Optimization of Data Encryption Modeling Using RSA Cryptography Algorithm As Security E-Mail Data

Indah Clara Sari*, Muhammad Zarlis¹, Tulus T²

¹ Department of Computer Informatics Engineering, Universitas Sumatera Utara
² Department of Mathematics, Universitas Sumatera Utara, Medan, Indonesia

Email: indahclarasari093@gmail.com *

Abstract. Along with advances in information technology, data security is a very important thing. RSA is an asymmetric cryptographic algorithm that uses a pair of keys, namely public key and private key. This research applies the RSA algorithm to solve the optimization problem in the encryption process by increasing the presentation of the encryption process more quickly and effectively with the aim of safely sent emails.

1. Introduction
Optimization of data encryption modeling using RSA cryptographic algorithms is a solution to overcome the weaknesses of the email data security system [1][2]. As we know, the level of security of the RSA algorithm depends on the length of the key and the key itself. To get a large prime number key, it is difficult to make it yourself, therefore a random number generator is used to generate the key. Optimization of data encryption modeling using RSA cryptographic algorithms is a solution to overcome the weaknesses of the email data security system [3-6]. As we know, the level of security of the RSA algorithm depends on the length of the key and the key itself. To get a large prime number key, it is difficult to make it yourself, therefore a random number generator is used to generate the key.

2. Methodology
In cryptography, messages or information that can be read is called plaintext or cleartext. The process carried out to change the original text (plaintext) into secret text (ciphertext) is called encryption. Unreadable messages are called secret text (ciphertext). The reverse process of encryption is called description. The description will return the secret text (ciphertext) to the original text (plaintext). Both the encryption and description processes require the use of a number of confidential information, which is often called a key [7].

2.1. Research Methods
In this study, the authors used an experimental research method. The experimental research method is a research method that can be manipulated to certain conditions in accordance with the needs or research objectives. In the condition of manipulation, there are two groups: the control group and the comparison group. The control group will be given certain treatment in accordance with the objectives of the research results and the results of that treatment will be made as a comparison to the comparison group.
2.2. Data Collection Methods
The data collection method that the writer uses in this research is a literature study. In a literature study, the authors collect data and information relevant to the topic or problem to be studied. The data and information the author obtained from scientific books, scientific essays, research reports, and other written sources both print and electronic, including previous studies sourced from libraries and the internet.

2.3. System Testing Methods
System testing by the author in this study includes validation testing and quality testing. Validation testing is done to find out whether the system that was built is correct as needed. Validation testing is done using the black box method, which is a test method that is only observing the results of execution through test data and checking the functionality of the program. In the black-box method, the test is carried out by running and executing each program module then observing the results or output of the process, whether it is in accordance with the desired process so that it will be known if there are errors. While the quality testing is done to test the quality level of the software or system produced through experimental methods which include testing the level of accuracy and testing of performance (processing time). Accuracy level testing is done to determine whether the software or system produced has a good level of accuracy in terms of the encryption process and the description process. Performance testing (processing time) is done to find out whether the software or system produced has good performance (processing time) in terms of encryption and process description.

2.4. Research Steps
2.4.1. Literature Study
The research began with a literature study related to the title taken. In this literature study, the author studies data security and cryptography sourced from scientific books, scientific essays, research reports, and other written sources both print and electronic, including previous studies sourced from libraries and the internet [7].

2.4.2. Key Optimization
After conducting a literature study on data security and cryptography, the next step is to perform a key optimization in the modeling of data encryption using the RSA cryptographic algorithm as email data security. The way to optimize the encryption key is the key length used by selecting large p and q values.

2.4.3. Implementation
After doing key optimization in modeling data encryption using RSA cryptographic algorithm as email data security, the next step is to implement the results of the optimization into the process of securing email data so that the security of the email data can be more guaranteed.

2.4.4. System Testing
After the implementation, the next step is to test the system. In this step, the writer tests the results of the implementation of optimization of the data encryption modeling using the RSA cryptographic algorithm as email data security. System testing includes testing the level of accuracy and performance testing (processing time).

2.4.5. Conclusions
After testing the system, the next step is to draw conclusions that aim to explain the suitability of system testing with the results to be achieved.

3. Results and Discussion
The system was built using NetBeans. with the programming language is Java. This system is tested with Personal Computer with 2.0 GHz processor specification Intel Core I5, 4 GB Memory. The test results of the average encryption process are optimization of RSA algorithm using the Genetic algorithm with a number of characters 20, 60 and 100 which are 1.192 µs, 1.467 µs and 1. 875 µs. The results of the average test of the encryption process time can be illustrated in a graph of Figure 1:
The test results of the average decryption process are optimization of RSA algorithm using the Genetic algorithm with a number of characters 20, 60 and 100 which are 0.9856 µs, 1.443 µs and 1.674 µs. The results of the average test of the decryption process time can be illustrated in a graph of Figure 2:

From the results of 3 tests, the average test results of the avalanche effect were obtained by replacing one character in a randomly generated key of 48.73%. The average avalanche effect results after replacing one character in the key, then the key is optimized using the Genetic algorithm that is 50.65%. The key Avalanche effect comparison before and after optimization can be illustrated in a graph of Figure 3:
4. Conclusion

Based on the results of research and discussion that has been done, the following conclusions can be drawn:

a. This software can improve the presentation of the encryption process more quickly and effectively with the aim of the email being sent securely.

b. The optimization process is done by improving the RSA Algorithm by using the Genetic algorithm and adding the complement method to the encryption and description to produce a stronger key.

c. The test results of the average encryption process are the optimization of the RSA algorithm using the Genetic algorithm with a number of characters 20, 60 and 100 namely 1.192 μs, 1.467 μs and 1.875 μs. These results indicate that the character length affects the encryption process time. The longer the plaintext character, the longer it will take.

d. The test results of the average decryption process are the optimization of the RSA algorithm using the Genetic algorithm with a number of characters 20, 60 and 100 namely 0.9856 μs, 1.443 μs, and 1.674 μs. These results show that the length of the character influences the description processing time. The longer the plaintext character, the longer it will take.

e. Result of Landslide The effect conducted on the test obtained an average value of 48.73% for keys without being optimized and 50.65% for keys optimized. From these results, it can be concluded that the optimization of the RSA algorithm using the Genetic algorithm has increased the value of the avalanche effect. So, key optimization has an effect on the results of bit changes in the ciphertext.

References

[1] Arifin, Z. 2009. Case Study of the Use of the RSA Algorithm as a Safe Cryptographic Algorithm. Informatika Mulawarman 3 (4): 7-14.

[2] Devha, C.P. 2013. Securing the Secret Message Using the Rivest Shank Adleman (RSA) Cryptographic Algorithm. Indonesian education university.

[3] Ginting, A., Isnanto, R.Z. & Windasari, I.P. 2015. Implementation of the RSA Cryptographic Algorithm for Email Encryption and Description. Computer Technology and Systems 2 (3): 253 - 258.

[4] Haqi, B. 2017. Creating a Queue Application with Java NetBeans IDE 8.0.2 and MySQL Database. 1st Edition. PT. Elex Media Komputindo: Jakarta.

[5] Manurung, J., Sirait, K. & Panggabean, J.F. 2018. Application of the RSA Algorithm for File Security. Mantik Penusa 2 (2): 112 - 116.

[6] Martono. 2017. RSA Algorithm Cryptographic Modification Model for Data Security in the E-Voting Database. Mediasisfo 2 (11): 896 - 910.

[7] Wahyadyatmika, A.P., Isnanto, R.Z. & Somantri, M. 2014. Implementation of RSA Cryptographic Algorithms in Electronic Mail (E-Mail). Transient 4 (3): 442 - 450.

[8] Wahyudi, D.D. & Luthfi, E.T. 2011. Building "AirWar" Game Applications on Java-Based Mobile Phones Using NetBeans IDE 6.5. TASI 4 (12): 11-14.