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.v2i9.142

A METHOD FOR ENCRYPTION AND DECRYPTION OF LARGE MESSAGES BY USING NON-SINGULAR MATRIX

Veena T

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

Email: veenavenki.t03@gmail.com

ABSTRACT

The objective of this paper is security for large messages helps to maintain secret by using 3 x 3 non-singular matrix modulo27 as key to transfer plain text to cipher text and invertible matrix modulo 27 of order 3 x 3 as key to transfer cipher text to plain text.

Keywords: Non-singular matrix, Plain text, Cipher text, Decryption, Encryption, Key matrix andcongruence modulo m.

INTRODUCTION:

Encryption is a process of converting normal message (plaintext) in to meaningless message (cipher text) whereas decryption is the process of converting meaningless message(cipher text) in to its original form(plaintext). Encryption is the method by which information is converted in to secret code. The key matrix is used to encrypt the messages, and its inverse is used to decrypt the encoded messages. It is important that the key matrix be kept secret. This paper helpful to maintain large messages confidentially.

Non singular matrix:

Non singular matrix is a square matrix whose determinant is not equal to zero.

Cryptography:

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix “graphy” means “writing”.

Plain text:

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

Ex: I AM IN DANGER ZONE SAVE ME

Cipher text:

A message written in secret code.

Ex: **A message** "I AM IN DANGER ZONE SAVE ME" is written in secret code as TCLQLMI_ZCYIAXWNOBURHGHKWNA

Key matrix:

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

Encryption:

The process of converting plain text in to an unintelligible format (cipher text) is called Encryption.

Decryption:

The process of converting cipher text in to a plain text is called decryption.

Congruence modulo m:

If m is a positive integer (>1) and a and b are any integers, then 'a' is said to be congruent to b modulo m iff m divides $(a-b)$. In symbols we write as $a \equiv b(modm)$

Definition:

Inverse of an integer a to modulo m is a^{-1} such that $a * a^{-1} \equiv 1modm$, where a^{-1} is called inverse of 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 $x * x^{-1} \equiv 1(modm)$

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

Method:

Suppose we given non singular matrix $K = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$ as an encryption key, such that K^{-1} exists and a message "I AM IN DANGER ZONE SAVE ME ".

To encrypt the message using 3 x 3 non singular matrix modulo27, first we have to assign each character to a single numerical value such that A=1,B=2,C=3,…….,Z=26 and space or _=0, next break the plain text (message) in to Trigraph and convert them in to column matrix as $\begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix}$ and multiply with key matrix to generate the following linear systems.

$$D_1 = p_1a_{11} + p_2a_{12} + p_3a_{13}$$
$$D_2 = p_1a_{21} + p_2a_{22} + p_3a_{23}$$
$$D_3 = p_1a_{31} + p_2a_{32} + p_3a_{33}$$

Or we can expressed as matrices multiplication

$$\begin{bmatrix} D_1 \\ D_2 \\ D_3 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \Rightarrow D = KP$$

Where P and D are column vectors of length 3, representing the plain text and cipher text respectively and K is a 3 x 3 matrix, which is known for both Sender and Receiver.

Example:

Use the key matrix $\boldsymbol{K = \begin{bmatrix} 2 & 1 & 2 \\ 3 & 2 & 3 \\ 1 & 1 & 3 \end{bmatrix}}$ encrypt the message “I AM IN DANGER ZONE SAVE ME ”

Sol^n: First break the plain text “I AM IN DANGER ZONE SAVE ME ” in to three consecutive character including space as follows.

I AM IN DANGER ZONE SAVE ME ⇒ I_A M _I   N _D ANG ER _   ZON E _S AVE _ME

Convert the character in to corresponding numerical vector values

I_A= $\begin{bmatrix} 9 \\ 0 \\ 1 \end{bmatrix}$, M _I = $\begin{bmatrix} 13 \\ 0 \\ 9 \end{bmatrix}$, N_D= $\begin{bmatrix} 14 \\ 0 \\ 4 \end{bmatrix}$, ANG= $\begin{bmatrix} 1 \\ 14 \\ 7 \end{bmatrix}$, ER_= $\begin{bmatrix} 5 \\ 18 \\ 0 \end{bmatrix}$, ZON= $\begin{bmatrix} 26 \\ 15 \\ 14 \end{bmatrix}$, E_S= $\begin{bmatrix} 5 \\ 0 \\ 19 \end{bmatrix}$,

AVE= $\begin{bmatrix} 1 \\ 22 \\ 5 \end{bmatrix}$, _ME= $\begin{bmatrix} 0 \\ 13 \\ 5 \end{bmatrix}$

By multiplying the key matrix by column vectors matrices (plaintext) in order to get the corresponding numerical vectors value, which can convert to corresponding cipher text.

$$\boldsymbol{D} = (\boldsymbol{K} * \boldsymbol{Plain\ text})\ \boldsymbol{mod27}$$

$$\boldsymbol{D} = \begin{bmatrix} \mathbf{2} & \mathbf{1} & \mathbf{2} \\ \mathbf{3} & \mathbf{2} & \mathbf{3} \\ \mathbf{1} & \mathbf{1} & \mathbf{3} \end{bmatrix} \begin{bmatrix} I \\ \_ \\ A \end{bmatrix} mod27 = \begin{bmatrix} \mathbf{2} & \mathbf{1} & \mathbf{2} \\ \mathbf{3} & \mathbf{2} & \mathbf{3} \\ \mathbf{1} & \mathbf{1} & \mathbf{3} \end{bmatrix} \begin{bmatrix} 9 \\ 0 \\ 1 \end{bmatrix} mod27 = \begin{bmatrix} 2(9) + 1(0) + 2(1) \\ 3(9) + 2(0) + 3(1) \\ 1(9) + 1(0) + 3(1) \end{bmatrix} mod27$$

$$= \begin{bmatrix} 20 \\ 30 \\ 12 \end{bmatrix} mod27 \ = \begin{bmatrix} 20 \\ 3 \\ 12 \end{bmatrix},$$

I_A ⟹ TCL

Similarly

$$\begin{bmatrix}\mathbf{2} & \mathbf{1} & \mathbf{2}\\ \mathbf{3} & \mathbf{2} & \mathbf{3}\\ \mathbf{1} & \mathbf{1} & \mathbf{3}\end{bmatrix}\begin{bmatrix}13\\0\\9\end{bmatrix} mod27 = \begin{bmatrix}2(13)+1(0)+2(9)\\3(13)+2(0)+3(9)\\1(13)+1(0)+3(9)\end{bmatrix} mod27 = \begin{bmatrix}44\\66\\40\end{bmatrix} mod27 = \begin{bmatrix}17\\12\\13\end{bmatrix},$$

M_I ⟹ QLM

$$\begin{bmatrix}\mathbf{2} & \mathbf{1} & \mathbf{2}\\ \mathbf{3} & \mathbf{2} & \mathbf{3}\\ \mathbf{1} & \mathbf{1} & \mathbf{3}\end{bmatrix}\begin{bmatrix}14\\0\\4\end{bmatrix} mod27 = \begin{bmatrix}2(14)+1(0)+2(4)\\3(14)+2(0)+3(4)\\1(14)+1(0)+3(4)\end{bmatrix} mod27 = \begin{bmatrix}36\\54\\26\end{bmatrix} mod27 = \begin{bmatrix}9\\0\\26\end{bmatrix},$$

N_D ⟹ I_Z

$$\begin{bmatrix}\mathbf{2} & \mathbf{1} & \mathbf{2}\\ \mathbf{3} & \mathbf{2} & \mathbf{3}\\ \mathbf{1} & \mathbf{1} & \mathbf{3}\end{bmatrix}\begin{bmatrix}1\\14\\7\end{bmatrix} mod27 = \begin{bmatrix}2(1)+1(14)+2(7)\\3(1)+2(14)+3(7)\\1(1)+1(14)+3(7)\end{bmatrix} mod27 = \begin{bmatrix}30\\52\\36\end{bmatrix} mod27 = \begin{bmatrix}3\\25\\9\end{bmatrix},$$

ANG ⟹ CYI

$$\begin{bmatrix}\mathbf{2} & \mathbf{1} & \mathbf{2}\\ \mathbf{3} & \mathbf{2} & \mathbf{3}\\ \mathbf{1} & \mathbf{1} & \mathbf{3}\end{bmatrix}\begin{bmatrix}5\\18\\0\end{bmatrix} mod27 = \begin{bmatrix}2(5)+1(18)+2(0)\\3(5)+2(18)+3(0)\\1(5)+1(18)+3(0)\end{bmatrix} mod27 = \begin{bmatrix}28\\51\\23\end{bmatrix} mod27 = \begin{bmatrix}1\\24\\23\end{bmatrix},$$

ER_ ⟹ AXW

$$\begin{bmatrix}\mathbf{2} & \mathbf{1} & \mathbf{2}\\ \mathbf{3} & \mathbf{2} & \mathbf{3}\\ \mathbf{1} & \mathbf{1} & \mathbf{3}\end{bmatrix}\begin{bmatrix}26\\15\\14\end{bmatrix} mod27 = \begin{bmatrix}2(26)+1(15)+2(14)\\3(26)+2(15)+3(14)\\1(26)+1(15)+3(14)\end{bmatrix} mod27 = \begin{bmatrix}95\\150\\83\end{bmatrix} mod27 = \begin{bmatrix}14\\15\\2\end{bmatrix},$$

ZON⟹NOB

$$\begin{bmatrix}\mathbf{2} & \mathbf{1} & \mathbf{2}\\ \mathbf{3} & \mathbf{2} & \mathbf{3}\\ \mathbf{1} & \mathbf{1} & \mathbf{3}\end{bmatrix}\begin{bmatrix}5\\0\\19\end{bmatrix} mod27 = \begin{bmatrix}2(5)+1(0)+2(19)\\3(5)+2(0)+3(19)\\1(5)+1(0)+3(19)\end{bmatrix} mod27 = \begin{bmatrix}48\\72\\62\end{bmatrix} mod27 = \begin{bmatrix}21\\18\\8\end{bmatrix},$$

E_S ⟹ URH

$$\begin{bmatrix}\mathbf{2} & \mathbf{1} & \mathbf{2}\\ \mathbf{3} & \mathbf{2} & \mathbf{3}\\ \mathbf{1} & \mathbf{1} & \mathbf{3}\end{bmatrix}\begin{bmatrix}1\\22\\5\end{bmatrix} mod27 = \begin{bmatrix}2(1)+1(22)+2(5)\\3(1)+2(22)+3(5)\\1(1)+1(22)+3(5)\end{bmatrix} mod27 = \begin{bmatrix}34\\62\\38\end{bmatrix} mod27 = \begin{bmatrix}7\\8\\11\end{bmatrix},$$

AVE⟹GHK

$$\begin{bmatrix}\mathbf{2} & \mathbf{1} & \mathbf{2}\\ \mathbf{3} & \mathbf{2} & \mathbf{3}\\ \mathbf{1} & \mathbf{1} & \mathbf{3}\end{bmatrix}\begin{bmatrix}0\\13\\5\end{bmatrix} mod27 = \begin{bmatrix}2(0)+1(13)+2(5)\\3(0)+2(13)+3(5)\\1(0)+1(13)+3(5)\end{bmatrix} mod27 = \begin{bmatrix}23\\41\\28\end{bmatrix} mod27 = \begin{bmatrix}23\\14\\1\end{bmatrix},$$

_ME ⟹ WNA

Then plain text “I AM IN DANGER ZONE SAVE ME” has been encrypted to “TCLQLMI_ZCYIAXWNOBURHGHKWNA”

To decrypt the message “TCLQLMI_ZCYIAXWNOBURHGHKWNA” to the original one, we use the inverse of key matrix, such that

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

adj(K)=$\begin{bmatrix} 3 & -1 & -1 \\ -6 & 4 & 0 \\ 1 & -1 & 1 \end{bmatrix} mod27$

$|K| = \begin{vmatrix} 2 & 1 & 2 \\ 3 & 2 & 3 \\ 1 & 1 & 3 \end{vmatrix}$

$\Rightarrow |K| = 2(6-3) - 1(9-3) + 2(3-2)$

$\Rightarrow |K| = 2(3) - 1(6) + 2(1)$

$\Rightarrow |K| = 6 - 6 + 2 = 2 \neq 0$

$K^{-1} = \frac{1}{2}\begin{bmatrix} 3 & -1 & -1 \\ -6 & 4 & 0 \\ 1 & -1 & 1 \end{bmatrix} mod27 = 2^{-1}\begin{bmatrix} 3 & -1 & -1 \\ -6 & 4 & 0 \\ 1 & -1 & 1 \end{bmatrix} mod27$

To find multiplicative inverse of determinant:

$x * x^{-1} \equiv 1(mod27)$

$\Longrightarrow 2 * 2^{-1} \equiv 1(mod27)$

$\Longrightarrow$2*14$\equiv$ $1(mod27)$

Since 2 inverse is 14

$K^{-1} = 14\begin{bmatrix} 3 & -1 & -1 \\ -6 & 4 & 0 \\ 1 & -1 & 1 \end{bmatrix} mod27 = \begin{bmatrix} 42 & -14 & -14 \\ -84 & 56 & 0 \\ 14 & -14 & 14 \end{bmatrix} mod27 = \begin{bmatrix} 15 & 13 & 13 \\ 24 & 2 & 0 \\ 14 & 13 & 14 \end{bmatrix}$

$D = (K^{-1} * cipher\ text)mod27$

$$\begin{bmatrix} 15 & 13 & 13 \\ 24 & 2 & 0 \\ 14 & 13 & 14 \end{bmatrix}\begin{bmatrix} T \\ C \\ L \end{bmatrix} mod27 = \begin{bmatrix} 15 & 13 & 13 \\ 24 & 2 & 0 \\ 14 & 13 & 14 \end{bmatrix}\begin{bmatrix} 20 \\ 3 \\ 12 \end{bmatrix} mod27$$

$$= \begin{bmatrix} 15(20) + 13(3) + 13(12) \\ 24(20) + 2(3) + 0(12) \\ 14(20) + 13(3) + 14(12) \end{bmatrix} mod27$$

$$= \begin{bmatrix} 495 \\ 486 \\ 487 \end{bmatrix} mod27 = \begin{bmatrix} 9 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} I \\ \_ \\ A \end{bmatrix},$$

TCL ⇒ **I_A**

Similarly

$$\begin{bmatrix} 15 & 13 & 13 \\ 24 & 2 & 0 \\ 14 & 13 & 14 \end{bmatrix}\begin{bmatrix} Q \\ L \\ M \end{bmatrix} mod27 = \begin{bmatrix} 15 & 13 & 13 \\ 24 & 2 & 0 \\ 14 & 13 & 14 \end{bmatrix}\begin{bmatrix} 17 \\ 12 \\ 13 \end{bmatrix} mod27 = \begin{bmatrix} 580 \\ 432 \\ 576 \end{bmatrix} mod27 = \begin{bmatrix} 13 \\ 0 \\ 9 \end{bmatrix},$$

QLM ⇒ **M_I**

$$\begin{bmatrix}15 & 13 & 13\\24 & 2 & 0\\14 & 13 & 14\end{bmatrix}\begin{bmatrix}I\\\_\\Z\end{bmatrix}mod27=\begin{bmatrix}15 & 13 & 13\\24 & 2 & 0\\14 & 13 & 14\end{bmatrix}\begin{bmatrix}9\\0\\26\end{bmatrix}mod27=\begin{bmatrix}473\\216\\490\end{bmatrix}mod27=\begin{bmatrix}14\\0\\4\end{bmatrix},$$

I_Z ⇒ N_D

$$\begin{bmatrix}15 & 13 & 13\\24 & 2 & 0\\14 & 13 & 14\end{bmatrix}\begin{bmatrix}C\\Y\\I\end{bmatrix}mod27=\begin{bmatrix}15 & 13 & 13\\24 & 2 & 0\\14 & 13 & 14\end{bmatrix}\begin{bmatrix}3\\25\\9\end{bmatrix}mod27=\begin{bmatrix}487\\122\\493\end{bmatrix}mod27=\begin{bmatrix}1\\14\\7\end{bmatrix},$$

CYI ⇒ ANG

$$\begin{bmatrix}15 & 13 & 13\\24 & 2 & 0\\14 & 13 & 14\end{bmatrix}\begin{bmatrix}A\\X\\W\end{bmatrix}mod27=\begin{bmatrix}15 & 13 & 13\\24 & 2 & 0\\14 & 13 & 14\end{bmatrix}\begin{bmatrix}1\\24\\23\end{bmatrix}mod27=\begin{bmatrix}626\\72\\648\end{bmatrix}mod27=\begin{bmatrix}5\\18\\0\end{bmatrix},$$

AXW ⇒ ER_

$$\begin{bmatrix}15 & 13 & 13\\24 & 2 & 0\\14 & 13 & 14\end{bmatrix}\begin{bmatrix}N\\O\\B\end{bmatrix}mod27=\begin{bmatrix}15 & 13 & 13\\24 & 2 & 0\\14 & 13 & 14\end{bmatrix}\begin{bmatrix}14\\15\\2\end{bmatrix}mod27=\begin{bmatrix}431\\366\\419\end{bmatrix}mod27=\begin{bmatrix}26\\15\\14\end{bmatrix},$$

NOB ⇒ ZON

$$\begin{bmatrix}15 & 13 & 13\\24 & 2 & 0\\14 & 13 & 14\end{bmatrix}\begin{bmatrix}U\\R\\H\end{bmatrix}mod27=\begin{bmatrix}15 & 13 & 13\\24 & 2 & 0\\14 & 13 & 14\end{bmatrix}\begin{bmatrix}21\\18\\8\end{bmatrix}mod27=\begin{bmatrix}653\\540\\640\end{bmatrix}mod27=\begin{bmatrix}5\\0\\19\end{bmatrix},$$

URH ⇒ E_S

$$\begin{bmatrix}15 & 13 & 13\\24 & 2 & 0\\14 & 13 & 14\end{bmatrix}\begin{bmatrix}G\\H\\K\end{bmatrix}mod27=\begin{bmatrix}15 & 13 & 13\\24 & 2 & 0\\14 & 13 & 14\end{bmatrix}\begin{bmatrix}7\\8\\11\end{bmatrix}mod27=\begin{bmatrix}352\\184\\356\end{bmatrix}mod27=\begin{bmatrix}1\\22\\5\end{bmatrix},$$

GHK ⇒ AVE

$$\begin{bmatrix}15 & 13 & 13\\24 & 2 & 0\\14 & 13 & 14\end{bmatrix}\begin{bmatrix}W\\N\\A\end{bmatrix}mod27=\begin{bmatrix}15 & 13 & 13\\24 & 2 & 0\\14 & 13 & 14\end{bmatrix}\begin{bmatrix}23\\14\\1\end{bmatrix}mod27=\begin{bmatrix}540\\580\\518\end{bmatrix}mod27=\begin{bmatrix}0\\13\\5\end{bmatrix},$$

WNA⇒_ME

Then decrypted message is “I AM IN DANGER ZONE SAVE ME”

Conclusion:

This paper concludes that the plain text can be transferred to cipher text using 3 x 3 non-singular matrix of modulo 27 as key to encrypt plain text and using invertible matrix of order 3 x 3 as a key to decrypt cipher text. The large information couldn’t decrypt without key matrix and congruence relations. The aim of this paper is to store information and also transfer over internet confidentially. This helps to protect the large messages to maintain military secrets.

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.

Cite this Article:

Veena T, " A METHOD FOR ENCRYPTION AND DECRYPTION OF LARGE MESSAGES BY USING NON-SINGULAR MATRIX ", *International Journal of Scientific Research in Modern Science and Technology (IJSRMST),* ***ISSN:*** *2583-7605 (Online), Volume 2, Issue 9, pp. 08- 14, September 2023.* ***Journal URL:*** *https://ijsrmst.com/*