Tema 10

Valachi Emilia M532

(4) Pentru a semna $m = 345$ folosind o schemă DSA,

Alice alege $p = 48731$, $q = 443$, $x = 7$.

Cheia secretă - $a = 242$.

a) Determinați cheia publică a lui Alice:

//

cheia secretă = a, cheia publică = (p, q, g, α)

unde:
- $g := x^{\frac{p-1}{q}} \pmod p$
- $\alpha = g^a \pmod p$

La noi, $g = 7^{\frac{48730}{443}} \pmod{48731} = 7^{110} \pmod{48731}$

⊙
$7^1 \pmod{48731} = 7$
$7^2 \pmod{48731} = 49$
$7^3 \pmod{48731} = 343$
$7^4 \pmod{48731} = 2401$
$7^5 \pmod{48731} = 16807$
$7^6 \pmod{48731} = 20287$
$7^7 \pmod{48731} = 48247$
$7^8 \pmod{48731} = 14543$
$7^9 \pmod{48731} = 45339$
$7^{10} \pmod{48731} = 30331$

$7^{50} \pmod{48731} = 3351$

$7^{110} \pmod{48731} = (7^{50} \cdot 7^{50} \cdot 7^9 \cdot 7) \pmod{48731} =$

$= (3351 \cdot 3351 \cdot 45339 \cdot 7) \pmod{48731} = (21071 \cdot 7 \cdot 45339) \pmod{48731} =$

$= (1804 \cdot 45339) \pmod{48731} = 5260$

$\Rightarrow \boxed{q = 5260}$

(3) $\alpha = g^{a \pmod p} \iff \alpha = 5260^{242} \pmod{48731}$

$5260^2 \pmod{48731} = 37123$ $\quad 5260^{128} \pmod{48731} =$

$5260^4 \pmod{48731} = 4449$ $\quad = 39302$

$5260^8 \pmod{48731} = 8815$

$5260^{16} \pmod{48731} = 27011$

$5260^{32} \pmod{48731} = 42320$

$5260^{64} \pmod{48731} = 20688$

$5260^{242} \pmod{48731} = (5260^{128} \cdot 5260^{64} \cdot 5260^{32} \cdot 5260^{16} \cdot 5260^2) \pmod{48731} =$

$= (\underbrace{39302 \cdot 20688}_{39321} \cdot \underbrace{42320 \cdot 27011}_{22451} \cdot 37123) \pmod{48731} = (14886 \cdot 37123) \pmod{48731}$

$= 44023$

$\Rightarrow$ cheia publică este $(48731, 443, 5260, 44023)$

b) Pentru semnătura digitală, Alice alege $k = 427$, fără a folosi o fct. de trunchiere. Det. semnătura digitală și verif. autenticitatea.

Semnătura lui Alice: (r, s),

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

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

(dar fără fct. de trunchiere)

• $r = \left(5260^{427} \pmod{48731}\right) \pmod{443} = 262$

• $5260^{427} \pmod{48731} = \left(5260^{242+128+32+16+8+1}\right) \pmod{48731}$

($5260^{242} = 26017$, $5260^{32+16+8+1} = 22453$)

$= (26017 \cdot 22453 \cdot 8885 \cdot 5260) \pmod{48731} =$

$= (12772 \cdot 27567) \pmod{48731} = 4249$

• $4249 \pmod{443} = 262$

$\Rightarrow \boxed{r = 262}$

• $s = \left(\frac{1}{427} \cdot 242 \cdot 262\right) \pmod{443} = \boxed{148,5}$

$(r, s) = (262, 148.5)$

Verif. autenticității

$[1 \leq r \leq q-1 \quad \text{și} \quad 1 \leq s \leq q-1]$

$\Rightarrow 1 \leq 262 \leq 442$ ✓ $\quad 1 \leq 148.5 \leq 442$ ✓

apoi, verif.

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

$g^{\frac{1}{s} \pmod q} = 5260^{\frac{1}{148.5} \pmod{443}} = 5260^{\frac{10}{1485}}$ (1)

$\alpha^{r s^{-1} \pmod q} = 44023^{\frac{2620}{1485} \pmod{443}} = 44023^{\frac{17648}{1000}}$ (2)

$(1) \cdot (2) \pmod p = \left(8964 \cdot \frac{10.594}{10.000}\right) \pmod{443} =$

$= 424 \neq r \Rightarrow$ semnătura este respinsă, dar cred că am greșit pe vreun calcul

(2) Pentru o semnătură RSA, Alice folosește cheia publică $K_e = (n = 28829, e)$, cu e - cel mai mic posibil exponent.

Det. semnătura folosită de Alice pt. a semna mesajul public $m = 1111$.

- Factorizarea lui $n = 28829$ în p și q prime:

$p = 127$, $q = 227$

$\varphi(28829) = (127-1)(227-1) = 28476$

- [Alegem $e \in \{3, 4, \dots, 28475\}$, $(28476, e) = 1$]

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

- [Alegem d a.î. $d \cdot e \equiv 1 \pmod{\varphi(n)}$]

$d \cdot 5 \equiv 1 \pmod{28476}$

$(5, 28476) = 1$

$\Rightarrow \underbrace{-5695}_{p} \cdot 5 + \underbrace{1}_{q} \cdot 28476 = 1$

$ax \equiv b \pmod m$

$ap + mq = (a, m)$

$x_0 = \frac{bp}{(a,m)} \pmod m$

$x_n = x_0 + \frac{n m}{(a,m)} \pmod m$

- $d_0 = 28476 - 5695$ ✗
- $d_1 = (-5695 + 28476) \pmod{28476} = 22781$

$\Rightarrow$ cheia privată: $K_d = (22781, 28829)$

cheie publică: $K_e = (5, 28829)$

Determinarea semnăturii:

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

$$S = 1111^{22751} \pmod{28829}$$

$1111^{20} \pmod{28829} = 18292$

$1111^{40} \pmod{28829} = 7890$

$1111^{400} \pmod{28829} = 10533$

$1111^{4000} \pmod{28829} = 18417$

$1110^{20000} \pmod{28829} = 10319$

$1111^{360} \pmod{28829} = 1145$

$1111^{2400} \pmod{28829} = 27309$

$$1111^{22751} \pmod{28829} = \left(1111^{20.000 + 2400 + 360 + 20 + 1}\right) \pmod{28829}$$

$$= (10.319 \cdot 27309 \cdot 1145 \cdot 18292 \cdot 1111) \pmod{28829}$$

$$= (12191 \cdot 14486 \cdot 10319) \pmod{28829} =$$

$$= 18667$$

$$\Rightarrow \boxed{S = 18667}$$

---

(3) Alice alege două numere prime $p = 1223$, $q = 1987$ și face publică cheia $k_c = (n = 2430401, e = 948047)$.

Ded. semnătura pt. mesajul public $m = 1070977$.

//

- $\varphi(2430401) = (1223-1)(1987-1) = 2.426.892$
- calculăm $d \in \{1, \dots, 2426891\}$ a.î. $d \cdot 948047 \equiv 1 \pmod{2426892}$

$(948047, 2426892) = 1$

$1 = \underbrace{1051235}_{p} \cdot 948047 + \underbrace{(-410657)}_{q} \cdot 2426892$

$d_0 = \frac{1051235}{1} \pmod{2426892} = 1.051.235$

$\Rightarrow$ cheia privată: $K_d = (d = 1.051.235, n = 2.430.401)$

- Det. semnătura lui 6:

$$s = m^d \pmod n$$

$$s = 1.070.777^{1051235} \pmod{2.430.401}$$

$1070777^5 \pmod n = 2207298$

$(1070777)^{10} \pmod n = 1503682 \rightarrow m^{10} \pmod n = 2110788$

$m^{100} \pmod n = 815648 \rightarrow m^{200} \pmod n = 199437$

$m^{1000} \pmod n = 86398$

$m^{10000} \pmod n = 1214159 \rightarrow m^{50000} \pmod n = 2085168$

$m^{100000} \pmod n = 1029529$

$m^{1.000.000} \pmod n = 1062348$

$m^d \pmod n = (m^{1.000.000 + 50.000 + 1000 + 200 + 30 + 5}) \pmod n$

$= (1062348 \cdot 2085168 \cdot 86398 \cdot 199437 \cdot 2110788 \cdot 2207298) \pmod n$

$= (907.308 \cdot 463528 \cdot 2207298) \pmod n = 153377$

$\Rightarrow \boxed{s = 153377}$