Journal of Applied Engineering and Technological Science
Vol 1(2) 2020 : 113-123

ANALYSIS AND DESIGN OF FILE SECURITY SYSTEM AES (ADVANCED ENCRYPTION STANDARD) CRYPTOGRAPHY BASED

Khairul Muttaqin[1], Jefril Rahmadoni[2]*
Universitas Samudra[1], Universitas Andalas[2]*
khairulmuttaqin@unsam.ac.id[1], jefrilrahmadoni@it.unand.ac.id[2]*

**Coresponding Author*

ABSTRACT

The times has made human needs are increasing, including information needs. Therefore, sending and storing data through electronic media requires a process that is able to guarantee the security and integrity of the data that requires an encoding process. Encryption is the process of changing an original data into confidential data that cannot be read. Meanwhile, the decryption process is a process where the confidential data received will be converted back into the original data. In this case the Advanced Encryption Standard (AES) algorithm is used as the latest cryptographic algorithm standard. The previous algorithm was considered unable to answer the challenges of the development of communication technology very quickly. AES is a cryptographic algorithm using the Rijndael algorithm that can encrypt and decrypt blocks of data over 128 bits with a key length of 128 bits. In this study the application of AES as a file security system is carried out, where the encryption and decryption process is carried out on the file. In testing the system a trial is performed on all files with different file sizes and for the results of the encryption process (ciphertext) in the form of files with the file format with the *.encrypted extension.

Keywords : *AES (Advanced Encryption Standard), Security System, Cryptography, Encryption-Decryption*

1. INTRODUCTION

Communicating with each other is one of human nature since it was here on earth. For humans to communicate serves as a means to understand one another. The development of technology and media to communicate from ancient times until now continues to experience development, before the media was found to document information, sending information from one place to another has already taken place.

With the advances in telecommunications and computers it also allows users to store data digitally. Digital data storage activities also have many risks, as well as activities on the internet network about the security of communication via the internet. This is clearly seen if in these activities there is information or data that is important or confidential can be accessed by other people who are not interested, because in the crime of communication and information technology also develops, as we often hear is hackers and crackers. At this time the problem of security on the computer becomes very important.

Data security on storage media that are often carried such as laptops, external hard drives or sky drives, lose or theft often occurs. If this happens the first thing to think about is the data contained in the storage memory even though the data already has a back-up but the important data and files become a main thought, especially the stored data is confidential or private.

Sending data and storing data through electronic media requires a process that can guarantee the security and integrity of the data sent. For that we need a process of encryption (encryption and decryption) of the data sent which is known as cryptography. Various cryptographic algorithms have been created by cryptographers for data security, such as the previous algorithm, the DES (Data Encryption Standard) cryptography, but the DES algorithm still has shortcomings and leaves a problem, especially in the hardware side and the key length is too short so a proposed AES Cryptographic Algorithm (proposed Advanced Encryption Standard) to solve the above problem.

2. LITERATURE REVIEW

Computer security courses is one of those subjects taught in the Information Systems major which is the security course this computer there is taught about cryptography (Rahmadoni, 2018). Advanced Encryption Standard (AES) algorithm is a cryptographic algorithm that can be used to generate data. AES algorithm is symmetric blokchipertext that can encrypt (decipher) and decrypt (decipher) information. Encryption changes data that cannot be read anymore called ciphertext; otherwise decryption is changing the ciphertext data into its original form which we know as plaintext. The AES algorithm uses cryptographic keys 128, 192, and 256 bits to encrypt and decrypt data in 128-bit blocks. The choice of data block and key size will determine the number of processes that must be passed for the encryption and decryption process. Comparison of the number of processes that must be passed for each input is shown in table 1 (Padate & Patel, 2014).

Table 1 – Parameter AES

	Long Lock	Block Size	Round Number
AES-128	4	4	1
AES-192	6	4	1
AES-256	8	4	1

Encryption is done at the time of delivery by changing the original data into confidential data, while decryption is done at the time of receipt by changing confidential data into original data. So the data sent during the sending process is confidential data, so the original data cannot be known by unauthorized parties. Original data can only be known by the recipient by using a secret key. (Pabokory, et al., 2015).

The encryption process in the AES algorithm consists of 4 types of bytes transformation, namely SubBytes, ShiftRows, Mixcolumns, and AddRoundKey. At the beginning of the encryption process, input that has been copied into the state will undergo an AddRoundKey byte transformation. After that, the state will undergo Subbytes, ShiftRows, MixColumns, and AddRoundKey transforms as many times as Nr. This process in the AES algorithm is called the round function. The last round is somewhat different from the previous rounds where in the last round, the state did not undergo a MixColumns transformation. (Budiantoro and Rohman, 2010).

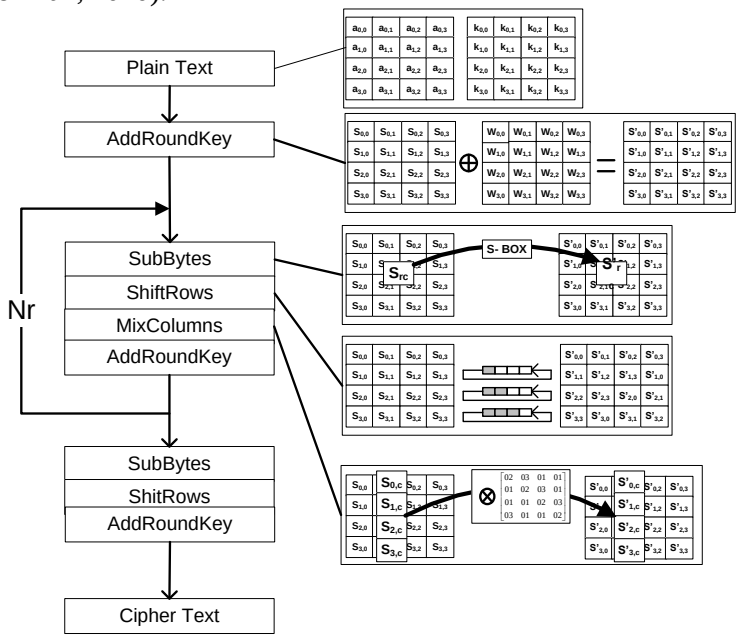

Fig. 1. AES Algorithm Encryption Process

Then for the decryption process AES algorithm is described in the flow chart below.

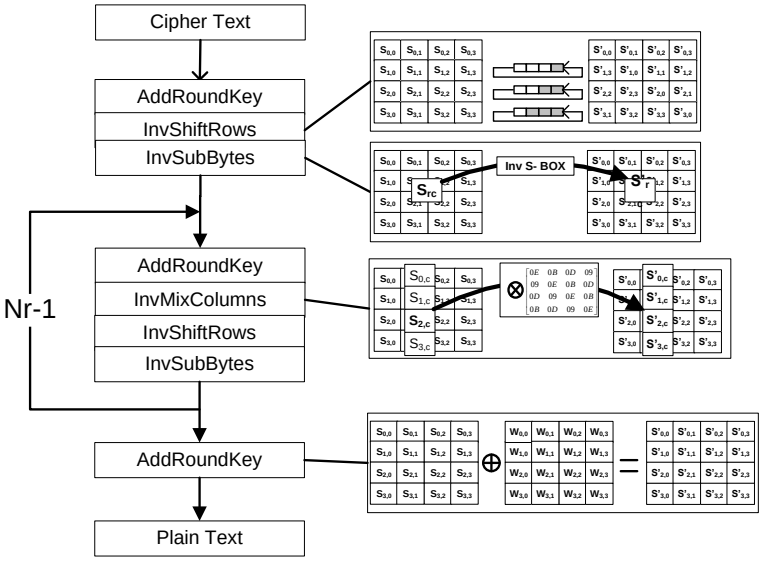

Fig. 2. AES Algorithm Description Process

The cipher transformation can be reversed and implemented in the opposite direction to produce an easily understood inverse cipher for the AES algorithm. The byte transforms used in inverse ciphers are InvShiftRows, InvSubBytes, InvMixColumns, and AddRoundKey (Bhaudhayana and Widiartha, 2015).

For AES the type of attack square attack is enough to be known as the best attack against AES l. Square attacks are attacks that utilize the byte orientation structure. This algorithm works well on square coppers that work in 6 cycles. If AES is 128-bit long, this attack is faster than exhaustive search up to 6 times AES iteration. However, for AES it is clear that this attack is not possible because of the number of rounds on AES, resulting in a greater safety limit for this algorithm.

In 2002 through a theoretical testing process it was found that AES might be broken down or solved. This attack method is called "XLS Attack". This attack was first published by Nicolas Courtois and Josep Pieprzyk in their paper entitled "Cryptanalysis of Block Ciphers with Overdefined Systems of Equations". This technique is claimed to solve AES faster than the exhaustive search method. XSL attacks rely on the success of analyzing the internal subsystem of the cipher to simultaneously reduce quadratic equations. This collection of equations is generally very large. For example, in 128 AES there are 8000 equations with a number of variables 1600. The method for solving this equation is called XSL (eXtended Sparse Linarization). If the equation can be solved, then the key can be obtained.

If solving the equation becomes a problem, an equation which is MQ (Multivariate Quadratic) is found. MQ equation is a problem that is NP-hard (Non-Polynomial). XSL attacks require efficient algorithms to resolve MQ. One technique for solving the MQ system is by linearization, which converts each quadratic equation into an independent variable that will produce a linear equation using an algorithm such as Gaussian elimination. In 2000, Courtois proposed an algorithm for MQ called XL (eXtended Linearisastion). This algorithm increases the number of equations by multiplying by a certain degree monomial. This algorithm will produce a form of structure called XSL. The XSL algorithm is formed from the XL algorithm by selectively selecting monomials(Chan, 2014).

3. RESEARCH METHODS

Methodology is a determining factor for the merits of writing scientific papers, and therefore the role of methodology is very important in writing scientific papers. Research methodology is a work step that needs to be done so that the preparation of a thesis becomes easier and can also be used as a guide for researchers in carrying out research.

The following framework used in this study can be illustrated as shown in Figure 3:

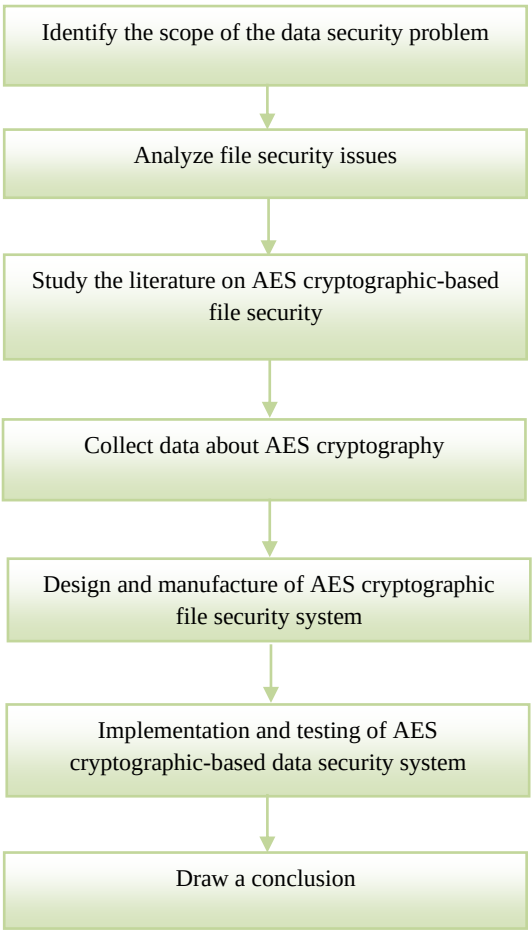

Fig. 3. Research Framework

Identify the scope of the data security problem
In the first stage in the framework of this research, the process undertaken is to identify the scope of data security issues, there are several problems that arise in the delivery of data from both the sender and recipient. One of them is theft, piracy and data changes made by people who are not responsible. This will be detrimental to even endanger people who send data or data recipients. Therefore, in order to prevent this from happening, a cryptographic (data randomization) technique is needed using the AES algorithm.

Analyze file security issues
At this stage we will analyze the problems that occur in file security. In the delivery of information, especially in the process of sending files need to be studied further regarding the security of the file, because the file that we send or receive is not necessarily safe and is not even the original or actual file. This can be seen from the problem of file theft and file changes that have been sent or received. File security problems can be overcome by applying the method of randomizing the original file to a random file (encryption) and returning a random file to the original file (decryption). Encryption and decryption are the methods used by Cryptography

Study the literature on AES cryptographic-based file security
Literature Study Phase (literature study) is carried out by collecting and studying all kinds of information related to cryptography, AES algorithm and all things related to the programming model, can be through books, journals and internet media.

Collect data about AES cryptography
At this stage is the process of introducing AES Cryptography Algorithm, starting from the definition of AES Algorithm, AES Algorithm Method, how AES Cryptography works, Key Length used, advantages and disadvantages of AES cryptography and other matters relating to AES cryptography.

Design and manufacture of AES cryptographic file security system
At this stage the system design and work will be carried out based on the results of the existing literature study. The design of a cryptographic-based file security system using the Advanced Encryption Standard algorithm is carried out in several stages, namely starting from making a flowchart design and continuing with the design of the program interface. after the design of this system is finished proceed with making the application program using web programming.

Implementation and testing of AES cryptographic-based data security system
At this stage the system implementation process is carried out where the results of the design and interface design are applied into the program. and at the system testing stage, there are several sample files that will be tested, namely, text files, documents, images and video files. The testing process is carried out in two stages, namely the encryption and decryption stages, if the results of both the encryption and decryption testing are in accordance with what is expected then the testing process is declared successful and has no errors.

Draw a conclusion
At this stage, the process of drawing conclusions from the entire research process, such as test results, the suitability of the programming used and the key processes in AES cryptography

4. RESULTS AND DISCUSSIONS

a. Overview of AES Cryptographic Application

In general, this AES Cryptography Application has a function to secure messages or files by means of the technique of changing the original message (plaintext) into a message or secret file (ciphertext) that cannot be understood or read by people who are not authorized. Figure 3.1 is a block diagram of the cryptographic application system that will be created.

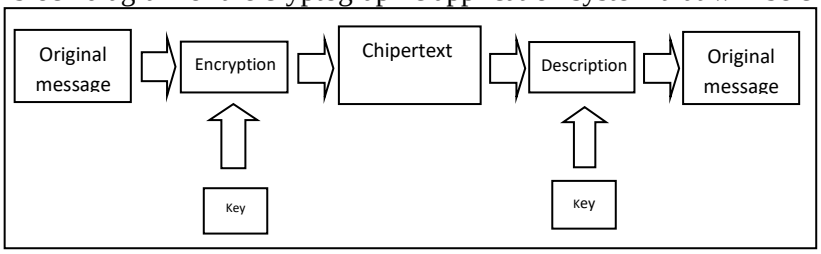

Fig. 4. Cryptographic Block Diagram

The application system requires input in the form of text messages or files before the encryption process. The encryption process is the process of converting the original message into a secret message where the encryption process uses the AES algorithm which is a symmetrical algorithm where this algorithm requires the same key when the encryption and decryption process. The decryption process is the process of changing a secret message into an original message or plaintext.

b. System Analysis

Input analysis in AES (Advanced Encryption Standard) cryptographic file security system consists of two types of input data, namely text data (messages) and data files, where the input process of the two types of data is done separately. For text data (text messages) input is performed in the process of encrypting text whose input data is in the form of text messages, while the data file is inputted in the process of encrypting files where the input data is computer files, such as document files, music, videos, application files and all types file that is on the computer.

In the process of decryption of text input types are divided into two types of types, namely message results in estimation (ciphertext) ascii code types and hexa numbers. Whereas the decryption of the input data files is in the form of text messages and encrypted files (ciphertext) with the extension *.encrypted

Process analysis that occurs in the AES (Advanced Encryption Standard) cryptographic file security system consists of encryption and decryption processes in which both processes apply to both text message data input and data file.

In the encryption process, the user is asked to enter messages or computer files to be encrypted and enter a password. Then the system will do the encryption process (change the original message into a random message) and produce messages or files that have been encrypted (messages that are random or unreadable).

In the decryption process, users are asked to input encrypted messages or files (random or unreadable messages) and enter the same password / key during encryption. Then the system will decrypt (convert random messages into original messages) and produce original messages or files that can be read.

Output of the AES (Advanced Encryption Standard) cryptographic file security system consists of two types of outputs, namely the output of text messages (secret messages) which are the result of the process of text encryption and the output files (secret files) which are the result of the file encryption process.

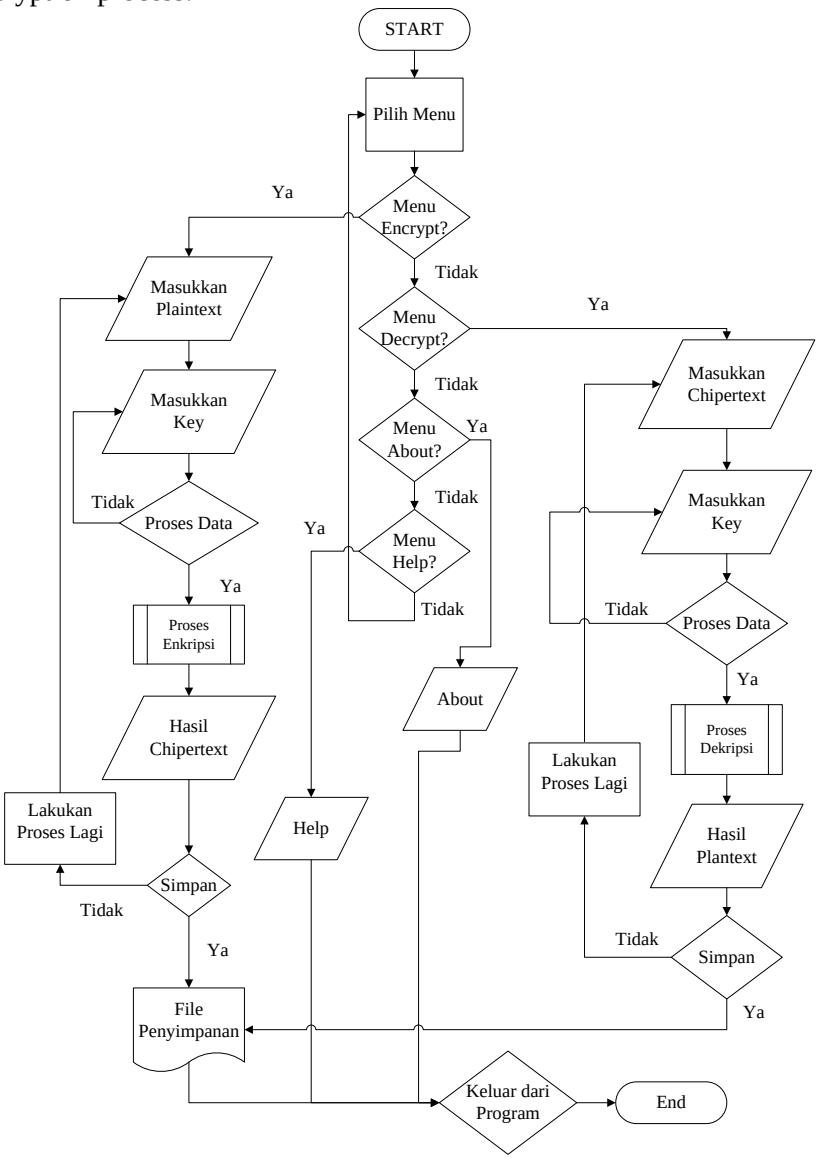

Fig. 5. Whole Flow Diagram of AES Cryptographic Application Process

Results and Discussion is a section that contains all scientific findings obtained as research data. This section is expected to provide a scientific explanation that can logically explain the reason for obtaining those results that are clearly described, complete, detailed, integrated, systematic, and continuous.

The discussion of the research results obtained can be presented in the form of theoretical description, both qualitatively and quantitatively. In practice, this section can be used to compare the results of the research obtained in the current research on the results of the research reported by previous researchers referred to in this study. Scientifically, the results of research obtained in the study may be new findings or improvements, affirmations, or rejection of a scientific phenomenon from previous researchers.

c. Display Interface

The display specifications of the cryptographic application explain how to use the application. With the application specifications, it is expected that users will find it easier or know how the application works, while the cryptographic application specifications made are as follows:

Testing The Encryption Menu

The encryption menu functions as a message scrambler or information so that it becomes a form that cannot be read by others and becomes a secret message. The encryption menu function in this program is divided into two parts namely Encrypt text and Encrypt File which runs according to design specifications. Display the text encryption and file encryption menu along with the results of the ciphertext can be seen in the image below.

Fig. 6. Encryption Test Menu Before Message Encrypted

Fig. 7. Encryption Test Menu AMessage Encrypted

For the encrypted ciphertext results can be seen in the picture below where the results are converted to hexadecimal numbers.

Fig. 8. The Result of Encrypt (ciphertext) Process in Text “Hello” with Key “1234”

Fig. 9. Encrypt File Menu with Image File Format: Master Clean Winter.jpg

Fig. 10. The Result of Encrypt (ciphertext) Process in Image File Master Clean Winter.jpg

Fig. 11. Encrypt File Menu with Video File

Fig. 12. The Result of Encrypt (ciphertext) Process in Video File

Fig. 13. Encrypt File Menu with Audio File

Fig. 14. The Result of Encrypt (ciphertext) Process in Audio File

Testing The Description Menu

Decryption menu functions to translate messages that have been randomized so that they can be read by the recipient of the message or by those who are entitled to receive the message. Decryption Menu function in this program is also divided into two parts, namely text decryption and file decryption that runs according to the design specifications. Display Decryption menu can be seen in the following picture.


Fig. 15. Description Test Menu Before Message Descripted


Fig. 16. Description Test Menu After Message Descripted

Fig. 17. Description Test Menu Before Image File Master Clean Winter.jpg Descripted


Fig. 18. Description Test Menu After Image File Master Clean Winter.jpg Descripted

5. CONCLUSION

From the results of the design and implementation of the cryptographic application program using the Advanced Encryption Standard (AES) algorithm, the following conclusions can be drawn: (1) From the results of tests conducted it is evident that the message or file generated is in the form of ciphertext that is the message or file that cannot be read so that it can be said that the system designed has been running well; (2) The use of web programming to build a file security system is apparently sufficient to implement the AES (Advanced Ecryption Standard) algorithm process; (3) Application of cryptography The Advanced Encryption Standard (AES) algorithm is very sensitive to changes in input keys, it is based on the fact that a change of key (encryption key differs from decryption key) will cause changes in data when restored to its original form in other words the file cannot returned in its original form.

REFERENCES

Bhaudhayana, G.W. & Widiartha, I.M. (2015). Implementasi Algoritma Kriptografi Aes 256 Dan Metode Steganografi Lsb Pada Gambar Bitmap. *Jurnal Ilmiah Ilmu Komputer Universitas Udayana*, 8(2).

Budihartono & Roman, N. (2010). Impelementasi Algoritma Enkripso Rijbdeal Pada Pembuatan Kunci Lisensi Program Pengubahan Atribut File. *Jurnal Computech & Bisnis*, 4(2).

Chan, A.S. (2014). Penerapan Kriptografi Rijndael Dalam Mengamankan File Mengunakan Interface Usb Flashdisk (Memory External). *Jurnal Pelita Informatika Budi Darma*, 3(2).

Fresly Nandar Pabokory, F.N., et al. (2015). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Jurnal Informatika Mulawarman*, 10(1).

Padate, R. & Patel, A. (2014). Encryption And Decryption of Text using AES Algorithm. *International Journal of Emerging Technology and Advanced Engineering*, 4(5)**.**

Rahmadoni, J. (2018). Perancangan Simulasi Pembelajaran Kriptografi Klasik Menggunakan Metode Web Based Learning. *INTECOMS: Journal of Information Technology and Computer Science*, *1*(1), 34-43. https://doi.org/https://doi.org/10.31539/intecoms.v1i1.160