Modified Multi Prime RSA Cryptosystem

MGhazali Kamardan[1], N Aminudin[1,2], Norziha Che-Him[1], Suliadi Sufahani[1], Kamil Khalid[1], Rozaini Roslan[1]

[1] Department of Mathematics and Statistic, Faculty of Science, Technology and Human Development, University Tun Hussein Onn Malaysia, Batu Pahat, Johor, Malaysia.
[2] Department of Insulated Gate Bipolar Transistor, Infineon Technology, Infineon Plant, Jalan A7, Kulim Hi-Tech, 09000 Kulim, Kedah, Malaysia.

Abstract. RSA [1] is one of the mostly used cryptosystem in securing data and information. Though, it has been recently discovered that RSA has some weaknesses and in advance technology, RSA is believed to be inefficient especially when it comes to decryption. Thus, a new algorithm called Multi prime RSA, an extended version of the standard RSA is studied. Then, a modification is made to the Multi prime RSA where another keys is shared secretly between the receiver and the sender to increase the securerity. As in RSA, the methodology used for modified Multi-prime RSA also consists of three phases; 1. Key Generation in which the secret and public keys are generated and published. In this phase, the secrecy is improved by adding more prime numbers and addition of secret keys. 2. Encryption of the message using the public and secret keys given. 3. Decryption of the secret message using the secret key generated. For the decryption phase, a method called Chinese Remainder Theorem is used which helps to fasten the computation. Since Multi prime RSA use more than two prime numbers, the algorithm is more efficient and secure when compared to the standard RSA. Furthermore, in modified Multi prime RSA another secret key is introduced to increase the obstacle to the attacker. Therefore, it is strongly believed that this new algorithm is better and can be an alternative to the RSA.

1. Introduction

Cryptography can be defined as a field of computer networks that transforms information into an unreadable form. Simply, this process is also known as encrypting a plaintext into a ciphertext, where plaintext refers to the true information and the ciphertext refers to the secret form of the information. This ciphertext can be broken or decrypted using a specific secret key. Cryptography uses mathematical techniques and acts as an effective method of keeping the information secret [2, 14, 15].

In cryptography, there are various systems and these systems are known as cryptosystem. This includes the Classic Cryptography which mainly consists of Symmetric Key cryptosystem. In this symmetric key cryptosystem, the same key is used for encryption and decryption. The security of a symmetric key cryptosystem should rely on the secrecy of the key. Examples of Classic Cryptography with symmetric key cryptosystem are symbols from ancient Egypt [3], Scytale from ancient Greece [4], Caesar's cipher method [5] and Jefferson Wheel Cipher [6].

On the other hand, there is also a Modern Cryptography which uses the Asymmetric Key cryptosystem. This cryptosystem requires two different keys, one for encryption and the other one for decryption. The security of asymmetric key cryptosystem is better when compared to the symmetric key cryptosystem because the secret does not only depend on one key but two keys to be decrypted.

Examples of asymmetric key cryptosystem are Diffie-Hellman Key Exchange Protocol [7], RSA [1] and Multi-prime RSA [8].

However, RSA cryptosystem has some weaknesses especially when decrypting messages; RSA cryptosystem was found to be a bit inefficient [9]. Thus, an improved RSA algorithm known as multi prime RSA had been introduced to overcome the problem [8]. In this paper, we introduce a modification of the multi prime RSA cryptosystem to increase the security of the system. We introduce another two keys which is shared secretly between the receiver and the sender. In the next section, the methodology to generate keys, encrypting and decrypting a message via modified Multi prime RSA is discussed. Then in section 3.0, an example result is shown. Later we discuss the efficiency and security of this cryptosystem and lastly the conclusion is made in the last section.

2. Methodology

The method uses the basics of Number Theory. From this section onward, the sender is represented as Alice and the receiver is represented as Bob. It starts with the Key Generation in which private, secret and public keys are generated by Bob who wants the message to be sent secretly. The public key will be published to the public without worrying the security of the system. The private key is the main point of the secrecy and will be kept alone by Bob. The last keys are meant to increase the security and Bob will share these key with Alice secretly.

Bob then, will published to public his public keys and secretly shares his secret key with Alice. Upon receiving those public and secret key, Alice can send secret message to Bob. She will proceed with the Encryption process in which the message known as plaintext is transformed into a secret form known as ciphertext.

Finally, the Decryption process where Bob upon received ciphertext need to convert back to plaintext or the secret form is revealed back into the original message.

2.1. Key Generation

In Key Generation, Bob chooses 3 or more distinct prime numbers $p, q, r, ...$ and multiply them to get the modulus for both Public Key and Private Key, n

$$n = p.q.r... \tag{1}$$

Then, he computes the Euler's Totient of n,

$$\phi(n) = (p-1)(q-1)(r-1)... \tag{2}$$

After that, Bob chooses the Encryption exponent, e which satisfying the condition that;

$$1 < e < \phi(n) \text{ and } \gcd(e, \phi(n) = 1 \tag{3}$$

Then computes the decryption exponent, d using the Extended Euclidean Algorithm,

$$d.e = 1(\mathrm{mod}\, e\phi(n)) \tag{4}$$

Bob sends n and e as the public key to Alice. Bob keeps d and $p, q, r, ...$ as his private keys. As a modification to the Multi prime RSA algorithm, in this new scheme Bob also shares two secret keys a and b to Alice. These keys are kept secret between Alice and Bob.

2.2. Encryption

In Encryption, Alice convert the message or plaintext into number code and label it as m and then encrypts the plaintext into chipertext, c by

$$c = (am + b)^e (\mathrm{mod}\, n) \tag{5}$$

Then Alice sends the chipertext c to Bob.

2.3. Decryption

Bob proceeds with the decryption by computing

$$m_p = \frac{c^d(\text{mod}\, p) - b}{a}$$
$$m_q = \frac{c^d(\text{mod}\, q) - b}{a}$$
$$mr = \frac{c^d(\text{mod}\, r) - b}{a}$$
$$\vdots \qquad (6)$$

Then by using Chinese Remainder Theorem and Fermat's Little Theorem, he can retrieve the plaintext by m

$$. m \equiv m_p \equiv m_q \equiv m_r \equiv \ldots$$

3. Result

This is the worked example of implementing modified Multi-prime RSA algorithm. Later, the efficiency and the security of Multi prime RSA are discussed.

3.1. Key Generation

Bob chooses several prime numbers for this example 5 prime numbers i.e. 2, 3, 5, 7, 11 and 13 and multiplies them to become modulus, n. Thus,

$$n = 3.5.7.11.13 = 30030$$

Then Bob also computes the Euler's Totient of n as follow

$$\emptyset n = (3-1).(5-1).(7-1).(11-1).(13-1) = 5760.$$

Now, Bob chooses the encryption exponent, e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n) = 1$

Bob chooses, $e = 7$

Then, Bob computes d with $d.e = 1(mod\ \emptyset(n))$.

Hence, d is 823.

Bob gives the public key $(n,e) = (30030, 7)$ to Alice. Bob also shares secret key $(a,b) = (2,-15)$ to Alice so she can send him a message.

3.2. Encryption

Now that Alice already has the public key, she decides to send a message to Bob.

For example, the message m is 10. Alice encrypt it to a ciphertext using

$$c = (am+b)^e(mod\ n) = [2(10) - 15]^7(mod\ 30030) \equiv 18065.$$

Alice now sends the ciphertext c to Bob as a secure message.

3.3. Decryption

Proceeding to decrypt the ciphertext using Chinese Remainder Theorem, Bob breaks the message into blocks so it can be decrypted faster.

$$m_2 = \frac{c^d(\text{mod}2) + 15}{2} = \frac{18065^{823}(\text{mod}2) + 15}{2}$$
$$m_3 = \frac{c^d(\text{mod}3) + 15}{2} = \frac{18065^{823}(\text{mod}3) + 15}{2}$$

$$m_5 = \frac{c^d \,(\mathrm{mod}5) + 15}{2} = \frac{18065^{823}\,(\mathrm{mod}5) + 15}{2}$$
$$m_7 = \frac{c^d \,(\mathrm{mod}7) + 15}{2} = \frac{18065^{823}\,(\mathrm{mod}7) + 15}{2}$$
$$m_{11} = \frac{c^d \,(\mathrm{mod}11) + 15}{2} = \frac{18065^{823}\,(\mathrm{mod}11) + 15}{2}$$
$$m_{13} = \frac{c^d \,(\mathrm{mod}13) + 15}{2} = \frac{18065^{823}\,(\mathrm{mod}13) + 15}{2}$$

Hence, using the Fermat’s Little Theorem [10], Bob gets

$$m_2 == \frac{1(\mathrm{mod}2) + 15}{2} = 8$$
$$m_3 == \frac{2(\mathrm{mod}3) + 15}{2} = 8.5$$
$$m_5 == \frac{0(\mathrm{mod}5) + 15}{2} = 7.5$$
$$m_7 == \frac{5(\mathrm{mod}7) + 15}{2} = 10$$
$$m_{11} == \frac{5(\mathrm{mod}11) + 15}{2} = 10$$
$$m_{13} == \frac{5(\mathrm{mod}13) + 15}{2} = 10$$

Since m_2, m_3 and m_5 at the lower modulo and inconsistent, their values can be ignored. On the other hand, the other modulo show consistent results i.e. $m_7 = m_{11} = m_{13} = 10$. So, providing all these, Bob has successfully decrypted the ciphertext back to the plaintext which is

$$m = m_7 = m_{11} = m_{13} = 10.$$

4. Discussions

We have successfully show algorithm of the modified multi RSA cryptosystem which work very well. Now, we are going to go through with the efficiency and security of this cryptosystem.

4.1. Efficiency

The Multi-prime RSA algorithm is efficient in terms of the fastness in decryption and the space saving when being implemented. According to the experimental results done by Compaq in 2000, the decryption using Multi-prime RSA is nearly 4 times faster than the standard RSA [11]. This can be expressed using the formula provided by Hinek, $\frac{3}{2r^3}(log_2 n)^3$ when r is the number of primes in the modulus and thus concludes that the more the number of primes used in the modulus, the shorter the time required for the decryption computation [12]. This makes sense since the decryption in Multi-prime RSA does not involve any exponentiations of big number like in the standard RSA. Whereas for the space used for decryption, through Chinese Remainder Theorem in Multi-prime RSA, the computations for decryption does not take a big space and hence, with each additional primes in the modulus, the space required will decrease [12].

4.2. Space Saving

Again, using the Chinese Remainder Theorem in Multi prime RSA helps to save more space for the decryption computations. Expressed by the formula $(log_2 p_r)$ where p_r is the largest prime in the modulus n, the space required for all decryption computation is small as compared to the standard RSA. Roughly, if all the primes are $\frac{(log_2 N)}{r}$-bits, the space required will decrease with each additional primes to the modulus [12].

4.3. Security

On the other hand, the security of Multi-prime RSA is undeniably better than the standard RSA. Three main attacks on Multi-prime RSA are Factoring Attacks, Small Private Exponent Attacks and Chinese Remainder Theorem Attacks. For Factoring Attacks, the modulus are to be factored and the most used methods for factoring primes is believed to be Elliptic Curve Method and Number Field Sieve [13]. This attacks only happen when the modulus, which is the product of the prime numbers happen to be small. Thus, the modulus needs to be big enough so it cannot be factored easily.

Whereas, Small Private Exponent Attacks is pretty similar with Chinese Remainder Theorem Attacks. The difficulty for both attacks comes when to reveal the private key, d provided that it is sufficiently small since attacker intends to reduce the decryption cost [12]. However, in Chinese Remainder Theorem, the exponent d does not only depends on one modulus but rather more than one since the modulus is broken down into blocks of its prime numbers. Hence, this makes these two literally different but has the same solution which is to provide a large secret exponent d so this attack can be avoided.

5. Conclusion

In conclusion, like classic RSA cryptosystem there are essentially three main phases in modified Multi prime RSA cryptosystem, which are Key Generation, Encryption and lastly Decryption. However, what makes them different is that in modified Multi-prime RSA, more than two prime numbers are used in the modulus whereas only two prime numbers are used in the standard RSA. Additionally, in the decryption process, modified Multi prime implement the Chinese Remainder Theorem unlike the standard RSA, where the classic Euler's Theorem is used to break the message. To increase the security of earlier version of Multi prime RSA, to secret keys is applied in encryption and decryption in the modified version.

By using Multi prime RSA algorithm, the efficiency of the decryption is improved when compared to the standard RSA. The implementation of Chinese Remainder Theorem helps to break down the big numbers into blocks of small numbers to make it easy to compute. Therefore, this helps to fasten the decryption process. On the other hand, the modified Multi prime RSA is more secured since the using of multi prime numbers increase the level of difficulty to break the security of the algorithm. In addition, the used of addition secret make more difficult to break. Thus, it is hope this new cryptosystem can be discussed further in future.

Acknowledgments

Authors would like to thank Universiti Tun Hussein Onn Malaysia (UTHM) and Office for Research, Innovation, Commercialization and Consultancy Management (ORICC), UTHM for kindly providing us with the internal funding.

References

[1] Rivest R, Shamir A and Adlemen L 1978 A method for obtaining digital signatures and public-key cryptosystem *Communications of the ACM* **21(2)** 120-6
[2] Malhotra M and Singh A 2013 Study of Various Cryptographic Algorithms *International Journal of Scientific Engineering and Research*. 77-88
[3] Simon S. 1999 *The Code Book: The Science of Secrecy from Ancient Egypt, to Quantum Cryptography* 1st ed (New York: Doubleday)
[4] Paarz C and Pelzl J 2009 *Understanding Cryptography: A Textbook for Students and Practitioners* 1st ed. (New-York: Springer)

[5] Holden J 2016 *The Mathematics of Secret: Cryptography from Caesar Ciphers to Digital Encryption* 1st ed. (Princeton University Press)

[6] Kahn D 1967 *The Code Breakers: The Story of Secret Writing* (New York: MacMillan)

[7] Diffie W and Hellman M E 1976 New Direction in Cryptography. *IEEE Transaction of Information Theory* 22.

[8] Ojha N and Padhye S 2014 Cryptanalysis of Multi prime RSA with Secret Key Greater than Public Key *International Journal of Network Security,* **16(1)** 53-57

[9] Boneh D 1999 Twenty Years of Attacks on the RSA Cryptosystem *Notices of the American Mathematical Society (AMS)* **46(2)** 203-213

[10] Lawrence C and Wade T 2002 *Introduction to Cryptography: With Coding Theory* 1st ed (New Jersey: Prentice Hall)

[11] Compaq 2000 *Cryptography using Compaq Multiprime technology in a parallel processing environment* ftp://ftp.compaq.com/pub/solutions/CompaqMultiPrimeWP.pdf

[12] Hinek M J 2006 On the Security of Multi-Prime RSA *Journal of Mathematical Cryptology* **2(2)** 117-147

[13] Yan S Y 2009 *Primality Testing and Integer Factorization in Public-Key Cryptography.* 2nd ed. (New York: Springer)

[14] Jayeola D, Ismail Z, Sufahani S F and Manliura D P 2017 Optimal Method for Investing on Assets using Black Litterman Model *Far East Journal of Mathematical Sciences* **101(5)** 1123-1131

[15] Zinober A and Sufahani S 2013 A Non-Standard Optimal Control Problem Arising in An Economics Application *Pesquisa Operacional* **33(1)** 63-71