Tutorial VI

13 November 2020 11:19

Other public key encryption systems

Rabin encryption

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

ElGamal encryption

Security definition for PKC

Chinese remainder theorem

$$x \equiv a_1 \mod n_1 \qquad \forall_{i,j} \ \gcd(n_i, n_j) = 1$$
$$x \equiv a_2 \mod n_2$$
$$\vdots$$
$$x \equiv a_k \mod n_k$$

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

$$N_i = N / n_i$$

$$x + N, \ x + 2N, \ \ldots$$

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

$$x \mod n_j$$
$$= \sum_{i=1}^{k} a_i N_i M_i \mod n_j$$
$$= a_j \underbrace{N_j M_j}_{\equiv 1} \mod n_j \quad (\text{because } \forall_{i \neq j} \ N_i \text{ is a multiple of } n_j)$$
$$= a_j \mod n_j$$

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

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

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

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

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

$x = 0 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 4 \cdot 12 \cdot 3$

$= 0 + 135 + 144 \mod 60$

$279 \mod 60$

$39 \mod 60$

Quadratic residues in $\mathbb{Z}_n^* = \{1, \dots, n-1\}$

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

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

$x \equiv a^{\frac{1}{2}} \mod n$ ⊸ notation for square root

$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ $\quad QR_5 = \{1, 4\}$

$1^2 = 1 \mod 5$

$2^2 = 4 \mod 5$

$3^2 = 4 \mod 5$

$4^2 = 1 \mod 5$

There are $\frac{p-1}{2}$ QRs in $\mathbb{Z}_p^*$ p prime

$x^2 \equiv a \mod p$

$(-x)^2 \equiv a \mod p$

Euler's criterion

For odd prime p

Integer division

$$a^{\frac{p-1}{2}} \begin{cases} = 1 \mod p \iff a \text{ is a QR} \mod p \\ \\ = -1 \mod p \iff a \text{ is a QNR} \mod p \end{cases}$$

Legendre symbol

$\left(\frac{a}{p}\right) = 1$ (a is QR)

$\left(\frac{a}{b}\right) = 0$ ($a \equiv 0 \mod p$)

$\left(\frac{a}{p}\right) = -1$ (a is QNR

$= -1 \mod p \iff a$ is a QNR $\mod p$ $\left(\frac{a}{p}\right) = -1$ (a is QNR

Jacobi symbol

Legendre symbols

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}$$

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

How to calculate square roots mod p?

C is a QR, find x s.t. $x^2 \equiv C \mod p$

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

1.) $p \equiv 3 \pmod 4$ → easy

$p \equiv 1 \pmod 4$ → a bit more involved but efficient

$$\sqrt{C} = \pm C^{\frac{p+1}{4}}$$

$\frac{p+1}{4}$: integer division

(1 by Euler's criterion)

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

Rabin cryptosystem

Elements: $n = pq$, p, q are large primes ($p, q \equiv 3 \mod 4$)

Public: n

Private: p, q

Encrypt $1 < w \leq p-1$ $\quad C = w^2 \mod n$ easy

Encrypt $1 < w \leq p-1$ $\quad C = w^2 \mod n$

Decrypt of c $\quad W = \sqrt{C} \mod n$

Hard if you do not know p,q
easy when you do

1.) How to decrypt with the knowledge of p and q

You can find

$$x^2 \equiv c \mod n$$

from

$$x^2 \equiv C \mod p \Rightarrow k \cdot p + C \equiv x^2$$

$$x^2 \equiv C \mod q \Rightarrow l \cdot q + C \equiv x^2$$

$$\Rightarrow m \cdot p \cdot q + C \equiv x^2$$

$$\left(\begin{matrix} k = m \cdot q \\ l = m \cdot p \end{matrix} \right)$$

$$X \equiv \sqrt{C} \mod p$$

$$X \equiv \sqrt{C} \mod q$$

these are easy to calculate
(different integers)

$$m_p \equiv \sqrt{C} \equiv \pm C^{\frac{p+1}{4}} \mod p$$

$$m_q \equiv \sqrt{C} \equiv \pm C^{\frac{p+1}{4}} \mod q$$

$x_1 \equiv m_p \mod p$ | $x_3 \equiv -m_p \mod p$

$x_1 \equiv m_p \mod p$ | $x_3 \equiv -m_p \mod p$
$x_1 \equiv m_q \mod q$ | $x_3 \equiv m_q \mod q$

$x_2 \equiv m_p \mod p$ | $x_4 \equiv -m_p \mod p$
$x_2 \equiv -m_q \mod q$ | $x_4 \equiv -m_q \mod q$

$\boxed{\text{Four different Solutions!}}$

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

$a_1 \; N_1 \; M_1 \qquad a_2 \; N_2 \; M_2$

$$x_1 \equiv (m_p \cdot q \cdot y_q + m_q \, p \cdot y_p) \mod n$$
$$x_2 \equiv (m_p \cdot q \cdot y_q - m_q \, p \cdot y_p) \mod n$$
$$x_3 \equiv (-m_p \cdot q \cdot y_q + m_q \, p \cdot y_p) \mod n$$
$$x_4 \equiv (-m_p \cdot q \cdot y_q - m_q \, p \cdot y_p) \mod n$$

$$x_1 + x_2 = 2 m_p \, q \, y_q$$
$$\gcd(x_1 + x_2, n) = q$$

$\boxed{\text{Exercise}}\boxed{6.1}$ decrypt $c = 56$
with $n = 143 = 11 \cdot 13 = p \cdot q$

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

$$\equiv 1^3 \mod 11$$
$$\equiv \pm 1 \mod 11$$

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

$$\Downarrow$$

$x_1 \equiv 1 \mod 11$	$x_2 \equiv 1 \mod 11$	$x_3 \equiv -1 \mod 11$	$x_4 \equiv -1 \mod 11$
$x_1 \equiv 2 \mod 13$	$x_2 \equiv -2 \mod 13$	$x_3 \equiv 2 \mod 11$	$x_4 \equiv -2 \mod 13$

$$y_p \equiv 11^{-1} \mod 13$$
$$\equiv 6 \mod 13$$

$$y_q \equiv 13^{-1} \mod 11$$
$$\equiv 6 \mod 11$$

$$x_1 = \overset{m_p}{1} \cdot \overset{q}{13} \cdot \overset{y_q}{6} + \overset{m_q}{2} \cdot \overset{p}{11} \cdot \overset{y_p}{6} \equiv 13 \cdot 6 + 22 \cdot 6 \mod 143$$

$$\boxed{\begin{aligned} x_1 &= 78 + 132 \mod 143 \\ x_2 &= 78 - 132 \mod 143 \\ x_3 &= -78 + 132 \mod 143 \\ x_4 &= -78 - 132 \mod 143 \end{aligned}}$$

How to attack the cryptosystem?

1.) Factor n

2.) Can you calculate $\sqrt{c}$ (all four of them) without factoring efficiently?

2.) Can you calculate $\sqrt{c}$ (all four of them) without factoring efficiently?

$$\gcd(x_1+x_2, n) = q$$

Unique decryption?

→ pattern in correct plaintext e.g. binary representation ends in 5 ones

$$m \text{ (n-bit)} \mapsto m \cdot 2^5 + 2^5 - 1$$

$$[m_n | \; | \; | \; | \; | m_0] \longmapsto [m_{n+5} | \ldots | m_5 | 1 | 1 | 1 | 1 | 1]$$

→

	J	P
x_1	-1	0
x_2	1	1
x_3	-1	1
x_4	1	0

R

$$(c, \underline{J, P})$$

El Gamal

1.) based on discrete logarithms

2.) has randomized encryptions

Elements: p - a large prime

g - primitive element in $\mathbb{Z}_p^*$ $\quad \{g, g^2, \ldots, g^{p-1}\} = \mathbb{Z}_p^*$

x - secret exponent $\{1, \ldots, p-1\}$

$$y \equiv g^x \bmod p$$

Public $\quad p, g, y$

Private x

ENCRYPTION: $w \in \mathbb{Z}_p^*$

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

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

3.) $b \equiv w \cdot y^r \mod p$

$w \to (a, b)$

DECRYPTION

$(a, b) \to w$

with knowledge of x

$$w \equiv b \cdot (a^x)^{-1} \equiv b \cdot a^{-x} \mod p$$
$$\equiv w \cdot y^r \cdot a^{-x} \mod p$$
$$\equiv w\, (g^x)^r \cdot (g^r)^{-x} \mod p$$
$$\equiv w \cdot g^{xr} \cdot g^{-rx} \mod p$$
$$\equiv w \mod p$$

with knowledge of r → keep r secret

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

Security of PKC

$$\forall_{m,c} \quad P(C=c) = P(C=c \mid M=m)$$

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

A, B are efficient algorithms

e - encryption function

M - plaintext distribution

$e[M]$ → ciphertext distribution

$\boxed{\eta(n) \text{ is a negligible function}}$

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

$A\left[e(M), h(M)\right]$ → Something that can be efficiently calculated from distribution of plaintexts an ciphertexts

$B\left[e(M)\right]$ → Something that can be efficiently calculated from distribution of ciphertexts only