Prof. Dr. Rudolf Mathar, Dr. Michael Reyer

Tutorial 12
- Proposed Solution -

Friday, July 12, 2019

Solution of Problem 1

a) $p = 11$ is a prime number, $a = 5$ is a quadratic residue (QR) modulo p.

1) $v = b^2 - 4a = b^2 - 4 \cdot 5 = b^2 - 20$.

   Choose: $b = 5 \Rightarrow v = 25 - 20 = 5$.
   With Euler's criterion (c is QR $\Leftrightarrow c^{\frac{p-1}{2}} \equiv 1 \pmod{p}$), compute:
   $5^{\frac{11-1}{2}} = 5^5 \equiv 1 \pmod{11}$.
   $\Rightarrow v = 5$ is a QR modulo 11. $\lightning$

   Choose: $b = 6 \Rightarrow v = 36 - 20 = 16 \equiv 5 \pmod{11}$.
   $\Rightarrow v = 5$ is a QR modulo 11. $\lightning$

   Choose: $b = 7 \Rightarrow v = 49 - 20 = 29 \equiv 7 \pmod{11}$.
   With Euler's criterion, compute:
   $7^5 \equiv 49 \cdot 49 \cdot 7 \equiv 5 \cdot 5 \cdot 7 \equiv -1 \pmod{11}$.
   $\Rightarrow v$ is a QNR modulo 11. ✓

2) Insert the values for a and b into the polynomial $f(x) = x^2 - 7x + 5$.

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

$$
\begin{array}{l}
x^6 : (x^2 - 7x + 5) = x^4 + 7x^3 - 2x - 3 \\
-\,(x^6 - 7x^5 + 5x^4) \\
\hline
+\,7x^5 - 5x^4 \\
-\,(7x^5 - 5x^4 + 2x^3) \\
\hline
-\,2x^3 \\
-\,(-2x^3 + 3x^2 - 10x) \\
\hline
-\,3x^2 + 10x \\
-\,(-3x^2 + 10x - 4) \\
\hline
4
\end{array}
$$

Hence, $r = 4$, and $(r, -r) = (4, 7)$.
// Validation $r^2 = a \mod 11$ is correct in both cases.

b) Both p and q satisfy the requirement for a Rabin cryptosystem: $p, q \equiv 3 \pmod{4}$.
For $c \mod p = 225 \mod 11 = 5$, we already know the square roots $x_{p,1} = 4$, $x_{p,2} = 7$.

For $c \mod q = 225 \mod 23 = 18$, compute the square roots $x_{q,1}$, $x_{q,2}$ with the auxiliary parameter $k_q = \frac{q+1}{4} = 6$:

$$\begin{aligned} x_{q,1} &= c^{k_q} = 18^6 = 18^3 \cdot 18^3 \equiv 13 \cdot 13 \equiv 8 \pmod{23}, \\ x_{q,2} &= -8 \equiv 15 \pmod{23}. \end{aligned}$$

Calculate $tq + sp = 1$:

$$\begin{aligned} 23 &= 2 \cdot 11 + 1 \\ \Rightarrow 1 &= 1 \cdot 23 - 2 \cdot 11. \end{aligned}$$

We set $a = tq = 23$ and $b = sp = -22$. Compute all four possible solutions:

$$\begin{aligned} m_{11} &= ax_{p,1} + bx_{q,1} = 23 \cdot 4 - 22 \cdot 8 = -84 \equiv 169 \pmod{253} \Rightarrow (...1001)_2 \quad ↯ \\ m_{12} &= ax_{p,1} + bx_{q,2} = 23 \cdot 4 - 22 \cdot 15 = -238 \equiv 15 \pmod{253} \Rightarrow (1111)_2 \quad ↯ \\ m_{21} &= ax_{p,2} + bx_{q,1} = 23 \cdot 7 - 22 \cdot 8 = -15 \equiv 238 \pmod{253} \Rightarrow (...1110)_2 \quad ↯ \\ m_{22} &= ax_{p,2} + bx_{q,2} = 23 \cdot 7 - 22 \cdot 15 = -169 \equiv 84 \pmod{253} \Rightarrow (...0100)_2 \quad \checkmark \end{aligned}$$

The solution is $m = m_{22} = 84$ since it ends on 0100 in the binary representation.
// Checking all solutions yields $c = 225$.

c) Since $c = 225$, one is enabled to compute two square roots in the reals, $m = \pm 15$. If naive Nelson chooses 1111, the result $m = 15$ is obvious, without knowing the factors of $n = p\,q$.

Solution of Problem 2

Decipher $m = \sqrt{c} \mod n = 4757 = 67 \cdot 71 = p\,q$ with $c = 1935$.

- Check $p, q \equiv 3 \pmod 4$ ✓
- Compute the square roots of c modulo p and c modulo q.

$$\begin{aligned} k_p &= \frac{p+1}{4} = 17, \quad k_q = \frac{q+1}{4} = 18, \\ x_{p,1} &= c^{k_p} \equiv 1935^{17} \equiv 59^{17} \equiv (-8)^{17} \equiv 40 \pmod{67}, \\ x_{p,2} &= -x_{p,1} \equiv 27 \pmod{67}, \\ x_{q,1} &= c^{k_q} \equiv 1935^{18} \equiv 18^{18} \equiv 36 \pmod{71}, \\ x_{q,2} &= -x_{q,1} \equiv 35 \pmod{71}. \end{aligned}$$

Bit	S	M
1	-8	-
0	64	-
0	9	-
0	14	-
1	62	40

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

- Compute the resulting square roots modulo n.
  $m_{i,j} = ax_{p,i} + bx_{q,j}$ solves $m_{i,j}^2 \equiv c \pmod{n}$ for $i, j \in \{1, 2\}$. We substitute $a = tq$ and $b = sp$. Then $tq + sp = 1$ yields $1 = 17 \cdot 71 + (-18) \cdot 67 = tq + sp$ from the Extended Euclidean Algorithm.

$$\Rightarrow a \equiv tq \equiv 17 \cdot 71 \equiv 1207 \pmod{n}$$
$$\Rightarrow b \equiv sp \equiv -18 \cdot 67 \equiv -1206 \pmod{n}.$$

The four possible solutions for the square root of ciphertext c modulo n are:

$$m_{1,1} \equiv ax_{p,1} + bx_{q,1} \equiv 107 \pmod{n} \Rightarrow 00000011010\underline{11},$$
$$m_{1,2} \equiv ax_{p,1} + bx_{q,2} \equiv 1313 \pmod{n} \Rightarrow 0010100100001,$$
$$m_{2,1} \equiv ax_{p,2} + bx_{q,1} \equiv 3444 \pmod{n} \Rightarrow 0110101110100,$$
$$m_{2,2} \equiv ax_{p,2} + bx_{q,2} \equiv 4650 \pmod{n} \Rightarrow 1001000101010.$$

The correct solution is $m_{1,1} = 107$, by the agreement given in the exercise. Calculating $\gcd(71, 67)$ gives

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