Advances in Computer, Signals and Systems (2021) 5: 95-97
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2021.050115
ISSN 2371-8838

A Brief Introduction to RSA Encryption

Shengning Zhang

The Experimental High School Attached To Beijing Normal University, Beijing, China
leo176637@163.com

Keywords: RSA Encryption, Reliability, Algorithm, Number theory

Abstract: RSA encryption is commonly used in the modern world now and we will make a brief introduction on this particular encryption method in this paper. We will focus on how RSA encryption works and why this encryption method is reliable.

1. Introduction

[2]RSA (Rivest–Shamir–Adleman) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym RSA comes from the surnames of Ron Rivest, Adi Shamir and Leonard Adleman, who publicly described the algorithm in 1977.

In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.

The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the ”factoring problem”. Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem is an open question. There are no published methods to defeat the system if a large enough key is used.

2. Basic Knowledge

In order to find out what RSA encryption truly is, we need to have a look on some basic number theory knowledge. The proof of all the following theorems can be found in [1] or any other book about elementary number theory and thus we will not discuss about them in this article.

2.1. Euler's Totient Function $\phi(n)$

For every positive integer n, we define ϕ(n) as the number of positive integers that are no more than n and are relatively prime to n.

For n $\in$ Z^+(n $\geqslant$ 2), by considering the prime factorization of n where $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, we have

$$\varphi(n) = \prod_{i=1}^{k} p_i^{\alpha_i}(1 - \frac{1}{p_i}) = n\prod_{i=1}^{k}(1 - \frac{1}{p_i})$$

This formula can help us calculate $\phi(n)$ for every given n.

If p is a prime number, then we have $\phi(p) = p - 1$.

2.2. Euler's Theorem

For $n \in Z^+ (n \geq 2)$, $a \in Z^+$, if $gcd(a,n) = 1$, or in the other words, a and n are relatively prime, then we have $a^{\phi(n)} \equiv 1 (\mod n)$.

2.3. Some key conclusions related to Euler's Theorem.

- (Fermat's Little Theorem)For $a \in Z_+$ and prime number p, if $gcd(a,p) = 1$, then we have $a^{p-1} \equiv 1 (\mod p)$
- $\forall h,m,n \in Z_+ (n \geq 2), m^{h\phi(n)+1} \equiv m (\mod n)$
- For $a,n \in Z_+$, if $gcd(a,n) = 1$, then there exists $b \in Z^+$ that satisfies $ab \equiv 1 (\mod n)$.

2.4. Chinese Remainder Theorem

If $n_1,n_2,...,n_k$ ($k \in Z_+$, $k \geq 2, n_i \geq 2$) are pairwise coprime and if $a_1,a_2,...,a_k$ are any integers, then the system

$$\begin{aligned} x &\equiv a_1 (\mod n_1) \\ x &\equiv a_2 (\mod n_2) \\ &... \\ x &\equiv a_k (\mod n_k) \end{aligned}$$

has a solution.

3. RSA Encryption

Now, after looking through the number theory knowledge we need to understand RSA encryption, let's take a look on how to set up a public key and a private key in RSA encryption and use the keys. The whole process can be divided into several steps:

(a) Select 2 random prime numbers p,q and compute their product $n (n = pq)$
(b) Compute $\phi(n)$
(c) Choose a random integer $1 < v < \phi(n)$ which satisfies $gcd(v,\phi(n)) = 1$
(d) Find d, the modular multiplicative inverse of v under $\mod \phi(n)$
(e) Set up the public key (n,v) and the private key (n,d)
(f) If m is the original message and c is the encrypted message, then we have $m^v \equiv c (\mod n)$
(g) If m is the original message and c is the encrypted message, then we have $c^d \equiv m (\mod n)$

(This can be easily proved by using the definition of d and the previous conclusions in part 2 of the article)

4. An Important Example

In order to understand the process of setting up public and private keys better, let's see an example with specific numbers.

(a) Let's choose p = 47, q = 53, and thus we have n = 47 × 53 = 2491
(b) $\phi(n) = \phi(pq) = (p-1)(q-1) = 46 \times 52 = 2392$
(c) Since gcd(17,2392) = 1,let's choose v = 17
(d) In order to find d that satisfies $vd \equiv 1 (\mod \phi(n))$, we just need to find an integer solution to the linear equation

$$vx + \phi(n)y = 1$$

In the other words, we need to find (x,y) where $x,y \in Z$ that satisfies

$$17x + 2392y = 1$$

This can be easily solved and thus we can find out that $(x,y) = (3377,-24)$ is a solution. Therefore, since $vx \equiv 1(\bmod \phi(n))$,we can let $d = x = 3377$.

(e) After the computation process, we finally get the public key (2491,17) and the private key (2491,3377).

5. The Reliability of RSA Encryption

Now, let's use the previous example to test the reliability of RSA encryption.

Suppose that person X sets up the public key $(n,v) = (2491,17)$ which is known by everyone and the private key $(n,d) = (2491,3377)$ which is known only by person Y.

Now, person X wants to send an encrypted message to person Y and let's assume that the original message is 65. X will use the public key to encrypt the message. To be more specific, if we use m to represent the original message that X wants to send and c to represent the message that Y gets, then according to the following formula

$$m^v \equiv c(\bmod n)$$

X can get c. Thus, X will send c instead of m to Y. Then, since Y got the private key (n,d), Y can get m through the formula $c^d \equiv m(\bmod n)$.

However, if a person Z who does not have the private key also wants to get m, then he or she will have to find out d. Therefore, since $ev \equiv 1(\bmod \phi(n))$, Z will have to find out $\phi(n)$ to get d. Moreover, according to the definition of n and $\phi(n)$, Z will have to find the prime factorization of n. In addition, if n is big enough, then it is almost impossible to achieve person Z's goal by using today's technology. Thus, RSA encryption is indeed currently reliable.

6. The Future of RSA Encryption

With the development of new technologies, RSA encryption is facing great challenges. Quantum computer can factor big numbers much faster than the normal computers we now have. Thus, the RSA encryption may be easily decrypted one day with the usage of the quantum computer.

Furthermore, besides computer that can compute faster, new algorithms to factor positive integers may also challenge RSA encryption. In addition, [3] is an interesting article related to this idea.

As a result, it is very possible that breaking the RSA encryption system is just a matter of time.

Acknowledgements

I would like to express my sincere gratitude to Professor Hubert Lewis Bray for giving me useful suggestions on this academic paper.

References

[1] Titu Andreescu, Dorin Andrica, Number theory:a problem-solving approach(2009)
[2] Wikipedia.org, RSA cryptosystem
[3] Claus Peter Schnorr, Factoring Integers by CVP and SVP Algorithms