Tutorial 6 SK

20 October 2021 18:06

Rabinov kryptosystém
- Čínska zvyšková veta
- Kvadratické rezíduá
- Eulerovo kritérium
- Legendre a Jakobi symboly

El Gamal kryptosystém

Čínska zvyšková veta

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

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

$$N_i = N / n_i$$

$$M_i = N_i^{-1} \mod n_i \qquad x + N,\; x + 2N, \ldots$$

$$x \mod n_j$$

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

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

$$\equiv a_j \overbrace{N_j M_j}^{\equiv 1 \mod n_j} \mod n_j \quad (\text{pre všetky } i \neq j \; N_i \text{ je násobkom } n_j)$$

$$\equiv a_j \mod n_j$$

$$x \equiv 0 \mod 3$$
$$x \equiv 3 \mod 4$$
$$x \equiv 4 \mod 5$$

Kvadratické reziduá in $\mathbb{Z}_n^*$

$a \in \mathbb{Z}_n^*$ je kvadratické rezíduum až $\exists x \in \mathbb{Z}_n^*$

s.t. $x^2 \equiv a \mod n$

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

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

$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ $\quad QR_{\mod 5} = \{1, 4\}$

$1^2 \equiv 1 \mod 5$

$2^2 \equiv 4 \mod 5$

$3^2 \equiv 4 \mod 5$

$4^2 \equiv 1 \mod 5$

$x^2 \equiv a \mod p$

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

Pre prvočíslo p existuje $\frac{p-1}{2}$ QR

Eulerovo kritérium

Pre nepárne prvočíslo p a číslo a $\quad \gcd(a,p)=1$

celočíselné delenie

Legendre symbol

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \mod p \iff \text{ak } a \text{ je QR} \mod p & \left(\frac{a}{p}\right)=1 \\ & \left(\frac{a}{p}\right)=0 \\ -1 \mod p \iff \text{ak } a \text{ je QNR} \mod p & \left(\frac{a}{p}\right)=-1 \end{cases}$$

Quadratic non-residuum

Jakobiho symbol

Legendre symbol

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

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

Ako spočítať odmocninu mod p?

C je QR, nájdi x, t.ž. $\quad x^2 = c \mod p$

$$x = \sqrt{c} \mod p$$

$p \equiv 3 \pmod 4 \to$ jednoduché (budeme používať)

$p \equiv 1 \pmod 4 \to$ zložitejšie [existuje efektívny algoritmus]

celočíselné delenie

$$\sqrt{c} = \pm c^{\frac{p+1}{4}} \mod p \qquad (p \equiv 3 \pmod 4)$$

$$\sqrt{c} = \pm c^{\frac{p+1}{4}} \bmod p \qquad (p \equiv 3 \pmod 4)$$

$$c^{\frac{p-1}{2}} \equiv 1 \bmod p \text{ (Euler)}$$

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

Rabinov kryptosystém

Základné stavebné prvky: $n = p \cdot q$, p, q sú veľké prvočísla, ($p, q \equiv 3 \bmod 4$)

Verejný kľúč: n

Privátny kľúč: p, q

Zašifrovať: $1 < w \leq p-1$ $\qquad c = w^2 \bmod n$

dešifrovať: c sa dešifruje ako $w = \sqrt{c} \bmod n$

jednoduché až poznáme p a q

ťažké bez znalosti p a q

Ako dešifrovať?

$m_p \equiv \pm\sqrt{c} \mod p \qquad m_p = c^{\frac{p+1}{4}} \mod p$

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

$$\boxed{\begin{aligned} x_1 &\equiv m_p \mod p \\ x_1 &\equiv m_q \mod q \end{aligned}}$$

$x = (k \cdot p + m_p)^2 \qquad x^2 \equiv k^2 p^2 + 2 \cdot k \cdot p\, m_p + m_p^2 \mod p$

$\equiv k'p + c \mod p$

$x = l \cdot q + m_q \qquad x^2 \equiv l'q + c \mod q$

$x^2 \equiv$

$$\boxed{\begin{aligned} X_2 &\equiv -m_p \mod p \\ x_2 &\equiv m_q \mod q \end{aligned}}$$

$$\boxed{\begin{aligned} X_3 &\equiv m_p \mod p \\ x_3 &\equiv -m_q \mod q \end{aligned}}$$

$$\boxed{\begin{aligned} X_4 &\equiv -m_p \mod p \\ x_4 &\equiv -m_q \mod q \end{aligned}}$$

$\mod q$

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

$\ell'_p = \ell'_q \Rightarrow$

$x^2 \equiv m'n + c \quad \mod n$

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

$$\begin{array}{lcccccc}
 & & a_1 \; N_1 \; M_1 & & a_2 \; N_2 \; M_2 & & N \\
X_1 & = & m_p \cdot q \cdot y_q & + & m_q \cdot p \cdot y_p & & \mod n \\
X_2 & = & -m_p \cdot q \cdot y_q & + & m_q \cdot p \cdot y_p & & \mod n \\
X_3 & = & m_p \cdot q \cdot y_q & - & m_q \cdot p \cdot y_p & & \mod n \\
X_4 & = & -m_p \cdot q \cdot y_q & - & m_q \cdot p \cdot y_p & & \mod n
\end{array}$$

$\boxed{\text{Exercise 6.1}}$ dešifrujte $c = 56$

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

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

$\equiv 56^{\frac{12}{4}} \mod 11$

$\equiv 56^3 \mod 11$

$\equiv \sqrt{56}$

$\equiv 56^3 \mod 11$

$\equiv 1^3 \mod 11$

$\equiv \pm 1 \mod 11$

$m_q \equiv \sqrt{2} \equiv \sqrt{56} \mod 13$

$\equiv \sqrt{4} \mod 13$

$\equiv \pm 2 \mod 13$

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

$= 6 \mod 11$ $\qquad$ $y_p = 6 \mod 13$

$$\boxed{\begin{aligned} x_1 &= 1\cdot 6\cdot 13 + 2\cdot 6\cdot 11 \\ x_2 &= 78 - 132 \\ x_3 &= -78 + 132 \\ x_4 &= -78 - 132 \end{aligned}}$$

$= 13\cdot 6 + 22\cdot 6 \mod 143$

$78 + 132 \mod 143$

$\mod 143$

$\mod 143$

$x_1 = 67 \mod 143$

$x_1^2 = 4489 \mod 143$

$= 4489 - 56 = 4433 = 31\cdot 143$

$\Rightarrow 4489 = 56 \mod 143$

Ako zautočiť ?

1.) Faktorizovať n

2.) Viem spočítať všetky 4 odmocniny bez faktorizácie? NIE

$\gcd(x_1 + x_2, n) = p \Rightarrow$ Faktorizácia n !

Unikátne dešifrovanie

1.) nejaký pattern v plaintexte : binárnu reprezentáciu správy končí piatimi jednotkami.

m ($n-5$ bitov) $m.2^5+31$

2.)

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

$x_1 = N - x_4$

(c, J, P)

3.) Ak $N = p \cdot q$ kde $p, q \equiv 3 \pmod 4$ ak $p \neq \pm q \mod 8$, potom $\left(\frac{2}{N}\right) = -1$

$\Downarrow$

pre každé $1 \leq x < N$ presne jedno z čísel $x, N-x, 2x, N-2x$ je QR modulo N.

$p \equiv 3 \mod 8 \quad q \equiv 7 \mod 8$

potom viem správy u kódovať ako $\overset{\text{párne}}{\forall x}$, t.ž.

$\left(\frac{x}{N}\right) = 1 \Rightarrow x$ alebo $-x$ je štvorec

$$x \Rightarrow \begin{array}{l} 2(2x+1) \\ 4(2x+1) \end{array} \quad \begin{array}{l} \left(\frac{2x+1}{N}\right) = -1 \\ \left(\frac{2x+1}{N}\right) = 1 \end{array}$$

$x \rightarrow \quad 4(2x+1)$ $\quad \left(\frac{2x+1}{N}\right) = 1$

$$\left(\frac{a.b}{N}\right) = \left(\frac{a}{N}\right) \cdot \left(\frac{b}{N}\right)$$

El Gamalov kryptosystém

1.) založený na diskrétnom logaritme

2.) má randomizované šifrovanie

Základné stavebné prvky: p – veľké prvočíslo

q – primitívny prvok $\mathbb{Z}_p^*$ $\quad \{1, q, q^2, \dots, q^{p-1}\} = \mathbb{Z}_p^*$

x – tajný exponent

$$\boxed{y = q^x \bmod p}$$

Verejné: y, q, p

tajné: x

Šifrovanie správy $w \in \mathbb{Z}_p^*$

1.) Náhodne zvol $r \in \{1, \dots, p-1\}$

2.) $a = q^r \bmod p$

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

$w \to (a,b)$

Dešifrovanie (a,b)

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

r musí zostať tajné

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

r musí byť náhodné!