Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 714-722 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Des Triple Algorithm in Security Office Data Security Mayor Pematangsiantar

Juli Wahyuni[1], Indra Gunawan[2], Ika Okta Kirana[3], Rafiqa Dewi[4], Solikhun[5]

[1,2,3,4,5]STIKOM Tunas Bangsa Pematangsiantar, Jln. Sudirman Blok A No. 1,2,3 Pematangsiantar

E-mail: juliwahyuni2019@gmail.com

ARTICLE INFO

Article history:
Received: 07/01 / 2020
Revised: 09/01 / 2020
Accepted: 01/02/2020

Keywords:
Cryptograph, DES, Triple DES, Employee

ABSTRACT

In this era, technology is increasingly advanced and rapid, where data confidentiality is one of the things that is very important for a company. Employee data is data that is very important for the company. So it needs a system that can secure a database of employees from various types of hecker attacks or eavesdroppers who can steal and damage data. Cryptography is a science based on mathematical techniques that deal with information security such as data confidentiality. Triple DES algorithm is a development of DES algorithm, the algorithm used is the same, only in Triple DES algorithm, the encryption and decryption process is done 3 times. Triple DES also has three different keys. The three keys used can be mutually independent (K1 ≠ K2 ≠ K3) or only two keys are mutually independent and one other key is the same as the first key (K1 ≠ K2 and K3 = K1). This algorithm can generate encryption that cannot be read or understood by humans and results in the exact decryption of the initial plaintext input.

1. Introduction

Every agency or company uses technology as a partner in completing its work. The development of an increasingly rapid era makes technology as a very important requirement for the company or for individuals. Technology can help to synchronize the work and problems faced by an agency or person quickly and accurately. Institutions make technology as a supporting factor where its role is very important. Technology creates information systems that can be used to secure data and can also be used to secure networks. Pematangsiantar Mayor's Office is engaged in services, drafting, policy and governance, where the agency uses computer science technology. During the author's research at the Pematangsiantar mayor's office, the author observed that employee data storage at the Pematangsiantar mayor's office was not yet equipped with a security system, so other parties could access the employee's data

Data is very important in an institution, organization or person. Especially if the data is on a computer network that is connected / connected to another network [1]. The development of information technology, we need a data security system so that there are no unwanted things, especially data tapping or theft, such as employee data. therefore very necessary for a data security system so that confidentiality of employee data can be maintained properly.

Therefore, to avoid the theft and damage of data, the authors use the Triple DES cryptographic algorithm for the process of data encryption and decryption. Cryptography is a technique in securing and sending data in a form that is only known by the party who opened it, so that it can secure data or information [2]. The Triple DES (Triple Data Encryption Standard) method is a cryptographic algorithm that can be used to generate data. Triple Data Encryption Standard (3DES) is the development of DES by doing the DES process three times with three different keys. 3DES has three 168bit keys (three 56bit keys from DES) [3].

In previous studies, [4]conducted research in the design of cryptographic systems in documents using the Triple DES algorithm and RSA. The results showed the application of a cryptographic system

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 714-722 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

was built to provide convenience for users in securing important documents so as to avoid user privacy disturbances by unauthorized parties. The Triple DES and RSA cryptographic system application display aims to facilitate the user in the application user process.

2. Literature Review

2.1 Data Security

"Data security is one of the important things in data exchange, especially data exchange in cyberspace in which there are many threats to the process itself" [5]. Data security is also very important in maintaining the confidentiality of information, especially those containing sensitive information whose contents may only be known by certain parties, so it is necessary to encode data so that some parties who do not have the authority will not be able to open the information sent.

2.2 Cryptography

The word cryptography comes from Greek. In Greek cryptography consists of words namely cryptos and graphia. cryptography is secret writing, the true meaning of cryptography is the study of how to maintain the confidentiality of a message, so that the contents of the message delivered are safe until the recipient of the message [6].

The following are four objectives of cryptography that are included in the aspect of information security, namely [7]:

1. Data confidentiality: Keeping data confidential from unauthorized parties who might try to read the data
2. Data Integrity (integrity): Ensuring the data sent is still the same as the data received without any changes or modifications to the data.
3. Authentication: Ensuring that the sender and recipient are truly guaranteed the authenticity of the two communicating parties must know one another.
4. Non-Repudiation (Non-Repudiation): The sender cannot deny that he has sent data because the sender will get proof that he has sent data to the recipient.

Following is the cryptographic terminology namely [8]:

1. Plaintext is data or information that can be read and understood by its meaning.
2. Ciphertext is a form of encrypted / unread or incomprehensible message.
3. Encryption is the process of encoding plaintext into ciphertext.
4. Decryption is the process of returning the ciphertext to the original plaintext
5. A key is a key that is used for encryption and decryption.

2.3 Triple DES algorithm

Triple DES algorithm is a development of the DES (Data Encryption Standard) algorithm. The difference between DES and Triple DES algorithms is basically the same, but the DES algorithm uses one 56bit key while Triple DES uses three 168bit keys. Triple Data Encryption Standard (Triple DES) is the development of DES by doing the DES process three times with three different keys. Triple DES has three 168bit keys (three times the 56bit key of DES) so the level of difficulty in guessing Chipertext is getting higher [9]

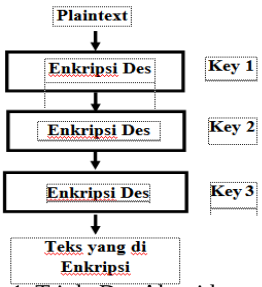

Fig 1. Triple Des Algorithm

2.4 Java

Java is an object-oriented programming language (OOP) and can be run on a variety of operating system platforms. Java as a programming language, java can make all forms of applications, desktops, web, etc., as made using other conventional programming languages [10].

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 714-722 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

2.5 NetBeans

NetBeans is one of the free OpenSource IDEs that is built on components called modules. a Java-based IDE (Integrated Development Environment) developed by Sun Microsystems to develop software.

3 Methodology

3.1 Research design

The research design conducted by the author in solving this problem is divided into two flowcharts viz.

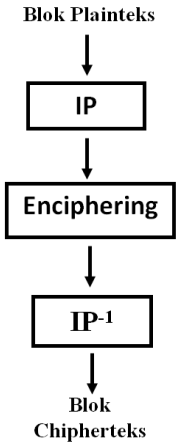

Fig 2. Global Schema Algorithm Dec

1. The plaintext block is permuted by an initial permutation matrix

2. The initial permutation results are then enciphered 16 times (16 cycles), each cycle using a different internal key.

3. The enciphering results are then mutated with an inverse iinitial permutation matrix (IP-1) into a ciphertext block.

4. Triple DES Algorithm Encryption Process Flowchart

Triple DES algorithm is a development of the DES algorithm, the algorithm used is the same, only in the Triple DES algorithm, the encryption and decryption process is carried out 3 times. Triple DES also has three different keys. The three keys used can be mutually independent (K1 ≠ K2 ≠ K3) or only two keys are mutually free and one other key is the same as the first key (K1 ≠ K2 and K3 = K1).

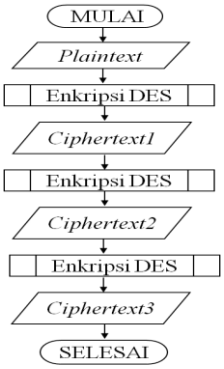

Fig 3. Flowchart Triple Encryption Algorithm Process Dec

The first step is to input the plaintext then do the encryption process using the Des algorithm so that the output is in the form of ciphertext1. The next step is to do the encryption process using des algorithm and get ciphertext2. the last step is to do the encryption process using the des algorithm and the

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 714-722 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

ciphertext3 (final) output is obtained.

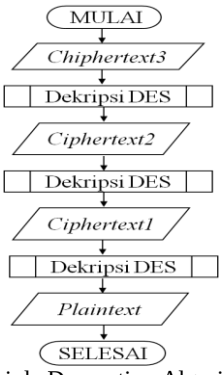

Fig 4. Flowchart Triple Decryption Algorithm Process Dec

He first step is inputting ciphertext3 then decryption process using Des algorithm to get the output in the form of ciphertext2. The next step is to do the decryption process using des algorithm and get ciphertext1. the last step is to do the decryption process using des algorithm and get the output in the form of plaintext.

3 Implementation

3.1 the results

To encrypt and decrypt files we can access via the main menu as shown in Figure 15. .

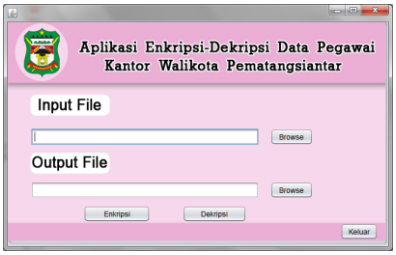

Fig 5. Main Menu Display

In the main menu there are several components, namely two text fields for selecting the input file and output file and two buttons for encryption and decryption and an exit button to exit the application

The process of forming file encryption, can be explained in Figure 16. following.

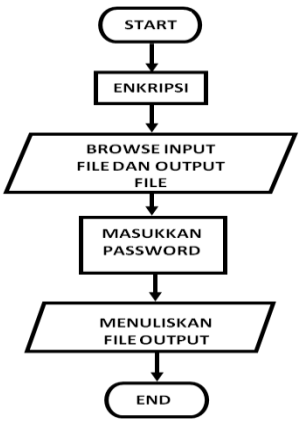

Fig 6. File Encryption Stages

he stages of file encryption with this cryptographic application are as follows:

1. Encrypt the file.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 714-722 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

2. Select the file to be encrypted (input file and output file). In this program the Triple DES algorithm is implemented to secure files with various extensions such as: .doc, .xls, .ppt, .pdf, and .jpg.
3. Enter the password. The password is entered according to the user's wishes.
4. The program will process the encryption and write the output file so that the data cannot be read.

To encrypt files, one must first select the input file and output file by clicking the browse button. After the browse button is clicked, an open dialog will appear as shown in Figure 17.

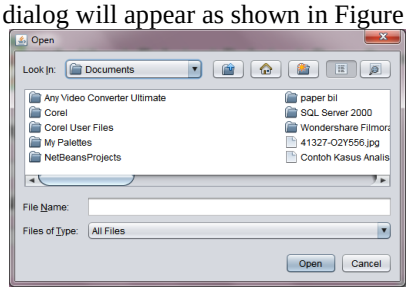

Fig 7. Display select file

Then select the file you want to encrypt, after that the location and name of the file will appear in the text field like Figure 18. Next

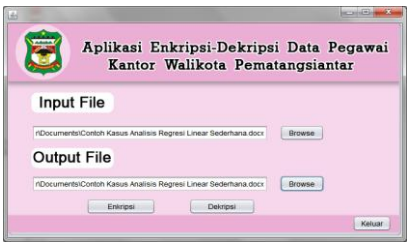

Fig 8. Display After Selecting a File

Then click the encryption button when the encryption button is clicked then a form will appear to input the key as shown 19. Next

Figure 9. Key Input Display

Then enter the key to encrypt the file that has been selected for Triple Des. The key length used must be 3 times that of Dec, which is 3x8 characters = 24 characters. When the Ok button is clicked, a notification will appear stating that the encryption was successful as shown in Figure 20. Next.

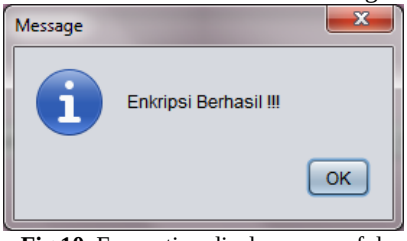

Fig 10. Encryption display successful

Below is an example of the results of encryption on several different file types.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 714-722 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

1. Document Files (.doc / .docx)
a. Decryption File

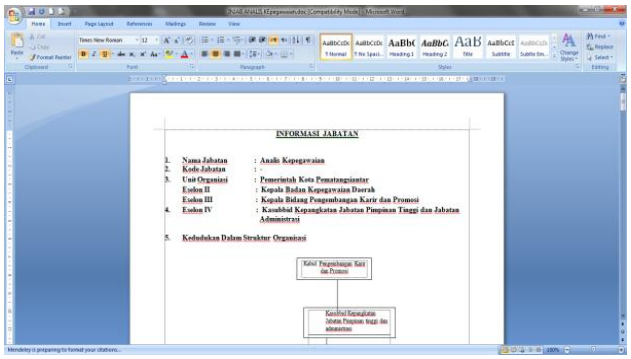

Fig 11 . Decryption Result File Analysis Staffing.docx

b. Encrypted File

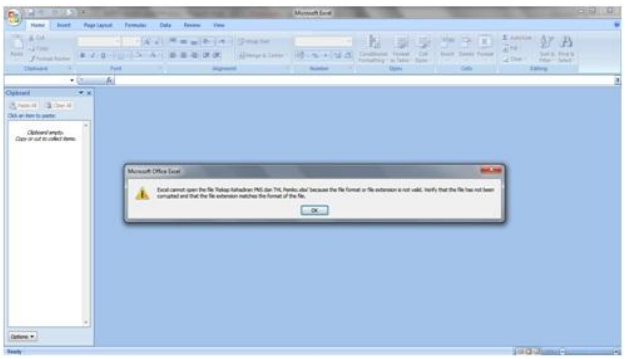

Fig 12. Encrypted Result File Analysis Staffing.docx

After encrypting the docx file above, this shows that the original encryption file cannot be opened and read its contents.

Decryption is the opposite of encryption, which returns the plaintext so that its contents can be opened and understood. the process of forming file decryption will be explained in Figure 13. following.

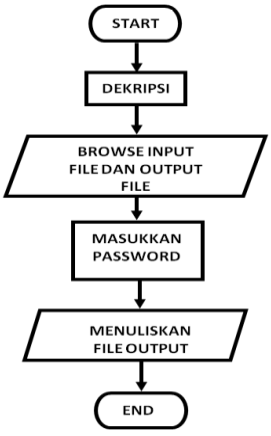

Fig 13. File Decryption Stages

The stages of file decryption with this cryptographic application are as follows:
1. Decrypt the file.
2. Select the file to be decrypted (input file and output file). In this program the Triple DES

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 714-722 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

algorithm is implemented to secure files with various extensions such as: .doc, .xls, .ppt, .pdf, and .jpg.
3. Enter the password to decrypt the file. The password entered must match the password during the encryption process.
4. The program will decrypt and write the output file, so the decrypted data file will return to the original file.

he stages of file decryption using this cryptographic application are as follows: First we will also choose the input file and output file by clicking the browse button. after the browse button is clicked, an open diaolog will appear as shown in Figure 14. following.

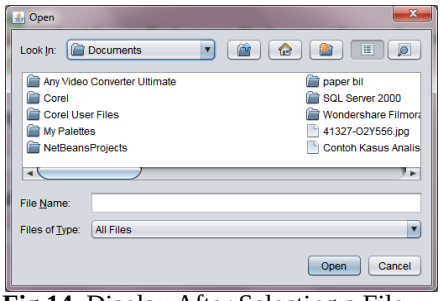

Fig 14. Display After Selecting a File

Then click the decryption button when the decryption button is clicked then a form will appear to input the key like Figure 15. following.

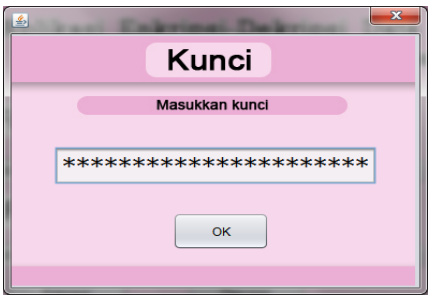

Fig 15. Key Input Display

When the OK button is clicked, a notification will appear stating the decryption was successful as shown in Figure 16. following.

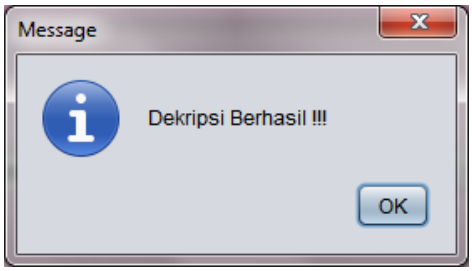

Fig 16. ecryption Display Successfully

If you enter the wrong key, 17 will appear. following.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 714-722 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

Fig 17. Display If the Key is Wrong

The decryption process is the process of changing the ciphertext into a plaintext whose purpose is to change the encrypted data or message content so that its contents can be opened and understood. To find out which files to be decrypted can be opened and their contents understood, it is necessary to analyze the contents of the file. Below is an example of an analysis of several files with different files.

1. Document Files (.doc / .docx)

a. Encrypted file

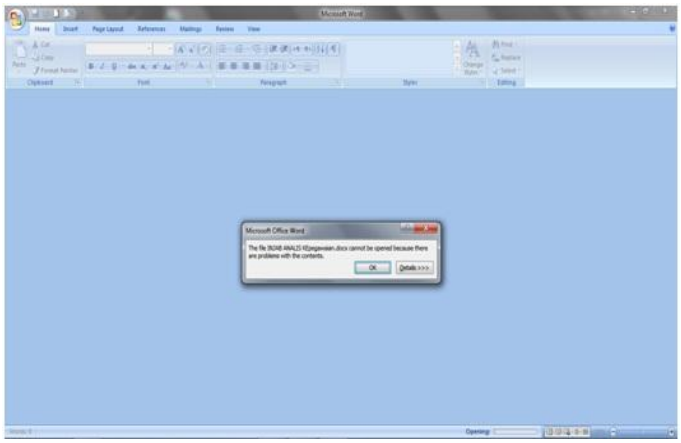

Fig 18. Encrypted file Injab Staffing Analysis.docx

b. Decrypted file

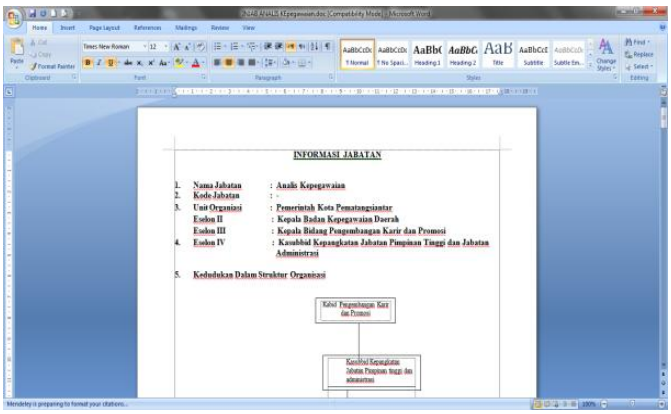

Fig 19. Decrypted file Injab Staffing Analysis.docx

After decrypting some of the above files, this indicates that the decrypted file will be able to open and understand its contents.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Jurnal Mantik
Volume 3 Number 4, February 2020, pp. 714-722 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik/index

5. Conclusion

After analyzing, designing, implementing, and evaluating the encryption application using the TRIPLE DES cryptographic algorithm, the conclusion is that this research has successfully tested the encryption application by applying the TRIPLE DES cryptographic algorithm that can secure files with various extensions, such as: .doc, .xls,. ppt, .pdf and .jpg. The design method using the TRIPLE DES algorithm is by the process of encryption and decryption of data carried out by implementing the DES algorithm three times. The encryption process produces a plaintext that cannot be read or understood, and the decryption process also produces the same plaintext as the original data input so that it can be read and understood again.

6. References

[1] A. H. Pangaribuan, "Perancangan Aplikasi Pengamanan Data Teks Dengan Metode Advanced Encryption Standard (AES) Dan Metode End Of File(EOF)," *J. INFOTEK*, vol. 1, no. 2, pp. 5–10, 2016.
[2] A. Fauzi, Novriyenni, Y. Maulita, and A. M. H. Pardede, "Analisi Hybrid Cryptosystem Algoritma Algoritma RSA Dan TRIPLE DES," *J. Tek. Inform. Kaputama*, vol. 1, no. 2, pp. 36–44, 2017.
[3] M. Sanwasih, "Penerapan Aplikasi Pengamanan Data / FileDengan Metode Enkripsi Dan Dekripsi Algoritma 3DES," *Semin. Nas. Teknol. Inf. dan Multimed.*, pp. 43–48, 2017.
[4] K. H. Kartika, A. Y. A. P, and S. Tendean, "Perancangan Sistem Kkriptografi Pada Document Menggunakan Algoritma TRIPLE DES Dan RSA," *J. Inteksis STMIK Widya Dharma.*, pp. 1–11, 2018.
[5] E. Budi, H. Sibarani, P. M. Zarlis, and R. W. Sembiring, "Analisis Kripto Sistem Algoritma AES Dan Elliptic Curve Cryp (ECC) Untuk Keamanan Data," 2017.
[6] Siswanto, Feriadi, G. P. Utama, and A. F. Achmad, "Pengamanan Data Dengan Menggunakan Algoritma Kriptografi AES, RC4 dan Komperesi LZ77 Berbasis Java Pada Badan Karantina Pertanian," *Semin. Nas. Telekomun. dan Inform.*, pp. 115–120, 2016.
[7] M. K. Harahap, "Analisis Perbandingan Algoritma Kriptografi Klasik Vigenere Cipher dan One Time Pad," *J. Nas. Inform. dan Teknol. Jar.*, vol. 1, no. 1, pp. 61–64, 2016.
[8] B. Purnama and M. Kom, "Pengamanan Pesan Rahasia Melalui Kriptografi Vigenere Cipher dengan Kunci Berlapis," *J. Ilm. Media Process.*, vol. 9, no. 3, pp. 264–269, 2014.
[9] Liana, Sutardi, and N. F. Muchlis, "Aplikasi Enkripsi dan Dekripsi Data Menggunakan Tiny Encyption Algoritma (Tea) Berbasis Java," *semanTIK*, vol. 4, no. 1, pp. 39–48, 2018.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.