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.v2i9.140

ENCRYPTION AND DECRYPTION OF MESSAGES BY USING MATRICES

Veena T

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

Email: veenavenki.t03@gmail.com

ABSTRACT

This paper focus on security for large or short messages helps to maintain army secrets by using 2 x 2 non-singular matrix modulo 27 as key to encrypt and invertible matrix modulo 27 of order 2 x 2 as key to decrypt messages.

Keywords: Cryptography, Plain text, Cipher text, Encryption and Decryption, Matrix, Key and non singular matrix.

INTRODUCTION:

Cryptography is a branch of computer science and Mathematics. It is a science of writing or reading coded messages. It is derived from the Greek kryptos, meaning hidden. The prefix "crypt" means "hidden" or "secret," and the suffix" graphy stands for "writing". Transmission and storage of multimedia data like images, audio and videos over the internet has increased in today's digital communication. Among the various multimedia data, messages are transmitted and used very often. It is necessary to protect the messages to maintain army secrets. For the purpose of privacy and security, we need to encrypt the message at the sender side and decrypt it at the receiver side.

Cipher text: A message written in secret code.

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.

Encryption: The process of converting plain text in to a cipher text is called encryption.

Ex: Plain text is **TERRORISTS WILL ARRIVE TODAY EVENING IN MUMBAI.**

Cipher text is **PLI_ _LKMQNSKXLIFLWRRVVMZZJZXJTVVFYBQRIOP_NPSUN**

Decryption: The process of converting cipher text to plain text is called decryption.

Key: Key is a secret piece of information which is used for encryption and decryption in cryptography.

Encryption=(key*plaintext)mod27

Decryption=(key^{-1}*cipher text)mod27

Method:

Consider a 2 x 2 non singular matrix $\boldsymbol{A} = \begin{bmatrix} \boldsymbol{a_{11}} & \boldsymbol{a_{12}} \\ \boldsymbol{a_{21}} & \boldsymbol{a_{22}} \end{bmatrix}$ as an encryption key, such that A^{-1} exists.

To encrypt a message **"TERRORISTS WILL ARRIVE TODAY EVENING IN MUMBAI"** use 2 x 2 non singular matrix modulo27. Next we have to assign each alphabet or character to a 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

Again break the plain text (message) in to digraph and convert vector matrix as $P = \begin{bmatrix} p_1 \\ p_2 \end{bmatrix}$ and multiplying with key matrix to obtain the following linear system

$$c_1 = p_1 a_{11} + p_2 a_{12}$$
$$c_2 = p_1 a_{21} + p_2 a_{22}$$

Or we can expressed as matrices multiplication

$$\begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \end{bmatrix} \Rightarrow C = AP$$

Here P and C are column vectors of length 2, representing plain text and cipher text respectively and A is a 2 x 2 matrix, which is known for both Sender and Receiver.

To decrypt message this table is needed

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

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

Example

1. Use the key matrix $\boldsymbol{A} = \begin{bmatrix} \boldsymbol{3} & \boldsymbol{2} \\ \boldsymbol{5} & \boldsymbol{4} \end{bmatrix}$, encrypt the message " TERRORISTS WILL ARRIVE TODAY EVENING IN MUMBAI" and to decrypt the message to the original one use its inverse of key matrix.

Sol^{n}: First break the plain text "TERRORISTS WILL ARRIVE TODAY EVENING IN MUMBAI" in to two consecutive letters, TERRORISTS_WILL_ARRIVE_TODAY_ EVENING_ IN_MUMBAI.

Convert each character in to corresponding numerical vector values.

TE=$\begin{bmatrix}20\\5\end{bmatrix}$, RR=$\begin{bmatrix}18\\18\end{bmatrix}$, OR=$\begin{bmatrix}15\\18\end{bmatrix}$, IS=$\begin{bmatrix}9\\19\end{bmatrix}$, TS=$\begin{bmatrix}20\\19\end{bmatrix}$, _W=$\begin{bmatrix}0\\23\end{bmatrix}$, IL=$\begin{bmatrix}9\\12\end{bmatrix}$, L_=$\begin{bmatrix}12\\0\end{bmatrix}$, AR=$\begin{bmatrix}1\\18\end{bmatrix}$,

RI=$\begin{bmatrix}18\\9\end{bmatrix}$, VE=$\begin{bmatrix}22\\5\end{bmatrix}$, T=$\begin{bmatrix}0\\20\end{bmatrix}$, OD=$\begin{bmatrix}15\\4\end{bmatrix}$, AY=$\begin{bmatrix}1\\25\end{bmatrix}$, _ E=$\begin{bmatrix}0\\5\end{bmatrix}$, VE=$\begin{bmatrix}22\\5\end{bmatrix}$, NI=$\begin{bmatrix}14\\9\end{bmatrix}$, NG=$\begin{bmatrix}14\\7\end{bmatrix}$,

_ I=$\begin{bmatrix}0\\9\end{bmatrix}$, N_=$\begin{bmatrix}14\\0\end{bmatrix}$, MU=$\begin{bmatrix}13\\21\end{bmatrix}$, MB=$\begin{bmatrix}13\\2\end{bmatrix}$, AI=$\begin{bmatrix}1\\9\end{bmatrix}$

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

$\boldsymbol{C = A * P\ mod27}$

$\boldsymbol{C} = \boldsymbol{A}$ *TE=$\begin{bmatrix}\mathbf{3} & \mathbf{2}\\\mathbf{5} & \mathbf{4}\end{bmatrix}\begin{bmatrix}20\\5\end{bmatrix} mod27 = \begin{bmatrix}70\\120\end{bmatrix} mod27 = \begin{bmatrix}16\\12\end{bmatrix}$ =PL

Therefore plain text TE becomes PL

i.e TE ⟹PL

$C = A$ *RR=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}18\\18\end{bmatrix} mod27 = \begin{bmatrix}90\\162\end{bmatrix} mod27 = \begin{bmatrix}9\\0\end{bmatrix}$ = I_

RR ⟹I_

$C = A$ *OR=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}15\\18\end{bmatrix} mod27 = \begin{bmatrix}81\\147\end{bmatrix} mod27 = \begin{bmatrix}0\\12\end{bmatrix}$ =_L

OR⟹_L

$C = A$ *IS=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}9\\19\end{bmatrix} mod27 = \begin{bmatrix}65\\121\end{bmatrix} mod27 = \begin{bmatrix}11\\13\end{bmatrix}$ =KM

IS⟹ KM

$C = A$ *TS=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}20\\19\end{bmatrix} mod27 = \begin{bmatrix}98\\176\end{bmatrix} mod27 = \begin{bmatrix}17\\14\end{bmatrix}$ =QN

TS⟹ QN

$C = A$ *_W=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}0\\23\end{bmatrix} mod27 = \begin{bmatrix}46\\92\end{bmatrix} mod27 = \begin{bmatrix}19\\11\end{bmatrix}$ =SK

_W⟹SK

$C = A$ *IL=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}9\\12\end{bmatrix} mod27 = \begin{bmatrix}51\\93\end{bmatrix} mod27 = \begin{bmatrix}24\\12\end{bmatrix}$ =XL

IL⟹XL

$C = A$ *L_=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}12\\0\end{bmatrix} mod27 = \begin{bmatrix}36\\60\end{bmatrix} mod27 = \begin{bmatrix}9\\6\end{bmatrix}$ =IF

L_⟹IF

$C = A$ *AR=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}1\\18\end{bmatrix} mod27 = \begin{bmatrix}39\\77\end{bmatrix} mod27 = \begin{bmatrix}12\\23\end{bmatrix}$ =LW

AR⟹LW

$C = A$ *RI=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}18\\9\end{bmatrix} mod27 = \begin{bmatrix}72\\126\end{bmatrix} mod27 = \begin{bmatrix}18\\18\end{bmatrix}$ =RR

RI⟹RR

$C = A$ *VE=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}22\\5\end{bmatrix} mod27 = \begin{bmatrix}76\\130\end{bmatrix} mod27 = \begin{bmatrix}22\\22\end{bmatrix}$ =VV

VE⟹VV

$C = A$ *_T=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}0\\20\end{bmatrix}mod27 = \begin{bmatrix}40\\80\end{bmatrix}mod27 = \begin{bmatrix}13\\26\end{bmatrix}$ =MZ

_T⟹MZ

$C = A$ *OD=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}15\\4\end{bmatrix}mod27 = \begin{bmatrix}53\\91\end{bmatrix}mod27 = \begin{bmatrix}26\\10\end{bmatrix}$ =ZJ

OD⟹ZJ

$C = A$ *AY=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}1\\25\end{bmatrix}mod27 = \begin{bmatrix}53\\105\end{bmatrix}mod27 = \begin{bmatrix}26\\24\end{bmatrix}$ =ZX

AY⟹ZX

$C = A$ *_E=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}0\\5\end{bmatrix}mod27 = \begin{bmatrix}10\\20\end{bmatrix}mod27 = \begin{bmatrix}10\\20\end{bmatrix}$ =JT

_E⟹JT

$C = A$ *VE=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}22\\5\end{bmatrix}mod27 = \begin{bmatrix}76\\130\end{bmatrix}mod27 = \begin{bmatrix}22\\22\end{bmatrix}$ =VV

VE⟹VV

$C = A$ *NI=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}14\\9\end{bmatrix}mod27 = \begin{bmatrix}60\\106\end{bmatrix}mod27 = \begin{bmatrix}6\\25\end{bmatrix}$ =FY

NI⟹FY

$C = A$ *NG=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}14\\7\end{bmatrix}mod27 = \begin{bmatrix}56\\98\end{bmatrix}mod27 = \begin{bmatrix}2\\17\end{bmatrix}$ =BQ

NG⟹BQ

$C = A$ *_I=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}0\\9\end{bmatrix}mod27 = \begin{bmatrix}18\\9\end{bmatrix}mod27 = \begin{bmatrix}18\\9\end{bmatrix}$ =RI

_I⟹RI

$C = A$ *N_=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}14\\0\end{bmatrix}mod27 = \begin{bmatrix}42\\70\end{bmatrix}mod27 = \begin{bmatrix}15\\16\end{bmatrix}$ =OP

N_⟹OP

$C = A$ *MU=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}13\\21\end{bmatrix}mod27 = \begin{bmatrix}81\\149\end{bmatrix}mod27 = \begin{bmatrix}0\\14\end{bmatrix}$ =_N

MU⟹_N

$C = A$ *MB=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}13\\2\end{bmatrix}, mod27 = \begin{bmatrix}43\\73\end{bmatrix}mod27 = \begin{bmatrix}16\\19\end{bmatrix}$ =PS

MB⟹PS

$C = A$ *AI=$\begin{bmatrix}3 & 2\\5 & 4\end{bmatrix}\begin{bmatrix}1\\9\end{bmatrix}, mod27 = \begin{bmatrix}21\\41\end{bmatrix}mod27 = \begin{bmatrix}21\\14\end{bmatrix}$ =UN

AI⟹UN

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

$$A^{-1} = \frac{adjA}{|A|}$$

$$adjA = \begin{bmatrix}4 & -2\\-5 & 3\end{bmatrix}$$

$$|A| = \begin{vmatrix}3 & 2\\5 & 4\end{vmatrix}$$

$$|A| = 12 - 10 = 2$$

$$A^{-1} = \frac{\begin{bmatrix} 4 & -2 \\ -5 & 3 \end{bmatrix}}{2} mod27$$

To find multiplicative inverse of determinant

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

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

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

Since 2 inverse is 14

$A^{-1} = 14\begin{bmatrix} 4 & -2 \\ -5 & 3 \end{bmatrix} mod27$

$$\Rightarrow \quad A^{-1} = \begin{bmatrix} 4(14) & -2(14) \\ -5(14) & 3(14) \end{bmatrix} mod27$$

$$\Rightarrow A^{-1} = \begin{bmatrix} 56 & -28 \\ -70 & 42 \end{bmatrix} mod27$$

$$\Rightarrow A^{-1} = \begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix}$$

Now multiplying the inverse matrix with column vector matrices which generated from matrix operations $A^{-1}P(mod27)$. Thus

D=A^{-1}*PL=$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix}\begin{bmatrix} 16 \\ 12 \end{bmatrix} mod27 = \begin{bmatrix} 20 \\ 5 \end{bmatrix}$ =TE , PL⇒TE

D=A^{-1}*I_=$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix}\begin{bmatrix} 9 \\ 0 \end{bmatrix} mod27 = \begin{bmatrix} 18 \\ 99 \end{bmatrix} mod27 = \begin{bmatrix} 18 \\ 18 \end{bmatrix}$ =RR , I_⇒ RR

D=A^{-1}*_L=$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix}\begin{bmatrix} 0 \\ 12 \end{bmatrix} mod27 = \begin{bmatrix} 15 \\ 18 \end{bmatrix} mod27 = \begin{bmatrix} 15 \\ 18 \end{bmatrix}$ =OR , _L ⇒ OR

D=A^{-1}*KM=$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix}\begin{bmatrix} 11 \\ 13 \end{bmatrix} mod27 = \begin{bmatrix} 360 \\ 316 \end{bmatrix} mod27 = \begin{bmatrix} 9 \\ 19 \end{bmatrix}$ =IS , KM ⇒ IS

D=A^{-1}*QN=$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix}\begin{bmatrix} 17 \\ 14 \end{bmatrix} mod27 = \begin{bmatrix} 398 \\ 397 \end{bmatrix} mod27 = \begin{bmatrix} 20 \\ 19 \end{bmatrix}$ =TS , QN ⇒ TS

D=A^{-1}*SK=$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix}\begin{bmatrix} 19 \\ 11 \end{bmatrix} mod27 = \begin{bmatrix} 324 \\ 374 \end{bmatrix} mod27 = \begin{bmatrix} 0 \\ 23 \end{bmatrix}$ =_W , SK ⇒ _W

D=A^{-1}*XL=$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix}\begin{bmatrix} 24 \\ 12 \end{bmatrix} mod27 = \begin{bmatrix} 360 \\ 444 \end{bmatrix} mod27 = \begin{bmatrix} 9 \\ 12 \end{bmatrix}$ =IL , XL ⇒ IL

D=A^{-1}*IF=$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix}\begin{bmatrix} 9 \\ 6 \end{bmatrix} mod27 = \begin{bmatrix} 174 \\ 189 \end{bmatrix} mod27 = \begin{bmatrix} 12 \\ 0 \end{bmatrix}$ =L_ , IF ⇒ L_

D=A^{-1}*LW =$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix} \begin{bmatrix} 12 \\ 23 \end{bmatrix} mod27 = \begin{bmatrix} 622 \\ 477 \end{bmatrix} mod27 = \begin{bmatrix} 1 \\ 18 \end{bmatrix}$ =AR , LW ⇒ AR

D=A^{-1}*RR =$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix} \begin{bmatrix} 18 \\ 18 \end{bmatrix} mod27 = \begin{bmatrix} 504 \\ 468 \end{bmatrix} mod27 = \begin{bmatrix} 18 \\ 9 \end{bmatrix}$ =RI, RR ⇒ RI

D=A^{-1}*VV =$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix} \begin{bmatrix} 22 \\ 22 \end{bmatrix} mod27 = \begin{bmatrix} 616 \\ 572 \end{bmatrix} mod27 = \begin{bmatrix} 22 \\ 5 \end{bmatrix}$ =VE, VV ⇒ VE

D=A^{-1}*MZ =$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix} \begin{bmatrix} 13 \\ 26 \end{bmatrix} mod27 = \begin{bmatrix} 702 \\ 533 \end{bmatrix} mod27 = \begin{bmatrix} 0 \\ 20 \end{bmatrix}$ =_T, MZ ⇒ _T

D=A^{-1}*ZJ =$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix} \begin{bmatrix} 26 \\ 10 \end{bmatrix} mod27 = \begin{bmatrix} 312 \\ 436 \end{bmatrix} mod27 = \begin{bmatrix} 15 \\ 4 \end{bmatrix}$ =OD, ZJ ⇒ OD

D=A^{-1}*ZX =$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix} \begin{bmatrix} 26 \\ 24 \end{bmatrix} mod27 = \begin{bmatrix} 676 \\ 646 \end{bmatrix} mod27 = \begin{bmatrix} 1 \\ 25 \end{bmatrix}$ =AY, ZX ⇒ AY

D=A^{-1}*JT =$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix} \begin{bmatrix} 10 \\ 20 \end{bmatrix} mod27 = \begin{bmatrix} 540 \\ 410 \end{bmatrix} mod27 = \begin{bmatrix} 0 \\ 5 \end{bmatrix}$ =_E, JT ⇒ _E

D=A^{-1}*VV =$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix} \begin{bmatrix} 22 \\ 22 \end{bmatrix} mod27 = \begin{bmatrix} 616 \\ 572 \end{bmatrix} mod27 = \begin{bmatrix} 22 \\ 5 \end{bmatrix}$ =VE, VV ⇒ VE

D=A^{-1}*FY =$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix} \begin{bmatrix} 6 \\ 25 \end{bmatrix} mod27 = \begin{bmatrix} 662 \\ 441 \end{bmatrix} mod27 = \begin{bmatrix} 14 \\ 9 \end{bmatrix}$ =NI, FY ⇒ NI

D=A^{-1}*BQ =$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix} \begin{bmatrix} 2 \\ 17 \end{bmatrix} mod27 = \begin{bmatrix} 446 \\ 277 \end{bmatrix} mod27 = \begin{bmatrix} 14 \\ 7 \end{bmatrix}$ =NG, BQ ⇒ NG

D=A^{-1}*RI =$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix} \begin{bmatrix} 18 \\ 9 \end{bmatrix} mod27 = \begin{bmatrix} 270 \\ 333 \end{bmatrix} mod27 = \begin{bmatrix} 0 \\ 9 \end{bmatrix}$ =_I, RI⇒_I

D=A^{-1}*OP =$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix} \begin{bmatrix} 15 \\ 16 \end{bmatrix} mod27 = \begin{bmatrix} 446 \\ 405 \end{bmatrix} mod27 = \begin{bmatrix} 14 \\ 0 \end{bmatrix}$ =N_, OP ⇒ N_

D=A^{-1}*_N =$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 14 \end{bmatrix} mod27 = \begin{bmatrix} 364 \\ 210 \end{bmatrix} mod27 = \begin{bmatrix} 13 \\ 21 \end{bmatrix}$ =MU , _N ⇒ MU

D=A^{-1}*PS =$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix} \begin{bmatrix} 16 \\ 19 \end{bmatrix} mod27 = \begin{bmatrix} 526 \\ 461 \end{bmatrix} mod27 = \begin{bmatrix} 13 \\ 2 \end{bmatrix}$ =MB , PS ⇒ MB

D=A^{-1}*UN =$\begin{bmatrix} 2 & 26 \\ 11 & 15 \end{bmatrix}\begin{bmatrix} 21 \\ 14 \end{bmatrix} mod2 = \begin{bmatrix} 406 \\ 441 \end{bmatrix} mod27 = \begin{bmatrix} 1 \\ 9 \end{bmatrix}$ =AI , UN ⇒ AI

Then the decrypted message is “**TERRORISTS WILL ARRIVE TODAY EVENING IN MUMBAI”**

Conclusion:

This paper concludes that the plain text can be transferred to cipher text using 2 x 2 non-singular matrix of modulo 27 as key to encrypt plain text and using inverse matrix of order 2 x 2 as a key to open cipher text. The large information couldn’t decrypt without key matrix and congruence relations. The purpose of this paper is to store information and also transfer over internet confidentially.

References

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

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

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

Cite this Article:

Veena T, "Encryption and Decryption of Messages By Using Matrices", *International Journal of Scientific Research in Modern Science and Technology (IJSRMST),* ***ISSN:*** *2583-7605 (Online), Volume 2, Issue 9, pp. 01- 07, September 2023.*

Journal URL: *https://ijsrmst.com/*