Tema 7

Cătălin Rîpeanu

118. Ana și Bob folosesc RSA. Ana are cheia secretă $(n = 12827, d = 2291)$. Determinați cheia sa publică și criptați textul IERI dacă lungimea în clar este 2 și lungimea blocurilor criptate este 3.

$e = ?$

$d \cdot e \equiv 1 (\bmod \varphi(n))$

$\sqrt{1.2.8.2.7}$ | 113

1 | $21 \cdot 1 = 21$

$= 28$ | $223 \cdot 3 = 669$

21

$= 727$

669

$[\sqrt{12827}] = 113$

$t = 114$

$t^2 - n = 114^2 - 12827 = 12996 - 12827 = 169 = 13^2 = s^2$

~~$\varphi(n) = (p-1)(q-1) = 12 \cdot 12 = 144$~~

$s = 13$

$n = (t-s)(t+s) = (114-13)(114+13) =$

$= 101 \cdot 127$

$\varphi(n) = (101-1)(127-1) = 100 \cdot 126 = 12600$

$e \cdot 2291 \equiv 1 \pmod{12600}$

$e = 2291^{-1} \pmod{12600}$

$12600 = 2291 \cdot 5 + 1145$
$2291 = 1145 \cdot 2 + 1$

$(12600, 2291) = 1 \Rightarrow \exists\, 2291^{-1}$

$X_{12600} = (1, 0) \qquad X_{2291} = (0, 1)$

$X_{1145} = (1,0) - 5(0,1) = (1, -5)$

$X_1 = X_{2291} - 2X_{1145} = (0,1) - 2 \cdot (1,-5) =$
$= (0,1) - (2,-10) = (-2, 11)$

$\Rightarrow 1 = -2 \cdot 12600 + 11 \cdot 2291 \Rightarrow$
$\Rightarrow 2291^{-1} \equiv 11 \pmod{12600}$

$\Rightarrow e = 11 \pmod{12600}$

$(n, e) = (12827, 11)$

$i = 8 \qquad e = 4 \qquad R = 17 \qquad i = 8$

$8^{11} \pmod{12827} \equiv 8 \cdot (8^2)^5 \pmod{12827} \equiv 8 \cdot 64 \cdot (64^2)^2 \equiv$
$\equiv 512 \cdot 4096^2 \equiv 512 \cdot 12327 \equiv 540$

$4^{11} (\mathrm{mod}\ 12827) \equiv 4 \cdot 16^5 \equiv 4 \cdot 16 \cdot (16^2)^2 \equiv$

$\equiv 64 \cdot 256^2 \equiv 64 \cdot 1401 \equiv 12702$

$17^{11} (\mathrm{mod}\ 12827) \equiv 17 \cdot (17^2)^5 (\mathrm{mod}\ 12827) \equiv$

$\equiv 17 \cdot 289 \cdot (289^2)^2 \equiv 4913 \cdot 6559^2 \equiv$

$\equiv 4913 \cdot 11580 \equiv 11329$

8 → 540

4 → 12702

17 → 11329

8 → 540

5.40 1.270.2 11.329 .540