TEMA 9

2. Criptosistemul Diffie-Hellman

$p = 17, g = 5$

Alice: $a = 3$

Bob: $b = 6$.

$k = ?$

A

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

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

B

$u = 5^6 \pmod{17} = (5^3)^2 = 6^2 = 36 = 2$

$k = 6^6 \pmod{17} = 3^6 \cdot (2^3)^2 = 3^6 \cdot \underbrace{64}_{-4} =$

$= \underbrace{36}_{2}{}^3 \cdot (-4) = 8 \cdot (-4) = -32 = 2$

$= g^3 \cdot (-4) = 9 \cdot \underbrace{81}_{-4} \cdot (-4) = 9 \cdot \underbrace{16}_{-1} = -9 = 8$

$\Rightarrow k = 8$

3. El Gamal

$k_e = (p, g, \alpha) = (31, 3, 19)$

$k = 3.$

$m = X = 23$

$\mu = g^a \pmod{p} = 3^3 \pmod{31} = 27$

$u = m \cdot \alpha^k \pmod{p} = 23 \cdot 19^3 \pmod{31} = (-8) \cdot (-12)^3 =$

$= -\underbrace{8 \cdot (-12)}_{\underbrace{96}_{3}} \cdot \underbrace{144}_{-11} = -33 = -2 = 29$

$\Rightarrow (27, 29)$

4. $(\rho, y, \alpha) = (53, 2, 30)$

$(u, v) = (24, 37)$

$u = 24$

$w = u^{p-1-\alpha} \pmod p = 24^{53-1-30} = 24^{22} \pmod{53} =$

$= (24^2)^{11} = \underbrace{576}_{46}{}^{11} = \underbrace{46}_{-7}{}^{11} = -7 \cdot (7^2)^5 = -7 \cdot \underbrace{49}_{-4}{}^5 =$

$= -7 \cdot (-4) \cdot (4^2)^2 = 28 \cdot \underbrace{16}_{-9}{}^2 = \underbrace{28}_{-25} \cdot (-9) = 225 = 13$

~~$v = s$~~ ~~$m = 1$~~

$m = v \cdot w \pmod p = \underbrace{37}_{-16} \cdot 13 \pmod{53} = -8 \cdot 26 = -4 \cdot \underbrace{52}_{-1} = 4$

$\rightarrow E$

5. $(u, v) = (30, 7)$

$p = 43, \ g = 3.$

$u = g^h \pmod p = 3^4 \pmod{43} \Rightarrow 3^4 \pmod{43} = 30$

?

.