Tutorial 6 ENG

20 October 2021 14:00

PUBLIC KEY ENCRYPTION

Rabin cryptosystem
- → Chinese remainder theorem
- → Quadratic residues
- → Euler's criterion
- → Legendre and Jacobi symbols

ElGamal cryptosystem

Security definition for PKC

Chinese remainder theorem

$x \equiv a_1 \mod n_1 \qquad \forall i,j \ \gcd(n_i, n_j) = 1$

$x \equiv a_2 \mod n_2$

$\vdots$

$x \equiv a_k \mod n_k$

$N = n_1 \cdot n_2 \cdot n_3 \cdots n_k \qquad x = \sum_{i=1}^{k} a_i N_i M_i \mod N$

$N_i = N / n_i \qquad x + N, \ x + 2N, \ \ldots$

$M_i = N_i^{-1} \mod n_i$

$x \mod n_j$

$= \sum_{i=1}^{k} a_i N_i M_i \mod n_j$

$\equiv a_j N_j M_j \mod n_j$ (because $\forall i \neq j \ N_i$ is a multiple of n_j)

$\equiv a_j \mod n_j$

Example

$N = 3 \cdot 4 \cdot 5 = 60$

$x \equiv 0 \mod 3 \qquad N_1 = 4 \cdot 5 = 20 \qquad M_1 \equiv 20^{-1} \equiv 2^{-1} \equiv 2 \mod 3$

$x \equiv 3 \mod 4 \qquad N_2 = 3 \cdot 5 = 15 \qquad M_2 \equiv 15^{-1} \equiv (-1)^{-1} \equiv 3 \mod 4$

$x \equiv 4 \mod 5 \qquad N_3 = 3 \cdot 4 = 12 \qquad M_3 \equiv 12^{-1} \equiv (2)^{-1} \equiv 3 \mod 5$

$x \equiv 0 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 4 \cdot 12 \cdot 3 \mod 60$

$\equiv 0 + 135 + 144 \mod 60$

$\equiv 15 + 24 \mod 60$

$\equiv 39 \mod 60$

Quadratic residues in $\mathbb{Z}_n^*$ → multiplicative group mod n

{set of all non-zero numbers (smaller than n) coprime to n}

$a \in \mathbb{Z}_n^*$ is a QR if $\exists x \in \mathbb{Z}_n^*$ s.t. $x^2 \equiv a \mod n$

$x \equiv \sqrt{a} \mod n$

$\mathbb{Z}_5^* = \{1,2,3,4\}$ $\quad QR_5 = \{1,4\}$ $\quad x \equiv a^{\frac{1}{2}} \bmod n$

$1^2 \equiv 1 \bmod 5$

$2^2 \equiv 4 \bmod 5$ $\quad$ There are $\frac{p-1}{2}$ QR_s in $\mathbb{Z}_p^*$ for prime p.

$(-2)^2 \equiv 4 \bmod 5$ $\quad x^2 \equiv a \bmod p$

$(-1)^2 \equiv 1 \bmod 5$ $\quad (-x)^2 \equiv a \bmod p$

Euler's Criterion $\quad$ Legendre Symbol

For an odd prime p, $\gcd(a,p)=1$

$a^{\frac{p-1}{2}}$ → integer division

$\equiv 1 \bmod p \Leftrightarrow a$ is a QR mod p $\quad \left(\frac{a}{p}\right) = 1$ ($a \in QR$)

$\left(\frac{q}{p}\right) = 0$ ($a \equiv 0 \bmod p$) $\quad$ q = quadratic nonresidue

$\equiv -1 \bmod p \Leftrightarrow a$ is a QNR mod p $\quad \left(\frac{a}{p}\right) = -1$ ($a \notin$ QR)

Legendre Symbol

Jacobi Symbol

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{d_1} \left(\frac{a}{p_2}\right)^{d_2} \cdots \left(\frac{a}{p_k}\right)^{d_k}$$

$b = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$

How to calculate square roots mod p? (p - prime)

C is a QR mod p. Find X s.t. $x^2 \equiv C \bmod p$

$x \equiv \sqrt{C} \bmod p$

1.) $p \equiv 3 \bmod 4$ → easy

$p \equiv 1 \bmod 4$ → a bit more involved (but efficient)

For $p \equiv 3 \bmod 4$, → integer division

$\sqrt{C} \equiv \pm C^{\frac{p+1}{4}} \bmod p$ $\quad =$ (1 by Euler's criterion)

$$\left(C^{\frac{p+1}{4}}\right)^2 \equiv C^{\frac{p+1}{2}} \equiv C \cdot C^{\frac{p-1}{2}} \equiv C \bmod p$$

$$C \cdot C^{\frac{p-1}{2}} = C^{\frac{p-1}{2}+1} = C^{\frac{p-1+2}{2}} = C^{\frac{p+1}{2}}$$

Rabin cryptosystem

Elements: $n = p \cdot q$ | p, q are huge primes $(p, q \equiv 3 \bmod 4)$

Public key: n

Private key: p, q

Encrypt: $1 < w \leq p-1$ $\quad c \equiv w^2 \bmod n$

Decryption: of c $\quad w \equiv \sqrt{c} \bmod n$

Decryption: of c $\quad w \equiv \sqrt{c} \mod n$

↓ is easy with the knowledge of p, q
hard without it

1.) How decrypt with knowledge of p and q?

You can find x s.t.
$x^2 \equiv c \mod n$ → 4 solutions

from m_p and m_q, s.t.

$m_p^2 \equiv c \mod p \quad \equiv \quad m_p \equiv \pm c^{\frac{p+1}{4}} \mod p$

$m_q^2 \equiv c \mod q \quad \equiv \quad m_q \equiv \pm c^{\frac{q+1}{4}} \mod q$

$x \equiv m_p \mod p \Rightarrow x = k \cdot p + m_p \quad x^2 = k^2 p^2 + 2k \cdot p \cdot m_p + m_p^2 \equiv c \mod p$

$x \equiv m_q \mod q \Rightarrow x = l \cdot q + m_q \quad x^2 = l^2 q^2 + 2 \cdot l \cdot q \cdot m_q + m_q^2 \equiv c \mod q$

$x^2 = k' \cdot p + c$
$x^2 = l' \cdot q + c$
$x^2 = m' \cdot pq + c$
$x^2 \equiv c \mod n$

$x_1 \equiv m_p \mod p$ $x_1 \equiv m_q \mod q$	$x_3 \equiv m_p \mod p$ $x_3 \equiv -m_q \mod q$
$x_2 \equiv -m_p \mod p$ $x_2 \equiv m_q \mod q$	$x_4 \equiv -m_p \mod p$ $x_4 \equiv -m_q \mod q$

Four different solutions

$y_q \equiv q^{-1} \mod p \qquad y_p \equiv p^{-1} \mod q$

$x_1 \equiv (m_p \cdot q \cdot y_q + m_q \cdot p \cdot y_p) \mod n$

$x_2 \equiv (-m_p \cdot q \cdot y_q + m_q \cdot p \cdot y_p) \mod n$

$x_3 \equiv (m_p \cdot q \cdot y_q - m_q \cdot p \cdot y_p) \mod n$

$x_4 \equiv (-m_p \cdot q \cdot y_q - m_q \cdot p \cdot y_p) \mod n$

How to attack the cryptosystem

1.) Factor n

2.) Can we calculate $\sqrt{c}$ (all four of them) $\bmod n$ without factorization?

$\gcd(x_1 + x_2, n) = p$ → solution to factorization.

Example: (Exercise 6.1)

decrypt $c = 56$ with $n = 143 = 11 \cdot 13 = p \cdot q$

$$m_p = \sqrt{c} \equiv \sqrt{56} \bmod 11$$
$$\equiv 56^{\frac{12}{4}} \bmod 11$$
$$\equiv 56^3 \bmod 11$$
$$\equiv 1^3 \bmod 11$$
$$\equiv \pm 1 \bmod 11$$

$$m_q \equiv \sqrt{56} \bmod 13$$
$$\equiv \sqrt{4} \bmod 13$$
$$\equiv \pm 2 \bmod 13$$

$x_1 \equiv 1 \bmod 11$, $x_1 \equiv 2 \bmod 13$ | $x_2 \equiv -1 \bmod 11$, $x_2 \equiv 2 \bmod 13$ | $x_3 \equiv 1 \bmod 11$, $x_3 \equiv -2 \bmod 13$ | $x_4 \equiv -1 \bmod 11$, $x_4 \equiv -2 \bmod 13$

$$y_p \equiv 11^{-1} \bmod 13 \qquad y_q \equiv 13^{-1} \bmod 11$$
$$\equiv 6 \bmod 13 \qquad \equiv 6 \bmod 11$$

$$x_1 \equiv \underbrace{m_p \cdot q \cdot y_q}_{1 \cdot 13 \cdot 6} + \underbrace{m_q \cdot p \cdot y_p}_{2 \cdot 11 \cdot 6} \equiv \underbrace{13 \cdot 6}_{78} + \underbrace{22 \cdot 6}_{132} \bmod 143$$

$x_1 \equiv 78 + 132 \equiv 67 \bmod 143$

$x_2 \equiv -78 + 132 \equiv 54 \bmod 143$

$x_3 \equiv 78 - 132 \equiv 89 \bmod 143$

$x_4 \equiv -78 - 132 \equiv \ldots \bmod 143$

$x_1 = N - x_4$

$(54)^2 \bmod 143$

Unique decryption?

→ pattern in correct plaintext e.g. binary representation of plaintext ends in 5 symbols '1'

m (n-bit) → $m \cdot 2^5 + 2^5 - 1$

→ Extra bits:

	Jacobi	Parity
x_1	-1	0
x_2	1	1
x_3	-1	1
x_4	1	0

$(c, \bar{3}, \bar{p})$

→ Williams - Rabin

Let $N = pq$, with $p, q \equiv 3 \pmod 4$. If $p \neq \pm q \pmod 8$ then $\left(\frac{2}{N}\right) = -1$. ⇒ For every $1 \leq x < N$ exactly one of $x, N-x, 2x, N-2x$ is a square modulo N.

$p \equiv 3 \bmod 8$
$q \equiv 7 \bmod 8$

then you want to map $m \to x$ which is even and $\left(\frac{x}{N}\right) = 1$ $\quad 1 \leq m < \frac{N}{8} - 1$

$$x = P(m) \begin{cases} 4(2m+1) & \text{if } \left(\frac{2m+1}{N}\right) = 1 \\ 2(2m+1) & \text{if } \left(\frac{2m+1}{N}\right) = -1 \end{cases}$$

El Gamal

1.) Based on discrete logarithm

2.) Has randomized encryption

Elements: p - large prime

q - primitive element in $Z_p^* = \{1, \dots, p-1\}$
$= \{q, q^2, q^3, \dots q^{p-1}\}$

x - secret exponent $\quad \{1, \dots, p-1\}$

$y = q^x \bmod p$

Public: p, q, y

Private: x

Encryption: $w \in Z_p^*$

1.) Choose a random $r \in \{1, \dots, p-1\}$

1.) Choose a random $r \in \{1, \dots, p-1\}$

2.) $a \equiv g^r \bmod p$

$b \equiv w \cdot y^r \bmod p$

$w \to (a, b)$

Decryption:

$w \equiv b \cdot (a^x)^{-1} \equiv b \cdot a^{-x} \bmod p$

$\equiv w \cdot g^r \cdot a^{-x}$

$\equiv w \cdot (g^x)^r \cdot (g^r)^{-x} \bmod p$

$\equiv w \cdot g^{x \cdot r} \cdot g^{-x \cdot r} \bmod p$

$\equiv w \bmod p$

Always keep r secret!

$w = b \cdot y^{-r} \bmod p$

Never reuse r!

Security definition PKC

$\forall m, c \quad P(C=c) = P(C=c \mid M=m)$

$\Leftrightarrow$

$\Pr\left[A\{e(M), h(M)\} = f(M)\right] \leq \Pr\left[B\{e(M)\} = f(M)\right] + \gamma(n)$

A, B are efficient algorithms (in size of private keys)

$e \to$ encryption function

$M \to$ plaintext distribution

$e\{M\} \to$ ciphertext distribution

$\gamma(n)$ is a negligible function

h, f functions $\{0,1\}^* \to \{0,1\}^n$

$A\{e(M), h(M)\} \to$ something that can be efficiently calculated from distribution of plaintexts and ciphertexts $\left(P(C=c \mid M=m)\right)$

$B\{e(M)\} \to$ something that can be efficiently $\left(P(C=c)\right)$

calculated from distribution of ciphertexts only