RSA Encryption Notes

Dr. J. K. Denny

December 1, 2021

Introduction

In 1977, the RSA encryption algorithm[1] was created by Ron Rivest, Adi Shamir, and Leonard Adleman (R.S.A.) at MIT. The algorithm depends on having two "keys" – one is a public key and one is a private key – that are based on large prime numbers. The algorithm works as follows.

- Bob wants to send Alice a secret message.
  1. Alice shares her public key (n, e) with Bob but never shares her private key, d.
  2. Bob converts his message into an integer M with $0 \leq M < n$.
  3. Then, Bob encodes M using Alice's public key, e, to get the ciphertext, C.
  4. Finally, Bob sends the encoded message to Alice.
- Now, Alice wants to decode Bob's message, C.
  1. Alice decodes the message C using her private key, d, to recover the message M.
  2. Alice converts the integer M back to plain text characters and reads the message.
- Note that if someone, say Eve, knows the public key, (n, e), and the encoded message, C, Eve won't be able to decode the message without d, the private key that only Alice has.

[1] You can obtain their original paper at https://people.csail.mit.edu/rivest/Rsapaper.pdf

The key breakthrough in the RSA cryptosystem is that Bob can encode a message using a publicly available key while knowing that no one can decode the message without having Alice's private key. (This is similar to Bob being able to lock a treasure chest with a key that anyone can have, but only Alice can open the treasure chest with her private key.)

The RSA algorithm depends heavily on the use of two large prime numbers, p, q, that are used to create $n = pq$. Currently, factoring a very, very large number into two extremely large primes is an incredibly difficult problem, which provides the security needed for the system to work.

1 How to do it

Suppose we have two large primes, p and q, and let $n = pq$.

1. Let $b = \text{lcm}(p-1, q-1)$.
2. Choose our encoding exponent, e, so that $\gcd(e, b) = 1$.
3. Take d to be the smallest positive integer that solves $ex \equiv 1 \mod b$.

- Encrypt
    1. If your message is an integer M, then encrypt the message by computing $C = M^e \mod n$.
- Decrypt
    1. To decode the encrypted message C, compute $M = C^d \mod n$.

Examples

Example 1

Let $p = 17, q = 29$ and then $n = 493$. Now $b = 112$. Let $e = 17$ so that $gcd(e, b) = 1$. Then, we get $d = 33$.

To encode the message $M = 123$, we compute

$$C = M^e = 123^{17} \mod 493 \equiv 140.$$

To decode, we compute

$$C^d = 140^{33} \mod 493 \equiv 123.$$

Example 2

Take $p = 3931, q = 2297$. Then, $n = 9029507$ and $b = 4511640$. If we take $e = 1049$, then we get $d = 331169$.

To encode the message $M = 1000$, we compute

$$C = M^e = 1000^{1049} \mod 9029507 \equiv 6162871.$$

To decode, we compute

$$C^d = 6162871^{331169} \mod 9029507 \equiv 1000.$$

2 Why it works

Theorem 2.1

If $a, b, d, n \in \mathbb{Z}^+$ and $d \mid n$ and $a \equiv b \pmod{n}$, then $a \equiv b \pmod{d}$.

Proof 2.1

Suppose $a, b, d, n \in \mathbb{Z}^+$ and $d \mid n$ and $a \equiv b \pmod{n}$. Then, $n \mid (a - b)$. Thus, there is an integer k so that $a - b = nk$. But, also, $d \mid n$. So, there is an integer l so that $n = dl$. Thus,

$$a - b = nk = d(lk).$$

So, $d \mid (a - b)$ and we have $a \equiv b \pmod{d}$.

Theorem 2.2

For positive integers n, e, the integer e has a multiplicative inverse modulo n iff $\gcd(n, e) = 1$.

Proof 2.2

Let n, e be positive integers. First suppose e has a multiplicative inverse modulo n. Call it d. Then, $d \cdot e \equiv 1 \mod n$. Thus, $n \mid (de-1)$. So, there is an integer k so that $de - 1 = nk$. This gives $n(-k) + de = 1$. Since any common divisor of n and e must divide both sides of this equation, we know the $\gcd(n, e)$ is 1.

Next, suppose $\gcd(n, e) = 1$. Then, there are integers s, d so that $ns + ed = 1$. Rewriting gives $ns = 1 - ed$ and so $n \mid (1 - ed)$. Hence, $e \cdot d \equiv 1 \mod n$.

Theorem 2.3: Fermat's Little Theorem (Fermat, 1640)

If p is prime and does not divide integer a, $a^{p-1} \equiv 1 \pmod{p}$.

Proof 2.3

Suppose p is prime and p does not divide $a \in \mathbb{Z}$. Now, we list the first $p - 1$ positive multiples of a:

$$a, 2a, 3a, \ldots, (p-1)a$$

Next, we show that the elements on this list are distinct.

Suppose that ra and sa are the same modulo p for some integers r, s. That is, $ra \equiv sa \pmod{p}$. Since $p \nmid a$, then a has a multiplicative inverse, b, modulo p. So, we can multiply by b and obtain $r \equiv s \pmod{p}$.

We conclude that the $p-1$ multiples of a listed above are distinct and nonzero. Working $\mod p$, the only possible values are $0, 1, 2, \ldots, p-1$. Since there are $p - 1$ distinct values on our list, they must be congruent

to $1, 2, 3, \ldots, p-1$ in some order. Thus,

$$a \cdot 2a \cdot 3a \cdots (p-1)a = 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

Note that since $p \nmid a$ and p is prime, the product on the left is nonzero modulo p.

Equivalently, we can write:

$$a^{p-1}(p-1)! = (p-1)! \pmod{p}.$$

Dividing by $(p-1)!$ gives $a^{p-1} = 1 \pmod{p}$.

Side note:

Fermat's Little Theorem is often used when hunting for prime numbers. Imagine that p is an integer that you think might be prime. Then, check $a^{p-1} \pmod{p}$ for lots of integers a that are not divisible by p. If you get $a^{p-1} \pmod{p} \equiv 1$ in all cases, the number *might* be prime and deserves further inspection. If you find just one a so that $a^{p-1} \pmod{p} \not\equiv 1$, then p is not a prime.

For example, consider $p = 119$. Then, begin checking:

$$2^{119-1} \equiv 30 \pmod{119}$$

So, we know 119 is not prime.

Consider $p = 127$. Then, begin checking:

$$\begin{aligned} 2^{127-1} &\equiv 1 \pmod{127} \\ 3^{127-1} &\equiv 1 \pmod{127} \\ 4^{127-1} &\equiv 1 \pmod{127} \\ 5^{127-1} &\equiv 1 \pmod{127} \\ 6^{127-1} &\equiv 1 \pmod{127} \end{aligned}$$

So, we know 127 *might* be prime and warrants further investigation.

Theorem 2.4: Chinese Remainder Theorem (Sunzi, 300 AD)

Let p and q be relatively prime integers greater than 1. If a is a positive integer so that $x \equiv a \pmod{p}$ and $x \equiv a \pmod{q}$, then $x \equiv a \pmod{pq}$.

Proof 2.4

Suppose $p, q > 1$ are relatively prime integers, a$\in \mathbb{Z}^+$,x $\equiv a \pmod{p}$, and $x \equiv a \pmod{q}$.

Now, let b be an integer such that $x \equiv b \pmod{pq}$. We want to prove $b = a$. Note that $b < pq$.

First, we prove $b \equiv a \pmod{p}$. Since $b \equiv x \pmod{pq}$, we have $pq \mid (b - x)$. So, $(b - x) = pqk$ for some integer k. Also, because $x \equiv a \pmod{p}$, we know $x - a = pl$ for some integer l. Adding these gives

$$b - a = pqk + pl = p(qk + l).$$

Thus, $p \mid (b - a)$ and so $b \equiv a \pmod{p}$. Similarly, we can prove $b \equiv a \pmod{q}$.

With these known, we can write $b = pt_1 + a = qt_2 + a$ for some integers t_1, t_2. This means $pt_1 = qt_2$. So, $p \mid qt_2$ and p, q relatively prime combine to give $p \mid t_2$. Similarly, $q \mid pt_1$ means that $q \mid t_1$. Thus, there are integers s_1, s_2 so that $t_1 = qs_1$ and $t_2 = ps_2$.

Importantly now, $pt_1 = qt_2$ means that $pqs_1 = pqs_2$. So, $s_1 = s_2$.

But, $pt_1 = pqs_1 < pt_1 + a = b < pq$ and $qt_2 = pqs_2 < qt_2 + a = b < pq$. Then, dividing out pq gives $s_1 < 1$ and $s_2 < 1$. So, $0 \leq s_1^2 < 1$ and $0 \leq s_2^2 < 1$. This is only possible if $s_1 = s_2 = 0$. So, $pt_1 = qt_2 = 0$ and hence $b = a$.

Example:

- (non-example) $37 \equiv 1 \pmod{4}$ and $37 \equiv 1 \pmod{6}$ but $37 \equiv 13 \pmod{24}$. (Problem:$\gcd(4, 6) = 2 \neq 1$. So, the hypotheses are not satisfied.)
- $7 \equiv 1 \pmod{2}$ and $7 \equiv 1 \pmod{3}$ and so $7 \equiv 1 \pmod{6}$.

Theorem 2.5: RSA algorithm (Rivest, Shamir, Adleman, 1977)

Let p and q be primes, and set $n = pq$ and $b = \text{lcm}(p-1, q-1)$. Suppose $M \in \mathbb{Z}^+$ is a message with $0 \leq M < n$. Take $e \in \mathbb{Z}^+$ so that $\gcd(b, e) = 1$. Finally, let d be the smallest integer that solves $e \cdot x \equiv 1 \pmod{b}$. Then,

$$(M^e)^d \pmod{n} \equiv M.$$

Proof 2.5

Let $C = M^e \pmod{n}$ be the encoded message. The Chinese Remainder Theorem says that if $M = C^d \pmod{p}$ and $M = C^d \pmod{q}$, then $M = C^d \pmod{n}$. So, we will prove that $M = C^d \pmod{p}$ and $M = C^d \pmod{q}$.

First, we prove $M = C^d \pmod{p}$. Since $C = M^e \pmod{n}$ and $p \mid n$, we know $C = M^e \pmod{p}$. So, $C^d = m^{ed} \pmod{p}$. Since $ed \equiv 1 \pmod{b}$, there is an integer k so that $ed = kb + 1$. Moreover, $(p-1)(q-1) \mid b$, so we know that $ed = kt(p-1)(q-1) + 1$ for some integer t.

Now, either $p \mid M$ or $p \nmid M$. If $p \mid M$, then $M \equiv 0 \pmod{p}$. So, $M^{ed} \equiv M \pmod{p}$ is true. If $p \nmid M$, then Fermat's Little Theorem says that $M^{(p-1)} \equiv 1 \pmod{p}$ and we compute the following:

$$\begin{aligned} M^{ed} &\equiv M \cdot M^{kt(p-1)(q-1)} \pmod{p} \\ &\equiv M \cdot \left(M^{(p-1)}\right)^{kt(q-1)} \pmod{p} \\ \text{(Fermat's Little Theorem)} \quad &\equiv M \cdot (1)^{kt(q-1)} \pmod{p} \\ &\equiv M \pmod{p} \end{aligned}$$

By a similar argument, we also get $M^{ed} \equiv M \pmod{q}$. Thus, the Chinese Remainder Theorem says that $C^d = M^{ed} \equiv M \pmod{n}$.