Tutorial VI

24 October 2019 10:01

Other public key encryption protocols

- → Rabin Cryptosystem
  - ↳ Chinese remainder theorem
- → ElGamal encryption
  - ↳ Shank's algorithm (baby step-giant step)
- → Security definition for public key cryptosystems
  - ↳ Negligible functions

Chinese remainder theorem

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

$$x \equiv a_2 \mod n_2$$

$$\vdots$$

$$\boxed{x}\ x+N,\ x+2N, \dots x+kN$$

$$x \equiv a_k \mod n_k$$

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

$$N_i = N/n_i$$

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

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

this is a multiple of n_j

$$a_i N_i M_i \equiv 0 \mod n_j \quad \forall i \neq j$$

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

$$= a_j N_j M_j \mod n_j$$

$$= a_j \underbrace{N_j M_j}_{1} \mod n_j$$

$$= a_j$$

Example

$$\begin{aligned}
x &\equiv 0 \mod 3 & N_1 &= 4.5 = 20 & M_1 &= 20^{-1} = 2^{-1} \mod 3 = 2 \\
x &\equiv 3 \mod 4 & N_2 &= 3.5 = 15 & M_2 &= (15)^{-1} = (-1)^{-1} \mod 4 = 3 \\
x &\equiv 4 \mod 5 & N_3 &= 3.4 = 12 & M_3 &= 12^{-1} = 2^{-1} \mod 5 = 3
\end{aligned}$$

$$N = 3.4.5$$

$$\begin{aligned}
x &\equiv a_1 N_1 M_1 + a_2 N_2 M_2 + a_3 N_3 M_3 \\
&\equiv 0 \cdot 20 \cdot 2 + 3 \cdot 15 \cdot 3 + 4 \cdot 12 \cdot 3 \quad (\text{mod } 60) \\
&\equiv 0 + 135 + 144 \equiv 279 \quad (\text{mod } 60) \\
&\equiv 39 \quad (\text{mod } 60)
\end{aligned}$$

Quadratic Residues in $(\mathbb{Z}_p^*)$

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

$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ if p is a prime there are $\frac{p-1}{2}$ QRs in $\mathbb{Z}_p^*$

$1^2 = 1 \mod 5$

$2^2 = 4 \mod 5$

$3^2 = 4 \mod 5$

$4^2 = 1 \mod 5$

Euler's criterion

Euler's criterion

integer division

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

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

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

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

$$0 \quad \text{or} \quad 0$$

$a = x^2$

$$\left((x^2)^{\frac{p-1}{2}} - 1\right) \equiv 0 \mod p$$

$$(x^{p-1} - 1) \equiv 0 \mod p$$

$$x^{p-1} \equiv 1 \mod p$$

How calculate square roots?

C is a QR mod p. How do we find x, s.t. $\boxed{\begin{array}{l} x^2 \equiv c \mod p \\ x = \sqrt{c} \mod p \end{array}}$

1.) $p \equiv 3 \pmod 4$ → easy

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

1 (Euler's criterion)

Let $p \equiv 3 \pmod 4$ integer division $\left(\frac{p+1}{\ }\right)^2$ $\quad \frac{p+1}{\ }$ $\quad \frac{p-1}{\ }$

Let $p \equiv 3 \pmod 4$)

$\sqrt{c} \equiv c^{\frac{p+1}{4}} \bmod p$ ← integer division

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

Rabin's cryptosystem

Elements: $n = p \cdot q$, p, q are primes $\boxed{p, q \equiv 3 \bmod 4}$

Public: n

Private: p, q

Encryption of message w: $c = w^2 \bmod n$

Decryption of c: $w = \sqrt{c} \bmod n$ $\boxed{1 \leq w \leq n-1}$

Decryption is efficient with knowledge of p and q:

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

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

$\Downarrow$

$m \cdot p \cdot q + c$

$k = m \cdot q$

$l = m \cdot p$

$\Downarrow$

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

$x \equiv \sqrt{c} \bmod q$

$m_p \equiv \sqrt{c} \equiv c^{\frac{p+1}{4}} \bmod p$ ← 2 solutions

$m_q \equiv \sqrt{c} \equiv c^{\frac{q+1}{4}} \bmod q$ ← 2 solutions

$\Downarrow$

$x \equiv m_p \bmod p$ → 4 combinations of m_p and m_q

$$\boxed{\begin{aligned} x &\equiv m_p \mod p \\ x &\equiv m_q \mod q \end{aligned}} \rightarrow 4 \text{ combinations of } m_p \text{ and } m_q$$

$\Downarrow$

4 Solutions!

$$\begin{aligned} y_q &\equiv q^{-1} \mod p \\ y_p &\equiv p^{-1} \mod q \end{aligned}$$

$$\begin{aligned} x_1 &\equiv m_p \cdot q \cdot y_q + m_q \cdot p \cdot y_p \\ x_2 &\equiv m_p \cdot q \cdot y_q - m_q \cdot p \cdot y_p \\ x_3 &\equiv -m_p \cdot q \cdot y_q + m_q \cdot p \cdot y_p \\ x_4 &\equiv -m_p \cdot q \cdot y_q - m_q \cdot p \cdot y_p \end{aligned}$$

$x_1 + x_2 = m_p \cdot q \cdot y_q$

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

Exercise 6.1

$n = 143 = 11 \cdot 13$

$c = 56$

$$\begin{aligned} m_p = \sqrt{c} \mod p &= \sqrt{56} \mod 11 \\ &= 56^{\frac{12}{4}} \equiv 56^3 \mod 11 \\ &\equiv 1^3 \equiv 1 \mod 11 \quad (-1) \end{aligned}$$

$$\begin{aligned} m_q = \sqrt{c} \mod q &= \sqrt{56} \mod 13 \\ &= \sqrt{4} \mod 13 \\ &= 2 \mod 13 \quad (-2) \end{aligned}$$

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

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

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

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

$$x_1 \equiv 1 \cdot 13 \cdot 6 + 2 \cdot 11 \cdot 6 \equiv \overset{78}{13 \cdot 6} + \overset{132}{22 \cdot 6} \mod 143$$

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

SECURITY

1.) if adversary can factor then they can decrypt Rabin

2.) is there an algorithm to find $\sqrt{c}$ mod n which doesn't factor?

No. It is as hard as factoring because $\gcd(x_1 + x_2, n) = q$ therefore factors are efficiently calculable.

El gamal cryptosystem

1.) based on discrete logarithm problem

2.) has randomized encryptions.

Elements:

discrete log problem

- p - a large prime
- q - primitive element in $\mathbb{Z}_p^*$ $\boxed{\{q, q^2, \dots, q^{p-1}\} = \mathbb{Z}_p^*}$
- x - secret exponent
- $y = q^x \bmod p$

PUBLIC: p, q, y

PRIVATE: x

encryption of $w \in \mathbb{Z}_p^*$: 1.) Choose random $r \in \{1, \dots, p-1\}$

$$a = q^r \bmod p$$
$$b = w \cdot y^r \bmod p$$

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

decryption of (a,b)

$$w = b \cdot a^{-x} = b \cdot (a^x)^{-1} \bmod p$$
$$= w \cdot y^r \cdot a^{-x} \bmod p$$
$$= w \cdot (q^x)^r \cdot (q^r)^{-x} \bmod p$$
$$= w \cdot q^{xr} \cdot q^{-xr} \bmod p$$
$$= w \bmod p$$

1.) knowing x enables decryption

2.) knowing r enables decryption

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

$\boxed{(a,b)} \rightarrow w$

$\boxed{(a,2b)} \rightarrow 2b(a^{-x}) \equiv 2 \cdot w \cdot y^{r} \cdot a^{-x} = 2w \mod p$

$(a, kb) \rightarrow kw$

$(a_1, b_1) \rightarrow w_1 \qquad (a_1 a_2, b_1 b_2) = b_1 b_2 \cdot (a_1 a_2)^{-x}$

$(a_2, b_2) \rightarrow w_2$

$$= w_1 \cdot y^{r_1} \cdot w_2 \, y^{r_2} \cdot a_1^{-x} \cdot a_2^{-x}$$

$$= w_1 w_2$$

$\boxed{\text{Malleability}}$

Shank's algorithm to solve discrete log problem

Naive solution requires $p-1$ exponentiations i the worst case

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

Giant step baby step algorithm

$m = \lceil \sqrt{p-1} \rceil \qquad y = q^{x} \mod p$ (find x)

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

$0 \le j \le m-1$

j	$q^{mj} \mod p$
0	1
1	q^{m}
⋮	⋮

$\boxed{\text{Baby step}}$

$0 \le i \le m-1$

i	$y \cdot q^{-i} \mod p$
0	y
1	$y q^{-1}$
⋮	⋮

1	
⋮	②
$m-1$	

1	$y\,g$
⋮	②
$m-1$	

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

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

$$x \equiv mj+i \quad \boxed{\mod p-1}$$

$j=0$

$mj+i \in (0, m-1)$

$j=1$

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

⋮

$\boxed{\text{Ex } 6.5} \Rightarrow$ Multiple solutions $\Rightarrow$ g is not a primitive element

Security of Public key cryptosystems

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

For public key enc:

$$\Pr\big(A(e(M), h(M)) = f(M)\big) < \Pr\big[B(h(M)) = f(M)\big] \boxed{+ \eta(n)}$$

A, B are efficient algorithms

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

e is the encryption algorithm

η is a negligible function

$B(h(M))$ is something you can calculate from knowledge of plaintext distribution

$\mu(n)$ is a negligible function if $\exists n_0$ s.t. $n > n_0$

$$f(n) < \frac{1}{p(n)}$$

for arbitrary polynomial $p(n)$