

Chứng minh CRT cho RSA

Đỗ Quốc Thế

January 8, 2021

1 Chứng minh CRT cho RSA

CRT: Cho $n_i \in \mathcal{P}$, $n_i \neq n_j, \forall i \neq j$, $a_i \in \mathbb{N}$. Hệ phương trình (1) có nghiệm duy nhất trong $\mathbb{Z}_{n_1 n_2 \dots n_k}$

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases} \quad (1)$$

RSA: Cho $p, q \in \mathcal{P}$, $p \neq q$, $n = pq$, $\phi = (p-1)(q-1)$, $\phi(p) = p-1$, $\phi(q) = q-1$. Chọn e sao cho $\gcd(e, \phi) = 1$, chọn d sao cho $ed \equiv 1 \pmod{\phi}$.

Encrypt: $c = m^e \pmod{n}$

Decrypt: $m = c^d \pmod{n}$

Ta có: $m \pmod{p} = (c^d \pmod{n}) \pmod{p} = c^d \pmod{p} = c^{d \pmod{\phi(p)}} \pmod{p}$

Giải thích: $d = k\phi(p) + d \pmod{\phi(p)}$

$$\begin{aligned} c^d \pmod{p} &= c^{k\phi(p)+d \pmod{\phi(p)}} \pmod{p} \\ &= (c^{\phi(p)})^k c^{d \pmod{\phi(p)}} \pmod{p} \\ &= 1^k c^{d \pmod{\phi(p)}} \pmod{p} \quad (\text{theo định lý Fermat nhỏ}) \\ &= c^{d \pmod{\phi(p)}} \pmod{p} \end{aligned}$$

Vậy ta có:

$$\begin{cases} m \equiv c^{d \pmod{\phi(p)}} \pmod{p} \\ m \equiv c^{d \pmod{\phi(q)}} \pmod{q} \end{cases} \quad (2)$$

Giải hệ CRT (2) ta được m

2 Chứng minh RSA đúng

2.1 Các bước thực hiện RSA

- (1) Chọn 2 số nguyên tố lớn p, q
- (2) Tính $n = pq$, $\phi = (p - 1)(q - 1)$
- (3) Chọn $e \in [2, \phi - 1]$ sao cho $\gcd(e, \phi) = 1$
- (4) Tìm $d \in [2, \phi - 1]$ sao cho $ed \equiv 1 \pmod{\phi}$
 d là số duy nhất cần tìm và $\gcd(d, \phi) = 1$
- (5) Công bố (e, n) là public key
- (6) Giữ (d, n) là private key

2.2 Chứng minh RSA

2.2.1 d duy nhất

2.2.2 Giải mã đúng

Ta cần chứng minh: $m = (m^e)^d \pmod{n}$

Ta có m là nghiệm duy nhất trong \mathbb{Z}_n của hệ (3) (theo chứng minh ở (2)):

$$\begin{cases} m \equiv c^d \pmod{p} \\ m \equiv c^d \pmod{q} \end{cases} \quad (3)$$

Ta cần chứng minh $m^{ed} \equiv c^d \pmod{p}$ và $m^{ed} \equiv c^d \pmod{q}$.

Thật vậy, ta có:

$$\begin{aligned} m^{ed} &\equiv m^{k\phi+1} \pmod{p} \\ &\equiv m \cdot m^{k(p-1)(q-1)} \pmod{p} \\ &\equiv m \cdot 1^{k(q-1)} \pmod{p} \quad (\text{theo định lý Fermat nhỏ}) \\ &\equiv m \pmod{p} \end{aligned}$$

Tương tự, ta có: $m^{ed} \equiv m \pmod{q}$