

Week 7

Topics : Generalised ElGamal
Public Key Cryptosystem

Chinese Remainder
Theorem

Rabin cryptosystem

Legendre and Jacobi
symbol

Jacobi Symbol (cont.)

• The discrete logarithm problem in (G, \circ) :

- **Problem Instance:** $I = (G, \alpha, \beta)$, where G is a finite group with group operation \circ , $\alpha \in G$ and $\beta \in H$, where $H = \{\alpha^i : i \geq 0\}$ is a subgroup of G generated by α .
- **Objective:** Find the unique integer a such that $0 \leq a \leq |H| - 1$ and $\alpha^a = \beta$, where the notation α^a means $\alpha \circ \alpha \circ \dots \circ \alpha$ (a times).

• Generalized ElGamal Public-key Cryptosystem:

- Let G be a finite group with group operation \circ , and let $H = \{\alpha^i : i \geq 0\}$ be a subgroup of G where discrete log problem is intractable and $\alpha \in H$.
- Let $P = G$, $C = G \times G$ and define $K = \{(G, \alpha, a, \beta) : \beta = \alpha^a\}$
- The values α and β are public and a is secret.
- $K = (G, \alpha, a, \beta)$, for random number $k \in \mathbb{Z}_{|H|}$ define $e_K(x, k) = (y_1, y_2)$ where $y_1 = \alpha^k$ and $y_2 = x \circ \beta^k$.
- For a ciphertext $y = (y_1, y_2)$, define $d_K(y_1, y_2) = y_2 \circ (y_1^a)^{-1}$.

• Chinese Remainder Theorem (CRT):

Suppose m_1, m_2, \dots, m_r are pairwise relatively prime, then the following system of simultaneous congruences

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_r \pmod{m_r}$$

has unique solution modulo $M = m_1 m_2 \dots m_r$, which is given by

$$x = \sum_{i=1}^r a_i M_i y_i \pmod{M},$$

where $M_i = M/m_i$ and $y_i = M_i^{-1} \pmod{m_i}$ for $1 \leq i \leq r$.

Example:
Consider the following system of simultaneous congruences

$$x \equiv 5 \pmod{7}$$

$$x \equiv 3 \pmod{11}$$

$$x \equiv 10 \pmod{13}$$

$$\Rightarrow a_1 = 5, a_2 = 3, a_3 = 10, m_1 = 7, \\ m_2 = 11, m_3 = 13, M_1 = 143, M_2 = 91, \\ M_3 = 77, M = 1001$$

Use extended Euclid's algorithm to find

$$y_1 = M_1^{-1} \pmod{m_1} = 5$$

$$y_2 = M_2^{-1} \pmod{m_2} = 4$$

$$y_3 = M_3^{-1} \pmod{m_3} = 12$$

Therefore the unique solution is

$$x = (715 \times 5 + 364 \times 3 + 924 \times 10) \pmod{M} \\ = 13907 \pmod{1001} \\ = 894.$$

● Quadratic Residue modulo p :

Let p be a prime and a be an integer. Then a is called a quadratic residue modulo prime p iff $y^2 \equiv a \pmod{p}$ has a solution in \mathbb{Z}_p .

● Example : $p = 11$, \mathbb{Z}_{11}

$$(\pm 1)^2 = 1, (\pm 2)^2 = 4, (\pm 3)^2 = 9$$

$$(\pm 4)^2 = 5, (\pm 5)^2 = 3, (\pm 6)^2 = 3$$

$$(\pm 7)^2 = 5, (\pm 8)^2 = 9, (\pm 9)^2 = 4$$

$$(\pm 10)^2 = 1$$

Therefore 1, 3, 4, 5 and 9 are quadratic residue modulo 11.

● Euler's criterion :

Let p be a prime, a is an integer. Then a is a quadratic residue modulo p iff

$$a^{(p-1)/2} \equiv 1 \pmod{p}$$

- Suppose $p \equiv 3 \pmod{4}$ and y is a quadratic residue modulo p , then,

$$\begin{aligned} (\pm y^{(p+1)/4})^2 &\equiv y^{(p+1)/2} \pmod{p} \\ &\equiv y^{(p-1)/2} \cdot y \pmod{p} \\ &\equiv y \pmod{p} \end{aligned}$$

Since by Euler's criterion $y^{(p-1)/2} \equiv 1 \pmod{p}$.

Therefore, $\pm y^{(p+1)/4} \pmod{p}$ are two square roots of $y \pmod{p}$.

Rabin Cryptosystem:

Let $n = pq$, where p and q are primes and $p, q \equiv 3 \pmod{4}$. Let $P = C = \mathbb{Z}_n^*$, and define $K = \{(n, p, q)\}$.

For $K = (n, p, q)$, define

$$e_K(x) = x^2 \pmod{n} \quad [\text{Encryption}]$$

and

$$d_K(y) = \sqrt{y} \pmod{n} \quad [\text{Decryption}]$$

The value n is the public key, while p and q are the private key.

● Example: Suppose $n = 77 = 7 \times 11$

$$\text{Then } e_K(x) = x^2 \pmod{77}$$

$$d_K(x) = \sqrt{x} \pmod{77}$$

Let $y = 23$ is a ciphertext Bob wants to decrypt.

$$7 \equiv 3 \pmod{4}, \quad 11 \equiv 3 \pmod{4}$$

$$\text{So, } \pm 23^{(7+1)/4} \equiv \pm 2^2 \equiv \pm 4 \pmod{7} = 4, 3$$

$$\text{and } \pm 23^{(11+1)/4} \equiv \pm 1^3 \equiv \pm 1 \pmod{11} = 1, 10$$

Now use Chinese Remainder theorem to solve,

$$x \equiv a \pmod{7}$$

$$x \equiv b \pmod{11}$$

where $a \in \{4, 3\}$, $b \in \{1, 10\}$.

We get four square roots of 23 modulo 77 to be $\pm 10, \pm 32 \pmod{77}$.

Possible plaintexts are $x = 10, 32, 45, 67$.

Verify ~~with~~ ^{each} value of x satisfies

$$23 \equiv x^2 \pmod{77}$$

We get ~~with~~ $y = 23$ is a valid ciphertext.

Def: Let p be a prime.
 $\mathcal{Q}R_p =$ set of quadratic residues mod p .
 $\overline{\mathcal{Q}R}_p =$ set of quadratic non-residues mod p .

Then $|\mathcal{Q}R_p| = |\overline{\mathcal{Q}R}_p|$.

Proof: All quadratic residues mod p are given in the set $\mathcal{Q}R_p$ as
 $\mathcal{Q}R_p = \{1^2, 2^2, \dots, (\frac{p-1}{2})^2 \pmod{p}\}$

It suffices to prove that
 $|\mathcal{Q}R_p| = \frac{p-1}{2}$ i.e., all these elements are distinct modulo p .

Consider $x^2 \equiv y^2 \pmod{p}$, $1 \leq x \leq \frac{p-1}{2}$
 $1 \leq y \leq \frac{p-1}{2}$

$$\Rightarrow x^2 - y^2 \equiv 0 \pmod{p}$$

$$\Rightarrow (x-y)(x+y) \equiv 0 \pmod{p}$$

$$\Rightarrow x \equiv y \pmod{p} \quad [\text{since } p \nmid (x+y) \text{ as } x+y < p].$$

Therefore all elements of $\mathcal{Q}R_p$ are distinct.

$$\text{Thus, } |\mathcal{Q}R_p| = \frac{p-1}{2} \Rightarrow |\overline{\mathcal{Q}R}_p| = (p-1) - |\mathcal{Q}R_p| = \frac{p-1}{2}.$$

● Definition (Legendre Symbol):

Suppose p is an odd prime. For any integer a , define the Legendre symbol $\left(\frac{a}{p}\right)$ as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \end{cases}$$

● Euler's Criterion:

Let p be a prime (odd). ~~then for~~
Then for any integer a ,

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

Proof:

case 1: $a \equiv 0 \pmod{p}$

$$\Rightarrow \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \equiv 0 \pmod{p}$$

case 2: $a \not\equiv 0 \pmod{p}$.

$$\left(a^{(p-1)/2}\right)^2 \equiv a^{p-1} \equiv 1 \pmod{p} \quad \left[\text{by Fermat's little th.} \right]$$

$$\Rightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{or} \\ a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

First case, $a \in \mathbb{Q}R_p \Rightarrow \left(\frac{a}{p}\right) = 1$

Second case, $a \in \overline{\mathbb{Q}R_p} \Rightarrow \left(\frac{a}{p}\right) = -1$

Therefore $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$

■

● Properties of Legendre Symbol:

1. If p is an odd prime, m, n are integers then,

$$\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right) \quad \text{if } m \equiv n \pmod{p}$$

$$2. \quad \left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \cdot \left(\frac{n}{p}\right)$$

$$3. \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$$4. \quad \left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{8} \\ -1, & \text{if } p \equiv \pm 3 \pmod{8} \end{cases}$$

5. If p, q are odd primes then

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \cdot \left(\frac{q}{p}\right) \quad [\text{Reciprocity Law}]$$

● Definition (Jacobi Symbol):

Suppose n is an odd positive integer, and the prime power factorization of n is $n = \prod_{i=1}^k p_i^{e_i}$.

Let a be an integer. The Jacobi symbol $\left(\frac{a}{n}\right)$ is defined to be,

$$\left(\frac{a}{n}\right) = \prod_{i=1}^k \left(\frac{a}{p_i}\right)^{e_i}$$

where $\left(\frac{a}{p_i}\right)$ is Legendre symbol.

● Example: $9975 = 3 \times 5^2 \times 7 \times 19$

$$\left(\frac{6278}{9975}\right) = \left(\frac{6278}{3}\right) \cdot \left(\frac{6278}{5}\right)^2 \left(\frac{6278}{7}\right) \left(\frac{6278}{19}\right)$$

$$= \left(\frac{2}{3}\right) \left(\frac{3}{5}\right)^2 \left(\frac{6}{7}\right) \left(\frac{8}{19}\right)$$

$$= (-1) (-1)^2 (-1) (-1)$$

$$= -1.$$

● Properties of Jacobi symbol :

Let m, n are odd positive integers, a, b are any integers.

$$1. \left(\frac{ab}{n} \right) = \left(\frac{a}{n} \right) \left(\frac{b}{n} \right)$$

$$2. \left(\frac{a}{mn} \right) = \left(\frac{a}{m} \right) \cdot \left(\frac{a}{n} \right)$$

$$3. \text{ If } a \equiv b \pmod{n} \text{ then } \left(\frac{a}{n} \right) = \left(\frac{b}{n} \right)$$

$$4. \left(\frac{-1}{n} \right) = (-1)^{\frac{n-1}{2}}$$

$$5. \left(\frac{2}{n} \right) = (-1)^{(n^2-1)/8}$$

$$6. \left(\frac{m}{n} \right) = \begin{cases} - \left(\frac{n}{m} \right), & \text{if } m \equiv n \equiv 3 \pmod{4} \\ \left(\frac{n}{m} \right), & \text{otherwise} \end{cases}$$

● Example :

$$\left(\frac{7411}{9283} \right) = - \left(\frac{9283}{7411} \right) \quad (\text{property 6})$$

$$= - \left(\frac{1872}{7411} \right) \quad (\text{property 3})$$

$$= - \left(\frac{2}{7411} \right)^4 \left(\frac{117}{7411} \right) \quad (\text{property 1})$$

$$= - \left(\frac{117}{7411} \right) \quad (\text{property 5})$$

$$= - \left(\frac{7411}{117} \right) \quad (\text{property 6})$$

$$= - \left(\frac{40}{117} \right) \quad (\text{property 3})$$

$$= - \left(\frac{2}{117} \right)^3 \left(\frac{5}{117} \right) \quad (\text{property 1})$$

$$= \left(\frac{5}{117} \right) \quad (\text{property 5})$$

$$= \left(\frac{117}{5} \right) \quad (\text{property 6})$$

$$= \left(\frac{2}{5} \right) \quad (\text{property 3})$$

$$= -1 \quad (\text{property 5})$$

• The Solovay - Strassen Algorithm:

- If $\left(\frac{a}{n} \right) \equiv a^{(n-1)/2} \pmod{n}$ then n is called pseudoprime base a .

$$\left(\frac{10}{91} \right) = -1 = 10^{45} \pmod{91}$$

$\Rightarrow 91$ is a pseudoprime base 10.

Algorithm: SOLOVAY-STRASSEN(n)

1. Choose a random integer a such that $1 \leq a \leq (n-1)$
2. $x \leftarrow \left(\frac{a}{n}\right)$
3. if $x = 0$
4. then return ("n is composite")
5. $y \leftarrow a^{(n-1)/2} \pmod{n}$
6. if $x \equiv y \pmod{n}$
7. then return ("n is prime")
8. else return ("n is composite")

● Goldwasser-Micali Public-key Cryptosystem

- Let p, q be two prime numbers and $n = pq$. Then $\left(\frac{a}{n}\right) = 1$, does not necessarily imply a is quadratic residue modulo n , because $\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right) \left(\frac{a}{q}\right) (= (-1) \cdot (-1) = 1) = 1$ does not imply $\left(\frac{a}{p}\right) = 1$ and $\left(\frac{a}{q}\right) = 1$ ~~also~~ always.

- a is quadratic residue modulo $n = pq$ iff a is quadratic residue modulo p and a is quadratic residue modulo q .

• The cryptosystem:

Setup:

1. Let p, q be two primes
2. $n = pq$
3. Let $\left(\frac{m}{p}\right) = -1 = \left(\frac{m}{q}\right)$
so that $\left(\frac{m}{n}\right) = 1$.

$$P = \{0, 1\}, \quad G = \mathbb{Z}_n^*, \quad K = \{(n, p, q, m)\}$$

For $K = (n, p, q, m)$, define

Encryption: $e_K(x, r) = m^x r^2 \pmod{n}$

Decryption:
$$d_K(y) = \begin{cases} 0 & \text{if } y \in QR(n) \\ 1 & \text{if } y \in \overline{QR}(n) \end{cases}$$

where $x = 0$ or 1 and $r, y \in \mathbb{Z}_n^*$

Note: r is chosen randomly from \mathbb{Z}_n^* at the time of encryption.