Tema 5 (9.) Criptați următorul text folosind criptosistemul Cezar, cu cheia H, pe un alfabet de 27 de caractere (A-Z_).

CRIPTOSISTEME_SIMETRICE

cheia H => 7

JYPW_VZPZ_LTLGZPTL_YPJL (+H)

XKBITMHLBLMYFYTLBFYMKBXY (-H)

(15) Mesaj în clar în engleză, criptat cu un criptosistem afin pe blocuri de 1 caract., fol. un alfabet de 26 de caractere (A-Z)

ΔTWAWASOGXNWXAΔKPKXEWAK

$E \to K : 4 \to 10$

$T \to \Delta : 19 \to 3$

$c = a \cdot m + b \pmod N$

$\Rightarrow \begin{cases} 10 = a \cdot 4 + b \pmod{26} \\ 3 = a \cdot 19 + b \pmod{26} \end{cases} \Rightarrow$

$\Rightarrow \begin{cases} 7 = a \cdot (-15) \\ 3 = a \cdot 19 + b \end{cases} \Rightarrow \begin{cases} 7 = a \cdot 11 \\ 3 = a \cdot 19 + b \mid \cdot 2 \end{cases} \Rightarrow \begin{cases} 7 = a \cdot 11 \\ 6 = a \end{cases}$

$\Rightarrow K \xrightarrow{c} E \xrightarrow{m} \quad \begin{cases} a' K + b' = E \\ a' \Delta + b' = T \end{cases} \Rightarrow \begin{cases} a' \cdot 10 + b' = 4 \\ a' \cdot 3 + b' = 19 \end{cases} \Rightarrow$

$\Rightarrow \begin{cases} 7a = 11 \ (= -15) \\ 3a + b = 19 \end{cases} \quad \begin{cases} 10a + b = 4 \\ 11a = -15 \end{cases}$

$c = a \cdot m + b \pmod N \Rightarrow m = (c - b) \cdot a^{-1} \pmod N$

$\begin{cases} 7a' = 11 \\ 3a' + b' = 19 \end{cases} \Rightarrow \begin{cases} a' = 9 \ (63 = 9 \cdot 7 = 26 \cdot 2 + 11) \\ 3 \cdot 9 + b' = 19 \end{cases} \Rightarrow 1 + b' = 19 \Rightarrow b' = 18$

$(a', b') = (9, 18)$ pt decriptare

	W	O	N	D	E	R	F	U	L
m	22	14	13	3	4	17	5	20	11
a·m+b	8	14	5	19	2	15	11	16	13
C	I	O	F	T	B	P	L	Q	N

→ criptare găsită!

	D	T	W	A	W	A	S	O	G	X	N	W	X	A	D	K	P	K	X	E	W	A	K
C	3	19	22	0	22	0	18	14	6	23	13	22	23	0	3	10	15	10	23	4	22	0	10
m	19	7	8	18	8	18	24	14	20	17	5	8	17	18	19	4	23	4	17	2	8	18	4
	T	H	I	S	I	S	Y	O	U	R	F	I	R	S	T	E	X	E	R	C	I	S	E

pt criptare: $E \to K : 4 \to 10$, $T \to D : 19 \to 3$

$$\Rightarrow \begin{cases} 10 = 4 \cdot a + b \\ 3 = 19 \cdot a + b \end{cases} \Rightarrow \begin{cases} 7 = 11a \\ 3 = 19a + b \end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases} a = 3 \ (33 = 11 \cdot a = 26 + 7) \\ 3 = 19 \cdot 3 + b \end{cases} \Rightarrow 3 = 5 + b \Rightarrow b = -2 \pmod{26} = 24$$

$(a, b) = (3, 24)$

criptare corectă!

	W	O	N	D	E	R	F	U	L
m	22	14	13	3	4	17	5	20	11
$C = am + b$	12	14	19	7	10	23	13	6	5
	M	O	L	H	K	X	N	G	F