International Journal of Scientific Research in Modern Science and Technology
ISSN: 2583 -7605 (Online)
© IJSRMST \ Vol. 2 \ Issue 9 \ September 2023
Available online at: www.ijsrmst.com
DOI: https://doi.org/10.59828/ijsrmst.v2i9.145

APPLICATIONS OF NON-SINGULAR MATRICES IN CRYPTOGRAPHY

Veena T

Assistant Professor, Department of Mathematics, Government First Grade College, Sira

Email: veenavenki.t03@gmail.com

ABSTRACT

The aim of this paper is security for large or short messages by using 4x4 non- singular matrices modulo 27 as the key to transfer plain text to cipher text and its invertible matrices modulo 27 of order 4x4 as the key to transfer cipher text to plain text. Cryptography is the science of using mathematics to encrypt and decrypt messages. It is the art of keeping information secret and safe.

Keywords: Plain text, Cipher text, Cryptography, Non-singular matrix, Encryption, Decryption, Congruence modulo n, Key matrix.

INTRODUCTION

Cryptography is a branch of Computer Science and Mathematics. It is the science of writing or reading coded messages. Cryptography is derived its name from a "Greek word called "Kryptos" which means "Hidden Secrets". It is originated about 4000 year ago.

One of the important applications of inverse of 4 x 4 non-singular square matrix is in cryptography. Cryptography is an art of communication between two persons by keeping the information(message) not known to others. It is based upon two factors namely encryption and decryption . Encryption means process of conversion of plain text to cipher text, on other hand decryption means process of conversion of cipher text to plain text using key matrix. The key matrix is non singular 4x4 matrices modulo 27.

Matrix: The arrangements of numbers in rows and columns is called matrix.

Key matrix: The key matrix is used to encrypt the messages and its inverse is used to decrypt the encoded messages.

Plain text: In cryptography, plain text is usually ordinary readable text before it is encrypted in to cipher text or readable text after it is decrypted.

Example: Plain text is **"CONFIDENTIAL LETTER IN CUPBOARD"**

Cipher text: A message written in secret code.

Example: Cipher text for **"CONFIDENTIAL LETTER IN CUPBOARD" is PCHKNYYQKTED VALLNTUSNONAZM – P**

Non -singular matrix: A square matrix is said to be non singular matrix if its determinant is not equal to zero.

Encryption: Encryption is the process of converting plain text (normal message) to cipher text (meaningless message or unreadable).

Decryption: Decryption is the process of converting cipher text (meaningless message) in to plain text (original message).

Congruent modulo n: The number a and b are congruent modulo n if and only if n|(a-b) and also if and only if n|(b-a)

Table 1

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
1	2	3	4	5	6	7	8	9	10	11	12	13
-26	-25	-24	-23	-22	-21	-20	-19	-18	-17	-16	-15	-14

N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	**Space or _**
14	15	16	17	18	19	20	21	22	23	24	25	26	0
-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1	

Table 2

Demonstrating the inverse of element modulo 27 which satisfies $x * x^{-1} \equiv 1(mod n)$

Number	2	4	5	7	8	10	11	13	14
Inverse	14	7	11	4	17	19	5	25	2

Number	16	17	19	20	22	23	25	26
Inverse	22	8	10	23	16	20	13	26

Encryption

Cipher text =(key*plain text) $\boldsymbol{mod}$27

Decryption

Plain text= (key^{-1}* cipher text) $\boldsymbol{mod}$27

Method:

Suppose we given non singular matrix A $= \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$

as an encryption key, such that A^{-1} exists and a message **"CONFIDENTIAL LETTER IN CUPBOARD"**

To encrypt the message using 4 x 4 non singular matrix modulo 27, first we have to assign each character to a single numerical value such that $A = 1, B = 2, C = 3, \ldots\ldots, Z = 26$ and space or _=0, next break the plain text (message) in to four consecutive character including space and convert them in to column matrix as $P = \begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{bmatrix}$ and multiply with key matrix to generate the following linear systems.

$D_1 = p_1a_{11} + p_2a_{12} + p_3a_{13} + p_4a_{14}$

$D_2 = p_1a_{21} + p_2a_{22} + p_3a_{23} + p_4a_{24}$

$D_3 = p_1a_{31} + p_2a_{32} + p_3a_{33} + p_4a_{34}$

$D_4 = p_1a_{41} + p_2a_{42} + p_3a_{43} + p_4a_{44}$

Or we can expressed as matrices multiplication

$$\begin{bmatrix} D_1 \\ D_2 \\ D_3 \\ D_4 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{bmatrix}$$

$\Rightarrow D = (A * P) mod 27$

Where P and D are column vectors of length 4, representing the plain text and cipher text respectively and A is a 4 x 4 non singular matrix, which is known for both Sender and Receiver.

1.Use the key matrix $A = \begin{bmatrix} \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{3} & \mathbf{2} \\ \mathbf{2} & \mathbf{-2} & \mathbf{-5} & \mathbf{-1} \\ \mathbf{3} & \mathbf{-1} & \mathbf{1} & \mathbf{5} \end{bmatrix}$ encrypt the message "CONFIDENTIAL LETTER IN CUPBOARD" and use its invertible matrix to decrypt.

Solution: First break the message in to four consecutive character including space as follows

CONFIDENTIAL LETTER IN CUPBOARD⇒ CONF IDEN TIAL _LET TER_

IN_C UPBO ARD_

Convert the character in to corresponding numerical values

$$\begin{bmatrix} C \\ O \\ N \\ F \end{bmatrix} = \begin{bmatrix} 3 \\ 15 \\ 14 \\ 6 \end{bmatrix}, \quad \begin{bmatrix} I \\ D \\ E \\ N \end{bmatrix} = \begin{bmatrix} 9 \\ 4 \\ 5 \\ 14 \end{bmatrix}, \quad \begin{bmatrix} T \\ I \\ A \\ L \end{bmatrix} = \begin{bmatrix} 20 \\ 9 \\ 1 \\ 12 \end{bmatrix}, \quad \begin{bmatrix} \_ \\ L \\ E \\ T \end{bmatrix} = \begin{bmatrix} 0 \\ 12 \\ 5 \\ 20 \end{bmatrix}, \quad \begin{bmatrix} T \\ E \\ R \\ \_ \end{bmatrix} = \begin{bmatrix} 20 \\ 5 \\ 18 \\ 0 \end{bmatrix}, \quad \begin{bmatrix} I \\ N \\ \_ \\ C \end{bmatrix} = \begin{bmatrix} 9 \\ 14 \\ 0 \\ 3 \end{bmatrix}, \quad \begin{bmatrix} U \\ P \\ B \\ O \end{bmatrix} = \begin{bmatrix} 21 \\ 16 \\ 2 \\ 15 \end{bmatrix},$$

$$\begin{bmatrix} A \\ R \\ D \\ \_ \end{bmatrix} = \begin{bmatrix} 1 \\ 18 \\ 4 \\ 0 \end{bmatrix}$$

Here $A = \begin{bmatrix} 0 & 1 & 2 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & -2 & -5 & -1 \\ 3 & -1 & 1 & 5 \end{bmatrix}$ is a non singular matrix

$D = (A * P)mod27$

Cipher text =(key matrix*plain text) $mod27$

$$\begin{bmatrix}0 & 1 & 2 & 0\\ 1 & 0 & 3 & 2\\ 2 & -2 & -5 & -1\\ 3 & -1 & 1 & 5\end{bmatrix}\begin{bmatrix}C\\ O\\ N\\ F\end{bmatrix} mod27 = \begin{bmatrix}0 & 1 & 2 & 0\\ 1 & 0 & 3 & 2\\ 2 & -2 & -5 & -1\\ 3 & -1 & 1 & 5\end{bmatrix}\begin{bmatrix}3\\ 15\\ 14\\ 6\end{bmatrix} mod27$$

$$= \begin{bmatrix}0(3)+1(15)+2(14)+0(6)\\ 1(3)+0(15)+3(14)+2(6)\\ 2(3)-2(15)-5(14)-1(6)\\ 3(3)-1(15)+1(14)+5(6)\end{bmatrix} mod27$$

$$= \begin{bmatrix}43\\ 57\\ -100\\ 38\end{bmatrix} mod27 = \begin{bmatrix}16\\ 3\\ -19\\ 11\end{bmatrix} = \begin{bmatrix}P\\ C\\ H\\ K\end{bmatrix}$$

$\boldsymbol{CONF \Longrightarrow PCHK}$

Similarly,

$$\begin{bmatrix}0 & 1 & 2 & 0\\ 1 & 0 & 3 & 2\\ 2 & -2 & -5 & -1\\ 3 & -1 & 1 & 5\end{bmatrix}\begin{bmatrix}I\\ D\\ E\\ N\end{bmatrix} mod27 = \begin{bmatrix}0 & 1 & 2 & 0\\ 1 & 0 & 3 & 2\\ 2 & -2 & -5 & -1\\ 3 & -1 & 1 & 5\end{bmatrix}\begin{bmatrix}9\\ 4\\ 5\\ 14\end{bmatrix} mod27$$

$$= \begin{bmatrix}14\\ 52\\ -29\\ 98\end{bmatrix} mod27 = \begin{bmatrix}14\\ 25\\ -2\\ 17\end{bmatrix} = \begin{bmatrix}N\\ Y\\ Y\\ Q\end{bmatrix}$$

$\boldsymbol{IDEN \Longrightarrow NYYQ}$

$$\begin{bmatrix}0 & 1 & 2 & 0\\ 1 & 0 & 3 & 2\\ 2 & -2 & -5 & -1\\ 3 & -1 & 1 & 5\end{bmatrix}\begin{bmatrix}T\\ I\\ A\\ L\end{bmatrix} mod27 = \begin{bmatrix}0 & 1 & 2 & 0\\ 1 & 0 & 3 & 2\\ 2 & -2 & -5 & -1\\ 3 & -1 & 1 & 5\end{bmatrix}\begin{bmatrix}20\\ 9\\ 1\\ 12\end{bmatrix} mod27$$

$$= \begin{bmatrix}11\\ 47\\ 5\\ 112\end{bmatrix} mod27 = \begin{bmatrix}11\\ 20\\ 5\\ 4\end{bmatrix} = \begin{bmatrix}K\\ T\\ E\\ D\end{bmatrix}$$

$\boldsymbol{TIAL \Longrightarrow KTED}$

$$\begin{bmatrix}0 & 1 & 2 & 0\\ 1 & 0 & 3 & 2\\ 2 & -2 & -5 & -1\\ 3 & -1 & 1 & 5\end{bmatrix}\begin{bmatrix}-\\ L\\ E\\ T\end{bmatrix} mod27 = \begin{bmatrix}0 & 1 & 2 & 0\\ 1 & 0 & 3 & 2\\ 2 & -2 & -5 & -1\\ 3 & -1 & 1 & 5\end{bmatrix}\begin{bmatrix}0\\ 12\\ 5\\ 20\end{bmatrix} mod27$$

$$= \begin{bmatrix}22\\ 55\\ -69\\ 93\end{bmatrix} mod27 = \begin{bmatrix}22\\ 1\\ -15\\ 12\end{bmatrix} = \begin{bmatrix}V\\ A\\ L\\ L\end{bmatrix}$$

$$\boldsymbol{-LET \Longrightarrow VALL}$$

$$\begin{bmatrix}0 & 1 & 2 & 0\\ 1 & 0 & 3 & 2\\ 2 & -2 & -5 & -1\\ 3 & -1 & 1 & 5\end{bmatrix}\begin{bmatrix}T\\ E\\ R\\ -\end{bmatrix} mod27 = \begin{bmatrix}0 & 1 & 2 & 0\\ 1 & 0 & 3 & 2\\ 2 & -2 & -5 & -1\\ 3 & -1 & 1 & 5\end{bmatrix}\begin{bmatrix}20\\ 5\\ 18\\ 0\end{bmatrix} mod27$$

$$= \begin{bmatrix}41\\ 74\\ -60\\ 73\end{bmatrix} mod27 = \begin{bmatrix}14\\ 20\\ -6\\ 19\end{bmatrix} = \begin{bmatrix}N\\ T\\ U\\ S\end{bmatrix}$$

$$\boldsymbol{TER- \Longrightarrow NTUS}$$

$$\begin{bmatrix}0 & 1 & 2 & 0\\ 1 & 0 & 3 & 2\\ 2 & -2 & -5 & -1\\ 3 & -1 & 1 & 5\end{bmatrix}\begin{bmatrix}I\\ N\\ -\\ C\end{bmatrix} mod27 = \begin{bmatrix}0 & 1 & 2 & 0\\ 1 & 0 & 3 & 2\\ 2 & -2 & -5 & -1\\ 3 & -1 & 1 & 5\end{bmatrix}\begin{bmatrix}9\\ 14\\ 0\\ 3\end{bmatrix} mod27$$

$$= \begin{bmatrix}14\\ 15\\ -13\\ 28\end{bmatrix} mod27 = \begin{bmatrix}14\\ 15\\ -13\\ 1\end{bmatrix} = \begin{bmatrix}N\\ O\\ N\\ A\end{bmatrix}$$

$$\boldsymbol{IN - C \Longrightarrow NONA}$$

$$\begin{bmatrix}0 & 1 & 2 & 0\\ 1 & 0 & 3 & 2\\ 2 & -2 & -5 & -1\\ 3 & -1 & 1 & 5\end{bmatrix}\begin{bmatrix}U\\ P\\ B\\ O\end{bmatrix} mod27 = \begin{bmatrix}0 & 1 & 2 & 0\\ 1 & 0 & 3 & 2\\ 2 & -2 & -5 & -1\\ 3 & -1 & 1 & 5\end{bmatrix}\begin{bmatrix}21\\ 16\\ 2\\ 15\end{bmatrix} mod27$$

$$= \begin{bmatrix}20\\ 57\\ -15\\ 124\end{bmatrix} mod27 = \begin{bmatrix}20\\ 3\\ -15\\ 16\end{bmatrix} = \begin{bmatrix}T\\ C\\ L\\ P\end{bmatrix}$$

$$\boldsymbol{UPBO \Longrightarrow TCLA}$$

$$\begin{bmatrix}0 & 1 & 2 & 0\\ 1 & 0 & 3 & 2\\ 2 & -2 & -5 & -1\\ 3 & -1 & 1 & 5\end{bmatrix}\begin{bmatrix}A\\ R\\ D\\ -\end{bmatrix} mod27 = \begin{bmatrix}0 & 1 & 2 & 0\\ 1 & 0 & 3 & 2\\ 2 & -2 & -5 & -1\\ 3 & -1 & 1 & 5\end{bmatrix}\begin{bmatrix}1\\ 18\\ 4\\ 0\end{bmatrix} mod27$$

$$= \begin{bmatrix}26\\ 13\\ -54\\ -11\end{bmatrix} mod27 = \begin{bmatrix}26\\ 13\\ 0\\ -11\end{bmatrix} = \begin{bmatrix}Z\\ M\\ -\\ P\end{bmatrix}$$

$ARD - \Rightarrow ZM - P$

"CONFIDENTIAL LETTER IN CUPBOARD" is encrypted as PCHKNYYQKTED VALLNTUSNONAZM − P

Next we convert encoded message **PCHKNYYQKTED VALLNTUSNONAZM − P** to original message by using its invertible matrix and congruence relations.

$$A = \begin{bmatrix}a_{11} & a_{12} & a_{13} & a_{14}\\ a_{21} & a_{22} & a_{23} & a_{24}\\ a_{31} & a_{32} & a_{33} & a_{34}\\ a_{41} & a_{42} & a_{43} & a_{44}\end{bmatrix}$$

$$|A| = \begin{vmatrix}a_{11} & a_{12} & a_{13} & a_{14}\\ a_{21} & a_{22} & a_{23} & a_{24}\\ a_{31} & a_{32} & a_{33} & a_{34}\\ a_{41} & a_{42} & a_{43} & a_{44}\end{vmatrix}$$

$$|A| = a_{11}\begin{vmatrix}a_{22} & a_{23} & a_{24}\\ a_{32} & a_{33} & a_{34}\\ a_{42} & a_{43} & a_{44}\end{vmatrix} - a_{21}\begin{vmatrix}a_{12} & a_{13} & a_{14}\\ a_{32} & a_{33} & a_{34}\\ a_{42} & a_{43} & a_{44}\end{vmatrix} + a_{31}\begin{vmatrix}a_{12} & a_{13} & a_{14}\\ a_{22} & a_{23} & a_{24}\\ a_{42} & a_{43} & a_{44}\end{vmatrix}$$
$$-a_{41}\begin{vmatrix}a_{12} & a_{13} & a_{14}\\ a_{22} & a_{23} & a_{24}\\ a_{32} & a_{33} & a_{34}\end{vmatrix}$$

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

$$|A| = 0\begin{vmatrix}0 & 3 & 2\\ -2 & -5 & -1\\ -1 & 1 & 5\end{vmatrix} - 1\begin{vmatrix}1 & 2 & 0\\ -2 & -5 & -1\\ -1 & 1 & 5\end{vmatrix} + 2\begin{vmatrix}1 & 2 & 0\\ 0 & 3 & 2\\ -1 & 1 & 5\end{vmatrix} - 3\begin{vmatrix}1 & 2 & 0\\ 0 & 3 & 2\\ -2 & -5 & -1\end{vmatrix}$$

$$\Rightarrow |A| = 0 - 1[1(-25+1) - 2(-10-1) + 0] + 2[1(15-2) - 2(0+2) + 0)] - 3[1(-3+10) - 2(0+4) + 0]$$

$$\Rightarrow |A| = -1[-24+22] + 2[13-4] - 3[7-8]$$

$$\Rightarrow |A| = -[-2] + 2[9] - 3[-1]$$

$$\Rightarrow |A| = 2 + 18 + 3 = 23$$

adj(A)=$\left[a_{ij}\right]^T$ or [Cofactors(A)]^T

$$A=\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{bmatrix}$$

Cofactors(A)=

$$\begin{bmatrix} +\begin{vmatrix} a_{22} & a_{23} & a_{24} \\ a_{32} & a_{33} & a_{34} \\ a_{42} & a_{43} & a_{44} \end{vmatrix} & -\begin{vmatrix} a_{21} & a_{23} & a_{24} \\ a_{31} & a_{33} & a_{34} \\ a_{41} & a_{43} & a_{44} \end{vmatrix} & +\begin{vmatrix} a_{21} & a_{22} & a_{24} \\ a_{31} & a_{32} & a_{34} \\ a_{41} & a_{42} & a_{44} \end{vmatrix} & -\begin{vmatrix} a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \\ a_{41} & a_{42} & a_{43} \end{vmatrix} \\ -\begin{vmatrix} a_{12} & a_{13} & a_{14} \\ a_{32} & a_{33} & a_{34} \\ a_{42} & a_{43} & a_{44} \end{vmatrix} & +\begin{vmatrix} a_{11} & a_{13} & a_{14} \\ a_{31} & a_{33} & a_{34} \\ a_{41} & a_{43} & a_{44} \end{vmatrix} & -\begin{vmatrix} a_{11} & a_{12} & a_{14} \\ a_{31} & a_{32} & a_{34} \\ a_{41} & a_{42} & a_{44} \end{vmatrix} & +\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{31} & a_{32} & a_{33} \\ a_{41} & a_{42} & a_{43} \end{vmatrix} \\ +\begin{vmatrix} a_{12} & a_{13} & a_{14} \\ a_{22} & a_{23} & a_{24} \\ a_{42} & a_{43} & a_{44} \end{vmatrix} & -\begin{vmatrix} a_{11} & a_{13} & a_{14} \\ a_{21} & a_{23} & a_{24} \\ a_{41} & a_{43} & a_{44} \end{vmatrix} & +\begin{vmatrix} a_{11} & a_{12} & a_{14} \\ a_{21} & a_{22} & a_{24} \\ a_{41} & a_{42} & a_{44} \end{vmatrix} & -\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{41} & a_{42} & a_{43} \end{vmatrix} \\ -\begin{vmatrix} a_{12} & a_{13} & a_{14} \\ a_{22} & a_{23} & a_{24} \\ a_{32} & a_{33} & a_{34} \end{vmatrix} & +\begin{vmatrix} a_{11} & a_{13} & a_{14} \\ a_{21} & a_{23} & a_{24} \\ a_{31} & a_{33} & a_{34} \end{vmatrix} & -\begin{vmatrix} a_{11} & a_{12} & a_{14} \\ a_{21} & a_{22} & a_{24} \\ a_{31} & a_{32} & a_{34} \end{vmatrix} & +\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} \end{bmatrix}$$

adj(A)=[Cofactors(A)]^T

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

$$\text{Cofactors}(A)=\begin{bmatrix} +\begin{vmatrix} 0 & 3 & 2 \\ -2 & -5 & -1 \\ -1 & 1 & 5 \end{vmatrix} & -\begin{vmatrix} 1 & 3 & 2 \\ 2 & -5 & -1 \\ 3 & 1 & 5 \end{vmatrix} & +\begin{vmatrix} 1 & 0 & 2 \\ 2 & -2 & -1 \\ 3 & -1 & 5 \end{vmatrix} & -\begin{vmatrix} 1 & 0 & 3 \\ 2 & -2 & -5 \\ 3 & -1 & 1 \end{vmatrix} \\ -\begin{vmatrix} 1 & 2 & 0 \\ -2 & -5 & -1 \\ -1 & 1 & 5 \end{vmatrix} & +\begin{vmatrix} 0 & 2 & 0 \\ 2 & -5 & -1 \\ 3 & 1 & 5 \end{vmatrix} & -\begin{vmatrix} 0 & 1 & 0 \\ 2 & -2 & -1 \\ 3 & -1 & 5 \end{vmatrix} & +\begin{vmatrix} 0 & 1 & 2 \\ 2 & -2 & -5 \\ 3 & -1 & 1 \end{vmatrix} \\ +\begin{vmatrix} 1 & 2 & 0 \\ 0 & 3 & 2 \\ -1 & 1 & 5 \end{vmatrix} & -\begin{vmatrix} 0 & 2 & 0 \\ 1 & 3 & 2 \\ 3 & 1 & 5 \end{vmatrix} & +\begin{vmatrix} 0 & 1 & 0 \\ 1 & 0 & 2 \\ 3 & -1 & 5 \end{vmatrix} & -\begin{vmatrix} 0 & 1 & 2 \\ 1 & 0 & 3 \\ 3 & -1 & 1 \end{vmatrix} \\ -\begin{vmatrix} 1 & 2 & 0 \\ 0 & 3 & 2 \\ -2 & -5 & -1 \end{vmatrix} & +\begin{vmatrix} 0 & 2 & 0 \\ 1 & 3 & 2 \\ 2 & -5 & -1 \end{vmatrix} & -\begin{vmatrix} 0 & 1 & 0 \\ 1 & 0 & 2 \\ 2 & -2 & -1 \end{vmatrix} & +\begin{vmatrix} 0 & 1 & 2 \\ 1 & 0 & 3 \\ 2 & -2 & -5 \end{vmatrix} \end{bmatrix}$$

$$\text{Cofactors}(A)=\begin{bmatrix} 19 & 29 & -3 & -5 \\ 2 & -26 & 13 & -9 \\ 9 & -2 & 1 & -6 \\ 1 & 10 & -5 & 7 \end{bmatrix}$$

adj(A)=[Cofactors(A)]^T

$$\text{adj}(A)=\begin{bmatrix} 19 & 2 & 9 & 1 \\ 29 & -26 & -2 & 10 \\ -3 & 13 & 1 & -5 \\ -5 & -9 & -6 & 7 \end{bmatrix}$$

$$A^{-1} = \frac{adj(A)}{|A|}$$

$$A^{-1} = \frac{\begin{bmatrix} 19 & 2 & 9 & 1 \\ 29 & -26 & -2 & 10 \\ -3 & 13 & 1 & -5 \\ -5 & -9 & -6 & 7 \end{bmatrix}(mod27)}{23}$$

$$\Rightarrow A^{-1} = (23)^{-1}\begin{bmatrix} 19 & 2 & 9 & 1 \\ 29 & -26 & -2 & 10 \\ -3 & 13 & 1 & -5 \\ -5 & -9 & -6 & 7 \end{bmatrix} mod27$$

$$\Rightarrow A^{-1} = 20\begin{bmatrix} 19 & 2 & 9 & 1 \\ 29 & -26 & -2 & 10 \\ -3 & 13 & 1 & -5 \\ -5 & -9 & -6 & 7 \end{bmatrix} mod27$$

$$\Rightarrow A^{-1} = \begin{bmatrix} 380 & 40 & 180 & 20 \\ 580 & -520 & -40 & 200 \\ -60 & 260 & 20 & -100 \\ -100 & -180 & -120 & 140 \end{bmatrix} mod27$$

$$\Rightarrow A^{-1} = \begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}$$

Decryption

Plain text= ((key matrix)$^{-1}$* cipher text) $mod27$

$$\begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}\begin{bmatrix} P \\ C \\ H \\ K \end{bmatrix} mod27 = \begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}\begin{bmatrix} 16 \\ 3 \\ -19 \\ 11 \end{bmatrix} mod27$$

$$= \begin{bmatrix} 2(16) + 13(3) - 18(19) + 20(11) \\ 13(16) - 7(3) + 13(19) + 11(11) \\ -6(16) + 17(3) - 20(19) - 19(11) \\ -19(16) - 18(3) + 12(19) + 5(11) \end{bmatrix} mod27$$

$$= \begin{bmatrix} -51 \\ 555 \\ -634 \\ -75 \end{bmatrix} mod27 = \begin{bmatrix} -24 \\ 15 \\ -13 \\ -21 \end{bmatrix} = \begin{bmatrix} C \\ O \\ N \\ F \end{bmatrix}$$

$\boldsymbol{PCHK \Longrightarrow CONF}$

Similarly

$$\begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}\begin{bmatrix} N \\ Y \\ Y \\ Q \end{bmatrix} mod27 = \begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}\begin{bmatrix} 14 \\ 25 \\ -2 \\ 17 \end{bmatrix} mod27$$

$$= \begin{bmatrix} 657 \\ 220 \\ -22 \\ -607 \end{bmatrix} mod27 = \begin{bmatrix} 9 \\ 4 \\ -22 \\ -13 \end{bmatrix} = \begin{bmatrix} I \\ D \\ E \\ N \end{bmatrix}$$

$$\boldsymbol{NYYQ \Longrightarrow IDEN}$$

$$\begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}\begin{bmatrix} K \\ T \\ E \\ D \end{bmatrix} mod27 = \begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}\begin{bmatrix} 11 \\ 20 \\ 5 \\ 4 \end{bmatrix} mod27$$

$$= \begin{bmatrix} 452 \\ -18 \\ 298 \\ -609 \end{bmatrix} mod27 = \begin{bmatrix} 20 \\ -18 \\ 1 \\ -15 \end{bmatrix} = \begin{bmatrix} T \\ I \\ A \\ L \end{bmatrix}$$

$$\boldsymbol{KTED \Longrightarrow TIAL}$$

$$\begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}\begin{bmatrix} V \\ A \\ L \\ L \end{bmatrix} mod27 = \begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}\begin{bmatrix} 22 \\ 1 \\ -15 \\ 12 \end{bmatrix} mod27$$

$$= \begin{bmatrix} 27 \\ 606 \\ -643 \\ -196 \end{bmatrix} mod27 = \begin{bmatrix} 0 \\ 12 \\ -22 \\ -7 \end{bmatrix} = \begin{bmatrix} \bar{L} \\ E \\ T \end{bmatrix}$$

$$\boldsymbol{VALL \Longrightarrow \_LET}$$

$$\begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}\begin{bmatrix} N \\ T \\ U \\ S \end{bmatrix} mod27 = \begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}\begin{bmatrix} 14 \\ 20 \\ -6 \\ 19 \end{bmatrix} mod27$$

$$= \begin{bmatrix} 560 \\ 329 \\ -225 \\ -459 \end{bmatrix} mod27 = \begin{bmatrix} 20 \\ 5 \\ -9 \\ 0 \end{bmatrix} = \begin{bmatrix} T \\ E \\ R \\ \_ \end{bmatrix}$$

$$\boldsymbol{NTUS \Longrightarrow TER\_}$$

$$\begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}\begin{bmatrix} N \\ O \\ N \\ A \end{bmatrix} mod27 = \begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}\begin{bmatrix} 14 \\ 15 \\ -13 \\ 1 \end{bmatrix} mod27$$

$$= \begin{bmatrix} 9 \\ 257 \\ -108 \\ -375 \end{bmatrix} mod27 = \begin{bmatrix} 9 \\ 14 \\ 0 \\ -24 \end{bmatrix} = \begin{bmatrix} I \\ N \\ \_ \\ C \end{bmatrix}$$

$\boldsymbol{NONA \Longrightarrow IN\_C}$

$$\begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}\begin{bmatrix} T \\ C \\ L \\ P \end{bmatrix} mod27 = \begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}\begin{bmatrix} 20 \\ 3 \\ -15 \\ 16 \end{bmatrix} mod27$$

$$= \begin{bmatrix} 129 \\ 610 \\ -673 \\ -174 \end{bmatrix} mod27 = \begin{bmatrix} 21 \\ 16 \\ -25 \\ -12 \end{bmatrix} = \begin{bmatrix} U \\ P \\ B \\ O \end{bmatrix}$$

$\boldsymbol{TCLP \Longrightarrow UPBO}$

$$\begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}\begin{bmatrix} Z \\ M \\ - \\ P \end{bmatrix} mod27 = \begin{bmatrix} 2 & 13 & 18 & 20 \\ 13 & -7 & -13 & 11 \\ -6 & 17 & 20 & -19 \\ -19 & -18 & -12 & 5 \end{bmatrix}\begin{bmatrix} 26 \\ 13 \\ 0 \\ -11 \end{bmatrix} mod27$$

$$= \begin{bmatrix} 1 \\ 126 \\ 274 \\ -783 \end{bmatrix} mod27 = \begin{bmatrix} 1 \\ 18 \\ 4 \\ 0 \end{bmatrix} = \begin{bmatrix} A \\ R \\ D \\ \_ \end{bmatrix}$$

$\boldsymbol{ZM\_P \Longrightarrow ARD\_}$

$\boldsymbol{PCHKNYYQKTED\ VALLNTUSNONAZM\_P \Longrightarrow CONFIDENTIAL\ LETTER\ IN\ CUPBOARD}$

Here the decrypted cipher text **PCHKNYYQKTED VALLNTUSNONAZM − P has encrypted to the original plain text "CONFIDENTIAL LETTER IN CUPBOARD"**

Conclusion:

This paper concludes that the plain text can be transferred to cipher text using 4 x 4 non-singular matrices modulo 27 as the key to encrypt plain text and using its invertible matrices of order 4 x 4 non-singular matrices modulo 27 as the key to decrypt cipher text. The large messages couldn't decrypt without key matrix and congruence relations. The aim of this paper is to store messages and also transfer over internet confidentially. This helps to protect the large messages to maintain military secrets. Even we can use 2x 2 non singular matrices modulo 27 and 3 x 3 non singular matrices modulo 27 as key to encrypt (encode) plain text and using its invertible matrices as the key to decrypt(decode) cipher text.

References:

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

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

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

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

Cite this Article:

Veena T, "APPLICATIONS OF NON-SINGULAR MATRICES IN CRYPTOGRAPHY", *International Journal of Scientific Research in Modern Science and Technology (IJSRMST),* ***ISSN:*** *2583-7605 (Online), Volume 2, Issue 9, pp. 15- 25, September 2023.* ***Journal URL:*** *https://ijsrmst.com/*