www.ijraset.com
IC Value: 13.98

Volume 4 Issue IV, April 2016
ISSN: 2321-9653

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

# Application of Non-Singular Matrices in Encryption and Decryption text of Cryptography

Babita Bist Ramola
*Asstt. Professor, Deptt. of Mathematics, S. D. College(Lahore), Ambala Cantt.*

***Abstract: Cryptography, the science of encrypting messages in secret codes, has played an important role in securing information since past times. The basic idea of cryptography is that information can be encoded using an encryption scheme and can be decoded by anyone who knows about the scheme. There are lots of encryption schemes ranging from very simple to very complex. Most of them are mathematical in nature. Since matrices have unique and very powerful concept and can be easily understood so it could be applied as an efficient way for encrypting and storing text. This article describes some of the techniques of cryptography using matrices. The technique is very simple and can be easily use for encryption of messages confidentially but also not so easy to break if someone does not know the key. The encryption system uses different type of matrices to store the text entered by the sender in the form of their positions and their inverses for decoding the text.***

***Key words: Cryptography, encryption, matrices, inverse***

## I. INTRODUCTION

People all over the world are engaged in communication through internet every day. It is very important to protect our essential data from unauthorized users. The main challenge in data communication is how to keep data secure against unlawful interference. One of the common serious attacks occurs when an unauthorized party can access to read modify and protected data. The data transferred from one system to another system over the public network can be protected by means of encryption. Each encryption creates cipher text that can be decrypted into plaintext. Cryptology has a long and rich history with many interesting basic cipher schemes that make possible to deepen into different mathematical topics.

Many papers try to use and improve matrix cryptography to solve this challenge of security. It requires the key matrix and its inverse in encryption and decryption respectively [1] [2]. But what happens when the inverse of the matrix does not exist? If it is not so, then how the decryption takes place. In order to overcome all the above discussed difficulties a number of non singular matrices-orthogonal, Hilbert and quadratic forms had been used in the past.

## II. BASICS

The cryptography using matrices basically involves encryption using a non-singular key matrix and decryption using inverse of key matrix.

Consider text message “ AMBALA”

To every letter we will associate a number. The easiest way to do that is to associate 0 to a blank or space, 1 to A, 2 to B, etc...

So our message string is

| A | M | B | A | L | A |
|---|---|---|---|---|---|
| 1 | 13 | 2 | 1 | 12 | 1 |

And corresponding message matrix is

$$A = \begin{pmatrix} 1 & 13 \\ 2 & 1 \\ 12 & 1 \end{pmatrix}$$

of order 3×2 (n<m)

To protect this message, we encode it by multiplying the message matrix with an encoding matrix or key (an arbitrarily chosen non singular matrix )

$$K = \begin{pmatrix} 4 & 3 \\ 2 & 2 \end{pmatrix}$$

©IJRASET: All Rights are Reserved

The resulting matrix is

$$X = AK = \begin{pmatrix} 1 & 13 \\ 2 & 1 \\ 12 & 1 \end{pmatrix} \begin{pmatrix} 4 & 3 \\ 2 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 30 & 29 \\ 10 & 8 \\ 50 & 38 \end{pmatrix}$$

The encoded numeric message is

30 29 10 8 50 38

Here plain text (original message) is in lowercase and cipher text (encoded message) is in uppercase.

Now after receiving the encoded message, receiver can decode it if knows the key which is inverse of encoding matrix

$$K^{-1} = \begin{pmatrix} 1 & -1.5 \\ -1 & 2 \end{pmatrix}$$

So the encoded message is again decoded as

$$M = XK^{-1} = \begin{pmatrix} 30 & 29 \\ 10 & 8 \\ 50 & 38 \end{pmatrix} \begin{pmatrix} 1 & -1.5 \\ -1 & 2 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 13 \\ 2 & 1 \\ 12 & 1 \end{pmatrix}$$

The Original message is obtained as

1 13 2 1 12 1
A M B A L A

But when the length of the text message is too large, the order of message matrix becomes high leading to high order encoding matrix. So the diagonal matrices induced from Quadratic forms [3] are preferred for encoding long text as their inverses can be easily calculated.

Consider the message : "HAPPY NEW YEAR"

Considering the standard codes as 0 for space , 1 for A, 2 for B and so on we have

H A P P Y N E W Y E A R
8 1 16 16 25 0 14 5 23 0 25 5 1 18 as original numeric message.

And the corresponding message matrix is

$$A = \begin{pmatrix} 8 & 1 & 16 \\ 16 & 25 & 0 \\ 14 & 5 & 23 \\ 0 & 25 & 5 \\ 1 & 18 & 0 \end{pmatrix}$$

of order 5 × 3.

Let we consider Quadratic form as $2x_1^2 + x_2^2 + x_3^2 + 2x_1x_2 - 4x_2x_3 – 2x_1x_3$

And the matrix of above form is

$$B = \begin{pmatrix} 2 & 1 & -1 \\ 1 & 1 & -2 \\ -1 & -2 & 1 \end{pmatrix}$$

©IJRASET: All Rights are Reserved

And corresponding canonical form is $-y_1^2 + y_2^2 + 4y_3^2$ and the diagonal matrix is given by

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix}$$

we consider above matrix as encoding matrix

$$E = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix}$$

The encoded matrix is given by

$$K = AE = \begin{pmatrix} 8 & 1 & 16 \\ 16 & 25 & 0 \\ 14 & 5 & 23 \\ 00 & 25 & 5 \\ 1 & 18 & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 4 \end{pmatrix}$$

$$= \begin{pmatrix} -8 & 1 & 64 \\ -16 & 25 & 0 \\ -14 & 5 & 92 \\ 0 & 25 & 20 \\ -1 & 18 & 0 \end{pmatrix}$$

So the encoded numeric message is
-8 1 64 -16 25 0 -14 5 92 0 25 20 -1 18 0
Now to decode the message, receiver can use inverse of the encoding matrix as

$$D = KE^{-1} = \begin{pmatrix} -8 & 1 & 64 \\ -16 & 25 & 0 \\ -14 & 5 & 92 \\ 0 & 25 & 20 \\ -1 & 18 & 0 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1/4 \end{pmatrix}$$

$$= \begin{pmatrix} -8 & 1 & 16 \\ -16 & 25 & 0 \\ -14 & 5 & 23 \\ 0 & 25 & 5 \\ -1 & 18 & 0 \end{pmatrix}$$

And the original message is obtain

8 1 16 16 25 0 14 5 23 0 25 5 1 18 0
H A P P Y  N E W  Y E A R

The orthogonal matrices [4] are also used to generate key matrix of classical Hill cipher to increase the security of communication text. The improvisation of cipher text becomes relatively more secure due to the utilization of orthogonal matrix.

The concept of one to one mapping matrix [5] is used for encryption where a column vector is introduced and defined the matrix elements by 1 or 0. The main concept in this method is to substitute row 1 by row n, row 2 by row n - 1. . . row n by row 1, and so on. Thus the one-to-one mapping matrix can be used to encode and decode the secret data.

Raja and Chakravarthy [6] used Hilbert matrices to encrypt the secret messages. The idea behind choosing the Hilbert matrices is that they are always invertible and have integer inverses .If the order is known then the inverse can be easily found and it is very difficult to find the inverse if the order is unknown. As the size of the Hilbert matrix is kept secret (known only to sender and receiver) because of the instability and it is difficult and practically impossible for anyone to retrieve the message without knowing the order.

## III. CONCLUSION

Matrices are well known tool for storage of huge data. In this paper, many of the important encryption techniques have been presented in order to make familiar with the various encryption schemes used in encrypting the data using different matrices. Every scheme has advantages and disadvantages based on their techniques which are mainly based on finding the inverse of key matrix.

## REFRENCES

[1] http://www. richland.edu / james /lecture /.../matrices/applications.html

[2] http:// aix1.uottawa.ca/~jkhoury/cryptography.htm

[3] Vasta B.S., Vasta Suchi..,Theory of Matrices.,Third edition., New Age International , India., 2010.

[4] ] Khan F. H., Shams R., “Hill Cipher Key Generation Algorithm by using Orthogonal Matrix”, International Journal of Innovative Science and Modern Engineering (IJISME), Volume-3 Issue-3, 2015.

[5] Wu T. M., Applied Mathematics and Computation, Volume 169, Issue 2, 2005

[6] Raja P. V K., Chakravarthy A. S. N., “a cryptosystem based on Hilbert matrix using cipher block chaining mode”, International Journal of Mathematics Trends and Technology, Issue 2011

©IJRASET: All Rights are Reserved