RESEARCHERID
THOMSON REUTERS

[Kumar, 6(6): June 2019] ISSN 2348 – 8034
IDSTM-2019 Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

APPLICATION OF MATRIX IN NETWORK SYSTEM FOR SECURITY PURPOSE

Vijai Kumar[*1] & Yogesh Arora[2]
[*1&2]Applied sciences and Humanities, Ganga Technical Campus, India

ABSTRACT

The evolution of science and technology has changed the world. In order to communicate with others we are very much dependent on network system. When we want our message to keep confidential then Cryptography, the art of encryption and decryption, with the help of matrices is used to secure the transmitted message. It plays a significance role in cellular communications such as e-commerce, computer passwords, pay-tv, sending emails, ATM cards, transmitted funds and digital signature. Now a day cryptography is consider as branch of computer science as well as mathematics. Basically cryptography is divided into two parts, one is symmetry and other is asymmetry. Both has own pros and cons.

KEYWORDS: Matrix, cryptography, symmetry, asymmetry, encrypt, decrypt

I. INTRODUCTION

Cryptography with the help of Matrix

The encryption process:-In fact, we can summarize the encryption which is the process of converting plaintext into ciphertext in four basic steps:

- Choose an (n×n) matrix *A* which is invertible, where *n* here maybe depends on the length of the message that needs to be encrypted.
- Change each plaintext to its numerical value, by using the table below:
- Form the (n×1) column vector *P*, having these numerical values as its entries.
  A B C D E F G H I J K L M
  1 2 3 4 5 6 7 8 9 10 11 1213
  N O P Q R S T U V W X Y Z space
  14 15 161718 19 20 21 22 2324 25 26 0
- Get each ciphertext vector *C* by multiplying *A* with *P*, and convert each entry of the ciphertext vector to its letter in the alphabet. The encryption algorithm of this method is:
  $C \equiv AP \bmod N$. where *C* is the column vector of the numerical values of ciphertext, *P* is the column vector of the numerical values of plaintext, *A*an ($n \times$ n) matrix, is the key of the algorithm, (this matrix must be invertible because we need the inverse of this matrix for the decryption process), and *N* is the number of letters of the alphabet used in the cryptography.

The decryption process The decryption which is the process of converting the ciphertext into plaintext could also be summarized in four basic steps:

- Get the inverse of the matrix *A;* say A^{-1}.
- Change each ciphertext to its numerical value.
- Put each ciphertext in a (*n*×1) column vector say*C*.
- Get each plaintext vector by multiplying A^{-1} with *C*, and convert each plaintext vector to its letter in the alphabet. The decryption algorithm of this method is:
  $P \equiv A^{-1}C \bmod N$. Where$A^{-1}$is the inverse of the matrix *A*.

In general, if $A = \begin{pmatrix} a11 & \cdots & a1n \\ \vdots & \ddots & \vdots \\ an1 & \cdots & ann \end{pmatrix}$ and P = $\begin{pmatrix} p11 \\ \\ \\ pn1 \end{pmatrix}$ then, in the encryption process, we get

ISSN 2348 – 8034
Impact Factor- 5.070

$C \equiv AP \bmod N$.i.e $\begin{pmatrix} c11 \\ \\ cn1 \end{pmatrix} \equiv \begin{pmatrix} a11 & \cdots & a1n \\ \vdots & \ddots & \vdots \\ an1 & \cdots & ann \end{pmatrix} \begin{pmatrix} p11 \\ \\ pn1 \end{pmatrix}$.Here when the size of the matrix *A* increases, or in other words when *n* increases, we will have the following advantages:

- 1. The cryptography process will be more complex and more difficult to decode.
- 2. The number of column vectors will decrease and we can encode any message consisting for example of 7 letters by using a (7×7) matrix in only one step. But there is one problem here, that is, it's not easy to get the inverse of the matrix used in the encryption process as *n* increases. Below, we give several other ways of using Hill cipher technique for encryption.

- **Using More Than One Key in Hill Cipher** In the Hill cipher, since the key used to encode or decode any message is a matrix, we can use the associative property of matrices to make the coding process more complex and more secure. Therefore; if we have two invertible matrices *A,B*, and a plaintext column vector *P* , then the general case is explained below.
- Given $A = \begin{pmatrix} a11 & \cdots & a1n \\ \vdots & \ddots & \vdots \\ an1 & \cdots & ann \end{pmatrix}$,$B = \begin{pmatrix} b11 & \cdots & b1n \\ \vdots & \ddots & \vdots \\ bn1 & \cdots & bnn \end{pmatrix}$ the encryption algorithm is:$C \equiv ABP \equiv A(BP) = \begin{pmatrix} a11 & \cdots & a1n \\ \vdots & \ddots & \vdots \\ an1 & \cdots & ann \end{pmatrix} \begin{pmatrix} b11 & \cdots & b1n \\ \vdots & \ddots & \vdots \\ bn1 & \cdots & bnn \end{pmatrix} \begin{pmatrix} p11 \\ \\ pn1 \end{pmatrix} = \begin{pmatrix} c11 \\ \\ cn1 \end{pmatrix} \bmod N.$

The decryption algorithm, on the other hand, is $P \equiv (AB)^{-1}C \equiv B^{-1}A^{-1}C = B^{-1}(A^{-1}C) \bmod N$.
In this way, we got a new cipher column vector *C*, because the matrix multiplication operation is an associative. Here, we also use the fact that $(XY)^{-1} = Y^{-1}X^{-1}$.
Generalizing the Above Algorithm In this case we can use *n* number of invertible matrices to encode or decode any message and the steps will be the same. This means that, if we have the invertible matrices *A, B, C, M* ….....,then the encryption algorithm will be:
Hence the decryption algorithm is:

Using The Affine Cipher Algorithm in Hill Cipher We can use the Affine cipher technique to make the Hill cipher more complex. Encryption algorithm here is given as:
where *A* is an invertible matrix and *B* is a column vector like the vectors *C* and *P*. For the decryption:

Using the Affine Cipher Algorithm in Hill Cipher with More Than One Key By using the following algorithm to encrypt any message we will get more complex process:
$C \equiv (AB\ldots\ldots M)P + K \pmod N$

$$\begin{pmatrix} c11 \\ \\ cn1 \end{pmatrix} \equiv \begin{pmatrix} a11 & \cdots & a1n \\ \vdots & \ddots & \vdots \\ an1 & \cdots & ann \end{pmatrix} \begin{pmatrix} b11 & \cdots & b1n \\ \vdots & \ddots & \vdots \\ bn1 & \cdots & bnn \end{pmatrix} \ldots\ldots \begin{pmatrix} m11 & \cdots & m1n \\ \vdots & \ddots & \vdots \\ mn1 & \cdots & mnn \end{pmatrix} \begin{pmatrix} p11 \\ . \\ . \\ pn1 \end{pmatrix} + \begin{pmatrix} k11 \\ . \\ . \\ kn1 \end{pmatrix} \bmod N.$$

The decryption here works as below;
$P \equiv (AB\ldots\ldots M)^{-1}(C-K) \pmod N$

Here are some examples now to illustrate the above facts.

3.5 Examples

Example 3.5.1 Encode the message **(I am Vijay)** by using Hill cipher algorithm where the matrix is

$$A=\begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}$$

Solution. First use the table below to convert letters in the message to their numerical values.

A B C D E F G HIJ KL M

1 2 3 4 5 6 7 89 10 11 12 13

N O P Q R S T U V W X Y Z

14 15 16 17 18 19 20 21 22 23 24 25 26 0 .Put also number 0 for the space between words. Group the plaintext letters into pairs and add 0 to fill out the last pair:

I am Vijay converted by numbers as 9 0 113 0 22910125 then;

$C \equiv AP \bmod N$

$$\begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}9\\ 0\end{pmatrix}=\begin{pmatrix}18\\ 9\end{pmatrix} \bmod 26$$

$$\begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 13\end{pmatrix}=\begin{pmatrix}15\\ 1\end{pmatrix} \bmod 26$$

$$\begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0\\ 22\end{pmatrix}=\begin{pmatrix}22\\ 0\end{pmatrix} \bmod 26$$

$$\begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}9\\ 10\end{pmatrix}=\begin{pmatrix}28\\ 9\end{pmatrix}=\begin{pmatrix}2\\ 9\end{pmatrix} \bmod 26$$

$$\begin{pmatrix}2 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 25\end{pmatrix}=\begin{pmatrix}27\\ 1\end{pmatrix}=\begin{pmatrix}1\\ 1\end{pmatrix} \bmod 26$$

Now the new message becomes :(RIOAV BIAA)

Let us convert it into original message with the help of inverse matrix $A^{-1}=\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}$

The algorithm for decryption matrix is

$P \equiv A^{-1}C \pmod N$

$$\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}18\\ 9\end{pmatrix}=\begin{pmatrix}9\\ 0\end{pmatrix} \bmod 26$$

$$\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}15\\ 1\end{pmatrix}=\begin{pmatrix}1\\ 13\end{pmatrix} \bmod 26$$

$$\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}22\\ 0\end{pmatrix}=\begin{pmatrix}0\\ 22\end{pmatrix} \bmod 26$$

$$\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}2\\ 9\end{pmatrix}=\begin{pmatrix}9\\ -16\end{pmatrix}=\begin{pmatrix}9\\ 10\end{pmatrix} \bmod 26$$

$$\begin{pmatrix}0 & 1\\ 1 & -2\end{pmatrix}\begin{pmatrix}1\\ 1\end{pmatrix}=\begin{pmatrix}1\\ -1\end{pmatrix}=\begin{pmatrix}1\\ 25\end{pmatrix} \bmod 26$$

Now these numbers (90113022910125) has a hidden message i.e. I am Vijay.

ISSN 2348 – 8034
Impact Factor- 5.070

II. CONCLUSION

We observe that if we select a matrix of big size then the message will be hard to break.

REFERENCE

1. *Charles C. Pinter, A Book of Abstract Algebra, Second Edition, QA162.P56, 1990.*
2. *I. H. Sheth, Abstract Algebra, 2002.*
3. *Joseph. A. Gallian, Contemporary Abstract Algebra, Sixth Edition, 2006.*
4. *Howard Anton-Chris Rorres, Elementary Linear Algebra Applications Version, Seven Edition, 1994.*
5. *P. B. Bhattacharya-S. K.Jain-S. R. Nagpaul, First Course in Linear Algebra, 1983.*
6. *N. S. Gopalakrishnan, University Algebra, Second Edition, June 1998.*
7. *Gareth A. Jones and J. Mary Jones, Elementary Number Theory, QA241, J62, 1998.*
8. *Neal. Koblitz, A Course in Number Theory and Cryptography, second Edition, 1991.*
9. *Lecture Note by Victor, Adamchik, Full 2005.*
10. *Lecture Note in Network Data Security by Rza, Bashirov.*
11. *Lester S. Hill, Cryptography in an Algebraic Alphabet, The American Mathematical Monthly Vol.36, June–July 1929, pp. 306–312*