Kumpulan jurnaL Ilmu Komputer (KLIK)
Volume 10 No. 01 2023
ISSN: 2406-7857

HILL-CIPHER METHOD WITH MATRICE IN TEXT CODING PROCESSING

Desi Vinsensia[1*], Kiky Maulana[2,] Dedy Nofrianto[3]
[1]Program Studi Manajemen Informatika, STMIK Pelita Nusantara Medan
[2,3] Program Studi Teknik Informatika, STMIK Pelita Nusantara Medan
[*]desivinsensia87@gmail.com

Abstract

Cryptography is one of the matrice applications that can be used to translate a message. This research discusses cryptography, which is the science or art of encryption with the aim of making messages incomprehensible to others. The cryptography method that will be used in this research is the Hill Cipher, ,which is one of the cryptographic techniques for encrypting a text by translating a message into a code over a matrice of numbers modulo 26 and converting the codes into the actual message using the decipher method over a matrice of numbers modulo 26. The purpose of this research is to develop the Hill Cipher in word encoding and decipher through the $n \times n$ matrices. The test result found that the hill cipher method and the decipher method are able to translate the actual text as long as the matrices given in the hill cipher algorithm have an inverse and determinant.

Keywords*: Hill-Cipher, criptograhy, matrices, plaintext*

Abstrak

Kriptografi merupakan salah satu aplikasi matriks yang dapat digunakan untuk menerjemahkan sebuah pesan. Penelitian ini membahas tentang kriptografi yang merupakan ilmu atau seni dari penyandian dengan tujuan agar pesan tidak dimengerti oleh orang lain. Metode kriptografi yang akan digunakan dalam penelitian ini adalah metode Hill Cipher dan metode Decipher yang merupakan kriptografi merupakan salah satu teknik kriptografi untuk mengenkripsi teks dengan menerjemahkan pesan ke dalam kode melalui matriks angka modulo 26 dan mengubah kode menjadi pesan yang sebenarnya dengan menggunakan metode penguraian melalui matriks angka modulo 26. Penelitian ini berfokus pada pengembangan algoritma Hill Cipher dalam penyandian kata dan Dechiper melalui matriks berodo $n \times n$. Hasil pengujian didapatkan bahwa metode Hill Cipher dan metode decipher mampu menterjemahkan teks yang sebenarnya selama matriks-matriks yang diberikan pada algoritma Hill Cipher memiliki invers dan determinan.

Kata kunci*: Hill-Cipher, Kriptografi, Matriks, plaintext*

1. INTRODUCTION

Todays, every needs of life is integrated with internet technology and network and needed to security for data. Security is required to protect information from various attacks that may spread confidential information [1]. Cryptography is one of the matrice applications that can be used to translate a message. Cryptography is derived from the Greek words cryptos (secret) and graphein (writing). So cryptography is defined as secret writing. Numerous definitions of cryptography have been proposed in the literature, including: cryptography is the science and art of sending and receiving secret messages or protecting stored data so that others unable understand [2]. A matrice is a rectangular array of numbers that contains unique entries. Matrice addition and subtraction, matrice multiplication, and scalar multiplication with matrices are all operations. Row operations, also known as elementary row operations, can be performed on matrices. Many definitions of cryptography have been proposed in the literature, including: cryptography is the science and art of sending and receiving secret messages or protecting stored data from being understood by others [3]

Goal of cryptography is to convert a plaintext message into an encrypted message (ciphertext) that is incomprehensible to those who do not have access to the message. This method has been studied by researchers, including: [4] proposed a secure variant of the Hill cipher method, which, due to its linear nature, is vulnerable to known plaintext attacks. The nonsingular matrices are also transformed into an invertible orthogonal matrices to serve as key matrices then generate the key matrice, the magic rectangle of order $m \times n$ is first converted into the magic square of order $n \times n$ [5].

Based on the rules, it generates the necessary key matrice. According to [6] proposed a Hill cipher method based on inverse matrices as keys, concluding that the Hill cipher method based on rectilinear matrices is more secure than the original Hill cipher method. While [7] investigated the performance of the Block Cipher algorithm, a popular key matrices cryptography algorithm. According to [8] the performance of cryptographic algorithms is analyzed to increase the security of the value so that cryptanalysts cannot steal it. The results showed that value transmission is more secure with hybrid cryptography using the Hill key and the RSA algorithm than with cryptography using the Hill cipher key. In addition, most imaging techniques also use symmetric and asymmetric cryptographic algorithms to encrypt digital media [9],[10]. While [11] uses an orthogonal matrix (where the transpose of a matrix is equal to its inverse) as the key matrix. The method is faster and easier because finding the transpose of a matrix is simpler than finding the inverse of the given matrix. Therefore, it facilitates the execution process more. [12] introduced a simplified method of encryption of data in blocks using logical XOR and shift operations, as well as Radix64 for data encoding and decoding. In addition, the Hill cipher method an easy approach to modify consists of three phases, key matrix generation encryption, and decryption using modulo 256.

According to [13] recommends discussing the fundamental matrices theory of multiplication between matrices and inverse matrices and applying the Hill Cipher method to text media because it has fast encryption and decryption speeds. This provides good method for safeguard data to transmitted open networks and

imitating encryption and decryption to 26 letters reduces security. Then also [14] discusses the basic theory of Hill cipher and the concept of multiplying a matrices and then performing the matrices inversion on plaintext. Furthermore, research by [15] uses the Hill cipher algorithm to encrypt and decrypt all types of messages, not only letters but converts Radix 64 by eliminating redundant data that occurs in plain text patterns.In this paper investigates the use of matrices in message translation then translated into other letters using matrices and operations on non-singular matrices on the set modulo integers. In addition this paper provide the process of converting matrices approximated by the Hill Cipher and Decipher methods into actual messages works . Furthermore, the paper illustrates the results of a practical algorithm (steps) for translating messages through matrices into understandable messages.

2. RESEARCH METHODOLOGY

Cryptography is the study of coding and decoding secret messages [16]. Cryptography technique there is a method called Hill Cipher created by Lester S. Hill in 1929 which aims to create an unbreakable cipher using frequency analysis techniques [17]. Hill Cipher method also used to combines $3\times3\times3$ Rubik's cube methods with Python software simulation to create a hybrid cryptographic algorithm as done by [18]. The Hill cipher fixed each of the same alphabets in the plaintext with the same alphabet in the ciphertext [19], because it uses matrix multiplication on the basis of the encryption and decryption process. This paper contains study case that depicts two stages of the process: the Hill cipher process and the decipher process. These methods make use of n-dimensional matrices that are determined later with uses coding on letters by using properties on the set of integers modulo 26 as shown on table 1 (because the number of letters is 26) and add punctuation such as ".", ",", "", "',", "?", "!", and "/", then use properties on the set of integers modulo 33 (depending on how many punctuation marks are added).

Table 1. The Alphabet Conversion

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

R	S	T	U	V	W	X	Y	Z	.	,	“	‘	?	!	/
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	0

The Hill's Cipher algorithm for encrypted codes against integers modulo m as follows:

a. Select an singular with integer entries $n\times n$ matrices $A=\lfloor a_{ij} \rfloor, i=1,2,\ldots,n$ and $j=1,2,\ldots,n$ to carry out the encoding.
b. Assume that each group consists of n plaintext letters such as $p_1, p_2, \ldots, p_n$. If there are an odd number of letters in the plaintext, add a dummy letter to

complete the last pair of letters, and replace each plaintext letter with its numeric counterpart.

c. Sequentially, convert each plaintext pairs of $p_1,\ldots,p_n$ to be a vector column $p=\begin{bmatrix} p_1 \\ \vdots \\ p_n \end{bmatrix}$

d. Create the corresponding ciphertext vector by multiplying A_p using the modulo m multiplication principle.

e. To create a ciphertext, transform each vector into its letters of the alphabet equivalent.

The following is the coding algorithm using the Dechiper method for integers modulo m, as follows:

a. Select an singular with integer entries $n \times n$ matrices $A=\lfloor a_{ij} \rfloor, i=1,2,\ldots,n$; $j=1,2,\ldots,n$ and determine the invers.

b. Assume that each group consists of n plaintext letters such as $c_1,c_2,\ldots,c_n$. If there are an odd number of letters in the ciphertext, add a dummy letter to complete the last pair of letters, and replace each ciphertext letter with its numeric.

c. Sequentially, convert each ciphertext pairs of $c_1,c_2,\ldots,c_n$ to be a vector column $b=\begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$

d. Create the corresponding plaintext vector by multiplying $A^{-1}c$ using the modulo m multiplication principle.

e. Convert each vector into its alphabetical equivalent to form plaintext.

3. **RESULT AND DISCUSSION**

Given text "KRIPTOGRAPHY TO SECURING TEXT MESSAGES" this message will be encrypted with the Hill cipher algorithm using the principle of multiplication modulo 26 with a 3×3 singular matrices as follows:

a. Given the matrices $C=\begin{bmatrix} 1 & 1 & 3 \\ 0 & 2 & 1 \\ 2 & 3 & 1 \end{bmatrix}$

b. Suppose every three consecutive plaintext letters are: KRI PTO GRA FIT OSE TEXT TME SSA GES. Since each plaintext has a pair, there is no need to add a dummy letter. Then replace each plaintext letter on the table 1 with its numeric letter .

c. The plaintext vectors for that sentence as sequentially are

$$\begin{bmatrix}11\\18\\9\end{bmatrix},\begin{bmatrix}16\\20\\15\end{bmatrix},\begin{bmatrix}7\\18\\1\end{bmatrix},\begin{bmatrix}6\\9\\20\end{bmatrix},\begin{bmatrix}15\\19\\5\end{bmatrix},\begin{bmatrix}3\\21\\18\end{bmatrix}\begin{bmatrix}9\\14\\7\end{bmatrix},\begin{bmatrix}20\\5\\24\end{bmatrix},\begin{bmatrix}20\\13\\5\end{bmatrix},\begin{bmatrix}19\\19\\1\end{bmatrix},\begin{bmatrix}7\\5\\19\end{bmatrix}$$

Table2. Process of Transform Plaintext Vector with Matrices C

Plaintext	Plaintext vector	Plaintext Vector (C_p), $C=\begin{bmatrix}1&1&3\\0&2&1\\2&3&1\end{bmatrix}$	Ciphertext
KRI	$\begin{bmatrix}11\\18\\9\end{bmatrix}$	$\begin{bmatrix}1&1&3\\0&2&1\\2&3&1\end{bmatrix}\begin{bmatrix}11\\18\\9\end{bmatrix}=\begin{bmatrix}56\\45\\85\end{bmatrix}=\begin{bmatrix}4\\19\\7\end{bmatrix}$	D S G
PTO	$\begin{bmatrix}16\\20\\15\end{bmatrix}$	$\begin{bmatrix}1&1&3\\0&2&1\\2&3&1\end{bmatrix}\begin{bmatrix}16\\20\\15\end{bmatrix}=\begin{bmatrix}51\\55\\107\end{bmatrix}=\begin{bmatrix}25\\3\\3\end{bmatrix}$	Y C C
GRA	$\begin{bmatrix}7\\18\\1\end{bmatrix},$	$\begin{bmatrix}1&1&3\\0&2&1\\2&3&1\end{bmatrix}\begin{bmatrix}7\\18\\1\end{bmatrix}=\begin{bmatrix}28\\37\\69\end{bmatrix}=\begin{bmatrix}2\\11\\17\end{bmatrix}$	B K P
FIT	$\begin{bmatrix}6\\9\\20\end{bmatrix}$	$\begin{bmatrix}1&1&3\\0&2&1\\2&3&1\end{bmatrix}\begin{bmatrix}6\\9\\20\end{bmatrix}=\begin{bmatrix}75\\38\\59\end{bmatrix}=\begin{bmatrix}23\\12\\7\end{bmatrix}$	W L G
OSE	$\begin{bmatrix}15\\19\\5\end{bmatrix}$	$\begin{bmatrix}1&1&3\\0&2&1\\2&3&1\end{bmatrix}\begin{bmatrix}15\\19\\5\end{bmatrix}=\begin{bmatrix}49\\43\\92\end{bmatrix}=\begin{bmatrix}23\\17\\14\end{bmatrix}$	W Q N
CUR	$\begin{bmatrix}3\\21\\18\end{bmatrix}$	$\begin{bmatrix}1&1&3\\0&2&1\\2&3&1\end{bmatrix}\begin{bmatrix}3\\21\\18\end{bmatrix}=\begin{bmatrix}78\\60\\87\end{bmatrix}=\begin{bmatrix}3\\8\\9\end{bmatrix}$	C H I
ING	$\begin{bmatrix}9\\14\\7\end{bmatrix}$	$\begin{bmatrix}1&1&3\\0&2&1\\2&3&1\end{bmatrix}\begin{bmatrix}9\\14\\7\end{bmatrix}=\begin{bmatrix}44\\35\\67\end{bmatrix}=\begin{bmatrix}18\\9\\15\end{bmatrix}$	R I O
TEX	$\begin{bmatrix}20\\5\\24\end{bmatrix}$	$\begin{bmatrix}1&1&3\\0&2&1\\2&3&1\end{bmatrix}\begin{bmatrix}20\\5\\24\end{bmatrix}=\begin{bmatrix}97\\34\\79\end{bmatrix}=\begin{bmatrix}19\\8\\1\end{bmatrix}$	S H A

Plaintext	Plaintext vector	Plaintext Vector (C_p), $C=\begin{bmatrix}1&1&3\\0&2&1\\2&3&1\end{bmatrix}$	Ciphertext
TME	$\begin{bmatrix}20\\13\\5\end{bmatrix}$	$\begin{bmatrix}1&1&3\\0&2&1\\2&3&1\end{bmatrix}\begin{bmatrix}20\\13\\5\end{bmatrix}=\begin{bmatrix}41\\31\\84\end{bmatrix}=\begin{bmatrix}15\\5\\6\end{bmatrix}$	O E F
SSA	$\begin{bmatrix}19\\19\\1\end{bmatrix}$	$\begin{bmatrix}1&1&3\\0&2&1\\2&3&1\end{bmatrix}\begin{bmatrix}19\\19\\1\end{bmatrix}=\begin{bmatrix}41\\39\\96\end{bmatrix}=\begin{bmatrix}15\\13\\18\end{bmatrix}$	O M R
GES	$\begin{bmatrix}7\\5\\19\end{bmatrix}$	$\begin{bmatrix}1&1&3\\0&2&1\\2&3&1\end{bmatrix}\begin{bmatrix}7\\5\\19\end{bmatrix}=\begin{bmatrix}69\\29\\48\end{bmatrix}=\begin{bmatrix}17\\3\\22\end{bmatrix}$	Q C V

The chipertext message for "KRIPTOGRAFI TO SECURING TEXT MESSAGES" is as follows, based on the processing results of the fourth and fifth steps of the calculation shown on table 2:

DSG YCC BKP WLG WQN CHI RIO SHA OEF OMR QCV

In order to convert chipertext to plaintext, the ciphertext of the previous hill cipher process was taken as follows:

1. Given $C=\begin{bmatrix}1&1&3\\0&2&1\\2&3&1\end{bmatrix}$. By solve elementary row operations for matrices as follows:

$$\left[C|I\right]\rightarrow ElementaryRowOperation\rightarrow\left[I\middle|C^{-1}\right] \quad (1)$$

$$\left(\begin{array}{ccc|ccc}1&1&3&1&0&0\\0&2&1&0&1&0\\2&3&1&0&0&1\end{array}\right) b_3-2b_1=\left(\begin{array}{ccc|ccc}1&1&3&1&0&0\\0&2&1&0&1&0\\0&1&-5&-2&0&1\end{array}\right)$$

$$\left(\begin{array}{ccc|ccc}1&1&3&1&0&0\\0&2&1&0&1&0\\0&1&-5&-2&0&1\end{array}\right) b_2-b_3=\left(\begin{array}{ccc|ccc}1&1&3&1&0&0\\0&1&6&2&1&-1\\0&1&-5&-2&0&1\end{array}\right)$$

$$\left(\begin{array}{ccc|ccc}1&1&3&1&0&0\\0&1&6&2&1&-1\\0&1&-5&-2&0&1\end{array}\right) b_3-b_2=\left(\begin{array}{ccc|ccc}1&1&3&1&0&0\\0&1&6&2&1&-1\\0&0&-11&-4&-1&2\end{array}\right)$$

$$\left(\begin{array}{ccc|ccc}1&1&3&1&0&0\\0&1&6&2&1&-1\\0&0&-11&-4&-1&2\end{array}\right) b_1-b_2=\left(\begin{array}{ccc|ccc}1&0&-3&-1&-1&1\\0&1&6&2&1&-1\\0&0&-11&-4&-1&2\end{array}\right)$$

$$\left(\begin{array}{ccc|ccc}1&0&-3&-1&-1&1\\0&1&6&2&1&-1\\0&0&-11&-4&-1&2\end{array}\right)\left(-\frac{1}{11}\right)b_3=\left(\begin{array}{ccc|ccc}1&0&-3&-1&-1&1\\0&1&6&2&1&-1\\0&0&1&\frac{4}{11}&\frac{1}{11}&-\frac{2}{11}\end{array}\right)$$

$$\left(\begin{array}{ccc|ccc}1&0&-3&-1&-1&1\\0&1&6&2&1&-1\\0&0&1&\frac{4}{11}&\frac{1}{11}&-\frac{2}{11}\end{array}\right) b_1+3b_3=\left(\begin{array}{ccc|ccc}1&0&0&\frac{1}{11}&-\frac{8}{11}&\frac{5}{11}\\0&1&6&2&1&-1\\0&0&1&\frac{4}{11}&\frac{1}{11}&-\frac{2}{11}\end{array}\right)$$

$$\left(\begin{array}{ccc|ccc}1&0&0&\frac{1}{11}&-\frac{8}{11}&\frac{5}{11}\\0&1&6&2&1&-1\\0&0&1&\frac{4}{11}&\frac{1}{11}&-\frac{2}{11}\end{array}\right) b_2-6b_3=\left(\begin{array}{ccc|ccc}1&0&0&\frac{1}{11}&-\frac{8}{11}&\frac{5}{11}\\0&1&0&-\frac{2}{11}&\frac{5}{11}&\frac{1}{11}\\0&0&1&\frac{4}{11}&\frac{1}{11}&-\frac{2}{11}\end{array}\right)$$

$$C^{-1}=\begin{bmatrix}\frac{1}{11}&\frac{-8}{11}&\frac{5}{11}\\\frac{-2}{11}&\frac{5}{11}&\frac{1}{11}\\\frac{4}{11}&\frac{1}{11}&\frac{-2}{11}\end{bmatrix}$$

The inverse of matrices C solved by using elementary row operations such as (1). Table 3 shows steps 2 to step 4 for the process of transforming the ciphertext vector from the inverse multiplication of the matrices. The ciphertext was converted to a vector column according to modulo 26. The vector in the plaintext is obtained

using the matrices multiplication principle. Furthermore, the result of vector plaintext transformed to plaintext lettering according on table 1 obtained:

KRI PTO GRA FIT OSE CUR ING TEX TME SSA GES

Table 3. Process of Transform Ciphertext vector with matrices C^{-1}

Cip-her text	Ciphertext vector's	Plaintext vector's	Plaintext
DSG	$\begin{bmatrix} 4 \\ 19 \\ 7 \end{bmatrix}$	$\begin{bmatrix} \frac{1}{11} & -\frac{8}{11} & \frac{5}{11} \\ -\frac{2}{11} & \frac{5}{11} & \frac{1}{11} \\ \frac{4}{11} & \frac{1}{11} & -\frac{2}{11} \end{bmatrix} \begin{bmatrix} 4 \\ 19 \\ 7 \end{bmatrix} = \begin{bmatrix} 11 \\ 18 \\ 9 \end{bmatrix}$	K R I
YCC	$\begin{bmatrix} 25 \\ 3 \\ 3 \end{bmatrix}$	$\begin{bmatrix} \frac{1}{11} & -\frac{8}{11} & \frac{5}{11} \\ -\frac{2}{11} & \frac{5}{11} & \frac{1}{11} \\ \frac{4}{11} & \frac{1}{11} & -\frac{2}{11} \end{bmatrix} \begin{bmatrix} 25 \\ 3 \\ 3 \end{bmatrix} = \begin{bmatrix} 16 \\ 20 \\ 15 \end{bmatrix}$	P T O
BKP	$\begin{bmatrix} 2 \\ 11 \\ 16 \end{bmatrix}$	$\begin{bmatrix} \frac{1}{11} & -\frac{8}{11} & \frac{5}{11} \\ -\frac{2}{11} & \frac{5}{11} & \frac{1}{11} \\ \frac{4}{11} & \frac{1}{11} & -\frac{2}{11} \end{bmatrix} \begin{bmatrix} 2 \\ 11 \\ 16 \end{bmatrix} = \begin{bmatrix} 7 \\ 18 \\ 1 \end{bmatrix}$	G R A
WLG	$\begin{bmatrix} 23 \\ 12 \\ 7 \end{bmatrix}$	$\begin{bmatrix} \frac{1}{11} & -\frac{8}{11} & \frac{5}{11} \\ -\frac{2}{11} & \frac{5}{11} & \frac{1}{11} \\ \frac{4}{11} & \frac{1}{11} & -\frac{2}{11} \end{bmatrix} \begin{bmatrix} 23 \\ 12 \\ 7 \end{bmatrix} = \begin{bmatrix} 6 \\ 9 \\ 20 \end{bmatrix}$	F I T

Cip-her text	Ciphertext vector's	Plaintext vector's	Plaintext
WQN	$\begin{bmatrix}23\\17\\14\end{bmatrix}$	$\begin{bmatrix}\frac{1}{11} & -\frac{8}{11} & \frac{5}{11}\\ -\frac{2}{11} & \frac{5}{11} & \frac{1}{11}\\ \frac{4}{11} & \frac{1}{11} & -\frac{2}{11}\end{bmatrix}\begin{bmatrix}23\\17\\14\end{bmatrix}=\begin{bmatrix}15\\19\\5\end{bmatrix}$	O S E
CHI	$\begin{bmatrix}3\\8\\9\end{bmatrix}$	$\begin{bmatrix}\frac{1}{11} & -\frac{8}{11} & \frac{5}{11}\\ -\frac{2}{11} & \frac{5}{11} & \frac{1}{11}\\ \frac{4}{11} & \frac{1}{11} & -\frac{2}{11}\end{bmatrix}\begin{bmatrix}3\\8\\9\end{bmatrix}=\begin{bmatrix}3\\21\\18\end{bmatrix}$	C U R
RIO	$\begin{bmatrix}18\\9\\15\end{bmatrix}$	$\begin{bmatrix}\frac{1}{11} & -\frac{8}{11} & \frac{5}{11}\\ -\frac{2}{11} & \frac{5}{11} & \frac{1}{11}\\ \frac{4}{11} & \frac{1}{11} & -\frac{2}{11}\end{bmatrix}\begin{bmatrix}18\\9\\15\end{bmatrix}=\begin{bmatrix}9\\14\\7\end{bmatrix}$	I N G
SHA	$\begin{bmatrix}19\\8\\1\end{bmatrix}$	$\begin{bmatrix}\frac{1}{11} & -\frac{8}{11} & \frac{5}{11}\\ -\frac{2}{11} & \frac{5}{11} & \frac{1}{11}\\ \frac{4}{11} & \frac{1}{11} & -\frac{2}{11}\end{bmatrix}\begin{bmatrix}19\\8\\1\end{bmatrix}=\begin{bmatrix}20\\5\\24\end{bmatrix}$	T E X
OEF	$\begin{bmatrix}15\\5\\6\end{bmatrix}$	$\begin{bmatrix}\frac{1}{11} & -\frac{8}{11} & \frac{5}{11}\\ -\frac{2}{11} & \frac{5}{11} & \frac{1}{11}\\ \frac{4}{11} & \frac{1}{11} & -\frac{2}{11}\end{bmatrix}\begin{bmatrix}15\\5\\6\end{bmatrix}=\begin{bmatrix}20\\13\\5\end{bmatrix}$	T M E

Cip-her text	Ciphertext vector's	Plaintext vector's	Plaintext
OMR	$\begin{bmatrix}15\\13\\18\end{bmatrix}$	$\begin{bmatrix}\frac{1}{11} & -\frac{8}{11} & \frac{5}{11}\\ -\frac{2}{11} & \frac{5}{11} & \frac{1}{11}\\ \frac{4}{11} & \frac{1}{11} & -\frac{2}{11}\end{bmatrix}\begin{bmatrix}15\\13\\18\end{bmatrix}=\begin{bmatrix}19\\19\\1\end{bmatrix}$	S S A
QCV	$\begin{bmatrix}17\\3\\22\end{bmatrix}$	$\begin{bmatrix}\frac{1}{11} & -\frac{8}{11} & \frac{5}{11}\\ -\frac{2}{11} & \frac{5}{11} & \frac{1}{11}\\ \frac{4}{11} & \frac{1}{11} & -\frac{2}{11}\end{bmatrix}\begin{bmatrix}17\\3\\22\end{bmatrix}=\begin{bmatrix}7\\5\\19\end{bmatrix}$	G E S

4. CONCLUSION

In this paper, the Hill Cipher method has been developed,which is one of the cryptographic techniques for encrypting a text by translating a message into a code over a matrice of numbers modulo 26 and converting the codes into the actual message using the decipher method over a matrice of numbers modulo 26. The developed matrices are n×n matrice of order 3. From the test results, it is found that the hill cipher method and the decipher method are able to translate the actual text as long as the matrices given in the hill cipher algorithm have an inverse and determinant. For future research, it is suggested to develop other methods in the field of cryptography if given an arbitrary matrices has not invertible.

REFERENCES

[1] M. D. L. Siahaan and A. P. U. Siahaan, "Application of Hill Cipher Algorithm in Securing Text Messages," *Int. J. Innov. Res. Multidiscip. F.*, vol. 4, no. 10, pp. 55–59, 2018.

[2] M. Stinson, Douglas Robert Paterson, *Cryptography Theory and Practice*, 4th ed. New york: CRC Press, 2018. doi: https://doi.org/10.1201/9781315282497.

[3] M. Maxrizal, "A New Method Of Hill Cipher," in *International Conference on Science and Technology for Sustainability*, 2016, no. November, p. 3.

[4] K. J. Liew and V. T. Nguyen, "Hill Cipher Key Generation Using Skew-symmetric Matrix," *Proc. 7th Int. Cryptol. Inf. Secur. Conf. 2020, Cryptol. 2020*, no. June, pp. 85–93, 2020.

[5] M. Viswambari and K. Mani, "Generation of Key Matrix for Hill Cipher using Magic Rectangle," *Proc. - 2nd World Congr. Comput. Commun. Technol. WCCCT 2017*, vol. 10, no. 5, pp. 51–54, 2017.

[6] A. Hidayat and T. Alawiyah, "Enkripsi dan Dekripsi Teks menggunakan Algoritma Hill Cipher dengan Kunci Matriks Persegi Panjang," *J. Mat. Integr.*, vol. 9, no. 1, p. 39, 2013, doi: 10.24198/jmi.v9i1.10196.

[7] V. S. Shetty, R. Anusha, K. Dileep, and P. Hegde, "A Survey on Performance Analysis of Block Cipher Algorithms," *Proc. 5th Int. Conf. Inven. Comput. Technol. ICICT 2020*, pp. 167–174, 2020, doi: 10.1109/ICICT48043.2020.9112491.

[8] L. J. Pangaribuan, "Kriptografi Hybrida Agloritma Hill Cipher Dan Rivest Shamir Adleman (RSA) Sebagai Pengembangan Kriptografi Kunci Simetris (Studi Kasus : Nilai Mahasiswa Amik Mbp)," *J. Teknol. Inf. Dan Komun.*, vol. 7, no. 1, pp. 11–26, 2018.

[9] C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, P. Kumaresan, and M. F. Ijaz, "Analytical study of hybrid techniques for image encryption and decryption," *Sensors (Switzerland)*, vol. 20, no. 18, pp. 1–19, 2020, doi: 10.3390/s20185162.

[10] D. Vamsi and P. R. CH, "Hybrid Image Encryption Using Elliptic Curve Cryptography, Hadamard Transform and Hill Cipher," *Webology*, vol. 19, no. 1, pp. 2357–2378, Jan. 2022, doi: 10.14704/web/v19i1/web19160.

[11] K. Madhusudhan Reddy, A. Itagi, S. Dabas, and B. K. Prakash, "Image encryption using orthogonal Hill Cipher algorithm," *Int. J. Eng. Technol.*, vol. 7, no. 4, pp. 59–63, 2018, doi: 10.14419/ijet.v7i4.10.20707.

[12] J. R. Paragas, A. M. Sison, and R. P. Medina, "Hill cipher modification: A simplified approach," *2019 IEEE 11th Int. Conf. Commun. Softw. Networks, ICCSN 2019*, no. June, pp. 821–825, 2019, doi: 10.1109/ICCSN.2019.8905360.

[13] A. R. Yuliandaru, "Teknik Kriptografi Hill Cipher Menggunakan Matriks," 2016.

[14] T. Alawiyah, A. B. Hikmah, W. Wiguna, M. Kusmira, H. Sutisna, and B. K. Simpony, "Generation of Rectangular Matrix Key for Hill Cipher Algorithm Using Playfair Cipher," *J. Phys. Conf. Ser.*, vol. 1641, no. 1, 2020, doi: 10.1088/1742-6596/1641/1/012094.

[15] V. Kalaichelvi, K. Manimozhi, P. Meenakshi, B. Rajakumar, and P. Vimaladevi, "A new variant of Hill cipher algorithm for data security," *Int. J. Pure Appl. Math.*, vol. 117, no. 15 Special Issue, pp. 581–588, 2017.

[16] A. J. Menezes, "Applied Cryptography," *Electr. Eng.*, vol. 1, no. [32, pp. 429–455, 1996, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.2838&rep=rep1&type=pdf

[17] S. W. Bray, *Introduction to Cryptography and Python*. 2020. doi: 10.1002/9781119612216.ch1.

[18] Nana; and P. W. Prasetyo, "2021_An implementation of Hill Cipher and ×3×3 rubik's.pdf," *Bull. Appl. Math. Math. Educ.*, vol. 1, no. 2, pp. 75–92, 2021.

[19] W. Shwetambari and M. Ujwala, "Development of Matrix for Cryptography," *J. Emerg. Technol. Innov. Res.*, vol. 7, no. 4, pp. 112–118, 2020.