© 2019 IJSRSET | Volume 6 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : https://doi.org/10.32628/IJSRSET

Encryption and Decryption of Messages Using two Different Non-Singular Matrices

Veena T
Assistant Professor, Department of Mathematics, Government First Grade College, Chickaballapur, India

ABSTRACT
The purpose of this article is to secure message transmission using two different 2×2 non- singular matrices as key. The encryption process involves converting plain text messages in to numerical values, splitting them in to pairs, and then encrypting each pair using matrix A followed by matrix B. This double encryption provides more effective to secure plain text messages. The decryption process involves finding the inverses of matrices B and A, and then decrypting each pair using B^(-1) followed by A^(-1). This double matrix encryption technique provides more effective security for messages transmission and to decrypt the messages.
Keywords : Non Singular Matrix, Cipher Text, Plain Text, Encryption, Decryption, Scilab and Wxmaxima.

Introduction

Now days its very important to keep information or message safely not knowing to others except sender and receiver those who work in military, medical field and banks etc. Cryptography plays a vital role to secure information or message safely and confidentially. Cryptography is a branch of Computer Science and Mathematics. It is the science of writing or reading coded messages. Cryptography is derived from a "Greek word called "crypto and graphy", Crypto means secret and graphy means writing. It is used to protect sensitive information during military and government communication, in sensitive medical information, security for individual information example email, personal information, security for electronic transactions like online shopping sites, credit cards, ATM card etc. Transmission and storage of multimedia data like video, audio and images over the internet has increased in today's digital communication. For the purpose of security and privacy, we need to encode the message at the sender side and decode it at the receiver side. In this paper plain text means ordinary message is encrypted using two different 2×2 non-singular matrices and decrypted using its inverses as a key matrix.

Plain text: Plain text is ordinary readable text before it is encrypted in to cipher text or readable text after it is decrypted.
Example: *"Enemies with twenty weapons"*
Cipher text : A message written in secret code is called cipher text .
Example : plain text is "**Enemies with twenty weapons**" its cipher text is [91 67], [87 64], [83 60] , [133 95], [197 142], [172 124], [80 60] , [181 130] , [178 130], [175 125], [181 130], [71 53], [161 117], [133 95].
Encryption: The process of converting plain text(readable text) in to cipher text (unreadable text) using secret key is called encryption.
Decryption: The process of converting cipher text in to plain text using secret key is called Decryption.

Method

First select two different non –singular matrices, A and B, of the same order, next convert plain text

message in to numerical values, afterwards split the numerical values in to pairs and encrypt each pair using non singular matrix A followed by non-singular matrix B, then we get cipher text. Finally find the inverses of matrices B and A, and then decrypt each pair using B^{-1} followed by A^{-1}.

Table-1. Assign each alphabet or character to single numerical value such that

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10

K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20

U	V	W	X	Y	Z	Space or _
21	22	23	24	25	26	0

Example: Use non-singular matrices *A* and *B* as key matrices where $A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}$, encrypt the message "ENEMIES WITH TWENTY WEAPONS" and decrypt the message using its inverses.

Solution: First break the plain text (message) into two consecutive letters

ENEMIES _WITH _TWENTY _WEAPONS_ and assign numerical values given in the Table-1.

$[E \quad N] = [5 \quad 14]$, $[E \quad M] = [5 \quad 13]$, $[I \quad E] = [9 \quad 5]$,

$[S \quad \_] = [19 \quad 0]$, $[W \quad I] = [23 \quad 9]$, $[T \quad H] = [20 \quad 8]$,

$[\_ \quad T] = [0 \quad 20]$, $[W \quad E] = [23 \quad 5]$, $[N \quad T] = [14 \quad 20]$

$[Y \quad \_] = [25 \quad 0]$, $[W \quad E] = [23 \quad 5]$, $[A \quad P] = [1 \quad 16]$

$[O \quad N] = [15 \quad 14]$, $[S \quad \_] = [19 \quad 0]$

Next multiply non-singular matrix A to above row matrices

$[E \quad N] * A = [5 \quad 14] * \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = [24 \quad 19]$

$[E \quad M] * A = [5 \quad 13] * \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = [23 \quad 18]$

$[I \quad E] * A = [9 \quad 5] * \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = [23 \quad 14]$

$[S \quad \_] * A = [19 \quad 0] * \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = [38 \quad 19]$

$[W \quad I] * A = [23 \quad 9] * \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = [55 \quad 32]$

$[T \quad H] * A = [20 \quad 8] * \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = [48 \quad 28]$

$[\_ \quad T] * A = [0 \quad 20] * \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = [20 \quad 20]$

$[W \quad E] * A = [23 \quad 5] * \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = [51 \quad 28]$

$[N \quad T] * A = [14 \quad 20] * \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = [48 \quad 34]$

$[Y \quad \_] * A = [25 \quad 0] * \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = [50 \quad 25]$

$[W \quad E] * A = [23 \quad 5] * \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = [51 \quad 28]$

$[A \quad P] * A = [1 \quad 16] * \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = [18 \quad 17]$

$[O \quad N] * A = [15 \quad 14] * \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = [44 \quad 29]$

$[S \quad \_] * A = [19 \quad 0] * \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = [38 \quad 19]$

Next multiply by non-singular matrix B

$[24 \quad 19] * B = [24 \quad 19] * \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} = [91 \quad 67]$

$[23 \quad 18] * B = [23 \quad 18] * \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} = [87 \quad 64]$

$[23 \quad 14] * B = [23 \quad 14] * \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} = [83 \quad 60]$

$[38 \quad 19] * B = [38 \quad 19] * \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} = [133 \quad 95]$

$[55 \quad 32] * B = [55 \quad 32] * \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} = [197 \quad 142]$

$[48 \quad 28] * B = [48 \quad 28] * \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} = [172 \quad 124]$

$[20 \quad 20] * B = [20 \quad 20] * \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} = [80 \quad 60]$

$[51 \quad 28] * B = [51 \quad 28] * \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} = [181 \quad 130]$

$[48 \quad 34] * B = [48 \quad 34] * \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} = [178 \quad 130]$

$[50 \quad 25] * B = [50 \quad 25] * \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} = [175 \quad 125]$

$[51 \quad 28] * B = [51 \quad 28] * \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} = [181 \quad 130]$

$[18 \quad 17] * B = [18 \quad 17] * \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} = [71 \quad 53]$

$[44 \quad 29]B = [44 \quad 29] * \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} = [161 \quad 117]$

$[38 \quad 19] * B = [38 \quad 19] * \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix} = [133 \quad 95]$

The encrypted cipher text is [91 67], [87 64], [83 60], [133 95], [197 142], [172 124], [80 60], [181 130] , [178 130], [175 125], [181 130], [71 53], [161 117], [133 95]

$|\boldsymbol{B}| = \begin{vmatrix} \mathbf{3} & \mathbf{2} \\ \mathbf{1} & \mathbf{1} \end{vmatrix} = \mathbf{3} - \mathbf{2} = \mathbf{1}$

$\boldsymbol{B^{-1}} = \frac{\boldsymbol{adj(B)}}{\boldsymbol{|B|}} = \frac{\begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix}}{1} = \begin{bmatrix} \mathbf{1} & \mathbf{-2} \\ \mathbf{-1} & \mathbf{3} \end{bmatrix}$

$[91 \quad 67] * B^{-1} = [91 \quad 67] * \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} = [24 \quad 19]$

$[87 \quad 64] * B^{-1} = [87 \quad 64] * \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} = [23 \quad 18]$

$[83 \quad 60] * B^{-1} = [83 \quad 60] * \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} = [23 \quad 14]$

$[133 \quad 95] * B^{-1} = [133 \quad 95] * \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} = [38 \quad 19]$

$[197 \quad 142] * B^{-1} = [197 \quad 142] * \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} = [55 \quad 32]$

$[172 \quad 124] * B^{-1} = [172 \quad 124] * \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} = [48 \quad 28]$

$[80 \quad 60] * B^{-1} = [80 \quad 60] * \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} = [20 \quad 20]$

$[181 \quad 130] * B^{-1} = [181 \quad 130] * \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} = [51 \quad 28]$

$$[178 \quad 130] * B^{-1} = [178 \quad 130] * \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} = [48 \quad 34]$$

$$[175 \quad 125] * B^{-1} = [175 \quad 125] * \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} = [50 \quad 25]$$

$$[181 \quad 130] * B^{-1} = [181 \quad 130] * \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} = [51 \quad 28]$$

$$[71 \quad 53] * B^{-1} = [71 \quad 53] * \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} = [18 \quad 17]$$

$$[161 \quad 117] * B^{-1} = [161 \quad 117] * \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} = [44 \quad 29]$$

$$[133 \quad 95] * B^{-1} = [133 \quad 95] * \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} = [38 \quad 19]$$

$$|\boldsymbol{A}| = \begin{vmatrix} \mathbf{2} & \mathbf{1} \\ \mathbf{1} & \mathbf{1} \end{vmatrix} = \mathbf{2} - \mathbf{1} = \mathbf{1}$$

$$\boldsymbol{A^{-1}} = \frac{\boldsymbol{adj(A)}}{|\boldsymbol{A}|} = \frac{\begin{bmatrix} \mathbf{1} & \mathbf{-1} \\ \mathbf{-1} & \mathbf{2} \end{bmatrix}}{\mathbf{1}} = \begin{bmatrix} \mathbf{1} & \mathbf{-1} \\ \mathbf{-1} & \mathbf{2} \end{bmatrix}$$

$$[24 \quad 19] * A^{-1} = [24 \quad 19] * \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} = [5 \quad 14] = [E \quad N]$$

$$[23 \quad 18] * A^{-1} = [23 \quad 18] * \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} = [5 \quad 13] = [E \quad M]$$

$$[23 \quad 14] * A^{-1} = [23 \quad 14] * \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} = [9 \quad 5] = [I \quad E]$$

$$[38 \quad 19] * A^{-1} = [38 \quad 19] * \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} = [19 \quad 0] = [S \quad \_]$$

$$[55 \quad 32] * A^{-1} = [55 \quad 32] * \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} = [23 \quad 9] = [W \quad I]$$

$$[48 \quad 28] * A^{-1} = [48 \quad 28] * \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} = [20 \quad 8] = [T \quad H]$$

$$[20 \quad 20] * A^{-1} = [20 \quad 20] * \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} = [0 \quad 20] = [\_ \quad T]$$

$$[51 \quad 28] * A^{-1} = [51 \quad 28] * \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} = [23 \quad 5] = [W \quad E]$$

$$[48 \quad 34] * A^{-1} = [48 \quad 34] * \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} = [14 \quad 20] = [N \quad T]$$

$$[50 \quad 25] * A^{-1} = [50 \quad 25] * \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} = [25 \quad 0] = [Y \quad \_]$$

$$[51 \quad 28] * A^{-1} = [51 \quad 28] * \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} = [23 \quad 5] = [W \quad E]$$

$$[18 \quad 17] * A^{-1} = [18 \quad 17] * \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} = [1 \quad 16] = [A \quad P]$$

$$[44 \quad 29] * A^{-1} = [44 \quad 29] * \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} = [15 \quad 14] = [O \quad N]$$

$$[38 \quad 19] * A^{-1} = [38 \quad 19] * \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} = [19 \quad 0] = [S \quad \_]$$

Then the decrypted message is “ENEMIES WITH TWENTY WEAPONS”

Conclusions

This paper concludes that the plain text can be transferred to cipher text using two different 2 x 2 non-singular matrices as the key to encrypt plain text and using its invertible matrices as the key to decrypt cipher text. The large messages can also encrypt and decrypt the text using non-sigular matrix .The aim of this paper is to secure messages and also transfer over internet confidentially. This helps to protect the large messages to maintain military secrets. Even we can use 3x 3 and 4 x 4 non singular matrices as key to encrypt (encode) plain text and using its invertible matrices as the key to decrypt(decode) cipher text. With the help of scilab and wxmaxima software we can calculate inverses of 3 x 3 , 4 x 4 and 5 x 5 non singular matrices within a fraction of second. Cryptography plays an vital role to secure information or message safely and confidentially. This paper helps to military peoples to secure the information or

messages not knowing to others except sender and receiver. Both sender and receiver must know secret key.

REFERENCES

[1]. Cryptography and network security : principles and practice , 4th Edition by William Stallings, Prntice Hall , Nov 26, 2005.

[2]. S.S.Dhenakaran, M IIayaraja. "Extension play fair Cipher using 16×16 Matrix "volume 48-No.7, June 2012.

[3]. Wissam Raji, An introductory course in elementary number theory, publisher Saylor foundation 2016.

[4]. W. Edwin Clark. Elementary Number Theory. University of south Florida, Dec 2002.

[5]. Dr.James H Yu and Mr. Tom K. Le. "Internet and network Security", "Journal of industrial technology", volume 17, Number1-November 2000 to January 2001.

[6]. Hongbo Zhou, Mutka and Lionel M. Ni Multiple-key Cryptography-based Distribted Certificate Authority in Mobile Ad-hoevNetworks, IEEE proceedings of GLOBESCOM,2005, 1681-1685.

[7]. Abdulaziz B.M Hamed and Ibrahim O.A.Albudawe. Cryptography using congruence modulo relations. American Journal of Engineering Research, 2017.

[8]. R. L. Rivest, The MDS message –digest algorithm , RFC 1321,April 1992.

[9]. O. Dunkelman, N, Keller, A Shamir, A practical-time attack on the KASUM cryptosystem used in GSM and 3G telephony," Advances in Cryptology , Proceed-ings Crypto'10 LNCS,T,Rabin, Ed., Springer, Heidelberg, 2010, in print.

[10]. Neha Sharma, Sachin Chirgaiya. A novel approach to Hill Cipher , international journal of computer applications, India , 2014.