Tema 10

1. $m = 343 \quad p = 48731 \quad q = 443 \quad x = 7 \quad a = 242$ DSA

a) cheia publică : (p, q, g, α)

$$g = x^{\frac{p-1}{q}} \pmod p$$
$$= 7^{\frac{48730}{443}} \pmod{48731}$$
$$= 7^{110} \pmod{48731}$$
$$= 5260$$

$$\alpha = g^a \pmod p$$
$$= 5260^{242} \pmod{48731}$$
$$= 3438$$

⇒ cheia publică : $(48731, 443, 5260, 3438)$

b) $k = 427$

$$r = (g^k \pmod p) \pmod q$$

$$g^k \pmod p = 5260^{427} \pmod{48731}$$
$$= 2717$$

$$r = 2717 \pmod{443} = 59$$

$$s = k^{-1}(h(m) + a \cdot r) \pmod q$$
$$= 427^{-1}(0 + 242 \cdot 59) \pmod{443}$$
$$= 427^{-1} \cdot 14.278 \pmod{443}$$

* $427^{-1} \pmod{443} =$ $\quad X_{443} = (1, 0) \quad X_{427} = (0, 1)$

$443 : 427 = 1$ rest 16

$X_{16} = X_{443} - X_{427} = (1, 0) - (0, 1) = (1, -1)$

$427 : 16 = 26$ rest 11 ⇒ $X_{11} = X_{427} - 26 X_{16} = (0, 1) - (26, -26) = (-26, 27)$

$16 : 11 = 1$ rest 5

$X_5 = X_{16} - X_{11} = (1,-1) - (-26,27) = (27,-28)$

$11 : 5 = 2$ rest 1

$X_1 = X_{11} - 2X_5 = (-26,27) - (54,-56) = (-80,83)$

$\Rightarrow 427^{-1} \equiv 83 \pmod{443}$

$* \; 14278 \pmod{443} = 102$

$\Rightarrow s = 83 \cdot 102 \pmod{443} = 8466 \pmod{443} = 49$

$\Rightarrow$ semnătura mesajului $(r = 59, s = 49)$

Verificare:

$r < q - 1$

$59 < 442$ adevărat

$s < q - 1$

$49 < 442$ adevărat

$$v = \left(g^{s^{-1} \cdot h(m) \pmod q} \cdot \alpha^{r s^{-1} \pmod q} \pmod p \right) \pmod q$$

$$* \; g^{s^{-1} h(m) \pmod q} = 5260^{49^{-1} \pmod{443}}$$

$\rightarrow 49^{-1} \pmod{443} = ?$ $\quad X_{443} = (1,0)$, $X_{49} = (0,1)$

$443 : 49 = 9$ rest 2

$X_2 = X_{443} - 9X_{49} = (1,0) - (0,9) = (1,-9)$

$49 : 2 = 24$ rest 1

$X_1 = X_{49} - 24X_2 = (0,1) - 24(1,-9) = (-24, 217)$

$\Rightarrow 49^{-1} \equiv 217 \pmod{443}$

$\Rightarrow 5260^{217} \pmod{443} = 328$

* $2^{r \cdot s^{-1}} \pmod 2 = 3438^{59 \cdot 49^{-1}} \pmod{443}$

$\rightarrow 59 \cdot 217 \pmod{443} = 12803 \pmod{443} = 399$

$3438^{399} \pmod{443} = 43$

$r = (328 \cdot 43 \pmod{48731}) \pmod{443}$

$= (14104 \pmod{48731}) \pmod{443}$

$= 14104 \pmod{443}$

$= 371$

$r = 59$ $\Rightarrow$ nu acceptam semnătura

2. $K_e = (n = 28829, e)$ aflat mai mic exponent.

$m = 11111$ RSA

$28829 = 127 \cdot 227 \Rightarrow p = 127$ și $q = 227$

$f(n) = (p-1)(q-1) = 126 \cdot 226 = 28476$

$S = m^e \pmod n$

$(f(n), e) = 1 \Leftrightarrow e \equiv 1 \pmod{28476}$

e cel mai mic exponent $\Rightarrow e = 28477$ $\Rightarrow$

$\Rightarrow S = 11111^{28477} \pmod{28829} = 11111$

3. $p = 1223$ $q = 1987$ $K_e = (n = pq = 2430101, e = 948047)$

$m = 1070777$

$S = m^e \pmod n = 1070777^{948047} \pmod{2430101} = 1473513$

4. $p=21739$ $g=7$ $a=15140$ El Gamal

a) cheia publică (p, g, α)

$\alpha = g^a \pmod p$

$= 7^{15140} \pmod{21739}$

$= 17702$

⇒ cheia publică $(21739, 7, 17702)$

b) $m=5331$; $K=10727$ semnătură + autenticitate

$m < p-1$

$5331 < 21738$ ✓

$(10727, 21738) = 1$ ✓

$r = g^K \pmod p$

$= 7^{10727} \pmod{21739} = \underline{15775}$

$s = K^{-1}(m - a \cdot r) \pmod{p-1}$

$= 10727^{-1}(5331 - 15140 \cdot 15775) \pmod{21738}$

$* \; 10727^{-1} \pmod{21738} = 6353$

$* \; (5331 - 15140 \cdot 15775) \pmod{21738} =$

$= (5331 - 238.833.500) \pmod{21738}$

$= -238.828.169 \pmod{21738}$

$= 7237$

$S = 6353 \cdot 7237 \pmod{21738}$

$= 45976661 \pmod{21738}$

$= 791$

la fel ⇒ semnătura este bună

Verificare $r < p-1 \iff 15.775 < 21.739$ ✓

$\alpha^r \cdot r^s \equiv g^m \pmod p$ $\quad \alpha^r \cdot r^s \pmod p = 17702^{15775} \cdot 15775^{791} \pmod{21739} = 13897$

$g^m \pmod p = 7^{5331} \pmod{21739} = 13897$