RSA Cryptographic Algorithm using Cubic Congruential Generator

Nurul Khairina¹, Muhammad Khoiruddin Harahap²

¹ Informatics Engineering Department, [Universitas Medan Area]
² Informatics Engineering Department, [Politeknik Ganesha Medan]

E-mail: nurulkhairina27@gmail.com¹, choir.harahap@yahoo.com²

Abstract. In the field of cryptography, the key and procedures for converting messages into secret messages have a very important role. The RSA key is built with a random number generator. The RSA key is made as strong as possible to increase ciphertext robustness. A key that is difficult to crack and requires a lot of time certainly has higher robustness. Two initial variables that are very important in building RSA keys are prime number p and prime number q. In this research, the p and q prime numbers are generated by Cubic Congruential Generator algorithm. The results of this study can be seen by testing the ciphertext robustness. Ciphertext test results that are resistant to cryptanalytic attacks certainly show the strength of the key that is built, including the selection of primes p and primes q. The ciphertext test shows that 90% of the greater primes p and primes q will achieve a higher percentage of ciphertext robustness, and 10% of the combination from small prime number p with large prime number q is also able to achieve the highest percentage of ciphertext robustness. This proves that the selection of prime number p and prime number q in generating RSA keys really can affect the ciphertext robustness.

1. Introduction

Cryptography is the science used to protect the integrity of data [1]. Cryptography is very closely related to the confidentiality [2], integrity and availability of confidential data [3]. Cryptographic algorithms have had rapid development from year to year. Since the RSA algorithm was first introduced by three researchers Ron Rivest, Adi Shamir, and Len Adleman [4] in 1977 - now, many researchers have been interested in continuing to develop, modify, and combine these RSA algorithms with other algorithms to obtain strong keys and robustness to attacks by a cryptanalyst [5].

On the RSA algorithm, choosing prime number p and prime number q [6] can affect the key and also the ciphertext. Ciphertext that is not resistant to cryptanalyst attacks will have a bad impact on data confidentiality [7]. This research uses Cubic Congruential Generator (CCG) to generate random numbers, where two primes will be taken which will be the p-value and q value to generate the key. The researcher was interested in combining the RSA algorithm with the Cubic Congruential Generator (CCG) algorithm to increase the ciphertext robustness to cryptanalyst attacks.

There are several studies related to this research, among others: Previous research has been carried out by [8]. This study generates prime numbers on a large scale using Mersenne Prime Number and tests them with Rabin Miller Primality Test. In the results of this study, it can be seen that the security of the RSA algorithm is higher when using prime numbers on a large scale.

Research on RSA with the Linear Congruential Generator (LCG) algorithm has been carried out by [9]. The results of this study indicate the existence of double-layer security as indicated by the presence of new tables arising from the results of randomizing ASCII tables and the process of encryption and decryption such as RSA in general.

Research conducted by [10] combines the AES (Advanced Encryption Standard) algorithm with RSA. The results showed that the results of encryption have high security and are difficult to solve.

Research conducted by [11] modifies RSA to be more unique. Modification of the RSA is done by using two different public keys and a private key obtained from a large factor N. This research also does double encryption and decryption, so that ciphertext will get better security.
Research conducted by [12] compares performance between RSA-based cryptosystem and ECG (Elliptic Curve Cryptography) – based cryptosystem. From the results of the study, ECG-based cryptosystem is better than RSA - based cryptosystem. Research conducted by [13]. The researchers conducted a combination of MD5 Hash, RSA and DSA algorithm. The results of the study show that researchers can achieve efficiency, authentication, and data integrity that are quite good.

Research on cryptography always prioritizes the robustness of keys and ciphertext. The results of this study will show several things, like what is the role of prime number p and prime number q for ciphertext robustness, how much the percentage of ciphertext robustness and how long is the estimated cracking times.

2. Methodology

In this study, the researchers want to combine the RSA algorithm and Cubic Congruential Generator algorithm. Here are the steps in the process of generating the key, encryption [14], and decryption [15] [16]:

2.1 Generating The Key :

a. Generate two different random numbers p and q with the Cubic Congruential Generator algorithm [17]:

\[ X_n = (aX_{n-1}^3 + bX_{n-1}^2 + cX_{n-1} + d) \mod m \]  

The following are the results of random numbers obtained with \( a = 1; \ b = 3; \ c = 4; \ d = 3; \ X_{n-1} = 3; \) and \( m = 14. \)

| No | \( X_n \) | \( X_n \mod n \) |
|----|----------|-----------------|
| 1  | 69       | 13              |
| 2  | 2759     | 1               |
| 3  | 11       | 11              |
| 4  | 1741     | 5               |

b. Test two numbers p and q with Fermat Primality Test Algorithm whether the numbers are primes or composite numbers. We take value \( p = 13 \) and \( q = 11. \)

\[ p = 13 \Rightarrow 2^{(13 – 1)} \equiv 1 \mod 13 = 2 \]  
Test result: \( p = \text{prime} \)

\[ q = 11 \Rightarrow 2^{(11 – 1)} \equiv 1 \mod 11 = 2 \]  
Test result: \( q = \text{prime} \)

c. Calculate \( n = p \cdot q \), make sure p is not equal to q

\[ n = p \cdot q = 13 \cdot 11 = 143 \]

d. Calculate \( \Phi(n) = (p-1) \cdot (q-1) = (13-1) \cdot (11-1) = 12 \cdot 10 = 120 \)

e. For the public key, select the value of e which is relatively primed to \( \Phi(n) \) where \( 1 < e < \Phi(n) \) and \( \gcd(e, \Phi(n)) = 1 \), we take \( e = 7. \)

\[ e \text{ evidence is relatively prime and } \Phi(n) : \]

\[ 7 \mod 120 = 7 \]

\[ 120 \mod 7 = 1 => \gcd = 1 \]

f. For the private key, \( d \) obtained by equation \( d \equiv 1 \mod (\Phi(n)) \), where \( (0 \leq d \leq n). \) After conducting the experiment, get it \( d = 223. \)

\[ \text{Proof: } d \cdot e \mod \Phi(n) = 1 \Rightarrow 223 \cdot 7 \mod 120 = 1 \]

g. We obtain the public key of the couple from e and n.

\[ \text{Public key } = (e, n) => (7, 143) \]
h. We obtain the private key of the couple from d and n.
   ➢ Private key = (d, n) => (223, 143)

2.2 Encryption Process:
   a. Take the public key e and n, where e = 7 and n = 143.
   b. Convert plaintext letter to ASCII Code
   c. Perform the encryption process with $c_i = m_i^e \mod n$, so obtained the ciphertext
      ➢ First Ciphertext:
      $$C_1 = m_1^e \mod n$$
      $$C_1 = 110^7 \mod 143 = 33 => (Ciphertext_1 = !)$$
   d. Repeat and continue the steps above until $C_5$.

   The results of the encryption process can be seen in Table 2 below:

| No | Plaintext | ASCII | $C_i$ | Ciphertext |
|----|-----------|-------|-------|------------|
| 1  | N         | 110   | 33    | !          |
| 2  | U         | 117   | 39    | '          |
| 3  | R         | 114   | 49    | 1          |
| 4  | U         | 117   | 39    | '          |
| 5  | L         | 108   | 4     | EOT        |

2.3 Decryption Process:
   a. Take the private key d and n, where d = 223 and n = 143.
   b. Convert each ciphertext letter to ASCII Code
   c. Perform the decryption process with $m_i = c_i^d \mod n$ so obtained the first plaintext
      ➢ First Plaintext:
      $$M_1 = c_1^d \mod n$$
      $$M_1 = 33^{223} \mod 143 = 110 => (Plaintext_1 = N)$$
   d. Repeat and continue the steps above until $M_5$.

   The results of the decryption process can be seen in Table 3 below:

| No | Ciphertext | ASCII | $M_i$ | Plaintext |
|----|------------|-------|-------|-----------|
| 1  | !          | 33    | 110   | N         |
| 2  | '          | 39    | 117   | U         |
| 3  | 1          | 49    | 114   | R         |
| 4  | '          | 39    | 117   | U         |
| 5  | EOT        | 4     | 108   | L         |

3 Result and Discussion
In this chapter a test will be conducted to find out the relationship between the values of prime number p and the prime number q to the ciphertext robustness and the estimating cracking times, which can be seen in detail in the table below:
Table 4. Relationship between the Values of Prime Number p and Prime Number q for The Ciphertext Robustness and Estimating Cracking Times

| No | Prime Number p | Prime Number q | Ciphertext Robustness | Estimating Cracking Times |
|----|----------------|----------------|-----------------------|--------------------------|
| 1  | 13             | 11             | 18 \% (Dangerously Low) | 19 hours                |
| 2  | 29             | 37             | 44 \% (Medium)        | 4 months                 |
| 3  | 71             | 73             | 59 \% (Medium)        | 39 thousand years        |
| 4  | 61             | 67             | 63 \% (Fairly Good)   | 386 thousand years       |
| 5  | 113            | 103            | 63 \% (Fairly Good)   | 386 thousand years       |
| 6  | 17             | 71             | 72 \% (Fairly Good)   | 120 million years        |
| 7  | 191            | 373            | 78 \% (Fairly Good)   | 4 billion years          |
| 8  | 271            | 317            | 82 \% (Excellent)     | 39 billion years         |
| 9  | 503            | 541            | 89 \% (Excellent)     | 4 trillion years         |
| 10 | 19             | 83             | 100\% (Excellent)     | 27 quadrillion years     |

Visualization of table 4 above can also be seen in the graph below:

Figure 1. Visualization from Ciphertext Robustness

In Table 4 and Figure 1 above, the large prime number of p and q has a high percentage of ciphertext robustness. In the ciphertext robustness test above, 9 out of 10 data show a significant percentage change along with the increasing prime number p and prime number q. However, there is one data with a combination of a small prime number (p = 19) and the large prime number (q = 83) that achieve ciphertext robustness reaches 100\%. Through these 10 test data, it can be said that the success rate of ciphertext robustness testing reaches ±90%.

4 Conclusion
The conclusions of this study are:
1. The selection of prime number p and prime number q in generating RSA keys can affect the ciphertext robustness.
2. From the tests conducted, 90% of the test results showed a greater prime number p and prime number q will achieve a higher percentage of ciphertext robustness.
3. From the tests conducted, 10% of the test result showed the combination of small prime number $p$ with large prime number $q$ is also able to achieve the highest percentage of ciphertext robustness.

5. Acknowledgment
Thanks to the Ministry of Research, Technology and Higher Education for funding this research in the Beginner Lecturer Research grant scheme in the fiscal year 2019.

References

[1] M. H. Dehkordi, A. Asgari, and A. Moradian, “A New Scheme to Secure Communication and Data, based on the Integration of Cryptography and Steganography,” *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 2, pp. 183–188, 2018.

[2] H. Al-Mahdi, M. Alruily, O. R. Shahin, and K. Alkhaldi, “Design and Analysis of DNA Encryption and Decryption Technique based on Asymmetric Cryptography System,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 2, pp. 499–506, 2019.

[3] S. K, “An Optimal RSA Encryption Algorithm for Secret Images,” *Int. J. Pure Appl. Math.*, vol. 118, no. 20, pp. 2491–2500, 2018.

[4] R. Prakash, P. Chithaluru, D. Sharma, and P. Srikanth, *Implementation of Trapdoor Functionality to Two-Layer Encryption and Decryption by Using RSA-AES Cryptography Algorithms*. Springer Singapore, 2018.

[5] M. I. Nazeer, G. A. Mallah, R. Bhatra, and R. A. Memon, “Implication of Genetic Algorithm in Cryptography to Enhance Security,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 6, pp. 375–379, 2018.

[6] A. Gambhir and R. Arya, “Performance Analysis and Implementation of DES Algorithm and RSA Algorithm with Image and Audio Steganography Techniques,” in *Computing, Communication and Signal Processing*, 2018, no. September, pp. 1021–1028.

[7] D. Rachmawati, M. A. Budiman, and A. F, “PDF File Encryption on Mobile Phone using Super-Encryption of Variably Modified Permutation Composition (VMPC) and Two Square Cipher Algorithm PDF File Encryption on Mobile Phone using Super-Encryption of Variably Modified Permutation Composition (VMPC),” in *2nd International Conference on Computing and Applied Informatics (ICCAI)*, 2018, pp. 1–4.

[8] D. Apdillah, M. K. Harahap, and N. Khairina, “Generating Mersenne Prime Number Using Rabin Miller Primality Probability Test to Get Big Prime Number in RSA Cryptography,” *Int. J. Inf. Syst. Technol.*, vol. 1, no. 1, pp. 1–7, 2017.

[9] M. K. Harahap and Rina, “Kombinasi Kriptografi RSA dengan Linear Congruential Generator,” *SinkrOn*, vol. 3, no. 1, pp. 267–271, 2018.

[10] V. A. L. Muthuraman, “An Efficient Technique for Cryptography with Enhanced Key Security,” *Int. J. Pure Appl. Math.*, vol. 118, no. 8, pp. 479–484, 2018.

[11] M. A. Islam, A. Islam, N. Islam, and B. Shabnam, “A Modified and Secured RSA Public Key Cryptosystem Based on ‘n’ Prime Numbers,” *J. Comput. Commun.*, vol. 6, pp. 78–90, 2018.

[12] D. Mahto and D. K. Yadav, “Performance Analysis of RSA and Elliptic Curve Cryptography,” *Int. J. Netw. Secur.*, vol. 20, no. 4, pp. 625–635, 2018.

[13] S. Bhat and V. Kapoor, “Secure and Efficient Data Privacy, Authentication and Integrity Schemes Using Hybrid Cryptography,” in *International Conference on Advanced Computing Networking and Informatics*, 2018, pp. 279–285.

[14] S. Keerthi, M. Mahita, J. N. Devi, and M. Nivedhitha, “Online User’s Behavior Data Preserving Using RSA Based Selective Aggregation,” *Int. J. Pure Appl. Math.*, vol. 118, no. 20, pp. 2347–2352, 2018.

[15] M. Jannah, B. Surarso, and Sutimin, “A Combination of Rivest Shamir Adleman (RSA) and Affine Cipher Method on Improvement of The Effectiveness and Security of Text Message,” in *ISNPINSIA*, 2019, pp. 1–7.
[16] C. Intila, B. Gerardo, and R. Medina, “A Study of Public Key ‘e’ in RSA Algorithm,” in *The International Conference on Information Technology and Digital Applications*, 2019, pp. 1–10.

[17] B. Schneier, *Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in C*. 1996.