Ricardo Reyes Carmona

Understanding the Mathematics behind RSA

To understand RSA, we must first cover the mathematical concepts used to allow for such an encryption system.

The foundation of RSA is built on a mathematical system called modular arithmetic. Modular Arithmetic allows mathematicians to observe patterns in the remainders when dividing integers. To start off let us observe a few examples of modular arithmetic.

Example 1

$$\begin{aligned} 13 &\mod 9 = 4 \\ 7 &\mod 9 = 7 \\ 27 &\mod 9 = 0 \end{aligned}$$

To demonstrate why these equations are true we should also look at:

Example 2

$$\begin{aligned} 13 &= 9 \cdot 1 + 4 \\ 7 &= 9 \cdot 0 + 7 \\ 27 &= 9 \cdot 3 + 0 \end{aligned}$$

After looking at this new set of equations we can see that the remainder is the key takeaway in modular arithmetic. In fact, another way to write Example 1 is:

$$\begin{aligned} 13 &\equiv 4 \mod 9 \\ 7 &\equiv 7 \mod 9 \\ 27 &\equiv 0 \mod 9 \end{aligned}$$

Now using Example 2 we can create a relationship:

$$a \equiv b \mod n \implies a = n \cdot k + b, k \epsilon \mathbb{Z}$$

Since we have covered the basics of Modular Arithmetic, we will now look at Modular Arithmetic Tables. Figure 1a is the Modular Arithmetic Table for Addition Mod Base 4 and Figure 1b is the Modular Arithmetic Table for Addition Mod Base 5.

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

(a) Module 4

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(b) Module 5

Figure 1: Modular Arithmetic Addition Tables

Just like we can create Modular Arithmetic Table for Addition, we can also create Modular Arithmetic Table for Multiplication.Figure 2a is the Modular Arithmetic Table for Multiplication Mod Base 4 and Figure 2b is the Modular Arithmetic Table for Multiplication Mod Base 5.

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(a) Module 4

$\otimes$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(b) Module 5

Figure 2: Modular Arithmetic Multiplication Tables

Since we have established these tables, we should now establish a new equation which can be applied using the Modular Arithmetic Table for Multiplication.

$$d \equiv \frac{1}{e} \mod n$$

or

$$d \cdot e \equiv 1 \mod n$$

If we were to visualize this in our Modular Arithmetic Table for Multiplication Mod Base 5, we should be able to go to column e and find a 1 in that column at row d. If we are not

able to do so then this statement is not valid. If we plot more Modular Arithmetic Tables for Multiplication then we would see that this specific statement is only valid when:

$$e \, \epsilon \, \phi(n) \;\; s.t. \;\; gcd(e, n) = 1$$

Just like how we can create Modular Arithmetic Tables for Multiplication, we can do a similar process for exponential ideas to find the smallest value for k such that:

$$a^k \equiv 1 \mod n$$

For the sake of length I will save us the need to write out many examples and instead explain to you mathematically how to find the smallest value for k to satisfy the statement. To begin we must cover Fermat's Little Theorem. Fermat's Little Theorem states that if p is a prime number, then for any integer a, $a^p - a$ is an integer multiple of p. Since we have covered modular arithmetic we can denote it as:

$$a^p \equiv a \mod p$$

Fermat's Little Theorem actually goes a further step and says that if $p \nmid a$ (a is not divisible by p), $a^{p-1} - 1$ is a multiple of p. In modular arithmetic notation this can be written as follows:

$$a^{p-1} \equiv 1 \mod p$$

We must also understand the Fundamental Theorem of Arithmetic. The Fundamental Theorem of Arithmetic states that every composite number greater than 1 has its own unique prime factorization(can be written out as a product of primes). This will become a vital piece of information for finding the smallest value of k. If we were do testing for small values of n we would find that all of the specific values of k have a least common multiple.This least common multiple can be found by breaking down n into its prime factorization. Ultimately, you can form the following conjecture:

$$a^k \equiv 1 \mod n$$

$$n = p_1 \cdot p_2 \cdot p_3 ..... \cdot p_n$$

$$k = LCM(p_1 - 1, p_2 - 1, p_3 - 1, ..., p_n - 1)$$

As you can see this is using the principle from Fermat's Little Theorem such that k is the Least Common Multiple of all the specific prime factors minus one of n. This concludes the general mathematics needed to perform RSA so now we will go through the process of performing RSA.

Process of RSA

RSA is a public-key cryptosystem used for for secure data transmission. While we go through the process it will hopefully become clear why RSA is so secure.

For this scenario let us say that Friend 1 wants to send a message to Friend 2. Friend 1 wants to say "Mathematics is the queen of sciences, and number theory is the queen of mathematics." to Friend 2. So:

$$\text{message} = \text{"Gauss was a genius!"}$$

Now that we have our message we need to convert it into a number sequence. We can use the American Standard Code for Information Interchange (ASCII). Converted our message becomes:

$$m = 071097117115115032119097115032097032103101110105117115033$$

Now Friend 2 must generate a key using the mathematics we have learned. First Friend 2 must chose two large distinct prime numbers. We can denote these primes as p and q. Friend 2 must find n such that $n = p \cdot q$. To cover:

$$p = \text{prime number 1}$$
$$q = \text{prime number 2}$$
$$n = p \cdot q$$

Friend 2 must also find the LCM of $(p-1)$ and $(q-1)$. In the real world this can be done through computing. We can denote the LCM as k.

$$k = LCM \text{ of } (p-1) \text{ and } (q-1)$$

Friend 2 will now have to pick a new value, e such that:

$$d \cdot e \equiv 1 \mod k$$

Friend 2 does this first by picking a value e such that gcd of e and k is one. Then through the help of a computer, Friend 2 is able to find the specific value d. This value d is the private key component.

Now Friend 2 can send the public key to Friend 1, which are n and e. Friend 2 will keep the value d private. Friend 1 can now send the message. Friend 1 will send the $m^e \mod n$ or c to Friend 2.

$$m^e \equiv c \mod n$$

Friend 2 can decrypt the message by raising c to the power of his private key,d, in mod n.

This is the beauty of RSA. The real magic of why it is very secure is because of Friend 2's choice in picking the prime numbers. In the real world, those prime numbers are humongous. Therefore that prime factorization for n is going to be very hard for another individual to crack. Making RSA a very secure way to transfer data.