Tema 10

Exercitiul 1

Pentru a semna mesajul m = 443 folosind o schemă de semnătură digitală: DSA, Alice alege p = 48731, q = 443 și x = 242 secretă a lui Alice este a = 242.

a) Det. cheia publică a lui Alice: (p, 2, g, α)

$g = 7^{(48731-1)/443} \pmod{48731}$

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

$= 49 \cdot 49^{54} \pmod{48731} = 49 \cdot (49^2)^{27} \pmod{48731} = 49 \cdot 2401^{27} \pmod{48731}$

$= 49 \cdot 2401 \cdot (2401^2)^{13} = 117649 \cdot (2401^2)^{13} \pmod{48731}$

$= 20187 \cdot (5764801)^{13} \pmod{48731} = 20187 \cdot (14543)^{13} \pmod{48731}$

$= 20187 \cdot 14543 \cdot (14543^2)^6 \pmod{14543} = 170150 \cdot (14543^2)^6 \pmod{48731}$

$\equiv 170150 \cdot (6305^2)^3 \pmod{48731} = 170150 \cdot 4960^3 \pmod{48731} =$

$23997 \quad 23997$

$23997 \cdot 4960 \cdot (4960^2) \pmod{48731} = 24018 \cdot 41176 \pmod{48731}$

$= 18254 \pmod{48731}$

$\alpha = 18254^{242} \pmod{48731} = (18254^2)^{121} \pmod{48731} = (34663^2)^{60} \cdot 34663$

$\pmod{48731} = (38127^2)^{30} \cdot 34663 \pmod{48731} = (36581^2)^{15} \cdot 34663$

$\pmod{48731} = (16301^2)^7 \cdot 16301 \cdot 34663 \pmod{48731} = 5962 \cdot 41189 \cdot$

$(41189^2)^3 \pmod{48731} = 13309 \cdot 12687 \pmod{48731} = 47099 \cdot 1476$

$\cdot 12687^2$ ☺ $\pmod{48731}$

$= 27718$

(b) $k = 127$?

$\frac{23}{3}$ $\frac{24}{11}$

69 56

2. Pentru a semnătură RSA, Alice folosește cheia publică $k_e = (m = 22225, e$

cu e al mai mic exponent natural nenumărat semnătura folosită de Alice pentru

a semna mesajul public $m = 11111$

$[\sqrt{28825}] = 169$

$\sqrt{28825}$	169
1	$25 - 25 = 156$
188	$329 - 9 = 2961$
156	
= 3229	
2961	
~~268~~	
368	

$t = 170$

$t^2 - m = 170^2 - 28825$

$= 71$

$t = 171$

$t^2 - m = 171^2 - 28825 = 4112$

$t = 172$

$t^2 - m = 755$

$t = 173$

$t^2 - m = 1100$

$t = 174$

$t^2 - m = 1447$ ...

$t = 177$

$t^2 - m = 2500 = 50^2$

$t = 177, \; s = 50$

$177^2 - 50^2 = (177 + 50)(177 - 50)$

$= 227 \cdot 127$

$28825 = 227 \cdot 127$

$p = 227, \; q = 127$

$\varphi(m_A) = (p_A - 1)(q_A - 1) = (127 - 1)(227 - 1) = 126 \cdot 226 = 28476$

$(\varphi(m), e_A) = 1$

$(28476, e_A) = 1$

$\downarrow$

$e_A = 3$

$(28476, 3) = (\varphi(m), e_A)$

$d_A \cdot e_A \equiv 1 \pmod{28476}$ $(d_A \cdot e_A \equiv 1 \pmod{\varphi(m)})$

$d_A = 3^{-1}$ modulo 28476 (calculăm inversul lui 3 modulo 28476 folosind algoritmul extins al lui Euclid)

$3x + 28476y = \gcd(3, 28476)$

$28476 = 3 \cdot 9492 + 0 \rightarrow 0 = 28476 - 3 \cdot 9492$

$3 = 0 + 3 \cdot 1 \rightarrow x = -9492 \quad y = 1$

$$\begin{array}{r|l} 28476 & 3 \\ \hline 27 & 9492 \\ \hline 14 & \\ 12 & \\ \hline 27 & \\ 27 & \\ \hline 0 & \end{array}$$

$d_A = -9492 \bmod 28476$

$d_A = -9492 + 28476 = 18984$

$$\begin{array}{r} 28476 \\ 9492 \\ \hline 18984 \end{array}$$

$k_{e_A} = (3, 28476)$ NU! $k_{e_A} = (3, 28829)$

$k_{d_A} = (18984, 28476)$ NU! $k_{d_A} = (18984, 28829)$

$D \equiv 11111^{18984} \pmod{28829}$

$D = (11111^2)^{9492} \pmod{28829} \equiv (28543)^{9492} \pmod{28829}$

$= (28543^2)^{4746} \pmod{28829} \equiv 16650^{4746} \pmod{28829} = (16650^2)^{2373}$

$\equiv 2836^{2373} \pmod{28829} = 2836 \cdot (2836^2)^{1186} \pmod{28829}$

$\equiv 2836 \cdot 10920^{1186} \pmod{28829} = 2836 \cdot 10920^{593} \pmod{28829}$

$= 2836 \cdot 10920 \cdot (10920^2)^{296} \bmod 28829 \equiv 6774 \cdot (9656^2)^{148} \pmod{28829}$

$\equiv 6224 \cdot 5350^{74} \pmod{28229}$

$\equiv 6224 \cdot (5350^2)^{37} \pmod{28229}$

$\equiv 6224 \cdot (24132^2)^{18} \cdot 24132 \pmod{28229}$

$\equiv 9738 \cdot (7624^2)^9 \cdot \pmod{28229}$

$\equiv 9738 \cdot 6112^9 \pmod{28229}$

$\equiv 9738 \cdot 6112 \cdot 6112^8 \pmod{28229}$

$\equiv 15600 \cdot (6112^2)^4$ (-11- -11-)

$\equiv 15600 \cdot (22983)^2$ (-11- -11-)

$\equiv 15600 \cdot 893^2$ (-11- -11-)

$\equiv 1560 \cdot 19066$ (-11- -11-)

$\equiv 20261$

$m = 1626227$

$m = p \cdot q = 2426852$

$\varphi(m) = (p-1)\cdot(q-1) = (1223-1)(1328-1) = 1222 \cdot 1326 = 2420772$

$e = 948047$ (invers lui 948047 modulo 2420772)

$Q_A = ?$

$\mathcal{K}_{2426852} = (1,0)$

$\mathcal{K}_{948047} = (0,1)$

$2426852 = 948047 \cdot 2 + 530758$

$948047 = 530758 \cdot 1 + 417289$

$530758 = 417289 \cdot 1 + 113469$

$417289 = 113469 \cdot 3 + 76602$

$113469 = 76602 \cdot 1 + 36942$

$76602 = 36942 \cdot 2 + 2718$

$36942 = 2718 \cdot 13 + 1608$

$2718 = 1608 \cdot 1 + 1110$

$1608 = 1110 \cdot 1 + 498$

$1110 = 498 \cdot 2 + 114$

$498 = 114 \cdot 4 + 42$

$114 = 42 \cdot 2 + 30$

$42 = 30 \cdot 1 + 12$

$30 = 12 \cdot 2 + 6$

$12 = 6 \cdot 2 + 0$

$\mathcal{K}_{530758} = (1,0) - (0,1) = (1,-1)$

$\mathcal{K}_{417289} = (0,1) - (1,-2) = (-1,4)$

$\mathcal{K}_{113469} = (1,-2) - (-1,4) = (2,-6)$

$\mathcal{K}_{76602} = (-1,4) - 3(2,-6) = (-1,4) - (6,-18)$

$= (-7,22)$

$\mathcal{K}_{36942} = (2,-6) - 1(-7,22)$

$= (2,-6) - (-7,22)$

~~$= (-9,60)$~~ $= (-5,-28)$

~~$\mathcal{K}_{1608} = \mathcal{K}_{(-5,-28)} + 1 \cdot \mathcal{K}_{2718}$~~

$\mathcal{E}_{2718} = \mathcal{E}_{76602} - 2 \cdot \mathcal{E}_{36842}$

$= (-7,22) - 2 \cdot (-5,-28)$

$= (-7,22) - (-10,-56)$

$= (3,78)$

$\mathcal{E}_{1608} = \mathcal{E}_{36842} - 13\,\mathcal{E}_{2713}$

$= (-5,-28) - 13 \cdot (3,76)$

$= (-5,-28) - (39,-1014)$

$= (-44,986)$

$\mathcal{E}_{1110} = (3,78) - (-44,986) = (47,908)$

$\mathcal{E}_{498} = (-44,986) - (47,908) = (-91,78)$

$\mathcal{E}_{114} = (47,908) - 2 \cdot (-91,78) = (229,752)$

$\mathcal{E}_{42} = (-91,78) - 4 \cdot (229,752) = (-1007,-2930)$

$\mathcal{E}_{30} = (229,752) - 2 \cdot (-1007,-2930) = (2243,6612)$

$\mathcal{E}_{12} = (-1007,-2930) - (2243,6612) = (-3250,-9542)$

$\mathcal{E}_6 = (2243,6612) - 2(-3250,-9542) = (8743,25696)$

$6 = 2713 \cdot 2 + 256$

$d = 2713$

$m = 1020777$

$n = m^d \bmod 2430101 = 1020777^{2713} \bmod 2430101$

$= 2086307$

4. $p = 21739$

$g = 7$

$a = 15140$

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

$(7^2)^{7570} \pmod{21739} = (49^2)^{3785} \pmod{21739}$

$= 2401 \cdot (2401^2)^{1892} \pmod{21739}$

$\equiv 2401 \cdot (3561^2)^{946} \pmod{21739}$

$\equiv 2401 \cdot (11859^2)^{473} \pmod{21739}$

$\equiv 2401 \cdot 6250 \cdot (6250^2)^{236} \pmod{21739}$

$\equiv 15424 \cdot (20255^2)^{118} \pmod{21739}$

$\equiv 15424 \cdot (13535^2)^{59} \pmod{21739}$

$\equiv 15424 \cdot 1672 \cdot (1672^2)^{29} \pmod{21739}$

$\equiv 6474 \cdot (12092^2)^{14} \pmod{21739}$

$\equiv 6474 \cdot (10168^2)^7 \pmod{21739}$

$\equiv 6474 \cdot 14464 \cdot (14464^2)^3 \pmod{21739}$

$\equiv 10063 \cdot 12890 \cdot 12890^2 \pmod{21739}$

$\equiv 20802 \cdot 15634 \pmod{21739}$

$\equiv 15891 \pmod{21739}$

$\alpha = 15891$

b) $m = 5331$

$k = 10227$

$r = 2^{10227} \pmod{21739}$

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

$= 10227^{-1} (5331 - 15140 \cdot r) \pmod{21738}$

$$7^{10727} \pmod{21739} = 7 \cdot (7^2)^{5363} \pmod{21739}$$

$$= 7 \cdot (49^2)^{2681} \pmod{21739}$$

$$= 343 \cdot (2401^2)^{1340} \cdot 2401 \pmod{21739}$$

$$\equiv 19200 \cdot (3966^2)^{670} \pmod{21739}$$

$$\equiv 19200 \cdot (11859^2)^{335} \pmod{21739}$$

$$\equiv 19200 \cdot 6200 \cdot (6200^2)^{167} \pmod{21739}$$

$$\equiv 7855 \cdot 20859 \cdot (20859^2)^{83} \pmod{21739}$$

$$\equiv 602 \cdot 13535 \cdot (13535^2)^{41} \pmod{21739}$$

$$\equiv 17684 \cdot 1672 \cdot (1672^2)^{20} \pmod{21739}$$

$$\equiv 2608 \cdot (12992^2)^{10} \pmod{21739}$$

$$\equiv 2608 \cdot (10468^2)^{5} \pmod{21739}$$

$$\equiv 2608 \cdot 11464 \cdot (11464^2)^{2} \pmod{21739}$$

$$\equiv 4947 \cdot 12899^2 \pmod{21739}$$

$$\equiv 4947 \cdot 15634 \pmod{21739}$$

$$\equiv 15775 \pmod{21739}$$

$$\boxed{R = 15775}$$

$$D = 10727^{-1} \cdot (5331 - 15440 \cdot 15775) \pmod{21738}$$