Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Qinwei He

Exercise 12
- Proposed Solution -

Friday, July 21, 2017

Solution of Problem 1

It is to prove that

$$a^x \equiv a^y \mod n \Leftrightarrow x \equiv y \mod \operatorname{ord}_n(a)$$

with $x, y \in \mathbb{Z}$, $a \in \mathbb{Z}_n^*$, $a \neq 1$, and $\operatorname{ord}_n(a) = k$.

"$\Rightarrow$" Let $a^x \equiv a^y \mod n \Rightarrow a^{x-y} \equiv 1 \mod n$ and $a^k \equiv 1 \mod n \Rightarrow \operatorname{ord}_n(a) = k$.
Recall: $\operatorname{ord}_n(a) = \min\{k \in \{1, \dots, \varphi(n)\} \mid a^k \equiv 1 \mod n\}\}$.

$$\begin{aligned} &k \mid (x-y) \\ \Rightarrow\ &x \equiv y \mod k \\ \Rightarrow\ &x \equiv y \mod \operatorname{ord}_n(a). \end{aligned}$$

"$\Leftarrow$" Let $x \equiv y \mod \operatorname{ord}_n(a) \Rightarrow k \mid (x-y) \Rightarrow x - y = kl, l \in \mathbb{Z}$.

$$\begin{aligned} &\Rightarrow a^{x-y} \equiv a^{kl} \equiv (a^k)^l \equiv 1^l \equiv 1 \mod n \\ &\Rightarrow a^{x-y} \equiv 1 \mod n \Rightarrow a^x \equiv a^y \mod n. \end{aligned}$$

Solution of Problem 2

a) The parameters of the given ElGamal cryptosystem are $p = 3571$, $a = 2$, $y = 2905$.

1) Check whether p is prime: Yes, use the MRPT in general or the exaustive search in this simple case. Since $\sqrt{3571} > 59$ it suffices to perform trial division for all primes less or equal to 59.
2) Check whether a is a primitive element modulo p:

$$a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod p, \ \forall i = 1, \dots, k,$$

with the prime factorization $p - 1 = \prod_{i=1}^{k} p_i^{t_i}$ as given in Proposition 7.5.
The prime factorization yields: $3570 = 2{\cdot}1785 = 2{\cdot}5{\cdot}357 = 2{\cdot}3{\cdot}5{\cdot}7{\cdot}17 = p_1p_2p_3p_4p_5$.

$$\begin{aligned} p_1 = 2: &\quad 2^{1785} \pmod p \equiv -1, \\ p_2 = 3: &\quad 2^{1190} \pmod p \equiv 3467 \\ p_3 = 5: &\quad 2^{714} \pmod p \equiv 2910, \\ p_4 = 7: &\quad 2^{510} \pmod p \equiv 2767, \\ p_5 = 17: &\quad 2^{210} \pmod p \equiv 1847. \end{aligned}$$

a is a primitive element modulo p.

b) The first part of both ciphertexts is equal. Bob has chosen the same session key twice.

c) One message $m_1 = 567$ is given. We perform a known-plaintext attack.

Let $\boldsymbol{c}_1 = (c_1, c_2)$ and $\boldsymbol{c}_2 = (c_3, c_4)$.

The session key k is the same, since the ciphertexts c_1 and c_3 are congruent:

$$c_1 \equiv c_3 \equiv a^k \pmod{p}.$$

With $y = a^x \pmod{p}$, K is computed by:

$$K = y^k \equiv a^{xk} \mod p,$$

in both cases.

For the known m_1, c_2 and p we can compute K^{-1}:

$$\begin{aligned} m_1 &\equiv K^{-1} c_2 \pmod{p} \\ \Leftrightarrow K^{-1} &\equiv c_2^{-1} m_1 \pmod{p}, \end{aligned}$$

and finally reveal m_2:

$$\begin{aligned} m_2 &\equiv c_4 K^{-1} \pmod{p} \\ &\equiv c_4 c_2^{-1} m_1 \pmod{p}. \end{aligned}$$

For the given values, we have:

$$\begin{aligned} c_2^{-1} &\equiv 347 \pmod{3571}, \\ m_2 &\equiv 1393 \cdot 347 \cdot 567 \pmod{3571} \\ &\equiv 678 \pmod{3571}. \end{aligned}$$

Solution of Problem 3

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

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

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.

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

□

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 4

"$\Rightarrow$" 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).

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