PARAMETER
JURNAL MATEMATIKA, STATISTIKA DAN TERAPANNYA

e-ISSN. 2829-6303
Vol. 05, No. 2, September 2026
Pages 319-332

Hill Cipher with Block Permutation Using a 97-Symbol Character Set: Entropy and Cryptanalytic Considerations

Diva Rizqie Aurellia[1], Yanuar Bhakti Wira Tama[2*], Winarni Winarni[3]

[123]Department of Mathematics, Institut Teknologi Kalimantan, Balikpapan, East Kalimantan 76127, Indonesia

E-mail Correspondence Author: *yanuar.bhakti@lecturer.itk.ac.id

Abstract

This study investigates a Hill-cipher implementation over a 97-symbol character set followed by a fixed block permutation. The character set consists of the 94 printable standard ASCII symbols excluding space, supplemented by ¥, €, and ±, and is mapped bijectively to the finite field F_{97}. Invertible key matrices of sizes 3×3, 4×4, and 5×5 are evaluated using Shannon entropy and character-frequency distributions. For the experimental text, preprocessing removes spaces and symbols outside the defined set, producing 1,302 symbols with plaintext entropy 4.4800 bits. A representative 4×4 experiment yields ciphertext entropy 6.5545 bits, close to the theoretical maximum $\log_2(97)$=6.5999 bits. Across three keys for each matrix size, the mean entropy values are 6.5209, 6.5443, and 6.5399 bits for 3×3, 4×4, and 5×5 matrices, respectively, showing no monotonic increase with matrix size. The block permutation changes symbol positions but preserves single-symbol frequencies and entropy. Moreover, because a fixed permutation matrix composed with a Hill key remains a linear transformation over F_{97}, the construction retains the known-plaintext vulnerability of Hill-type ciphers. Accordingly, the results demonstrate strong single-symbol statistical uniformity of the ciphertext, but should not be interpreted as evidence of modern cryptographic security.

Keywords: *Block permutation, finite field F_{97}, hill cipher, shannon entropy, 97-symbol character set.*

: https://doi.org/10.30598/parameterv4i1pp319-332

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution-ShareAlike 4.0 International License.

Copyright © 2026 The Author(s).
Research Ariticle ***Open Acces***
Email: jurnalparameter@gmail.com
Homepage: https://ojs3.unpatti.ac.id/index.php/parameter

Submitted: November 2025
Accepted: September 2026

1. INTRODUCTION

Along with the rapid development of the digital world today, concerns about the level of security of data stored and data transmitted digitally have also become an important issue. In addition, data and information exchange is something that is frequently carried out by individuals as well as groups. With the advancement of technology that facilitates data and information exchange, it has also become easier for such information to be exposed, manipulated, and misused. The negative impact of technological development makes security in information exchange and data storage as well as text protection, increasingly important. Text documents face integrity and security issues in the modern digital world [1]. Thus, in this context, text is not necessarily safe from unauthorized access, making confidentiality and security crucial.

One way to maintain the security and confidentiality of information is through cryptography, which is the field of study that examines data encryption techniques to preserve confidentiality and security. In cryptography, the original message (plaintext) is transformed into an encoded form (ciphertext) through a process called encryption, while the process of converting ciphertext back into plaintext is called decryption. Using cryptographic techniques, the message sent goes through an encryption process, so that it can only be read by a person who has the secret key [2]. Several well-known classical cryptographic algorithms include the Caesar Cipher, Vigenère Cipher, Affine Cipher, and Hill Cipher [3]. Classical cryptography hides information transforming plaintext into an unintelligible form [4]. There are many cryptographic applications besides those already mentioned, ranging from asymmetric cryptography for digital signatures [5] and key exchange [6], and so on, to symmetric cryptography such as in medical IoT [7], image processing [8], [9], developments based on the Hill Cipher [10], and hybrid schemes of them [11], [12], [13].

Several related studies have addressed text protection and classical cryptographic constructions [14], [15], [16], [17] while Hill Cipher studies have also extended the conventional 26-character alphabet to larger symbol sets containing 53, 94, or 95 symbols [18], [19], [20]. This study implements the Hill Cipher on a 97-symbol character set with the addition of a fixed block-permutation method. The permutation rearranges the positions of symbols within each block after the Hill transformation. The 97-symbol set consists of 94 printable standard ASCII characters excluding space, supplemented by ¥, €, and ±. The space character is excluded so that the symbol set has prime cardinality 97 and can be mapped bijectively to the finite field F_{97}. Because a fixed permutation changes only symbol positions, it does not change single-symbol frequencies or Shannon entropy.

This research is limited to the use of key matrices of sizes 3 × 3, 4 × 4, and 5 × 5, with the focus on examining how these variations affect the statistical characteristics of the resulting ciphertext. The evaluation uses character-frequency distributions and Shannon entropy, together with a direct comparison between plaintext and ciphertext. The 97 symbols are mapped to the finite field F_{97}; therefore, a key matrix A is valid when $\det(A) \neq 0$ in F_{97}, which guarantees that A is invertible. Related Hill-based schemes have combined linear transformations with permutation or scrambling operations [12], [13]. The contribution of the present study is the implementation and statistical evaluation of a Hill Cipher over the 97-symbol set followed by a fixed block permutation, rather than a claim of a fundamentally new secure cipher. The cryptanalytic discussion also considers the linearity of the combined transformation and the known-plaintext weakness that remains for fixed Hill-type mappings [21], [22].

2. METHOD

The proposed system operates on a finite alphabet of 97 symbols that is encoded as elements of the finite field F_{97}. Each plaintext block is first encoded as a vector, transformed by an invertible Hill key matrix, and then subjected to a fixed coordinate permutation. The experimental plaintext is the Indonesian-language passage shown in **Figure 1**; it is used solely as a reproducible test string for the statistical analysis. The procedure is described in the following subsections.

2.1 Character Set, Message Cleaning, and Padding

Let S denote the 97-symbol character set in **Table 1**. It contains the 94 printable standard ASCII characters from "!" through "~" (space excluded) together with the three supplemental symbols ¥, €, and ±. A bijection phi from S to F_{97} assigns the integer values 0,…,96 shown in the table. During preprocessing, spaces and any symbols not contained in S are removed, while punctuation marks that belong to S are retained. This rule resolves the distinction between valid punctuation and characters that are genuinely outside the defined alphabet. The space character is intentionally excluded so that the alphabet contains exactly 97 symbols, allowing a direct bijective representation over the prime field F_{97}. The three supplemental symbols ¥, €, and ± are included to increase the 94 non-space printable ASCII symbols to this prime cardinality.

Table 1. 97-Symbol Character Set and F_{97} Encoding

Value in F_{97}	Symbol	Value in F_{97}	Symbol	Value in F_{97}	Symbol
0	¥	33	A	66	b
1	!	34	B	67	c
2	"	35	C	68	d
3	#	36	D	69	e
4	$	37	E	70	f
5	%	38	F	71	g
6	&	39	G	72	h
7	'	40	H	73	i
8	(	41	I	74	j
9	)	42	J	75	k
10	*	43	K	76	l
11	+	44	L	77	m
12	,	45	M	78	n
13	-	46	N	79	o
14	.	47	O	80	p
15	/	48	P	81	q
16	0	49	Q	82	r
17	1	50	R	83	s
18	2	51	S	84	t
19	3	52	T	85	u
20	4	53	U	86	v
21	5	54	V	87	w
22	6	55	W	88	x
23	7	56	X	89	y
24	8	57	Y	90	z
25	9	58	Z	91	{
26	:	59	[	92	|
27	;	60	\	93	}
28	<	61	]	94	~

Value in F_{97}	Symbol	Value in F_{97}	Symbol	Value in F_{97}	Symbol
29	=	62	^	95	€
30	>	63	_	96	±
31	?	64	`		
32	@	65	a		

The original test passage contains 1,498 characters when spaces are counted. After the preprocessing rule above, 1,302 symbols remain. If the cleaned length is not divisible by the selected block size n, up to n−1 padding symbols from S are appended to complete the final block. The short illustrative example in Section 3.1 uses "_2" as two padding symbols; the padding is removed after successful decryption when the original message length is known.

2.2 Encryption and Decryption

Let a plaintext block be represented by the column vector p in F_{97}^n, and let A in $GL_n(F_{97})$ be the Hill key matrix. Since 97 is prime, F_{97} is a field; therefore, A is invertible if and only if $\det(A) \neq 0$ in F_{97}. The Hill encryption and decryption transformations are given in **Equation (1)** and **Equation (2)**, respectively.

$$\boldsymbol{C = E_A\,(P) = A \cdot P \bmod 97} \tag{1}$$

The corresponding Hill decryption is given by **Equation (2).**

$$\boldsymbol{P = D_A(C)\ = A^{-1} \cdot C \bmod 97} \tag{2}$$

The inverse A^{-1} is computed by Gauss–Jordan elimination with all row operations carried out in F_{97}. A related modular implementation of Gauss–Jordan elimination for cryptographic matrix inversion over $\mathbb{Z}/256\mathbb{Z}$ was reported by Tama and Mujahidin **[23]**. For the second stage, let $\boldsymbol{\pi} \in \boldsymbol{S}_n$ be a fixed permutation and let $\boldsymbol{P_\pi}$ denote its permutation matrix. The forward and inverse permutation maps are given in **Equation (3)** and **Equation (4)**.

$$e_\pi(\boldsymbol{x}) = P_\pi \boldsymbol{x}\ = \left(x_{\pi(1)}, x_{\pi(2)}, \dots, x_{\pi(m)}\right)^T \tag{3}$$

$$\mathbf{d}_{\boldsymbol{\pi}}(\boldsymbol{y}) = \mathbf{P}_{\boldsymbol{\pi}}^{-1}\boldsymbol{y} = \mathbf{P}_{\boldsymbol{\pi}}^{\boldsymbol{T}}\boldsymbol{y} = \left(\mathbf{y}_{\boldsymbol{\pi}^{-1}(1)}, \mathbf{y}_{\boldsymbol{\pi}^{-1}(2)}, \dots, \mathbf{y}_{\boldsymbol{\pi}^{-1}(m)}\right)^{\boldsymbol{T}} \tag{4}$$

The complete two-stage transformation can therefore be written as

$$\mathbf{z} = \boldsymbol{P_\pi A}\mathbf{p}\ (\mathbf{mod\ 97}), \qquad \mathbf{p} = \boldsymbol{A^{-1}P_\pi^{T}}\mathbf{z}\ (\mathbf{mod\ 97})$$

Because $\boldsymbol{P_\pi A}$ is an invertible matrix over F_{97}, the fixed Hill–permutation construction remains linear. The permutation stage changes only coordinate positions and therefore preserves the multiset of ciphertext symbols, their single-symbol frequencies, and their Shannon entropy.

2.3 Character Distribution and Shannon Entropy

Character-frequency distributions are compared for the cleaned plaintext and ciphertext, and Shannon entropy is used as a measure of single-symbol statistical uniformity **[24]**. For symbol $\boldsymbol{i}$, let $\boldsymbol{n}_i$ be its observed count in a text of length N and define $\boldsymbol{p}_i = \frac{\boldsymbol{n_i}}{\boldsymbol{N}}$. The Shannon entropy is given by **Equation (5)**; symbols with $\boldsymbol{p}_i = \mathbf{0}$ contribute zero to the sum.

$$H(X) = -\sum_{i=0}^{96} p_i \log_2 p_i, \qquad p_i = \frac{n_i}{N} \tag{5}$$

For a uniform distribution over 97 symbols, the maximum possible entropy is

$$H_{\max} = \log_2(97) \approx 6.5999 \text{ bits}$$

The normalized entropy $H/H_{\max}$ is used to indicate how close an empirical symbol distribution is to the uniform ideal. A value near $H_{\max}$ indicates a flat single-symbol distribution, but does not by itself establish resistance to known-plaintext, chosen-plaintext, or other structural attacks.

3 RESULTS AND DISCUSSION

The implementation is evaluated in three stages: a short worked example verifies encryption and decryption, a longer plaintext is used to examine character distributions and entropy, and the security scope of the fixed linear construction is discussed separately. All arithmetic in the Hill stage is performed modulo 97 using the encoding in **Table 1**.

3.1. Encryption

The following example illustrates the complete two-stage transformation and verifies that the original plaintext is recovered by the inverse operations. Suppose the Hill key matrix is.

$$K = \begin{bmatrix} 5 & 17 & 4 & 1 \\ 8 & 3 & 9 & 7 \\ 6 & 2 & 12 & 11 \\ 10 & 13 & 14 & 15 \end{bmatrix}$$

and the plaintext is "Matematika". Because the block size is 4, two padding symbols "_2" are appended, giving "Matematika_2". Each character is mapped to its F_{97} value according to **Table 1**.

The encoding of the padded plaintext is shown below.

M	a	t	e	m	a	t	i	k	a	_	2
45	65	84	69	77	65	84	73	75	65	63	18

Hence, the given plaintext is divided into three blocks as follows:

$$P_1 = \begin{bmatrix} 45 \\ 65 \\ 84 \\ 69 \end{bmatrix}, \; P_2 = \begin{bmatrix} 77 \\ 65 \\ 84 \\ 73 \end{bmatrix}, \; P_3 = \begin{bmatrix} 75 \\ 65 \\ 63 \\ 18 \end{bmatrix}$$

Next, the block is multiplied by the key matrix K. For example, the computation P_1 yields the ciphertext block C_1 as follows:

$$C_1 = \begin{bmatrix} 5 & 17 & 4 & 1 \\ 8 & 3 & 9 & 7 \\ 6 & 2 & 12 & 11 \\ 10 & 13 & 14 & 15 \end{bmatrix} \cdot \begin{bmatrix} 45 \\ 65 \\ 84 \\ 69 \end{bmatrix} mod\ 97 = \begin{bmatrix} (5 \times 45) + (17 \times 65) + (4 \times 84) + (1 \times 69) \\ (8 \times 45) + (3 \times 65) + (9 \times 84) + (7 \times 69) \\ (6 \times 45) + (2 \times 65) + (12 \times 84) + (11 \times 69) \\ (10 \times 45) + (13 \times 65) + (14 \times 84) + (15 \times 69) \end{bmatrix}$$

$$= \begin{bmatrix} 225 + 1105 + 336 + 69 \\ 360 + 195 + 756 + 483 \\ 270 + 130 + 1008 + 759 \\ 450 + 845 + 1176 + 1035 \end{bmatrix} mod\ 97 = \begin{bmatrix} 1735 \\ 1794 \\ 2167 \\ 3506 \end{bmatrix} mod\ 97 \equiv \begin{bmatrix} 86 \\ 48 \\ 33 \\ 14 \end{bmatrix} = \begin{bmatrix} \text{V} \\ \text{P} \\ \text{A} \\ . \end{bmatrix}$$

by applying the same procedure, the ciphertext resulting from P_2 and P_3 the Hill Cipher is obtained as follows:

$$C_1 = \begin{bmatrix} v \\ P \\ A \\ . \end{bmatrix}, C_2 = \begin{bmatrix} X \\ I \\ k \\ \& \end{bmatrix}, C_3 = \begin{bmatrix} \$ \\ A \\ o \\ ? \end{bmatrix}$$

or, equivalently, the final ciphertext is obtained "vPA.XIk&$Ao?".

Subsequently, applying the Permutation Cipher with key $\boldsymbol{K}_{\pi(x)} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

yields the following result:

$$C_1 = K_{\pi(x)} \cdot \begin{bmatrix} v \\ P \\ A \\ . \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 86 \\ 48 \\ 33 \\ 14 \end{bmatrix} = \begin{bmatrix} 0+0+0+14 \\ 0+48+0+0 \\ 86+0+0+0 \\ 0+0+33+0 \end{bmatrix} = \begin{bmatrix} 14 \\ 48 \\ 86 \\ 33 \end{bmatrix} = \begin{bmatrix} . \\ P \\ v \\ A \end{bmatrix}$$

$$C_2 = K_{\pi(x)} \cdot \begin{bmatrix} X \\ I \\ k \\ \& \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 56 \\ 41 \\ 75 \\ 6 \end{bmatrix} = \begin{bmatrix} 0+0+0+6 \\ 0+41+0+0 \\ 56+0+0+0 \\ 0+0+75+0 \end{bmatrix} = \begin{bmatrix} 6 \\ 41 \\ 56 \\ 75 \end{bmatrix} = \begin{bmatrix} \& \\ I \\ X \\ k \end{bmatrix}$$

$$C_3 = K_{\pi(x)} \cdot \begin{bmatrix} \$ \\ A \\ o \\ ? \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ 33 \\ 79 \\ 31 \end{bmatrix} = \begin{bmatrix} 0+0+0+31 \\ 0+33+0+0 \\ 4+0+0+0 \\ 0+0+79+0 \end{bmatrix} = \begin{bmatrix} 31 \\ 33 \\ 4 \\ 79 \end{bmatrix} = \begin{bmatrix} ? \\ A \\ \$ \\ o \end{bmatrix}$$

Finally, the last ciphertext is obtained ".PvA&IXk?A$o".

3.2. Decryption

In decryption, we attempt to recover the message that has been encrypted using the Hill Cipher and the Permutation Cipher. Since the encryption process first applies the Hill Cipher followed by the Permutation Cipher, the decryption process must apply the Permutation Cipher first, followed by the Hill Cipher. For the permutation matrix, its inverse can be obtained by transposing the matrix. Thus, the inverse key matrix for the permutation is obtained $\boldsymbol{K}_{\pi^{-1}(x)} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$. The first step of decryption using the inverse permutations as follows:

$$C_1 = K_{\pi^{-1}(x)} \cdot \begin{bmatrix} . \\ P \\ v \\ A \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 14 \\ 48 \\ 86 \\ 33 \end{bmatrix} = \begin{bmatrix} 0+0+86+0 \\ 0+48+0+0 \\ 0+0+0+33 \\ 14+0+0+0 \end{bmatrix} = \begin{bmatrix} 86 \\ 48 \\ 33 \\ 14 \end{bmatrix} = \begin{bmatrix} v \\ P \\ A \\ . \end{bmatrix}$$

$$C_2 = K_{\pi^{-1}(x)} \cdot \begin{bmatrix} \& \\ I \\ X \\ k \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 6 \\ 41 \\ 56 \\ 75 \end{bmatrix} = \begin{bmatrix} 0+0+56+0 \\ 0+41+0+0 \\ 0+0+0+75 \\ 6+0+0+0 \end{bmatrix} = \begin{bmatrix} 56 \\ 41 \\ 75 \\ 6 \end{bmatrix} = \begin{bmatrix} X \\ I \\ k \\ \& \end{bmatrix}$$

$$C_3 = K_{\pi^{-1}(x)} \cdot \begin{bmatrix} ? \\ A \\ \$ \\ o \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 31 \\ 33 \\ 4 \\ 79 \end{bmatrix} = \begin{bmatrix} 0+0+4+0 \\ 0+33+0+0 \\ 0+0+0+79 \\ 31+0+0+0 \end{bmatrix} = \begin{bmatrix} 4 \\ 33 \\ 79 \\ 31 \end{bmatrix} = \begin{bmatrix} \$ \\ A \\ o \\ ? \end{bmatrix}$$

Next, the Hill key matrix is inverted over F_{97} using Gauss–Jordan elimination. All row operations below are performed modulo 97. Starting from the augmented matrix $[K \mid I_4]$,

$$\left[\begin{array}{cccc|cccc} 5 & 17 & 4 & 1 & 1 & 0 & 0 & 0 \\ 8 & 3 & 9 & 7 & 0 & 1 & 0 & 0 \\ 6 & 2 & 12 & 11 & 0 & 0 & 1 & 0 \\ 10 & 13 & 14 & 15 & 0 & 0 & 0 & 1 \end{array}\right].$$

Because $5^{-1} \equiv 39 \pmod{97}$, normalize the first pivot using $R_1 \leftarrow 39R_1$:

$$\left[\begin{array}{cccc|cccc} 1 & 81 & 59 & 39 & 39 & 0 & 0 & 0 \\ 8 & 3 & 9 & 7 & 0 & 1 & 0 & 0 \\ 6 & 2 & 12 & 11 & 0 & 0 & 1 & 0 \\ 10 & 13 & 14 & 15 & 0 & 0 & 0 & 1 \end{array}\right].$$

Apply $R_2 \leftarrow R_2 - 8R_1$, $R_3 \leftarrow R_3 - 6R_1$, and $R_4 \leftarrow R_4 - 10R_1$:

$$\left[\begin{array}{cccc|cccc} 1 & 81 & 59 & 39 & 39 & 0 & 0 & 0 \\ 0 & 34 & 22 & 83 & 76 & 1 & 0 & 0 \\ 0 & 1 & 46 & 68 & 57 & 0 & 1 & 0 \\ 0 & 76 & 6 & 13 & 95 & 0 & 0 & 1 \end{array}\right].$$

Since $34^{-1} \equiv 20 \pmod{97}$, set $R_2 \leftarrow 20R_2$, then apply $R_1 \leftarrow R_1 - 81R_2$, $R_3 \leftarrow R_3 - R_2$, and $R_4 \leftarrow R_4 - 76R_2$:

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 18 & 21 & 12 & 29 & 0 & 0 \\ 0 & 1 & 52 & 11 & 65 & 20 & 0 & 0 \\ 0 & 0 & 91 & 57 & 89 & 77 & 1 & 0 \\ 0 & 0 & 31 & 50 & 5 & 32 & 0 & 1 \end{array}\right].$$

Because $91^{-1} \equiv 16 \pmod{97}$, set $R_3 \leftarrow 16R_3$, then apply $R_1 \leftarrow R_1 - 18R_3$, $R_2 \leftarrow R_2 - 52R_3$, and $R_4 \leftarrow R_4 - 31R_3$:

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 95 & 85 & 66 & 3 & 0 \\ 0 & 1 & 0 & 20 & 28 & 73 & 41 & 0 \\ 0 & 0 & 1 & 39 & 66 & 68 & 16 & 0 \\ 0 & 0 & 0 & 5 & 93 & 58 & 86 & 1 \end{array}\right].$$

Finally, use $5^{-1} \equiv 39 \pmod{97}$ to set $R_4 \leftarrow 39R_4$, followed by $R_1 \leftarrow R_1 - 95R_4$, $R_2 \leftarrow R_2 - 20R_4$, and $R_3 \leftarrow R_3 - 39R_4$:

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 64 & 31 & 18 & 78 \\ 0 & 1 & 0 & 0 & 44 & 35 & 85 & 93 \\ 0 & 0 & 1 & 0 & 39 & 23 & 63 & 31 \\ 0 & 0 & 0 & 1 & 38 & 31 & 56 & 39 \end{array}\right].$$

Therefore,

$$K^{-1} = \begin{bmatrix} 64 & 31 & 18 & 78 \\ 44 & 35 & 85 & 93 \\ 39 & 23 & 63 & 31 \\ 38 & 31 & 56 & 39 \end{bmatrix} \pmod{97}.$$

Finally, applying $p_i = K^{-1}c_i \pmod{97}$ gives:

$$\mathbf{p}_1 = K^{-1}\mathbf{c}_1 \pmod{97} = (45,65,84,69)^{\mathsf{T}}$$

$$\mathbf{p}_2 = K^{-1}\mathbf{c}_2 \pmod{97} = (77,65,84,73)^{\mathsf{T}}$$

$$\mathbf{p}_3 = K^{-1}\mathbf{c}_3 \pmod{97} = (75,65,63,18)^{\mathsf{T}}$$

The recovered vectors map to “Mate”, “mati”, and “ka_2”, respectively. Combining them gives “Matematika_2”. Removing the two known padding symbols returns the original plaintext “Matematika”, confirming the correctness of the encryption–decryption implementation.

3.3. Cryptosystem Implementation and Entropy Analysis

For the longer experiment, the Hill and permutation stages are applied to the passage shown in **Figure 1** using several invertible key matrices. The original passage contains 1,498 characters including 196 spaces. Applying the preprocessing rule removes the spaces and leaves 1,302 symbols, as shown in **Figure 2**. For the 4×4 experiment, two padding symbols are required, so the encrypted sequence contains 1,304 symbols.

```
Negara menyepakati gencatan senjata tarif selama 90 hari, AS menurunkan tarif dari 145%
menjadi 30%, dan Tiongkok dari 125% menjadi 10% sebagai upaya meredakan ketegangan perang
dagang yang telah membebani pertumbuhan global (White House, 2025). Meskipun demikian,
lonjakan aktivitas impor oleh perusahaan-perusahaan AS sebelum berakhirnya masa gencatan
tarif menyebabkan biaya pengiriman kontainer dari Tiongkok ke AS naik drastis, bahkan
diperkirakan mencapai $8.500 per unit pada pertengahan Juni (New York Post, 2025). Di sisi
lain, ekonomi Tiongkok menunjukkan tanda-tanda perlambatan, dengan pertumbuhan produksi
industri, konsumsi, dan investasi yang melemah akibat tekanan tarif dan sektor properti
yang masih rapuh. Target pertumbuhan 5% yang ditetapkan Beijing kini dianggap sulit tercapai
tanpa kebijakan stimulus tambahan (Wall Street Journal, 2025). Upaya relokasi produksi
dari Tiongkok ke negara lain oleh perusahaan AS juga menghadapi tantangan besar, seperti
biaya tinggi, kurangnya infrastruktur, dan kualitas produksi yang tidak konsisten. Selain
itu, kebijakan tarif yang tidak menentu dari Presiden Trump, termasuk ancaman tarif 25%
terhadap iPhone buatan luar negeri memicu ketidakpastian bisnis yang semakin luas (Time,
2025). Meskipun indeks saham utama AS sempat menguat setelah kesepakatan pengurangan tarif,
risiko terhadap stabilitas ekonomi global tetap besar seiring meningkatnya kekhawatiran
investor terhadap kebijakan perdagangan yang agresif (Investors.com, 2025).
```

Figure 1. Plaintext

Figure 2 shows the cleaned plaintext after the 196 spaces have been removed. All remaining punctuation belongs to the 97-symbol set in **Table 1**; no valid punctuation is discarded. The cleaned plaintext therefore has length 1,302 and uses 52 distinct symbols.

```
Negaramenyepakatigencatansenjatatarifselama90hari,ASmenurunkantarifdari145%menjadi30%,dan
Tiongkokdari125%menjadi10%sebagaiupayameredakanketeganganperangdagangyangtelahmembebanipe
rtumbuhanglobal(WhiteHouse,2025).Meskipundemikian,lonjakanaktivitasimporolehperusahaan-
perusahaanASsebelumberakhirnyamasagencatantarifmenyebabkanbiayapengirimankontainerdariTio
ngkokkeASnaikdrastis,bahkandiperkirakanmencapai$8.500perunitpadapertengahanJuni(NewYorkPo
st,2025).Disisilain,ekonomiTiongkokmenunjukkantanda-
tandaperlambatan,denganpertumbuhanproduksiindustri,konsumsi,daninvestasiyangmelemahakibat
tekanantarifdansektorpropertiyangmasihrapuh.Targetpertumbuhan5%yangditetapkanBeijingkinid
ianggapsulittercapaitanpakebijakanstimulustambahan(WallStreetJournal,2025).Upayarelokasip
roduksidariTiongkokkenegaralainolehperusahaanASjugamenghadapitantanganbesar,sepertibiayat
inggi,kurangnyainfrastruktur,dankualitasproduksiyangtidakkonsisten.Selainitu,kebijakantar
ifyangtidakmenentudariPresidenTrump,termasukancamantarif25%terhadapiPhonebuatanluarnegeri
memicuketidakpastianbisnisyangsemakinluas(Time,2025).MeskipunindekssahamutamaASsempatmeng
uatsetelahkesepakatanpengurangantarif,risikoterhadapstabilitasekonomiglobaltetapbesarseir
ingmeningkatnyakekhawatiraninvestorterhadapkebijakanperdaganganyangagresif(Investors.com,
2025).
```

Figure 2. Plaintext After Cleaning

Applying the 4×4 Hill key matrix and the fixed permutation matrix shown below produces the ciphertext blocks displayed in **Figure 3**.

```
4I&< wjQ| C:<= k-$, 8Cs& "8€m #y52 ZbAR o}sP 631% XOl: Po~C -]il sN/Y $€+d 9F/@ I|[s waxs
?"eQ `G|= lu8! lAq± Rv}j <SDZ 7E>x gNd_ p;Gs c[jK BHhL vfT? ;+N, d]Iy T4NX AL€3 );-k 6J¥:
1B#D -+WG wdP" XanL GQ^B Rb'r 1rO] }Bj& G$M? __Ni >P%D St/¥ oq@€ x?hz pg*2 @-\h V?dB OT|B
D&{H 9FqW -tPB <Dh, AL€3 h7e0 qYCp "7'p t~O< ?N2€ lM5u [bYX t<Ed n1BG ±i=k {vdU O(1N u"U{
*LAZ kJ)9 (p>2 !T`< 7en\ fbL% .z34 S/OU 3+/x €7P- )'0g v~{} Jtz3 @u1~ (*3^ I^:: prVB ¥%Xh
'*8} OR{p T4x- M3OY 7/g6 (@k& LRk5 I&E$ rm0E _io5 E/Zc ObD± h?7J gRLE ":x{ F2Zg 7!cN 8%c¥
R3kx 2]Xc ±oFG ,OAA €8,- 3;pj rHuC SJ^E Wuhm d€`R zlKK }l*€ ^\w- €L<c cK6h vb=Y kHP" p-E(
V.7Z $U&O *@UP 1B#D n%8v K+{^ 5X7o 2_B& IEN( <`7c %¥k1 KltA ,q:Y 1Qqi ±To( ,sp, y.h> ¥*R0
#%I@ /Kuh e:2l hAP¥ fbL% r[~o Q0€Q UpK6 G$M? J7rw 9Jcs URJ& y3-3 #i2v cf<Y n%8v K+{^ ~~pA
:,_y (>3g O?-= /AXr flV_ |']& SZl7 s~[Y mW&4 rjhV _io5 ;-~6 UF?L 9+y? I$@T Mt1d `8*3 V.7Z
jBG] (j.* FsK" v/p_ N~^& M±zR €8,- =&B@ ltBG sviH n:€= 2_B& '94d *Xd8 <SDZ TW`n q'Sc !x*V
xbe: g{Il n1BG ±i=k Q8qI k±P$ "]`t a68| 9F/@ <1|¥ ~.Y( oHMe G$M? S;!} HR3= OB.) +*+7 ±9iM
ifmO @NRI jx€R #Lgh :dvX A;`g Hu~f _ii¥ |NA/ I{oF WM-\ s@lH CKOK X8<| by,. D,+x eQJm jW~5
€w:C -ADn c}b~ -VlL -9uY Vgdy Forr {fo< r[5i b*=O 6PZ_ 6i1c b<Lu `;Kw fbL% `cbE Z7WU >f|V
.'/& >R=; `nfE 9Y}D 4Wc: CDwe FylD ~h±I mqMB x:bG 7]L9 oc/W Bpn7 RGQH \0K) I\j" a¥6` 0%cr
@7O~ el9R phto c?Uy 6i>e M;¥Q *~8= w/D< (*}h 41^u }~Yg :$=o ¥/)] 9{;q |9j¥ p=#} -+WG 9F/@
EZ#3 ±,3Q GOv+ z>6¥ ZM`F `#eq ^d"¥ ~Jj] mV>€ St/¥ @PB$ {`n\ L#x{ p3O" i^BA %#j& \5S] <|lE
f#&5 _(z1 1Qqi ±To( pm\z z>6¥ kk1y 9+y? 4d=' 6hG~ 6J¥: f!C% lEuy t$P~ LHQ: ±To( jJ!; €`ZM
0%cr QZ:<
```

Figure 3. Ciphertext

Figure 4 presents a grouped bar plot comparing the relative frequency distribution of each character in the cleaned plaintext and the representative ciphertext. The x-axis displays the actual symbols according to the numerical mapping (0–96) in **Table 1**. The plaintext exhibits a noticeably uneven distribution, with several symbols occurring much more frequently than others. In contrast, the ciphertext shows a flatter distribution across the character set. For a character set containing 97 symbols, the theoretical uniform probability of each symbol is 1/97≈0.0103. Although the ciphertext frequencies do not exactly attain this value for every symbol, their distribution is considerably more balanced than that of the plaintext. This observation indicates that the encryption process reduces the visible single-symbol frequency structure of the original message and therefore reduces the information available to simple character-frequency analysis.

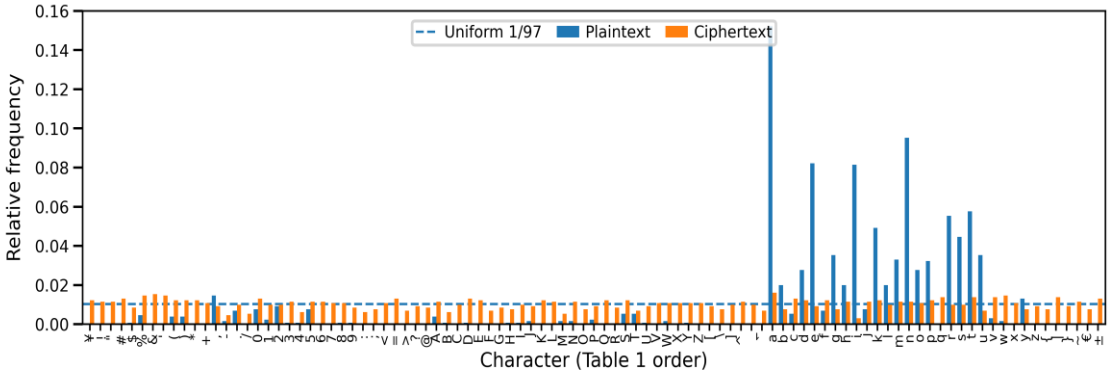


Figure 4. Character frequencies in plaintext and ciphertext

The difference between the plaintext and ciphertext distributions can be further evaluated using Shannon entropy. For a character set containing 97 symbols, the maximum possible entropy under a uniform distribution is $H_{max} = log_2(97) \approx 6.5999$ bits. For the representative ciphertext shown in **Figure 4**, the entropy obtained using **Equation (5)** is 6.5545 bits, compared with 4.4800 bits for the cleaned plaintext. The ciphertext value is close to the theoretical maximum, which is consistent with the flatter relative-frequency distribution observed in **Figure 4**. The entropy analysis was subsequently extended to Hill Cipher key matrices of sizes 3×3, 4×4, and 5×5, as presented in **Table 2**. The permutation stage is not evaluated separately using Shannon entropy because a permutation changes only the positions of the ciphertext symbols and

does not alter their frequency distribution. Consequently, for a fixed Hill Cipher output, applying the permutation preserves the Shannon entropy. Therefore, the entropy values reported in this study primarily characterize the statistical distribution generated by the Hill Cipher transformation, whereas the permutation layer provides positional rearrangement.

Table 2. Ciphertext Entropy for Nine Invertible Key Matrices

No.	Matrix size	Key matrix	Entropy (bits)
1	3×3	$\begin{bmatrix}17 & 22 & 11\\ 8 & 3 & 5\\ 14 & 9 & 7\end{bmatrix}$	6.5074
2	3×3	$\begin{bmatrix}12 & 45 & 7\\ 23 & 56 & 78\\ 34 & 90 & 11\end{bmatrix}$	6.5306
3	3×3	$\begin{bmatrix}42 & 15 & 61\\ 7 & 26 & 89\\ 83 & 19 & 17\end{bmatrix}$	6.5246
4	4×4	$\begin{bmatrix}5 & 17 & 4 & 1\\ 8 & 3 & 9 & 7\\ 6 & 2 & 12 & 11\\ 10 & 13 & 14 & 15\end{bmatrix}$	6.5545
5	4×4	$\begin{bmatrix}21 & 15 & 33 & 76\\ 40 & 67 & 55 & 80\\ 19 & 45 & 11 & 72\\ 37 & 28 & 84 & 65\end{bmatrix}$	6.5450
6	4×4	$\begin{bmatrix}17 & 31 & 42 & 25\\ 36 & 18 & 21 & 8\\ 58 & 65 & 41 & 12\\ 49 & 72 & 15 & 29\end{bmatrix}$	6.5334
7	5×5	$\begin{bmatrix}5 & 17 & 4 & 1 & 9\\ 8 & 3 & 9 & 7 & 6\\ 6 & 2 & 12 & 11 & 3\\ 10 & 13 & 14 & 15 & 5\\ 7 & 8 & 6 & 9 & 2\end{bmatrix}$	6.5225
8	5×5	$\begin{bmatrix}11 & 3 & 7 & 2 & 14\\ 6 & 5 & 9 & 10 & 1\\ 8 & 13 & 4 & 15 & 12\\ 2 & 6 & 11 & 8 & 3\\ 7 & 9 & 10 & 5 & 13\end{bmatrix}$	6.5485
9	5×5	$\begin{bmatrix}35 & 20 & 11 & 75 & 23\\ 54 & 44 & 25 & 67 & 80\\ 64 & 27 & 62 & 88 & 92\\ 28 & 37 & 87 & 90 & 34\\ 46 & 78 & 65 & 54 & 29\end{bmatrix}$	6.5486

The entropy results do not show a monotonic relationship between matrix dimension and single-symbol entropy. For the three 3×3 keys, the mean entropy is 6.5209 bits with sample standard deviation 0.0120; for the 4×4 keys, 6.5443±0.0106 bits; and for the 5×5 keys, 6.5399±0.0150 bits. These means correspond to 98.80%, 99.16%, and 99.09% of Hmax, respectively. Thus, the 4×4 group has the highest mean in this small experiment,

but the differences among the three dimensions are modest and do not support the claim that a larger matrix automatically produces higher entropy.

Using 97 symbols provides a convenient algebraic setting because the encoding is over the prime field F_{97}. This guarantees that every matrix with nonzero determinant has an inverse and avoids the extra coprimality complications that occur for composite moduli such as 94 or 95. This is an implementation advantage rather than, by itself, a proof of stronger cryptographic security. Compared with previous 53-, 94-, and 95-symbol Hill implementations **[18], [19], [20]**, the present alphabet raises the theoretical single-symbol entropy ceiling to $log_2(97) \approx 6.5999$ bits, and the measured ciphertext entropies approach that ceiling. The result should therefore be interpreted as improved statistical use of the available symbol space, not as elimination of the structural weaknesses of Hill encryption. This study remains closely connected to previous ASCII-based and hybrid Hill-cipher research. Earlier implementations have used expanded symbol sets containing 53, 94, or 95 characters **[18], [19], [20]**, while other Hill-based schemes incorporate permutation, scrambling, or chaotic transformations **[12], [13], [14]**. In the present system, using 97 symbols raises the theoretical single-symbol entropy ceiling to $log_2(97) = 6.5999$ bits and, because 97 is prime, places the matrix operations in the finite field F_{97}. This simplifies the criterion for key invertibility compared with composite moduli such as 94 or 95. However, these algebraic conveniences should not be interpreted as proof of stronger cryptographic security. Likewise, the fixed permutation layer rearranges symbol positions but does not alter their frequencies or Shannon entropy, and Section 3.4 shows that the combined transformation remains linear. Thus, relative to previous work, the contribution is best understood as a 97-symbol finite-field implementation with a direct plaintext–ciphertext statistical comparison and an explicit discussion of cryptanalytic limitations.

3.4. Security Scope and Limitations

Let P_π denote the fixed permutation matrix and let $A \in GL_n(F_{97})$ be the Hill key matrix. For a plaintext block p, the complete two-stage transformation can be expressed using the effective matrix M, as shown in **Equation (6)**.

$$\mathbf{z} = P_\pi A\mathbf{p} = M\mathbf{p}, \quad M = P_\pi A \in GL_n(\mathbb{F}_{97}) \tag{6}$$

Thus, the Hill–permutation construction is algebraically equivalent to a single invertible linear transformation over F_{97}. Suppose an attacker obtains n linearly independent plaintext blocks $p_1, \dots, p_n$ and their corresponding ciphertext blocks $z_1, \dots, z_n$. Define $X = [p_1 \cdots p_n]$ and $Z = [z_1 \cdots z_n]$. Since X is invertible, the effective matrix can be recovered as.

$$M = ZX^{-1}, \quad det(X) \neq 0 \tag{7}$$

This is the classical known-plaintext weakness of Hill-type ciphers **[21]**. A fixed coordinate permutation therefore does not remove this vulnerability; it only changes the visible order of symbols within each block.

For reference, the nominal Hill-key space for block size n is the general linear group $GL_n(F_{97})$, whose cardinality is given in **Equation (8)**.

$$|GL_n(\mathbb{F}_{97})| = (97^n - 1)(97^n - 97)\cdots(97^n - 97^{n-1}) \tag{8}$$

For $n = 3$, 4, and 5, the base-2 logarithm of this cardinality is approximately 59.38, 105.58, and 164.98 bits, respectively. These values are nominal key-space sizes, not equivalent attack complexities, because recovery through **Equation (7)** can be much cheaper when suitable plaintext–ciphertext pairs are available. Moreover, treating the permutation as a separate fixed key does not enlarge the set of distinct effective linear maps beyond $GL_n(F_{97})$, since $P_\pi A$ is itself an element of that group. Cryptanalytic studies of Hill and modified Hill constructions therefore motivate evaluating structural attacks in addition to entropy **[8], [21], [22]**. A practical limitation of the present implementation is the exclusion of the space character. Consequently, word boundaries are removed during preprocessing, which may reduce readability and practical usability after decryption unless the original spacing information is preserved or reconstructed separately. Future implementations may employ an alternative 97-symbol mapping or an auxiliary mechanism to preserve spaces.

4 CONCLUSION

This study implemented a Hill Cipher over a 97-symbol character set mapped bijectively to F_{97} and followed it with a fixed block permutation. For the experimental passage, preprocessing produced 1,302 symbols with plaintext entropy 4.4800 bits, while a representative 4×4 ciphertext reached 6.5545 bits compared with the ideal 6.5999 bits. Across three keys for each dimension, the mean ciphertext entropies were 6.5209, 6.5443, and 6.5399 bits for 3×3, 4×4, and 5×5 matrices, so the experiment does not show a monotonic entropy increase with matrix size. The use of the prime modulus 97 gives a clean finite-field setting in which every key matrix with nonzero determinant is invertible, but this algebraic convenience does not by itself imply stronger security. The fixed permutation preserves single-symbol frequencies and entropy, and its composition with the Hill matrix remains linear; consequently, the construction retains the known-plaintext vulnerability of Hill-type ciphers. The results therefore support the conclusion that the scheme produces ciphertext with high single-symbol statistical uniformity, not that it achieves modern cryptographic security. Future work should introduce genuinely nonlinear or key-dependent transformations and evaluate known- and chosen-plaintext attacks, key sensitivity, avalanche behavior, and other security metrics beyond Shannon entropy.

Acknowledgments

The authors would like to express their sincere gratitude to LPPM Institut Teknologi Kalimantan (ITK) for supporting this research. The authors also thank the Department of Mathematics, Institut Teknologi Kalimantan, for academic and technical assistance during the completion of this study.

Funding Information

This research was funded by LPPM Institut Teknologi Kalimantan.

Author Contributions Statement

First Author: Data curation, software, investigation, and writing–original draft.
Second Author: Conceptualization, methodology, supervision, formal analysis, and validation.
Third Author: Writing–review & editing and validation.
All authors discussed the results and contributed to the final manuscript.

Conflict of Interest Statement

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Informed Consent

Not applicable, as this study does not involve human participants, personal data, or identifiable information.

Ethical Approval

Not applicable, as this research does not involve experiments with humans or animals.

Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] U. Khadam, M. M. Iqbal, M. Alruily, M. A. Al Ghamdi, M. Ramzan, And S. H. Almotiri, "Text Data Security And Privacy In The Internet Of Things: Threats, Challenges, And Future Directions," *Wirel. Commun. Mob. Comput.*, Vol. 2020, Pp. 1–15, Feb. 2020, Doi: 10.1155/2020/7105625.

[2] Y. S. Santoso, "Message Security Using A Combination Of Hill Cipher And Rsa Algorithms," *Jurnal Matematika Dan Ilmu Pengetahuan Alam Lldikti Wilayah 1 (Jumpa)*, Vol. 1, No. 1, Pp. 20–28, Mar. 2021, Doi: 10.54076/Jumpa.V1i1.38.

[3] L. S. Hill, "Cryptography In An Algebraic Alphabet," *The American Mathematical Monthly*, Vol. 36, No. 6, P. 306, Jun. 1929, Doi: 10.2307/2298294.

[4] S. Subramani, S. M, K. A, And S. K. Svn, "Review Of Security Methods Based On Classical Cryptography And Quantum Cryptography," *Cybern. Syst.*, Vol. 56, No. 3, Pp. 302–320, Apr. 2025, Doi: 10.1080/01969722.2023.2166261.

[5] Y. B. W. Tama, A. Adam, And A. P. Pratama, "Algorithm Design Of Curve25519 In Elliptic Curve Digital Signature," 2025, P. 040005. Doi: 10.1063/5.0262241.

[6] I. Muchtadi-Alamsyah And Y. Bhakti Wira Tama, "Implementation Of Elliptic Curve25519 In Cryptography," In *Theorizing Stem Education In The 21st Century*, Intechopen, 2020. Doi: 10.5772/Intechopen.88614.

[7] J. Jin, M. Wu, A. Ouyang, K. Li, And C. Chen, "A Novel Dynamic Hill Cipher And Its Applications On Medical Iot," *Ieee Internet Things J.*, Vol. 12, No. 10, Pp. 14297–14308, May 2025, Doi: 10.1109/Jiot.2025.3525623.

[8] H. Wen, Y. Lin, L. Yang, And R. Chen, "Cryptanalysis Of An Image Encryption Scheme Using Variant Hill Cipher And Chaos," *Expert Syst. Appl.*, Vol. 250, P. 123748, Sep. 2024, Doi: 10.1016/J.Eswa.2024.123748.

[9] D. Ranti, Achmad Fauzi, And M. P. U. Sitompul, "Digital Image Security Analysis Using Hill Cipher And Aes Algorithm," *Journal Of Artificial Intelligence And Engineering Applications (Jaiea)*, Vol. 4, No. 1, Pp. 487–496, Oct. 2024, Doi: 10.59934/Jaiea.V4i1.665.

[10] Z. Qowi And N. Hudallah, "Combining Caesar Cipher And Hill Cipher In The Generating Encryption Key On The Vigenere Cipher Algorithm," *J. Phys. Conf. Ser.*, Vol. 1918, No. 4, P. 042009, Jun. 2021, Doi: 10.1088/1742-6596/1918/4/042009.

[11] S. Arifin, D. Wijonarko, M. M. Manurung, Roni, P. W. Prasetyo, And F. S. Pramudya, "Strengthening Image Security With Unimodular Hill Cipher And Advanced Encryption Standard," *Journal Of Computer Science*, Vol. 21, No. 5, Pp. 1071–1082, May 2025, Doi: 10.3844/Jcssp.2025.1071.1082.

[12] Y. Xi, Y. Ning, J. Jin, And F. Yu, "A Dynamic Hill Cipher With Arnold Scrambling Technique For Medical Images Encryption," *Mathematics*, Vol. 12, No. 24, P. 3948, Dec. 2024, Doi: 10.3390/Math12243948.

[13] D. Khalaf, K. Hussain, And M. Darwish, "Enhanced Hill Cipher Encryption Using Chaotic Logistic Maps For Improved Security And Key Randomness," *Jes. Journal Of Engineering Sciences*, Vol. 53, No. 5, Pp. 170–195, Sep. 2025, Doi: 10.21608/Jesaun.2025.434995.

[14] S. Lukmaini, Y. B. W. Tama, And K. Nugraheni, "Penerapan Algoritma Hill Cipher Dan Permutasi Pada Sistem Kriptografi Polyalphabetic," *Epsilon: Jurnal Matematika Murni Dan*

Terapan (Epsilon: Journal Of Pure And Applied Mathematics), vol. 18, no. 2, p. 149, Nov. 2024, doi: 10.20527/epsilon.v18i2.12845.

[15] Y. B. W. Tama and M. F. Fahmi, "Sistem Kriptografi Klasik Dengan Memanfaatkan Orde Dari Grup Titik Pada Kurva Eliptik Bentuk Montgomery," *Euler : Jurnal Ilmiah Matematika, Sains dan Teknologi*, vol. 11, no. 2, pp. 361–371, Dec. 2023, doi: 10.37905/euler.v11i2.23009.

[16] R. Rasudin, Z. Zulfan, and P. Rizki, "Analisis Perbandingan Keamanan Kriptografi Klasik Pada Algoritma Secure Hill Cipher Berbasis Kode Ascii Dan Monoalphabetic," *Jurnal Teknologi Terapan and Sains 4.0*, vol. 3, no. 1, p. 729, Mar. 2022, doi: 10.29103/tts.v3i1.9411.

[17] M. N. Sutoyo, Q. Qammaddin, R. Rahayu, and N. K. R. Kariani, "Pengamanan Data Berbasis Hill Cipher dengan Operasi Modulo pada Karakter ASCII," *Techno.Com*, vol. 23, no. 4, pp. 786–795, Nov. 2024, doi: 10.62411/tc.v23i4.11523.

[18] F. D. T. Amijaya, S. Syaripuddin, Q. Q. A'yun, Y. N. Nasution, W. Wasono, and Moh. N. Huda, "Hill Cipher algorithm using two keywords and 94 ASCII characters," 2022, p. 050006. doi: 10.1063/5.0111696.

[19] N. Bahtiar, A. P. Widodo, and N. P. Puspita, "Key Matrix Generation Using Random Functions in Hill Cipher Modulo 95 Cryptography," *Integra: Journal of Integrated Mathematics and Computer Science*, vol. 2, no. 1, pp. 1–6, Mar. 2025, doi: 10.26554/integrajimcs.20252111.

[20] M. As Saidah, A. Saputra, and Z. Zulkipli, "Enhanced Data Security Using 5x5 Hill Cipher with Modular 53," *Jurnal Bangkit Indonesia*, vol. 13, no. 2, pp. 1–6, Oct. 2024, doi: 10.52771/bangkitindonesia.v13i2.323.

[21] C. Li, D. Zhang, and G. Chen, "Cryptanalysis of an image encryption scheme based on the Hill cipher," *Journal of Zhejiang University-SCIENCE A*, vol. 9, no. 8, pp. 1118–1123, Aug. 2008, doi: 10.1631/jzus.A0720102.

[22] S. Khazaei and S. Ahmadi, "Ciphertext-only attack on d×d Hill in O(d13)," *Inf. Process. Lett.*, vol. 118, pp. 25–29, Feb. 2017, doi: 10.1016/j.ipl.2016.09.006.

[23] Y. B. W. Tama and S. Mujahidin, "Grayscale image cryptosystem using sub-matrix multiplications and Gauss Jordan elimination in $\mathbb{Z}/256\mathbb{Z}$," 2026, p. 020001. doi: 10.1063/5.0308775.

[24] Y. B. W. Tama and S. Mujahidin, "Implementation of the Elliptic Curve Cryptography Method in Digital Image Security in Medical Images," *SPECTA Journal of Technology*, vol. 8, no. 3, pp. 233–241, Dec. 2024, doi: 10.35718/specta.v8i3.1253.