Tema 8

nr 22 :

Alice și Bob doresc să stabilească o cheie secretă K (pe care doar ei să o cunoască) 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.

rezolvare: Alice calculează $u = g^a = 5^3 \pmod{17} = 125 \bmod 17 \equiv 6$

Bob calculează $K = u^b = 6^6 \pmod{17} = 46656 \bmod 17 \equiv 8$

cheia secretă $K = 8$

$46656 : 17 = 2744$

459

-75

68

76

68

-8