Cosmos Multidisciplinary Research E-Journal
Online Available at www.cmrj.in
Recognized International Peer Reviewed Journal
Impact Factor 4.94
ISSN No. 2456-1665

Application of Matrix to Cryptography

Dr. Aruna M. Kulkarni
SAJVPM'S Smt.S. K. Gandhi College,
Kada, Dist. Beed, Maharastra
abhiarud@gmail.com

INTRODUCTION

The roots of cryptography are found in Roman and Egyptian civilizations. Cryptography is the art and science of keeping messages secure. The primary goal of cryptography is to secure important data. When information is transformed from a useful form of understanding to an opaque form of understanding, this is called encryption. When the information is reverted back into a useful form, it is called decryption. The information in its useful form is called plane text while the information in its encrypted form is called cipher text.

PRELIMINARIES

Define any suitable 3×3 matrix A as

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

This is known as encoding matrix.

The inverse of matrix A i.e. A^{-1} is a decoding matrix.

ANALYSIS AND INTERPRETATION

Encryption: suppose we want to send the message

INDIA IS MY COUNTRY

Our encoding matrix is

$$A = \begin{bmatrix} -2 & -2 & -3 \\ 0 & 1 & 1 \\ 3 & 2 & 3 \end{bmatrix}$$

Now associate each letter of our above text message with its position in the alphabet A is 1, B is 2, C is 3, and so on lastly z is 26 and assign a number 27 to a space between two words.

Thus the message becomes

I	N	D	I	A	$*$	I	S	$*$	M	Y	$*$	C	O	U	N	T	R	Y
9	14	4	9	1	27	9	19	27	13	25	27	3	15	21	14	20	18	25

Since we are using 3×3 matrix so above enumerated message break into a sequence of 3×1 vectors as

$$\begin{bmatrix} 9 \\ 14 \\ 4 \end{bmatrix} \begin{bmatrix} 9 \\ 1 \\ 27 \end{bmatrix} \begin{bmatrix} 9 \\ 19 \\ 27 \end{bmatrix} \begin{bmatrix} 13 \\ 25 \\ 27 \end{bmatrix} \begin{bmatrix} 3 \\ 15 \\ 21 \end{bmatrix} \begin{bmatrix} 14 \\ 20 \\ 18 \end{bmatrix} \begin{bmatrix} 25 \\ 27 \\ 27 \end{bmatrix}$$

Now write the above vectors as columns of a matrix. Perform the matrix multiplication of this matrix with the encoding matrix as

$$\begin{bmatrix} -2 & -2 & -3 \\ 0 & 1 & 1 \\ 3 & 2 & 3 \end{bmatrix} \begin{bmatrix} 9 & 9 & 9 & 13 & 3 & 14 & 25 \\ 14 & 1 & 19 & 25 & 15 & 20 & 27 \\ 4 & 27 & 27 & 27 & 21 & 18 & 27 \end{bmatrix}$$

Gives the matrix

$$\begin{bmatrix} -58 & -101 & -137 & -157 & -99 & -122 & -185 \\ 18 & 28 & 46 & 52 & 36 & 38 & 54 \\ 67 & 110 & 146 & 170 & 102 & 136 & 210 \end{bmatrix}$$

Now the columns of this matrix is the encoded message which is transmitted in the linear form as

$$\begin{matrix} -58 & 18 & 67 & -101 & 28 & 110 & -137 & 46 & 146 \\ -157 & 52 & 170 & -99 & 36 & 102 & -122 & 38 & 136 \\ -185 & 54 & 210 \end{matrix}$$

The receiver writes this string as a sequence of 3×1 column matrices and this is the decode message. Now repeat the technique using the inverse of encoding matrix.

The decoding matrix is the inverse of matrix A $i.e. A^{-1}$ where

$$A^{-1} = \begin{bmatrix} 1 & 0 & 1 \\ 3 & 3 & 2 \\ -3 & -2 & -2 \end{bmatrix}$$

To decode the message perform matrix multiplication as

$$\begin{bmatrix} 1 & 0 & 1 \\ 3 & 3 & 2 \\ -3 & -2 & -2 \end{bmatrix} \begin{bmatrix} -58 & -101 & -137 & -157 & -99 & -122 & -185 \\ 18 & 28 & 46 & 52 & 36 & 38 & 54 \\ 67 & 110 & 146 & 170 & 102 & 136 & 210 \end{bmatrix}$$

$$= \begin{bmatrix} 9 & 9 & 9 & 13 & 3 & 14 & 25 \\ 14 & 1 & 19 & 25 & 15 & 20 & 27 \\ 4 & 27 & 27 & 27 & 21 & 18 & 27 \end{bmatrix}$$

Now columns of this matrix written in linear form gives us original message

9	14	4	9	1	27	9	19	27	13	25	27	3	15	21	14	20	18	25	27	27
I	*N*	*D*	*I*	*A*	*	*I*	*S*	*	*M*	*Y*	*	*C*	*O*	*U*	*N*	*T*	*R*	*Y*	*	*

Thus we got the message

INDIA IS MY COUNTRY

In similar way the orthogonal matrices are also used to generate key matrix to increase the security of communication text. The improvisation of cipher text becomes relatively more secure due to the utilization of orthogonal matrix.

CONCLUSION

Matrices are well known tool for storage of huge data. In this article very simple encryption technique has 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.

REFERENCES

- Matrices by Laljee Prasad
- A Text Book of Matrices by Hari Kishan
- Stallings,w.: cryptography and network security, prentice Hall (4th edition) (2005)
- Wu T. M. Applied Mathematics and computation, volume 169,Issue 2, 2005.