$85 = 2 \cdot 30 + 25 \cdot = (2|(25) = CZ$

Tema 9 - Criptografie

2. k-cheie secretă → Diffie-Hellman

$p = 17$
$g = 5$
în $\mathbb{Z}_{17}$
$a = 3, b = 6$
$k = ?$

A
$u = 5^3 \pmod{17}$
$u = 6$
$k = 2^3 \pmod{23}$
$k = 8$

B
$v = 5^6 \pmod{17}$
$v = 2$
$k = 6^6 \pmod{17}$
$k = 8$

3. El-Gamal.
cheia publică (31, 3, 19)
mesajul: $x = 23$
param $k = 3$
→ mesajul criptat

$p = 31$
$g = 3$
$\alpha = 19$
criptare:
$u = g^k \pmod p = 3^3 \pmod{31} = 27$
$v = u \cdot \alpha^k \pmod p = 23 \cdot 19^3 \pmod{31} = 23 \cdot 19 \cdot 19^2 \pmod{31}$
$= 3 \cdot 20 \pmod{31} = 29$

$\Rightarrow (u, v) = (27, 29)$

4. cheia publică (53, 2, 30) → sistem El-Gamal
mesajul criptat $(u, v) = (24, 37)$
→ mesajul în clar

$p = 53$ $u = 24$
$g = 2$ $v = 37$
$\alpha = 30$

$\alpha = g^a \pmod p$
$30 = 2^a \pmod{53}$
calculând, aflăm $a = 13$

$w = u^{p-1-a} \pmod p \Rightarrow w = 24^{53-1-13} \pmod{53}$
$w = 24^{39} \pmod{53}$
$w = 24 \cdot (24^2)^{19} \pmod{53} = 24 \cdot 46 \cdot (46^2)^9 \pmod{53} = 44 \cdot 49 \cdot (49^2)^4$
$= 36 \cdot (16^2)^2 = 36 \cdot 44^2 = 36 \cdot 28 = 1 \Rightarrow w = 1$

$m = v \cdot w \pmod p = 37 \cdot 1 \pmod{53} \Rightarrow m = 37 \Rightarrow (7) = H$

5. (30, 7) → mesaj (criptat. El-Gamal)
cheia publică (p = 43, g = 3)
——→
decriptare mesaj

u = 30
v = 7
p = 43
g = 3

Întrucât nu cunoaștem nici a sau nici α pt a face decriptarea, vom alege un a minim (0 < a < p-1)
Aleg a = 5 (minim)

$\Rightarrow w = g^{p-1-a} \pmod p$
$w = 3^{43-1-5} \pmod{43}$

$w = 3^{37} \pmod{43}$
$w = 3(3^2)^{18} \pmod{43}$
$w = 3 \cdot (9^2)^9 \pmod{43}$
$w = 3 \cdot 38 \cdot (38^2)^4 \pmod{43}$
$w = 28 \cdot (25^2)^2 \pmod{43}$
$w = 28 \cdot 23^2 \pmod{43}$
$w = 28 \cdot 13 \pmod{43}$
$w = 20$

$m = v \cdot w \pmod p = 7 \cdot 20 \pmod{43} \Rightarrow m = 11 \Rightarrow$ L

6. El Gamal.
cheia privată (p = 71, g = 33, a = 34)
——→
a) cheia publică
b) k = 3, mesaj = AZI
mesaj criptat = ?
——||

a) $\alpha = g^a \pmod p = 33^{34} \pmod{71} = (33^2)^{17} \pmod{71}$
$= 24 \cdot (24^2)^8 \pmod{71} = 24 (8^2)^4 \pmod{71}$
$= 24 \cdot (64^2)^2 \pmod{71} = 24 \cdot 49^2 \pmod{71}$
$= 24 \cdot 58 \pmod{71} = 43 \Rightarrow \alpha = 43$

⇒ cheia privată (71, 33, 43)

b) k = 3

mesaj AZi

A = 0 = u_1

Z = (25) = v

i = 8 = u_2

$w_1 = u_1^{p-1-a} \pmod p = 0$; $w_2 = u_2^{p-1-a} \pmod p \neq 8^{71-1-34} \pmod{71}$

$w_2 = 8^{36} \pmod{71}$

$w_2 = (8^3)^{12} \pmod{71}$

$w = (64^2)^6 \pmod{71}$

$w_2 = (49^2)^4 \cdot 49 \pmod{71}$

$w_2 = (58^2)^2 \cdot 49 \pmod{71}$

$w_2 = 27^2 \cdot 49 \pmod{71}$

$w_2 = 15 \cdot 49 \pmod{71}$

$w_2 = 8$

$u_1 = v \cdot w_1 \pmod p = 25 \cdot 0 = 0 \Rightarrow A$

$u_2 = v \cdot w_2 \pmod p = 25 \cdot 8 \pmod{71}$

$\Rightarrow u_2 = 58$

↓

28 $\Rightarrow$!

mesajul criptat este A!

b) k = 3

mesaj AZi

$u = g^k \pmod p = 33^3 \pmod{71} = 33 \cdot 33^2 \pmod{71} = 33 \cdot 24 \pmod{71}$

$\Rightarrow u = 11$

$\alpha^k \pmod p = 43^3 \pmod{71} = 43 \cdot 43^2 \pmod{71} = 43 \cdot 3 \pmod{71} = 58$

A = 0 $\Rightarrow$ $v_1 = 0 \cdot 58 \pmod{71} = 0$

Z = 25 $\Rightarrow$ $v_2 = 25 \cdot 58 \pmod{71} = 30$

i = 8 $\Rightarrow$ $v_3 = 8 \cdot 58 \pmod{71} = 38$

$\Rightarrow (u, v_1) = (11, 0)$

$(u, v_2) = (11, 30)$

$(u, v_3) = (11, 38)$