IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

ENCRYPTION AND DECRYPTION OF MESSAGES BY USING MATRICES

Mr.Rakeyshh Sidu Byakuday
Lecturer in Mathematics, DKTE Society's Yashwantrao Chavan Polytechnic, Ichalkaranji, Maharashtra, India
Miss.Tejaswini Kumar Pattekari
Lecturer in Mathematics, DKTE Society's Yashwantrao Chavan Polytechnic, Ichalkaranji, Maharashtra, India
Mr.Sunil Tatyaso Farande
Lecturer in Mathematics, DKTE Society's Yashwantrao Chavan Polytechnic, Ichalkaranji, Maharashtra, India

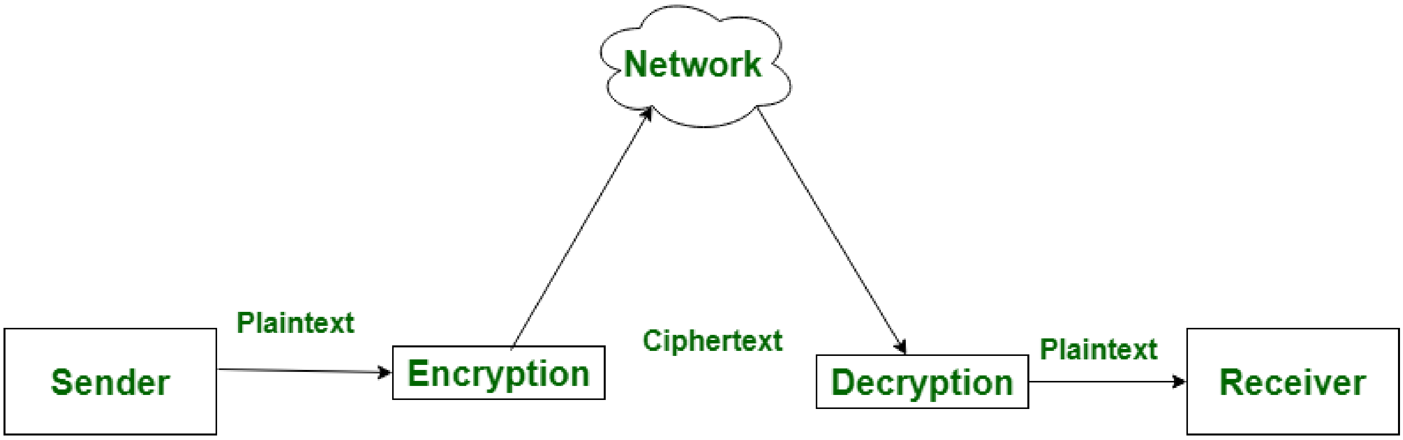
Abstract: This paper includes encoding and decoding using nonhomogeneous matrix method AM =X. Where A is encoding Matrix and in M is message matrix. X is unknown message.

Index Terms **- Encoding, decoding, Inverse Matrix, Nonhomogeneous Matrix method.**

I. INTRODUCTION

What is cryptography?
Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. The art of cryptography has been used to code messages for thousands of years and continues to be used in bank cards, computer passwords, and ecommerce. Basic idea of cryptography is that information can be encoded using an encryption scheme and decoded by decryption scheme. There are lots of encryption methods ranging from very simple to very complex. Most of them are mathematical in nature.

Encryption is the process of converting normal message (plaintext) into meaningless message (Ciphertext).
Decryption is the process of converting meaningless message (Ciphertext) into its original form (Plaintext).



Matrix encryption is one among the encrypting methods.

Sensitive information sent over the internet every second like, personal information, credit card number, bank account numbers etc are encoded or encrypted

What is Matrix?

Matrix, a set of numbers arranged in rows and columns so as to form a rectangular. The numbers are called the elements, or entries, of the matrix.

e. g A= $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ number of rows=2 and number of columns=2

what is Inverse of Matrix?

The **inverse of matrix** is a matrix, which on multiplication with the given matrix gives the multiplicative identity. For a square matrix A, its inverse is A^{-1}, and A · A^{-1} = A^{-1}· A = I, where I is the identity matrix. The matrix whose determinant is non-zero and for which the inverse matrix can be calculated is called an invertible matrix. For example, the inverse of A = A= $\begin{bmatrix} 1 & -1 \\ 0 & 2 \end{bmatrix}$ is A= $\begin{bmatrix} 1 & 1/2 \\ 0 & 1/2 \end{bmatrix}$ as

A.A^{-1} = $\begin{bmatrix} 1 & -1 \\ 0 & 2 \end{bmatrix} . \begin{bmatrix} 1 & 1/2 \\ 0 & 1/2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$=I

A^{-1}.A= $\begin{bmatrix} 1 & 1/2 \\ 0 & 1/2 \end{bmatrix} . \begin{bmatrix} 1 & -1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$=I

How to find inverse?

In the case of Real Numbers, the inverse of any real number *a* was the number a^{-1}, such that *a* times a^{-1} equals 1. We knew that for a real number, the inverse of the number was the Reciprocal of the number, as long as the number wasn't zero. The inverse of a square matrix A, denoted by A^{-1}, is the matrix so that the product of A and A^{-1} is the identity matrix. The identity matrix that results will be the same size as matrix A.

The formula to find the inverse of a matrix is: A^{-1} = 1/|A| · Adj A, where

- |A| is the determinant of A and
- Adj A is the adjoint of A

Note: For a matrix to have its inverse exists:

- The given matrix should be a square matrix.
- The determinant of the matrix should not be equal to zero.

Determinanat: The determinant of matrix is the single unique value representation of a matrix. The determinant of the matrix can be calculated with reference to any row or column of the given matrix. The determinant of the matrix is equal to the summation of the product of the elements and its cofactors, of a particular row or column of the matrix**.**

Singular Matrix: A matrix having a determinant value of zero is referred to as a singular matrix. For a singular matrix A, |A| = 0. The inverse of a singular matrix does not exist.

Non-Singular Matrix: A matrix whose determinant value is not equal to zero is referred to as a non-singular matrix. For a non-singular matrix |A| ≠ 0 and hence its inverse exists.

Adjoint of Matrix: The ad joint matrix is the transpose of the cofactor matrix .

Rules for Row and Column Operations of a Determinant:

The following rules are helpful to perform the row and column operations on determinants

- The value of the determinant remains unchanged if the rows and columns are interchanged.
- The sign of the determinant changes, if any two rows or (two columns) are interchanged.
- If any two rows or columns of a matrix are equal, then the value of the determinant is zero.

- If every element of a particular row or column is multiplied by a constant, then the value of the determinant also gets multiplied by the constant.
- If the elements of a row or a column are expressed as a sum of elements, then the determinant can be expressed as a sum of determinants.

Methods to Find Inverse of Matrix

The inverse of a matrix can be found using two methods. The inverse of a matrix can be calculated through elementary operations and through the use of an adjoint of a matrix. The elementary operations on a matrix can be performed through row or column transformations. Also, the inverse of a matrix can be calculated by applying the inverse of matrix formula through the use of the determinant and the adjoint of the matrix. For performing the inverse of the matrix through elementary column operations we use the matrix X and the second matrix B on the right-hand side of the equation.

[1] Elementary row or column operations
[2] Inverse of matrix formula (using the adjoint and determinant of matrix)

Let us check each of the methods described below.

Elementary Row Operations

To calculate the inverse of matrix A using elementary row transformations, we first take the augmented matrix [A | I], where I is the identity matrix whose order is the same as A. Then we apply the row operations to convert the left side A into I. Then the matrix gets converted into [I | A^{-1}].

Elementary Column Operations

We can apply the column operations as well just like how the process was explained for row operations to find the inverse of matrix.

Inverse of Matrix Formula

The inverse of matrix A can be computed using the inverse of matrix formula, A^{-1} = (adj A)/(det A). i.e., by dividing the adjoint of a matrix by the determinant of the matrix. The inverse of a matrix can be calculated by following the given steps:

Step 1: Calculate the minors of all elements of A.
Step 2: Then compute the cofactors of all elements and write the cofactor matrix by replacing the elements of A by their corresponding cofactors.
Step 3: Find the adjoint of A (written as adj A) by taking the transpose of the cofactor matrix of A.
Step 4: Multiply adj A by the reciprocal of the determinant.

Method/Procedure to encrypt using Nonhomogeneous Matrix Method

Assigning numbers to each letter in the alphabets:

1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
10	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
J	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**
19	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**0**
S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**Space**

Matrix Encryption

We need two thinks

Encoder is a matrix

Decoder is it's inverse

For example

Let A be the encoding matrix, M be the message matrix, and X will be the encrypted matrix then, Mathematically, the operation is

To encode X=AM

The sizes of A and M will have to be consistent.

To decode M=A^{-1} X

The encoding matrix A must have inverse for this scheme to work.

Encode the message "THE EAGLE HAS LANDED"

Encoding matrix $$A=\begin{pmatrix}3&0&1&1\\1&2&5&0\\1&1&3&0\\2&0&1&1\end{pmatrix}$$

Message Matrix $$M=\begin{pmatrix}20&5&5&19&14\\8&1&0&0&4\\5&7&8&12&5\\0&12&1&1&4\end{pmatrix}$$

Encryption –Lock

$$X=AM$$

$$X=\begin{pmatrix}3&0&1&1\\1&2&5&0\\1&1&3&0\\2&0&1&1\end{pmatrix}\begin{pmatrix}20&5&5&19&14\\8&1&0&0&4\\5&7&8&12&5\\0&12&1&1&4\end{pmatrix}$$

$$X=\begin{pmatrix}65&34&24&70&51\\61&42&45&79&47\\43&27&29&55&33\\45&25&19&51&37\end{pmatrix}$$

The matrix X is meaningless

Decryption –Unlock

To convert meaningless matrix to message matrix we need inverse matrix of A.

$$A^{-1}=\begin{pmatrix}1&0&0&-1\\2&3&-5&-2\\-1&-1&2&1\\-1&1&-2&2\end{pmatrix}$$

To obtain massage matrix M, multiply to meaningless matrix X by inverse matrix A^{-1} .
i.e

$$M=A^{-1}X$$

$$M=\begin{pmatrix}1&0&0&-1\\2&3&-5&-2\\-1&-1&2&1\\-1&1&-2&2\end{pmatrix}\begin{pmatrix}65&34&24&70&51\\61&42&45&79&47\\43&27&29&55&33\\45&25&19&51&37\end{pmatrix}$$

Message Matrix $\mathbf{M}=\begin{pmatrix} \mathbf{20} & \mathbf{5} & \mathbf{5} & \mathbf{19} & \mathbf{14} \\ \mathbf{8} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{4} \\ \mathbf{5} & \mathbf{7} & \mathbf{8} & \mathbf{12} & \mathbf{5} \\ \mathbf{0} & \mathbf{12} & \mathbf{1} & \mathbf{1} & \mathbf{4} \end{pmatrix}$

Decode massage is "The Eagle has Landed"

Conclusion

In this paper Using nonhomogeneous Method Encode and decode message securely and safely It will help in the sector wherever security of message required

References

1.K Thiagarajan *et al* 2018 *J. Phys.: Conf. Ser.* **1000** 012148 Encryption and decryption algorithm using algebraic matrix approach
National Conference on Mathematical Techniques and its Applications (NCMTA 18) IOP Publishing.
2. P. Zimmerman, "An Introduction to Cryptography", Doubleday & Company, Inc., United State of America, USA, 1999.
3. C. Shannon, "Communication Theory of Secrecy Systems", Bell Systems Technical Journal, MD Computing, vol. 15, pp. 57-64,
1998.
4. H. Mohan, and R. Raji. "Performance Analysis of AES and MARS Encryption Algorithms".
International Journal of Computer Science Issues (IJCSI), Vol. 8, issue 4. 2011.
5. www.google .com
6.Book of Applied Mathematics-I Tech max publications ,pune written by Dr.N.R Dasre,S.R Mitkari, M.V Ghotkar, B.B Gadekar.
7. Kalaichelvi V, Manimozhi K, Meenakshi P, Rajakumar B, Vimaladevi P A New variant of Hill Cipher Algorithm for Data Security
, International Journal of Pure and Applied Mathematics, Volume 117 No. 15 2017, 581-588 ISSN: 1311-8080 (printed version); ISSN:
1314-3395 (on-line version) url: http://www.ijpam.eu
8. Ismail I A, Amin Mohammed, Diab Hossam, How to Repair the Hill Cipher, Journal of Zhejiang University Science, 7(12), pp. 2022-
2030, 2006.
9. A. H. Rushdi and F. Mousa, "Design of a Robust Cryptosystem Algorithm for Noninvertible Matrices Based on Hill Cipher "Intl
Journal of Computer Science and Network Security , vol.9, no.5, 2009 pp. 11-16 10. Yeh YS, Wu TC, Chang CC, Yang WC. "A New
Cryptosystem Using Matrix Transformation". 25th IEEE International Carnahan Conference on Security Technology 1991: 131-138
11. Chefranov A. G., "Secure Hill Cipher Modification SHC-M" Proc. Of the First International Conference on Security of Information
and Network (SIN2007) 7-10 May 2007, Gazimagusa (TRNC) North Cyprus, Elci, A., Ors, B., and Preneel, B (Eds) Trafford Publishing,
Canada, 2008: pp 34-37, 2007
12. Y. Mahmoud Ahmed, Chefranov A. G., " Hill Cipher Modification Based on Pseudo-Random Eigen values HCM-PRE" Submitted
to Turkish Journal of Electrical Engineering & Computer Science on 2-03-2010
13. William Stallings, "Cryptography and Network Security", 5th Edition. 7. Bruce Schneier, "Applied Cryptography" , John Wiley & Sons, Inc 1996 8. Richard Smith "Internet Cryptography",Pearson Edn Pvt.Ltd
14..Neha Sharma, Sachin Chirgaiya. A novel approach to Hill Cipher , international journal of computer applications, India , 2014.
15.Wissam Raji, An introductory course in elementary number theory, publisher Saylor foundation 2016.