Prof. Dr. Rudolf Mathar, Dr. Michael Reyer

Tutorial 11
- Proposed Solution -

Friday, July 5, 2019

Solution of Problem 1

It is to prove that

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

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

"$\Rightarrow$" Let $a^x \equiv a^y \pmod{n} \Rightarrow a^{x-y} \equiv 1 \pmod{n}$.
Assume $x \not\equiv y \pmod{l} \Leftrightarrow \exists\, 1 \leq r < l, m \in \mathbb{N} : x - y = l\, m + r$, and hence,

$$a^{x-y} = a^{l\,m+r} = (a^l)^m\, a^r \equiv a^r \not\equiv 1 \pmod{n}.$$

Thus, $x \equiv y \pmod{l}$.

"$\Leftarrow$" Let $x \equiv y \pmod{\operatorname{ord}_n(a)} \Rightarrow \exists\, m \in \mathbb{Z} : x - y = l\, m$.

$$\Rightarrow a^{x-y} \equiv a^{lm} \equiv (a^l)^m \equiv 1^m \equiv 1 \pmod{n}$$
$$\Rightarrow a^{x-y} \equiv 1 \pmod{n} \Rightarrow a^x \equiv a^y \pmod{n}.$$

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 $\sqrt{3571} < 60$ it suffices to perform trial division for all primes less or equal to 59.

2) Check whether a is a primitive element modulo p:

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

with the prime factorization $p - 1 = \prod_{i=1}^{k} p_i^{t_i}$ as given in Proposition 7.5.
The prime factorization yields: $3570 = 2 \cdot 1785 = 2 \cdot 5 \cdot 357 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 = p_1 p_2 p_3 p_4 p_5$.

I need to calculate some powers of 2 up to 1785. For preparation calculate

$$\begin{aligned}
2^{2^0} \mod p &= 2^1 \mod p = 2\\
2^{2^1} \mod p &= 2^2 \mod p = 4\\
2^{2^2} \mod p &= 2^4 \mod p = 16\\
2^{2^3} \mod p &= 2^8 \mod p = 256\\
2^{2^4} \mod p &= 2^{16} \mod p = 1258\\
2^{2^5} \mod p &= 2^{32} \mod p = 611\\
2^{2^6} \mod p &= 2^{64} \mod p = 1937\\
2^{2^7} \mod p &= 2^{128} \mod p = 2419\\
2^{2^8} \mod p &= 2^{256} \mod p = 2263\\
2^{2^9} \mod p &= 2^{512} \mod p = 355\\
2^{2^{10}} \mod p &= 2^{1024} \mod p = 1040\\
2^{82} \mod p &= 2^{64}2^{16}2^2 \mod p = 1725
\end{aligned}$$

and now

$$\begin{aligned}
p_5 = 17: &\ 2^{210} \mod p = 2^{128}2^{64}2^{16}2^2 \mod p = 2419 \cdot 2^{82} \mod p = 1847,\\
p_4 = 7: &\ 2^{510} \mod p = (2^{210})^2 2^{82} 2^8 \mod p = 22767,\\
p_3 = 5: &\ 2^{714} \mod p = 2^{510}(2^{82})^2 2^{32} 2^8 = 2910,\\
p_2 = 3: &\ 2^{1190} \mod p = 2^{1024}2^{128}2^{32}2^4 2^2 \mod p = 3467\\
p_1 = 2: &\ 2^{1785} \mod p = -1.
\end{aligned}$$

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 $y = a^x \mod p$, 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:

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

a_n	b_n	f_n	r_n	c'_n	d_n
			3571	1	0
			2192	0	1
3571	2192	1	1379	1	-1
2192	1379	1	813	-1	2
1379	813	1	566	2	-3
813	566	1	247	-3	5
566	247	2	72	8	-13
247	72	3	31	-27	44
72	31	2	10	62	-101
31	10	3	1	-213	347

We need to calculate c_2^{-1} by the EEA. And finally get,

$$\gcd(p, c_2) = \gcd(3571, 2192) = 1 = -213 \cdot 3571 + 347 \cdot 2192.$$

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

Let p be prime, g a 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 $a \equiv \left(g^i\right)^2 \pmod{p}$, a is a quadratic residue modulo p. □

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.

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

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

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

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

□

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

Proof. $p = 2$: trivial, as $\left|\mathbb{Z}_p^*\right| = 1$. $p > 2$: "$\Rightarrow$": Let $a \equiv g^k \pmod p$, $b \equiv g^l \pmod p$. With $a \cdot b$ quadratic residue modulo p:

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

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

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

a, b are quadratic non-residues modulo p. Then

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

□

Solution of Problem 4

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

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

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).

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