Enhanced Data Security Using 5x5 Hill Cipher with Modular 53

Muthiah As Saidah[1], Aggry Saputra[2], Zulkipli[3]

[1] Program Studi Sistem Informasi, Sekolah Tinggi Teknologi Indonesia Tanjung Pinang

[2,3] Program Studi Teknik Informatika, Sekolah Tinggi Teknologi Indonesia Tanjung Pinang
Pompa Air Street No. 28, Tanjungpinang, Riau Islands, Indonesia

[1]muthiahassaidah40@gmail.com (penulis korespondensi)

[2]aggrysaputra@gmail.com

[3]zulkipli@sttindonesia.ac.id

Abstract—**This research presents an optimized approach to the Hill Cipher encryption and decryption algorithm using a 5x5 matrix and modular 53 arithmetic. The traditional Hill Cipher, a well-known symmetric key algorithm, typically utilizes smaller matrices and modular arithmetic, which may not provide sufficient security for contemporary applications. By expanding the key matrix to a 5x5 structure and adopting a larger modulus of 53, the complexity and security of the cipher are significantly enhanced. The study details the methodology for constructing and implementing the 5x5 key matrix, as well as the processes for encryption and decryption under the modular 53 system. The computational efficiency and security improvements achieved through this optimization are analyzed. Comparative assessments with the conventional Hill Cipher demonstrate that the enhanced approach offers superior resistance against cryptographic attacks while maintaining manageable computational requirements. The results of this research indicate that the proposed optimized Hill Cipher can serve as a robust encryption method suitable for securing sensitive data in various modern applications. This study contributes to the field of cryptography by providing a more secure and efficient variant of the classical Hill Cipher algorithm.**

Keywords—Hill Cipher, Data Security, Key Matrix Construction, Modular Arithmetic

I. Introduction

In mathematics, cryptography plays a crucial role [1]. Cryptography is one of the most important fields of technology and aims to provide data and information security using various algorithms [2]. Cryptography is also referred to as a tool to ensure the confidentiality of messages.The Hill cipher is a symmetric encryption algorithm that uses linear matrix transformations and modulo operations to encrypt plaintext into ciphertext with a high level of data processing efficiency [1], [3], [4], [5]. Research on modification and development of encryption is a crucial step to address hacking threats and optimize the security of sensitive data and information [6]. The objective of this research is to optimize the Hill cipher cryptography algorithm using a key matrix 5×5 with modulo 53 operations. The strength of the key matrix depends on its inverse; the more complex the calculations, the harder it is for intruders to decipher the original message [5], [7].

Furthermore, by optimizing this algorithm, it is expected to enhance security in the process of transmitting and storing information, especially in an era where hacking is increasingly complex and difficult to avoid. These efforts are crucial in protecting individual privacy and maintaining overall system security, ensuring that sensitive data remains secure despite potential threats from irresponsible parties [8].

II. Literatur review

A. Cryptography

The security of a cryptographic system depends on the strength of the algorithm used and the secrecy of the key used to encrypt and decrypt data [9], [10]. Cryptography operates on the following principles [11] :

1) *Confidentiality :* the principle of confidentiality means that no one can understand the received message except the person who has the decryption key.

2) *Authentication* : the principle of authentication means verifying the identity of a user or system so that it can be trusted.

3) *Integrity* : the principle of integrity is the assurance that data is accurate and unchanged.

4) *Non-repudiation* : the principle of non-repudiation means that in the event of a dispute, it asserts that the sender cannot deny having sent the message.

Furthermore, the main components used in cryptographic systems are as follows [5], [11] :

1) *Sender* : someone, a group, or an organization initiating communication, known as the message sender.

2) *Receivers* : the message recipient or the destination of the message originating from the sender.

DOI : 10.52771/bangkitindonesia.v13i2.323
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

3) Plaint Text : The original message conveyed by the sender to the receiver.

4) Chipertext : a message that cannot be understood by anyone or a message that has no meaning; in cryptography, the original message (plaintext) is transformed into an unreadable message (ciphertext) before actual transmission of the message.

5) Encryption Algorithm : the process of transforming information or messages into secret code. Substitution and alteration of plaintext to obtain ciphertext.

6) Decryption Algorithm : a procedure known as cipher decryption transforms ciphertext into plaintext.

7) Secret Key : Secret key is a variable used by algorithms to encrypt and decrypt data. The secret key can be numeric or alphanumeric text, or it can be a unique symbol.The selection of keys in cryptography is crucial because the security of encryption algorithms depends on the secret key.

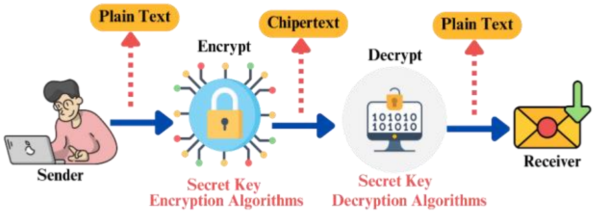

Fig 1. Cryptography Process

Cryptography algorithm is a procedure used to conceal the content of secret messages so that it cannot be accessed by unauthorized individuals. Based on the type of key used, cryptography algorithms are divided into three, namely [5], [11], [12] :

1) Symmetric Encryption : Symmetric encryption is a cryptography algorithm that uses only one key for both encryption and decryption. The sender encrypts plaintext using a key and sends the encrypted result, known as ciphertext, to the receiver. The receiver then uses the same key to decrypt the ciphertext and convert it back into plaintext. Because a single key is used for both functions, Secret key cryptography is also known as symmetric encryption, examples of which include Caesar cipher, AES, and DES [13], [14][15].

2) Asymmetric Encryotion : Public key cryptography, also known as asymmetric cryptography, is a system of encryption that uses two different keys for the encryption and decryption processes: the public key, which can be accessed by everyone, and the private key, which must be kept secret.

3) Hash function, in cryptography : Hashing is a commonly used technique to encrypt data quickly using standard algorithms. Hash value is typically generated by applying an algorithm to a specific text. Cryptographic hash functions cannot be reversed; therefore, once the data is encrypted, neither the same nor any other algorithm can decrypt the message. Hash functions keep data secure, so even if the data is stolen, the thief cannot exploit it.Hash function can also be used to validate digital signatures, ensuring that the signature is associated with a specific individual when signing documents online.

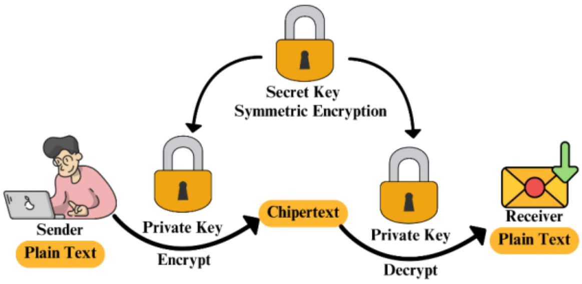

Fig 2. *Symmetric Encryption*

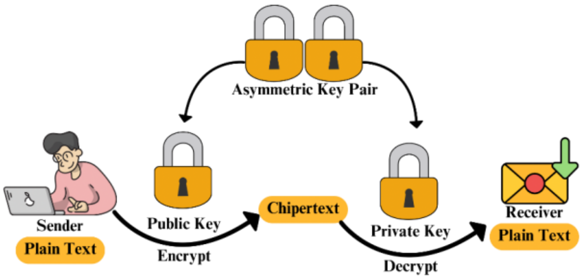

Fig 3. *Asymmetric Encryotion*

B. Hill Chiper

Hill Cipher is an encryption method in cryptography that utilizes a key matrix to transform plaintext into ciphertext [6].The Hill cipher is a cryptographic method that uses a nonsingular square matrix as a key to perform the encryption and decryption processes [16]. Hill Cipher is an encryption algorithm that employs linear algebra concepts, where each letter is represented by a number. The message to be encrypted or decrypted is divided into blocks of n letters and multiplied by a nonsingular square matrix using modulo arithmetic based on the alphabet size used. The key matrix used is typically randomly generated as a square matrix that must be invertible. The size of the matrix is determined by the block size of the ciphertext. This means that for a block size of n, the key matrix has a size of n × n [4].

III. METHODS

A. Encryption Algorithm

The plaintext is divided into blocks of fixed size, typically matching the size of the key matrix used. Next, the key matrix is multiplied by each vector of plaintext characters to obtain a new vector representing the encrypted characters.The new vector is converted back into characters using reverse mapping, resulting in ciphertext. This research uses Z53, where [6]:

DOI : 10.52771/bangkitindonesia.v13i2.323
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

TABEL I
HIIL CHIPERTEXT MODIFICATION Z53

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

The key matrix to be used is a 5 × 5 matrix, modified from the key matrix used in the classical hill cipher.

$$\mathcal{K} = \begin{bmatrix} k_{11} & k_{12} & k_{13} & k_{14} & k_{15} \\ k_{21} & k_{22} & k_{23} & k_{24} & k_{25} \\ k_{31} & k_{32} & k_{33} & k_{34} & k_{35} \\ k_{41} & k_{42} & k_{43} & k_{44} & k_{45} \\ k_{51} & k_{52} & k_{53} & k_{54} & k_{55} \end{bmatrix}$$

The formula used for the encryption process in the hill cipher [4], [6] :

$$\Upsilon = E(\mathcal{K},\mathcal{X}) = \mathcal{X}\mathcal{K} \ mod\, n \tag{1}$$

where $\mathcal{K}$ is the key matrix, χ is the plaintext, and Υ is the ciphertext.

B. Decryption Algorithm

The decryption algorithm is used to solve the ciphertext. The receiver must have the same key matrix as used for encryption, but with the inverse matrix calculated using modulo arithmetic. The encrypted message is divided into blocks of the same size as the key matrix. Each block is transformed into a vector of numerical values, similar to the encryption process. The inverse of the key matrix is multiplied by each vector of ciphertext characters to generate a new vector representing the decrypted characters. The new vector is converted back into characters using the inverse mapping, thereby returning the original text (plaintext).The formula used for the decryption process in the hill cipher [4], [6] :

$$\mathcal{X} = \mathcal{D}(\mathcal{K},\Upsilon) = \Upsilon\mathcal{K}^{-1} \ mod\, n \tag{2}$$

Where, $\mathcal{K}^{-1} = Adj\mathcal{K}.(Det\mathcal{K})^{-1} mod\, n$

IV. RESULT AND DISCUSSIONS

A. Encryption Simulation

In this research, data encryption will be conducted using mathematical calculations with the formulas mentioned earlier, as well as utilizing Matlab. The encrypted data consists of the phrase ”Cryptography Ensures Data Confidentiality And Integrity” secured using a 5 × 5 matrix encryption key. Next, as an example, the following nonsingular matrix is used as the key matrix and the selected key matrix must have an inverse:

$$\mathcal{K} = \begin{bmatrix} \mathbf{3} & \mathbf{5} & \mathbf{7} & \mathbf{5} & \mathbf{2} \\ \mathbf{2} & \mathbf{6} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{4} & \mathbf{7} & \mathbf{3} & \mathbf{6} & \mathbf{0} \\ \mathbf{3} & \mathbf{2} & \mathbf{4} & \mathbf{2} & \mathbf{1} \\ \mathbf{4} & \mathbf{6} & \mathbf{7} & \mathbf{9} & \mathbf{12} \end{bmatrix}$$

Step 1. The plaintext is divided into blocks of size equal to the key matrix, which is 5 x 1 :

$$\begin{bmatrix} C \\ r \\ y \\ p \\ t \end{bmatrix} = \begin{bmatrix} 2 \\ 43 \\ 50 \\ 41 \\ 45 \end{bmatrix}, \begin{bmatrix} o \\ g \\ r \\ a \\ p \end{bmatrix} = \begin{bmatrix} 40 \\ 32 \\ 43 \\ 26 \\ 41 \end{bmatrix}, \begin{bmatrix} h \\ y \\ space \\ E \\ n \end{bmatrix} = \begin{bmatrix} 33 \\ 50 \\ 52 \\ 4 \\ 39 \end{bmatrix},$$

$$\begin{bmatrix} s \\ u \\ r \\ e \\ s \end{bmatrix} = \begin{bmatrix} 44 \\ 46 \\ 43 \\ 30 \\ 44 \end{bmatrix}, \begin{bmatrix} space \\ D \\ a \\ t \\ a \end{bmatrix} = \begin{bmatrix} 52 \\ 3 \\ 26 \\ 45 \\ 26 \end{bmatrix}, \begin{bmatrix} space \\ C \\ o \\ n \\ f \end{bmatrix} = \begin{bmatrix} 52 \\ 2 \\ 40 \\ 39 \\ 31 \end{bmatrix}$$

$$\begin{bmatrix} i \\ d \\ e \\ n \\ t \end{bmatrix} = \begin{bmatrix} 34 \\ 29 \\ 30 \\ 39 \\ 45 \end{bmatrix}, \begin{bmatrix} i \\ a \\ l \\ i \\ t \end{bmatrix} = \begin{bmatrix} 34 \\ 26 \\ 37 \\ 34 \\ 45 \end{bmatrix}, \begin{bmatrix} y \\ space \\ A \\ n \\ d \end{bmatrix} = \begin{bmatrix} 50 \\ 52 \\ 0 \\ 39 \\ 29 \end{bmatrix},$$

$$\begin{bmatrix} space \\ I \\ n \\ t \\ e \end{bmatrix} = \begin{bmatrix} 52 \\ 8 \\ 39 \\ 45 \\ 30 \end{bmatrix}, \begin{bmatrix} g \\ r \\ i \\ t \\ y \end{bmatrix} = \begin{bmatrix} 32 \\ 43 \\ 34 \\ 45 \\ 50 \end{bmatrix}$$

Step 2. The key matrix is multiplied by each vector of plaintext characters to obtain a new vector representing the encrypted characters, where :

$$\Upsilon = E(\mathcal{K},\mathcal{X}) = \mathcal{K}\mathcal{X} \ mod\ 53 \tag{3}$$

$$\Upsilon_1 = \begin{bmatrix} 3 & 5 & 7 & 5 & 2 \\ 2 & 6 & 1 & 0 & 1 \\ 4 & 7 & 3 & 6 & 0 \\ 3 & 2 & 4 & 2 & 1 \\ 4 & 6 & 7 & 9 & 12 \end{bmatrix} \begin{bmatrix} 2 \\ 43 \\ 50 \\ 41 \\ 45 \end{bmatrix} mod\ 53 = \begin{bmatrix} 18 \\ 39 \\ 16 \\ 48 \\ 41 \end{bmatrix}$$

$$\Upsilon_2 = \begin{bmatrix} 3 & 5 & 7 & 5 & 2 \\ 2 & 6 & 1 & 0 & 1 \\ 4 & 7 & 3 & 6 & 0 \\ 3 & 2 & 4 & 2 & 1 \\ 4 & 6 & 7 & 9 & 12 \end{bmatrix} \begin{bmatrix} 20 \\ 32 \\ 43 \\ 26 \\ 41 \end{bmatrix} mod\ 53 = \begin{bmatrix} 51 \\ 38 \\ 33 \\ 25 \\ 1 \end{bmatrix}$$

$$\Upsilon_3 = \begin{bmatrix} 3 & 5 & 7 & 5 & 2 \\ 2 & 6 & 1 & 0 & 1 \\ 4 & 7 & 3 & 6 & 0 \\ 3 & 2 & 4 & 2 & 1 \\ 4 & 6 & 7 & 9 & 12 \end{bmatrix} \begin{bmatrix} 33 \\ 50 \\ 52 \\ 4 \\ 39 \end{bmatrix} mod\ 53 = \begin{bmatrix} 16 \\ 33 \\ 26 \\ 30 \\ 28 \end{bmatrix}$$

$$\Upsilon_4 = \begin{bmatrix} 3 & 5 & 7 & 5 & 2 \\ 2 & 6 & 1 & 0 & 1 \\ 4 & 7 & 3 & 6 & 0 \\ 3 & 2 & 4 & 2 & 1 \\ 4 & 6 & 7 & 9 & 12 \end{bmatrix} \begin{bmatrix} 44 \\ 46 \\ 43 \\ 30 \\ 44 \end{bmatrix} mod\ 53 = \begin{bmatrix} 0 \\ 27 \\ 12 \\ 23 \\ 14 \end{bmatrix}$$

$$\Upsilon_5 = \begin{bmatrix} 3 & 5 & 7 & 5 & 2 \\ 2 & 6 & 1 & 0 & 1 \\ 4 & 7 & 3 & 6 & 0 \\ 3 & 2 & 4 & 2 & 1 \\ 4 & 6 & 7 & 9 & 12 \end{bmatrix} \begin{bmatrix} 52 \\ 3 \\ 26 \\ 45 \\ 26 \end{bmatrix} mod\ 53 = \begin{bmatrix} 47 \\ 15 \\ 47 \\ 11 \\ 12 \end{bmatrix}$$

$$\Upsilon_6 = \begin{bmatrix} 3 & 5 & 7 & 5 & 2 \\ 2 & 6 & 1 & 0 & 1 \\ 4 & 7 & 3 & 6 & 0 \\ 3 & 2 & 4 & 2 & 1 \\ 4 & 6 & 7 & 9 & 12 \end{bmatrix} \begin{bmatrix} 52 \\ 2 \\ 40 \\ 39 \\ 31 \end{bmatrix} mod\ 53 = \begin{bmatrix} 14 \\ 28 \\ 46 \\ 5 \\ 4 \end{bmatrix}$$

$$\Upsilon_7 = \begin{bmatrix} 3 & 5 & 7 & 5 & 2 \\ 2 & 6 & 1 & 0 & 1 \\ 4 & 7 & 3 & 6 & 0 \\ 3 & 2 & 4 & 2 & 1 \\ 4 & 6 & 7 & 9 & 12 \end{bmatrix} \begin{bmatrix} 34 \\ 29 \\ 30 \\ 39 \\ 45 \end{bmatrix} mod\ 53 = \begin{bmatrix} 0 \\ 52 \\ 27 \\ 32 \\ 33 \end{bmatrix}$$

$$\Upsilon_8 = \begin{bmatrix} 3 & 5 & 7 & 5 & 2 \\ 2 & 6 & 1 & 0 & 1 \\ 4 & 7 & 3 & 6 & 0 \\ 3 & 2 & 4 & 2 & 1 \\ 4 & 6 & 7 & 9 & 12 \end{bmatrix} \begin{bmatrix} 34 \\ 26 \\ 37 \\ 34 \\ 45 \end{bmatrix} mod\ 53 = \begin{bmatrix} 9 \\ 41 \\ 50 \\ 44 \\ 19 \end{bmatrix}$$

$$\Upsilon_9 = \begin{bmatrix} 3 & 5 & 7 & 5 & 2 \\ 2 & 6 & 1 & 0 & 1 \\ 4 & 7 & 3 & 6 & 0 \\ 3 & 2 & 4 & 2 & 1 \\ 4 & 6 & 7 & 9 & 12 \end{bmatrix} \begin{bmatrix} 50 \\ 52 \\ 0 \\ 39 \\ 29 \end{bmatrix} mod\ 53 = \begin{bmatrix} 27 \\ 17 \\ 3 \\ 43 \\ 45 \end{bmatrix}$$

$$\Upsilon_{10} = \begin{bmatrix} 3 & 5 & 7 & 5 & 2 \\ 2 & 6 & 1 & 0 & 1 \\ 4 & 7 & 3 & 6 & 0 \\ 3 & 2 & 4 & 2 & 1 \\ 4 & 6 & 7 & 9 & 12 \end{bmatrix} \begin{bmatrix} 52 \\ 8 \\ 39 \\ 45 \\ 30 \end{bmatrix} mod\ 53 = \begin{bmatrix} 12 \\ 9 \\ 15 \\ 24 \\ 22 \end{bmatrix}$$

$$\Upsilon_{11} = \begin{bmatrix} 3 & 5 & 7 & 5 & 2 \\ 2 & 6 & 1 & 0 & 1 \\ 4 & 7 & 3 & 6 & 0 \\ 3 & 2 & 4 & 2 & 1 \\ 4 & 6 & 7 & 9 & 12 \end{bmatrix} \begin{bmatrix} 32 \\ 43 \\ 34 \\ 45 \\ 50 \end{bmatrix} mod\ 53 = \begin{bmatrix} 26 \\ 35 \\ 6 \\ 34 \\ 39 \end{bmatrix}$$

Step 3.

$$\begin{bmatrix} 18 \\ 39 \\ 16 \\ 48 \\ 41 \end{bmatrix} = \begin{bmatrix} S \\ n \\ Q \\ w \\ p \end{bmatrix}, \begin{bmatrix} 51 \\ 38 \\ 33 \\ 25 \\ 1 \end{bmatrix} = \begin{bmatrix} z \\ m \\ h \\ Z \\ B \end{bmatrix}, \begin{bmatrix} 16 \\ 33 \\ 26 \\ 30 \\ 28 \end{bmatrix} = \begin{bmatrix} Q \\ h \\ a \\ e \\ c \end{bmatrix},$$

$$\begin{bmatrix} 0 \\ 27 \\ 12 \\ 23 \\ 14 \end{bmatrix} = \begin{bmatrix} A \\ b \\ M \\ X \\ O \end{bmatrix}, \begin{bmatrix} 47 \\ 15 \\ 47 \\ 11 \\ 12 \end{bmatrix} = \begin{bmatrix} v \\ P \\ v \\ L \\ M \end{bmatrix}, \begin{bmatrix} 14 \\ 28 \\ 46 \\ 5 \\ 4 \end{bmatrix} = \begin{bmatrix} O \\ c \\ u \\ F \\ E \end{bmatrix}$$

$$\begin{bmatrix} 0 \\ 52 \\ 27 \\ 32 \\ 33 \end{bmatrix} = \begin{bmatrix} A \\ space \\ b \\ g \\ h \end{bmatrix}, \begin{bmatrix} 9 \\ 41 \\ 50 \\ 44 \\ 19 \end{bmatrix} = \begin{bmatrix} J \\ p \\ y \\ s \\ T \end{bmatrix}, \begin{bmatrix} 27 \\ 17 \\ 3 \\ 43 \\ 45 \end{bmatrix} = \begin{bmatrix} b \\ R \\ D \\ r \\ t \end{bmatrix},$$

$$\begin{bmatrix} 12 \\ 9 \\ 15 \\ 24 \\ 22 \end{bmatrix} = \begin{bmatrix} M \\ J \\ P \\ Y \\ W \end{bmatrix}, \begin{bmatrix} 26 \\ 35 \\ 6 \\ 34 \\ 39 \end{bmatrix} = \begin{bmatrix} a \\ j \\ G \\ i \\ n \end{bmatrix}$$

Chipertext : SnQwpzmhZBQhaecAbMXOvPvLMOcuFEA BghJpysTbRDrtMJPYWajGin

B. *Decryption Simulation*

The decryption algorithm is performed to decrypt the ciphertext.

$$\mathcal{K} = \begin{bmatrix} \mathbf{3} & \mathbf{5} & \mathbf{7} & \mathbf{5} & \mathbf{2} \\ \mathbf{2} & \mathbf{6} & \mathbf{1} & \mathbf{0} & \mathbf{1} \\ \mathbf{4} & \mathbf{7} & \mathbf{3} & \mathbf{6} & \mathbf{0} \\ \mathbf{3} & \mathbf{2} & \mathbf{4} & \mathbf{2} & \mathbf{1} \\ \mathbf{4} & \mathbf{6} & \mathbf{7} & \mathbf{9} & \mathbf{12} \end{bmatrix}$$

$$\mathcal{X} = \mathcal{D}(\mathcal{K}, \Upsilon) = \Upsilon\mathcal{K}^{-1}\ mod\ n \tag{4}$$

Dimana, $\mathcal{K}^{-1} = Adj\mathcal{K}.(Det\mathcal{K})^{-1} mod\ n$

Step 1. Calculating the inverse of the key matrix using modulo arithmetic.

$$|\mathcal{K}| = \begin{vmatrix} 3 & 5 & 7 & 5 & 2 \\ 2 & 6 & 1 & 0 & 1 \\ 4 & 7 & 3 & 6 & 0 \\ 3 & 2 & 4 & 2 & 1 \\ 4 & 6 & 7 & 9 & 12 \end{vmatrix} = 3382\ mod\ 53 = 43$$

$$(Det\mathcal{K})^{-1} = |\mathcal{K}|^{-1} = (43)^{-1} mod\ 53 = 37 \tag{5}$$

$$\mathcal{K}^{-1} = \mathcal{K}^{-1} = Adj\mathcal{K}.(Det\mathcal{K})^{-1} mod\ 53 \tag{6}$$

So the obtained value of the inverse of the key matrix is as Follows

$$\mathcal{K}^{-1} = \begin{bmatrix} \mathbf{6} & \mathbf{40} & \mathbf{2} & \mathbf{40} & \mathbf{10} \\ \mathbf{4} & \mathbf{15} & \mathbf{47} & \mathbf{16} & \mathbf{10} \\ \mathbf{49} & \mathbf{36} & \mathbf{43} & \mathbf{49} & \mathbf{51} \\ \mathbf{11} & \mathbf{35} & \mathbf{2} & \mathbf{45} & \mathbf{18} \\ \mathbf{21} & \mathbf{7} & \mathbf{42} & \mathbf{40} & \mathbf{28} \end{bmatrix}$$

Based on the matrix property, κ × κ-1 is the identity matrix.

Step 2. Calculating the determinant of the key matrix.

$$\mathcal{X} = \mathcal{D}(\mathcal{K}, \Upsilon) = \mathcal{K}^{-1}\Upsilon\ mod\ n$$

DOI : 10.52771/bangkitindonesia.v13i2.323
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

$$\mathcal{X}_1 = \begin{bmatrix} 6 & 40 & 2 & 40 & 10 \\ 4 & 15 & 47 & 16 & 10 \\ 49 & 36 & 43 & 49 & 51 \\ 11 & 35 & 2 & 45 & 18 \\ 21 & 7 & 42 & 40 & 28 \end{bmatrix} \begin{bmatrix} 18 \\ 39 \\ 16 \\ 48 \\ 41 \end{bmatrix} mod\ 53 = \begin{bmatrix} 2 \\ 43 \\ 50 \\ 41 \\ 45 \end{bmatrix} = \begin{bmatrix} C \\ r \\ y \\ p \\ t \end{bmatrix}$$

$$\mathcal{X}_2 = \begin{bmatrix} 6 & 40 & 2 & 40 & 10 \\ 4 & 15 & 47 & 16 & 10 \\ 49 & 36 & 43 & 49 & 51 \\ 11 & 35 & 2 & 45 & 18 \\ 21 & 7 & 42 & 40 & 28 \end{bmatrix} \begin{bmatrix} 51 \\ 38 \\ 33 \\ 25 \\ 1 \end{bmatrix} mod\ 53 = \begin{bmatrix} 40 \\ 32 \\ 43 \\ 26 \\ 41 \end{bmatrix} = \begin{bmatrix} o \\ g \\ r \\ a \\ p \end{bmatrix}$$

$$\mathcal{X}_3 = \begin{bmatrix} 6 & 40 & 2 & 40 & 10 \\ 4 & 15 & 47 & 16 & 10 \\ 49 & 36 & 43 & 49 & 51 \\ 11 & 35 & 2 & 45 & 18 \\ 21 & 7 & 42 & 40 & 28 \end{bmatrix} \begin{bmatrix} 16 \\ 33 \\ 26 \\ 30 \\ 28 \end{bmatrix} mod\ 53 = \begin{bmatrix} 33 \\ 50 \\ 52 \\ 4 \\ 39 \end{bmatrix} = \begin{bmatrix} h \\ y \\ space \\ E \\ n \end{bmatrix}$$

$$\mathcal{X}_4 = \begin{bmatrix} 6 & 40 & 2 & 40 & 10 \\ 4 & 15 & 47 & 16 & 10 \\ 49 & 36 & 43 & 49 & 51 \\ 11 & 35 & 2 & 45 & 18 \\ 21 & 7 & 42 & 40 & 28 \end{bmatrix} \begin{bmatrix} 0 \\ 27 \\ 12 \\ 23 \\ 14 \end{bmatrix} mod\ 53 = \begin{bmatrix} 44 \\ 46 \\ 43 \\ 30 \\ 44 \end{bmatrix} = \begin{bmatrix} s \\ u \\ r \\ e \\ s \end{bmatrix}$$

$$\mathcal{X}_5 = \begin{bmatrix} 6 & 40 & 2 & 40 & 10 \\ 4 & 15 & 47 & 16 & 10 \\ 49 & 36 & 43 & 49 & 51 \\ 11 & 35 & 2 & 45 & 18 \\ 21 & 7 & 42 & 40 & 28 \end{bmatrix} \begin{bmatrix} 47 \\ 15 \\ 47 \\ 11 \\ 12 \end{bmatrix} mod\ 53 = \begin{bmatrix} 52 \\ 3 \\ 26 \\ 45 \\ 26 \end{bmatrix} = \begin{bmatrix} space \\ D \\ a \\ t \\ a \end{bmatrix}$$

$$\mathcal{X}_6 = \begin{bmatrix} 6 & 40 & 2 & 40 & 10 \\ 4 & 15 & 47 & 16 & 10 \\ 49 & 36 & 43 & 49 & 51 \\ 11 & 35 & 2 & 45 & 18 \\ 21 & 7 & 42 & 40 & 28 \end{bmatrix} \begin{bmatrix} 14 \\ 28 \\ 46 \\ 5 \\ 4 \end{bmatrix} mod\ 53 = \begin{bmatrix} 52 \\ 2 \\ 40 \\ 39 \\ 31 \end{bmatrix} = \begin{bmatrix} space \\ C \\ o \\ n \\ f \end{bmatrix}$$

$$\mathcal{X}_7 = \begin{bmatrix} 6 & 40 & 2 & 40 & 10 \\ 4 & 15 & 47 & 16 & 10 \\ 49 & 36 & 43 & 49 & 51 \\ 11 & 35 & 2 & 45 & 18 \\ 21 & 7 & 42 & 40 & 28 \end{bmatrix} \begin{bmatrix} 0 \\ 52 \\ 27 \\ 32 \\ 33 \end{bmatrix} mod\ 53 = \begin{bmatrix} 34 \\ 29 \\ 30 \\ 39 \\ 45 \end{bmatrix} = \begin{bmatrix} i \\ d \\ e \\ n \\ t \end{bmatrix}$$

$$\mathcal{X}_8 = \begin{bmatrix} 6 & 40 & 2 & 40 & 10 \\ 4 & 15 & 47 & 16 & 10 \\ 49 & 36 & 43 & 49 & 51 \\ 11 & 35 & 2 & 45 & 18 \\ 21 & 7 & 42 & 40 & 28 \end{bmatrix} \begin{bmatrix} 9 \\ 41 \\ 50 \\ 44 \\ 19 \end{bmatrix} mod\ 53 = \begin{bmatrix} 34 \\ 26 \\ 37 \\ 34 \\ 45 \end{bmatrix} = \begin{bmatrix} i \\ a \\ l \\ i \\ t \end{bmatrix}$$

$$\mathcal{X}_9 = \begin{bmatrix} 6 & 40 & 2 & 40 & 10 \\ 4 & 15 & 47 & 16 & 10 \\ 49 & 36 & 43 & 49 & 51 \\ 11 & 35 & 2 & 45 & 18 \\ 21 & 7 & 42 & 40 & 28 \end{bmatrix} \begin{bmatrix} 27 \\ 17 \\ 3 \\ 43 \\ 45 \end{bmatrix} mod\ 53 = \begin{bmatrix} 50 \\ 52 \\ 0 \\ 39 \\ 29 \end{bmatrix} = \begin{bmatrix} y \\ space \\ A \\ n \\ d \end{bmatrix}$$

$$\mathcal{X}_{10} = \begin{bmatrix} 6 & 40 & 2 & 40 & 10 \\ 4 & 15 & 47 & 16 & 10 \\ 49 & 36 & 43 & 49 & 51 \\ 11 & 35 & 2 & 45 & 18 \\ 21 & 7 & 42 & 40 & 28 \end{bmatrix} \begin{bmatrix} 12 \\ 9 \\ 15 \\ 24 \\ 22 \end{bmatrix} mod\ 53 = \begin{bmatrix} 52 \\ 8 \\ 39 \\ 45 \\ 30 \end{bmatrix} = \begin{bmatrix} space \\ I \\ n \\ t \\ e \end{bmatrix}$$

$$\mathcal{X}_{11} = \begin{bmatrix} 6 & 40 & 2 & 40 & 10 \\ 4 & 15 & 47 & 16 & 10 \\ 49 & 36 & 43 & 49 & 51 \\ 11 & 35 & 2 & 45 & 18 \\ 21 & 7 & 42 & 40 & 28 \end{bmatrix} \begin{bmatrix} 26 \\ 35 \\ 6 \\ 34 \\ 39 \end{bmatrix} mod\ 53 = \begin{bmatrix} 32 \\ 43 \\ 34 \\ 45 \\ 50 \end{bmatrix} = \begin{bmatrix} g \\ r \\ i \\ t \\ y \end{bmatrix}$$

Plaintext: Cryptography Ensures Data Confidentiality And Integrity

Based on the decryption stages above, it is evident that the complexity of the key matrix inversion operations is crucial in maintaining the security of the original message against decryption attempts by unauthorized parties.

V. Conclusons

In conclusions, the study demonstrates that the employment of a randomly chosen 5 × 5 nonsingular key matrix for encryption and decryption of data, combined with modular 53, presents a viable approach to enhancing data security. The effectiveness depends on the complexity of the matrix's inverse operations, which heightens the difficulty for unauthorized entities attempting to decrypt the original message. Therefore, integrating larger-order key matrices with higher moduli significantly strengthens the encryption system's robustness, enhancing its resilience against sophisticated cryptanalysis attacks, especially in complex application scenarios.

Referensi

[1] M. Y. M. P. 2023, S. Kaliswaran, "Image Encryption Using A Combination Of The Hill Cipher, Fibonacci Matrix, And Elliptic Curve Cryptography," *J. Data Acquis. Process.*, vol. 4, no. 1, pp. 88–100, 2023, doi: 10.5281/zenodo.98549833.

[2] M. D. Gietaneh and T. B. Akele, "Enhancing the Hill Cipher Algorithm and Employing a One Time Pad Key Generation Technique," *Abyssinia J. Eng. Comput.*, vol. 3, no. 1, pp. 1–10, Jan. 2023, doi: 10.20372/AJEC.2023.V3.I1.808.

[3] A. A. Kumar, S. Kiran, and D. S. Reddy, "Modified Hill Cipher with Invertible Key Matrix Using Radix 64 Conversion BT - Futuristic Communication and Network Technologies," N. Subhashini, M. A. G. Ezra, and S.-K. Liaw, Eds., Singapore: Springer Nature Singapore, 2023, pp. 175–184.

[4] S. Ameen, "Capital University Of Science And Technology , Islamabad A Key Recovery Attack on Modified Hill Encryption Scheme by," 2023.

[5] M. Hanif and J. Naime, "Analyzing The Security System Through Matrices In Cryptography," no. April, pp. 0–44, 2024, doi: 10.13140/RG.2.2.24576.03847.

[6] Tulus, S. Sy, K. A. Sugeng, R. Simanjuntak, and J. L. Marpaung, "Improving data security with the utilization of matrix columnar transposition techniques," *E3S Web Conf.*, vol. 501, 2024, doi: 10.1051/e3sconf/202450102004.

[7] S. Sujarwo, "Key analysis of the hill cipher algorithm (Study of literature)," *J. Mandiri IT*, vol. 12, no. 3, pp. 135–141, Jan. 2024, doi: 10.35335/MANDIRI.V12I3.250.

[8] M. A. Saidah, "Analisis Komparasi Cybercrime Web Defacement dan Darknet Exposure di Indonesia (Studi Kasus : Lanskap Keamanan Siber di Indonesia Tahun 2022 dan Tahun 2023) | Prosiding Seminar Nasional Ilmu Sosial dan Teknologi (SNISTEK)," Prosiding Seminar Nasional Ilmu Sosial Dan Teknologi (SNISTEK), 6. Accessed: Oct. 17, 2024. [Online]. Available: https://ejournal.upbatam.ac.id/index.php/prosiding/article/view/9345

[9] S. K. M. K. K. A. R. M. F. A. Abdul Muni, "Kriptografi Untuk Keamanan Sistem Informasi Copyright @2024 by Abdul Muni, S.Kom., M.Kom., dkk.," 2024, Accessed: Oct. 17, 2024. [Online]. Available: https://books.google.co.id/books?id=iY8YEQAAQBAJ

DOI : 10.52771/bangkitindonesia.v13i2.323
p-ISSN: 2337-4055 **e-ISSN:** 2776-9267

[10] D. Ariyus and U. Amikom, "Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi," p. 372, 2023, Accessed: Oct. 17, 2024. [Online]. Available: https://books.google.co.id/books?id=3SSTJONEmX0C

[11] R. M. Al-Amri, D. N. Hamood, and A. K. Farhan, "Theoretical Background of Cryptography," *Mesopotamian J. CyberSecurity*, vol. 2023, pp. 7–15, 2023, doi: 10.58496/MJCS/2023/002.

[12] G. E. Rahimova, "Ways to explore cryptography methods," *E3S Web Conf.*, vol. 538, p. 02024, 2024, doi: 10.1051/e3sconf/202453802024.

[13] P. Gaži and S. Tessaro, "Secret-key cryptography from ideal primitives: A systematic overview," in *2015 IEEE Information Theory Workshop (ITW)*, 2015, pp. 1–5. doi: 10.1109/ITW.2015.7133163.

[14] Y. Chen, R. Xie, H. Zhang, D. Li, and W. Lin, "Generation of high-order random key matrix for Hill Cipher encryption using the modular multiplicative inverse of triangular matrices," *Wirel. Networks*, vol. 30, no. 6, pp. 5697–5707, Aug. 2024, doi: 10.1007/S11276-023-03330-8/METRICS.

[15] I. M. A. Bhaskara, M. P. A. Ariawan, I. B. A. Peling, and I. P. A. Prayudha, "Studi Literatur: Analisa Perbandingan Teori Tentang Tingkat Keamanan Antar Algoritma Simetris," *J. Bangkit Indones.*, vol. 13, no. 1, pp. 40–45, 2024, doi: 10.52771/bangkitindonesia.v13i1.278.

[16] S. A. Salman, Y. M. Mohialden, A. Abdulhameed, and N. M. Hussien, "A Novel Method for Hill Cipher Encryption and Decryption Using Gaussian Integers Implemented in Banking Systems," *Iraqi J. Comput. Sci. Math.*, vol. 5, no. 1, pp. 277–284, 2024, doi: 10.52866/ijcsm.2024.05.01.019.