DOSOFTEI GEORGIANA-PARASCHEVA

TEMA 10

1. Pentru a semna mesajul $m = 343$ folosind o schemă de semnătură digitală DSA, Alice alege $p = 48731$, $q = 443$, $x = 7$. Cheia secretă a lui Alice este $a = 242$.

a) Determinați cheia publică a lui Alice.

b) Pentru semnătura digitală, Alice alege $k = 427$, fără a folosi o funcție de trunchiere. Determinați semnătura digitală și verificați autenticitatea acesteia.

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

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

$\alpha = g^a \pmod p$

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

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

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

$r = (5260^{427} \pmod{48731}) \pmod{443} = (2717 \pmod{48731}) \pmod{443} =$

$= 59 \pmod{443}$

$s = 427^{-1}(242 \cdot 59 + 343) \pmod{443} = 83\,(14278 + 343) \pmod{443}$

$= 83 \cdot 14621 \pmod{443} = 1213543 \pmod{443} = 116 \pmod{443}.$

$(r, s) = (59, 116)$

Verificare: $1 \le r \le q-1 \Leftrightarrow 1 \le 59 \le 442$

$1 \le s \le q-1 \Leftrightarrow 1 \le 116 \le 442.$

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

Determinați semnătura folosită de Alice pentru a semna mesajul public $m = 11111$.

$n = p \cdot q$

$[\sqrt{n}] = [\sqrt{28829}] = 169$

$\sqrt{28829}$ | 169
1 | $26 \cdot 6 = 156$
188 | $329 \cdot 9 = 2961$
156
$= 3229$
2961
$= 268$

$t = [\sqrt{n}] + 1 = 170$

$t^2 - n = 170^2 - 28829 = 28900 - 28829 = 71$

$t = 171$

$t^2 - n = 171^2 - 28829 = 29241 - 28829 = 412$

$t = 172$

$t^2 - n = 172^2 - 28829 = 29584 - 28829 = 755$

$t = 173$

$t^2 - n = 173^2 - 28829 = 29929 - 28829 = 1100$

$t = 174$

$t^2 - n = 174^2 - 28829 = 30276 - 28829 = 1447$

$t = 175$

$t^2 - n = 175^2 - 28829 = 30625 - 28829 = 1796$

$t = 176$

$t^2 - n = 176^2 - 28829 = 30976 - 28829 = 2147$

$t = 177$

$t^2 - n = 177^2 - 28829 = 31329 - 28829 = 2500 = 50^2$

$n = 177^2 - 50^2 = (177-50)(177+50) = \underbrace{127}_{p} \cdot \underbrace{227}_{q}$

$\varphi(n) = (p-1)(q-1) = (127-1)(227-1) = 126 \cdot 226 = 28476$

$(\varphi(n), e) = 1 \Rightarrow e = 5$

$de \equiv 1 \pmod{28476} \Leftrightarrow d = e^{-1} \pmod{28476} \Leftrightarrow$

$\Leftrightarrow d = 5^{-1} \pmod{28476} \Leftrightarrow d \equiv -5695 \pmod{28476} = 22781$ (mod 2847

$x_{28476} = (1,0) \qquad x_5 = (0,1)$

$28476 : 5 = 5695$

25

$=34$

30

$=47$

45

$=26$

25

$=1$

$x_1 = x_{28476} - 5695 x_5 = (1,0) - (0,5695) =$

$= (1, -5695)$

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

$S = 11\,111^{22781} \pmod{28\,829} = 7003 \pmod{28\,829}$

3. Alice alege două numere prime $p = 1223$ și $q = 1987$ și face publică cheia $K_e = (n = p \cdot q = 2430101, e = 948047)$.

Determinați semnătura pe care trebuie să o atașeze Alice mesajului public $m = 1070777$.

$$\varphi(n) = (p-1)(q-1) = 1222 \cdot 1986 = 2426892$$

$$d = e^{-1} \pmod{\varphi(n)} \Leftrightarrow d = 948047^{-1} \pmod{2426892}$$

$x_{2426892} = (1,0)$ $x_{948047} = (0,1)$

$2426892 : 948047 = 2$
1896094
$= 530798$

$x_{530798} = x_{2426892} - 2x_{948047} = (1,0) - (0,2) = (1,-2)$

$948047 : 530798 = 1$
530798
417249

$x_{417249} = x_{948047} - 1 \cdot x_{530798} = (0,1) - (1,-2) = (-1,3)$

$530798 : 417249 = 1$
417249
113549

$x_{113549} = x_{530798} - 1 \cdot x_{417249} = (1,-2) - (-1,3) = (2,-5)$

$417249 : 113549 = 3$
340647
$= 76602$

$x_{76602} = x_{417249} - 3x_{113549} = (-1,3) - 3(2,-5) = (-7,18)$

$113549 : 76602 = 1$
76602
36947

$x_{36947} = x_{113549} - x_{76602} = (2,-5) - (-7,18) = (9,-23)$

$76\,602 : 36\,947 = 2$
$73\,894$
2708

$x_{2708} = x_{76\,602} - 2x_{36\,947} = (-7, 18) - 2(9, -23) = (-25, 64)$

$36\,947 : 2708 = 13$
2708
$= 9867$
8124
1743

$x_{1743} = x_{36\,947} - 13x_{2708} = (9, -23) - 13(-25, 64) =$
$= (334, -855)$

$2708 : 1743 = 1$
1743
$= 965$

$x_{965} = x_{2708} - x_{1743} = (-25, 64) - (334, -855) = (-359, 919)$

$1743 : 965 = 1$
965
778

$x_{778} = x_{1743} - x_{965} = (334, -855) - (-359, 919) = (693, -1774)$

$965 : 778 = 1$
778
187

$x_{187} = (-359, 919) - (693, -1774) = (-1052, 2693)$

$778 : 187 = 4$
748
$= 30$

$x_{30} = (693, -1774) - 4(-1052, 2693) = (4901, -12\,546)$

$187 : 30 = 6$
180
$= 7$

$x_7 = (-1052, 2693) - 6(4901, -12\,546) = (-30\,458, 77\,969)$

$30 : 7 = 4$
$\underline{28}$
$= 2$

$x_2 = (4901, -12\,546) - 4(-30\,458, 77\,969) = (126\,733, -324\,422)$

$7 : 2 = 3$
$\underline{6}$
1

$x_1 = (-30458, 77\,969) - 3(126\,733, -324, 422) = (-410\,657, 1\,051\,23$

$d = 1\,051\,235 \pmod{2\,426\,892}$

$s = m^d \pmod n = 1070\,777^{1\,051\,235} \pmod{2430101} =$
$= 153\,337 \pmod{2430101}$

4. Alice alege numărul prim $p = 21739$, generatorul $g = 7$, și cheia secretă $a = 15140$.

a) Determinați cheia publică a lui Alice pentru criptosistemul El Gamal.

b) Pentru a semna mesajul $m = 5331$, Alice alege $k = 10727$. Determinați semnătura digitală a lui Alice și apoi verificați autenticitatea ei.

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

$\alpha = g^a \pmod p = 7^{15140} \pmod{21739} = 49^{7570} \pmod{21739} =$

$= (49^2)^{3785} \pmod{21739} = 2401^{3785} \pmod{21739} =$

$= 2401 \cdot (2401^2)^{1892} = 2401 \cdot 5764\,801^{1892} = 3966^{1892} \cdot 2401 =$

$= 2401 \cdot (3966^2)^{946} = 2401 \cdot 15729156^{946} = 2401 \cdot 11859^{946} =$

$= 2401 \cdot 140\,635\,881^{473} = 2401 \cdot 6290^{473} = 2401 \cdot 6290 \cdot 6290^{472} =$

$= 15\,102\,290 \cdot (6290^2)^{236} = 15\,424 \cdot 39\,564\,100^{236} = 15\,424 \cdot 20859^{236} =$

$= 15\,424 \cdot (20859^2)^{118} = 15424 \cdot 435\,097\,881^{118} = 15\,424 \cdot (13\,535^{29})^{29} =$

$= 15\,424 \cdot 183\,196\,225^{59} = 15\,424 \cdot 1672^{59} = 15\,424 \cdot 1672 \cdot (1672^{29})^{29} =$

$= 25\,788\,928 \cdot (1672^2)^{29} = 6\,474 \cdot 2\,795\,584^{29} = 6474 \cdot 12\,992^{29} =$

$= 17702 \pmod{21739}$

b) $r = g^k \pmod p$

$s = k^{-1}(m - ar) \pmod{p-1}$

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

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