Prof. Dr. Rudolf Mathar, Jose Calvo, Markus Rothe

Tutorial 2
- Proposed Solution -

Friday, November 6, 2015

Solution of Problem 1

p prime, g primitive element modulo p and $a, b \in \mathbb{Z}_p^*$.

a) a is a quadratic residue modulo $p \;\Leftrightarrow\; \exists i \in \mathbb{N}_0 : a \equiv g^{2i} \mod p$

Proof. "$\Rightarrow$": a is a quadratic residue modulo p, i.e. $\exists k \in \mathbb{Z}_p^* : k^2 \equiv a \mod p$. g is a primitive element, i.e. $\exists l \in \mathbb{N}_0 : k \equiv g^l \mod p$. Then,

$$k^2 \equiv g^{2l} \equiv a \mod p\,.$$

"$\Leftarrow$": $\exists i \in \mathbb{N}_0 : a \equiv g^{2i} \mod p$. With $a \equiv (g^i)^2 \mod p$, a is a quadratic residue modulo i. □

b) If p is odd, then exactly one half of the elements $x \in \mathbb{Z}_p^*$ are quadratic residues modulo p.

Proof. p even: $|\mathbb{Z}_2^*| = 1$

p odd: $\left|\mathbb{Z}_p^*\right| = p - 1$ is even.

$$\mathbb{Z}_p^* = \langle g \rangle = \left\{g^0, g^1, \ldots, g^{p-2}\right\}$$
$$A := \left\{g^0, g^2, g^4, \ldots, g^{p-3}\right\}, |A| = \frac{p-1}{2}$$

$x \in A$, i.e. $\exists i \in \mathbb{N}_0 : x \equiv g^{2i} \mod p \overset{a)}{\Rightarrow} x$ is a quadratic residue modulo p

$x \in \mathbb{Z}_p^* \setminus A$ and assume x is quadratic residue modulo $p \overset{a)}{\Rightarrow} \exists i \in \mathbb{N}_0 : x \equiv g^{2i} \mod p$

$\Rightarrow x \in A$, a contradiction. (Note: $2i \mod (p-1)$ is even)

□

c) $a \cdot b$ is a quadratic residue modulo $p \Leftrightarrow \begin{cases} a, b \text{ are quadratic residues modulo } p \\ a, b \text{ are quadratic nonresidues modulo } p \end{cases}$

Proof. $p = 2$: trivial, as $\left|\mathbb{Z}_p^*\right| = 1$.

$p > 2$: "$\Rightarrow$": Let $a \equiv g^k \mod p$, $b \equiv g^l \mod p$. With $a \cdot b$ quadratic residue modulo p:

$$\begin{aligned} &\exists i \in \mathbb{N}_0 : a \cdot b \equiv g^{2i} \mod p \\ &\Rightarrow a \cdot b \equiv g^{k+l} \equiv g^{2i} \mod p \\ &\Rightarrow k + l \equiv 2i \mod (p-1) \\ &\text{(Note: } p-1 \text{ even } \Rightarrow k+l \mod (p-1) \text{ even)} \\ &\Rightarrow \begin{cases} k, l \text{ even} & \overset{a)}{\Rightarrow} a, b \text{ are quadratic residues} \\ k, l \text{ odd} & \overset{a)}{\Rightarrow} a, b \text{ are quadratic nonresidues} \end{cases} \end{aligned}$$

"$\Leftarrow$": a, b are quadratic residues modulo p. Then

$$a \cdot b \equiv g^{2k} \cdot g^{2l} \equiv g^{2(k+l)} \mod p \overset{a)}{\Rightarrow} a \cdot b \text{ quadratic residue modulo } p\,.$$

a, b are quadratic nonresidues modulo p. Then

$$a \cdot b \equiv g^{2k+1} \cdot g^{2l+1} \equiv g^{2(k+l+1)} \mod p \overset{a)}{\Rightarrow} a \cdot b \text{ quadratic residue modulo } p\,.$$

□

Solution of Problem 2

a) Apply the encryption function.

$$\begin{aligned} n &= p \cdot q = 199 \cdot 211 = 41989\,, \\ c &= e_K(32767) = m \cdot (m+B) \mod n \\ &= 32767 \cdot (32767 + 1357) \mod 41989 \\ &\equiv 16027 \mod 41989 \end{aligned}$$

b) Start with the encryption function and solve for m.

$$\begin{aligned} c &\equiv m^2 + B \cdot m \mod n \\ c + \left(\frac{B}{2}\right)^2 &\equiv m^2 + B \cdot m + \left(\frac{B}{2}\right)^2 \mod n \\ c + \left(\frac{B}{2}\right)^2 &\equiv \left(m + \frac{B}{2}\right)^2 \mod n \end{aligned}$$

Using the Extended Euclidean Algorithm, the multiplicative inverse of 2 modulo n is calculated as $2^{-1} \equiv 20995 \mod 41989$. With

$$\begin{aligned} \tilde{c} &:= c + \left(\frac{B}{2}\right)^2 \mod n \\ &\equiv 16027 + (1357 \cdot 20995)^2 \mod n \\ &\equiv 4013 \mod n\,, \end{aligned}$$

and

$$\begin{aligned} \tilde{m} &:= m + \frac{B}{2} \mod n \\ &\equiv m + 1357 \cdot 20995 \mod n \\ &\equiv m + 21673 \mod n\,, \end{aligned}$$

we can conclude

$$\begin{aligned} \tilde{c} &\equiv \tilde{m}^2 \mod n \\ 4013 &\equiv \tilde{m}^2 \mod n\,. \end{aligned}$$

This form is the standard Rabin Cryptosystem. In order to find the square root modulo n, we use Proposition 9.4. First, find

$$1 = \underbrace{s \cdot p}_{=:b} + \underbrace{t \cdot q}_{=:a}$$

using the Extended Euclidean Algorithm.

$$\begin{aligned}
211 &= 1 \cdot 199 + 12 \\
199 &= 16 \cdot 12 + 7 \\
12 &= 1 \cdot 7 + 5 \\
7 &= 1 \cdot 5 + 2 \\
5 &= 2 \cdot 2 + 1 \\
\Rightarrow 1 &= 5 - 2 \cdot 2 \\
&= 5 - 2 \cdot (7 - 1 \cdot 5) = 3 \cdot 5 - 2 \cdot 7 \\
&= 3 \cdot (12 - 1 \cdot 7) - 2 \cdot 7 = 3 \cdot 12 - 5 \cdot 7 \\
&= 3 \cdot 12 - 5 \cdot (199 - 16 \cdot 12) = 83 \cdot 12 - 5 \cdot 199 \\
&= 83 \cdot (211 - 1 \cdot 199) - 5 \cdot 199 = 83 \cdot 211 - 88 \cdot 199 \\
\Rightarrow b &= -88 \cdot 199 = -17512 \\
a &= 83 \cdot 211 = 17513
\end{aligned}$$

Next, we calculate the square roots modulo p and q (this is Proposion 9.3).

$$\begin{aligned}
x^2 &\equiv 4013 \equiv 33 \mod p \\
\Rightarrow x_1 &= 33^{\frac{p+1}{4}} = 33^{50} \equiv 86 \mod 199 \\
x_2 &= -x_1 \equiv 113 \mod 199\,, \\
y^2 &\equiv 4013 \equiv 4 \mod q \\
\Rightarrow y_1 &= 4^{\frac{q+1}{4}} = 4^{53} \equiv 209 \mod 211 \\
y_2 &= -y_1 = 2 \mod 211
\end{aligned}$$

Then, $f_{x_i,y_j} = ax_i + by_j$ are solutions to $f^2 = 4013 \mod n$.

$$\begin{aligned}
f_{x_1,y_1} &= a \cdot x_1 + b \cdot y_1 \mod n \\
&\equiv 17513 \cdot 86 - 17512 \cdot 209 \mod 41989 \\
&\equiv 36503 - 6965 \mod 41989 \\
&\equiv 29538 \mod 41989 \\
f_{x_1,y_2} &= 17513 \cdot 86 - 17512 \cdot 2 \mod 41989 \\
&\equiv 36503 - 35024 \mod 41989 \\
&\equiv 1479 \mod 41989 \\
f_{x_2,y_1} &= 17513 \cdot 113 - 17512 \cdot 209 \mod 41989 \\
&\equiv 5486 - 6965 \mod 41989 \\
&\equiv 40510 \equiv -f_{x_1,y_2} \mod 41989 \\
f_{x_2,y_2} &= 17513 \cdot 113 - 17512 \cdot 2 \mod 41989 \\
&\equiv 5486 - 35024 \mod 41989 \\
&\equiv 12451 \equiv -f_{x_1,y_1} \mod 41989
\end{aligned}$$

With

$$\begin{aligned} \tilde{m}^2 &\equiv \tilde{c} \mod n \\ \tilde{m} &\equiv f_{x_i,y_j} \mod n \\ m_{x_i,y_j} + 21673 &\equiv f_{x_i,y_j} \mod n \\ m_{x_i,y_j} &\equiv f_{x_i,y_j} - 21673 \mod n \end{aligned}$$

the four possible messages can now be calculated.

$$\begin{aligned} m_{x_1,y_1} &= 29538 - 21673 \equiv 7865 \mod n \\ m_{x_1,y_2} &= 1479 - 21673 \equiv 21795 \mod n \\ m_{x_2,y_1} &= 40510 - 21673 \equiv 18837 \mod n \\ m_{x_2,y_2} &= 12451 - 21673 \equiv 32767 \mod n \end{aligned}$$

Message m_{x_2,y_2} is the original one, but, knowing only the cryptogram and the private key, this message cannot be identified as the original one.

Solution of Problem 3

Decipher $m = \sqrt{c} \mod n$ with $c = 1935$.

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

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

- Compute the resulting square root modulo n. $m_{i,j} = ax_{p,i} + bx_{q,j}$ solves $m_{i,j}^2 \equiv c \mod n$ 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.

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

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

$$
\begin{aligned}
m_{1,1} \equiv ax_{p,1} + bx_{q,1} \equiv 107 \mod n \Rightarrow 0000001101011,\\
m_{1,2} \equiv ax_{p,1} + bx_{q,2} \equiv 1313 \mod n \Rightarrow 0010100100001,\\
m_{2,1} \equiv ax_{p,2} + bx_{q,1} \equiv 3444 \mod n \Rightarrow 0110101110100,\\
m_{2,2} \equiv ax_{p,2} + bx_{q,2} \equiv 4650 \mod n \Rightarrow 1001000101010.
\end{aligned}
$$

The correct solution is m_1, by the agreement given in the exercise.