IMPLEMENTATION OF ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM AS A SECURITY SYSTEM FOR ARCHIVING DATA AT DIGITAL LIBRARY IN PUSLITBANG GEOLOGICAL KELAUTAN

Zaenal Firdaus[1] Didit Andri Jatmiko[2]

[1]Teknik Informatika-Universitas Komputer Indonesia
Jalan Dipatiukur No 112-116 Bandung. 40312
E-mail :jenalfirdaus@email.unikom.ac.id[1] didit@email.unikom.ac.id[2]

ABSTRACT

The Research Center for Marine Geology is the Center for Research and Development of Marine Geology managed by government agencies under the ESDM department. At its inception, PPGL was supported by four technical fields, namely: Marine Geology, Marine Geophysics, Marine Operations, Information and General Affairs, with 222 people. Some of the facilities and infrastructure owned are from P3G.

Some of the problems that occur in the Marine Geology Research Center are data security. Data from the results of field research reports and other important data are easily accessible to all parts of the company that do not have the right to find out. Therefore we need a system to protect data from irresponsible parties. Cryptography is one technique to secure data. Cryptography using the Advanced Encryption Standard algorithm has the same block size and key, namely 128 bits, 192 bits, and 256 bits for the encryption and decryption process. This data security system is built to help protect important company data, such as data from field research reports. and company personal data. Conclusions obtained based on implementation and testing carried out to users, this system is able to provide strong security in data, protect data and easy to use.

Keywords: Cryptography, Advanced Encryption Standard, Algorithm, Encryption, Decryption.

PRELIMINARY

1.1 Background

The Research Center for Marine Geology is the Center for Research and Development of Marine Geology managed by government agencies under the ESDM department. At its inception, PPGL was supported by four technical fields, namely: Marine Geology, Marine Geophysics, Marine Operations, Information and General Affairs, with 222 people. Some of the facilities and infrastructure owned are from P3G.

Digital library in Pulitbang is one of the public service facilities located in the research institute of marine geology research center, especially filing, the archiving process is done manually / conventional, for example by storing reports in a folder which is then stored in a file cabinet. Of course this method is not effective and efficient because the more reports that will be archived, the greater the space needed to store the archive.

At the moment P3GL faces problems in report security, free reports are accessed by various parties and there are no safeguards in report reports including research reports, mapping, inventory, and investigations so that people can read and change because there is no application to encrypt files, then from that a good security is needed so that reports on the computer become safer.

Based on the existing problems, an application is needed to secure the filing report in the P3GL agency. In this case specifically to restrict other parties from seeing reports in order to reduce unauthorized use by P3GL. One way is to make the information data unreadable / incomprehensible to others. For this reason the research will using security with cryptographic techniques that can make digital information data illegible using the Advanced Encryption Standard (AES) algorithm.

Thus, this study will focus on building a system security application entitled "Implementation of the Advanced Encryption Standard (AES) Algorithm as a Security System for Archiving Data at Digital Libraries in the Marine Geology Research Center".

1.2 Identification of Problems

From the background described above the problems faced are:

1. There are no restrictions on access rights to view digital data archiving.
2. How to apply the Advanced Encryption Standard (AES) algorithm in encrypting confidential data so that the encrypted data cannot be read or understood by other parties.

1.3 Purpose and Objectives

Based on the research discussed, the purpose of this thesis is to implement an advanced encryption standard (AES) algorithm as a security system for archiving data in digital libraries. While the purpose of this study is:

1. Make restrictions on access rights to view digital data archiving.
2. Creating an application that can encrypt and decrypt data using the Advanced Encryption Standard algorithm that will be used to secure important data from a government agency at the Marine Geology Research Center.

1.4 Limitation of Problems

In completing the final project proposal, the problem is given so that the desired goals and objectives can be achieved. The limitations of the problem are as follows:

1. Report format that can be encrypted is .pdf
2. Before the data is hidden, encryption is first done with the password being converted into bytes using SHA-1
3. The password authentication process uses the SHA-1 hash function.
4. 4. This system will produce a ciphertext with the .pdf file format.
5. 5. Website-based system. Using PHP, Html and other web creation libraries.

2. ANALYSIS OF DESIGN AND IMPLEMENTATION

2.1 System Analysis

System analysis is a stage that aims to find out and observe what is involved in a system. The discussion on this system analysis is problem analysis, algorithm analysis, non-functional requirements analysis, and functional requirements analysis.

2.1.1 Problem Analysis

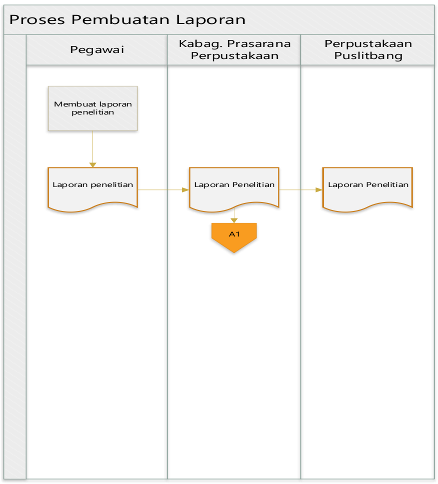
Problem analysis is the problem translation phase that existed before the system was built and aimed to help develop this cryptographic application. The following is a description of the problems that include the following:

1. There are no restrictions on access rights to view data filing reports on the results of research from the Marine Geology Research Center. This results in other people who have no interest being able to see and misuse the report file data.
2. An original report file that is submitted certainly can be seen many times and this causes other irresponsible people to abuse the report.

2.1.2 Analysis of the System in Run

Based on the results of observations and direct interviews obtained procedures performed by the Marine Geology Research Center in the system of archiving report data security in the Digital Library. Broadly speaking there are several steps that are carried out as follows:

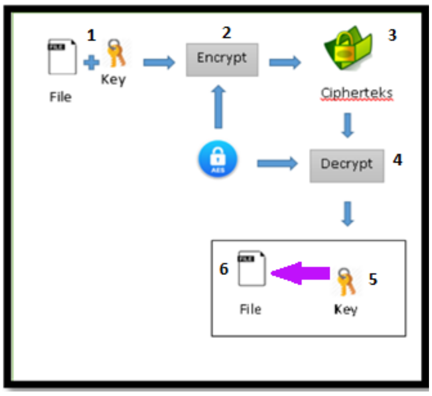
1. Research center staff make the results of research reports that have been carried out while serving outside the city of Bandung.
2. The results of the research report are printed to be filed into the Library at the Research Center for Marine Geology.
3. Research center staff submit the results of research report documents to the Marine Geology Research Center library.
4. Head of Infrastructure Library Research Center receives the research report document.



Gambar 1. System Analysis that is running

2.1.3 Analysis of the System that was built

The system built is a system that can perform cryptography of document files. This cryptographic process is carried out so that the document file from the research report cannot be seen / read using the file opening system. This can be done assuming that each document file that will be subject to cryptographic algorithms will experience value added so that the file cannot be read by a normal file opening system. For more details the process that will occur in the application to be built is as follows :



Gambar 2. Analysis of the System that was built

The system analysis built is a complete picture of the analysis of the system to be built. The systems built are as follows:

1. Research center staff generate private keys and public keys. Private keys stored by employees and private keys must be maintained properly because this key will be used for the decryption process. If this key is successfully obtained by another party parties.

1. The public key that has been raised in the first phase will be sent to the Head of the Infrastructure Research and Development Agency. This key is useful for encrypting document files. This delivery can be done through other networks outside the application. This key is safe because if the public key is successfully retrieved, the other party cannot do the decryption process because the decryption process only uses the private key.
2. The third stage is when the public key has been obtained by the sub-directorate of infrastructure, the research center will search the document file.
3. After the file and key are ready, they will be entered into the encryption system. In this process the file will be encrypted by inserting a decryption delimiting value on one byte array index. In the encryption process, it will produce a file with the format .pdf.
4. When the encryption process has been carried out and produces an encrypted file then the company will then send the encrypted file to the Head of Infrastructure Development Agency.
5. Encrypted files that have arrived at the research center infrastructure will be used in the decryption process. By using the previously stored private key and the encrypted file, the decryption process can be done. This decryption process will return the encrypted file to the original document file.

2.1.4 Analysis of the Encryption Process *Advanced Encryption Standard*(AES)

he AES algorithm encryption process in round 0 and round 1. Suppose that the plaintext and key used are examples of cases like the following that have added dammy data:

Plaintext: "UNIKOM9807645317"
Key: "ADMIN09512345678"

The first step is to change the plaintext and key above to become a hexadecimal form where the next process will all use the hexadecimal form. The conversion results will be like this:

Plaintext : "40 45 44 49 20 41 4C 59 41 4E 54 4F 32 30 31 36"
Key : "52 49 4A 4E 44 41 45 4A 31 32 33 34 35 36 37 38"

After converting plainteks and keys into hexadecimal, we will arrange the plaintext and key into a 4x4 matrix as shown below:

44	20	41	32
45	41	4E	30
44	4C	54	31
49	59	4F	36

52	44	31	35
49	41	32	36
4A	45	33	37
4E	4C	34	38

Before entering the initial round or round 0, we must first look for the round key for each round. In round 0, the subKey is the same as the first input key. In round 0 the plaintext will go through the AddRounKey process where at this stage XOR calculations occur between plaintext and key.

The XOR process occurs for each cell in the matrix above, for example the Text matrix [1,1] Key XOR matrix [1,1] and Text matrix [2,1] Key XOR matrix [2,1], and so on. Below this will be simulated the XOR process between the 1st row of the 1st column on each matrix.

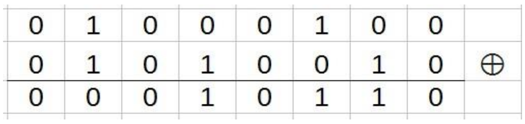
1st row of 1st column of plaintext matrix: 44
1st row of 1st column of key matrix: 52

To do an XOR first change the shape from hexa to binary form so as below.

1st row 1st column of plaintext matrix (8 bit binary): 01000100

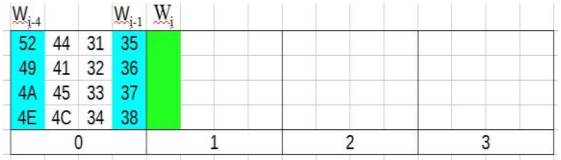
1st row of 1st column of key matrix (8-bit binary): 01010010

Then compare the two parameters bits per bit according to the description in table 2.2 so that it produces



0	1	0	0	0	1	0	0	
0	1	0	1	0	0	1	0	⊕
0	0	0	1	0	1	1	0	

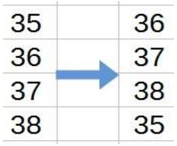
Gambar 3. Analisis Matrik AES



W_{i-4}			W_{i-1}	W_i			
52	44	31	35				
49	41	32	36				
4A	45	33	37				
4E	4C	34	38				
0				1		2	3

Gambar 4. Analisis Matrik AES2

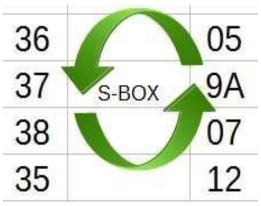
To obtain the i column from the 4x4 matrix, columns to i-4 and i-1 are needed from the existing round key. As in the table above, to obtain the first column from the 1st subKey, the first and 4th columns of the 0th subKey are needed. How to get it is as follows: Specifically for the first column in each round key the calculation method is different from the calculation in columns 2, 3 and 4. First, take the Wi-1 column then the top cell is moved to the lowest cell or the term RotWord.



35		36
36	→	37
37		38
38		35

Gambar 5. Analisis Matrik AES3

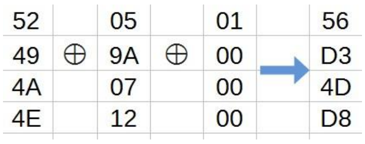
After that the results are substituted with an S-Box where the procedure for substitution has been explained in section 3.1.2.1. The substitution results with S-Box are as follows:



36		05
37	S-BOX	9A
38		07
35		12

Gambar 6. Analisis Matrik AES4

After substitution, the results will be XORed with the Wi-4 column and the first column of the Rcon table which is found in section 3.1.2.5. Of course the procedure for XOR is also the cell against cells whose sequence of rows and columns are the same. XOR results are shown in the image below.

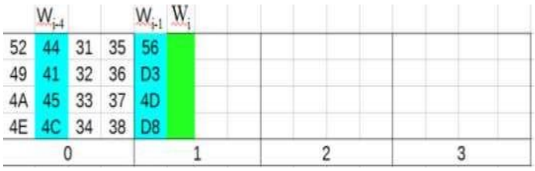


52		05		01		56
49	⊕	9A	⊕	00	→	D3
4A		07		00		4D
4E		12		00		D8

Gambar 7. Analisis Matrik AES5

After obtaining the first column from the 1st subKey, the subKey table will look like this

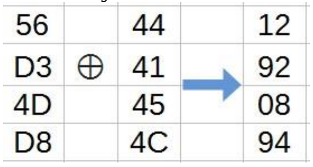
.



	W_{i-4}			W_{i-1}	W_i				
52	44	31	35	56					
49	41	32	36	D3					
4A	45	33	37	4D					
4E	4C	34	38	D8					
0				1				2	3

Gambar 8. Analisis Matrik AES6

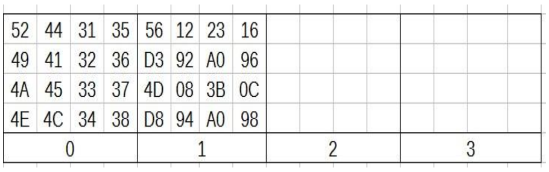
Now we will look for column 2 of the 1st subKey, where columns i-1 and i-4 are also needed from the subKey table. The way to find the second column is simpler than by looking for the first column, just XOR column i1 and i-4 only. The result will be like this.



56		44		12
D3	⊕	41	→	92
4D		45		08
D8		4C		94

Gambar 9. Analisis Matrik AES7

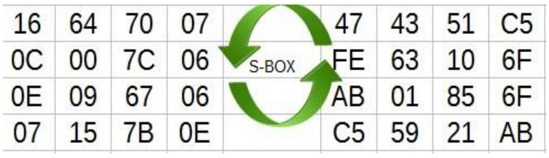
Next to get the 3rd and 4th columns the same way as the 2nd column. So the overall results will be like this.



52	44	31	35	56	12	23	16								
49	41	32	36	D3	92	A0	96								
4A	45	33	37	4D	08	3B	0C								
4E	4C	34	38	D8	94	A0	98								
0				1				2				3			

Gambar 10. Analisis Matrik AES8

After completing getting the subKey for the 1st round we will proceed to the subBytes process. In this section we make the S-Box substitution process against the addRoundKey results in the 0th round. Where the results are as follows.

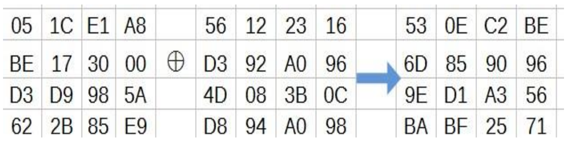


16	64	70	07		47	43	51	C5
0C	00	7C	06	S-BOX	FE	63	10	6F
0E	09	67	06		AB	01	85	6F
07	15	7B	0E		C5	59	21	AB

Gambar 11. Analisis Matrik AES9

Next is the addRoundKey process, same as addRoundKey which occurs in round 0, in this process the mixColumns results obtained above are XORED with the 1st round subkey that we have obtained earlier. The result is as follows:

.



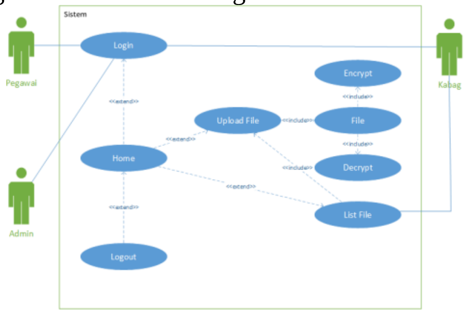
05	1C	E1	A8		56	12	23	16		53	0E	C2	BE
BE	17	30	00	⊕	D3	92	A0	96	→	6D	85	90	96
D3	D9	98	5A		4D	08	3B	0C		9E	D1	A3	56
62	2B	85	E9		D8	94	A0	98		BA	BF	25	71

Gambar 12. Analisis Matrik AES10

The following is the result of the 1st round, for the 2nd to 9th round just repeat the process above, and for the last round or 10th round, skip the mixColumns process. After that, we will get the results of encryption from the input plaintext.

2.1.5 Use case Diagram

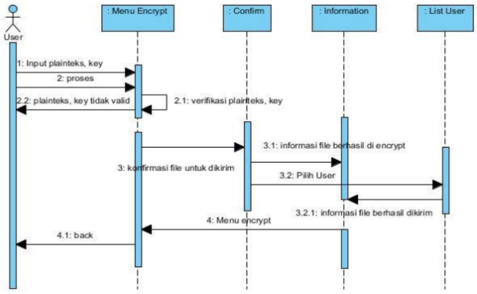
Use case diagram is a diagram that shows the functionality of a system or class and how the system interacts with the outside world and describes the system functionally visible to the user. From the identification of the actors involved above, the use case diagram can be seen in Figure 13.



Gambar 13. *Use case Diagram*

2.1.6 *Sequence Diagram* Enkripsi File

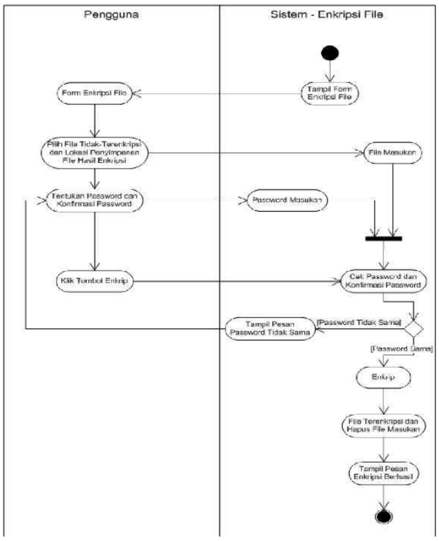
Interaction between actor users and use cases Encryption is explained in the Sequence Diagram in Figure 14 as follows:


User
: Menu Encrypt
: Confirm
: Information
: List User
1: Input plainteks, key
2: proses
2.2: plainteks, key tidak valid
2.1: verifikasi plainteks, key
3.1: informasi file berhasil di encrypt
3: konfirmasi file untuk dikirim
3.2: Pilih User
3.2.1: informasi file berhasil dikirim
4: Menu encrypt
4.1: back

Gambar 13. *Sequence Diagram Enkripsi File*

2.1.7 *Aktivity Diagram Enkripsi File*

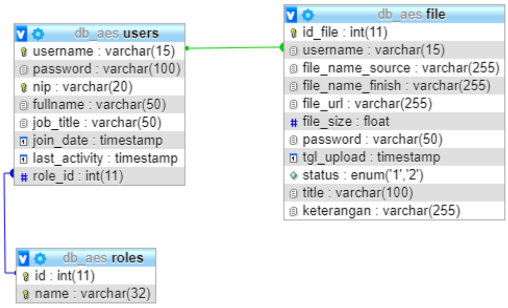
The interaction between user actors and the File Encryption case is explained in the activity diagram in Figure 3.22 as follows
:


Pengguna
Sistem - Enkripsi File
Tampil Form Enkripsi File
Form Enkripsi File
Pilih File Tidak-Terenkripsi dan Lokasi Penyimpanan File Hasil Enkripsi
File Masukan
Tentukan Password dan Konfirmasi Password
Password Masukan
Klik Tombol Enkrip
Cek Password dan Konfirmasi Password
Tampil Pesan Password Tidak Sama
[Password Tidak Sama]
[Password Sama]
Enkrip
File Terenkripsi dan Hapus File Masukan
Tampil Pesan Enkripsi Berhasil

Gambar 14. ***Aktivity Diagram Enkripsi File***

2.1.8 Relationship Scheme

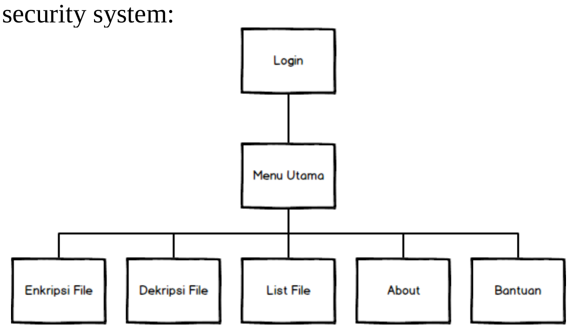
Table Database Relations describes relationships between tables in this research database. Following is the Database Relationship Table.



Gambar 15. Skema Relasi

2.1.9 Struktur Menu

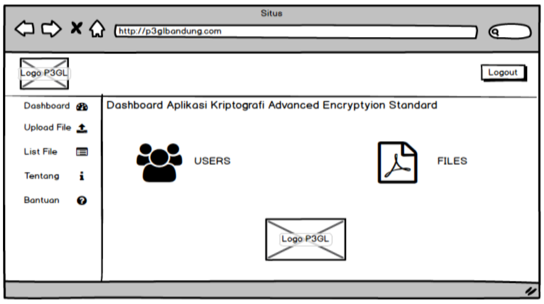
In Figure 16 below is the menu structure of the data security system:



Gambar 16. Struktur Menu

2.1.10 Interface Design

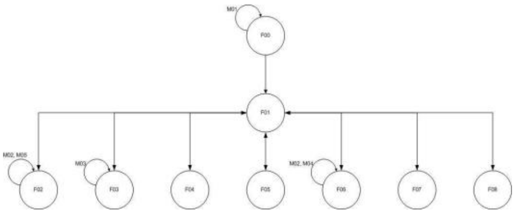
The interface design is made to give a concept to the implementation of making an interface later on the system. The following is an illustration of the interface design in a data security system
:



Gambar 17. Antarmuka AES

2.1.11 Semantic network Menu

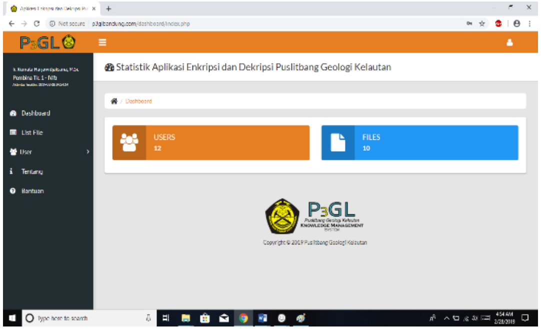
Semantic network is a graphical representation of knowledge that shows the relationship between various objects, consisting of circles connected with arrows that show objects and information about these objects. The following is Figure 18 which describes the semantic network in the data security system
:



Gambar 18. Jaringan Semantik

2.1.12 Interface Implementation

In this section, it will be described regarding the appearance of this application interface starting from the first time it is run until it has finished running. The following will be given an explanation and a picture of the displays in this application
.


P3GL
Statistik Aplikasi Enkripsi dan Dekripsi Puslitbang Geologi Kelautan
Dashboard
USERS
12
FILES
10
Dashboard
List File
User
Tentang
Bantuan
P3GL

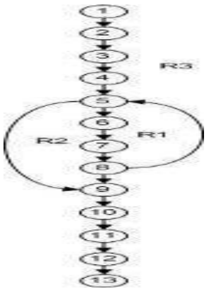
Gambar 19. Implementasi Antarmuka AES

3. RESULTS AND DISCUSSION

3.1 Alpha Testing

Alpha testing is used to test applications with various conditions, the method used in alpha testing is the white-box method. The white-box test is used to ensure all commands and conditions for the implementation of the AES algorithm.

The following is the AES encryption flow graph shown in Figure 20



Gambar 20. *Flow Graph AES*

3.2 Beta Testing

Beta testing is done through performance testing or trial directly to users to try the new system and the results of these experiments are recorded to determine the level of accuracy and speed of the system.

No.	Nama *File*	Rincian *File*	Ukuran *File* (KB)	Waktu Enkrip (detik)	Ukuran *File* Hasil (KB)	Rasio
1	Potensi Energi.pdf	Teks, Gambar	18.358	3,18	18.358	100%
2	Buku Panduan emonDAK SDA.pdf	Teks, Gambar	21.512	3,24	21.512	100%
3	DAK 26 JANUARI 2012 SDA BANDUNG.pdf	Teks, Gambar	38.212	5,52	38.212	100%
4	emondak_bg3.pdf	Teks, Gambar	19.574	2,76	19.574	100%
5	eMonDAK2012.pdf	Teks	21.532	3,17	21.532	100%
6	Sebaran_Sedimen.pdf	Teks	35.131	5,14	35.131	100%
7	Laporan-P3GL.pdf	Teks, Gambar	26.228	3,78	26.228	100%
8	Dokumen-Atlas.pdf	Teks, Gambar	22.893	3,24	22.893	100%
9	ymsgr1150_0192.pdf	Teks	18.920	2,69	18.920	100%

Tabel 1. Pengujian Beta

4. CONCLUSIONS AND SUGGESTION

4.1 Conclusions

Based on the results of research, system analysis, system design, system implementation, and system testing, conclusions can be taken as follows:

1. System that can be used to process encryption and decryption of files with various sizes and types of files, using the AES algorithm.
2. The file size of the encrypted attachment is not affected by the attachment file format, but is influenced by the initial size of the attached file. The larger the file size and the longer the AES key is used, the greater the size of the encryption file produced.
3. When the decryption process requires more computing compared to the encryption process, so the need for the decryption process takes longer compared to the encryption process.

4.2 SUGGESTION

This AES Cryptography System can be further developed, therefore constructive suggestions and criticisms suggest several improvements to the system as follows:

1. For relatively large files before the encryption process, it would be better if compressed first, this is useful to speed up the process of encryption and decryption using the AES algorithm.

5. BIBLIOGRAPHY

[1] Daemen, J; V, Rijmen. 2002. “The Design of Rijndael.” AES—Advanced Encryption Standard. Information Security and Cryptography. SpringerVerlag, Berlin, Heidelberg, New York.

[2] Handayani, Dewi. 2001. *Sistem Berkas*. Yogyakarta: J&J.

[3] Menezes, A.; van Oorschot, P.; Vanstone, S. 1996. *Handbook of Applied Cryptography*. Canada: CRC Press.

[4] Surakhmad, Winarno. 1980. *Pengantar Penelitian Ilmiah: Dasar, Metode, dan Teknik*. Bandung: Tarsito.

[5] Sommerville, Ian. 2001. *Software Engineering 6th*. Addison Wesley.

[6] Munir, Rinaldi. (2004). *Bahan Kuliah IF5054 Kriptografi*. Departemen Teknik Informatika: Institut Teknologi Bandung.

[7] Schneier, Bruce. 1996. *Applied Cryptography 2nd Edition.* Fusionopolis Walk: John Wiley & Sons.

[8] Nechvatal, James, dkk. 2000. *Report on the Development of the Advance Encryption Standard (AES).* NIST.

[9] Kurniawan, Yusuf. 2004. Kriptografi Keamanan Internet dan Jaringan Komunikasi. Bandung: Informatika.

[10] Rosa A.S dan M.Shalahuddin, "Rekayasa Perangkat Lunak", Bandung, *Informatika, 2013*.

[11] M. K. MZ, "Pengujian perangkat lunak metode black-box berbasis equivalence partitions pada aplikasi sistem informasi sekolah," *Jurnal Mikrotik* , vol. 6, p. 3, 2016.

[12] Sukrisno, et. al., 2007, Implementasi Steganografi Teknik EOF Dengan Gabungan Enkripsi Rijndael, Shift Cipher Dan Fungis Hash MD5, tersedia pada:http://p3m.amikom.ac.id/p3m/ TEKNIK%20EOF.pdf -., tanggal akses : 24 Februari 2019.

[13] Rifki Sadikin, 2012, Kriptografi Untuk Keamanan Jaringan, Penerbit ANDI, Yogyakarta.