Tutorial VI group 2

24 October 2019 16:01

Other Public Key encryption systems

Rabin encryption

- → Chinese remainder theorem
- → Quadratic residues
- → Euler's criterion

El Gamal encryption

- → Shank's giant step, baby step algorithm

Security definition for PKC

- → Negligible functions

Chinese remainder theorem

$$x \equiv a_1 \mod n_1 \quad \forall_{i,j}\ \gcd(n_i, n_j) = 1$$

$$x \equiv a_2 \mod n_2$$

$$\vdots$$

$$x \equiv a_k \mod n_k$$

$$N = n_1 \cdot n_2 \cdot \ldots n_k$$

$$N_i = N / n_i$$

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

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

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

P

$$x \bmod n_j$$

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

$$= a_j \overbrace{N_j M_j}^{\equiv 1} \mod n_j \quad \left(\text{because if } i \neq j \ N_i \text{ is a multiple of } n_j\right)$$

$$= a_j \mod n_j$$

Example

$x \equiv 0 \mod 3 \qquad N_1 = 4.5 = 20 \qquad M_1 \equiv 20^{-1} \equiv 2^{-1} \mod 3 = 2$

$x \equiv 3 \mod 4 \qquad N_2 = 3.5 = 15 \qquad M_2 \equiv 15^{-1} \equiv (-1)^{-1} \mod 4 = 3$

$x \equiv 4 \mod 5 \qquad N_3 = 3.4 = 12 \qquad M_3 \equiv 12^{-1} \equiv 2^{-1} \mod 5 = 3$

$N = 3.4.5$

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

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

$$= 279 \mod 60$$

$$= 39 \quad \checkmark$$

Quadratic residues in $(\mathbb{Z}_p^* = \{1, \dots, p-1\})$

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

$x \equiv \sqrt{a} \mod p$ notation for square

$\left(\frac{1}{?}\right)$

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

$x \equiv a^{\frac{1}{2}} \mod p$

notation for square root

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

$1^2 = 1 \mod 5$

$2^2 = 4 \mod 5$

$3^2 = 4 \mod 5$

$4^2 = 1 \mod 5$

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

Euler's criterion

integer division

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

$a^{p-1} \equiv 1 \mod p$ (Fermat's little theorem)

$a^{p-1} - 1 \equiv 0 \mod p$

$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \mod p$ $\qquad (a-b)(a+b) = a^2 - b^2$

$\mathcal{P} \quad = 0 \quad \vee \quad = 0 \quad \mathcal{R}$

$a = x^2$

$(x^2)^{\frac{p-1}{2}} - 1$

$x^{p-1} - 1$

$x^{p-1} - 1 \equiv 0 \mod p$ (Fermat's little theorem)

How do I find 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 harder but efficient

$\sqrt{c} \equiv \pm c^{\frac{p+1}{4}}$ → 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: $n = p \cdot q$, p, q are large primes ($p, q \equiv 3 \mod 4$)

Public: n

Private: p, q

Encrypt $1 < W \leq p-1$: $c = W^2 \mod n$

Decryption of c: $W = \sqrt{c} \mod n$

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

You can find solution

$x^2 \equiv c \mod n$

from

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

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

$m \cdot p \cdot q + c \equiv x^2$

$k = m \cdot q$

$l = n \cdot p$

these are different integers

$X \equiv \sqrt{c} \mod p$ $\qquad m_p \equiv \sqrt{c} \equiv \pm c^{\frac{p+1}{4}} \mod p \mapsto 2$ solutions

$X \equiv \sqrt{c} \mod q$ $\qquad m_q = \sqrt{c} \equiv \pm c^{\frac{q+1}{4}} \mod q \mapsto 2$ solutions

P $\qquad \Downarrow$

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

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

Four differen CRT instances $\Rightarrow$ 4 solutions

$$\boxed{\begin{aligned} X_1 &\equiv m_p \cdot q \cdot y_q + m_q \cdot p \cdot y_p \\ X_2 &\equiv m_p \cdot q \cdot y_q - m_q \cdot p \cdot y_p \\ X_3 &\equiv -m_p \cdot q \cdot y_q + m_q \cdot p \cdot y_p \\ X_4 &\equiv -m_p \cdot q \cdot y_q - m_q \cdot p \cdot y_p \end{aligned}}$$

$x_1 + x_2 = 2 m_p q y_q$

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

Exercise 6.1

decrypt $c = 56$

with $n = 143 = 11 \cdot 13 = p \cdot q$

$m_p \equiv \sqrt{c} \mod p = \sqrt{56} \mod 11$

$$m_p \equiv \sqrt{c} \mod p = \sqrt{56} \mod 11$$
$$= 56^{\frac{12}{4}} \mod 11$$
$$= 56^3 \mod 11$$
$$= (1)^3 \mod 11$$
$$= \pm 1$$

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

$$\Downarrow$$

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

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

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

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

How to attack this cryptosystem?

1.) Factor n, then using p and q decrypt

2.) Is there an algorithm that calculates x_1, x_2, x_3, x_4 without factoring?

if yes, it is as hard as factoring because $\gcd(x_1 + x_2, n) = q$ can be calculated efficiently.

El Gamal encryption

1.) based on discrete logarithms

2.) has randomized encryptions

Elements:

p - a large prime

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

x - secret exponent

$y \equiv g^x \bmod p$

PUBLIC: p, g, y

PRIVATE: x

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

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

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

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

$w \to (a, b)$

Dec: $(a,b) \to w$

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

1.) Knowing x can be used to decrypt

2.) Knowing r can be used to decrypt

$$b \cdot g^{-r} \equiv w \mod p$$

Vulnerabilities of El Gamal

$(a,b) \to w \qquad b \cdot a^{-x} = w \cdot g^{r} \cdot a^{-x} = w$

$(a, 2b) \to \qquad 2b \cdot a^{-x} = 2w \cdot g^{r} a^{-x} = 2w$

$(a, kb) \to \qquad = kw$

$(a_1, b_1) \to \boxed{w_1}$

$(a_2, b_2) \to w_2$

$(a_1 a_2, b_1 b_2) \to b_1 b_2 \cdot (a_1 a_2)^{-x}$

$\to w_1 \cdot \cancel{g^{r_1}} w_2 \cdot \cancel{g^{r_2}} \cdot \cancel{(g^{r_1})^{-x}} \cdot \cancel{(g^{r_2})^{-x}}$

$\to w_1 w_2$

Shank's algorithm - calculates discrete logarithm.

$g^{x} \equiv y \mod p \qquad$ - find x

Naive solution requires $p-1$ exponentiations (in the worst case)

Shank's algorithm requires $2 \cdot \lceil \sqrt{p-1} \rceil$ exponentiations

Shank's algorithm requires $2 \cdot \lceil \sqrt{p-1} \rceil$ exponentiations

Giantstep-babystep paradigm

$m = \lceil \sqrt{p-1} \rceil$

$0 \leq j \leq m-1$

$\boxed{\text{Giant step}}$

j	$g^{mj} \bmod p$
0	1
1	g^m
⋮	⋮
	z
$m-1$	

Baby step

$0 \leq i \leq m-1$

i	$y g^{-i} \bmod p$
0	y
1	$y g^{-1}$
⋮	$y g^{-2}$
	⋮
	z
$m-1$	

$$g^{mj} \equiv z \equiv y g^{-i} \mod p$$

$$g^{mj} \equiv y g^{-i} \mod p$$

$$g^{mj+i} \equiv y \mod p$$

$j=0$ iterate i

$mj+i \in \{0, \dots, m-1\}$

$j=1$

$mj+i \in \{m, \dots 2m-1\}$

Security of PKC

$$\forall m, c \quad \Pr(M=m) \overset{\not\leq}{=} P(M=m \mid C=c)$$

$$\Pr\left(A[e(M), h(M)] = f(M)\right) \overset{\not\leq}{<} \Pr\left(B[e(M)] = f(M)\right)$$

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

A, B are efficient algorithms

e - encryption function $\quad$ e(M) - distribution of ciphertext

M - plaintext distribution $\quad$ $\eta(n)$ is a negligible function

h, f are functions $\quad \{0,1\}^* \longrightarrow \{0,1\}^n$

$A[e(M), h(M)]$ ~> something we can efficiently calculate from distribution of plaintexts and ciphertexts

$B[h(M)]$ ~> something that we can callulate from M

$\boxed{\eta(n) \text{ is a negligible function}}$: $\exists\, n_0$, s.t. $\forall n > n_0$

$\eta(n) < \frac{1}{p(n)}$ for an arbitrary polynomial p(n)