Tema 10
Cătălin Răpleanu

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

(a) Det. cheia publică a lui Alice
(b) Pt. semnătura digitală, Alice alege $k = 427$, fără a folosi o funcție de trunchiere. Det. semnătura digitală și verif. autenticitatea acesteia.

a) cheia publică (p, q, g, α)

$p = 48731$
$q = 443$

$g = x^{(p-1)/q} \pmod p$

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

$= (7^2)^{55} \pmod{48731} \equiv 49 \cdot (49^2)^{27} \equiv 49 \cdot (2401)^{27} \equiv$

$\equiv 49 \cdot 2401 \cdot (2401^2)^{13} \equiv 20187 \cdot 14543 \cdot (14543^2)^6 \equiv$

$\equiv 23997 \cdot (6399^2)^3 \equiv 23997 \cdot 38985 \cdot 38985^2 \equiv$

Scanned with CamScanner

$\equiv 34038 \cdot 7797 \equiv 5260 \pmod{48731}$

$g = 5260$

$\alpha = g^{a} \pmod{p}$

$\alpha = 5260^{242} \pmod{48731} \equiv (5260^2)^{121} \equiv$

$\equiv 37123 \cdot (37123^2)^{60} \equiv 37123 \cdot 4449^{60} \equiv$

$\equiv 37123 \cdot (4449^2)^{30} \equiv 37123 \cdot (8815^2)^{15} \equiv$

$\equiv 37123 \cdot 27011 \cdot (27011^2)^{7} \equiv 40297 \cdot 42320 \cdot (42320^2)^3 \equiv$

$\equiv 27695 \cdot 20688 \cdot 20688^2 \equiv 23793 \cdot 37702 \equiv$

$\equiv 3438 \pmod{48731}$

Cheia publică $(48731, 443, 5260, 3438)$

b) semnătura : (r, s)

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

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

$\equiv 5260 \cdot (5260^2)^{210} \equiv 5260 \cdot (37123^2)^{105} \equiv$

~~[illegible]~~

$$\equiv 5260 \cdot 4449 \cdot (4449^2)^{52} \equiv 10860 \cdot (8815^2)^{26} \equiv$$

$$\equiv 10860 \cdot (27011^2)^{13} \equiv 10860 \cdot 42320 \cdot (42320^2)^{6} \equiv$$

$$\equiv 13139 \cdot (20688^2)^{3} \equiv 13139 \cdot 37702 \cdot 37702^2 \equiv$$

$$\equiv 15963 \cdot 6265 \equiv 12183$$

$$r = 12183 \pmod{443} = 222 \pmod{443}$$

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

$$42\cancel{4}7^{-1} \pmod{443}$$

$$443 = 427 \cdot 1 + 16$$
$$427 = 16 \cdot 26 + 11$$
$$16 = 11 \cdot 1 + 5$$
$$11 = 5 \cdot 2 + 1$$

$$X_{443} = (1,0), \quad X_{427} = (0,1)$$
$$X_{16} = (1,-1)$$
$$X_{11} = (0,1) - 26 \cdot (1,-1) = (0,1) - (26,-26) = (-26,27)$$
$$X_5 = X_{16} - X_{11} = (1,-1) - (-26,27) = (27,-28)$$
$$X_1 = X_{11} - 2 \cdot X_5 = (-26,27) - 2(27,-28) = (-80,83)$$

Scanned with CamScanner

$\Rightarrow 427^{-1} = 83 \pmod{443}$

$s = 83 \cdot 121 \pmod{443}$

$s = 297 \pmod{443}$

Semnatura $= (222, 297)$

$1 < 222 < 442$

$1 < 297 < 442$

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

$r = \left(\alpha^{r s^{-1} \pmod{q}} \pmod{p}\right) \pmod{q}$

$s^{-1} \pmod{443}$

$443 = 297 \cdot 1 + 146$

$297 = 146 \cdot 2 + 5$

$146 = 5 \cdot 29 + 1 \Rightarrow 1 = 146 - 5 \cdot 29$

$1 = 146 - 29(297 - 2 \cdot 146)$

$1 = 146 - 29 \cdot 297 + 58 \cdot 146$

$1 = 59 \cdot 146 - 29 \cdot 297$

$1 = 59(297 - 443) - 29 \cdot 297$

$1 = 30 \cdot 297 - 59 \cdot 443$

Scanned with CamScanner

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

Det. semnătura folosită de Alice pt-a semna mesajul public $m = 11111$.

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

$d \cdot e \equiv 1 \pmod{\varphi(n)} \Rightarrow d \equiv e^{-1} \pmod{\varphi(n)}$ ✓

$\varphi(n) = (p-1)(q-1)$ ✓, unde $n = pq$ ✓

$\sqrt{2\,88\,29}$ | 169

1 | $26 \cdot 6 = 156$

188 | $329 \cdot 9 = 2961$

156

$= 3229$

2961

$= 268$

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

$t = 170$

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

$t = 171$

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

$t = 172$

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

$t = 173$

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

$t = 174$

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

~~$t = 227$~~

~~$t^2 - n = 51529 - 28829 = 22700$~~

$t = 177$

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

$n = t^2 - s^2 = (t - s)(t + s) = 127 \cdot 227$

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

$\varphi(n) = 28476$

$e \in \{3, 4, \ldots, 28475\}$ a.î. $(\varphi(n), e) = 1$

$\Rightarrow$ pt. $e = 5$, $(28476, 5) = 1$

$\Rightarrow e = 5$

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

$28476 = 5 \cdot 5695 + 1 \Rightarrow 1 = 28476 - 5 \cdot 5695 \Rightarrow$

$\Rightarrow 5^{-1} \equiv -5695 (\bmod 28476) \equiv 22781 (\bmod 22781)$

$\Rightarrow d = 22781$

Scanned with CamScanner

$s = m^d \pmod n$

$s = 11111^{22781} \pmod{28829} \equiv$

$\equiv 11111 \cdot (11111^2)^{11390} \equiv 11111 \cdot (8543^2)^{5695} \equiv$

$\equiv 11111 \cdot 16650 \cdot (16650^2)^{2847} \equiv$

$\equiv 2457 \cdot 2836 \cdot (2836^2)^{1423} \equiv$

$\equiv 20263 \cdot 28434 \cdot (28434^2)^{711} \equiv$

$\equiv 10577 \cdot 11880 \cdot (11880^2)^{355} \equiv 17978 \cdot 16445 \cdot (16445^2)^{177} \equiv$

$\equiv 6815 \cdot 22005 \cdot (22005^2)^{88} \equiv 24446 \cdot (8141^2)^{44} \equiv$

$\equiv 24446 \cdot (26839^2)^{22} \equiv 24446 \cdot (10527^2)^{11} \equiv$

$\equiv 24446 \cdot 27882 \cdot (27882^2)^5 \equiv 28154 \cdot 3110 \cdot (3110^2)^2 \equiv$

$\equiv 5267 \cdot 14385^2 \equiv 5267 \cdot 22492 \equiv 7003$

$s = 7003$

Scanned with CamScanner

3) $p = 1223$, $q = 1987$

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

Det. semnătura pt. $m = 1070777$

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

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

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

$d \equiv 948047^{-1} \pmod{2426892}$

$(2426829, 948047) =$

$2426829 = 948047 \cdot 2 + 530735$

$948047 = 530735 \cdot 1 + 417312$

$530735 = 417312 \cdot 1 + 113423$

$417312 = 113423 \cdot 3 + 77043$

$113423 = 77043 \cdot 1 + 36380$

$77043 = 36380 \cdot 2 + 4283$

$36380 = 4283 \cdot 8 + 2116$

$4283 = 2116 \cdot 2 + 51$

$2116 = 51 \cdot 41 + 25$

$51 = 25 \cdot 2 + 1$

Scanned with CamScanner

$x_{2426829} = (1,0)$, $x_{948047} = (0,1)$

$x_{530735} = (1,-2)$

$x_{417312} = (-1,3)$

$x_{113423} = (1,-2) - (-1,3) = (2,-5)$

$x_{77043} = (-1,3) - 3\cdot(2,-5) = (-7,18)$

$x_{36380} = (2,-5) - (-7,18) = (9,-23)$

$x_{4283} = (-7,18) - 2(9,-23) = (-25,64)$

$x_{2116} = (9,-23) - 8(-25,64) = (209,-535)$

$x_{51} = (-25,64) - 2\cdot(209,-535) = (-443,1134)$

$x_{25} = (209,-535) - 41(-443,1134) =$

$= (18372,-47029)$

$x_1 = (-443,1134) - 2(18372,-47029) =$

$= (-37187, 95192)$

$\Rightarrow d = 95192 \pmod{\varphi(n)}$

$D = 1070777^{95192} \pmod{2430101} \equiv$

$\equiv \cancel{472}\ 420212^{47596} \equiv 2126082^{23798} \equiv$

$\equiv 482890^{11899} \equiv 482890 \cdot 2410645^{5949} \equiv$

$\equiv 2092727 \cdot 1870281^{2974} \equiv 2092727 \cdot 456935^{1487} \equiv$

Scanned with CamScanner

$\equiv 328447 \cdot 176507^{743} \equiv 705173 \cdot 826229^{372} \equiv$

$\equiv 705173 \cdot 107925^{186} \equiv 705173 \cdot 331532^{93} \equiv$

$\equiv 1978432 \cdot 2428895^{46} \equiv 1978432 \cdot 1454436^{23} \equiv$

$\equiv 689444 \cdot 598404^{11} \equiv 510303 \cdot 2244462^{5} \equiv$

$\equiv 488666 \cdot 576040^{2} \equiv 488666 \cdot 1510454 \equiv$

$\equiv 787129$

$n = 787129$

4) $n = 21739$

$g = 7$

$a = 15140$

(a) cheia publică $(n; g; \alpha)$

$\alpha = g^{a} \pmod{n}$

$\alpha = 7^{15140} \pmod{21739} \equiv (7^{4})^{3785} \equiv 2401^{3785} \equiv$

$\equiv 2401 \cdot (2401^{2})^{1892} \equiv 2401 \cdot (3966^{2})^{946} \equiv$

$\equiv 2401 \cdot (11859^{2})^{473} \equiv 2401 \cdot 6290 \cdot (6290^{2})^{236} \equiv$

$\equiv 15424 \cdot (20859^{2})^{118} \equiv 15424 \cdot (13535^{2})^{59} \equiv$

Scanned with CamScanner

$\equiv 15424 \cdot 1672 \cdot (1672^2)^{29} \equiv 6474 \cdot 12992^{29} \equiv$

$\equiv 6474 \cdot 12992 \cdot (12992^2)^{14} \equiv 2017 \cdot (10468^2)^{7} \equiv$

$\equiv 2017 \cdot 14464 \cdot (14464^2)^{3} \equiv 150 \cdot 12899^{3} \equiv$

$\equiv 150 \cdot 12899 \cdot 15634 \equiv 17702$

$\Rightarrow (p; g; \alpha) = (21739, 7, 17702)$

(b) pt. $m = 5331$

$k = 10727$

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

$g^k \pmod p = 7^{10727} \pmod{21739} \equiv 7 \cdot 7^{10726} \equiv$

$\equiv 7 \cdot 49 \cdot 49^{5362} \equiv 343 \cdot 2401^{2681} \equiv 19200 \cdot (3966^2)^{1340} \equiv$

$\equiv 1920 \cdot (11859^2)^{670} \equiv 1920 \cdot (6290^2)^{335} \equiv 11655 \cdot (20859^2)^{167} \equiv$

$\equiv 11655 \cdot 20859 \cdot (13535^2)^{83} \equiv 4408 \cdot 1672 \cdot (1672^2)^{41} \equiv$

$\equiv 655 \cdot 12992 \cdot (12992^2)^{20} \equiv 9811 \cdot (10468^2)^{10} \equiv 9811 \cdot (14464^2)^{5} \equiv$

$\equiv 9811 \cdot 12899 \cdot (12899^2)^{2} \equiv 9370 \cdot 15634^{2} \equiv 9370 \cdot 10379 \equiv$

$\equiv 12683$

$r = g^h \pmod p = 12683$

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

$h^{-1} \pmod{21738} = 10727^{-1} \pmod{21738}$

$21738 = 10727 \cdot 2 + 284$

$10727 = 284 \cdot 37 + 219$

$284 = 219 \cdot 1 + 65$

$219 = 65 \cdot 3 + 24$

$65 = 24 \cdot 2 + 17$

$24 = 17 \cdot 1 + 7$

$17 = 7 \cdot 2 + 3$

$7 = 3 \cdot 2 + 1$

$x_{21738} = (1, 0), \quad x_{10727} = (0, 1)$

$x_{284} = (1, -2)$

$x_{219} = (0, 1) - 37(1, -2) = (-37, 75)$

$x_{65} = (1, -2) - (-37, 75) = (38, -77)$

$x_{24} = (-37, 75) - 3(38, -77) = (-151, 306)$

$x_{17} = (38, -77) - 2(-151, 306) = (340, -689)$

$x_7 = (-151, 306) - (340, -689) = (-491, 995)$

$x_3 = (340, -689) - 2 \cdot (-491, 995) = (1322, -2679)$

$x_1 = (-491, 995) - 2 \cdot (1322, -2679) = (-3135, 6353)$

$10727^{-1} \equiv 6353 \pmod{21738}$

$s = 6353(5331 - 15140 \cdot 12683) \pmod{21738} =$

Scanned with CamScanner

$= 6353(5331 - 8866) \pmod{21738} =$

$= 6353 \cdot 18203 = 19237 \pmod{21738}$

$(r, s) = (12683, 19237)$

Scanned with CamScanner