ISSN: 2456-8686, Volume 4, Issue 2, 2020:92-102
DOI : http://doi.org/10.26524/cm85

Journal of Computational Mathematica

Open Access

An Approach for Encryption and Decryption Using Matrix Theory

V. Swathy[1*] and V. Balaji[2]
[1,2]Department of Mathematics,Sacred Heart College, Tirupattur District, India.

Abstract

In this paper, a method for encryption and decryption have been discussed using matrix theory and we have illustrated an example for this method.

Key words: Encryption, Decryption, Matrix, Key Matrix.

AMS classification: $94A60, 94B27, 94B40$.

1. Introduction

Cryptography is the research and practise of safe communication strategies in the presence of adversaries identified by third parties. It deals with the development and analysis of protocols that prevent malicious third parties from accesing information that is shared between two entities, thus pursuing the different aspects of information security. The encryption process is comprised of a Algorithm, with a key [4]. The ordinary readable text is known as plain text. The transformed message is known as cipher text. The key is the value independent of the plaintext.
The conversion process of plain text to cipher text is called encryption algorithm and cipher text to plain text is called decryption algorithm. In [1], they have developed a technique for encryption and decryption using matrix theory.

2. Mathematical concepts

Theorem 2.1 A text message of strings of some length size L can be converted into a matrix called a message matrix R of size $n > m$ and n is the least such that $m \times n \geq L$ depending upon the length of the message with the help of suitably chosen numerical and zeros [3].

[2]pulibala70@gmail.com

ISSN: 2456-8686, Volume 4, Issue 2, 2020:92-102
DOI : http://doi.org/10.26524/cm85

3. Algorithms

Encryption Algorithm:

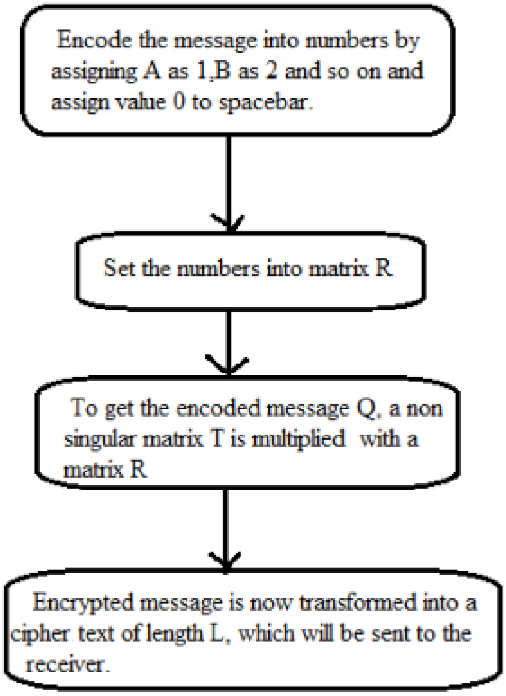

Figure 1: Procedure for Encoding

Decryption Algorithm :

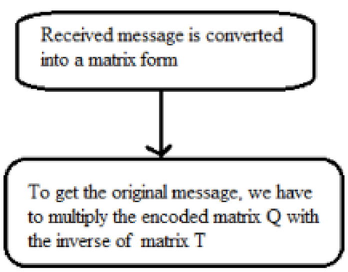

Figure 2: Procedure for Decoding

4. Results and Discussions

Illustration 4.1 The message which we are going to send to the receiver is ***MEET ME AT BUTTERFLY GALAXY TO GET HONEY***
Now let us convert the message into numbers ,

[2]pulibala70@gmail.com

ISSN: 2456-8686, Volume 4, Issue 2, 2020:92-102
DOI : http://doi.org/10.26524/cm85

13 5 5 20 0 13 5 0 1 20 0 2 21 20 20 5 18 6 12 25 0 7 1 12 1 24 25 0 20 15 0 7 5 20 0 8 15 14 5 25

Setting these numbers into a matrix form R as below,

$$R = \begin{bmatrix} 13 & 5 & 5 & 20 & 0 \\ 13 & 5 & 0 & 1 & 20 \\ 0 & 2 & 21 & 20 & 20 \\ 5 & 18 & 6 & 12 & 25 \\ 0 & 7 & 1 & 12 & 1 \\ 24 & 25 & 0 & 20 & 15 \\ 0 & 7 & 5 & 20 & 0 \\ 8 & 15 & 14 & 5 & 25 \end{bmatrix}$$

Now let us assume a non singular matrix T as, $T = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

as an encryption key then T^{-1} is $\begin{bmatrix} 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

We now multiplied matrix R with a non singular matrix T to get the encoded matrix Q .

[2]pulibala70@gmail.com

ISSN: 2456-8686, Volume 4, Issue 2, 2020:92-102
DOI : http://doi.org/10.26524/cm85

$$Q = RT = \begin{bmatrix} 13 & 5 & 5 & 20 & 0 \\ 13 & 5 & 0 & 1 & 20 \\ 0 & 2 & 21 & 20 & 20 \\ 5 & 18 & 6 & 12 & 25 \\ 0 & 7 & 1 & 12 & 1 \\ 24 & 25 & 0 & 20 & 15 \\ 0 & 7 & 5 & 20 & 0 \\ 8 & 15 & 14 & 5 & 25 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$Q = \begin{bmatrix} 13 & 18 & 23 & 43 & 43 \\ 13 & 18 & 18 & 19 & 39 \\ 0 & 2 & 23 & 43 & 63 \\ 5 & 23 & 29 & 41 & 66 \\ 0 & 7 & 8 & 20 & 21 \\ 24 & 49 & 49 & 69 & 84 \\ 0 & 7 & 12 & 32 & 32 \\ 8 & 23 & 37 & 42 & 67 \end{bmatrix}.$$

The encoded message to be sent is

13 18 23 43 43 13 18 18 19 39 0 2 23 43 63 5 23 29 41 66 0 7 8 20 21 24 49 49 69 84 0 7 12 32 32 8 23 37 42 67 .

To get the original message receiver should multiply by T^{-1}

[2]pulibala70@gmail.com

ISSN: 2456-8686, Volume 4, Issue 2, 2020:92-102
DOI : http://doi.org/10.26524/cm85

$$R = RTT^{-1} = \begin{bmatrix} 13 & 18 & 23 & 43 & 43 \\ 13 & 18 & 18 & 19 & 39 \\ 0 & 2 & 23 & 43 & 63 \\ 5 & 23 & 29 & 41 & 66 \\ 0 & 7 & 8 & 20 & 21 \\ 24 & 49 & 49 & 69 & 84 \\ 0 & 7 & 12 & 32 & 32 \\ 8 & 23 & 37 & 42 & 67 \end{bmatrix} \begin{bmatrix} 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Therefore, the decoded message is,
13 5 5 20 0 13 5 0 1 20 0 2 21 20 20 5 18 6 12 25 0 7 1 12 1 24 25 0 20 15 0 7 5 20 0 8 15 14 5 25
Hence, we received the original plaintext by changing the numbers into alphabets. We get the original message as ***MEET ME AT BUTTERFLY GALAXY TO GET HONEY***

NOTE: We have used Matlab for matrix multiplication.

5. Congruence Modulo Method

Definition 5.1 Let r be a positive integer, we say that u is congruent to v(mod r) if r(u-v) where u and v are integers i.e., $u = v + sr$ and $s \in z$, we write $u \equiv v(modr)$ is called congruence relation, the number r is the modulus of congruence[2],[5].

Definition 5.2 Inverse of an integer h to modulo r is h^{-1} such that $[h.h]^{-1} \equiv 1(modr)$, where h^{-1} is called inverse of h.

Illustration 5.3 First we are going to assign numbers from 1 to 26 to the 26 alphabets starting from A to Z and 0 to spacebar.Since we are going to use congruence method so let us take matrix modulo 27. Consider the message that is plain text as ***MEET ME AT BUTTERFLY GALAXY TO GET HONEY***

[2]pulibala70@gmail.com

ISSN: 2456-8686, Volume 4, Issue 2, 2020:92-102
DOI : http://doi.org/10.26524/cm85

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

Now let us assign the numbers to the above words by using above table , and we are going to arrange it in 5×1 matrix.

$$\text{MEET} = \begin{bmatrix} 13 \\ 5 \\ 5 \\ 20 \\ 0 \end{bmatrix}; \text{ME AT}= \begin{bmatrix} 13 \\ 5 \\ 0 \\ 1 \\ 20 \end{bmatrix}; \text{ BUTT} = \begin{bmatrix} 0 \\ 2 \\ 21 \\ 20 \\ 20 \end{bmatrix}; \text{ERFLY} = \begin{bmatrix} 5 \\ 18 \\ 6 \\ 12 \\ 25 \end{bmatrix};$$

$$\text{GALA} = \begin{bmatrix} 0 \\ 7 \\ 1 \\ 12 \\ 1 \end{bmatrix}; \text{XY TO}= \begin{bmatrix} 24 \\ 25 \\ 0 \\ 20 \\ 15 \end{bmatrix}; \text{ GET} = \begin{bmatrix} 0 \\ 7 \\ 5 \\ 20 \\ 0 \end{bmatrix}; \text{HONEY} = \begin{bmatrix} 8 \\ 15 \\ 14 \\ 5 \\ 25 \end{bmatrix};$$

[2]pulibala70@gmail.com

ISSN: 2456-8686, Volume 4, Issue 2, 2020:92-102
DOI : http://doi.org/10.26524/cm85

Let the key matrix T= $\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$ and $T^{-1} = \begin{bmatrix} 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

$$T^{-1} = \begin{bmatrix} 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} mod(27) = \begin{bmatrix} 1 & 26 & 0 & 0 & 0 \\ 0 & 1 & 26 & 0 & 0 \\ 0 & 0 & 1 & 26 & 0 \\ 0 & 0 & 0 & 1 & 26 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Now we multiplied the column vector corresponding to key matrix,

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 13 \\ 5 \\ 5 \\ 20 \\ 0 \end{bmatrix} mod(27) = \begin{bmatrix} 16 \\ 3 \\ 25 \\ 20 \\ 0 \end{bmatrix} = \begin{bmatrix} P \\ C \\ Y \\ T \\ \ \end{bmatrix} = PCYT$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 13 \\ 5 \\ 0 \\ 1 \\ 20 \end{bmatrix} mod(27) = \begin{bmatrix} 12 \\ 26 \\ 21 \\ 21 \\ 20 \end{bmatrix} = \begin{bmatrix} L \\ Z \\ U \\ U \\ T \end{bmatrix} = LZUUT$$

[2]pulibala70@gmail.com

ISSN: 2456-8686, Volume 4, Issue 2, 2020:92-102
DOI : http://doi.org/10.26524/cm85

$$\begin{bmatrix}1&1&1&1&1\\0&1&1&1&1\\0&0&1&1&1\\0&0&0&1&1\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}0\\2\\21\\20\\20\end{bmatrix}mod(27)=\begin{bmatrix}9\\9\\7\\13\\20\end{bmatrix}=\begin{bmatrix}I\\I\\G\\M\\T\end{bmatrix}=IIGMT$$

$$\begin{bmatrix}1&1&1&1&1\\0&1&1&1&1\\0&0&1&1&1\\0&0&0&1&1\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}5\\18\\6\\12\\25\end{bmatrix}mod(27)=\begin{bmatrix}12\\7\\16\\10\\25\end{bmatrix}=\begin{bmatrix}L\\G\\P\\J\\Y\end{bmatrix}=LGPJY$$

$$\begin{bmatrix}1&1&1&1&1\\0&1&1&1&1\\0&0&1&1&1\\0&0&0&1&1\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}0\\7\\1\\12\\1\end{bmatrix}mod(27)=\begin{bmatrix}21\\21\\14\\13\\1\end{bmatrix}=\begin{bmatrix}U\\U\\N\\M\\A\end{bmatrix}=UUNMA$$

$$\begin{bmatrix}1&1&1&1&1\\0&1&1&1&1\\0&0&1&1&1\\0&0&0&1&1\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}24\\25\\0\\20\\15\end{bmatrix}mod(27)=\begin{bmatrix}3\\6\\8\\8\\15\end{bmatrix}=\begin{bmatrix}C\\F\\H\\H\\O\end{bmatrix}=CFHHO$$

[2]pulibala70@gmail.com

ISSN: 2456-8686, Volume 4, Issue 2, 2020:92-102
DOI : http://doi.org/10.26524/cm85

$$\begin{bmatrix}1&1&1&1&1\\0&1&1&1&1\\0&0&1&1&1\\0&0&0&1&1\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}0\\7\\5\\20\\0\end{bmatrix} mod(27) = \begin{bmatrix}5\\5\\25\\20\\0\end{bmatrix} = \begin{bmatrix}E\\E\\Y\\T\\ \end{bmatrix} = EEYT$$

$$\begin{bmatrix}1&1&1&1&1\\0&1&1&1&1\\0&0&1&1&1\\0&0&0&1&1\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}8\\15\\14\\5\\25\end{bmatrix} mod(27) = \begin{bmatrix}13\\5\\17\\3\\25\end{bmatrix} = \begin{bmatrix}M\\E\\Q\\C\\Y\end{bmatrix} = MEQCY$$

Hence the message to be sent is,

PCYT LZUUTIIGMTLGPJYUUNMACFHHOEEYT MEQCY

By multiplying the inverse of key matrix T, receiver can decrypt the message easily.

$$\begin{bmatrix}1&26&0&0&0\\0&1&26&0&0\\0&0&1&26&0\\0&0&0&1&26\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}P\\C\\Y\\T\\ \end{bmatrix} mod(27) = \begin{bmatrix}1&26&0&0&0\\0&1&26&0&0\\0&0&1&26&0\\0&0&0&1&26\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}16\\3\\25\\20\\0\end{bmatrix} mod(27) = \begin{bmatrix}13\\5\\5\\20\\0\end{bmatrix} \Rightarrow MEET$$

$$\begin{bmatrix}1&26&0&0&0\\0&1&26&0&0\\0&0&1&26&0\\0&0&0&1&26\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}L\\Z\\U\\U\\T\end{bmatrix} mod(27) = \begin{bmatrix}1&26&0&0&0\\0&1&26&0&0\\0&0&1&26&0\\0&0&0&1&26\\0&0&0&0&1\end{bmatrix}\begin{bmatrix}12\\26\\21\\21\\20\end{bmatrix} mod(27) = \begin{bmatrix}13\\5\\0\\1\\20\end{bmatrix} \Rightarrow ME\ AT$$

[2]pulibala70@gmail.com

ISSN: 2456-8686, Volume 4, Issue 2, 2020:92-102
DOI : http://doi.org/10.26524/cm85

$$\begin{bmatrix} 1 & 26 & 0 & 0 & 0 \\ 0 & 1 & 26 & 0 & 0 \\ 0 & 0 & 1 & 26 & 0 \\ 0 & 0 & 0 & 1 & 26 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} I \\ I \\ G \\ M \\ T \end{bmatrix} mod(27) = \begin{bmatrix} 1 & 26 & 0 & 0 & 0 \\ 0 & 1 & 26 & 0 & 0 \\ 0 & 0 & 1 & 26 & 0 \\ 0 & 0 & 0 & 1 & 26 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 9 \\ 9 \\ 7 \\ 13 \\ 20 \end{bmatrix} mod(27) = \begin{bmatrix} 0 \\ 2 \\ 21 \\ 20 \\ 20 \end{bmatrix} \Rightarrow BUTT$$

$$\begin{bmatrix} 1 & 26 & 0 & 0 & 0 \\ 0 & 1 & 26 & 0 & 0 \\ 0 & 0 & 1 & 26 & 0 \\ 0 & 0 & 0 & 1 & 26 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} L \\ G \\ P \\ J \\ Y \end{bmatrix} mod(27) = \begin{bmatrix} 1 & 26 & 0 & 0 & 0 \\ 0 & 1 & 26 & 0 & 0 \\ 0 & 0 & 1 & 26 & 0 \\ 0 & 0 & 0 & 1 & 26 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 12 \\ 7 \\ 16 \\ 10 \\ 25 \end{bmatrix} mod(27) = \begin{bmatrix} 5 \\ 18 \\ 6 \\ 12 \\ 25 \end{bmatrix} \Rightarrow ERFLY$$

$$\begin{bmatrix} 1 & 26 & 0 & 0 & 0 \\ 0 & 1 & 26 & 0 & 0 \\ 0 & 0 & 1 & 26 & 0 \\ 0 & 0 & 0 & 1 & 26 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} U \\ U \\ N \\ M \\ A \end{bmatrix} mod(27) = \begin{bmatrix} 1 & 26 & 0 & 0 & 0 \\ 0 & 1 & 26 & 0 & 0 \\ 0 & 0 & 1 & 26 & 0 \\ 0 & 0 & 0 & 1 & 26 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 21 \\ 21 \\ 14 \\ 13 \\ 1 \end{bmatrix} mod(27) = \begin{bmatrix} 0 \\ 7 \\ 1 \\ 12 \\ 1 \end{bmatrix} \Rightarrow GALA$$

$$\begin{bmatrix} 1 & 26 & 0 & 0 & 0 \\ 0 & 1 & 26 & 0 & 0 \\ 0 & 0 & 1 & 26 & 0 \\ 0 & 0 & 0 & 1 & 26 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} C \\ F \\ H \\ H \\ O \end{bmatrix} mod(27) = \begin{bmatrix} 1 & 26 & 0 & 0 & 0 \\ 0 & 1 & 26 & 0 & 0 \\ 0 & 0 & 1 & 26 & 0 \\ 0 & 0 & 0 & 1 & 26 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 6 \\ 8 \\ 8 \\ 15 \end{bmatrix} mod(27) = \begin{bmatrix} 24 \\ 25 \\ 0 \\ 20 \\ 15 \end{bmatrix} \Rightarrow XY\ TO$$

[2]pulibala70@gmail.com

$$\begin{bmatrix} 1 & 26 & 0 & 0 & 0 \\ 0 & 1 & 26 & 0 & 0 \\ 0 & 0 & 1 & 26 & 0 \\ 0 & 0 & 0 & 1 & 26 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} E \\ E \\ Y \\ T \end{bmatrix} mod(27) = \begin{bmatrix} 1 & 26 & 0 & 0 & 0 \\ 0 & 1 & 26 & 0 & 0 \\ 0 & 0 & 1 & 26 & 0 \\ 0 & 0 & 0 & 1 & 26 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 5 \\ 5 \\ 25 \\ 20 \\ 0 \end{bmatrix} mod(27) = \begin{bmatrix} 0 \\ 7 \\ 5 \\ 20 \\ 0 \end{bmatrix} \Rightarrow GET$$

$$\begin{bmatrix} 1 & 26 & 0 & 0 & 0 \\ 0 & 1 & 26 & 0 & 0 \\ 0 & 0 & 1 & 26 & 0 \\ 0 & 0 & 0 & 1 & 26 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} M \\ E \\ Q \\ C \\ Y \end{bmatrix} mod(27) = \begin{bmatrix} 1 & 26 & 0 & 0 & 0 \\ 0 & 1 & 26 & 0 & 0 \\ 0 & 0 & 1 & 26 & 0 \\ 0 & 0 & 0 & 1 & 26 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 13 \\ 5 \\ 17 \\ 3 \\ 25 \end{bmatrix} mod(27) = \begin{bmatrix} 8 \\ 15 \\ 14 \\ 5 \\ 25 \end{bmatrix} \Rightarrow HONEY$$

Finally, we decrypyted the original message ***MEET ME AT BUTTERFLY GALAXY TO GET HONEY***.

3. Conclusion

This paper introduces the method for sending the secret messages. The key matrix and congruence modulo should be understood to decrypt the message more securely between the receiver and the sender.

References

[1] L.Vinothkumar and V.Balaji, Encryption and Decryption Technique Using Matrix Theory, Journal of computational Mathematics, vol.3, Issue-2.2019;1-7.

[2] W. Edwin Clark, Elementary Number Theory, University of South Florida (2002).

[3] Koblitz, Algebraic aspects of Cryptography, Springer-Velag, Berlin Heidelberg, Newyork.

[4] A. Menzes, P. Van oorschot and S. Vanstoe, Hand book of applied Cryptography, CRC Press, (1997).

[5] P. Shanmugam and C. Loganathan, Involuntory Matrix in Cryptography, IJRRAS, 6(4)(2011).

[2]pulibala70@gmail.com