Public Key Cryptography

1 Chinese Remainder Theorem (CRT)

Bézout's Identity

Lemma. $a, b \in \mathbb{Z} \implies \exists x, y \in \mathbb{Z} : \gcd(a, b) = ax + by.$

Chinese Remainder Theorem (CRT)

Theorem. *Given a system of k linear congruences:*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

where $m_1, m_2, \ldots, m_k$ are pairwise coprime. Let $M = \prod_{i=1}^{k} m_i$. Then, the unique solution of the system of congruences is given by

$$\begin{aligned} X &\equiv \sum_{i=1}^{k} a_i M_i b_i \pmod{M} \\ &\equiv a_1 M_1 b_1 + a_2 M_2 b_2 + \cdots + a_k M_k b_k \pmod{M}. \end{aligned}$$

where $M_i = M/m_i$ and $b_i \equiv M_i^{-1} \pmod{m_i}$.

Proof. (Existence) Define

$$\begin{aligned} M &:= \prod_{i=1}^{k} m_i = m_1 m_2 \cdots m_k \quad \text{and} \\ M_i &:= \frac{M}{m_i} = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k. \end{aligned}$$

By Bézout's identity, we know that

$$\exists b_i, c_i \in \mathbb{Z} : M_i b_i + m_i c_i = \gcd(M_i, m_i) = 1.$$

because M_i has not m_i as factor. Note that

(1) $M_i b_i + m_i c_i = 1 \Leftrightarrow M_i b_i = (-c_i) m_i + 1 \Leftrightarrow M_1 b_i \equiv 1 \pmod{m_i}$.

(2) Let $i, j \in \{1, 2, \cdots, k\}$ with $i \neq j$. Then

$$\begin{aligned} \gcd(m_i, m_j) = 1 &\implies m_j \in \{m_1, m_2, \cdots, m_{i-1}, m_{i+1}, \cdots, m_k\} \\ &\implies m_j \mid M_i \quad \because M_i = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_k \\ &\implies m_j \mid M_i - 0 \\ &\implies M_i \equiv 0 \pmod{m_j}. \end{aligned}$$

Thus, we have

$$\begin{cases} M_i b_i \equiv 1 \pmod{m_i} & \cdots\cdots(1) \\ M_i b_i \equiv 0 \pmod{m_j} \text{ for } j \neq i & \cdots\cdots(2). \end{cases}$$

Then we claim that $X = \sum_{i=1}^{k} a_i M_i b_i$ is a solution to the system of linear congruences:

$$\begin{aligned} X - a_i = \left(\sum_{j=1}^{k} a_j M_j b_j \right) - a_i = \sum_{\substack{j=1 \\ j \neq i}}^{k} a_j M_j b_j + a_i M_i b_i - a_i = \sum_{j=1, j\neq i}^{k} a_j M_j b_j + a_i (M_i b_i - 1) \\ \equiv \left[\sum_{j=1, j\neq i}^{k} a_j \cdot \left(\cancelto{0}{M_j b_j} \right) \right] + a_i (M_i b_i - 1) \pmod{m_i} \quad \text{by (2)} \\ \equiv a_i \cancelto{0}{(M_i b_i - 1)} \pmod{m_i} \quad \text{by (1)} \\ \equiv 0 \pmod{m_i}. \end{aligned}$$

Therefore, we have:

$$X - a_i \equiv 0 \pmod{m_i}$$

Hence X satisfies all of the linear congruence.

(Uniqueness) Let X_0, X_1 are roots of the system of linear equations. Let $1 \leq i \leq k$. Then

$$X_0 \equiv a_i \equiv X_1 \pmod{m_i}$$

and so

$$m_i \mid X_0 - X_1.$$

Hence $m_1 m_2 \cdots m_k \mid X_0 - X_1$, i.e.,

$$X_1 \equiv X_2 \pmod{M = m_1 m_2 \cdots m_k}.$$

□

2 Special Case of CRT

CRT - Special Case

Corollary. *Consider a system of two linear congruences:*

$$\begin{aligned} x &\equiv a_1 \pmod{p} \\ x &\equiv a_2 \pmod{q} \end{aligned}$$

where p, q are coprime. Let $N = pq$. Then, the unique solution of the system of congruences is given by

$$\boxed{x = a_1 q q_p^{-1} + a_2 p p_q^{-1} \mod N}$$

where $q_p^{-1} = q^{-1} \mod p$ and $p_q^{-1} = p^{-1} \mod q$.

Remark 1. Recall that Bézout's identity : $a, b \in \mathbb{Z} \implies \exists x, y \in \mathbb{Z} : \gcd(a,b) = ax + by$. Especially,

$$p, q \text{ are coprime} \implies \exists x, y \in \mathbb{Z} : px + qy = 1.$$

Since p, q are coprime, we know that $\exists x, y \in \mathbb{Z} : px + qy = 1$ and so

$$px = (-y)q + 1 \implies px \equiv 1 \pmod{q} \implies x = p^{-1} \mod q.$$

Similarly, $y = q^{-1} \mod p$. Thus we have $px + qy = 1 \implies pp_q^{-1} + qq_p^{-1} = 1$. Consequently,

$$\boxed{x = a_1 qq_p^{-1} + a_2 pp_q^{-1} \mod N} \implies x = a_1 qq_p^{-1} + a_2(1 - qq_p^{-1}) \mod N$$
$$\implies \boxed{x = (a_1 - a_2)qq_p^{-1} + a_2 \mod N}.$$

3 RSA-CRT Algorithm

Algorithm 1: RSA-CRT Algorithm

Data: The security parameter k, a public key (N, e), a ciphertext C.
Result: The plaintext message $\mathcal{M}$ corresponding to the ciphertext C.

```
/* Key Generation                                                    */
Function KeyGen (1^k):
    p, q ← random prime numbers of k/2 bits each ;        // Generate two primes
    N ← pq ;                                              // Compute modulus
    φ(N) ← (p − 1)(q − 1) ;                               // Compute Euler's phi function
    e ← integer e ∈ (1, φ(N)) s.t. gcd(e, φ(N)) = 1 ;     // Choose encryption exponent
    d ← integer d ∈ (1, φ(N)) s.t. ed ≡ 1 (mod φ(N)) ;    // Compute decryption exponent
    d_p ← d mod p − 1 ;                                   // Compute decryption exponent for p
    d_q ← d mod q − 1 ;                                   // Compute decryption exponent for q
    q_inv ← integer q_inv ∈ (1, p − 1) s.t. q q_inv ≡ 1 (mod p) ;  // Compute q inverse modulo p
    Set the RSA public key as (N, e);
    Set the RSA secret key as (p, q, d_p, d_q, q_inv);
End Function

/* Encryption                                                        */
Function Enc (N, e, M):
    C ← M^e mod N ;                                       // Encrypt with e and N
End Function

/* Decryption                                                        */
Function Dec (C):
    m_1 ← C^(d_p) mod p ;                                 // Decrypt with d_p and p
    m_2 ← C^(d_q) mod q ;                                 // Decrypt with d_q and q
    m ← (m_1 − m_2) q q_inv + m_2 mod N ;                 // m = (m_1 − m_2) q q_inv + m_2 mod N
    return m;
End Function
```

Proof of Decryption. Note that

$$\begin{aligned} ed \equiv 1 \pmod{(p-1)(q-1)} &\implies \exists k \in \mathbb{Z} : ed = 1 + k(p-1)(q-1), \\ d_p = d \mod p-1 &\implies \exists k_p \in \mathbb{Z} : d = (p-1)k_p + d_p. \end{aligned}$$

Consider $m_1 := \mathcal{C}^{d_p} \mod p$. From $\mathcal{C} = \mathcal{M}^e \mod pq$, we have

$$\begin{aligned} \mathcal{C} \equiv \mathcal{M}^e \pmod{pq} \Leftrightarrow pq \mid \mathcal{C} - \mathcal{M}^e &\Leftrightarrow \mathcal{C} - \mathcal{M}^e = k_N \cdot pq \text{ for some } k_N \in \mathbb{Z} \\ &\Leftrightarrow \mathcal{C} - \mathcal{M}^e = (k_N q) \cdot p \\ &\Leftrightarrow p \mid \mathcal{C} - \mathcal{M}^e \\ &\Leftrightarrow \boxed{\mathcal{C} \equiv \mathcal{M}^e \pmod{p}}. \end{aligned}$$

Then

$$m_1 = \mathcal{C}^{d_p} \mod p = (\mathcal{M}^e)^{d-(p-1)k_p} \mod p = \left(\mathcal{M}^{ed}\right) \cdot \mathcal{M}^{-e(p-1)k_p} \mod p.$$

Clearly, either $\gcd(\mathcal{M}, p) = 1$ or $\gcd(\mathcal{M}, p) \neq 1$:

(Case I) Let $\gcd(\mathcal{M}, p) = 1$. By Fermat's little theorem, we get

$$\mathcal{M}^{-e(p-1)k_p} = \left(\mathcal{M}^{p-1}\right)^{-ek_p} \equiv 1^{-ek_p} = 1 \pmod{p}.$$

Thus,

$$\begin{aligned} m_1 = \mathcal{C}^{d_p} \mod p &= \left(\mathcal{M}^{ed}\right) \cdot \cancelto{1}{\mathcal{M}^{-e(p-1)k_p}} \mod p \quad \text{by FLT} \\ &\equiv \mathcal{M}^{k(p-1)(q-1)+1} \pmod{p} \\ &\equiv \left(\cancelto{1}{\mathcal{M}^{p-1}}\right)^{k(q-1)} \cdot \mathcal{M} \pmod{p} \quad \text{by FLT} \\ &\equiv \mathcal{M} \pmod{p}. \end{aligned}$$

That is, $m_1 \equiv \mathcal{M} \pmod{p}$.

(Case II) Let $\gcd(\mathcal{M}, p) \neq 1$, i.e., $\exists l \in \mathbb{Z} : \mathcal{M} = pl$ since p is a primes[a]. Then we have

$$\mathcal{M} = pl \implies p \mid \mathcal{M} - 0 \implies \mathcal{M} \equiv 0 \pmod{p}.$$

Recall that $\boxed{\mathcal{C} \equiv \mathcal{M}^e \pmod{p}}$. Then $\mathcal{C} \equiv \mathcal{M}^e \equiv 0^e = 0 \pmod{p}$ and so

$$m_1 = \mathcal{C}^{d_p} \mod p = 0^{d_p} \mod p = 0 \mod p = 0.$$

That is, $m_1 \equiv 0 \pmod{p}$. Therefore

$$\begin{cases} \mathcal{M} \equiv 0 \pmod{p} \\ m_1 \equiv 0 \pmod{p} \end{cases} \implies m_1 \equiv \mathcal{M} \pmod{p}.$$

[a]Since p is a prime, p has factors 1 and p only. Then $\gcd(\mathcal{M}, p) \neq 1$ means that p is only common factor.

Here, we obtain $m_1 \equiv \mathcal{M} \pmod{p}$. Similarly, we have $m_2 \equiv \mathcal{M} \pmod{q}$. Then, the plaintext message $\mathcal{M}$ is a solution to the following system of two linear congruences:

$$\begin{aligned} \mathcal{M} &\equiv m_1 \pmod{p}, \\ \mathcal{M} &\equiv m_2 \pmod{q}. \end{aligned}$$

Then, **Remark 1** guarantees that

$$\mathcal{M} = (m_1 - m_2)qq_{inv} + m_2 \mod pq.$$

$\square$

Department of Information Security, Cryptography and Mathematics, Kookmin University