

# File Cryptography Optimization Based on Vigenere Cipher and Advanced Encryption Standard (AES)

**Muslih\*<sup>1</sup>, L. Budi Handoko<sup>2</sup>**

*Informatics Engineering, Computer Science Faculty, Dian Nuswantoro University*

*E-mail : Muslih@dsn.dinus.ac.id\*<sup>1</sup>, handoko@dsn.dinus.ac.id<sup>2</sup>*

*\*Corresponding author*

**Aditya Rizqy<sup>3</sup>**

*Informatics Engineering, Computer Science Faculty, Dian Nuswantoro University*

*E-mail : aditya.rizqy@gmail.com<sup>3</sup>*

---

**Abstract** - The rapid The main problem in the misuse of data used in crime is the result of a lack of file security. This study proposes a data security method to protect document files using the Advanced Encryption Standard (AES) algorithm combined with the Vigenere Cipher. This research carried out 2 processes, namely the encryption process and the decryption process. The encryption process will be carried out by the AES algorithm and then encrypted again with the Vigenere Cipher algorithm. The experiments show that the proposed method can encrypt files properly, where there are changes in the value of the document file and the encrypted file cannot be opened and the description results do not cause changes to the original file. The results of this study are that the system is able to work properly so as to produce file encryption and decryption using the AES method combined with the Vigenere Cipher. In document files, the largest difference in encryption and decryption time is 8 seconds, while in image files the difference in encryption and decryption time is 17 seconds. This longest time difference is generated by large files.

**Keywords** – File, Cryptography, Vigenere Cipher, Advanced Encryption Standard (AES)

## 1. INTRODUCTION

---

The information exchanged can be in the form of data, files, messages, music, videos and pictures. Data is one example of one of the most important assets in the ongoing life of companies, government agencies, educational institutions and even individuals. Information exchange media can simplify and speed up the desired exchange of information. That way, humans can solve their problems easily and quickly. If the exchange of information is carried out without strict data security, it is impossible for the data to be stolen by unauthorized persons. In this day and age, problems related to data security and confidentiality are things that must be considered in communicating using a computer [1]–[4]. There have been frequent cases of leakage of confidential data by unauthorized parties such as hackers and crackers which have resulted in huge losses for the data owner [5], [6]. This of course will disturb the data owners, as well as parties who wish to communicate in order to exchange information for both personal and group interests. So that it can be said that the protection of the originality of data or information is an important requirement in the present and beyond.

There are several ways to protect data, one of which is to apply cryptography. In today's information technology, ways have been developed to minimize various kinds of attacks, for

example tapping and changing data by irresponsible persons. This transformation produces a solution for 2 (two) kinds of data security problems, namely privacy and authentication issues [1]. Cryptography [2] is securing data to documents by using encryption techniques for data to documents so that they cannot be read or understood. By using cryptography, information in the form of data is encrypted into a form that cannot be read or understood. In cryptography, there are two processes, namely encryption and decryption. The message to be encrypted is referred to as plaintext (plain text). So called because this information can easily be read and understood by anyone. The algorithm used to encrypt and decrypt a plaintext involves the use of some form of key. Plaintext messages that have been encrypted (or encoded) are known as ciphertexts [6], [7].

Cryptography provides several services that support improving data or information security. Confidentiality is something that is highlighted to protect information from being accessed by irresponsible people. Starting from changing plaintext or actual messages into ciphertext or messages that have a code. People who are entitled to access it must have a key or keys. Encryption is changing the original message or plaintext into coded messages or ciphertext. While Decryption is changing back the encoded message or ciphertext into the real message or plaintext. The key or key is only known by the person who has the right. There are classical and modern methods in cryptography. Examples of classic cryptography are Vigenere Cipher, Autokey Cipher, Reverse cipher, Super Encryption, and many more. According to [2] modern cryptography is a stream cipher, block cipher, Data Encryption Standard (DES), Advance Encryption Standard (AES), International Data Encryption Algorithm (IDEA), A5, RC4 and many more. In this paper the author combines classical cryptography and modern.

AES is a cryptographic algorithm that can be used to secure various types of data where the algorithm is a symmetric ciphertext block that can encrypt and decrypt information [8], [9]. AES is one of the emerging algorithms for use in symmetric key cryptography. AES is a block cipher algorithm that uses a permutation and substitution system (P-Box and S-Box) different from the Feistel network used by DES [4]. There are 3 types of AES, namely AES-128, AES-192, AES-256. The division of these types of AES groups is based on the length of the key used. The numbers after the word AES describe the length of the key used in each AES. AES has advantages in terms of security, speed, and characteristics of the algorithm and its implementation.

Vigenere is an algorithm that is used to encrypt data or messages in a way, data or information will be encoded using a keyword (Key) in the form of a word. Each alphabet in the data or information is matched exactly with the alphabet contained in the specified keyword, then the encryption or encryption process is carried out [10]. The Vigenere Cipher in essence is almost the same as the basic Caesar Cipher, namely using encoding or encryption every letter in plaintext becomes another alphabet in ciphertext. The fundamental difference in Caesar Cipher with Vigenere Cipher is that the letters are the same in plaintext not all are encrypted to become the exact same alphabet in ciphertext. Therefore, the Vigenere Cipher shift of the alphabet is determined by the alphabet that is in the key (Key) and the word in it is always repeated [7]. The most important goal of Vigenere Cipher is to hide the relationship between plaintext and ciphertext by using keywords to make a benchmark determining the shift of the alphabet. The most important advantage of Vigenere Cipher over previous classic cryptographic methods (Caesar Cipher) is that substitutions for the cipher have polyalphabetic properties, where the same alphabet has different substitution alphabet - different [11], [12]. Vigenère is a method of encoding alphabetic text by using a series of Caesar ciphers alphabetically based on the keyword. The Vigenère encoding is a simplified form derived from the polyalphabetic substitution cipher. In using the Vigenere Cipher algorithm to encrypt, a key is needed to minimize leakage of the confidential data.

Based on the advantages possessed by AES (Advanced Encryption Standard) and the ease of use of the Vigenere Cipher algorithm in encrypting simple text, in this final project the AES (Advanced Encryption Standard) algorithm is used to encrypt files first, then the key is encrypted. back to using the Vigenere Cipher.

## 2. RESEARCH METHOD

### 2.1. Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) symmetric algorithm that uses the same key for the encryption and decryption process. The AES algorithm has three key options, namely types: AES-128, AES-192 and AES-256. Each type uses a different internal key, namely the round key for each round process [8]. The AES algorithm encryption process consists of 4 types of transformation bytes, namely SubBytes, ShiftRows, MixColumns, and AddRoundKey. An illustration of the AES encryption process can be described as in Figure 1. Figure 1 has been describe using detail explanation in Figure 2. The AES-128 encryption loop process is done 10 times ( $a=10$ ), as follows:

1. Addroundkey
2. Round a-1 times, the processes that are carried out in each round are: SubBytes, ShiftRows, MixColumns, and AddRoundKey.
3. Final round, is the process for the last round which includes SubBytes, ShiftRows, and AddRoundKey. Whereas in the AES-128 decryption process, the loop process is also done 10 times ( $a = 10$ ).

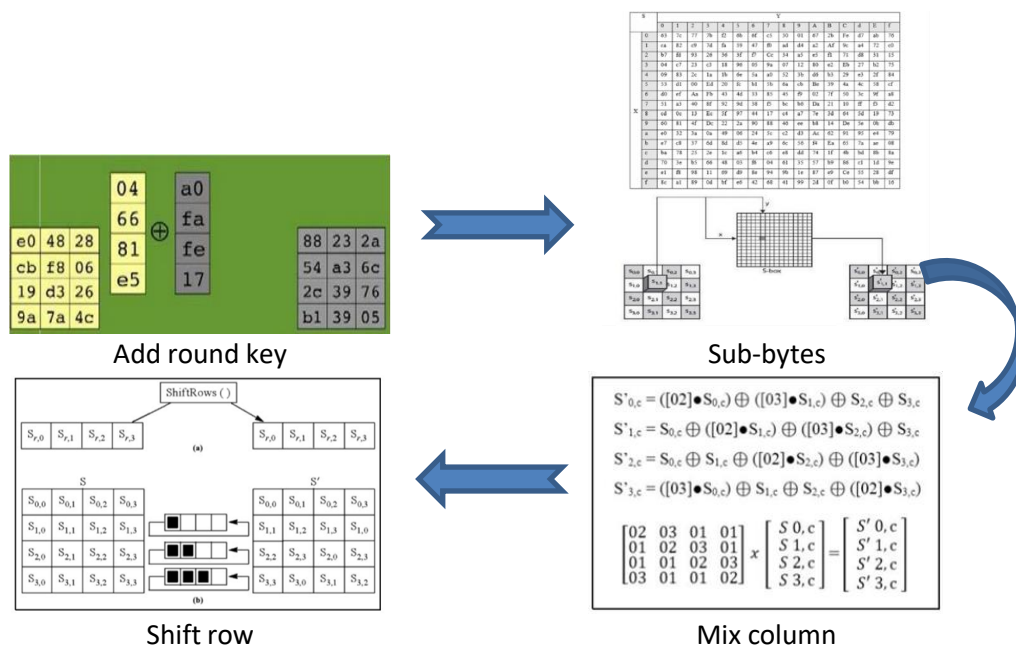


Figure 1. AES Stages

The Add Round Key works by XORing between the initial states (plaintext), with the cipherkey at this stage also called the initial round. The SubBytes process is an operation that will perform non-linear substitution by replacing each state byte with a byte in a table called the S-Box table. In the sub bytes illustration above, there are column and row numbers. Each box in the cipher block contains information in hexadecimal form, consisting of two digits which can

be numbers, letters, or numbers, all of which are listed in the Rijndael S-Box. This is as stated in the previous discussion. At each step it takes one of the squares in the matrix to match the left digit as the row and the digit on the right as the column. After knowing the columns and rows, you can retrieve a table content from the Rijndael S-Box. ShiftRows operates on each row of the state table. This process works by shifting the bytes in the last 3 rows (rows 1, 2 and 3) with the number of rotations depending on the number of rows and not exceeding Nb, with an Nb value of 4-word which can be seen in table 1. Where bytes are in the 1st line will be shifted left 1 time, the bytes in the 2nd line will be shifted left 2 times, and the bytes in the 3rd line will be shifted left 3 times. While line 0 does not experience a shift. MixColumns is to multiply each element of the chipper block using a matrix. The MixColumns transform operates on each column of the state by treating each 4-byte state column as a four-term polynomial in the Galois field or GF (28) and modulo (x4+1) then multiplied by the fixed polynomial a(x), expressed as follows a (x) = {03}x3 + {01}x2 + {01}x + {02}.

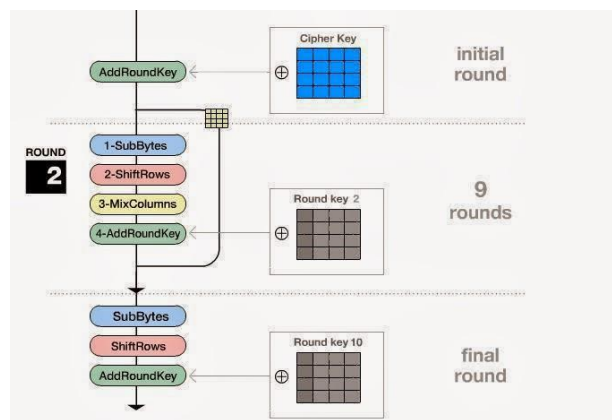


Figure 2. Common AES Scheme

## 2.2. Vigenere Cipher

Vigenere Cipher is a manual compound alphabet encryption method (polyalphabetical substitution cipher) [13], [14]. The Vigenere Cipher basically uses a technique that is not much different from the Caesar Cipher [15].

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 3. Vigenere Cipher Tabula Recta

The rule is, in the Vigenere Cipher, each character in the plaintext can be encrypted with a different key. The first character in the plaintext is encrypted using a key which is the first character of the keyword and likewise for the next step. The polyalphabetic nature of the Vigenere Cipher is implemented with a Vigenere square [14]. Its periodic nature is seen when the key length is the same as the plaintext length. If the key length is only one character, the encryption is the same as a regular Caesar Cipher. The Vigenere square is used to make the encryption process with the Vigenre Cipher easy. The leftmost column of the square declares the key character, but the topmost row declares the plaintext character [5], [10], [16]. Each line in the square declares a character. Ciphertext characters obtained using CaesarOCipher where the displacement of plaintext characters is ensured by the decimal value of the key character.

### 2.3. Proposed Method

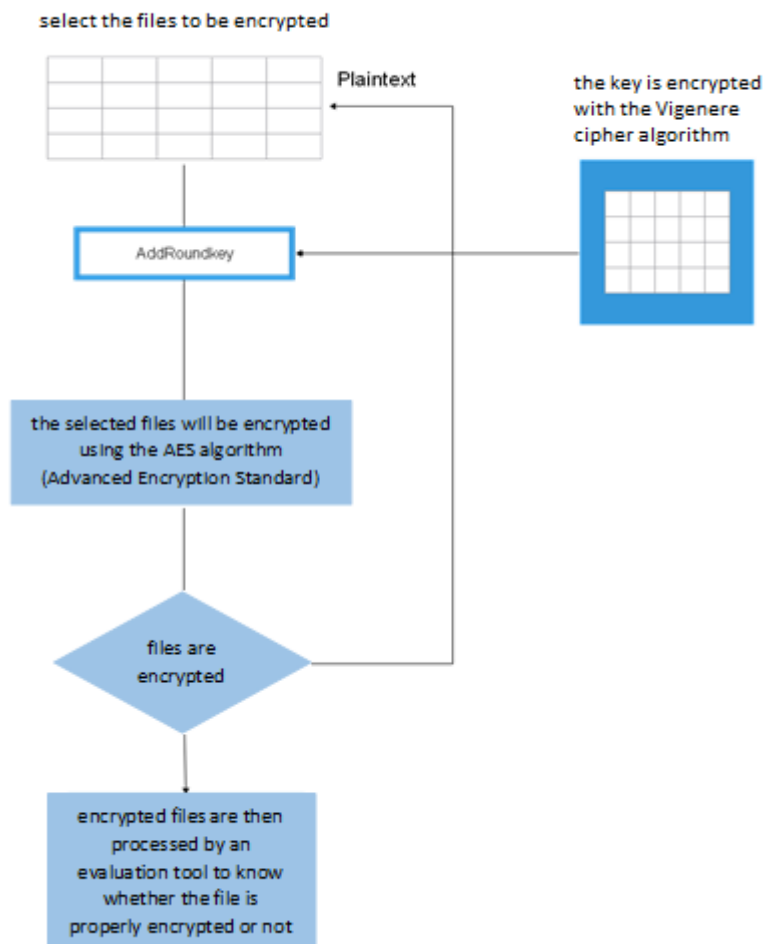


Figure 4. Encryption Scheme

The explanation of Figure 14 above is:

1. The user will select one of the files to be encrypted.
2. If have selected the file to be encrypted, then specify the key to decrypt the file.
3. After determining the key, then the key is encrypted by the Vigenere Cipher algorithm.

4. After encrypting the key, then the file will be encrypted using the AES (Advanced Encryption Standard) algorithm.
5. If the encryption is successful, then the encrypted file is encrypted properly.
6. If encryption fails, return again to select files to be encrypted using AES (Advanced Encryption Standard).
7. If the encryption is successful, the next step is to evaluate the results of the encryption using an evaluation tool.
8. If the evaluation results state that the encryption works well, then the encryption can be said to be successful.

The explanation of Figure 5 :

1. The first step to describe this research is to decrypt the key encrypted by the Vigenere Cipher algorithm.
2. After the key is perfectly decrypted, then the key is used to open / decrypt file encryption encrypted by the AES (Advanced Encryption Standard) algorithm.
3. Then comes the original file from the encryption.

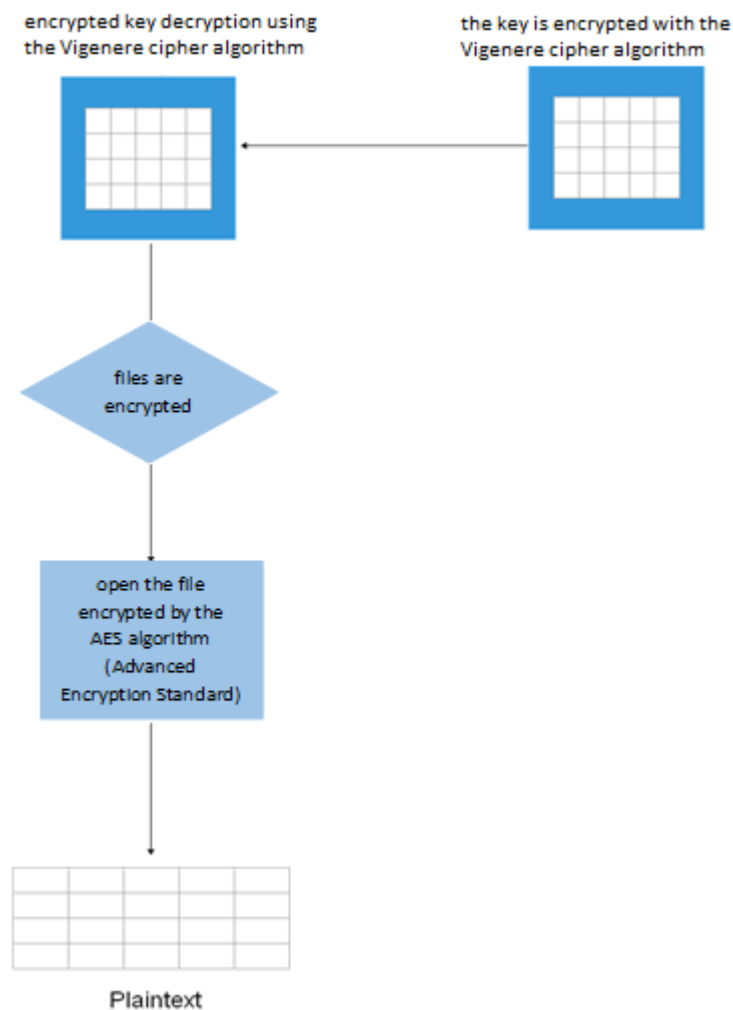


Figure 5. Decryption Scheme

## 2.4. Data Collection

Table 1. Image File






No.	Image	Format File	Dimension	File size (bytes)
1.		.jpg	1920x1080	5,289
2.		.jpg	1920x1080	14,992
3.		.png	1920x1080	18,084
4.		.png	1920x1080	1,616
5.		.bmp	512x512	263,222

Table 1 shows the image files used for encryption testing. There are 5 image files taken from HDW (<http:hdw.eweb4.com/bmp/>). There are various formats, dimensions and file sizes on the website. Table 2 shows the document files used for encryption testing. There are 5 document files taken from the researcher's PC.

## 3. RESULTS AND DISCUSSION

In this sub-chapter, the researcher will show how to implement AES and Vigenere Cipher to encrypt and decrypt document files. The steps taken in the encryption and decryption process for document files are explained below, namely the AES Encryption Algorithm and the Vigenere Cipher. The first step is to enter the document file, where the file entered is a file with TXT format. After the file process is entered, the system will process the file towards the encryption process. The encryption process is carried out as a matter of changing the original file into another file which turns into a file that cannot be opened and is no longer known by other people. After the encryption process is carried out, the encryption results appear where the encryption result is a result of the original file encryption process.

### 3.1. Encryption Process

Data Encryption The data encryption process stage designs a program to develop the AES and Vigenere Cipher algorithms. The encryption process requires several steps. Where to find out the value in the document file, namely by changing the file value which was originally binary converted to hexadecimal, for the initial stages of AES and Vigenere Cipher encryption, namely by XORing the plaintext or initial state on iv that has been input, then the results are encrypted with AES, the first AES process is the initial round then it is continued on the four transformations, namely:

1. Subbytes
2. Shiftrows

- 3. Mix-columns
- 4. Addround key

Table 2. Encrypt Result using Image File






Image and file type	Dimension	Original size	Encryption size	Encryption file size	16 char AES key	Vigenere cipher key	Vigenere key result
 .jpg	1920x1080	5,289	5,289	5,289	univdiannu swanto	udinus	oqgixauqvh mouqbb
 .jpg	1920x1080	14,992	14,992	14,992	qwertyuiop lkjhgf	oke	egifdcissdv oxrkt
 .png	1920x1080	18,084	18,084	18,084	zxcvbnmlkj hgfdsa	presiden	oognjqyza lyngwn
 .png	1920x1080	1,616	1,616	1,616	qazwsxedcr fvtgby	apel	qpdhsmioc ggtvfj
 .bmp	512x512	263,222	263,222	263,222	vigenereku aesaes	cuka	xcqepybem okeuos

Table 3. Encrypt Result using Document File

File name	Format File	Dimension	Original size	Encryption size	Encryption file size	16 char AES key	Vigenere cipher key
BAB 1	.docx	582,298	582,298	582,298	satuduatigaempat	angka	snzedunzsgarszat
Contoh skript	.pdf	1,001,002	1,001,002	1,001,002	merekasemuacinta	saya	eepecaqeeuycanra
http buku	.txt	306	306	306	semuakarenakitaa	yaiyalah	qeusavaycniieah
ppt	.pptx	399,201	399,201	399,201	akukaudandirimuu	jahat	jkbktdhdhnrppmnd
Surat balasan KP	.docx	356,304	356,304	356,304	tujuhdelapanlima	nomor	giviysxogbnxwdn

### 3.2. Decryption Process

The first stage is the decryption file, where the decryption file is the process of returning the original file after the encryption process is carried out. The decryption process means files that cannot be opened initially become original files. The result of the decryption is the file returns to normal. Chiphertext decryption in the Decryption process requires stages such as the encryption process. the initial stages of ciphertext decryption using AES and Vigenere Cipher, for the initial stages of AES and Vigenere Cipher decryption, namely by decrypting the key generated by the Vigenere Cipher then the last block with the AES algorithm, the AES decryption process goes through four transformations, namely:

1. Addroundkey



2. invShiftRows
3. Invmix-Columns
4. invSubbytes

The four transformations above are repeated 10 times and in the first iteration without going through the invmix-columns process then the results are XORed with the AES key, this process is usually called the initial round, the last result of the decryption is XORed with the previous ciphertext block or iv specifically for the first ciphertext block. below. This is the result of the decryption using MATLAB.

Table 4. Encrypt Decrypt Time Execution using Image File

Encryption time (Second)	Decryption time (Second)
5.462 s	6.936 s
16.381 s	20.703 s
18.906 s	24.663 s
1.774 s	2.271 s
279.874 s	362.752 s

Table 5. Encrypt Decrypt Time Execution using Document File

Encryption time (Second)	Decryption time (Second)
619.952 s	795.925 s
1049.468 s	1420.782 s
0.366 s	0.467 s
446.355 s	619.630 s
407.449 s	494.857 s

#### 4. CONCLUSION

Application of AES-128 bit and Vigenere Cipher capable of encrypting document files (.docx, .pdf, .txt, .pptx) image files (.jpg, .bmp) as evidenced by changes in value in document files and image files, changes in these values through the AES encryption process and the Vigenere Cipher. AES uses 16 different characters while the Vigenere Cipher also uses a different key. The AES-128 and Vigenere Cipher algorithms can encrypt file extensions document files (.docx, .pdf, .txt, .pptx) image files (.jpg, .bmp) and produce files with document file extensions (.docx, .pdf, .txt, .pptx) image files (.jpg, .bmp) that can no longer be opened and descriptions make no changes to the files. In future research, modern cryptographic algorithms or a combination of classical and modern cryptography can be used to speed up file execution time. The executable file can be added so that it is more diverse and can be varied using color and grayscale images.

#### REFERENCES

- [1] J. P. Sermeno, K. A. S. Secugal, and N. E. Mistio, "Modified Vigenere cryptosystem: An integrated data encryption module for learning management system," *International Journal of Applied Science and Engineering*, vol. 18, no. 4(Special Issue), pp. 1–10, 2021, doi: 10.6703/IJASE.202106\_18(4).003.
- [2] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, and A. A. M. Khalaf, "Efficient Combination of RSA Cryptography, Lossy, and Lossless Compression Steganography Techniques to Hide Data," *Procedia Comput Sci*, vol. 182, pp. 5–12, 2021, doi: 10.1016/j.procs.2021.02.002.
- [3] K. R. Ilaga and C. A. Sari, "Analysis of Secure Image Crypto-Stegano Based on Electronic Code Book and Least Significant Bit," *Journal of Applied Intelligent System*, vol. 3, no. 1, pp. 28–38, 2018.

- [4] K. Prasad and H. Mahato, "Cryptography using generalized Fibonacci matrices with Affine-Hill cipher," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 8, pp. 2341–2352, Nov. 2022, doi: 10.1080/09720529.2020.1838744.
- [5] D. Suprihant *et al.*, "Combination Vigenere Cipher and One Time Pad for Data Security," *International Journal of Engineering & Technology*, vol. 7, no. 2, pp. 92–94, 2018.
- [6] A. Susanto, D. R. I. Moses Setiadi, E. H. Rachmawanto, C. A. Sari, R. R. Ali, and I. U. Wahyu Mulyono, "Dual Security Method for Digital Image using HBV Encryption and Least Significant Bit Steganography," in *Journal of Physics: Conference Series*, May 2019, vol. 1201, no. 1. doi: 10.1088/1742-6596/1201/1/012024.
- [7] C. A. Sari, G. Ardiansyah, D. R. I. Moses Setiadi, and E. H. Rachmawanto, "An improved security and message capacity using AES and Huffman coding on image steganography," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 17, no. 5, pp. 2400–2409, 2019, doi: 10.12928/TELKOMNIKA.v17i5.9570.
- [8] S. L. Chikouche and N. Chikouche, "An improved approach for lsb-based image steganography using AES algorithm," in *2017 5th International Conference on Electrical Engineering - Boumerdes (ICEE-B)*, Oct. 2017, pp. 1–6. doi: 10.1109/ICEE-B.2017.8192077.
- [9] E. H. Rachmawanto, K. Prasetyo, C. A. Sari, I. M. S. De Rosal, and N. Rijati, "Secured PVD Video Steganography Method based on AES and Linear Congruential Generator," in *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, Nov. 2018, pp. 163–167. doi: 10.1109/ISRITI.2018.8864466.
- [10] F. Mushtaq Sher Ali and F. Hassan Sarhan, "Enhancing Security of Vigenere Cipher by Stream Cipher," *Int J Comput Appl*, vol. 100, no. 1, pp. 975–8887, 2014.
- [11] N. Laila and A. S. Rms, "IMPLEMENTASI STEGANOGRAFI LSB DENGAN ENKRIPSI VIGENERE CIPHER PADA CITRA," *Computer Science Informatics Journal*, vol. 1, no. 2, 2018.
- [12] B. B. Ahamed and M. Krishnamoorthy, "SMS Encryption and Decryption Using Modified Vigenere Cipher Algorithm," *Journal of the Operations Research Society of China*, Aug. 2020, doi: 10.1007/s40305-020-00320-x.
- [13] E. Irfan Riaz Shohab Sandhu *et al.*, "An Enhanced Vigenere Cipher For Data Security," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, vol. 5, no. 03, 2016, [Online]. Available: [www.ijstr.org](http://www.ijstr.org)
- [14] L. Budi Handoko, "SEKURITI TEKS MENGGUNAKAN VIGENERE CIPHER DAN HILL CIPHER," *Bit (Fakultas Teknologi Informasi Universitas Budi Luhur)*, vol. 19, no. 1, pp. 37–47, 2022.
- [15] D. Gautam, C. Agrawal, P. Sharma, M. Mehta, and P. Saini, "An Enhanced Cipher Technique Using Vigenere and Modified Caesar Cipher," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*, May 2018, pp. 1–9. doi: 10.1109/ICOEI.2018.8553910.
- [16] E. Rahmawan Pramudya and L. Budi Handoko, "KRIPTOGRAFI VIGENERE UNTUK MENGAMANKAN PESAN TEKS BERBASIS OCR (OPTICAL CHARACTER RECOGNITION)," in *Proceeding SENDIU*, 2021, pp. 460–467.