Tema 10 – Criptografie

1. $m = 343$, $p = 48.731$, $q = 443$, $x = 7$, $a = 242$ DSA

a) cheia pub. : $(p, q, g, d) = (48.731, 443, 5260, 3438)$

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

$\equiv 7^{\frac{48730}{443}} \pmod{48731}$

$\equiv 7^{110} \pmod{48731}$

$= \boxed{5260}$

$d = g^a \pmod p$

$= 5260^{242} \pmod{48731}$

$= \boxed{3438}$

b) $k = 427$

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

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

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

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

$\equiv 427^{-1}(0 + 242 \cdot 59) \pmod{443}$

$\equiv 427^{-1} \cdot 14278 \pmod{443}$

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

$(427, 443) = 1$ $\Rightarrow$ semnătura $(59, 49)$

$443 = 1 \cdot 427 + 16$

$427 = 26 \cdot 16 + 11$

$16 = 1 \cdot 11 + 5$

$11 = 2 \cdot 5 + 1$ $\Rightarrow$ $1 = 11 - 2 \cdot 5 = 11 - 2(16 - 11) = 3 \cdot 11 - 2 \cdot 16$

$= 3(427 - 26 \cdot 16) - 2 \cdot 16 = 3 \cdot 427 - 80 \cdot 16$

$= 3 \cdot 427 - 80(443 - 427)$

$= \boxed{83} \cdot 427 + (-80) \cdot 443$

Verif. $r < q - 1 \iff 59 < 442$ (A)

$s < q - 1 \iff 49 < 442$ (A)

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

$= (5260^{49^{-1} \pmod{443}} \cdot 3438^{59 \cdot 49^{-1} \pmod{443}} \pmod{48731}) \pmod{443}$

$= (5260^{217} \cdot 3438^{59 \cdot 217} \pmod{48.731}) \pmod{443}$

$= (328 \cdot 3438^{399} \pmod{48.731}) \pmod{443}$

$= (328 \cdot 43 \pmod{48.731}) \pmod{443}$

$= 14.104 \pmod{443} = 371 \neq 59 \Rightarrow$ (F) nu acceptăm semn.

2. $k_e = (n = 28\,829, e)$ (RSA)

e cel mai mic exp.

$m = 11.111$

28829	127
227	227
1	

$\Rightarrow p = 127$, $q = 227$

$\ell(n) = (p-1)(q-1) = 126 \cdot 226 = 28.476$

$s = m^e \pmod n$

$(\ell(n), e) = 1 \iff e \equiv 1 \pmod{28.476} \Rightarrow e = 28.477$

e cel mai mic exp

$s = 11.111^{28.477} \pmod{28\,829} = 1111$

3. $p = 1223$

$q = 1987$

$k_e = (n = pq = 2\,430\,101, e = 948.047)$

$m = 1.070.777$

$s = m^e \pmod n = 1070.777^{948.047} \pmod{2.430.101} = 1473.513$

4. $p = 21\,739$ (El Gamal)

$a = 15.140$

$g = 7$

a) (p, g, d) cheia publică

$d = g^a \pmod p$

$= 7^{15.140} \pmod{21.739}$

$= 17.702 \Rightarrow (21.739, 15.140, 7)$

b) $m = 5331$, $k = 10\,727$

$m < p-1 \iff 5331 < 21\,738$ (A), $(10.727, 21\,738) = 1$ (A)

$r = g^k \pmod p$

$= 7^{10.727} \pmod{21.739} = 15.775$

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

$= 10727^{-1}(5331 - 15140 \cdot 15.775) \pmod{21738}$

$= 6353\ (5331 - 238.833.500) \pmod{21738}$

$= 6.353 \cdot (-238.828.169) \pmod{21.738}$

$= 6.353 \cdot 7237 \pmod{21.738}$

$= 45.976.661 \pmod{21.738}$

$= 791$

Verif. $r < q-1 \iff 15.775 < 21.739$ (A)

$a^u \cdot r^s \equiv g^m \pmod p$

$a^u \cdot r^s \pmod p = 17702^{15775} \cdot 15775^{791} \pmod{21739} = 13.897$

$g^m \pmod p = 7^{5331} \pmod{21.739} = 13.897$ // $\Rightarrow$

$\Rightarrow$ semnătura este bună