Tutorial 11

P1/

$a^t \equiv a^\gamma \pmod n \Leftrightarrow t \equiv \gamma \pmod \ell$

with $t, \gamma \in \mathbb{Z}$, $a \in \mathbb{Z}_n^*$, $a \neq 1$, $\ell = \text{ord}_n(a)$

„$\Rightarrow$" $a^t \equiv a^\gamma \pmod n \Rightarrow a^{t-\gamma} \equiv 1 \pmod n$

Assume $t \not\equiv \gamma \pmod \ell \Leftrightarrow \exists\, 1 \leq r < \ell, m \in \mathbb{N} : t - \gamma = \ell \cdot m + r$

$\Rightarrow a^{t-\gamma} = a^{\ell \cdot m + r} = \underbrace{(a^\ell)^m}_{\equiv 1} \cdot a^r \equiv 1^m \cdot a^r \equiv a^r \not\equiv 1 \pmod n$ ↯

$\Rightarrow t \equiv \gamma \pmod \ell$

„$\Leftarrow$" Let $t \equiv \gamma \pmod \ell \Rightarrow \exists\, m \in \mathbb{N} : t - \gamma = \ell \cdot m$

$\Rightarrow a^{t-\gamma} \equiv a^{\ell m} \equiv \underbrace{(a^\ell)^m}_{\equiv 1} \equiv 1 \pmod n$

$\Rightarrow a^t \equiv a^\gamma \pmod n$ ✓

P2/ El Gamal cryptosystem $p = 3571$, $a = 2$, $y = 2905$

a) 1) Check whether p is prime.

$\lceil \sqrt{p} \rceil = \sqrt{3571} < 60$

$\Rightarrow$ just need to check if p is divisible by primes ≤ 59

In general: apply, e.g., MRPT

2) Check whether a is PE following Prop 7.5, check that

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

$p - 1 = \prod_{i=1}^{k} p_i^{t_i}$ is the prime factorization of $p-1$.

$3570 = 2 \cdot 1785 = 2 \cdot 5 \cdot 357 = 2 \cdot 3 \cdot 5 \cdot 119 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 17$
$= p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5$

Precalculations:

$2^{2^n} \bmod p \qquad n = 0, \dots, 10$

$\vdots$

$2^{2^{10}} = 2^{1024}$

$2^{82} = 2^{64} \cdot 2^{16} \cdot 2^2 \equiv 1725 \pmod p$

$p_5 = 17 : 2^{210} = 2^{128} \cdot 2^{82} \equiv 1847 \pmod p \not\equiv 1$

$p_4 = 7 : 2^{510} = (2^{210})^2 \cdot 2^{82} \cdot 2^8 \equiv 2267 \not\equiv 1 \pmod p$

$p_3 = 5 : 2^{714} = 2^{510} (2^{82})^2 \cdot 2^{32} \cdot 2^8 \equiv 2910 \not\equiv 1 \pmod p$

$p_2 = 3 : 2^{1190} = 2^{1024} 2^{128} 2^{32} 2^4 2^2 \equiv 3487 \not\equiv 1 \pmod p$

$p_1 = 2 : 2^{1785} \bmod p = -1 \Rightarrow a$ is PE

b) $\underline{c}_1 = (1537, 2192)$; $\underline{c}_2 = (1537, 1393)$

In El Gamal: $k \in \{2, \dots, p-2\}$

$c_1 = a^k \bmod p$

Bob has chosen the same session key k twice.

c) $m_1 = 567$; $\underline{c}_1 = (c_1, c_2)$; $\underline{c}_2 = (c_3, c_4)$

Same session key

$c_1 \equiv c_3 \equiv a^k \pmod p$

$\gamma = a^t \bmod p$, K is computed:

$K \equiv \gamma^k \equiv a^{tk} \pmod p$ in both cases ✓

For the known c_2, m_1, and p we may compute k^{-1}

$m_1 \equiv k^{-1} c_2 \pmod p$

$\Leftrightarrow k^{-1} \equiv m_1 \cdot c_2^{-1} \pmod p$

And finally for m_2

$$m_2 \equiv k^{-1} c_4 \equiv m_1 \cdot c_2^{-1} \cdot c_4 \pmod p$$

$$\equiv 567 \cdot 347 \cdot 1393 = 678 \pmod{3571}$$

c_2^{-1} is calculated by EEA: $\gcd(p, c_2)$

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

P3| p prime, g a primitive element mod p $a, b \in \mathbb{Z}_p^*$

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

"$\Rightarrow$" a is QR mod p, i.e., $\exists k \in \mathbb{Z}_p^* : k^2 \equiv a \pmod p$.
g is a PE, i.e. $\exists \ell \in \mathbb{N}_0 \quad k \equiv g^\ell \pmod p$. Then,

$k^2 \equiv g^{2\ell} \equiv a \pmod p$ ✓

"$\Leftarrow$" $\exists i \in \mathbb{N}_0 : a \equiv g^{2i} \pmod p$. with $a \equiv (g^i)^2 \pmod p$
$\Rightarrow$ a is a QR mod p

b) If p is odd : $|\mathbb{Z}_p^*| = p-1$ is even

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

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

$t \in A$ i.e., $\exists i \in \mathbb{N}_0 : t = g^{2i} \bmod p \overset{a)}{\Rightarrow}$ is a QR mod p

$t \in \mathbb{Z}_p^* \setminus A \wedge t$ is QR mod p $\Rightarrow \exists i \in \mathbb{N}_0 : t \equiv g^{2i} \pmod p$

$\Rightarrow t \in A$, a contradiction

c) a·b is QR mod p $\Leftarrow$ { a, b are QR mod p ; a, b are QNR mod p }

"$\Rightarrow$" p = 2 ✓

$p > 2 \Rightarrow$ Let $a \equiv g^k \pmod p$ $b \equiv g^\ell \pmod p$

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

$\Rightarrow a \cdot b \equiv g^{k+\ell} \equiv g^{2i}$

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

$\Rightarrow$ { k, ℓ even $\Rightarrow$ a, b are QR ; k, ℓ odd $\Rightarrow$ a, b are QNR }

„⇐" a, b are QR mod p

$\Rightarrow a \cdot b \equiv g^{2k} \cdot g^{2\ell} \equiv g^{2(k+\ell)} \pmod{p} \Rightarrow a \cdot b$ is QR mod p

a, b are QNR mod p

$\Rightarrow a \cdot b \equiv g^{2k+1} \cdot g^{2\ell+1} \equiv g^{2(k+\ell+1)} \pmod{p} \Rightarrow a \cdot b$ is QR mod p