non possiamo andare per tentativi, quindi dobbiamo trovare un modo per eliminare questi problemi.
Sapresti individuare perché la moltiplicazione per 3 ha dato problemi, ma non quella per 5?

_____

Quindi come devono essere scelti a e b?

_____

Esercizio Costruire il cifrario affine di chiave (2;1) e cifra il seguente messaggio

Quindi riscrivi in forma completa l'articolo 1 della costituzione:

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