Tema 10

1. DSA

$m = 343$

$p = 48731$

$l = 443$

$x = 7$

$a = 242$

a) ~~$m = p \cdot q$~~

$g = x^{\frac{p-1}{2}} \pmod p \Rightarrow g^2 = 1 \pmod p$

$g = 7^{\frac{48731-1}{443}} \pmod{48731} \Rightarrow g = 7^{\frac{48730}{443}} \pmod{48731}$

$\Rightarrow g = 7^{110} \pmod{48731} \Rightarrow g = 5260 \pmod{48731}$

$\alpha = g^{q} \pmod{p} \Rightarrow \alpha = 443^{242} \; 5260^{242} \pmod{48731} =$

$= 3438$

Cheia publică $(p, q, g, \alpha) = (48731, 443, 5260, 3438)$

b) $k = 427$

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

$s = k^{-1}(h(m) + ar) \pmod{q}$

Semnătura (r, s)

$r = (5260^{427} \pmod{48731}) \pmod{443}$

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

$s = 427^{-1} \pmod{443}$

$443 : 427 = 1$
427
$= 16$

$427 : 16 = 26$
32
$\overline{107}$
96
$= 11$

$16 : 11 = 1$
11
$= 5$

$11 : 5 = 2$
10
1

$x_{443} = (1, 0) \quad x_{427} = (0, 1)$

$x_{16} = (1,0) - (0,1) = (1,-1)$

$x_{11} = (0,1) - 26 \cdot (1,-1) =$

$= (0,1) - (26,-26) =$

$= (-26,27)$

$x_5 = (1,-1) - (-26,27) = (27,-28)$

$x_1 = (-26,27) - (27,-28) = (-53,55)$

$427^{-1} \pmod{443} = 55$

(fără trunchiere) $\Rightarrow h(m) = m$

$s = 55(343 + 242 \cdot 59) \pmod{443}$

$s = 55(343 + 14278) \pmod{443}$

$s = 55(343 + 102) \pmod{443}$

$s = 55 \cdot 445 \pmod{443}$

$s = 55 \cdot 2 \Rightarrow s = 110$

$(r,s) = (59,110)$

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

$s^{-1} \cdot m \pmod{q}$

$110^{-1} \cdot 343 \pmod{443}$

~~$443 : 110 =$~~

443 : 110 = 4
440

= 3

110 : 3 = 36
9

= 20
18

= 2

3 : 2 = 1
2

1

$x_{443} = (1,0)$ $x_{110} = (0,1)$

$x_3 = (1,0) - 4(0,1) = (1,0) - (0,4) = (1,-4)$

$x_2 = (0,1) - 36 \cdot (1,-4) = (0,1) - (36,-144) = (-36,145)$

$x_1 = (1,-4) - (-36,145) = (37,-149)$

$-149 \cdot 343 \pmod{443} = 294 \cdot 343 \pmod{443} =$

$= 100842 \pmod{443} = 281$

$n \cdot n^{-1} \pmod{443}$

$59 \cdot 110^{-1} \pmod{443}$

$59 \cdot 281 \pmod{294} \pmod{443} = 17346 \pmod{443}$

$= 69$

$g^{281} \cdot \alpha^{69} \pmod{p} =$

$5260^{281} \cdot 3438^{69} \pmod{48731}$

$2482 \cdot 19386 \pmod{48731}$

$48116052 \pmod{48731}$

8242

$59 = 8242 \pmod{443}$

$55 = 268$??

2. RSA

$K_e = (n = 28829, e)$

e cel mai mic posibil

$S = ?$ $\quad m = 11111$

$S = m^d \pmod{n}$

$m = S^e \pmod{n}$

$\sqrt{28829} = 169$

1	
188	
156	26 . 6
3229	
2961	
268	3 . 3

$[28829] = 169$

$169^2 - 170^2 = -268$

$169^2 - 28829^2 = -268 = -2 \cdot 134$

$170^2 - 28829 = 71$

$171^2 - 28829 = 412$

$\sqrt{412}$

$172^2 - 28829 = 755$

$173^2 - 28829 = 1100$

$174^2 - 28829 = 1447$

⋮

$28829 = 127 \cdot 227$

$\varphi(n) = 126 \cdot 226 = 28476$

$(e, \varphi) = 1$

$(e, 28476) = 1 \Rightarrow e = 5$

$d = e^{-1} \pmod{28476} = 22781$

$S = m^d \bmod n = 11111^{22781} \bmod 28829 = 7003$

$e = 5 \quad d = 22781 \quad S = 7003$

3. $p = 1223$

$q = 1987$

$k_e = (n = p \cdot q = 2430101, e = 948047)$

$n = 1070777$

RSA

$\varphi(n) = (1223 - 1)(1987 - 1) = 1222 \cdot 1986 = 2426892$

$d = 948047^{-1} \bmod 2426892 = 1051235$

$S = m^d \bmod n = 1070777^{1051235} \bmod = 153337$

$d = 1051235, \quad S = 153337$

4. $p = 21739$

$g = 7$

$a = 15140$

$m = 5331$

$\lambda = 10727$

a) $\alpha = g^a \bmod p = 7^{15140} \bmod 21739 = 17702$

$(p, g, \alpha) = (21739, 7, 17702)$

a) $r = g^\lambda \bmod p = 7^{10727} \bmod 21739 = 15775$

$\lambda^{-1} \bmod (p-1) = 10727^{-1} \bmod 21738 = 7357$

$t = m - ar \bmod (p-1) \quad 5331 - 15140 \cdot 15775 \bmod 21738 =$

$= 15541$

$s = \lambda^{-1} t \bmod (p-1) = 7357 \cdot 15541 \bmod 21738 = 791$

$\alpha^r r^s \bmod p = 17702^{15775} \cdot 15775^{791} \bmod 21739 = 7^{5331} \bmod 21739$

$(r, s) = (15775, 791)$