

Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Markus Rothe

Exercise 12

- Proposed Solution -

Thursday, July 13, 2017

Solution of Problem 1

It is to prove that

$$a^x \equiv a^y \pmod{n} \Leftrightarrow x \equiv y \pmod{\text{ord}_n(a)}$$

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

“ \Rightarrow ” Let $a^x \equiv a^y \pmod{n} \Rightarrow a^{x-y} \equiv 1 \pmod{n}$ and $a^k \equiv 1 \pmod{n} \Rightarrow \text{ord}_n(a) = k$.

Recall: $\text{ord}_n(a) = \min\{k \in \{1, \dots, \varphi(n) \mid a^k \equiv 1 \pmod{n}\}\}$.

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

“ \Leftarrow ” Let $x \equiv y \pmod{\text{ord}_n(a)} \Rightarrow k \mid (x - y) \Rightarrow x - y = kl, l \in \mathbb{Z}$.

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

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 exhaustive 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 :

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

with the prime factorization $p - 1 = \prod_{i=1}^k p_i^{t_i}$ as given in Proposition 7.5.

The prime factorization yields: $3570 = 2 \cdot 1785 = 2 \cdot 5 \cdot 357 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 = p_1 p_2 p_3 p_4 p_5$.

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

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

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:

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

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 :

$$\begin{aligned} m_2 &\equiv c_4K^{-1} \pmod{p} \\ &\equiv c_4c_2^{-1}m_1 \pmod{p}. \end{aligned}$$

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 $p \Leftrightarrow \exists i \in \mathbb{N}_0 : a \equiv g^{2i} \pmod{p}$

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

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

“ \Leftarrow ”: $\exists i \in \mathbb{N}_0 : a \equiv g^{2i} \pmod{p}$. With $a \equiv (g^i)^2 \pmod{p}$, a is a quadratic residue modulo p . \square

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

$$\mathbb{Z}_p^* = \langle g \rangle = \{g^0, g^1, \dots, g^{p-2}\}$$

$$A := \{g^0, g^2, g^4, \dots, g^{p-3}\}, |A| = \frac{p-1}{2}$$

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

$x \in \mathbb{Z}_p^* \setminus A$ and assume x is quadratic residue modulo $p \stackrel{a)}{\Rightarrow} \exists i \in \mathbb{N}_0 : x \equiv g^{2i} \pmod{p}$
 $\Rightarrow x \in A$, a contradiction. (Note: $2i \pmod{p-1}$ 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 $|\mathbb{Z}_p^*| = 1$.

$p > 2$: “ \Rightarrow ”: Let $a \equiv g^k \pmod{p}$, $b \equiv g^l \pmod{p}$. With $a \cdot b$ quadratic residue modulo p :

$$\exists i \in \mathbb{N}_0 : a \cdot b \equiv g^{2i} \pmod{p}$$

$$\Rightarrow a \cdot b \equiv g^{k+l} \equiv g^{2i} \pmod{p}$$

$$\Rightarrow k + l \equiv 2i \pmod{p-1}$$

(Note: $p-1$ even $\Rightarrow k+l \pmod{p-1}$ even)

$$\Rightarrow \begin{cases} k, l \text{ even} & \stackrel{a)}{\Rightarrow} a, b \text{ are quadratic residues} \\ k, l \text{ odd} & \stackrel{a)}{\Rightarrow} a, b \text{ are quadratic nonresidues} \end{cases}$$

“ \Leftarrow ”: a, b are quadratic residues modulo p . Then

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

a, b are quadratic nonresidues modulo p . Then

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

□

Solution of Problem 4

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

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

where the last congruence follows from Fermat’s Theorem.

" \Leftarrow " $c^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Rightarrow c \in \mathbb{Z}_p^*$ 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).

$$\Rightarrow \exists j : c \equiv y^j \pmod{p}$$

$$\Rightarrow c^{\frac{p-1}{2}} \equiv (y^j)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

$$\Rightarrow p-1 \mid j(p-1)/2 \Rightarrow j \text{ must be even}$$

$$\Rightarrow \exists x \in \mathbb{Z}_p^* : x \equiv y^{\frac{j}{2}} \pmod{p}$$

$$\Rightarrow x^2 \equiv y^j \equiv c \pmod{p}$$

$$\Rightarrow c \text{ is QR modulo } p$$