Tema 10 - Criptografie

1. $M = 343$
semnătură digitală DSA
$p = 48731$
$q = 443$
α
$x = 7$
$a = 242$ (cheia secretă a lui Alice)

a) cheia publică = ?
b) $k = 427$, fără fct. de funcție
semnătura digitală + verif autenticitate

a) cheia publică: (p, q, g, α)

$\alpha = g^a \pmod q$

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

$\Rightarrow g = 7^{110} \pmod{48731} = (7^2)^{55} \pmod{48731} = 49(49^2)^{27} \pmod{48731}$

$= 49 \cdot 2401 \cdot (2401^2)^{13} \pmod{48731} = 20187 \cdot 14643 \cdot (14543^2)^6 \pmod{48731}$

$= 23997 \cdot (630q^2)^3 \pmod{48731} = 23997 \cdot 38985 \cdot 38985^2 \pmod{48731}$

$= 34038 \cdot 7797 \pmod{48731} = \underline{5260}$

$\alpha = 5260^{242} \pmod p = (5260^2)^{121} \pmod{48731} = 37123 \cdot (37123^2)^{60} \pmod{48731}$

$= 37123 \cdot (449^2)^{30} \pmod{48731} = 37123 \cdot (8815^2)^{15} \pmod{48731} = 37123 \cdot 27011 \cdot (27011^2)^7 \pmod{48731}$

$= 40297 \cdot 42320 \cdot (42320^2)^3 \pmod{48731} = 27695 \cdot 20688 \cdot 20688^2 \pmod{48731}$

$= 23793 \cdot 37702 \pmod{48731} = \underline{3438}$

$\Rightarrow$ cheia publică: $(p = 48731, q = 443, g = 5260, \alpha = 184)$

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

$g^k \pmod p = 5260^{427} \pmod{48731} = 5260 \cdot (5260^2)^{213} \pmod{48731}$

$= 5260 \cdot 37123 \cdot (37123^2)^{106} \pmod{48731} = 1863 \cdot (449^2)^{53} \pmod{48731}$

$= 1863 \cdot 8815 \cdot (8815^2)^{26} \pmod{48731} = 48729 \cdot (27011^2)^{13} \pmod{48731}$

$= 48729 \cdot 42320 \cdot (42320^2)^6 \pmod{48731} = 12822 \cdot (20688^2)^3 \pmod{48731}$

$= 12822 \cdot 37702 \cdot 37702^2 \pmod{48731} = 3524 \cdot 6265 \pmod{48731}$

$= \underline{2717}$

$r = 2717 \pmod{443} = 59$; $h(m) = m = 343$ (nu s fol. fct de trunchiere)

$s = k^{-1}(h(m) + ax) \pmod q = 424^{-1}(343 + 242 \cdot 59) \pmod{443}$

$424^{-1} \pmod{443} = 83$

$443 = 1 \cdot 424 + 16 \Rightarrow X_{16} = (1,0) - (0,1) = (1,-1)$

$424 = 26 \cdot 16 + 11 \Rightarrow X_{11} = (0,1) - 26(1,-1) = (-26, 27)$

$16 = 1 \cdot 11 + 5 \Rightarrow X_5 = (1,-1) - (-26,27) = (27,-28)$

$11 = 2 \cdot 5 + 1 \Rightarrow X_1 = (-26,27) - 2(27,-28) = (-80, \underline{83})$

$s = 83(343 + 242 \cdot 59) \pmod{443} = 83(343 + 102) \pmod{443} = 83 \cdot 445 \pmod{443}$

$= 166$

$\Rightarrow$ semnătura digitală : $(r, s) = (59, 166)$

verificare :

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

$s^{-1} \pmod q = 166^{-1} \pmod{443} = -8 = \underline{435}$

$443 = 2 \cdot 166 + 111 \Rightarrow X_{111} = (1,0) - 2(0,1) = (1,-2)$

$166 = 1 \cdot 111 + 55 \Rightarrow X_{55} = (0,1) - (1,-2) = (-1,3)$

$111 = 2 \cdot 55 + 1 \Rightarrow X_1 = (1,-2) - 2(-1,3) = (3,-8)$

$s^{-1} \cdot h(m) \pmod q = 435 \cdot 343 \pmod{443} = \underline{357}$

$g^{357} \pmod p = 5260^{357} \pmod{48731} = 25843$

$r \cdot s^{-1} \pmod q = 59 \cdot 435 \pmod{443} = 414$

$\alpha^{414} \pmod p = 3438^{414} \pmod{48731} = 41081$

$r = (41081 \cdot 25843 \pmod{48731}) \pmod{443} = 2717 \pmod{443} = 59$ ✓

↳ semnătura este autentică

2. Semnătură RSA

cheia publică $k_e = (n = 28829, e)$, e = cel mai mic exponent posibil

$m = 11111$

semnătura folosită pt a semna mesajul public m.

$s = m^d \pmod n$

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

$\varphi(n) = (p-1)(q-1)$

$n = p \cdot q$

$[\sqrt{28829}] = 169$

$\Rightarrow t = 170 \Rightarrow t^2 - n = 170^2 - 28829 = (169+1)^2 - 28829$

$= 169^2 - 28829 + 2 \cdot 169 + 1 = -99 + 338 + 1 = 240$

$\Rightarrow t = 171 \Rightarrow t^2 - n = 171^2 - 28829 = 170^2 + 341 - 28829 = 240 + 341$

$= 581$

$t = 172 \Rightarrow t^2 - n = 172^2 - 28829 = 171^2 + 343 - 28829 = 5811 + 343 = 924$

$t = 173 \Rightarrow t^2 - n = 924 + 345 = 1269$

$t = 174 \Rightarrow t^2 - n = 1269 + 347 = 1616$

$t = 175 \Rightarrow t^2 - n = 1619 + 349 = 2068$

$t = 176 \Rightarrow t^2 - n = 2068 + 351 = 2419$

$t = 177 \Rightarrow t^2 - n = 2419 + 353 = \ldots 2$

$28829 = 127 \cdot 227$

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

$d = e^{-1} \pmod{\varphi(n)} = 5^{-1} \pmod{28476}$

e = cel mai mic exponent posibil $\Rightarrow$ $e = 5$ (28476 se divide prin 2, 3)

$\Rightarrow d = 22781$

$s = m^d \pmod{n} \Rightarrow s = 11111^{22781} \pmod{28829}$

$\Rightarrow s = 11111 \cdot (11111^2)^{11390} \pmod{28829} = 11111 \cdot (8543^2)^{5695} \pmod{28829}$

$= 11111 \cdot 16660 \cdot (16650^2)^{2847} \pmod{28829}$

$= 2457 \cdot 2836 \cdot (2836^2)^{1423} \pmod{28829}$

$= 20263 \cdot 28434 \cdot (28434^2)^{711} \pmod{28829}$

$= 10577 \cdot 11880 \cdot (11880^2)^{355} \pmod{28829}$

$= 17978 \cdot 16445 \cdot (16445^2)^{177} \pmod{28829}$

$= 6815 \cdot 22005 \cdot (22005^2)^{88} \pmod{28829}$

$= 24446 \cdot (8141^2)^{44} \pmod{28829}$

$= 24446 \cdot (26839^2)^{22} \pmod{28829}$

$= 24446 \cdot (10527^2)^{11} \pmod{28829}$

$= 24446 \cdot 27882 \cdot (27882^2)^{5} \pmod{28829}$

$= 28154 \cdot 3110 \cdot (3110^2)^{2} \pmod{28829}$

$= 5267 \cdot 14385^2 \pmod{28829}$

$= 5267 \cdot 22492 \pmod{28829}$

$= 7003$

$\Rightarrow s = 7003$

3. $p = 1223$

$q = 1987$

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

$m = 1070777$

semnătura folosită pt mesajul m

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

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

$2426892 = 2 \cdot 948047 + 530798 \Rightarrow x_{530798} = (1,0) - 2(0,1) = (1,-2)$

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

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

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

$113549 = 1 \cdot 76602 + 36947 \Rightarrow x_{36947} = (2,-5) - (-7,18) = (9,-23)$

$76602 = 2 \cdot 36947 + 2708 \Rightarrow x_{2708} = (-7,18) - 2(9,-23) = (-25,64)$

$36947 = 13 \cdot 2708 + 1743 \Rightarrow x_{1743} = (9,-23) - 13(-25,64) = (334,-855)$

$2708 = 1 \cdot 1743 + 965 \Rightarrow x_{965} = (-25,64) - (334,-855) = (-359,919)$

$1743 = 1 \cdot 965 + 778 \Rightarrow x_{778} = (334,-855) - (-359,919) = (693,-1774)$

$965 = 1 \cdot 778 + 187 \Rightarrow x_{187} = (-359,919) - (693,-1774) = (1052,-2693)$

$778 = 4 \cdot 187 + 30 \Rightarrow x_{30} = (693,-1774) - 4(-1052,2693) = (4901,-12546)$

$187 = 6 \cdot 30 + 7 \Rightarrow x_7 = (-1052,2693) - 6(4901,-12546) = (-30458,77969)$

$30 = 4 \cdot 7 + 2 \Rightarrow x_2 = (4901,-12546) - 4(-30458,77969) = (126733,-324282)$

$7 = 3 \cdot 2 + 1 \Rightarrow x_1 = (-30458,77969) - 3(126733,-324282) = (410657,-1051235)$

$\Rightarrow d = 1051235$

$\Delta = m^d \pmod{n} = 1070777^{1051235} \pmod{2430101}$

$\Delta = 153337$