An Application of Hill Cipher by Using Modular Matrices

Santosh Kumar Sharma
Amity School of Engineering and Technology, Amity University Madhya Pradesh, Gwalior -474001, sksharma1@gwa.amity.edu

Abstract-In this paper; I present the encryption and decryption of the English text using the techniques of Hill cipher by using 3X3 matrices. This paper presents the numerous examples to describe the encryption and decryption process by using the process of modular matrices.

***Key Words*-Hill Cipher, Encryption, Decryption**

I. INTRODUCTION

In the classical cryptography it is evidence that Caesar employed the method of cryptography, where each letter is transformed by one specific substitute letter, which is sometimes, is called the Caesar cipher [1] in the honor of Caesar. When Bob encrypts the message send by Alice using the Caesar cipher substitution and allows to Eve's to found it. Then it's very easy for Eve's to decrypts the message by applying all possible 26 shifts. In this simple substitution cipher equivalent ciphertext letter writes underneath the plaintext letter as describes below

Plaintext: A B C D E F G H I J K L M N
O P Q R S T U V W X Y Z

Ciphertext: D E F G H I J K L M N O P Q
R S T U V W X Y Z A B C

Consider the plaintext message

MEET ME TOMORROW

is transferred into the ciphertext message as

PHHW PH WRPRUURZ

The Caesar cipher can easily describes by congruence theory to assign the numerical values corresponding to each letter represented as:

A B C D E F G H I
0001 02 0304 050607 08
J K L M N O P Q R
09 101112 13 14 15 16 17
S T U V W X Y Z
1819 20 2122 23 24 25

If P_T represents the digit equivalent to plaintext letter and $C_T$represents the digit equivalent to ciphertext letter, then encryption process is describe by the following congruence

$$C_T \equiv P_T + 3\ (mod\ 26)$$

And the plaintext is recovered by the reverse process in term of congruence $P_T \equiv C_T - 3\ (mod\ 26)$

$$\equiv C_T + 23\ (mod\ 26)$$

The encryption scheme where each letters of the plaintext is substituted by the corresponding cipher letters is referred as mono alphabetic cipher.

To improve the simple mono alphabetic cipher techniques, polyalphabetic cipher have introduced in which a plaintext letter is represented by more than one equivalent cipher text letters by the use of some sort of key.

Vigenere cipher most important example of polyalphabetic cipher, which was introduced by Vigenere.

In the Vigenere polyalphabetic cipher[2], alphabets are numbered from A = 00 to Z = 25 and the corresponding letters of the keyword is repeated beneath the plaintext message as according to length of it. Then the cipher text message is obtained by adding each plaintext digit to corresponding number of key just beneath on it by modulo 26.

The Vigenere cipher can be illustrated with the help of keyword PEACE which equivalent numerical version is 15 04 00 02 04. By repeating this sequence beneath to digital equivalence of the plaintext message

GIVE YOUR BEST

That produces in the digital form of

06 08 21 04 24 14 20 17 01 04 18 19
15 04 00 02 04 15 04 00 02 04 15 04

By addition modulo 26 the digits corresponding to plaintext message are given below:
21 12 21 06 02 03 24 17 03 08 07 23
is converted to the cipher text as
VMVG CDYR DIHX
It is noticed that the same letters in plaintext are represented by distinct letters in ciphertext.

II.APPLICATION OF HILL ALGORITHM

In 1929 Lester Hill [1] further generalized the polyalphabetic cipher to ensure the greater security in polyalphabetic cipher. The Hill cipher was the first cryptographic technique based on linear algebra. In the Hill algorithm first the plaintext message divided into the form of block of some particular number of letter say *n.* The last block is possibly filling out by introducing some dummy letters. Then the plaintext is encrypted in block to block substitution in the form of a system of n linear congruences in term of n variables in which the numerical value corresponding to each letter are assigned as

A = 00 to Z = 25

For n = 3, the simplest form of Hill algorithm takes successively 3 letters and transforms the numerical values of $P_1P_2P_3$ in the form of equivalent cipher text number $C_1C_2C_3$ as

$$C_1 \equiv (T_{11}P_1 + T_{21}P_2 + T_{31}P_3) mod\ 26$$
$$C_2 \equiv (T_{12}P_1 + T_{22}P_2 + T_{32}P_3) mod\ 26$$
$$C_3 \equiv (T_{13}P_1 + T_{23}P_2 + T_{33}P_3) mod\ 26$$

The above system of the linear congruences may be expressed in the form of row vectors and matrices as

$$[C_1 \quad C_2 \quad C_3] \equiv [P_1 \quad P_2 \quad P_3] \begin{bmatrix} T_{11} & T_{12} & T_{13} \\ T_{21} & T_{22} & T_{23} \\ T_{31} & T_{32} & T_{33} \end{bmatrix} mod\ 26$$

This may be describes in form of matrix congruence as

$$C_T \equiv P_T T mod\ 26$$

Where C_T and P_T are the row vectors of length 3 and T is a 3 × 3 matrix represents encryption key.
For the illustration of Hill algorithm, for example consider the plaintext

ANY ONE CAN

And the encryption key

$$T = \begin{bmatrix} 13 & 3 & 16 \\ 23 & 18 & 20 \\ 11 & 1 & 3 \end{bmatrix}$$

The digital equivalence of plaintext message is
00 13 24 14 13 04 02 00 13
Now divide it into blocks of the letters, that constitutes the following vectors$[00 \quad 13 \quad 24]$, $[14 \quad 13 \quad 04]$ and $[02 \quad 00 \quad 13]$.
Multiplying each vectors by invertible matrix T using multiplication modulo 26. The vectors yields as

$$[00 \quad 13 \quad 24]T$$
$$= [563 \quad 258 \quad 338] mod\ 26$$
$$= [17 \quad 24 \quad 00]$$

the corresponding digital equivalence of this vector is RYA.
Continuing in similar fashion, we get

$$[14 \quad 13 \quad 05]T$$
$$= [536 \quad 281 \quad 499] mod\ 26$$
$$= [16 \quad 21 \quad 05]$$

And

$$[02 \quad 00 \quad 13]T$$
$$= [169 \quad 19 \quad 91] mod\ 26$$
$$= [13 \quad 19 \quad 13]$$

The ciphertext for the entire plaintext is RYA QVF NTN.
Decryption requires finding inverse of the matrix T .We may obtain

$$DetT = -1905 \equiv 19\ (mod\ 26)$$

The inverse of matrix T, T^{-1} can obtained by the formula

$$T^{-1} = \frac{Adj.T}{DetT}$$

We can calculate the inverse as

$$T^{-1} = \begin{bmatrix} 10 & 25 & 14 \\ 23 & 1 & 18 \\ 25 & 12 & 21 \end{bmatrix}$$

This is demonstrate as

$$T.T^{-1} = \begin{bmatrix} 13 & 3 & 16 \\ 23 & 18 & 20 \\ 11 & 1 & 3 \end{bmatrix} \begin{bmatrix} 10 & 25 & 14 \\ 23 & 1 & 18 \\ 25 & 12 & 21 \end{bmatrix}$$

$$= \begin{bmatrix} 599 & 520 & 572 \\ 1144 & 833 & 1066 \\ 208 & 312 & 235 \end{bmatrix} mod\ 26$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

After applying the matrix $T^{-1}$to the ciphertext, the plaintext is recovered as

$$P_T \equiv C_T T^{-1} mod\ 26$$

For the generation of keymatrix for encryption and decryption, [3-7] be referred.

II. CONCLUSION

The present paper describes the process of encryption and decryption of English texts by using Hill cipher algorithm on the basis of 3X3 modular matrices. There are multiple ciphertext letters corresponding to plaintext letters, which are uniquely represented according to the selection of keyword. That shows the strength of this cipher.

REFERENCES

[1] J. Hoffstein, J. Pipher, and J.H. Silverman, “ An Introduction to Mathematical Cryptography” Springer (2008).

[2] W. Stalling, “Cryptography and Network Security-Principles and Practice” 3rd Edition, Prentice Hall (2003).

[3] A.N. Borodzhieva, “ MS Excel- Based Application for Encryption and Decryption of English Texts with the Hill Cipher on the Basis of 3X3 Matrix” Proc. XXV International Scientific Conference Electronics- ET 2016, September 12- 14, 2016, Sozopol, Bulgaria.

[4] P.E. Coggins and T. Glatzer, “ An Algorithm for a Matrix Based Enigma Encoder from a Variation of the Hill Cipher as as Application of 2X2 Matrices” 2020, PRIMUS, 30(1), pp.1-18.

[5] J.R. Paragos, A. M. Sison and R. P. Medina” Hill Cipher Modification: A Simplified Approach” 2019, IEEE 11th International Conference on Communication Software and Networks, ICCSN2019, 8905360, pp. 821-825.

[6] K. Mani and A.B. Begum, “ Generation of Keymatrix for Hill Cipher Encryption using Quadratic Form” 2019, International Journal of Scientific and Technology Research” 8(10), pp. 964-968.

[7] K. Mani and M. Viswambri, “Generation of Key Matrix for Hill Cipher using Magic Rectangle” 2017, Advances in Computational Sciences and Technology, 10(5), pp. 1081-1090.