(17) Știind că s-a folosit o criptare afină pe blocuri de un caracter, un alfabet de 26 de caractere (A–Z) și că E, T sunt criptate respectiv în Y, T, desifrați mesajul

QA OOY QQ EVHE QV

Rezolvare

$$\begin{matrix} T \to T \\ Y \to E \end{matrix} \Rightarrow \begin{cases} T \cdot a' + b' = T \\ Y \cdot a' + b' = E \end{cases} \Rightarrow \begin{cases} 19a' + b' = 19 \\ 24a' + b' = 4 \end{cases} \pmod{26}$$

$$(-)$$

$$-5a' = 15$$

$$21a' = 15 \mid \cdot 21^{-1} \equiv 5$$

Verificăm $(21, 26) = 1 \Rightarrow \exists\, 21^{-1}$ în $\mathbb{Z}_{26}$

$(21, 26) = d$

$d = 26u + 21v$, $u, v \in \mathbb{Z}$

$X_{26} = (1,0)$

$X_{21} = (0,1)$

$26 = 21 \cdot 1 + 5$

$21 = 5 \cdot 4 + 1$

$5 = 1 \cdot 5 + 0$

ultimul cmmdc.

$X_{26} = X_{21} \cdot 1 + X_5$

$X_5 = X_{26} - X_{21} = (1,0) - (0,1) = (1,-1)$

$X_{21} = X_5 \cdot 4 + X_1$

$X_1 = X_{21} - 4X_5 = (0,1) - 4(1,-1)$

$= (0,1) - (4,-4) = (\underbrace{-4}_{u}, \underbrace{5}_{v})$

$1 = 26 \cdot (-4) + 21 \cdot 5 \pmod{26}$

$1 = 21 \cdot 5 \pmod{26} \Rightarrow 21^{-1} = 5$

$a' = 15 \cdot 5$

$a' = 75 \bmod 26$

$a' = 23 \Rightarrow a' = -3 \bmod 26$

$24 \cdot 23 + b' = 4$

$b' = 4 - 552$

$b' = -548 \pmod{26}$

$b' = -2 \bmod 26$

Q	A	O	O	Y	Q	Q	E	V	H	E	Q	V
C	Y	i	i	E	C	C	M	N	D	M	C	N

$16 \cdot (-3) + (-2) = -48 - 2 = -50 \bmod 26 = -24 \bmod 26 = 2 = \boxed{C}$

$A \cdot (-3) + (-2) = -2 \pmod{26} = 24 = \boxed{Y}$

$14 \cdot (-3) + (-2) = -42 - 2 = -44 \pmod{26} = -18 = 8 \bmod 26 = \boxed{I}$

$4 \cdot (-3) + (-2) = -12 - 2 = -14 = 12 = \boxed{M}$

$7 (-3) + (-2) = -21 - 2 = -23 = 3 = \boxed{D}$

$-5 \cdot (-3) + (-2) = 13 = \boxed{N}$