# Chứng minh CRT cho RSA

Đỗ Quốc Thế

January 9, 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 $\mathbb{Z}_{n_1 n_2 \ldots n_k}$

$$\begin{cases} x & \equiv a_1 \ (mod\ n_1) \\ x & \equiv a_2 \ (mod\ n_2) \\ & \vdots \\ x & \equiv a_k \ (mod\ n_k) \end{cases} \tag{1}$$

**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 $ed \equiv 1\ (mod\ \phi)$.

**Encrypt**: $c = m^e\ mod\ n$

**Decrypt**: $m = c^d\ mod\ n$

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

Giải thích: $d = k\phi(p) + d\ mod\ \phi(p)$

$$\begin{aligned} c^d\ mod\ p &= c^{k\phi(p)+d\ mod\ \phi(p)}\ mod\ p \\ &= (c^{\phi(p)})^k c^{d\ mod\ \phi(p)}\ mod\ p \\ &= 1^k c^{d\ mod\ \phi(p)}\ mod\ p \qquad \textit{(theo định lí Fermat nhỏ)} \\ &= c^{d\ mod\ \phi(p)}\ mod\ p \end{aligned}$$

Vậy ta có:

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

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 $ed \equiv 1\ (mod\ \phi)$
$d$ 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

Ta có $ed \equiv 1\ (mod\ \phi)$
Giả sử $\exists d' \neq d \in \mathbb{Z}_\phi$ sao cho $ed' \equiv 1\ (mod\ \phi)$
Ta có: $ed = k\phi + 1$, $ed' = k'\phi + 1$
$\Rightarrow\ ed - ed' = (k - k')\phi$
$\Rightarrow\ \phi \mid ed - ed'$
$\Rightarrow\ \phi \mid e(d - d')$
mà $gcd(e, \phi) = 1 \Rightarrow \phi \mid d - d'$
$\Rightarrow d \equiv d'\ (mod\ \phi)$

### 2.2.2 Giải mã đúng

Ta cần chứng minh: $m = (m^e)^d\ mod\ n$
Trước hết, ta có: Với $p, q \in \mathcal{P}$

$$\begin{cases} x & \equiv y\ (mod\ p) \\ x & \equiv y\ (mod\ q) \end{cases}$$

Thì $x \equiv y\ (mod\ pq)$
*Chứng minh*:

$$\begin{cases} x - y = kp \\ x - y = k'q \end{cases} \quad \Rightarrow \quad \begin{cases} p \mid x - y \\ q \mid x - y \end{cases}$$

mà $gcd(p, q) = 1 \Rightarrow\ pq \mid x - y$
$\Rightarrow x \equiv y\ (mod\ pq)$
Ta có:

$$\begin{aligned} (m^e)^d\ mod\ n &= m^{ed}\ mod\ n \\ &= m^{k\phi+1}\ mod\ n \\ &= m.m^{k(p-1)(q-1)}\ mod\ n \end{aligned} \tag{3}$$

Xét $x = m^{k(p-1)(q-1)}$ ta có:

$$\begin{aligned} x\ mod\ p &= m^{k(p-1)(q-1)}\ mod\ p \\ &= \left(m^{p-1}\right)^{k(q-1)}\ mod\ p \\ &= 1^{k(q-1)}\ mod\ p \qquad \textit{(theo định lí Fermat nhỏ)} \\ &= 1 \end{aligned}$$

$\Rightarrow x \equiv 1\ (mod\ p)$

$$\begin{aligned} x\ mod\ q &= m^{k(p-1)(q-1)}\ mod\ q \\ &= \left(m^{q-1}\right)^{k(p-1)}\ mod\ q \\ &= 1^{k(p-1)}\ mod\ q \qquad \textit{(theo định lí Fermat nhỏ)} \\ &= 1 \end{aligned}$$

$\Rightarrow x \equiv 1\ (mod\ q)$
Vậy ta có:

$$\begin{cases} x \equiv 1\ mod\ p \\ x \equiv 1\ mod\ q \end{cases} \quad \Rightarrow \quad x \equiv 1\ mod\ pq \quad \Rightarrow \quad x \equiv 1\ mod\ n$$

$(3) \Rightarrow (m^e)^d\ mod\ n\ = m.m^{k(p-1)(q-1)}\ mod\ n = m\ mod\ n$