International Journal of Research and Review
Vol.7; Issue: 2; February 2020
Website: www.ijrrjournal.com
Research Paper *E-ISSN: 2349-9788; P-ISSN: 2454-2237*

Combination Analysis of Data Encryption Standard (DES) Algorithm and LUC Algorithm on File Security

Fahmi Ruziq[1], Poltak Sihombing[2], Sawaluddin[2]

[1]Postgraduate Students at Universitas Sumatera Utara, Medan, Indonesia
[2]Postgraduate Lecturer at Universitas Sumatera Utara, Medan, Indonesia

Corresponding Author: Fahmi Ruziq

ABSTRACT

Cryptography is a science of encryption techniques, where the data to be encrypted will be encrypted using a key into data that is difficult to read for other parties who do not have a decryption key. DES algorithm is a symmetric cipher block cryptographic algorithm that uses a block size of 64 bits and a key size of 56 bits. LUC algorithm is an asymmetric cryptographic algorithm that uses two primes to generate public keys and secret keys. Hybrid crypto systems can provide a greater level of security. In this study the DES algorithm will be used to encrypt the message, while the LUC algorithm is used to encrypt the DES external key before the key is sent to the recipient. The results of the study are the length of the file character is directly proportional to the time of the encryption and decryption process. In combination the DES algorithm and the LUC algorithm are very dependent on the LUC key generation process. If the p value and the q value used are greater the longer the LUC key generation process. The repeated encryption process with the same DES external keywords using the LUC algorithm will produce different cipherkeys. Message security using hybrid DES and LUC algorithm cryptography is better because the cipherkey generated from DES external key encryption is different and longer.

Keywords: Cryptography, DES, LUC, Hybrid Crypto

INTRODUCTION

Communication is one of the many basic human traits that become a means for mutual understanding between one another. Along with the times, the way of human communication has been developing continuously. Exchange of messages between people can be done in various ways such as exchanging messages in the form of text in the form of documents, images, portable document files (PDF), or in other forms.

The security of messages and information is very important in communicating. Many cyber crimes look for security holes to enter and manipulate. The security and confidentiality of messages is a priority. In ensuring the security and confidentiality of messages, it is necessary to have a technique to encode messages or information called cryptography. Cryptography is a science that studies art or how to guarantee a message so that the message cannot be interpreted by other parties who do not have authority in it. There are four objectives of cryptography, among others, confidentiality, data integrity, authentication and non-repudiation.

There are two processes in cryptography, encryption and decryption, which aim to secure messages or information. The process of securing messages or information so that it cannot be understood and read without the help of knowledge or special tools is called encryption. Meanwhile, the process of returning the encrypted information into information that can be understood again is called decryption (Primartha R, 2011).

There are two types of cryptography, including classical and modern cryptography. In applying it, people rely

more on the advantages of modern cryptography in the process of securing data, but there are still many people who use classical cryptography by combining two classic cryptographic algorithms (Sadikin, 2012).

Based on the keys used, there are two parts of cryptography, namely symmetric cryptography and asymmetric cryptography. The difference between the two cryptography lies in the key. Symmetric algorithm systems use similar keys, both for the encryption and decryption processes, such as the classic cipher algorithm, stream cipher, DES, RC4 and AES. While the asymmetric algorithm uses different keys in encryption and decryption, such as the ECC, RSA, ElGamal, LUC, and Rabin algorithms.

Ryndel V. Amorado et al. (2019) in his research on improved data encryption standard algorithm (DES) based on filtering and striding techniques explained that various attacks such as brute force and cryptanalysis attacks can be used to break DES because of the small key size and simple and uniform XOR distribution operations. The improved DES was evaluated and compared to the original DES using the avalanche effect yielded an average of 55% avalanche effect.

Nadia Mustafa Mohammed Alhag et al. (2018) in his research on Enhancing the standard data encryption algorithm (DES) increasing the DES algorithm by increasing the key length (1024 bits) which will be divided into 16 keys (64 bits each). The results of the proposed algorithm are much better than the old algorithm.

Combining several algorithms is also called a hybrid algorithm. Hybrid algorithm can be used to improve the security of messages and keys by combining a number of symmetric and asymmetric algorithms to increase security and become more secure and powerful (Jain & Agrawal, 2014).

Adnan Abdul-Aziz Gutub et al. (2012) in his research on hybrid crypto hardware using symmetric-key and public-key cryptosystems proposes a hybrid crypto system that utilizes the benefits of symmetric and public-key cryptographic methods. The DES algorithm is used for data encryption and the RSA algorithm is used for key encryption before key exchange. Combining both the symmetric and public-key algorithm provides greater security and some unique features that are only possible in hybrid systems.

Symmetric cryptography has a problem in agreeing to exchange keys, because it uses the same key during the encryption and decryption process. So in order to increase the strength of cryptography in securing messages, it can be combined with standard data encryption algorithm (DES) and LUC algorithm.

In this study, what is meant by a combination of standard data encryption algorithm (DES) and LUC algorithm is a hybrid crypto system that utilizes the DES algorithm to encrypt messages, while the LUC algorithm is used to encrypt the DES external key before the key is sent to the recipient of the message that can provide greater level of security.

The DES algorithm includes a symmetrical cryptographic system and belongs to a type of code block. DES operates on 64-bit block sizes. DES encrypts the original 64-bit message into a 64-bit coded message using 56 internal key bits. DES ciphertext was obtained from various substitution processes and plaintext transpositions 16 times (Kahate, 2013).

One of the asymmetric algorithms that is strong enough is the LUC algorithm. This algorithm was developed by Peter J. Smith in 1993 together with Michael Lennon in New Zealand. The LUC algorithm works based on the Lucas Function. This algorithm was developed from the RSA algorithm after Smith examined the weakness of the algorithm. But later in its application it was found that the text encrypted using the LUC algorithm produced a ciphertext that was larger than the plaintext. Therefore, in this study the authors chose the LUC algorithm only to encrypt the DES external key which is only 64-bit in size. Combining the DES

algorithm and the LUC algorithm can increase security so messages are more difficult to solve by cryptanalysts.

RESEARCH METHODS

The message you want to secure can be done both with symmetric and asymmetric cryptographic algorithms, and can be done using one algorithm or more than one algorithm by combining them. For maximum message security, the researchers combined the DES algorithm with the LUC algorithm. In this technique, the message is encrypted first with the DES algorithm, then the external key of the DES algorithm is encrypted with the LUC algorithm.

In this study, researchers used direct input text data with the format *. Txt, *. Doc, and *. Docx which are included in the ASCII table. Research material was obtained from several sources, such as journals, books, proceedings, electronic reading sources, and the results of consultations with lecturers.

In the analysis of this algorithm process, all processes involved in this research will be discussed, namely the DES algorithm key generation, the DES algorithm encryption process, the LUC algorithm key generation process, the DES external key encryption process using the LUC algorithm, the DES external key decryption process using the LUC algorithm, and DES algorithm decryption process.

RESULT

Test Result

At this stage, the researcher examines the processing time to determine the effect of the test character size and test file extension on the encryption and decryption processing time using the DES algorithm and the combination of the DES algorithm and the LUC algorithm. Researchers tested files with sizes of 100, 200, 300, 400 and 500 characters. The test is done three times for each file. Then the results of the process will be calculated.

The following are some pictures from the results of testing several files with the extension .doc:

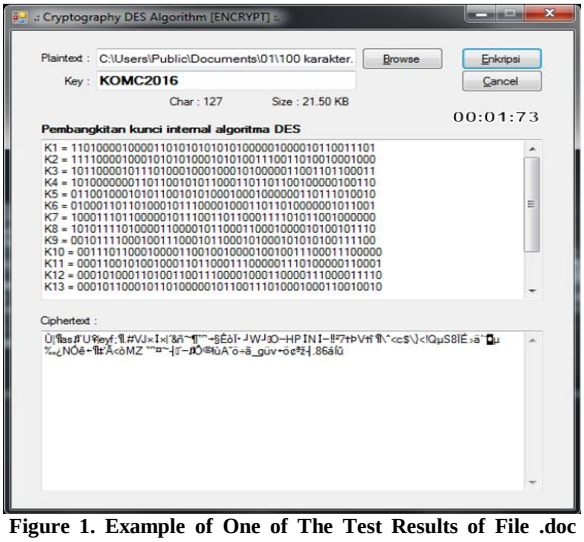

Figure 1. Example of One of The Test Results of File .doc Encryption Using the DES Algorithm

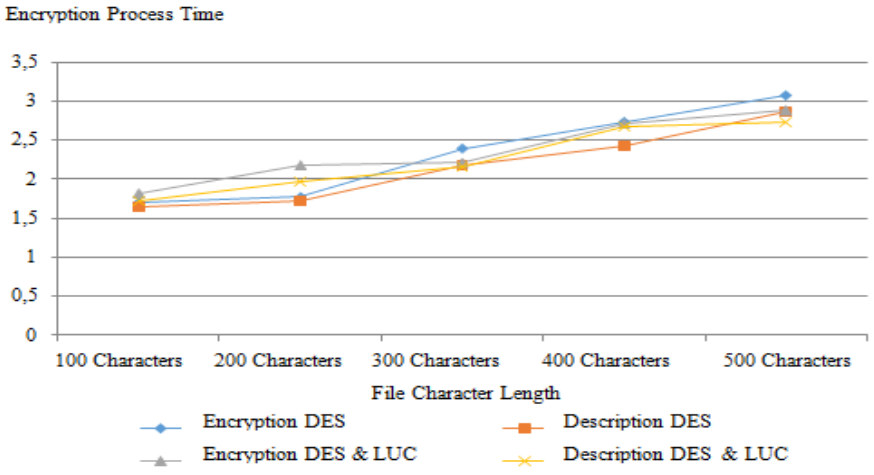

Figure 2. Graph of Character Length of .txt File for Encryption and Decryption Process Time

The following is an explanation of all the test results above:

1.The test results at the time of the process show the conclusion that the longer the number of characters of the test file that will be used for the encryption and decryption process, the longer the time needed in the algorithm process. That is because the encryption process carried out by the DES algorithm is performed per block, each block consisting of 8 characters or 64 bits. And every 64 bits are carried out the same process. Then it results in a computational process that the longer the character the longer the process time.

2.The results of the time testing process of the combination of the DES algorithm and the LUC algorithm are very dependent on the LUC key generation process. If the p value and q value used are greater then the longer the LUC key generation process in the search for decryption key values. This will affect the following:

-Encryption process time is getting longer because in this study the message delivery stage can only be done if the external key encryption is complete. This is because in the process of encrypting using the LUC algorithm in the stage of finding the decryption value with the formula e.d mod RN which must produce a value of 1.

-And the decryption process will also be longer, because the key value of the LUC decryption algorithm generated is getting bigger. This is because the greater the key value, the more iterations are performed in the LUC algorithm decryption calculation.

3.In the DES external encryption key process using the LUC algorithm if repeated attempts to encrypt repeatedly using the same keywords will result in different cipherkeys. Because the p value and q value in the key generation process of the LUC algorithm is done randomly.

4.Message security using hybrid cryptographic algorithm Data Encryption Standard (DES) and LUC is better because the cipherkey generated from DES external encryption key is different and longer. This makes it very difficult to guess the key because the number of key characters sent to the recipient is not the same as the actual number of key characters.

CONCLUSION AND SUGGESTION

CONCLUSION

From the results of the analysis of the combination of DES algorithm and LUC algorithm on file security, researchers can conclude that:

1.The test results in the real time process show the conclusion that the longer the number of test file characters that will be used for the encryption and decryption process, the longer the real time needed in the algorithm process.

2.The real time test results of the combination of the DES algorithm and the LUC algorithm are very dependent on the generation of the LUC key, the greater the p value and the value of q, the longer the process of generating the LUC key in the search for decryption key values. And this will have an impact on the message encryption and decryption process.

3.In the DES external key encryption process using the LUC algorithm if repeated attempts to encrypt repeatedly using the same keywords will result in different cipherkeys.

4.The security of messages using hybrid cryptographic data encryption standard algorithm (DES) and LUC is better because the cipherkey generated from DES external key encryption is different and longer. This makes it very difficult to guess the key because the number of key characters sent to the recipient is not the same as the actual number of key characters.

SUGGESTION

In the results of this study, the super encryption method applied in the combination of the DES algorithm and the LUC algorithm was successfully carried out because it could be proven by the plaintext that was inputted before the encryption process was the same as the results of the decryption process ciphertext. However, in the generation of LUC algorithm keys, the

determination of prime numbers p and q is only limited to 1 to 100, because the time of the key generation process will take a long time if not limited. Development can be done using algorithms that are faster than the LUC algorithm so as to increase security in the DES external key exchange.

REFERENCES

1. Alhag, N.M.M., & Mohamed, Y.A.M. 2018. An Enhancement of Data Encryption Standards Algorithm (DES). *IEEE International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE)* : 1-6.
2. Amorado, R.V., Sison, A.M., & Medina, R.P. 2019. *Enhanced Data Encryption Standard (DES) Algorithm based on Filtering and Striding Techniques*. Proceedings of International Conference on Information Science and Systems, Tokyo: 16-19 Maret 2019. Hal. 252-256.
3. Jain, M & Agrawal, A. 2014. *Implementation of Hybrid Cryptography Algorithm*. International Journal of Core Engineering & Management. IJCEM 1(3):126-142.
4. Gutub, A.A.A., & Khan, F.A.A. (2012). Hybrid Crypto Hardware Utilizing Symmetric-Key & Public-Key Cryptosystems. *IEEE International Conference on Advanced Computer Science Applications and Technologies (ACSAT)* : 1-6.
5. Kahate, Atul. 2013. *Cryptography and Network Security*. Tata McGraw-Hill Education: New Delhi.
6. Primartha R. 2011. *Penerapan Enkripsi dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES)*. Jurnal Sistem Informasi (JSI) 3(2):371-387.
7. Sadikin, R. 2012. *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*. Andi: Yogyakarta.

How to cite this article: Ruziq F, Sihombing P, Sawaluddin. Combination analysis of data encryption standard (DES) algorithm and LUC algorithm on file security. International Journal of Research and Review. 2020; 7(2): 140-144.

******