Research Article
Volume 14:01, 2025

Journal of Applied & Computational Mathematics

ISSN: 2168-9679 Open Access

Security System through Matrices in Cryptography

Jannatul Naime[1], Muhammad Hanif[1*] and A N M Rezaul Karim[2]

[1]*Department of Applied Mathematics, Noakhali Science and Technology University, Noakhali, Bangladesh*

[2]*Department of Computer Science and Engineering, International Islamic University Chittagong Kumira, Chittagong, Bangladesh*

Abstract

Communication over the internet must be secure to prevent intercepting or accessing sensitive information. Attempts are being made to protect confidential information by providing maximum security over the network. One of such techniques is using matrix multiplication for Hill Cipher cryptosystem, which is not easily breakable. The traditional Hill Cipher algorithm uses 2 × 2 and 3 × 3 matrix for generating keys. In this paper, we enhance the existing algorithm by using 4 × 4 matrix to generate the keys and to demonstrate the application of this algorithm created in MATLAB programming language. We also compare the time consumed to encode and decode the message by the traditional Hill Cipher algorithm. The enhanced Hill Cipher algorithm to get a clear idea which algorithm is more efficient and reliable and not easily breakable by the intruders.

Keywords: 2D and 3D matrix transformations • Hill Cipher algorithm • Cryptography • MATLAB programming

Introduction

A significant quantity of digital data is exchanged across insecure routes today. Hacking is always a possibility when sharing private and confidential photographs over an open network. Researchers now have the difficult task of creating appropriate encryption methods to thwart various cryptanalytic attacks [1]. A tool for ensuring message confidentiality is cryptography. The phrase "composing mystery" has a unique connotation in Greek [2]. In plaintext, the working cycle that modifies the actual message is referred to as cypher text. The scrambling conversation loop recovers the chip text's original plaintext. Cryptography [3], which may be regarded as an ancient technology that has been used up to this point, ensures that the data supplied are protected with the ultimate goal of assuring the receiver can access this information from registered roots. Models date to 2000 BCE, when "hidden" hieroglyphic hieroglyphs were utilized by the extinct Egyptians, much as other evidence of the Caesar Code or Riddle creation in ancient Rome. Cryptography is regularly used by billions of people throughout the world to safeguard information and data, but most of them are unaware that they are doing so [4,5]. The development of encryption is headed for an unavoidable future with endless possibilities. Since hacking is difficult to prevent, we can use encryption techniques to ensure the security of our sensitive data, even if it is compromised [6].

Materials and Methods

Cryptography basic terms

Plain text: The original message that the person wishes to communicate with the other is defined as plain text. In cryptography the actual message that has to be send to the other end is given a special name as plain text.

Ciphertext: The message that cannot be understood by anyone or meaningless message is what we call as cipher text. In cryptography the original message is transformed into non readable message before the transmission of actual message.

Encryption algorithm: It performs various methods, for example, replacement and change on the plaintext to acquire cipher text.

Decryption algorithm: It is the precisely inverse system of encryption strategy. To acquire unique plaintext, it utilizes cipher text and mystery key.

Key

A key is a numeric or alpha numeric text or can be a unique symbol. The key can be used at the time of encryption takes place on the plain text and at the time of decryption takes place on the Cipher text. The selection of key in cryptography is very important since the security of encryption algorithm depends directly on it (Figure 1).

***Address for Correspondence:** Muhammad Hanif, Department of Applied Mathematics, Noakhali Science and Technology University, Noakhali, Bangladesh; E-mail: drhanifmurad@nstu.edu.bd*

Received: 05 July, 2024, Manuscript No. JACM-24-140881; **Editor assigned:** 07 July, 2024, PreQC No. JACM-24-140881 (PQ); **Reviewed:** 21 July, 2024, QC No. JACM-24-140881; **Revised:** 06 February, 2025, Manuscript No. JACM-24-140881 (R); **Published:** 13 February 2025, DOI: 10.37421/2168-9679.2025.14.599

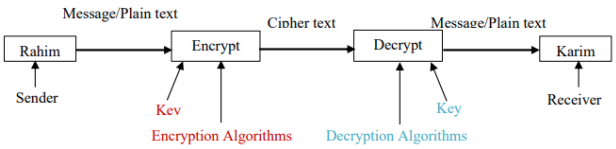

Figure 1. Cryptographic process.

Matrix

A rectangular array of (real or complex) numbers of the form

$$\begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix}$$

is called a matrix. The numbers x_{11}, $\cdots$, x_{mn} are called the elements of the matrix. The above matrix has m rows and n columns and is called an $(m \times n)$ matrix [7].

Circulant matrix: A circulant matrix is a square matrix in which all row vectors are composed of the same elements and each row vector is rotated one element to the right relative to the preceding row vector. An $n \times n$ circulant matrix is defined by n parameters, the elements in the first row, and each subsequent row is a cyclic shift forward of the one above:

$$C = \begin{bmatrix} c_1 & c_2 & \cdots & c_n \\ c_n & c_1 & \cdots & \vdots \\ \vdots & \ddots & \ddots & c_2 \\ c_2 & \cdots & c_n & c_1 \end{bmatrix}$$

For example,

$$A = \begin{bmatrix} 5 & 9 & 8 \\ 8 & 5 & 9 \\ 9 & 8 & 5 \end{bmatrix} \text{ or, } \begin{bmatrix} 15 & 6 & 11 & 5 \\ 5 & 15 & 6 & 11 \\ 11 & 5 & 15 & 6 \\ 6 & 11 & 5 & 15 \end{bmatrix}$$

Now, $|A| = \begin{bmatrix} 5 & 9 & 8 \\ 8 & 5 & 9 \\ 9 & 8 & 5 \end{bmatrix}$

$$\Rightarrow |A| = 5\begin{vmatrix} 5 & 9 \\ 8 & 5 \end{vmatrix} - 9\begin{vmatrix} 8 & 9 \\ 9 & 5 \end{vmatrix} + 8\begin{vmatrix} 8 & 5 \\ 9 & 8 \end{vmatrix}$$

$$= 5(25 - 72) - 9(40 - 81) + 8(64 - 45)$$

$$= 5(-47) - 9(-41) + 8(19)$$

$$= -235 + 369 + 152$$

$$= 521 - 235 = 286$$

Symmetric matrix: A symmetric matrix is a square matrix that is equal to its transpose. *i.e.*, $A=A^T$. For example,

$$A = \begin{bmatrix} 1 & 7 & 3 \\ 7 & 4 & 5 \\ 3 & 5 & 1 \end{bmatrix} = A^T = \begin{bmatrix} 1 & 7 & 3 \\ 7 & 4 & 5 \\ 3 & 5 & 1 \end{bmatrix}$$

Skew-symmetric matrix: A skew-symmetric matrix is a square matrix whose transpose equals to its negative *i.e.*, $A=-A^T$. For example,

$$A = \begin{bmatrix} 0 & 2 & 4 \\ -2 & 0 & 3 \\ -4 & -3 & 0 \end{bmatrix} = -\begin{bmatrix} 0 & 2 & 4 \\ -2 & 0 & 3 \\ -4 & -3 & 0 \end{bmatrix} = -A^T$$

Existing Hill Cipher

The Hill Cipher was invented by Lester S. Hill in 1929. Unlike the others though it is extendable to work on different sized blocks of letters. So, technically it is a poly-graphic substitution Cipher, as it can work on digraphs, trigraphs or theoretically any sized blocks. The Hill Cipher uses an area of mathematics called Linear Algebra. It was the first Cipher that was able to operate on 3 symbols at once.

Method to encrypt using Hill Cipher: To encrypt a message using the Hill Cipher we must first turn our keyword into a key matrix. We also turn the plaintext into digraphs or trigraphs and each of these into a column vector. We then perform matrix multiplication modulo the length of the alphabet (*i.e.*, 26) on each vector. These vectors are then converted back into letters to produce the Cipher text. The plaintext is transformed into by the following procedure:

Step 1. Choose a 3 × 3 matrix with integer values.

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

Step 2. Group successive plaintext tellers into triples, adding an arbitrary "dummy" letter to fill out the last pair if the plaintext has an odd number of letters and replace each plaintext letter by its numerical value. The numerical value of the alphabet is shown in the below table:

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

Step 3. Successively convert each plaintext triple $P_1P_2P_3$ into a column vector.

$$P = \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}$$

And form the product AP we will call P a plaintext vector and AP the corresponding cipher text vector.

Step 4. Convert each cipher text vector into its alphabetic equivalent.

Proposed Hill Cipher

Step 1. Firstly, convert the message into a block and each blocks contain 4 alphabets. Choose a 4 × 4 matrix with integer values.

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$$

Step 2. Select a 4 × 4 key matrix and convert the plaintext vector into a numerical integer value.

Step 3. Successively convert each plaintext $P_1P_2P_3P_4$ into a column vector.

$$P = \begin{bmatrix} p_1 \\ p_2 \\ P_3 \\ P_4 \end{bmatrix}$$

And form the product AP we will call P a plaintext vector and AP the corresponding cipher text vector.

Step 4. Convert each Cipher text vector into its alphabetic equivalent.

Example of hill cipher encryption using 4 × 4 key matrix

Step 1: Encryption.

Message: APPLIED MATHEMATICS Key

Matrix: K =

$$\begin{bmatrix} 2 & 1 & 3 & 5 \\ 1 & 4 & 5 & 6 \\ 3 & 2 & 1 & 7 \\ 4 & 5 & 3 & 7 \end{bmatrix}$$

Step 2: Encryption

Message: APPLIED MATHEMATICS

Assign: Numerical value of the alphabet and convert the message in block with 4 alphabets in each block.

$$\begin{bmatrix} A \\ P \\ P \\ L \end{bmatrix} = \begin{bmatrix} 0 \\ 15 \\ 15 \\ 11 \end{bmatrix} \quad \begin{bmatrix} I \\ E \\ D \\ M \end{bmatrix} = \begin{bmatrix} 8 \\ 4 \\ 3 \\ 12 \end{bmatrix} \quad \begin{bmatrix} A \\ T \\ H \\ E \end{bmatrix} = \begin{bmatrix} 0 \\ 19 \\ 7 \\ 4 \end{bmatrix} \quad \begin{bmatrix} M \\ A \\ T \\ I \end{bmatrix} = \begin{bmatrix} 12 \\ 0 \\ 19 \\ 8 \end{bmatrix} \quad \begin{bmatrix} C \\ S \\ A \\ A \end{bmatrix} = \begin{bmatrix} 2 \\ 18 \\ 0 \\ 0 \end{bmatrix}$$

Step 3: Encryption

Message: APPLIED MATHEMATICS

Cipher text=(K × Plaintext) Mod 26

$$C_1 = \begin{bmatrix} 2 & 1 & 3 & 5 \\ 1 & 4 & 5 & 6 \\ 3 & 2 & 1 & 7 \\ 4 & 5 & 3 & 7 \end{bmatrix} \times \begin{bmatrix} 0 \\ 15 \\ 15 \\ 11 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} (2\times 0)+(1\times 15)+(3\times 15)+(5\times 11) \\ (1\times 0)+(4\times 15)+(5\times 15)+(6\times 11) \\ (3\times 0)+(2\times 15)+(1\times 15)+(7\times 11) \\ (4\times 0)+(5\times 15)+(3\times 15)+(7\times 11) \end{bmatrix} (\text{mod } 26)$$

$$= \begin{bmatrix} 0+15+45+55 \\ 0+60+75+66 \\ 0+30+15+77 \\ 0+75+45+77 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 115 \\ 201 \\ 122 \\ 197 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 11 \\ 19 \\ 18 \\ 15 \end{bmatrix}$$

$$C_2 = \begin{bmatrix} 2 & 1 & 3 & 5 \\ 1 & 4 & 5 & 6 \\ 3 & 2 & 1 & 7 \\ 4 & 5 & 3 & 7 \end{bmatrix} \times \begin{bmatrix} 8 \\ 4 \\ 3 \\ 12 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} (2\times 8)+(1\times 4)+(3\times 3)+(5\times 12) \\ (1\times 8)+(4\times 4)+(5\times 3)+(6\times 12) \\ (3\times 8)+(2\times 4)+(1\times 3)+(7\times 12) \\ (4\times 8)+(5\times 4)+(3\times 3)+(7\times 12) \end{bmatrix} (\text{mod } 26)$$

$$= \begin{bmatrix} 16+4+9+60 \\ 8+16+15+72 \\ 24+8+3+84 \\ 32+20+9+84 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 89 \\ 111 \\ 119 \\ 145 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 11 \\ 7 \\ 15 \\ 15 \end{bmatrix}$$

$$C_3 = \begin{bmatrix} 2 & 1 & 3 & 5 \\ 1 & 4 & 5 & 6 \\ 3 & 2 & 1 & 7 \\ 4 & 5 & 3 & 7 \end{bmatrix} \times \begin{bmatrix} 0 \\ 19 \\ 7 \\ 4 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} (2\times 0)+(1\times 19)+(3\times 7)+(5\times 4) \\ (1\times 0)+(4\times 19)+(5\times 7)+(6\times 4) \\ (3\times 0)+(2\times 19)+(1\times 7)+(7\times 4) \\ (4\times 0)+(5\times 19)+(3\times 7)+(7\times 4) \end{bmatrix} (\text{mod } 26)$$

$$= \begin{bmatrix} 0+19+21+20 \\ 0+76+35+24 \\ 0+38+7+28 \\ 0+95+21+28 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 60 \\ 135 \\ 73 \\ 144 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 8 \\ 5 \\ 21 \\ 14 \end{bmatrix}$$

$$C_4 = \begin{bmatrix} 2 & 1 & 3 & 5 \\ 1 & 4 & 5 & 6 \\ 3 & 2 & 1 & 7 \\ 4 & 5 & 3 & 7 \end{bmatrix} \times \begin{bmatrix} 12 \\ 0 \\ 19 \\ 8 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} (2\times 12)+(1\times 0)+(3\times 19)+(5\times 8) \\ (1\times 12)+(4\times 0)+(5\times 19)+(6\times 8) \\ (3\times 12)+(2\times 0)+(1\times 19)+(7\times 8) \\ (4\times 12)+(5\times 0)+(3\times 19)+(7\times 8) \end{bmatrix} (\text{mod } 26)$$

$$= \begin{bmatrix} 24+0+57+40 \\ 12+0+95+48 \\ 36+0+19+56 \\ 48+0+57+56 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 121 \\ 155 \\ 111 \\ 161 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 17 \\ 25 \\ 7 \\ 5 \end{bmatrix}$$

$$C_5 = \begin{bmatrix} 2 & 1 & 3 & 5 \\ 1 & 4 & 5 & 6 \\ 3 & 2 & 1 & 7 \\ 4 & 5 & 3 & 7 \end{bmatrix} \times \begin{bmatrix} 2 \\ 18 \\ 0 \\ 0 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} (2\times 2)+(1\times 18)+(3\times 0)+(5\times 0) \\ (1\times 2)+(4\times 18)+(5\times 0)+(6\times 0) \\ (3\times 2)+(2\times 18)+(1\times 0)+(7\times 0) \\ (4\times 2)+(5\times 18)+(3\times 0)+(7\times 0) \end{bmatrix} (\text{mod } 26)$$

$$= \begin{bmatrix} 4+18+0+0 \\ 2+72+0+0 \\ 6+36+0+0 \\ 8+90+0+0 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 22 \\ 74 \\ 42 \\ 98 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 22 \\ 22 \\ 16 \\ 20 \end{bmatrix}$$

Step 4: Encryption

Message: APPLIED MATHEMATICS

Convert each cipher text vector into its alphabetic equivalent.

$$C_1 = \begin{bmatrix} 11 \\ 19 \\ 18 \\ 15 \end{bmatrix} = \begin{bmatrix} L \\ T \\ S \\ P \end{bmatrix} \qquad C_2 = \begin{bmatrix} 11 \\ 7 \\ 15 \\ 15 \end{bmatrix} = \begin{bmatrix} L \\ H \\ P \\ P \end{bmatrix} \qquad C_3 = \begin{bmatrix} 8 \\ 5 \\ 21 \\ 14 \end{bmatrix} = \begin{bmatrix} I \\ F \\ V \\ O \end{bmatrix}$$

$$C_4 = \begin{bmatrix} 17 \\ 25 \\ 7 \\ 5 \end{bmatrix} = \begin{bmatrix} R \\ Z \\ H \\ F \end{bmatrix} \qquad C_5 = \begin{bmatrix} 22 \\ 22 \\ 16 \\ 20 \end{bmatrix} = \begin{bmatrix} W \\ W \\ Q \\ U \end{bmatrix}$$

APPLIED MATHEMATICS=LTSPLHP PIFVORZHFWWQU

Example of Hill Cipher decryption using 4 × 4 key matrix

Step 1: Decryption.

Ciphertext: LTSPLHP PIFVORZHFWWQU Key

matrix: K=

$$\begin{bmatrix}2&1&3&5\\1&4&5&6\\3&2&1&7\\4&5&3&7\end{bmatrix}$$

determinant of key |K| =

$$\begin{vmatrix}2&1&3&5\\1&4&5&6\\3&2&1&7\\4&5&3&7\end{vmatrix} = 126 \pmod{26} = 22$$

$|K|^{-1} = (22)^{-1} \bmod 26 = 16$

Transpose of key K^T=

$$\begin{bmatrix}2&1&3&4\\1&4&2&5\\3&5&1&3\\5&6&7&7\end{bmatrix}$$

$$a_{11} = \begin{vmatrix}4&2&5\\5&1&3\\6&7&7\end{vmatrix} = 55, a_{12} = -\begin{vmatrix}1&2&5\\3&1&3\\5&7&7\end{vmatrix} = -54, \quad a_{13} = \begin{vmatrix}1&4&5\\3&5&3\\5&6&7\end{vmatrix} = -42,$$

$$a_{14} = -\begin{vmatrix}1&4&2\\3&5&1\\5&6&7\end{vmatrix} = 49$$

$$a_{21} = \begin{vmatrix}1&3&4\\5&1&3\\6&7&7\end{vmatrix} = 54, a_{22} = -\begin{vmatrix}2&3&4\\3&1&3\\5&7&7\end{vmatrix} = -18, \quad a_{23} = \begin{vmatrix}2&1&4\\3&5&3\\5&6&7\end{vmatrix} = 0,$$

$$a_{24} = -\begin{vmatrix}2&1&3\\3&5&1\\5&6&7\end{vmatrix} = -21$$

$$a_{31} = \begin{vmatrix}1&3&4\\4&2&5\\6&7&7\end{vmatrix} = 49, a_{32} = -\begin{vmatrix}2&3&4\\1&2&5\\5&7&7\end{vmatrix} = 0, \quad a_{33} = \begin{vmatrix}2&1&4\\1&4&5\\5&6&7\end{vmatrix} = -42,$$

$$a_{34} = -\begin{vmatrix}2&1&3\\1&4&2\\5&6&7\end{vmatrix} = 7$$

$$a_{41} = \begin{vmatrix}1&3&4\\4&2&5\\5&1&3\end{vmatrix} = 16, a_{42} = -\begin{vmatrix}2&3&4\\1&2&5\\3&1&3\end{vmatrix} = -18, \quad a_{43} = \begin{vmatrix}2&1&4\\1&4&5\\3&5&3\end{vmatrix} = -42,$$

$$a_{44} = -\begin{vmatrix}2&1&3\\1&4&2\\3&5&1\end{vmatrix} = 28$$

Cofactor matrix of transpose of key

$$\begin{bmatrix}55&-54&-42&49\\54&-18&0&-21\\49&0&-42&7\\16&-18&-42&28\end{bmatrix}$$

$$K^{-1} = (|K|^{-1} \times \text{adj } K) \bmod 26 = 16 \times \begin{bmatrix}55&-54&-42&49\\54&-18&0&-21\\49&0&-42&7\\16&-18&-42&28\end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix}880&-864&-672&784\\864&-288&0&-336\\784&0&-672&122\\256&-288&-672&448\end{bmatrix} \pmod{26} = \begin{bmatrix}22&20&4&4\\6&24&0&2\\4&0&4&18\\22&24&4&6\end{bmatrix}$$

Step2: Decryption

Ciphertext: LTSPLHP PIFVORZHFWWQU

Assign: Numerical value of the alphabet and convert the Cipher text in block with 4 alphabets in each block.

$$\begin{bmatrix}L\\T\\S\\P\end{bmatrix} = \begin{bmatrix}11\\19\\18\\15\end{bmatrix} \quad \begin{bmatrix}L\\H\\P\\P\end{bmatrix} = \begin{bmatrix}11\\7\\15\\15\end{bmatrix} \quad \begin{bmatrix}I\\F\\V\\O\end{bmatrix} = \begin{bmatrix}8\\5\\21\\14\end{bmatrix} \quad \begin{bmatrix}R\\Z\\H\\F\end{bmatrix} = \begin{bmatrix}17\\25\\7\\5\end{bmatrix} \quad \begin{bmatrix}W\\W\\Q\\U\end{bmatrix} = \begin{bmatrix}22\\22\\16\\20\end{bmatrix}$$

Step 3: Decryption

Ciphertext: LTSPLHP PIFVORZHFWWQU Plain

text=(K^{-1} × Cipher text) Mod 26

$$P_1 = \begin{bmatrix}22&20&4&4\\6&24&0&2\\4&0&4&18\\22&24&4&6\end{bmatrix} \times \begin{bmatrix}11\\19\\18\\15\end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix}(22\times11)+(20\times19)+(4\times18)+(4\times15)\\(6\times11)+(24\times19)+(0\times18)+(2\times15)\\(4\times11)+(0\times19)+(4\times18)+(18\times15)\\(22\times11)+(24\times19)+(4\times18)+(6\times15)\end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix}242+380+72+60\\66+456+0+30\\44+0+72+270\\242+456+72+90\end{bmatrix} \pmod{26} = \begin{bmatrix}754\\552\\386\\860\end{bmatrix} \pmod{26} = \begin{bmatrix}0\\6\\22\\2\end{bmatrix}$$

$$P_2 = \begin{bmatrix}22&20&4&4\\6&24&0&2\\4&0&4&18\\22&24&4&6\end{bmatrix} \times \begin{bmatrix}11\\7\\15\\15\end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix}(22\times11)+(20\times7)+(4\times15)+(4\times15)\\(6\times11)+(24\times7)+(0\times15)+(2\times15)\\(4\times11)+(0\times7)+(4\times15)+(18\times15)\\(22\times11)+(24\times7)+(4\times15)+(6\times15)\end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix}242+140+62+60\\66+168+0+30\\44+0+60+270\\242+168+60+90\end{bmatrix} \pmod{26} = \begin{bmatrix}504\\264\\374\\560\end{bmatrix} \pmod{26} = \begin{bmatrix}10\\4\\10\\14\end{bmatrix}$$

$$P_3 = \begin{bmatrix}22&20&4&4\\6&24&0&2\\4&0&4&18\\22&24&4&6\end{bmatrix} \times \begin{bmatrix}8\\5\\21\\14\end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix}(22\times8)+(20\times5)+(4\times21)+(4\times14)\\(6\times8)+(24\times5)+(0\times21)+(2\times14)\\(4\times8)+(0\times5)+(4\times21)+(18\times14)\\(22\times8)+(24\times5)+(4\times21)+(6\times14)\end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix}176+100+84+56\\48+120+0+28\\32+0+84+252\\176+120+84+84\end{bmatrix} \pmod{26} = \begin{bmatrix}416\\196\\368\\464\end{bmatrix} \pmod{26} = \begin{bmatrix}0\\14\\4\\22\end{bmatrix}$$

$$P_4 = \begin{bmatrix}22&20&4&4\\6&24&0&2\\4&0&4&18\\22&24&4&6\end{bmatrix} \times \begin{bmatrix}17\\25\\7\\5\end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix}(22\times17)+(20\times25)+(4\times7)+(4\times5)\\(6\times17)+(24\times25)+(0\times7)+(2\times5)\\(4\times17)+(0\times25)+(4\times7)+(18\times5)\\(22\times17)+(24\times25)+(4\times7)+(6\times5)\end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix}374+500+28+20\\102+600+0+10\\68+0+28+90\\374+600+28+30\end{bmatrix} \pmod{26} = \begin{bmatrix}922\\712\\186\\1032\end{bmatrix} \pmod{26} = \begin{bmatrix}12\\10\\4\\18\end{bmatrix}$$

$$P_5 = \begin{bmatrix}22&20&4&4\\6&24&0&2\\4&0&4&18\\22&24&4&6\end{bmatrix} \times \begin{bmatrix}22\\22\\16\\20\end{bmatrix} \pmod{26}$$

$$= \begin{bmatrix} (22\times 22)+(20\times 22)+(4\times 16)+(4\times 20) \\ (6\times 22)+(24\times 22)+(0\times 16)+(2\times 20) \\ (4\times 22)+(0\times 22)+(4\times 16)+(18\times 20) \\ (22\times 22)+(24\times 22)+(4\times 16)+(6\times 20) \end{bmatrix} (\text{mod } 26)$$

$$= \begin{bmatrix} 484+440+64+80 \\ 132+528+0+40 \\ 88+0+64+360 \\ 484+528+64+120 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 1068 \\ 700 \\ 512 \\ 1196 \end{bmatrix} (\text{mod } 26) = \begin{bmatrix} 2 \\ 24 \\ 18 \\ 0 \end{bmatrix}$$

Step 4: Decryption

Ciphertext: LTSPLHP PIFVORZHFWWQU

Convert each plain text vector into its alphabetic equivalent.

$$P_1 = \begin{bmatrix} 0 \\ 6 \\ 22 \\ 2 \end{bmatrix} = \begin{bmatrix} A \\ G \\ W \\ C \end{bmatrix} \qquad P_2 = \begin{bmatrix} 10 \\ 4 \\ 10 \\ 14 \end{bmatrix} = \begin{bmatrix} K \\ E \\ K \\ O \end{bmatrix} \qquad P_3 = \begin{bmatrix} 0 \\ 14 \\ 4 \\ 22 \end{bmatrix} = \begin{bmatrix} A \\ O \\ E \\ W \end{bmatrix}$$

$$P_4 = \begin{bmatrix} 12 \\ 10 \\ 4 \\ 18 \end{bmatrix} = \begin{bmatrix} M \\ K \\ E \\ S \end{bmatrix} \qquad P_5 = \begin{bmatrix} 2 \\ 24 \\ 18 \\ 0 \end{bmatrix} = \begin{bmatrix} C \\ Y \\ S \\ A \end{bmatrix}$$

LTSPLHP PIFVORZHFWWQU=AGWCKEK OAOEWMKESCYSA

Result and Discussion

Output of existing Hill Cipher algorithm using 3 × 3 key matrix

Using MATLAB code, we input different message with the key matrix 3 × 3 then find the output of execution time of encrypt and decrypt message.

For message "Linear"

Profile Summary

Generated 23-Jul-2023 16:23:34 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
Linear	1	6.212 s	6.212 s	

For message "Algebra"

Profile Summary

Generated 23-Jul-2023 16:26:57 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
Algebra	1	8.098 s	8.098 s	

Profile Summary

Generated 23-Jul-2023 16:28:31 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
Calculus	1	14.039 s	14.039 s	

For message "Astronomy"

Profile Summary

Generated 23-Jul-2023 16:30:52 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
Astronomy	1	16.752 s	16.752 s	

For message "Technology"

Profile Summary

Generated 23-Jul-2023 16:34:11 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
Technology	1	18.415 s	18.415 s	

For message "Integration"

Profile Summary

Generated 23-Jul-2023 16:38:58 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)

For message "Cryptography"

Profile Summary

Generated 23-Jul-2023 16:40:44 using cpu time.

Profile Summary

Generated 23-Jul-2023 16:44:01 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
Steganography	1	23.380 s	23.380 s	

For message "Aeromechanical"

Profile Summary

Generated 23-Jul-2023 16:47:46 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
Aeromechanical	1	29.447 s	29.447 s	

For message "Differentiation"

Profile Summary

Generated 23-Jul-2023 16:50:15 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
Differentiation	1	34.003 s	34.003 s	

Table of existing Hill Cipher using 3 × 3 key matrix input data and corresponding time

We have used the message linear, algebra, calculus, astronomy, technology, integration, cryptography, steganography, aeromechanical and differentiation in the input of the above code of Hill Cipher algorithm using 3 × 3 key matrix and got the execution time of encryption and decryption of respective messages. We have used messages of different length where message length of linear, algebra, calculus, astronomy, technology, integration, cryptography,

steganography, aeromechanical and differentiation are respectively 6, 7, 8, 9, 10, 11, 12, 13, 14 and 15 (Table 1).

Sl.No.	Message	Number of letters	Execution time (in second)
1	Linear	6	6.212
2	Algebra	7	8.098
3	Calculus	8	14.039
4	Astronomy	9	16.752
5	Technology	10	18.415
6	Integration	11	21.542
7	Cryptography	12	22.969
8	Steganography	13	23.38
9	Aeromechanical	14	29.447
10	Differentiation	15	34.003

Table 1. Execution time using 3 × 3 key matrix.

Graphical representation of existing Hill Cipher using 3 × 3 key matrix

Considering execution time as y-axis and message length as x-axis, we represent the above data of Hill Cipher using 3 × 3 key matrix graphically as follows in Figure 2.

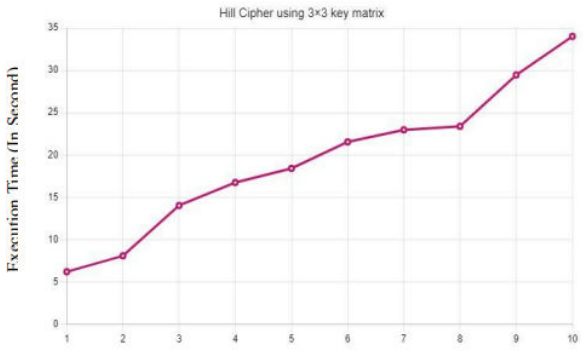

Figure 2. Hill Cipher using 3 × 3 key matrix.

Output of proposed Hill Cipher algorithm using 4 × 4 key matrix

Using MATLAB code, we input different message with the key matrix 4 × 4 then find the output of execution time of encrypt and decrypt message.

For message "Linear

Profile Summary

Generated 23-Jul-2023 17:01:46 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot

Profile Summary

Generated 23-Jul-2023 17:05:54 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
Algebra	1	9.863 s	9.863 s	

For message "Calculus"

Profile Summary

Generated 23-Jul-2023 17:09:49 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
Calculus	1	14.646 s	14.646 s	

For message "Astronomy"

Profile Summary

Generated 23-Jul-2023 17:11:24 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)
Astronomy	1	18.425 s	18.425 s	

Profile Summary

Generated 23-Jul-2023 17:13:42 using cpu time.

Function Name	Calls	Total Time	Self Time*	Total Time Plot (dark band = self time)

Table of proposed Hill Cipher using 4 × 4 key matrix input data and corresponding time

We have used the message linear, algebra, calculus, astronomy, technology, integration, cryptography, steganography, aeromechanical and differentiation in the input of the above code of hill cipher algorithm using 4 × 4 key matrix and got the execution time of encryption and decryption of respective messages. We have used messages of different length where message length of linear, algebra, calculus, astronomy, technology, integration, cryptography, steganography, aeromechanical and differentiation are respectively 6, 7, 8, 9, 10, 11, 12, 13, 14 and 15 (Table 2).

Sl. no.	Message	Number of letters	Execution time (in second)
1	Linear	6	6.88
2	Algebra	7	9.863
3	Calculus	8	14.646
4	Astronomy	9	18.425
5	Technology	10	20.381
6	Integration	11	23.047
7	Cryptography	12	25.919
8	Steganography	13	27.664
9	Aeromechanical	14	33.859
10	Differentiation	15	40.237

Table 2. Execution time using 4 × 4 key matrix.

Graphical representation of proposed Hill Cipher using 4 × 4 key matrix

Considering execution time as y-axis and message length as x-axis, we represent the above data of Hill Cipher using 4 × 4 key matrix graphically as follows in Figures 3 and 4.

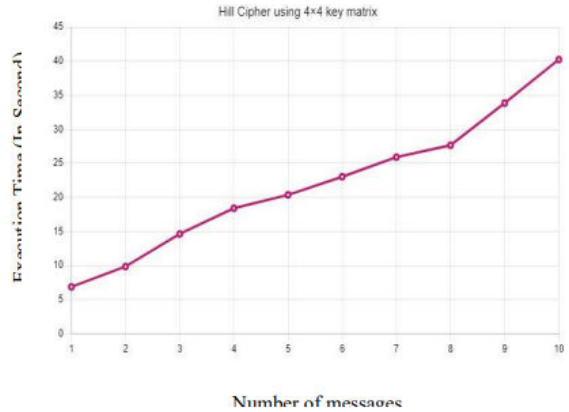

Figure 3. Hill Cipher using 4 × 4 key.

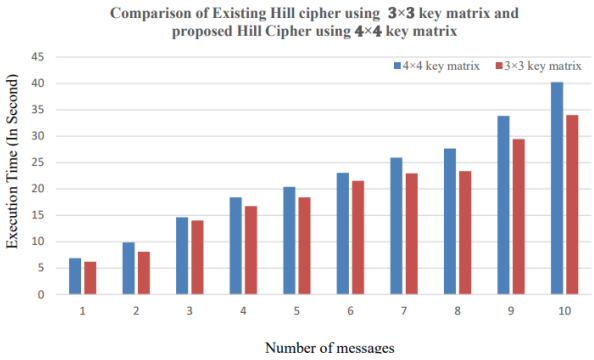

Figure 4. Comparison of Hill Cipher using 3 × 3 and 4 × 4 key matrix.

By analyzing above output of the code and the graph of the both algorithms we conclude that proposed Hill cipher algorithm using 4 × 4 key matrix is more complicated and time consuming than the existing Hill Cipher algorithm using 3 × 3 key matrix which makes it more secure than the existing Hill Cipher algorithm.

Conclusion

In this paper, we have proposed the Hill Cipher algorithm using 4 × 4 key matrix as against the traditional Hill Cipher algorithm of 3 × 3 key matrix. The important aspect of Hill Cipher cryptography is the selection of key matrix and which blocks of key matrix use to generate matrix multiplication. In this technique symmetric key use for both encryption and decryption. The security of Hill cipher cryptosystem is based on the hope that the encryption function is one way and so it is computationally infeasible for an intruder to decrypt a cipher text. As 4 × 4 key matrix is used here, the strength of key is dependent on the inverse of 4 × 4 key matrix. The calculation will be complex it will be more difficult to any intruders to find the original message. In this paper, the algorithms are generated using only small numbers of key matrix but large numbers can be implemented using the code of MATLAB language written in result and discuss section. Hence by comparing the time consumed to encrypt and decrypt a message using traditional and enhanced Hill Cipher we can state that the enhanced Hill Cipher is more efficient and reliable and also not easily breakable by the intruders. In future we may improve or enhance the Hill cipher algorithm more by using more than 3 × 3 or 4 × 4 key matrix. This will make the multiplication of n × n matrix more complicated and our message will be much more secured from the intruders, as they will not be able to easily decipher the Cipher text.

Acknowledgement

We are grateful to the Ministry of Science and Technology, Bangladesh for providing the financial support to work with this article.

References

1. Shwetambari, W., and M. Ujwala. "Development of Matrix for Cryptography." *J Emerg Technol Innov Res* 7 (2020): 112-118.
2. Kumar, R. "A new symmetric key algorithm for modern cryptography." I*ntern J Sci Res Devel* 2 (2014): 302-306.
3. Zeriouh, M., A. Chillali, and Abdelkarim Boua. "Cryptography based on the matrices." *Bol Soc Paran Mat* 3 (2019): 75-83.
4. Sharma, N., and S. Chirgaiya. "A review of modern hill cipher techniques." *JSRD* 1 (2013): 2198-202.
5. Parmar, S. K., and K. C. Dave. "A review on various most common symmetric encryptions algorithms." *J Sci Res Dev* 1 (2013).
6. Sheth, Ravi K., and Sarika P. Patel. "Analysis of cryptography techniques." *Int J Adv Res* 1 (2015).
7. Halunen, Kimmo, and Outi-Marja Latvala. "Cryptography for human senses." VTT Technical Research Centre of Finland, Finland (2018).

How to cite this article: Naime, Jannatul, Muhammad Hanif and A N M Rezaul Karim. "Security System through Matrices in Cryptography." *J Appl Computat Math* 14 (2025): 599