Tema 8

Cătălin Răpeanu

18. Alice şi Bob doresc să stabilească o cheie secretă
ă (pe care să o cunoască doar ei) folosind criptosistemu
iffie-Hellman. Ei aleg numărul prim $p=17$ şi
generatorul $g=5$ al lui Z_{17}. Alice alege exponentul
ecret $a=3$, iar Bob alege exponentul secret $b=6$. Det.
cheia k.

$$u = g^{a} \pmod{p}$$

$$u = 5^{3} \pmod{17} = 5 \cdot 5^{2} \pmod{17} =$$

$$= 5 \cdot 8 \pmod{17} = 6 \pmod{17}$$

$$k = u^{b} \pmod{p}$$

$$k = 6^{6} \pmod{17} = (6^{2})^{3} \pmod{17} = 2^{3} \pmod{17}$$

$$= 8 \pmod{17}$$

$$v = g^{b} \pmod{p}$$

$$v = 5^{6} \pmod{17} = (5^{2})^{3} \pmod{17} = 8^{3} \pmod{17} =$$

$$= 8 \cdot 13 \pmod{17} = 2 \pmod{17}$$

$$k = v^{a} \pmod{p}$$

$$k = 2^{3} \pmod{17} = 8 \pmod{17}$$

$$\boxed{k = 8}$$