Journal of Information System and Application Development
Volume 2 Number 2 September 2024 page 131-143
P-ISSN: 2988-5698 | E-ISSN: 2988-4721
https://jurnal.unmer.ac.id/index.php/jisad

Layered security model through integration of Vigenere and Hill Cipher in digital message encryption

Argia Putri Ramadhani*, Nanda Putri Tami, Asih Lestari, Moh. Erkamim
Smart City Information System, Faculty of Engineering, Universitas Tunas Pembangunan, Surakarta, Indonesia

E-mail: *f0223005_argiaputriramadhani@student.utp.ac.id

Abstract. The rapid development of digitalization has a significant impact on data and information protection. One approach to protecting data and information is through the use of cryptography. This study aims to combine the use of the Vigenere and Hill Cipher algorithms in modeling to maintain the security and confidentiality of digital messages. The focus of this study is on the encryption process of digital messages in the form of text. Layered security in this study utilizes the advantages of each algorithm. The combination of these two algorithms is designed to increase encryption complexity and reduce vulnerability to cryptanalysis attacks. The encryption process begins by using the Vigenere Cipher to encrypt the initial message, then the results are re-encrypted using the Hill Cipher. The results of the study show that this layered security model can improve data security and make it difficult for unauthorized parties to crack it. The combination of the Vigenere and Hill Cipher algorithms can be an alternative layered security for digital message encryption in an effort to protect information and data from security threats in the digital era.

Keywords: cryptography, Vigenere Chiper, Hill Chiper, layered security, digital message

Submitted: 26-07-2024 | ***Accepted:*** 01-08-2024 | ***Published:*** 13-09-2024

How to Cite:
A. P. Ramadhani, N. P. Tami, A. Lestari, M. Erkamim, "Layered security model through integration of Vigenere and Hill Cipher in digital message encryption," *Journal of Information System and Application Development*, vol. 2, no. 2, pp. 131-143, September 2024, doi: 10.26905/jisad.v2i2.14005.

INTRODUCTION

The seemingly endless development of information technology causes problems in digital data security, such as cybercrime, data theft, operational disruption, wiretapping and so on. Therefore, there is a need for security in overcoming these problems, one of the simple solutions that can be applied is data encryption, which is expected to be able to prevent hacking by unauthorized parties.

Proper techniques in data encryption are very important so that sensitive information can be kept confidential and secure. One example is by using cryptographic techniques, where this cryptographic technique can not only be used in encoding digital data but can also be used in decoding codes or passwords.

Cryptography techniques themselves are divided into 2 types, namely classical cryptography and modern cryptography. Classical cryptography is a message encoding technique that has been in use for thousands of years before the invention of computers and modern technology. This technique uses mathematical methods and manipulation of letters or characters in the original technique to produce an encrypted message that is difficult for people who do not have the same key or method to read or understand.

Modern cryptography, on the other hand, is a more sophisticated and complex message encoding technique designed to overcome the weaknesses of classical cryptography techniques and to protect information from stronger attacks. These techniques typically use more complex and more secure algorithms, and require longer and more complex keys.

DOI: 10.26905/jisad.v2i2.14005

Information and data security is an important concern for most organizations and individuals in today's era of digital development. As more sensitive data is transmitted and stored electronically, threats to confidentiality, integrity, and availability of information are also increasing. One of the techniques that can be used in data security is cryptography. To ensure the security and integrity of a data, an encoding process is needed. With this method of encoding, the original data will not be read by uninterested parties [1].

The science and art that studies techniques to secure communications or information from unauthorized persons is known as cryptography. In other words, cryptography is a way of hiding information so that it can only be read by those who have a special key. The word cryptography comes from the Greek language, namely crypto which means secret and graphia which means writing [2]. So in general, cryptography is understood as the process of writing or sending messages in a secret and hidden manner [3].

There are four main objectives of cryptography and this is also included in the aspect of information security, namely Confidentiality, Integrity, Authentication, Non-Repudiation. Confidentiality means ensuring that only authorized parties can access data or information. Integrity means ensuring that information cannot be altered or modified during transmission. Furthermore, Authentication means ensuring that the parties involved in the communication are authentic and accurate. And finally, non-repudiation is to prevent the sender of information from denying that they are the one who sent the message. There are several terms in cryptography, as shown in Figure 1.

1. Encryption is the process of converting original information (plaintext) into an unreadable form (ciphertext) using encryption algorithms and keys.
2. Decryption or the process of converting ciphertext back into its original form (plaintext) using an algorithm and a decryption key.
3. Plaintext is the original information or data that has not been encrypted and can be read and understood.
4. Ciphertext or encrypted text that cannot be read by unauthorized parties.
5. A key or a value or information used in the encryption and decryption process. In cryptography, keys are crucial because they determine the results of encryption and decryption [4].

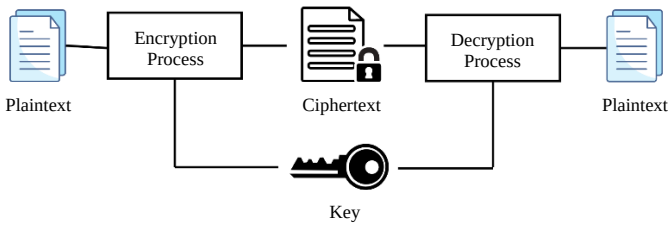

Figure 1. Cryptographic Process Flow Using Symmetric Keys

Based on the use of keys, cryptographic algorithms are divided into two types, namely symmetric and asymmetrical [5]. Symmetric cryptography is an encryption method that uses the same key to encrypt and decrypt messages. The security of this symmetric cryptography depends on the secrecy of the key. Asymmetric cryptography, on the other hand, is an encryption method that uses different key pairs for encryption and decryption. This key pair consists of a public key and a private key. Some examples that fall under symmetric cryptography are Vigenere Cipher and Hill Cipher.

Vigenere Cipher is one of the most common and popular methods of encoding text. Vigenere cipher is a text encoding method that uses a substitution table based on the letters of a keyword. This algorithm was introduced in the 16th century or around 1986 and published by a diplomat who is also a cryptologist from France, namely Blaise de Vigenère. However, this algorithm has already been explained in the book La Cifra del Sig by Giovan Battista Velaso in 1553 [6]. Vigenere Cipher has a mathematical formula which is (1)(2):

Encryption

$$Ci = (Pi + Ki) \ mod \ 26 \quad (1)$$

Decryption

$$Pi = (Ci - Ki) \ mod \ 26 \quad (2)$$

Information:
Ci = Ciphertext Character to - i
Pi = Plaintext Character to - i
Ki = Key Character to - I

The Hill Cipher is a type of substitution polyalphabetic cipher created by Lester S. Hill in 1929. It uses the basic technique of modulo arithmetic against matrices so that it is very difficult for cryptanalysts to solve or break into [7]. Hill cipher is a linear algebra-based text encoding method that uses a matrix to encrypt blocks of plaintext. This cryptographic technique uses a square matrix as the key used to perform encryption and decryption. Hill Cipher does not replace every equal letter in the plaintext with other letters in the ciphertext because it uses the matrix as the basis for encryption and decryption. Hill ciphers, which are polyalphabetic ciphers, can be categorized as block ciphers because the text to be processed will be divided into blocks of a certain size [8]. Hill Cipher has a mathematical formula which is (3)(4):

Encryption

$$Ci = (K \times Pi) \ mod \ 26 \quad (3)$$

Decryption

$$Pi = \left(K^{-1} \times Ci\right) \ mod \ 26 \quad (4)$$

Information:
Ci = Ciphertext Character to - i
Pi = Plaintext Character to - i
K^{-1} = Inverse of the key matrix

Previous studies have combined many Vigenere cipher algorithms with other cryptographic algorithms as well as new combinations with different methods. According to Noviyanti & Mira, (2022) with a study entitled Analysis of Caesar Cipher Vigenere Cipher and Hill Cipher Classical Cryptographic Algorithms, several studies show that classical cryptographic algorithms, such as Caesar Cipher, Vigenere Cipher, and Hill Cipher, are increasingly easily directed by irresponsible parties. Because of this, data editing, be it text messages, files, or images, needs to be modified before it is implemented [9].

The results of another study by Aurillya & Sicily (2023) titled Vigenere Cipher and Hill Cipher Algorithm Modification Application Using Temperature Conversion, show that the modified integration of Vigenere and Hill Ciphers, along with the temperature conversion equation, provides a robust framework for encrypting and decrypting messages, thereby significantly improving the security of digital communications [10]. According to Roman Gusmana et al., (2023) with the title Implementation of the Hill Cipher Algorithm Using 2x2 Matrix Keys in Securing Text Data, the results show the effectiveness of the Hill Cipher algorithm in encrypting and decrypting textual data, showing its potential as a reliable cryptographic method to protect sensitive information [11].

Another study titled Application of Vigenere Cipher and Hill Cipher Algorithms Using Mass Units with the results of this study highlights the effectiveness of combining Vigenere and Hill Cipher algorithms to create a more secure data encryption system, which ultimately facilitates safer communication in an increasingly digital world [12]. Another study titled "Evaluation of Vigenère

Cipher Performance on Encrypted Digital Data", shows that although Vigenère cipher can provide a good level of security, it has significant vulnerability to various forms of attack, especially frequency analysis and other modern techniques. These studies also highlight the importance of using strong keys and additional methods to improve the security of encryption using Vigenère ciphers [13].

The research entitled Vigenere Cipher Algorithm Implementation Algorithm for Encryption and Decryption in Drug Data Prescription at the Mertoyudan 1 Health Center, Magelang Regency shows that Vigenere Cipher is very suitable to be used in securing drug data based on the number of characters, the drug name and the key (key) of the day and the same number of characters. The implementation of the system that has been developed has been able to provide convenience for Doctors, Pharmacists and Patients and with the existence of this Drug Prescription Data Encryption System is useful to protect data from poor data misuse [14]. The results of the study entitled Combination and Modification of Vigenere Cipher and Hill Cipher Using Hybrid Methods of Postal Code, Trigonometry, and Temperature Conversion as Message Security, show that the results of research and implementation of the system for message security using classical algorithms, especially combining and modifying Vigenere Cipher and Hill Cipher using Hybrid Methods of Postal Code, Trigonometry, and Temperature Conversion are not easy for cryptanalysts to Solve ciphertext, as it has a layered level of difficulty to secure messages [15].

From the results of another study conducted by Muhammad Azmi & Zulkarnaen, (2021) with the title Implementation of a Caesar Cipher and Hill Cipher Combination Using Morse Cryptography Modification for Text-Based Message Security, it shows the process of combining the Caesar Cipher and Hill Cipher Algorithms modified into Morse cipher, where the encryption results will be difficult for irresponsible parties to crack. The process of ciphertext into an image file will make it difficult for irresponsible people to decipher messages sent in the form of images. The execution time of the encryption process depends on the number of characters that are encrypted. [16].

METHOD

During the encryption process, researchers first used the Vigenere Cipher algorithm to convert messages from plaintext to ciphertext. Then, the generated ciphertext will be re-encrypted using the Hill Cipher algorithm. This process is illustrated in the illustration in Figure 2. The use of Vigenere Cipher as a first step and later Hill Cipher in a layered security model has several significant considerations and advantages, one of which is the increased complexity of encryption.

By applying the Vigenere Cipher algorithm first, the plaintext will be converted into a random shape, so that the original plaintext pattern will be hidden. When the encryption results of the Vigenere Cipher algorithm are further encrypted using Hill Cipher, the end result becomes more random and difficult to crack because Hill Cipher modifies the text based on matrix transformations, which is more difficult to analyze compared to Vigenere Cipher or other simple substitution algorithms. The combined encryption process of the Vigenere cipher and Hill cipher is done by manual calculations. The manual calculation in this encryption process uses the formula listed in mathematical equations (1) and (3).

The encryption process using the Vigenere cipher is carried out based on a predetermined symmetry key. After that, the ciphertext from the Vigenere cipher will be re-encrypted using a Hill cipher with a predefined key matrix. This process adds an extra layer of security, making the final ciphertext more random and difficult to identify.

In the manual calculation using the Vigenere Cipher algorithm, with the plaintext: DEPLOY the entire Red Beret Army, and the key used: READY. When viewed based on the placement of the index in Figure 4, the plaintext and key occupy the same position as in Figure 2. Then, the result of this Vigenere Cipher encryption will be re-encrypted using Hill Cipher, with the matrix key: $\begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}$

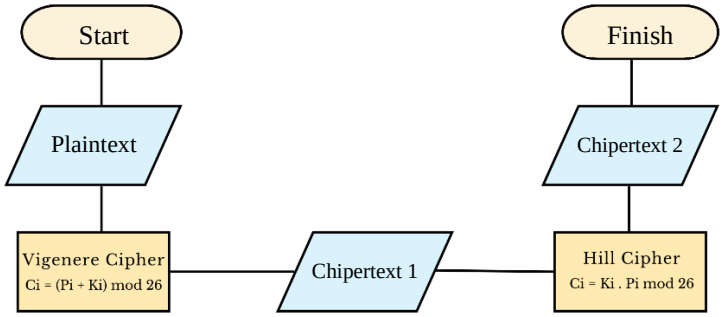

Figure 2. Encryption Flow Vigenere-Hill Cipher

During the decryption process, the conversion of ciphertext to plaintext will also be carried out in two stages. This process is described in detail in Figure 3. In the first stage, ciphertext that has been encrypted using the Hill cipher will be decrypted first to obtain the ciphertext results from the previous Vigenere cipher encryption process. The Hill cipher decryption process involves using an inverse key matrix from the key matrix used during encryption. After obtaining the ciphertext from Hill cipher, the next step is to decrypt the ciphertext using the Vigenere cipher to obtain the original plaintext. The manual calculation of the decryption process uses the formula listed in the mathematical equations (4) and (2).

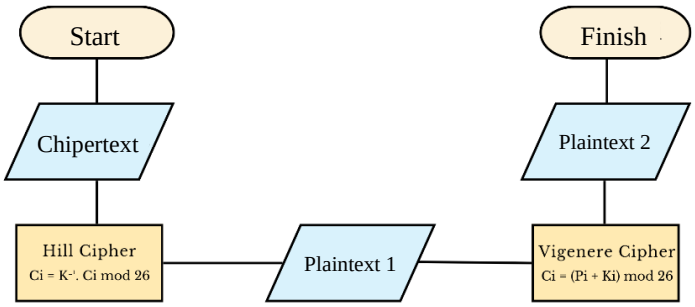

Figure 3. Decryption Flow Hill-Vigenere Cipher

RESULTS AND DISCUSSION

Layered Security Encryption Process using Vigenere and Hill Cipher

To make the encryption process easier, it is simulated on a sample plaintext as well as a predefined key. The initial step begins by placing the alphabetic positions A-Z and initiating the index from 0 to 25, as shown in Table 1.

Table 1. Placement of Alphabet A-Z According to Index 0-25

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext Indexation for Vigenere Cipher based on case study is shown in Table 2. Furthermore, the encryption process is carried out using the Vigenere Cipher algorithm with manual calculations, as described in the mathematical formulas in equation (5).

Table 2. Plaintext Indexing According to a Case Study for the Vigenere Cipher

K	E	R	A	H	K	A	N	S	E	L	U	R	U	H
10	4	17	0	7	10	0	13	18	4	11	20	17	20	7
S	I	A	P	S	I	A	P	S	I	A	P	S	I	A
18	8	0	15	18	8	0	15	18	8	0	15	18	8	0
P	A	S	U	K	A	N	B	A	R	E	T	M	E	R	A	H
15	0	18	20	10	0	13	1	0	17	4	19	12	4	17	0	7
P	S	I	A	P	S	I	A	P	S	I	A	P	S	I	A	P
15	18	8	0	15	18	8	0	15	18	8	0	15	18	8	0	15

$$
\begin{aligned}
Ci &= (K+S)\ mod\ 26 = (10+18)\ mod\ 26 = 28\ mod\ 26 = 2\ (C)\\
Ci &= (E+I)\ mod\ 26 = (4+8)\ mod\ 26 = 12\ mod\ 26 = 12\ (M)\\
Ci &= (R+A)\ mod\ 26 = (17+0)\ mod\ 26 = 17\ mod\ 26 = 17\ (R)\\
Ci &= (A+P)\ mod\ 26 = (0+15)\ mod\ 26 = 15\ mod\ 26 = 15\ (P)\\
Ci &= (H+S)\ mod\ 26 = (7+18)\ mod\ 26 = 25\ mod\ 26 = 25\ (Z)\\
Ci &= (K+I)\ mod\ 26 = (10+8)\ mod\ 26 = 18\ mod\ 26 = 18\ (S)\\
Ci &= (A+A)\ mod\ 26 = (0+0)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)\\
Ci &= (N+P)\ mod\ 26 = (13+15)\ mod\ 26 = 28\ mod\ 26 = 2\ (C)\\
Ci &= (S+S)\ mod\ 26 = (18+18)\ mod\ 26 = 36\ mod\ 26 = 10\ (K)\\
Ci &= (E+I)\ mod\ 26 = (4+8)\ mod\ 26 = 12\ mod\ 26 = 12\ (M)\\
Ci &= (L+A)\ mod\ 26 = (11+0)\ mod\ 26 = 11\ mod\ 26 = 11\ (L)\\
Ci &= (U+P)\ mod\ 26 = (20+15)\ mod\ 26 = 35\ mod\ 26 = 9\ (J)\\
Ci &= (R+S)\ mod\ 26 = (17+18)\ mod\ 26 = 35\ mod\ 26 = 9\ (J)\\
Ci &= (U+I)\ mod\ 26 = (20+8)\ mod\ 26 = 28\ mod\ 26 = 2\ (C)\\
Ci &= (H+A)\ mod\ 26 = (7+0)\ mod\ 26 = 7\ mod\ 26 = 7\ (H)\\
Ci &= (P+P)\ mod\ 26 = (15+15)\ mod\ 26 = 30\ mod\ 26 = 4\ (C)\\
Ci &= (A+S)\ mod\ 26 = (0+18)\ mod\ 26 = 18\ mod\ 26 = 18\ (S)\\
Ci &= (S+I)\ mod\ 26 = (18+8)\ mod\ 26 = 26\ mod\ 26 = 0\ (A)\\
Ci &= (U+A)\ mod\ 26 = (20+0)\ mod\ 26 = 20\ mod\ 26 = 20\ (U)\\
Ci &= (K+P)\ mod\ 26 = (10+15)\ mod\ 26 = 25\ mod\ 26 = 25\ (Z)\\
Ci &= (A+S)\ mod\ 26 = (0+18)\ mod\ 26 = 18\ mod\ 26 = 18\ (S)\\
Ci &= (N+I)\ mod\ 26 = (13+8)\ mod\ 26 = 21\ mod\ 26 = 21\ (V)\\
Ci &= (B+A)\ mod\ 26 = (1+0)\ mod\ 26 = 1\ mod\ 26 = 1\ (B)\\
Ci &= (A+P)\ mod\ 26 = (0+15)\ mod\ 26 = 15\ mod\ 26 = 15\ (P)\\
Ci &= (R+S)\ mod\ 26 = (17+18)\ mod\ 26 = 35\ mod\ 26 = 9\ (J)\\
Ci &= (E+I)\ mod\ 26 = (4+8)\ mod\ 26 = 12\ mod\ 26 = 12\ (M)\\
Ci &= (T+A)\ mod\ 26 = (19+0)\ mod\ 26 = 19\ mod\ 26 = 19\ (T)\\
Ci &= (M+P)\ mod\ 26 = (12+15)\ mod\ 26 = 27\ mod\ 26 = 1\ (B)\\
Ci &= (E+S)\ mod\ 26 = (4+18)\ mod\ 26 = 22\ mod\ 26 = 22\ (W)\\
Ci &= (R+I)\ mod\ 26 = (17+8)\ mod\ 26 = 25\ mod\ 26 = 25\ (Z)\\
Ci &= (A+A)\ mod\ 26 = (0+0)\ mod\ 26 = 0\ mod\ 26 = 0\ (A)\\
Ci &= (H+P)\ mod\ 26 = (7+15)\ mod\ 26 = 22\ mod\ 26 = 22\ (W)
\end{aligned}
\tag{5}
$$

Based on the mathematical formulas in equation (5), the first ciphertext obtained was CMRPZSACKMLJJCHESAUZSVBPJMTBWZAW. Furthermore, according to the layered security model used in this study, the results of the first ciphertext were re-encrypted with the Hill Cipher algorithm. In the initial stage, indexation will be carried out according to the results of the first ciphertext, as shown in Figure 3.

$\begin{bmatrix} C \\ M \end{bmatrix}$	=	$\begin{bmatrix} 2 \\ 12 \end{bmatrix}$	$\begin{bmatrix} K \\ M \end{bmatrix}$	=	$\begin{bmatrix} 10 \\ 12 \end{bmatrix}$	$\begin{bmatrix} S \\ A \end{bmatrix}$	=	$\begin{bmatrix} 18 \\ 0 \end{bmatrix}$	$\begin{bmatrix} J \\ M \end{bmatrix}$	=	$\begin{bmatrix} 9 \\ 12 \end{bmatrix}$
$\begin{bmatrix} R \\ P \end{bmatrix}$	=	$\begin{bmatrix} 17 \\ 15 \end{bmatrix}$	$\begin{bmatrix} L \\ J \end{bmatrix}$	=	$\begin{bmatrix} 11 \\ 9 \end{bmatrix}$	$\begin{bmatrix} U \\ Z \end{bmatrix}$	=	$\begin{bmatrix} 20 \\ 25 \end{bmatrix}$	$\begin{bmatrix} T \\ B \end{bmatrix}$	=	$\begin{bmatrix} 19 \\ 1 \end{bmatrix}$
$\begin{bmatrix} Z \\ S \end{bmatrix}$	=	$\begin{bmatrix} 25 \\ 18 \end{bmatrix}$	$\begin{bmatrix} J \\ C \end{bmatrix}$	=	$\begin{bmatrix} 9 \\ 2 \end{bmatrix}$	$\begin{bmatrix} S \\ V \end{bmatrix}$	=	$\begin{bmatrix} 18 \\ 21 \end{bmatrix}$	$\begin{bmatrix} W \\ Z \end{bmatrix}$	=	$\begin{bmatrix} 22 \\ 25 \end{bmatrix}$
$\begin{bmatrix} A \\ C \end{bmatrix}$	=	$\begin{bmatrix} 0 \\ 2 \end{bmatrix}$	$\begin{bmatrix} H \\ E \end{bmatrix}$	=	$\begin{bmatrix} 7 \\ 4 \end{bmatrix}$	$\begin{bmatrix} B \\ P \end{bmatrix}$	=	$\begin{bmatrix} 1 \\ 15 \end{bmatrix}$	$\begin{bmatrix} A \\ W \end{bmatrix}$	=	$\begin{bmatrix} 0 \\ 22 \end{bmatrix}$

Figure 3. Indexation of the First Ciphertext Results

Furthermore, the results of this first encryption will be processed using Hill Cipher with manual calculations using the key $\begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix}$ and mathematical formulas listed in equation (3) to ensure the accuracy of the encryption results. Through the application of the mathematical formula of equations (6), the ciphertext OYBZATGIEGXVYRAXKSLQVYVJCFPXPSOK was obtained.

$$Ci = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} C \\ M \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} 2 \\ 12 \end{bmatrix} = \begin{bmatrix} (2 \times 2) & + & (3 \times 12) \\ (1 \times 2) & + & (4 \times 12) \end{bmatrix} = \begin{bmatrix} (4) & + & (36) \\ (2) & + & (48) \end{bmatrix} =$$
$$\begin{bmatrix} 40 \\ 50 \end{bmatrix} mod\ 26 = \begin{bmatrix} 14 \\ 26 \end{bmatrix} = \begin{bmatrix} O \\ Y \end{bmatrix}$$
$$Ci = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} R \\ P \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} 17 \\ 15 \end{bmatrix} = \begin{bmatrix} (2 \times 17) & + & (3 \times 15) \\ (1 \times 17) & + & (4 \times 15) \end{bmatrix} = \begin{bmatrix} (34) & + & (45) \\ (17) & + & (48) \end{bmatrix} =$$
$$\begin{bmatrix} 79 \\ 77 \end{bmatrix} mod\ 26 = \begin{bmatrix} 1 \\ 25 \end{bmatrix} = \begin{bmatrix} B \\ Z \end{bmatrix}$$
$$Ci = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} Z \\ S \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} 25 \\ 18 \end{bmatrix} = \begin{bmatrix} (2 \times 25) & + & (3 \times 18) \\ (1 \times 25) & + & (4 \times 18) \end{bmatrix} = \begin{bmatrix} (50) & + & (54) \\ (25) & + & (72) \end{bmatrix} =$$
$$\begin{bmatrix} 109 \\ 97 \end{bmatrix} mod\ 26 = \begin{bmatrix} 0 \\ 19 \end{bmatrix} = \begin{bmatrix} A \\ T \end{bmatrix}$$
$$Ci = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} A \\ C \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \end{bmatrix} = \begin{bmatrix} (2 \times 0) & + & (3 \times 2) \\ (1 \times 0) & + & (4 \times 2) \end{bmatrix} = \begin{bmatrix} (0) & + & (6) \\ (0) & + & (8) \end{bmatrix} =$$
$$\begin{bmatrix} 6 \\ 8 \end{bmatrix} mod\ 26 = \begin{bmatrix} 6 \\ 8 \end{bmatrix} = \begin{bmatrix} G \\ I \end{bmatrix}$$
$$Ci = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} K \\ M \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} 10 \\ 12 \end{bmatrix} = \begin{bmatrix} (2 \times 10) & + & (3 \times 12) \\ (1 \times 10) & + & (4 \times 12) \end{bmatrix} = \begin{bmatrix} (20) & + & (36) \\ (10) & + & (48) \end{bmatrix} =$$
$$\begin{bmatrix} 56 \\ 58 \end{bmatrix} mod\ 26 = \begin{bmatrix} 4 \\ 6 \end{bmatrix} = \begin{bmatrix} E \\ G \end{bmatrix}$$
$$Ci = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} L \\ J \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} 11 \\ 9 \end{bmatrix} = \begin{bmatrix} (2 \times 11) & + & (3 \times 9) \\ (1 \times 11) & + & (4 \times 9) \end{bmatrix} = \begin{bmatrix} (22) & + & (27) \\ (11) & + & (36) \end{bmatrix} =$$
$$\begin{bmatrix} 49 \\ 47 \end{bmatrix} mod\ 26 = \begin{bmatrix} 23 \\ 21 \end{bmatrix} = \begin{bmatrix} X \\ V \end{bmatrix}$$
$$Ci = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} J \\ C \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} 9 \\ 2 \end{bmatrix} = \begin{bmatrix} (2 \times 9) & + & (3 \times 2) \\ (1 \times 9) & + & (4 \times 2) \end{bmatrix} = \begin{bmatrix} (18) & + & (6) \\ (9) & + & (8) \end{bmatrix} =$$
$$\begin{bmatrix} 24 \\ 17 \end{bmatrix} mod\ 26 = \begin{bmatrix} 24 \\ 17 \end{bmatrix} = \begin{bmatrix} Y \\ R \end{bmatrix}$$

$$Ci = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} H \\ E \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 4 \end{bmatrix} \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} (2 \times 7) & + & (3 \times 4) \\ (1 \times 7) & + & (4 \times 4) \end{bmatrix} = \begin{bmatrix} (14) & + & (12) \\ (7) & + & (16) \end{bmatrix} =$$
$$\begin{bmatrix} 26 \\ 23 \end{bmatrix} mod\ 26 = \begin{bmatrix} 0 \\ 23 \end{bmatrix} = \begin{bmatrix} A \\ X \end{bmatrix}$$

$$Ci = \begin{bmatrix}2 & 3\\1 & 4\end{bmatrix}\begin{bmatrix}S\\A\end{bmatrix} = \begin{bmatrix}2 & 3\\1 & 4\end{bmatrix}\begin{bmatrix}18\\0\end{bmatrix} = \begin{bmatrix}(2\times 18) & + & (3\times 0)\\(1\times 18) & + & (4\times 0)\end{bmatrix} = \begin{bmatrix}(36) & + & (0)\\(18) & + & (0)\end{bmatrix} =$$
$$\begin{bmatrix}36\\18\end{bmatrix} mod\ 26 = \begin{bmatrix}10\\18\end{bmatrix} = \begin{bmatrix}K\\S\end{bmatrix}$$
$$Ci = \begin{bmatrix}2 & 3\\1 & 4\end{bmatrix}\begin{bmatrix}U\\Z\end{bmatrix} = \begin{bmatrix}2 & 3\\1 & 4\end{bmatrix}\begin{bmatrix}20\\25\end{bmatrix} = \begin{bmatrix}(2\times 20) & + & (3\times 25)\\(1\times 20) & + & (4\times 25)\end{bmatrix} = \begin{bmatrix}(40) & + & (75)\\(20) & + & (100)\end{bmatrix} =$$
$$\begin{bmatrix}115\\120\end{bmatrix} mod\ 26 = \begin{bmatrix}11\\16\end{bmatrix} = \begin{bmatrix}L\\Q\end{bmatrix}$$
$$Ci = \begin{bmatrix}2 & 3\\1 & 4\end{bmatrix}\begin{bmatrix}S\\V\end{bmatrix} = \begin{bmatrix}2 & 3\\1 & 4\end{bmatrix}\begin{bmatrix}18\\21\end{bmatrix} = \begin{bmatrix}(2\times 18) & + & (3\times 21)\\(1\times 18) & + & (4\times 21)\end{bmatrix} = \begin{bmatrix}(36) & + & (63)\\(18) & + & (84)\end{bmatrix} =$$
$$\begin{bmatrix}99\\102\end{bmatrix} mod\ 26 = \begin{bmatrix}21\\24\end{bmatrix} = \begin{bmatrix}V\\Y\end{bmatrix}$$
$$Ci = \begin{bmatrix}2 & 3\\1 & 4\end{bmatrix}\begin{bmatrix}B\\P\end{bmatrix} = \begin{bmatrix}2 & 3\\1 & 4\end{bmatrix}\begin{bmatrix}1\\15\end{bmatrix} = \begin{bmatrix}(2\times 1) & + & (3\times 15)\\(1\times 1) & + & (4\times 15)\end{bmatrix} = \begin{bmatrix}(2) & + & (45)\\(1) & + & (60)\end{bmatrix} =$$
$$\begin{bmatrix}47\\61\end{bmatrix} mod\ 26 = \begin{bmatrix}21\\9\end{bmatrix} = \begin{bmatrix}V\\J\end{bmatrix}$$
$$Ci = \begin{bmatrix}2 & 3\\1 & 4\end{bmatrix}\begin{bmatrix}J\\M\end{bmatrix} = \begin{bmatrix}2 & 3\\1 & 4\end{bmatrix}\begin{bmatrix}9\\12\end{bmatrix} = \begin{bmatrix}(2\times 9) & + & (3\times 12)\\(1\times 9) & + & (4\times 12)\end{bmatrix} = \begin{bmatrix}(18) & + & (36)\\(9) & + & (48)\end{bmatrix} =$$
$$\begin{bmatrix}54\\57\end{bmatrix} mod\ 26 = \begin{bmatrix}2\\5\end{bmatrix} = \begin{bmatrix}C\\F\end{bmatrix}$$
$$Ci = \begin{bmatrix}2 & 3\\1 & 4\end{bmatrix}\begin{bmatrix}T\\B\end{bmatrix} = \begin{bmatrix}2 & 3\\1 & 4\end{bmatrix}\begin{bmatrix}19\\1\end{bmatrix} = \begin{bmatrix}(2\times 19) & + & (3\times 1)\\(1\times 19) & + & (4\times 1)\end{bmatrix} = \begin{bmatrix}(38) & + & (3)\\(19) & + & (4)\end{bmatrix} =$$
$$\begin{bmatrix}41\\23\end{bmatrix} mod\ 26 = \begin{bmatrix}15\\23\end{bmatrix} = \begin{bmatrix}P\\X\end{bmatrix}$$
$$Ci = \begin{bmatrix}2 & 3\\1 & 4\end{bmatrix}\begin{bmatrix}W\\Z\end{bmatrix} = \begin{bmatrix}2 & 3\\1 & 4\end{bmatrix}\begin{bmatrix}22\\25\end{bmatrix} = \begin{bmatrix}(2\times 22) & + & (3\times 25)\\(1\times 22) & + & (4\times 25)\end{bmatrix} = \begin{bmatrix}(44) & + & (75)\\(22) & + & (100)\end{bmatrix} =$$
$$\begin{bmatrix}119\\122\end{bmatrix} mod\ 26 = \begin{bmatrix}15\\18\end{bmatrix} = \begin{bmatrix}P\\S\end{bmatrix}$$
$$Ci = \begin{bmatrix}2 & 3\\1 & 4\end{bmatrix}\begin{bmatrix}A\\W\end{bmatrix} = \begin{bmatrix}2 & 3\\1 & 4\end{bmatrix}\begin{bmatrix}0\\22\end{bmatrix} = \begin{bmatrix}(2\times 0) & + & (3\times 22)\\(1\times 0) & + & (4\times 22)\end{bmatrix} = \begin{bmatrix}(0) & + & (66)\\(0) & + & (88)\end{bmatrix} =$$
$$\begin{bmatrix}66\\88\end{bmatrix} mod\ 26 = \begin{bmatrix}14\\10\end{bmatrix} = \begin{bmatrix}O\\K\end{bmatrix} \quad (6)$$

Layered Security Decryption Process using Hill and Vigenere Cipher

In the encryption process using manual calculations, the final ciphertext has been obtained, namely OYBZATGIEGXVYRAXKSLQVYVJCFPXPSOK. To convert these ciphertks back into plaintext, a decryption process is carried out which also goes through two stages. The first stage, the decryption process will begin using the Hill Cipher algorithm. Furthermore, the initial plaintext obtained will be returned to the original plaintext using the Vigenere cipher. The Vigenere cipher algorithm in the decryption process uses the same key as when performing encryption. Meanwhile, in Hill Cipher, the decryption process begins by looking for the inverse value of the key matrix. Refer to the mathematical formula listed in equation (4).

The first step to finding the inverse value of a key matrix is to calculate the determinant value of that key matrix. The mathematical formula for calculating determinants can be seen in equation (7). This process is important to ensure that the decryption process runs correctly and generates a plaintext that matches the original message.

$$det(K) = \det\begin{bmatrix}a & b\\c & d\end{bmatrix} = \big((a\times d) - (b\times c)\big) \quad (7)$$

Next, insert the key matrix used in the Hill Cipher algorithm during encryption into the formula to calculate the determinants listed in equation (8). The determinant value of the predefined key matrix when encrypting using Hill Cipher is 5, as calculated in equation (8).

$$\det(K) = \det\begin{bmatrix}2 & 3\\ 1 & 4\end{bmatrix} = \big((2\times 4) - (3\times 1)\big) = \big((8) - (3)\big) = 5 \tag{8}$$

The next step is to calculate the inverse of the key matrix, denoted as $^{K-1}$, using the mathematical formula listed in equation (9). Next, enter the values that have been obtained into the mathematical formula to calculate the matrix inverse, as stated in equation (10).

$$K^{-1} = \frac{1}{det(k)}\ mod\ 26 \begin{bmatrix} d & -b\\ -c & a\end{bmatrix} \tag{9}$$

$$K^{-1} = \frac{1}{5} mod\ 26 \begin{bmatrix} 4 & -3\\ -1 & 2\end{bmatrix} \tag{10}$$

Before multiplying by the matrix, it is necessary to calculate the value of $\frac{1}{5} mod\ 26$. To find the value of $\frac{1}{5} mod\ 26$, a number must be found that if multiplied by the number 5 and then modulated by 26 will result in the number 1.

$$(5\times 1)\ mod\ 26 = 5\ mod\ 26 = 5$$
$$(5\times 10)\ mod\ 26 = 50\ mod\ 26 = 24$$
$$(5\times 15)\ mod\ 26 = 75\ mod\ 26 = 23$$
$$\boldsymbol{(5\times 21)\ mod\ 26 = 105\ mod\ 26 = 1} \tag{11}$$

Thus, the result of $\frac{1}{5} mod\ 26$ is 21. As calculated in equation (11). Next, the process will be continued with manual calculations in (10) and continued in (12), based on the mathematical formula listed in equation (9).

$$K^{-1} = \frac{1}{5}\ mod\ 26 \begin{bmatrix} 4 & -3\\ -1 & 2\end{bmatrix} = 21\begin{bmatrix} 4 & -3\\ -1 & 2\end{bmatrix} = \begin{bmatrix}(21\times 4) & (21\times -3)\\ (21\times -1) & (21\times 2)\end{bmatrix} =$$
$$\begin{bmatrix} 84 & -63\\ -21 & 42\end{bmatrix} mod\ 26 = \begin{bmatrix}6 & 15\\ 5 & 16\end{bmatrix} \tag{12}$$

A matrix value $\begin{bmatrix}6 & 15\\ 5 & 16\end{bmatrix}$ is obtained, which will be used as the key for the Hill Cipher decryption process. This result refers to the calculation listed in equation (12). Furthermore, indexation will also be carried out according to the results of the final ciphertext, as shown in Figure 4.

$\begin{bmatrix}\mathbf{O}\\ \mathbf{Y}\end{bmatrix}$	=	$\begin{bmatrix}\mathbf{14}\\ \mathbf{24}\end{bmatrix}$	$\begin{bmatrix}\mathbf{E}\\ \mathbf{G}\end{bmatrix}$	=	$\begin{bmatrix}\mathbf{4}\\ \mathbf{6}\end{bmatrix}$	$\begin{bmatrix}\mathbf{K}\\ \mathbf{S}\end{bmatrix}$	=	$\begin{bmatrix}\mathbf{10}\\ \mathbf{18}\end{bmatrix}$	$\begin{bmatrix}\mathbf{C}\\ \mathbf{F}\end{bmatrix}$	=	$\begin{bmatrix}\mathbf{2}\\ \mathbf{5}\end{bmatrix}$
$\begin{bmatrix}\mathbf{B}\\ \mathbf{Z}\end{bmatrix}$	=	$\begin{bmatrix}\mathbf{1}\\ \mathbf{25}\end{bmatrix}$	$\begin{bmatrix}\mathbf{X}\\ \mathbf{V}\end{bmatrix}$	=	$\begin{bmatrix}\mathbf{23}\\ \mathbf{21}\end{bmatrix}$	$\begin{bmatrix}\mathbf{L}\\ \mathbf{Q}\end{bmatrix}$	=	$\begin{bmatrix}\mathbf{11}\\ \mathbf{16}\end{bmatrix}$	$\begin{bmatrix}\mathbf{P}\\ \mathbf{X}\end{bmatrix}$	=	$\begin{bmatrix}\mathbf{15}\\ \mathbf{23}\end{bmatrix}$
$\begin{bmatrix}\mathbf{A}\\ \mathbf{T}\end{bmatrix}$	=	$\begin{bmatrix}\mathbf{0}\\ \mathbf{19}\end{bmatrix}$	$\begin{bmatrix}\mathbf{Y}\\ \mathbf{R}\end{bmatrix}$	=	$\begin{bmatrix}\mathbf{24}\\ \mathbf{17}\end{bmatrix}$	$\begin{bmatrix}\mathbf{V}\\ \mathbf{Y}\end{bmatrix}$	=	$\begin{bmatrix}\mathbf{21}\\ \mathbf{24}\end{bmatrix}$	$\begin{bmatrix}\mathbf{P}\\ \mathbf{S}\end{bmatrix}$	=	$\begin{bmatrix}\mathbf{15}\\ \mathbf{18}\end{bmatrix}$
$\begin{bmatrix}\mathbf{G}\\ \mathbf{I}\end{bmatrix}$	=	$\begin{bmatrix}\mathbf{6}\\ \mathbf{8}\end{bmatrix}$	$\begin{bmatrix}\mathbf{A}\\ \mathbf{X}\end{bmatrix}$	=	$\begin{bmatrix}\mathbf{0}\\ \mathbf{23}\end{bmatrix}$	$\begin{bmatrix}\mathbf{V}\\ \mathbf{J}\end{bmatrix}$	=	$\begin{bmatrix}\mathbf{21}\\ \mathbf{9}\end{bmatrix}$	$\begin{bmatrix}\mathbf{O}\\ \mathbf{K}\end{bmatrix}$	=	$\begin{bmatrix}\mathbf{14}\\ \mathbf{10}\end{bmatrix}$

Figure 4. Indexation of the Final Ciphertext Result

Furthermore, the results of this final ciphertext will be processed using Hill Cipher with manual calculations using the key $\begin{bmatrix}6 & 15\\ 5 & 16\end{bmatrix}$ and mathematical formulas listed in equation (4), to ensure the accuracy of the decryption results.

$$Pi = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}O\\Y\end{bmatrix} = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}14\\24\end{bmatrix} = \begin{bmatrix}(6\times14) & + & (15\times24)\\(5\times14) & + & (16\times24)\end{bmatrix} = \begin{bmatrix}(84) & + & (360)\\(70) & + & (384)\end{bmatrix} = \begin{bmatrix}444\\454\end{bmatrix} mod\ 26 = \begin{bmatrix}2\\12\end{bmatrix} = \begin{bmatrix}C\\M\end{bmatrix}$$

$$Pi = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}B\\Z\end{bmatrix} = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}1\\25\end{bmatrix} = \begin{bmatrix}(6\times1) & + & (15\times25)\\(5\times1) & + & (16\times25)\end{bmatrix} = \begin{bmatrix}(6) & + & (375)\\(5) & + & (400)\end{bmatrix} = \begin{bmatrix}381\\405\end{bmatrix} mod\ 26 = \begin{bmatrix}17\\15\end{bmatrix} = \begin{bmatrix}R\\P\end{bmatrix}$$

$$Pi = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}A\\T\end{bmatrix} = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}0\\19\end{bmatrix} = \begin{bmatrix}(6\times0) & + & (15\times19)\\(5\times0) & + & (16\times19)\end{bmatrix} = \begin{bmatrix}(0) & + & (285)\\(0) & + & (304)\end{bmatrix} = \begin{bmatrix}285\\304\end{bmatrix} mod\ 26 = \begin{bmatrix}25\\18\end{bmatrix} = \begin{bmatrix}Z\\S\end{bmatrix}$$

$$Pi = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}G\\I\end{bmatrix} = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}6\\8\end{bmatrix} = \begin{bmatrix}(6\times6) & + & (15\times8)\\(5\times6) & + & (16\times8)\end{bmatrix} = \begin{bmatrix}(36) & + & (120)\\(30) & + & (128)\end{bmatrix} = \begin{bmatrix}156\\158\end{bmatrix} mod\ 26 = \begin{bmatrix}0\\2\end{bmatrix} = \begin{bmatrix}A\\C\end{bmatrix}$$

$$Pi = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}E\\G\end{bmatrix} = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}4\\6\end{bmatrix} = \begin{bmatrix}(6\times4) & + & (15\times6)\\(5\times4) & + & (16\times6)\end{bmatrix} = \begin{bmatrix}(24) & + & (90)\\(20) & + & (96)\end{bmatrix} = \begin{bmatrix}114\\116\end{bmatrix} mod\ 26 = \begin{bmatrix}10\\12\end{bmatrix} = \begin{bmatrix}K\\M\end{bmatrix}$$

$$Pi = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}X\\V\end{bmatrix} = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}23\\21\end{bmatrix} = \begin{bmatrix}(6\times23) & + & (15\times21)\\(5\times23) & + & (16\times21)\end{bmatrix} = \begin{bmatrix}(138) & + & (315)\\(115) & + & (336)\end{bmatrix} = \begin{bmatrix}453\\451\end{bmatrix} mod\ 26 = \begin{bmatrix}11\\9\end{bmatrix} = \begin{bmatrix}L\\J\end{bmatrix}$$

$$Pi = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}Y\\R\end{bmatrix} = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}24\\17\end{bmatrix} = \begin{bmatrix}(6\times24) & + & (15\times17)\\(5\times24) & + & (16\times17)\end{bmatrix} = \begin{bmatrix}(144) & + & (255)\\(120) & + & (272)\end{bmatrix} = \begin{bmatrix}399\\392\end{bmatrix} mod\ 26 = \begin{bmatrix}9\\2\end{bmatrix} = \begin{bmatrix}J\\C\end{bmatrix}$$

$$Pi = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}A\\X\end{bmatrix} = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}0\\23\end{bmatrix} = \begin{bmatrix}(6\times0) & + & (15\times23)\\(5\times0) & + & (16\times23)\end{bmatrix} = \begin{bmatrix}(0) & + & (345)\\(0) & + & (368)\end{bmatrix} = \begin{bmatrix}345\\368\end{bmatrix} mod\ 26 = \begin{bmatrix}7\\4\end{bmatrix} = \begin{bmatrix}H\\E\end{bmatrix}$$

$$Pi = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}K\\S\end{bmatrix} = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}10\\18\end{bmatrix} = \begin{bmatrix}(6\times10) & + & (15\times18)\\(5\times10) & + & (16\times18)\end{bmatrix} = \begin{bmatrix}(60) & + & (270)\\(50) & + & (288)\end{bmatrix} = \begin{bmatrix}330\\338\end{bmatrix} mod\ 26 = \begin{bmatrix}18\\0\end{bmatrix} = \begin{bmatrix}S\\A\end{bmatrix}$$

$$Pi = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}L\\Q\end{bmatrix} = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}11\\16\end{bmatrix} = \begin{bmatrix}(6\times11) & + & (15\times16)\\(5\times11) & + & (16\times16)\end{bmatrix} = \begin{bmatrix}(66) & + & (240)\\(55) & + & (256)\end{bmatrix} = \begin{bmatrix}306\\311\end{bmatrix} mod\ 26 = \begin{bmatrix}20\\25\end{bmatrix} = \begin{bmatrix}U\\Z\end{bmatrix}$$

$$Pi = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}V\\Y\end{bmatrix} = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}21\\24\end{bmatrix} = \begin{bmatrix}(6\times21) & + & (15\times24)\\(5\times21) & + & (16\times24)\end{bmatrix} = \begin{bmatrix}(126) & + & (360)\\(105) & + & (384)\end{bmatrix} = \begin{bmatrix}486\\489\end{bmatrix} mod\ 26 = \begin{bmatrix}18\\21\end{bmatrix} = \begin{bmatrix}S\\V\end{bmatrix}$$

$$Pi = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}V\\J\end{bmatrix} = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}21\\9\end{bmatrix} = \begin{bmatrix}(6\times21) & + & (15\times9)\\(5\times21) & + & (16\times9)\end{bmatrix} = \begin{bmatrix}(126) & + & (135)\\(105) & + & (144)\end{bmatrix} = \begin{bmatrix}261\\249\end{bmatrix} mod\ 26 = \begin{bmatrix}1\\15\end{bmatrix} = \begin{bmatrix}B\\P\end{bmatrix}$$

$$Pi = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}C\\F\end{bmatrix} = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}2\\5\end{bmatrix} = \begin{bmatrix}(6\times2) & + & (15\times5)\\(5\times2) & + & (16\times5)\end{bmatrix} = \begin{bmatrix}(12) & + & (75)\\(10) & + & (80)\end{bmatrix} = \begin{bmatrix}87\\90\end{bmatrix} mod\ 26 = \begin{bmatrix}9\\12\end{bmatrix} = \begin{bmatrix}J\\M\end{bmatrix}$$

$$Pi = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}P\\X\end{bmatrix} = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}15\\23\end{bmatrix} = \begin{bmatrix}(6\times15) & + & (15\times23)\\(5\times15) & + & (16\times23)\end{bmatrix} = \begin{bmatrix}(90) & + & (345)\\(75) & + & (368)\end{bmatrix} = \begin{bmatrix}435\\443\end{bmatrix} mod\ 26 = \begin{bmatrix}19\\1\end{bmatrix} = \begin{bmatrix}T\\B\end{bmatrix}$$

$$Pi = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}P\\S\end{bmatrix} = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}15\\18\end{bmatrix} = \begin{bmatrix}(6\times15) & + & (15\times18)\\(5\times15) & + & (16\times18)\end{bmatrix} = \begin{bmatrix}(90) & + & (270)\\(75) & + & (288)\end{bmatrix} = \begin{bmatrix}360\\363\end{bmatrix} mod\ 26 = \begin{bmatrix}22\\25\end{bmatrix} = \begin{bmatrix}W\\Z\end{bmatrix}$$

$$Pi = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}O\\K\end{bmatrix} = \begin{bmatrix}6 & 15\\5 & 16\end{bmatrix}\begin{bmatrix}14\\10\end{bmatrix} = \begin{bmatrix}(6\times14) & + & (15\times10)\\(5\times14) & + & (16\times10)\end{bmatrix} = \begin{bmatrix}(84) & + & (150)\\(70) & + & (160)\end{bmatrix} = \begin{bmatrix}234\\230\end{bmatrix} mod\ 26 = \begin{bmatrix}0\\22\end{bmatrix} = \begin{bmatrix}A\\W\end{bmatrix} \quad (13)$$

Based on manual calculations, the first decryption result resulted in an unreadable and meaningless message, namely CMRPZSACKMLJJCHESAUZSVBPJMTBWZAW. Next, this ciphertext will be further processed using the Vigenere Cipher algorithm with the key "READY". This decryption process aims to return the ciphertext into plaintext that can be read clearly. The initial step involves indexing to adjust between the ciphertext and the key used, as shown in Table 3. The decryption process is carried out using manual calculations, referring to the mathematical functions listed in equations(14).

Table 3. Indexing for Decryption Using Vigenere Cipher

C	M	R	P	Z	S	A	C	K	M	L	J	J	C	H
2	12	17	15	25	18	0	2	10	12	11	9	9	2	7
S	I	A	P	S	I	A	P	S	I	A	P	S	I	A
18	8	0	15	18	8	0	15	18	8	0	15	18	8	0
E	S	A	U	Z	S	V	B	P	J	M	T	B	W	Z	A	W
4	18	0	20	25	18	21	1	15	9	12	19	1	22	25	0	22
P	S	I	A	P	S	I	A	P	S	I	A	P	S	I	A	P
15	18	8	0	15	18	8	0	15	18	8	0	15	18	8	0	15

$$
\begin{aligned}
Pi &= (C - S)\ mod\ 26 = (2 - 18)\ mod\ 26 = (-16)\ mod\ 26 = 10\ (K)\\
Pi &= (M - I)\ mod\ 26 = (12 - 8)\ mod\ 26 = (4)\ mod\ 26 = 4\ (E)\\
Pi &= (R - A)\ mod\ 26 = (17 - 0)\ mod\ 26 = (17)\ mod\ 26 = 17\ (R)\\
Pi &= (P - P)\ mod\ 26 = (15 - 15)\ mod\ 26 = (0)\ mod\ 26 = 0\ (A)\\
Pi &= (Z - S)\ mod\ 26 = (25 - 18)\ mod\ 26 = (7)\ mod\ 26 = 7\ (H)\\
Pi &= (S - I)\ mod\ 26 = (18 - 8)\ mod\ 26 = (10)\ mod\ 26 = 10\ (K)\\
Pi &= (A - A)\ mod\ 26 = (0 - 0)\ mod\ 26 = (0)\ mod\ 26 = 0\ (A)\\
Pi &= (C - P)\ mod\ 26 = (2 - 15)\ mod\ 26 = (-13)\ mod\ 26 = 13\ (N)\\
Pi &= (K - S)\ mod\ 26 = (10 - 18)\ mod\ 26 = (-8)\ mod\ 26 = 18\ (S)\\
Pi &= (M - I)\ mod\ 26 = (12 - 8)\ mod\ 26 = (4)\ mod\ 26 = 4\ (E)\\
Pi &= (L - A)\ mod\ 26 = (11 - 0)\ mod\ 26 = (11)\ mod\ 26 = 11\ (L)\\
Pi &= (J - P)\ mod\ 26 = (9 - 15)\ mod\ 26 = (-6)\ mod\ 26 = 20\ (U)\\
Pi &= (J - S)\ mod\ 26 = (9 - 18)\ mod\ 26 = (-9)\ mod\ 26 = 17\ (R)\\
Pi &= (C - I)\ mod\ 26 = (2 - 8)\ mod\ 26 = (-6)\ mod\ 26 = 20\ (U)\\
Pi &= (H - A)\ mod\ 26 = (7 - 0)\ mod\ 26 = (7)\ mod\ 26 = 7\ (H)\\
Pi &= (E - P)\ mod\ 26 = (4 - 15)\ mod\ 26 = (-11)\ mod\ 26 = 15\ (P)\\
Pi &= (S - S)\ mod\ 26 = (18 - 18)\ mod\ 26 = (0)\ mod\ 26 = 0\ (A)\\
Pi &= (A - I)\ mod\ 26 = (0 - 8)\ mod\ 26 = (-8)\ mod\ 26 = 18\ (S)\\
Pi &= (U - A)\ mod\ 26 = (20 - 0)\ mod\ 26 = (20)\ mod\ 26 = 20\ (U)\\
Pi &= (Z - P)\ mod\ 26 = (25 - 15)\ mod\ 26 = (10)\ mod\ 26 = 10\ (K)\\
Pi &= (S - S)\ mod\ 26 = (18 - 18)\ mod\ 26 = (0)\ mod\ 26 = 0\ (A)\\
Pi &= (V - I)\ mod\ 26 = (21 - 8)\ mod\ 26 = (13)\ mod\ 26 = 13\ (N)\\
Pi &= (B - A)\ mod\ 26 = (1 - 0)\ mod\ 26 = (1)\ mod\ 26 = 1\ (B)\\
Pi &= (P - P)\ mod\ 26 = (15 - 15)\ mod\ 26 = (0)\ mod\ 26 = 0\ (A)\\
Pi &= (J - S)\ mod\ 26 = (9 - 18)\ mod\ 26 = (-9)\ mod\ 26 = 17\ (R)\\
Pi &= (M - I)\ mod\ 26 = (12 - 8)\ mod\ 26 = (4)\ mod\ 26 = 4\ (E)\\
Pi &= (T - A)\ mod\ 26 = (19 - 0)\ mod\ 26 = (19)\ mod\ 26 = 19\ (T)\\
Pi &= (B - P)\ mod\ 26 = (1 - 15)\ mod\ 26 = (-14)\ mod\ 26 = 12\ (M)\\
Pi &= (W - S)\ mod\ 26 = (22 - 18)\ mod\ 26 = (4)\ mod\ 26 = 4\ (E)\\
Pi &= (Z - I)\ mod\ 26 = (25 - 8)\ mod\ 26 = (17)\ mod\ 26 = 17\ (R)\\
Pi &= (A - A)\ mod\ 26 = (0 - 0)\ mod\ 26 = (0)\ mod\ 26 = 0\ (A)\\
Pi &= (W - P)\ mod\ 26 = (22 - 15)\ mod\ 26 = (7)\ mod\ 26 = 7\ (H)
\end{aligned}
\tag{14}
$$

For the manual calculation of this decryption process, the results were obtained in the form of a plaintext of the entire RED Beret troops. These results show that the decryption process has successfully returned the ciphertext into a clearly readable message form that matches the original text.

CONCLUSIONS AND SUGGESTIONS

The study provides a digital text message encryption model by combining the Vigenere Cipher and Hill Cipher algorithms in a layered security model for digital message encryption. This modeling shows that the combination of the two algorithms results in a significant level of encryption complexity, thereby reducing the chances of digital messages being successfully cracked by unauthorized parties. This double encryption process begins with Vigenere Cipher followed by Hill Cipher, providing extra protection against messages sent in digital form. The results of this study indicate that this multi-layered security approach can be an alternative to protect information and data in the digital era that is full of security threats.

In addition to the combination of Vigenere and Hill Cipher, it is hoped that future research can explore more combinations of other algorithms, both classical and modern cryptography. And test the combination of these algorithms on different types of data such as images, audio, or other non-text data.

BIBLIOGRAPHY

[1] I. Y. Sari *et al.*, *Data and Information Security*. 2021.

[2] F. Az-Zahra, R. Marwati, and R. Sispiyati, "Implementation of QR Code with Enhanced Secure Hash Algorithm (SHA)-256 and Rivest Shamir Adleman (RSA) for Digital Document Authentication," *J. EurekaMatika*, vol. 12, no. 1, pp. 11–22, 2024, [Online]. Available: https://ejournal.upi.edu/index.php/JEM

[3] N. Chafid and H. Soffiana, "Implementation of Caesar's Classical Cryptographic Algorithm for the Design and Development of Web-Based E-Voting Applications (Case Study: SMAN 10 Tangerang)," *J. Ilm. Science and Technology*.Vol. 6 No. 2 pp. 133–145, 2022, doi:10.47080/centec.v6i2.2249.

[4] R. W. Asiani and I. Yanti, "Application of Caesar Cipher and Hill Cipher Cryptography in Sending Secret Messages as a Realistic Mathematics Learning Media in Modulo.pdf Material," *Baitul 'Ulum J. Library Science. and Inf.*, vol. 6, no. 1, pp. 79–97, 2022.

[5] R. Wardhani, S. R. Nurshiami, and N. Larasati, "Encryption and Decryption Computing Using Hill Cipher Algorithm," *J. Ilm. Mat. and Educators. Mat.*, Vol. 14, No. 1, p. 45, 2022, doi: 10.20884/1.JMP.2022.14.1.5727.

[6] N. B. Putra, B. C. Andika, A. D. P. Bagas, and M. Ridwan, "Implementation of the Vigenere Cipher Dalam," vol. 1, no. 1, pp. 42–50, 2023.

[7] N. D. Sari and D. Arius, "Modification of Hill Cipher Algorithm with Periodic Table of Chemical Elements Using Mobile Operator Number Codes in Indonesia," *J. Technol. Inf.*, Vol. 4 No. 2 pp. 202–207, 2020, doi: 10.36294/juri.v4I2.1339.

[8] Sukma Achriadi, Hardisal, Asmaidi, and M. Sulthan Hanafi, "Encryption and Description of RGB Values in Images Using the Hill Chiper Algorithm," *J. Inotera*, vol. 9, no. 1, pp. 48–52, 2024, doi: 10.31572/inotera.vol9.iss1.2024.id282.

[9] Noviyanti. P and Mira, "Analysis of Classical Cryptographic Algorithms of Caesar Cipher Viginere Cipher and Hill Cipher – Study Literature," *J. Inf. Technol.*, vol. 2, no. 1, pp. 23–30, 2022, doi: 10.46229/jifotech.v2i1.387.

[10] A. Queency and S. Sylviani, "Application of Vigenere Cipher and Hill Cipher Algorithm Modification Using Temperature Conversion," vol. 4, no. 1, 2023.

[11] R. Gusmana, Haryansyah, and Adimulya Dyas Wibisono, "Implementation of Hill Cipher Algorithm Using 2x2 Matrix Key in Securing Text Data," *Gener. J.*, vol. 7, no. 3, pp. 31–39, 2023, doi: 10.29407/gj.v7i3.21105.

[12] V. Saputra Ginting, "Application of Vigenere Cipher and Hill Cipher Algorithms Using Mass Units," *J. Technol. Inf.*, vol. 4, no. 2, pp. 241–246, 2020.

[13] H. Hersan Pratama, Rw. Fergy Pamungkas, and N. Rahmadika, "Evaluation of Vigenère Cipher Performance on Encrypted Digital Data," vol. 1, no. 1, pp. 32–41, 2023, [Online]. Available: https://jurnal.ittc.web.id/index.php/jct/

[14] D. Astuti and C. Sundari, "Implementation of Vigenere Cipher Algorithm for Encryption and Decryption in Drug Data Prescription at Mertoyudan 1 Health Center, Magelang Regency," *J. Tek. Inf. and Komput.*, vol. 5, no. 2, p. 341, 2022, doi: 10.37600/tekinkom.v5i2.534.

[15] C. A. Haris and D. Ariyus, "Combination and Modification of Vigenere Cipher and Hill Cipher Using

Hybrid Methods of Postal Code, Trigonometry, and Temperature Conversion as Message Security," *Inform. Mulawarman J. Ilm. Computational Science.*, vol. 15, no. 2, p. 90, 2020, doi: 10.30872/jim.v15i2.3746.

[16] M. Azmi and Z. Zulkarnaen, "Implementation of Caesar Cipher and Hill Cipher Combination Using Morse Cryptography Modification for Text-Based Message Security," 2021. doi: 10.35746/jtim.v3i1.124.