Advanced Methods of Cryptography

Chair for Theoretical Information Technology

RWTH AACHEN UNIVERSITY

Prof. Dr. Rudolf Mathar, Dr. Michael Reyer, Jose Leon, Qinwei He

Exercise 2
- Proposed Solution -

Friday, November 3, 2017

Solution of Problem 1

”$\Rightarrow$” c is QR modulo p with Definition 9.1 it follows

$$\exists\, x \in \mathbb{Z}_p^* : x^2 \equiv c \mod p \Rightarrow c^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \mod p,$$

where the last congruence follows from Fermat’s Theorem.

”$\Leftarrow$” $c^{\frac{p-1}{2}} \equiv 1 \mod p \Rightarrow c \in \mathbb{Z}_p^*$ as c has an inverse modulo p.
Let y be a primitive element (PE), i.e., y is a generator of $\mathbb{Z}_p^*$. Note that there exists a primitive element with respect to Theorem 7.2 a).

$$\begin{aligned}
&\Rightarrow \quad \exists\, j : c \equiv y^j \mod p \\
&\Rightarrow \quad c^{\frac{p-1}{2}} \equiv (y^j)^{\frac{p-1}{2}} \equiv 1 \mod p \\
&\Rightarrow \quad p-1 \mid j(p-1)/2 \Rightarrow j \text{ must be even} \\
&\Rightarrow \quad \exists\, x \in \mathbb{Z}_p^* : x \equiv y^{\frac{j}{2}} \mod p \\
&\Rightarrow \quad x^2 \equiv y^j \equiv c \mod p \\
&\Rightarrow \quad c \text{ is QR modulo } p
\end{aligned}$$

Solution of Problem 2

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.

$$\mathbb{Z}_p^* = \langle g \rangle = \left\{g^0, g^1, \ldots, g^{p-2}\right\}$$
$$A := \left\{g^0, g^2, g^4, \ldots, g^{p-3}\right\}, |A| = \frac{p-1}{2}$$
$$x \in A, \text{i.e. } \exists i \in \mathbb{N}_0 : x \equiv g^{2i} \mod p \overset{a)}{\Rightarrow} x \text{ is a quadratic residue modulo } p$$
$$x \in \mathbb{Z}_p^* \setminus A \text{ and assume } x \text{ is quadratic residue modulo } p \overset{a)}{\Rightarrow} \exists i \in \mathbb{N}_0 : x \equiv g^{2i} \mod p$$
$$\Rightarrow x \in A, \text{a contradiction. (Note: } 2i \mod (p-1) \text{ is even)}$$

□

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:

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

"$\Leftarrow$": 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 3

$$n = p \cdot q = 31 \cdot 79 = 2449$$

a) Apply Algorithm 7 *(Finding pseudo-squares modulo $n = pq$).*

1. $a = 10 \rightarrow \left(\frac{a}{p}\right) = 1$
   $a = 11 \rightarrow \left(\frac{a}{p}\right) = -1$ ✓
2. $b = 17 \rightarrow \left(\frac{b}{q}\right) = -1$ ✓
3. Compute $y \in \{0, 1, \ldots, n-1\}$ with

$$\begin{aligned} y &\equiv a \mod p\,, \\ y &\equiv b \mod q\,, \end{aligned}$$

by applying the Chinese remainder theorem to solve the system of congruences.

$$\begin{gathered} m_1 = p,\ \ m_2 = q,\ \ a_1 = a,\ \ a_2 = b,\ \ x = y, \\ M = m_1 \cdot m_2 = n = p \cdot q,\ \ M_1 = m_2 = q,\ \ M_2 = m_1 = p, \\ y_1 = M_1^{-1} = q^{-1} = 11 \mod m_1,\ \ y_2 = M_2^{-1} = p^{-1} = 51 \mod m_2, \\ \Rightarrow y = a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 = a \cdot q \cdot 11 + b \cdot p \cdot 51 \\ = 11 \cdot 79 \cdot 11 + 17 \cdot 31 \cdot 51 \equiv 2150 \mod n \end{gathered}$$

b)

$$\begin{aligned} \left(\frac{1418}{31}\right) &= -1 \quad \Rightarrow m_1 = 1 \\ \left(\frac{2150}{31}\right) &= -1 \quad \Rightarrow m_2 = 1 \\ \left(\frac{2153}{31}\right) &= 1 \quad\ \ \Rightarrow m_3 = 0 \\ &\Rightarrow m = (1, 1, 0) \end{aligned}$$

Solution of Problem 4

a) From the requirement of a weak key, $c \overset{!}{=} m$, it follows:

$$c = \sum\nolimits_{i=1}^{n} m_i \beta_i \overset{(i)}{=} \sum\nolimits_{i=1}^{n} m_i 2^{i-1} = m$$

with (i) $\beta_i = r w_i \mod q \Rightarrow \beta_i = w_i = 2^{i-1} \mod q = 2^{i-1}$ with $r = 1$, since the modulus is larger than each w_i with $q > 2^{n-1} + 2^{n-2} + \cdots + 2^1 + 2^0$.

b) Proof by contradiction:

$$\begin{aligned} \beta_i &\overset{!}{=} \beta_j \mod q \\ \Rightarrow r w_i &\equiv r w_j \mod q \quad //\ r^{-1} \mod q \text{ exists, as } \gcd(r, q) = 1. \\ \Rightarrow w_i &\equiv w_j \mod q \end{aligned}$$

But w_i, w_j must be different for $i \neq j$ as $w_{k+1} > \sum_{i=1}^{k} w_i$ by assumption. ↯

Thus, β_i, β_j are pair-wise different for $i \neq j$.

c) Compute the difference of the ciphertexts:

$$\begin{aligned}|c - c'| &= |\textstyle\sum_{i=1}^{n} m_i\beta_i - \sum_{k=1}^{n} m'_k\beta_k| \\ &= |(m_j - m'_j)\beta_j| \\ &= |m_j - m'_j|\beta_j \\ &= \beta_j, \quad \text{with condition b)}\end{aligned}$$

The single *bit error* is at position j. All other $\beta_i \neq \beta_j$ cancel out and $|m_j - m'_j| = 1$. This single bit error can be read from the known public $\boldsymbol{\beta}$.

d) With the given $w_4 = 63$, we can compute the other four w_i:

$$\begin{aligned}w_5 &= 2 \cdot 63 + 1 = 127 \\ q &= 257 > \textstyle\sum_{i=1}^{5} w_i = 243 \\ w_3 &= (63 - 1)\tfrac{1}{2} = 31 \\ w_2 &= (31 - 1)\tfrac{1}{2} = 15 \\ w_1 &= (15 - 1)\tfrac{1}{2} = 7\end{aligned}$$

Then, with $r = \beta_1 w_1^{-1} \mod q$ and using the hint for the inverse of w_3, we get:

$$r = \beta_3 w_3^{-1} \mod q = 230 \cdot 199 \mod 257 = 24$$

This provides $(\boldsymbol{w}, q, r) = ((7, 15, 31, 63, 127), 257, 24)$.

e) $d = cr^{-1} \mod q$

From the EEA we obtain $r^{-1} \equiv 75 \mod 257$.

Then, $d = 846 \cdot 75 \mod 257 \equiv 228$.

Now we can decode the bits of the message as follows:

$$\begin{aligned}d = 228 &> w_5 \Rightarrow m_5 = 1 \\ 228 - 127 = 101 &> w_4 \Rightarrow m_4 = 1 \\ 101 - 63 = 38 &> w_3 \Rightarrow m_3 = 1 \\ 38 - 31 = 7 &= w_1 \Rightarrow m_2 = 0, m_1 = 1\end{aligned}$$

The resulting plaintext message is:

$$m = m_1 2^0 + m_2 2^1 + m_3 2^2 + m_4 2^3 + m_5 2^4 = 1 + 4 + 8 + 16 = 29$$