© 2018 IJSRST | Volume 4 | Issue 5 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

A Comparative Study of Matrix Encoding and Hill Cipher Algorithm

E. Mathivadhana*[1], K. Sivasankari[2]
*[1]Department of Mathematics, IFET College of Engineering,Villupuram, Tamilnadu, India
[2]Department of Physics, IFET College of Engineering,Villupuram, Tamilnadu, India

ABSTRACT

Nowadays, the technology is advancing in the field of networking; it gives importance to provide security for the data transmission. Cryptography is one of the technique, provides secure data transmission without losing its confidentiality and integrity. In this paper, discussion is on comparing the importance of encoding and decoding using matrix encoding and Hill cipher techniques. The proposed algorithms proved to be highly efficient in their respective grounds, but there are certain areas that remained open, related to these algorithms, and have not yet been thoroughly discussed. This paper also presents an appropriate future scope related to these open fields.

Keywords : Cryptography, Matrix Encoding And Hill Cipher

I. INTRODUCTION

Cryptography [1] is one such way of transferring the data in a secure way, a single key is for both encryption and decryption purposes. The sharing of this key becomes insecure sometimes. With the development of human intelligence, the art of cryptography has become more complex in order to make information more secure. Number theory [2] plays a role in coding theory, for the implementation and analysis of public-key cryptosystems.

Encryption

Encryption is the process of encoding a message or information in such a way that only authorized parties can access it. Encryption does not itself prevent interference that need to insure that this information is invulnerable to snoop, but denies the intelligible content to a would-be interceptor. For digital data exchange, an encryption scheme usually provides a pseudo-random encryption key generated by an algorithm. It is possible to decrypt the message without controlling the key. A well-designed encryption technique, considerable computational resources and skills are required. An endorsed recipient can easily decrypt the message with the key provided by the creator to recipients but not to unauthorized users.

Decryption

Decryption is the method of encoded or encrypted text or other data and converting it back into plaintext that the computer can read and recognize. It may be accomplished manually or automatically and may also be performed with a set of keys or passwords.

II. METHODS AND MATERIAL

Matrix theory

A set of mn numbers, real or complex, arranged in a rectangular array of m rows and n columns such as

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}_{m \times n}$$

is called a matrix of order m×n. This is often written as $\mathbf{A} = [a_{ij}], 1 \le i \le m, 1 \le j \le n$. The element a_{ij} occurring in the i^{th} row and the j^{th} column is called $(i,j)^{th}$ element of the matrix A.

Invertible matrix

A square matrix $(A)_{n\times n}$ is said to be an invertible matrix[3] if and only if there exists another square matrix $(B)_{n\times n}$ such that $AB=BA=I_n$ .If the square matrix has invertible matrix or non-singular if and only if its determinant value is non-zero. Moreover, if the square matrix A is not invertible or singular if and only if its determinant is zero.

Matrix Encoding & Decoding process:

Encoding Process:

1. The text message of length l can be converted into a stream of Numerals using an accessible scheme for both the sender and the receiver.
2. Place the numerals into a matrix of order m× n where n < m and n is the least such that mxn ≥ l where n depends on the size of the message matrix M.
3. Multiply this message matrix by the encoding key A of size n and get the encoded matrix C.
4. The message matrix can be converted into the stream of numbers that contains the encrypted message and sent to the receiver.

Decoding Process:

1. The encrypted message into a matrix can be placed by the encrypted stream of numbers.
2. Multiply the encoded matrix C with the decoding key B = A^{-1} (The inverse of A) to get back the message matrix M.
3. The message matrix can be converted into a stream of numbers with the help of the originally used method.
4. Convert this stream of numerals in to the text of the original message.

(ii) **Hill Cipher**

The Hill cipher [5][6] is a polygraphic substitution cipher based on linear algebra. Invented by Lester S. Hill in 1929, it was the first polygraphic cipher in which it was practical (though barely) to operate on more than three symbols at once.

Modular arithmetic:

For a positive integer n, two numbers a and b are said to be congruent modulo n, if their difference a – b is an integer multiple of n (that is, if there is an integer k such that a – b = kn). This congruence relation is typically considered when a and b are integers, and is denoted a=b (mod n)

III. RESULTS AND DISCUSSION

Application of matrix encoding

Encryption:

Consider the message

M = **"BE HAPPY ALWAYS"**

and the encoding key matrix A is invertible matrix.

$$A=\begin{bmatrix}-3 & -3 & -4\\ 0 & 1 & 1\\ 4 & 3 & 4\end{bmatrix}$$

From the above message, each letter can be denoted by its position in the following manner:

B	E	*	H	A	P	P	Y	*	A	L	W	A	Y	S
2	5	0	8	1	16	16	25	0	1	12	23	1	25	19

Here, it is used 3×3 matrices, so as to break the enumerated message above into a sequence of 3×1 vectors:

$$\begin{bmatrix}2\\5\\0\end{bmatrix}\quad\begin{bmatrix}8\\1\\16\end{bmatrix}\quad\begin{bmatrix}16\\25\\0\end{bmatrix}\quad\begin{bmatrix}1\\12\\23\end{bmatrix}\quad\begin{bmatrix}1\\25\\19\end{bmatrix}$$

The above sequence can be written in the columns of a matrix as follows:

$$\begin{bmatrix}2 & 8 & 16 & 1 & 1\\ 5 & 1 & 25 & 12 & 25\\ 0 & 16 & 0 & 23 & 19\end{bmatrix}$$

Then the vectors of column of a matrix can be multiplied by the encoding matrix as follows:

$$\begin{bmatrix}-3 & -3 & -4\\ 0 & 1 & 1\\ 4 & 3 & 4\end{bmatrix}\begin{bmatrix}2 & 8 & 16 & 1 & 1\\ 5 & 1 & 25 & 12 & 25\\ 0 & 16 & 0 & 23 & 19\end{bmatrix}$$

Apply matrix multiplication, and then the resultant matrix is the encoded message as given below:

$$\begin{bmatrix} -21 & -91 & -123 & -131 & -154 \\ 5 & 17 & 25 & 35 & 44 \\ 23 & 99 & 139 & 132 & 155 \end{bmatrix}$$

The encoded message is transmitted in the following linear form:

$$C = -21, 5, 23, -91, 17, 99, -123, 25, 139, -131, 35, 132, -154, 44, 155$$

Decryption:

To decode the message, the ciphertext C is converted into the plaintext.

$$C = -21, 5, 23, -91, 17, 99, -123, 25, 139, -131, 35, 132, -154, 44, 155$$

The above string can be written in the sequence of column of matrix.

$$\begin{bmatrix} -21 & -91 & -123 & -131 & -154 \\ 5 & 17 & 25 & 35 & 44 \\ 23 & 99 & 139 & 132 & 155 \end{bmatrix}$$

The decoding matrix B is the inverse of the encoding matrix A as given below:

$$B = \begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix}$$

To decode the message, the matrix multiplication is performed with the sequence of column matrix and the decoding matrix B.

$$\begin{bmatrix} 1 & 0 & 1 \\ 4 & 4 & 3 \\ -4 & -3 & -3 \end{bmatrix} \begin{bmatrix} -21 & -91 & -123 & -131 & -154 \\ 5 & 17 & 25 & 35 & 44 \\ 23 & 99 & 139 & 132 & 155 \end{bmatrix}$$

The resultant matrix is

$$\begin{bmatrix} 2 & 8 & 16 & 1 & 1 \\ 5 & 1 & 25 & 12 & 25 \\ 0 & 16 & 0 & 23 & 19 \end{bmatrix}$$

The columns of this matrix can be written in linear form that gives the original message:

2	5	0	8	1	16	16	25	0	1	12	23	1	25	19
B	E	*	H	A	P	P	Y	*	A	L	W	A	Y	S

The original message M = **"BE HAPPY ALWAYS"**

Application of Hill Cipher:

Encryption:

Consider the Message & Key

M = **"BEHAPPYALWAYS"**

K=BACKUPS

$$K = \begin{bmatrix} 2 & 1 & 3 \\ 11 & 21 & 16 \\ 19 & 0 & 0 \end{bmatrix}$$

From the above message, each letter can be denoted by its position in the following manner:

B	E	H	A	P	P	Y	A	L	W	A	Y	S	*	*
2	5	8	1	16	16	25	1	12	23	1	25	19	0	0

Here, it is used 3×3 matrices, so as to break the enumerated message above into a sequence of 3×1 column vectors:

$$\begin{bmatrix} B \\ E \\ H \end{bmatrix} \begin{bmatrix} A \\ P \\ P \end{bmatrix} \begin{bmatrix} Y \\ A \\ L \end{bmatrix} \begin{bmatrix} W \\ A \\ Y \end{bmatrix} \begin{bmatrix} S \\ * \\ * \end{bmatrix}$$

Then convert into numeric column vectors

$$\begin{bmatrix} 2 \\ 5 \\ 8 \end{bmatrix} \begin{bmatrix} 1 \\ 16 \\ 16 \end{bmatrix} \begin{bmatrix} 25 \\ 1 \\ 12 \end{bmatrix} \begin{bmatrix} 23 \\ 1 \\ 25 \end{bmatrix} \begin{bmatrix} 19 \\ 27 \\ 27 \end{bmatrix}$$

Then the vectors of each column of a matrix can be multiplied by the encoding matrix& take mod 27 as follows:

i.e. $C = K * M \bmod 27$

$$\begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \begin{bmatrix} 2 \\ 5 \\ 8 \end{bmatrix} \bmod 27 = \begin{bmatrix} 6 \\ 12 \\ 11 \end{bmatrix} = \begin{bmatrix} F \\ L \\ K \end{bmatrix}$$ and so on

Finally we get,

$$\begin{bmatrix} F \\ L \\ K \end{bmatrix} \begin{bmatrix} L \\ I \\ S \end{bmatrix} \begin{bmatrix} F \\ B \\ P \end{bmatrix} \begin{bmatrix} N \\ Z \\ E \end{bmatrix} \begin{bmatrix} K \\ T \\ J \end{bmatrix}$$

The ciphertext is **"FLKLISFBPNZEKTJ"**

Decryption:

The ciphertext is **"FLKLISFBPNZEKTJ"**

& the shared key $K = \begin{bmatrix} 2 & 1 & 3 \\ 11 & 21 & 16 \\ 19 & 0 & 0 \end{bmatrix}$

Find the multiplicative inverse modulo 27 for the shared key.

Then $K^{-1} = \begin{bmatrix} 0 & 0 & 10 \\ 10 & 15 & 13 \\ 24 & 4 & 25 \end{bmatrix}$

Now the ciphertext can be converted in 3×1column vector

$$\begin{bmatrix} F \\ L \\ K \end{bmatrix} \quad \begin{bmatrix} L \\ I \\ S \end{bmatrix} \quad \begin{bmatrix} F \\ B \\ P \end{bmatrix} \quad \begin{bmatrix} N \\ Z \\ E \end{bmatrix} \quad \begin{bmatrix} K \\ T \\ J \end{bmatrix}$$

Then convert into numeric column vectors

$$\begin{bmatrix} 6 \\ 12 \\ 11 \end{bmatrix} \quad \begin{bmatrix} 12 \\ 9 \\ 19 \end{bmatrix} \quad \begin{bmatrix} 6 \\ 2 \\ 16 \end{bmatrix} \quad \begin{bmatrix} 14 \\ 26 \\ 5 \end{bmatrix} \quad \begin{bmatrix} 11 \\ 20 \\ 10 \end{bmatrix}$$

Then the vectors of each column of a matrix can be multiplied by the encoding matrix& take mod 27 as follows:

i.e. $P = K^{-1} * C \bmod 27$

$$\begin{bmatrix} 3 & 10 & 20 \\ 20 & 9 & 17 \\ 9 & 4 & 17 \end{bmatrix} \begin{bmatrix} 6 \\ 12 \\ 11 \end{bmatrix} \bmod 27 = \begin{bmatrix} 2 \\ 5 \\ 8 \end{bmatrix} = \begin{bmatrix} B \\ E \\ H \end{bmatrix}$$ and so on.

Finally we get,

$$\begin{bmatrix} B \\ E \\ H \end{bmatrix} \quad \begin{bmatrix} A \\ P \\ P \end{bmatrix} \quad \begin{bmatrix} Y \\ A \\ L \end{bmatrix} \quad \begin{bmatrix} W \\ A \\ Y \end{bmatrix} \quad \begin{bmatrix} S \\ * \\ * \end{bmatrix}$$

The plaintext is **"BE HAPPY ALWAYS"**

IV. CONCLUSION

The matrix theory is one type of code, which is extremely difficult to break the message. The large matrix is also used to encrypt or decrypt the message, but it is not secure. Cryptanalysis of an intercept encrypted using the Hill Cipher is certainly possible, especially for small key sizes. Here encoding and decoding using matrix encoding and Hill cipher techniques are studied, in that Hill cipher techniques is more secure than matrix encoding.

V. REFERENCES

[1]. Stallings, W. "Cryptography and Network Security" 4th edition, Prentice Hall (2015).

[2]. Petersen, K., "Notes on Number Theory and Cryptography" (2000).

[3]. Camp, D. R.. "Secret codes with matrices". Mathematics Teacher, 78(9), 676–680 (1985).

[4]. Thangarasu.N, "Encryption Using Lester Hill Cipher Algorithm", International Journal of Innovative Research in Advanced Engineering (IJIRAE). (December 2015) ISSN: 2349-2763 Issue 12, Volume 2.

[5]. Bibhudendra Acharya, "Image Encryption Using Advanced Hill Cipher Algorithm", Int. J. of Recent Trends in Engineering and Technology, (Nov 2009) Vol. 1, No. 1.