Tutoriel 12

P2 $c = 1935$; $n = 4757 = 67 \cdot 71 = p \cdot q$

- Note : $p, q \equiv 3 \pmod 4$
- Compute square roots of c modulo p and q

$k_p = \frac{p+1}{4} = 17$; $k_q = \frac{q+1}{4} = 18$

$t_{p,1} = c^{k_p} = 1935^{17} \equiv 59^{17} \equiv (-8)^{17} \equiv 40 \pmod{67}$

$t_{p,2} = -t_{p,1} \equiv 27 \pmod{67}$

$t_{q,1} = c^{k_q} = 1935^{18} \equiv 18^{18} \equiv 36 \pmod{71}$

$t_{q,2} = -t_{q,1} \equiv 35 \pmod{71}$

Bit	S	M
1	-8	
0	$64 \equiv -3$	-
0	9	-
0	14	-
1	$62 \equiv -5$	40

Bit	S	M
1	18	
0	40	
0	38	
1	24	6
0	36	

- Compute the resulting square roots of c modulo n

$m_{i,j} = a \cdot t_{p,i} + b \cdot t_{q,j}$ solves $m_{i,j}^2 \equiv c \pmod n$ $i, j = 1, 2$

Let $t \cdot q + s \cdot p = 1$ (from EEA), then $a = t \cdot q$ and $b = s \cdot p$

In our case $1 = 17 \cdot 71 + (-18) \cdot 67$ from EEA

$a = 17 \cdot 71 \equiv 1207 \pmod n$

$b = -18 \cdot 67 \equiv -1206 \pmod n$

$\Rightarrow$ $m_{11} \equiv 1207 \cdot 40 - 1206 \cdot 36 \equiv \boxed{107} = m = (\ldots 1011)_2$

$m_{12} \equiv 1313 = (\ldots 0001)_2 \pmod n$

$m_{21} \equiv 3444 = (\ldots 0100)_2$

$m_{22} \equiv 4650 = (\ldots 1010)_2$

a_n	b_n	f_n	r_n	c_n	d_n
			71	1	0
			67	0	1
71	67	1	4	1	-1
67	4	16	3	-16	17
4	3	1	1	17	-18

P1/ a) $p = 11$; $a = 5$

1) $r = b^2 - 4 \cdot a = b^2 - 20$

With Euler's criterion: r is QR $\Leftrightarrow r^{\frac{p-1}{2}} \equiv 1 \pmod p$

$b = 5$: $r = 25 - 20 = 5 \Rightarrow r^{\frac{p-1}{2}} = 5^5 \equiv 1 \pmod{11}$ ↯

$b = 6$: $r = 36 - 20 \equiv 5 \pmod{11} \Rightarrow r^{\frac{p-1}{2}} \equiv 1 \pmod{11}$ ↯

$b = 7$: $r = 49 - 20 \equiv 7 \pmod{11} \Rightarrow 7^5 \equiv -1 \pmod{11}$ ✓

2) $f(x) = x^2 - bx + a = x^2 - 7x + 5$

3) Compute $r = x^{\frac{p+1}{2}} = x^6$ modulo $f(x)$

$x^6 : (x^2 - 7x + 5) = x^4 + 7x^3 - 2x - 3 + \frac{4}{f(x)}$

$-(x^6 - 7x^5 + 5x^4)$

$7x^5 - 5x^4$

$-(7x^5 - 5x^4 + 2x^3)$

$-2x^3$

$-(-2x^3 + 13x^2 - 10x)$

$-3x^2 + 10x$

$-(-3x^2 + 10x - 4)$

4

$\Rightarrow r = 4$ and $(r_1 - r) = (4, 7)$

b) Given $n = p \cdot q = 11 \cdot 23 = 253$, $c = 225$; $p, q \equiv 3 \pmod 4$

from a) $t_{p,1} = 4$; $t_{p,2} = 7$

$k_q = \frac{q+1}{4} = 6$

$t_{q_1} = c^{k_q} = 225^6 \equiv 18^6 \equiv 8 \pmod{23}$

$t \cdot q + s \cdot p = 1$ $\quad 23 = 2 \cdot 11 + 1 \Leftrightarrow 1 = 1 \cdot 23 - 2 \cdot 11$

$a = t \cdot q = 23$; $b = s \cdot p = -22$

$m_{i,j} = a \, t_{p,i} + b \, t_{q,j}$

$m_{1,1} \equiv 169 = (\ldots 1001)_2$

$m_{1,2} \equiv 15 = (\ldots 1111)_2$

$m_{2,1} \equiv 238 = (\ldots 1110)_2$

$m_{2,2} \equiv 84 = (\ldots 0100)_2$ ✓

c) Since calculating square roots in the reals $m = 15 = \sqrt{225}$ can be easily computed.