DOSOFTEI GEORGIANA-PARASCHEVA

TEMA 8

1. Alice și Bob doresc să stabilească o cheie secretă k (pe care să o cunoască doar ei) folosind criptosistemul Diffie-Hellman. Ei aleg numărul prim $p = 17$ și generatorul $g = 5$ al lui $\mathbb{Z}_{17}$. Alice alege exponentul secret $a = 3$, iar Bob alege exponentul secret $b = 6$. Determinați cheia k.

$u = g^a = 5^3 \pmod{17} = 25 \cdot 5 \pmod{17} = 8 \cdot 5 \pmod{17} =$
$= 40 \pmod{17} = 6 \pmod{17}$

$k = u^b = 6^6 \pmod{17} = (6^2)^3 \pmod{17} = 36^3 \pmod{17} =$
$= 2^3 \pmod{17} = 8 \pmod{17}$.

2. Alice utilizează un criptosistem El-Gamal și are cheia publică (31, 3, 19). Bob dorește să-i trimită mesajul X și alege parametrul $k = 3$. Să se determine mesajul criptat. Alfabetul folosit are 30 de caractere, în care literele A-Z au echivalenții numerici 0-25, $\sqcup = 26$, $? = 27$, $! = 28$ și $, = 29$.

$X = 25$

$p = 31$
$g = 3$
$\alpha = 19$
$k = 3$

$u = g^k \pmod{p} = 3^3 \pmod{31} = 27 \pmod{31}$

$v = 25 \cdot \alpha^k \pmod{p} = 25 \cdot 19^3 \pmod{31} = 25 \cdot 19 \cdot 361 \pmod{31}$
$= 25 \cdot 19 \cdot 20 \pmod{31} = 9500 \pmod{31} = 14 \pmod{31}$

X criptat este O