Correctness Proof of RSA

Yufei Tao

Department of Computer Science and Engineering
Chinese University of Hong Kong

The previous lecture, we have learned the algorithm of using a pair of private and public keys to encrypt and decrypt a message. In this lecture, we will complete the discussion by proving the algorithm's correctness.

We will need some definitions and theorems from number theory.

Definition

Given an integer $p > 0$, define $\mathbb{Z}_p$ as the set $\{0, 1, ..., p-1\}$.

If $a = b \pmod{p}$, then all the following hold for any integer $c \geq 0$:

$$\begin{aligned} a + c &= b + c \pmod{p} \\ a - c &= b - c \pmod{p} \\ ac &= bc \pmod{p} \\ a^c &= b^c \pmod{p} \end{aligned}$$

Theorem

Let a, p be two integers that are co-prime to each other. Then, there is only a unique integer $x \in \mathbb{Z}_p$ satisfying

$$ax = b \pmod{p}$$

regardless of the value of b.

The proof is elementary and left to you.

Example: In $\mathbb{Z}_8$, $3x = 2$ has a unique $x = 6$.

Corollary

If a and p are co-prime to each other, then 0, a, $2a$, ..., $(p-1)a$ are all distinct after modulo p.

Theorem (Fermat's Little Theorem)

If p is a prime number, for any non-zero $a \in \mathbb{Z}_p$, it holds that $a^{p-1} = 1 \pmod{p}$.

Example: In $\mathbb{Z}_5$, $1^4 = 1 \pmod{p}$, $2^4 = 1 \pmod{p}$, $3^4 = 1 \pmod{p}$, and $4^4 = 1 \pmod{p}$.

Proof.

By the corollary in Slide 4, we know that $a, 2a, ..., (p-1)a$ after modulo p have a one-one correspondence to the values in $\{1, 2, ..., p-1\}$. Therefore:

$$\begin{aligned} a \cdot 2a \cdot ... \cdot (p-1)a &= (p-1)! \pmod{p}. \\ \Rightarrow a^{p-1}(p-1)! &= (p-1)! \pmod{p}. \end{aligned}$$

The above implies $a^{p-1} = 1 \pmod{p}$. $\square$

Theorem (Chinese Remainder Theorem)

Let p and q be two co-prime integers. If $x = a \pmod{p}$ and $x = a \pmod{q}$, then $x = a \pmod{pq}$.

Example: Since 37 = 2 (mod 5) and 37 = 2 (mod 7), we know that 37 = 2 (mod 35).

Proof.

Let $b = x$ (mod pq). We will prove $b = a$. Note that $b < pq$.

First observe that because $x = a$ (mod p), we know $b = a$ (mod p). Similarly, $b = a$ (mod q). Hence, we can write $b = pt_1 + a = qt_2 + a$ for some integers t_1, t_2. This means that $pt_1 = qt_2$, and they are a common multiple of p and q. However, as p and q are co-prime, the smallest non-zero common multiple of p and q is pq. Given the fact that $b < pq$. we conclude that $pt_1 = qt_2 = 0$. □

Review: RSA Preparation

Bob carries out the following:

1. Choose two large prime numbers p and q randomly.
2. Let $n = pq$.
3. Let $\phi = (p-1)(q-1)$.
4. Choose a large number $e \in [2, \phi - 1]$ that is co-prime to ϕ.
5. Compute $d \in [2, \phi - 1]$ such that

$$e \cdot d = 1 \pmod{\phi}$$

   There is a unique such d. Furthermore, d must be co-prime to ϕ.

6. Announce to the whole word the pair (e, n), which is his public key.
7. Keep the pair (d, n) secret to himself, which is his private key.

We now prove the statement at line 5 of the previous slide:

- There is a unique such d.

Proof.

Follows directly from the theorem in Slide 4. □

- d must be co-prime to ϕ.

Proof.

Let t be the greatest common divisor of d and ϕ, and suppose $d = c_1 t$ and $\phi = c_2 t$. From $ed = 1 \pmod{\phi}$, we know $ed = c_3\phi + 1$ for some integer c_3. Hence:

$$\begin{aligned} ec_1 t &= c_3 c_2 t + 1 \\ \Rightarrow t(ec_1 - c_3 c_2) &= 1 \end{aligned}$$

which implies $t = 1$. □

Encryption: Knowing the public key (e, n) of Bob, Alice wants to send a message $m \leq n$ to Bob. She converts m to C as follows:

$$C = m^e \pmod{n}$$

Decryption: Using his private key (d, n), Bob recovers m from C as follows:

$$C^d \pmod{n}$$

Theorem (RSA's Correctness)

$m = C^d \pmod{n}$.

Proof.

It suffices to prove $m = C^d \pmod{p}$ and $m = C^d \pmod{q}$, because they lead to $m = C^d \pmod{n}$ by the Chinese Remainder Theorem.

First, we prove $m = C^d \pmod{p}$. From $C = m^e \pmod{n}$, we know $C = m^e \pmod{p}$, and hence, $C^d = m^{ed} \pmod{p}$. As $ed = 1 \pmod{(p-1)(q-1)}$, we know that $ed = t(p-1)(q-1) + 1$ for some integer t. Therefore:

$$\begin{aligned} m^{ed} &= m \cdot m^{t(p-1)(q-1)} \pmod{p} \\ &= m \cdot (m^{(p-1)})^{t(q-1)} \pmod{p} \\ \text{(Fermat's Little Theorem)} \quad &= m \cdot (1)^{t(q-1)} \pmod{p} \\ &= m \pmod{p} \end{aligned}$$

By symmetry, we also have $m^{ed} = m \pmod{q}$. $\square$