Chứng minh CRT cho RSA

Đỗ Quốc Thế

January 6, 2021

CRT: Cho $n_i \in \mathcal{P},\ n_i \neq n_j, \forall i \neq j,\ a_i \in \mathbb{N}$. Hệ phương trình (3) có nghiệm duy nhất trong $\mathbb{Z}_{n_1 n_2 \dots n_k}$

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

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 thấy:
$m\ mod\ p = (c^d\ mod\ n)\ mod\ p = c^d\ mod\ p = c^{d\ mod\ \phi(p)}\ mod\ p$
$\Rightarrow m \equiv c^{d\ mod\ \phi(p)}\ (mod\ p)$
Tương tự:
$m \equiv c^{d\ mod\ \phi(q)}\ (mod\ q)$

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

$$\begin{aligned} c^d\ mod\ p &= c^{k\phi(p)+d\ mod\ \phi(p)}\ mod\ p \\ &= (c^{\phi(p)})^k c^{d\ mod\ \phi(p)}\ mod\ p \\ &= (1)^k c^{d\ mod\ \phi(p)}\ mod\ p \\ &= c^{d\ mod\ \phi(p)}\ mod\ p \end{aligned}$$

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

$$\begin{aligned} \mathcal{L}^{-1}\left\{f(d)\right\} &= \mathcal{L}^{-1}\left\{f_1(\delta) \cdot f_2(\delta)\right\} \\ &= \exp(mt) \star \left\{\tfrac{l}{2\sqrt{\pi t^3}} \exp(-l^2/4t)\right\} \\ &= F_1 * F_2 \end{aligned}$$

Tìm nghiệm của hệ pt:

$$\begin{cases} x & \equiv a \ (mod \ p) \\ x & \equiv b \ (mod \ q) \end{cases} \tag{3}$$

với $p, q \in \mathcal{P}$

Vì $p, q \in \mathcal{P} \Rightarrow \exists p' \equiv p^{-1} \ (mod \ q), \ \exists q' \equiv q^{-1} \ (mod \ p)$

Đặt $y = aq'q + bp'p$, ta thấy: $y \equiv a \ (mod \ p)$ và $y \equiv b \ (mod \ q)$
$\Rightarrow y$ là nghiệm duy nhất của (3) trong $\mathbb{Z}_{pq}$