PROC. INTERNAT. CONF. SCI. ENGIN. ISSN 2597-5250 | EISSN 2598-232X
Volume 1, October 2017 | Pages: 157-163

A Modifying of Hill Cipher Algorithm with 3 Substitution Caesar Cipher

Azzam Mujaddid*, Sumarsono**
Informatics Department, Faculty of Science and Technology, UIN Sunan Kalijaga Yogyakarta
Jl. Marsda Adisucipto No 1 Yogyakarta 55281, Indonesia. Tel. +62-274-540971, Fax. +62-274-519739.
Email: mujaddid29@gmail.com*, sumarsono@uin-suka.ac.id**

Abstract. *Mujaddid A, Sumarsono. 2017. A Modifying of Hill Cipher Algorithm with 3 Substitution Caesar Cipher. Proc Internat Conf Sci Engin 1: 157-163.* The hill cipher algorithm has the uniqueness of using matrix multiplication in the process where the key used is a matrix that has weaknesses in the process of encryption and decryption. In this paper will be modified to the encryption process with caesar cipher substitution. The principle of the hill cipher algorithm using the multiplication of the 2x2 key matrix of keys is enhanced through process modification lies in the combination of initial character determination using the substitution of 3 caesar ciphers. From the results of this modification can be seen that the more the number of characters processed the time required will be longer. The magnitude of the determinant also affects time and size during the poses. A 1 character increment occurs if the initial character of the encryption process is an odd number.

Keywords: Hill cipher, caesar cipher, chriptography

INTRODUCTION

Cryptography is one alternative to solving digital document security. Because in a cryptographic document will be changed to a certain character according to a given generator key, this process is called encryption. Only people who have a key can do the decryption process or translate the digital document. One of the many encryption algorithms in cryptography is the Hill cipher algorithm. The hill cipher algorithm uses a key generator with a matrix. The characters in the original document will be converted into a new character in accordance with the rules of matrix multiplication.

The hill cipher algorithm is one of the symmetric key algorithms, which uses the matrix as the key for encryption and decryption. The basic matrix theory used in Hill ciphers is inter-matrix multiplication and inverse in matrix. This method was invented by Lester S. Haw in 1929, the hill cipher algorithm is the application of modulo arithmetic to cryptography. This cryptographic technique uses a square matrix key as the key used to perform encryption and decryption. By implementing Hill Cipher algorithm in the document file will certainly keep the security of the document. One of the weaknesses of the Hill cipher algorithm is that when the matrix-shaped key is known, the cryptographic process is automatically determined using the hill cipher algorithm, since only this algorithm uses the matrix key. A modification in the process of encryption and decryption is required.

There needs to be an alternative in keeping a document file, one alternative is to implement cryptographic algorithms Hill cipher modified with caesar cipher algorithm so that the digital document data has strong security and maintain the confidentiality of the data. Alternative in implementing this algorithm can be done with the help of java programming, so it is not implemented manually, considering the data in keep the secrecy is digital. Then it will be tested the algorithm performance.

Literature Review

Research conducted by Edgar Dika Santosa discussed the hill cipher algorithm by performing a combination of initial character determination using substitution algorithm. The research undertaken focuses on database security of an information system through encryption. The conclusion of his research is that this algorithm can be well implemented in the database of invertory systems [14].

Research by Niken Puspita and Nurdin Bahtiar utilizes ASCII code and Matrix Operation as the main study in performing a short character encryption process with Hill cipher algorithm. Makes matrix multiplication the center of problem solving [8].

The research by Annelis uses hybrid cryptography techniques using a combination of Caesar Cipher and RSA algorithms for message encoding. The Caesar Cipher algorithm is a Symmetry Key algorithm used to encode messages and the RSA algorithm is an asymmetry key algorithm used to encode the caesar cipher symmetry key [1].

MATERIALS AND METHODS

Subjects in this study is a hill cipher cryptography algorithm that modified its performance on the document type *. txt. The algorithm uses symmetric key cryptography that is the same key in the process of encryption and decryption. While the method in the programming algorithm is cryptography hill cipher and caesar cipher algorithm.

RESULTS AND DISCUSSION

Hill Cipher Encryption Process

The Hill cipher encryption process begins with a palintext and will generate the ciphertext result of the key multiplication as in figure 1.

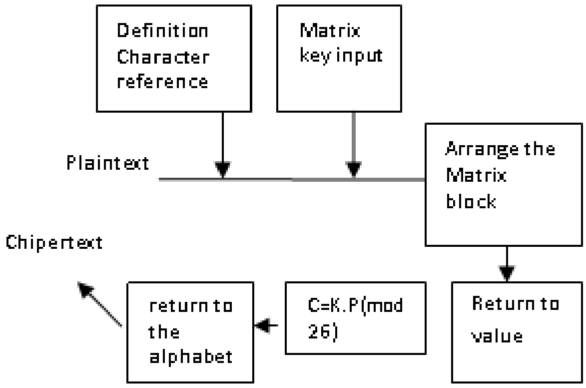

Figure 1. Workflow of Hill Cipher encryption process.

a. Define alphabetic characters to be converted into numbers according to hill cipher rules. This is what determines the encryption process.
b. Key Matrix Input is symbolized by K, the key matrix will be processed by plaintext. Conditions in performing key inputs are inverse matrices. The key used is the 2x2 order matrix.
c. Arrange Plaintext into matrix blocks to form matrices to be converted into numbers according to the definition of conversion reference.
d. Alphabetical characters will be converted into values or figures in order to perform matrix operations.
e. The formula of the multiplication between the plaintext and the key is C = K.P (Mod 26) where C is the Ciphertext, K is the Key, P is the Plaintext and mod 26 as the determinant of changing the return value from the numeric character to the alphabetic character to become a ciphertext.
f. After multiplication of the key with the plaintext, the multiplication will be converted into alphabetical form. So the plaintext is encrypted.

The mathematical calculation of the document encryption process is as follows:

1. Document with extension .txt contains data
2. The Matrix key provided for encryption is $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$

The definition of alphabetical change to numbers in the hill cipher rule is as in table 1.

Table 1. Conversion Alphabet to Number Hill cipher.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**
1	2	3	4	5	6	7	8	9	10
K	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**
11	12	13	14	15	16	17	18	19	20
U	**V**	**W**	**X**	**Y**	**Z**				
21	22	23	24	25	26				

3. Construct the block matrix form to multiplication.
4. Transform data from alphabetic characters into numeric characters according to the conversion table in the hill cipher algorithm so that the document data becomes a number character.
5. For example calculation in the document data there is the word "Ali Akbar" then the multiplication process is as follows.

Plaintext = Ali Akbar
Conversion into Value:

A → 1, L → 12 , I → 9, A → 1, K →11 , B→ 2, A→1, R→ 18.

Construct into matrix blocks

$$\begin{matrix} 1 & 9 & 11 & 1 \\ 12 & 1 & 2 & 18 \end{matrix}$$

Covers a key with a block matrix.

$$C = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} x \begin{matrix} 1 & 9 & 11 & 1 \\ 12 & 1 & 2 & 18 \end{matrix}$$

$$C = \begin{matrix} 14 & 19 & 24 & 20 \\ 13 & 10 & 13 & 19 \end{matrix}$$

Perform modulo 26 to transform the value from number to alphabet

$$C = \begin{matrix} 14 & 19 & 24 & 20 \\ 13 & 10 & 13 & 19 \end{matrix} \text{ mod } 26$$

Chipertext obtained is 14,13,19,10,24,13,20, 19 will be converted in the form of value to be

14 → N, 13 → M, 19→S, 10→ J, 24 → X, 13→ M, 20→T, 19→S

Chipertext generated from the encryption process with the hill cipher algorithm is NMS JXMTS.

6. The encryption process ends and generates a ciphertext.

Hill Cipher Decryption Process

The process that occurs in the decryption hill cipher has in common with the encryption process that performs multiplication counting operations on the matrix, which distinguishes the key forms used. The key used is the inverse of the initial key. If K is the key for encryption then K^{-1} is the key to decrypt. Here is the step of decryption process of hill cipher algorithm as in figure 2.

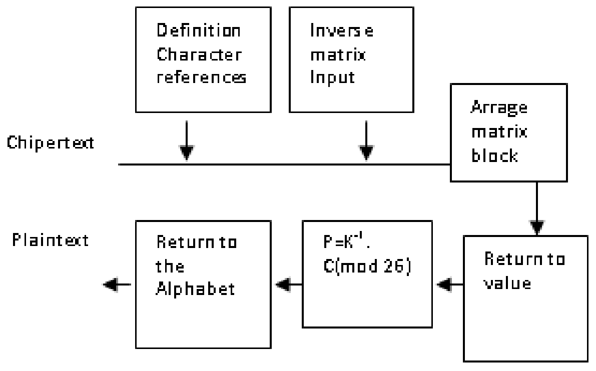

Figure 2. Workflow Hill Cipher decryption process.

a. Chipertext obtained from the encryption process using hill cipher algorithm will be done encryption process in accordance with the encryption key provided.
b. Defines the conversion of alphabetic characters into digits and inverse the matrix keys used.
c. Arrange characters into matrix blocks for later calculation operations on characters.
d. The characters will be converted according to the hill cipher rules as in table 1.
e. The formula of the multiplication between plaintext and key is P = K^{-1}.C (mod 26) where C is Ciphertext, K is Key, P is Plaintext and mod 26 as the determinant of changing the return value from numeric character to alphabetic character to become a plaintext.
f. After the multiplication of the key with the ciphertext, the multiplication will be converted again into alphabetical form. So the ciphertext is decrypted.

The mathematical calculations in the decryption process are as follows:

1. In the document contains data encryption on two words that generate NMS JXMTS ciphertext then will be done decryption process according to hill cipher algorithm rules with key encryption matrix $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$.
2. The key of the encryption matrix will be converted to an inverse from $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ to $\begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$ expressed as K^{-1}.
3. Ciphertext in alphabetical form will be converted to number N→14, M→13, S→ 19, J→10, X→24, M→13, T→20, S→19.
4. Arranged into block matrix in order to do matrix operation. So the ciphertext symbolized C becomes:

$$C = \begin{matrix} 14 & 19 & 24 & 20 \\ 13 & 10 & 13 & 19 \end{matrix}$$

5. Multiplying by the formula P = K^{-1}.C (mod 26)

$$C = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \; x \; \begin{matrix} 14 & 19 & 24 & 20 \\ 13 & 10 & 13 & 19 \end{matrix}$$

The results $C = \begin{matrix} 1 & 9 & 11 & 1 \\ 12 & 1 & 2 & 18 \end{matrix}$

Done modulo 26 will be

$$C = \begin{matrix} 1 & 9 & 11 & 1 \\ 12 & 1 & 2 & 18 \end{matrix} \text{ mod } 26$$

Plaintext obtained from NMS JXMTS ciphertext in the form of numbers 1,12,9,1,11,2,1,18 will be converted into alphabetical form 1→A ,12→L ,9→I ,1→A,11→K,2→B,1→A,18→R.

6. The decryption process is done by using hill cipher algorithm rules from NMS JXMTS ciphertext to plaintext ALI AKBAR.

Modified Encryption Process

The framework of the modification algorithm is similar to the workflow in accordance with the theory of the hill cipher algorithm, only modifications are made to the number of characters and substitution of the caesar cipher in its definition.

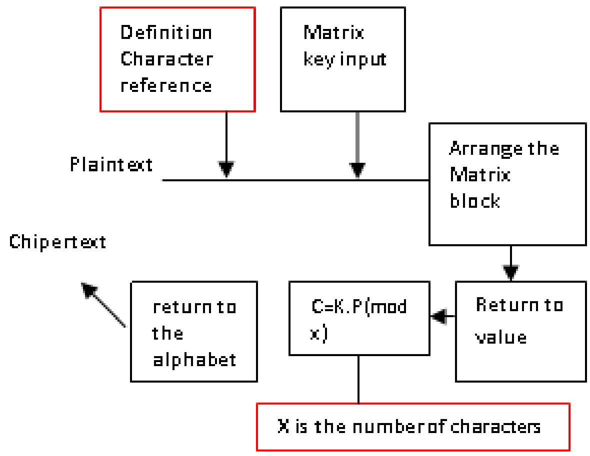

Figure 3. Workflow modified encryption process.

In this research substitution is done with the key that has been given in 3. So if the hill cipher algorithm without character modification begins with "a" then in algortima modification of this initial character terseut will be substituted with 3 characters afterwards. This affects the matrix multiplication formula in the encryption process, the number of modulo is said to be x, x is the number of characters defined at the beginning.

The following description of step hill cipher algorithm with modifications:

a. To define an acceptable alphabet character when encryption process, the character can be seen in table 2, the location of the modification is at this stage. The addition of characters and substitution of caesar cipher is done when defining alphabetic characters. Once given the substitution key 3 the conversion table changes can be seen in table 3

Table 2. Character to number modified.

Character	Number	Character	Number	Character	Number
a	0	s	18	K	36
b	1	t	19	L	37
c	2	u	20	M	38
d	3	v	21	N	39
e	4	w	22	O	40
f	5	x	23	P	41
g	6	y	24	Q	42
h	7	z	25	R	43
i	8	A	26	S	44
j	9	B	27	T	45
k	10	C	28	U	46
l	11	D	29	V	47
m	12	E	30	W	48
n	13	F	31	X	49
o	14	G	32	Y	50
p	15	H	33	Z	51
q	16	I	34	.	52
r	17	J	35	spasi	53
				,	54
				Enter	55

Table 3. Character to number modified with 3 substitution Caesar.

Character	Number	Character	Number	Character	Number
d	0	v	18	N	36
e	1	w	19	O	37
f	2	x	20	P	38
g	3	y	21	Q	39
h	4	z	22	R	40
i	5	A	23	S	41
j	6	B	24	T	42
k	7	C	25	U	43
l	8	D	26	V	44
m	9	E	27	W	45
n	10	F	28	X	46
o	11	G	29	Y	47
p	12	H	30	Z	48
q	13	I	31	.	49
r	14	J	32	spasi	50
s	15	K	33	,	51
t	16	L	34	enter	52
u	17	M	35	a	53
				b	54
				c	55

With the new character table allows the hill algorithm to process characters that are irregularly of typeface and large, with or without spaces and enter.

b. Key Matrix Input is symbolized by K, the key matrix will be processed by plaintext. The requirement in performing the key input is the inverse matrix. The key used is a 2x2 berry matrix.

c. Arrange Plaintext into matrix block to form matrix to be converted into numbers according to definition of conversion reference If the character is odd number then it will be added one character of pengfixap that is character of space which does not change meaning of word in plaintext.

d. Alphabetical characters will be converted into values or figures in order to perform matrix operations.

e. The formula of multiplication between plaintext and key is different from ordinary hill cipher key, because modification has been made then the formula applied for encryption process is C = KP (mod x), where C is Ciphertext, K is Key, P is Plaintext and x number of characters Which is used in the encryption process to determine the outcome of the encryption process. In this case x is 56.

f. After multiplication of the key with the plaintext, the multiplication will be converted into alphabetical form. So the plaintext is encrypted.

Examples of mathematical calculations are as follows:

a) Referring to the previous plaintext of “Ali Akbar” character

b) The Matrix key provided for encryption is $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$

The definition of alphabetical change to a number in the hill cipher rule that has been modified in accordance with table 3

c) The calculation process is as follows
Plaintext = Ali Akbar
Conversion into Value:

A → 23 , l → 8 ,i → 5 , spasi →50 , A → 23, k →7 , b→ 54 , a→53, r→ 14.

Construct into matrix blocks

$$\begin{matrix} 23 & 5 & 23 & 53 & 14 \\ 8 & 50 & 7 & 52 & \end{matrix}$$

The number of characters is odd. So that the last matrix element does not have a pair, the addition of karakarak spacing as a pengmentap so that the matrix block after the addition is as follows:

$$\begin{matrix} 23 & 5 & 23 & 54 & 14 \\ 8 & 50 & 7 & 53 & 50 \end{matrix}$$

Multiplying a key with a block matrix.

$$C = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \; x \; \begin{matrix} 23 & 5 & 23 & 53 & 14 \\ 8 & 49 & 7 & 52 & 49 \end{matrix}$$

$$C = \begin{matrix} 54 & 59 & 53 & 158 & 77 \\ 31 & 54 & 30 & 103 & 63 \end{matrix}$$

Perform modulo 56 to transform the value from number to alphabet

$$C = \begin{matrix} 54 & 4 & 53 & 49 & 22 \\ 31 & 55 & 30 & 51 & 8 \end{matrix} \text{ mod } 56$$

Chipertext obtained is 54,31,4,55,53,30,49, 51, 22,8 will be converted in the form of value to be 54→ b ,31→ I, 4→h, 55→c,53→a, 30→H,49→ titik ,51→koma ,22→z,8 →l
Chipertext generated from the encryption process with the hill cipher algorithm is bIhcaH., Zl

d) The encryption process ends and generates a ciphertext.

Modified Decryption Process

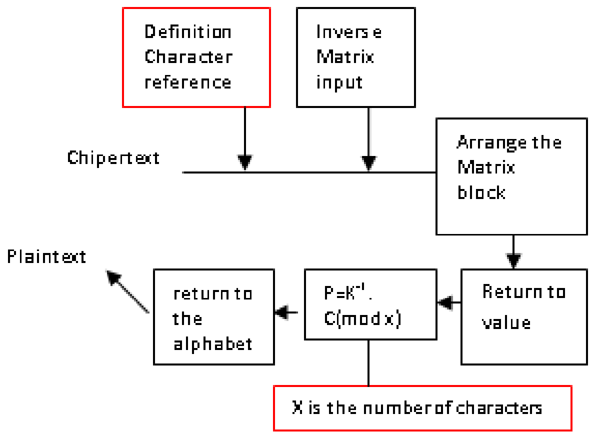

Figure 4. Workflow modified decryption process.

In the decryption framework uses a hill cipher algorithm with modifications, using a reversal of the modified hier algortima encryption process.

a) Character definitions with modification of caesar substitution follow in table 3 which is the key to the decryption process.
b) The given key matrix is the same as the modified encryption process key matrix, but in the process used is the inverse of the key matrix.
c) Construct cipertext characters into matrix blocks to perform calculation operations with key matrices.
d) Alphabetical characters that have been compiled into block shapes are converted into numeric characters according to the table of character definitions in table 3.
e) The mathematical formula used in the decryption process is P = K^{-1}.C (mod x) where P is Plaintext, K^{-1} is the inverse of K (key matrix), C is Ciphertext and x is the number of characters used in the decryption process. In this case x is 56.

Transforming the value of the form of the letters according to the module results from table 3
Examples of mathematical calculations are as follows:

a) Referring to the previous plaintext of the character bIhcaH., Zl
b) The key of the encryption matrix will be converted to an inverse from $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ to $\begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$ expressed as K^{-1}. The definition of alphabetical change to a number in the hill cipher rule that has been modified in accordance with table 3
c) The calculation process is as follows
Ciphertext = bIhcaH., Zl
Conversion into Value:

54→ b ,31→ I,4→h,55→c,53→a,30→H,49→ titik ,51→koma ,22→z,8 →l

Construct into matrix blocks

$$\begin{matrix} 54 & 4 & 53 & 49 & 22 \\ 31 & 55 & 30 & 51 & 8 \end{matrix}$$

Multiplying a key with a block matrix.

$$C = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} x \begin{matrix} 54 & 4 & 53 & 49 & 22 \\ 31 & 55 & 30 & 51 & 8 \end{matrix}$$

$$C = \begin{matrix} 23 & -51 & 23 & -2 & 14 \\ 8 & 106 & 7 & 53 & -6 \end{matrix}$$

Perform modulo 56 (total characters defined) to transform the value from number to alphabet

$$C = \begin{matrix} 23 & 5 & 23 & 54 & 14 \\ 8 & 50 & 7 & 53 & 50 \end{matrix} \text{ mod } 56$$

Chipertext obtained is 23.8,5,50,23,7,54, 53,14,50 will be converted in the form of a value to be A → 23 , l → 8 ,i → 5 , spasi →50 , A → 23, k →7 , b→ 54 , a→53, r→ 14.
Chipertext generated from the encryption process with the hill cipher algorithm is Ali Akbar

d) The decryption process ends and produces a plaintext.

Program Implementation

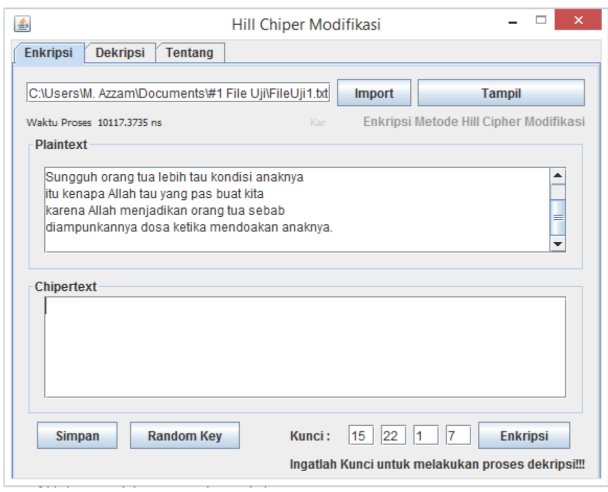

Figure 5. The view of encryption.

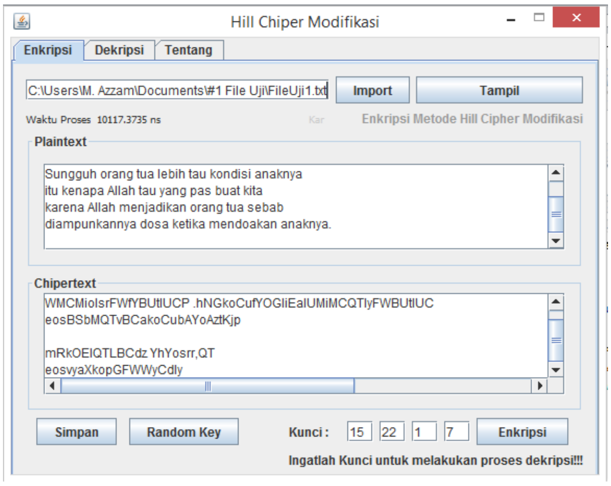

Figure 6. The view of decryption.

Figure 5 and 6 describe the appearance of programs created using java's desktop programming.

Testing

Table 4. The Results of encryption process.

No	Filename	Number of Character		Size (Bytes)		Time (ns)
		After	Before	After	Before	
1	FileUji1.txt	248	248	255	248	802.69
2	FileUji2.txt	1646	1646	1844	1646	35192.14
3	FileUji3.txt	2469	2470	2767	2470	67146.82
4	FileUji4.txt	3292	3292	3690	3292	109321.30
5	FileUji5.txt	4115	4116	4613	4116	119362.30
6	FileUji6.txt	4938	4938	5536	4938	163526.68
7	FileUji7.txt	5761	5762	6459	5762	183164.67
8	FileUji8.txt	6584	6584	7382	6584	221024.78
9	FileUji9.txt	7407	7408	8305	7408	230355.39
10	FileUji10.txt	8230	8230	9228	8230	243616.66

From the results of experiments conducted on the encryption process using 10 training data with different sizes can be drawn the first conclusion that the number of characters after and before the encryption is fixed, but there are exceptions for the characters that amount to odd. Odd characters will increment 1 character as a complement character in the encryption process. Can be seen in figure 5. The second file size before the encryption process is done with the file size after encryption has a size reduction in all tested train data, the size of the file in bytes follows the number of characters present in the file. Comparison of file size can be seen in figure 6. The third conclusion is the larger the file size then the time required in the encryption process the longer. This can be noted in Figure 6.

In the second experiment, 10 training data files will be encrypted and decrypted using different matrix. The matrix used is the following matrix $\begin{bmatrix}1 & 0\\12 & 1\end{bmatrix}$, $\begin{bmatrix}17 & 6\\1 & 5\end{bmatrix}$, $\begin{bmatrix}12 & 1\\25 & 13\end{bmatrix}$. The matrix used is randomly selected but still observes the key rules on the hill cipher that is the invertible matrix that has the inverse. These three matrices have different determinants, 1, 79, and 131. In the second experiment it is concerned that there is a greater influence of the determinant of the matrix used against the required process time.

After the second experiment, the time required data to determine the key determinants used.

Table 5. Second timing encryption process differences.

No	Filename	Encryption Process Time (ns)		
		Derterminant 1	Determinant 79	Determinant 131
1	FileUji1.txt	775.71	795.97	796.07
2	FileUji2.txt	29667.04	30194.91	30585.33
3	FileUji3.txt	47755.23	50721.94	51343.01
4	FileUji4.txt	68298.29	71392.84	94922.97
5	FileUji5.txt	99717.99	100137.34	107208.85
6	FileUji6.txt	131726.94	135442.55	137495.26
7	FileUji7.txt	145194.41	169568.68	174727.57
8	FileUji8.txt	172330.74	175502.18	177135.17
9	FileUji9.txt	178287.12	197186.56	215171.06
10	FileUji10.txt	244183.39	254202.94	256330.52

CONCLUSIONS

After review and implementation of hill cipher algorithm with process modification on encryption and decryption of plaintext document can be drawn the following conclusion:

1. This research succeeded in conducting study and applying hill cipher algorithm with modification for encryption and descriptive process using substitution of caesar cipher algortima in plaintext document using 2x2 berry key matrix.
2. This research successfully apply the process of encryption and decryption using hill cipher modification algorithm using java programming.
3. The encryption process affects the file size, after the file size encryption process is reduced, to be in accordance with the number of characters, if in the file has an odd character of eating will increase one character as a fulfillment. The larger the file size the time it takes takes longer.
4. The size of the file before the encryption process and after the decryption process meliliki difference, but the file contents have the same number of characters in the case of even character
5. The determinant of the key matrix affects the processing time of the encryption process and the decryption process.

REFERENCES

Annelis, S. 2010. *Pengkodean Pesan Menggunakan Perpaduan nCaesar Cipher dan RSA Pada Kriptografi Hibrida*. Skripsi. Universitas Andalas.

Febriansyah, 2015 ”*Analisis dan perancangan keamanan data menggunakan Algoritma Kriptografi DES (Data Encryption Standard)* Universitas Bina Darma

Forouzan, Behrouz.2010 *Cryptogrphy and Netwprk Security*. MCGraw-*Hill*, Newyork.

Lusiana, Veronica 2015*“Implementasi Kriptografi pada file Dokumen menggunakan Algoritma AES-128*”

Munir, Rinaldi 2006. Diktat kuliah IF5054 Kriptografi. Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, ITB

Mishra, Anupama.2013. *Enhancing Security of Caesar Cipher using different Method*.IJRET. Vol 2. P 332.

Prayudi, Yudi, Idham Halik. 2005. *Studi Analisis Algoritma Rivest Code 6 (RC6) Dalam Enkripsi/Dekripsi Data*. Seminar Nasional Aplikasi Teknologi Informasi 2005 (SNATI 2005), Yogyakarta.

Puspita, Niken Prima dan Nurdin Bahtiar 2014 “*Kriptografi Hill cipher dengan menggunakan operasi Matriks*” Matematika. UNDIP Semarang

Sadikin, Rifki. 2012. *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*. Penerbit Andi, Yogyakarta

Sansasni, S. 2008. *Penggunaan Aritmatika Modulo dan Balikan Modulo pada modifikasi Algoritma Knapsack. Makalah* Bandung. Teknik Informatika ITB Bandung

Security, Komputer. 2009. *Teknik Keamanan Komputer, Enkripsi & Dekripsi*. http://security- komputer. blogspot.com/ 2009/12/ teknik-kemanan komputerenkripsi.html. Diakses 20 Maret 2017 11.50

Wirdasari, Dian. 2008. *Prinsip Kerja Kriptografi dalam Mengamankan Informasi*, Jurnal SAINTIKOM Vol.5 No.2.

Yuliandaru, Adam Rotal 2015 “*Teknik Kriptogradi Hill cipher menggunakan Matriks*” STEI ITB Bandung.

Edgar Dika Santosa, 2015,” *Implementasi Algoritma Caesar Cipher dan Hill Cipher Pada Database Sistem Inventori Tb Mita Jepara*”, http://eprints.dinus.ac.id/ 15251/1/ jurnal_15246.pdf

THIS PAGE INTENTIONALLY LEFT BLANK