

A TECHNIQUE FOR ENCODING AND DECODING USING MATRIX THEORY

T.Ranjani¹, A.Manshath², V.Maheshwari³ and V.Balaji⁴

¹Department of Mathematics, D.K.M College for Women, Vellore - 632001.

²Department of Mathematics and Actuarial science,
B.S.Abdur Rahman Crescent Institute of Science and Technology, Chennai - 600 048.

³Department of Mathematics,
Vels Institute of Science, Technology and Advanced studies, Chennai - 600117.

⁴Department of Mathematics, Sacred Heart College, Tirupattur - 635601.

E-mail: pulibala70@gmail.com

Abstract

In this paper, we have discussed an algorithm for encryption and decryption using matrix theory and we have worked two examples for this algorithm.

Key Words: Encryption, Decryption, Key Matrix.

2010 AMS Sub Class : 94A60,94B27,94B40

1. Introduction

The art and technology of concealing the messages to introduce secrecy in information safety is diagnosed as cryptography. The technique of disguising a message in such a way on hide its substance is coding. An encrypted message is cipher text. The approach of turning cipher text into plain text is decryption. The encryption process is comprised of a Algorithm, with a key [3]. The key is the value independent of the plaintext. In [5], they have developed a technique for encryption and decryption using matrix theory.

1.1. Prerequisite

Theorem 1.1 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. [2]

1.2. Algorithms

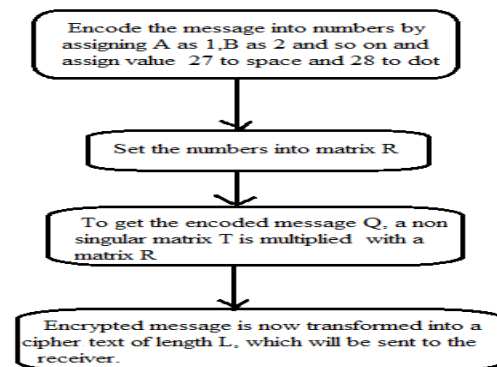


Figure 1. Procedure for encoding

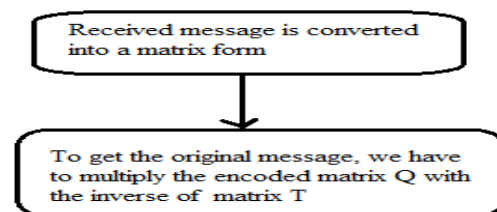


Figure 2. Procedure for decoding

2. Results and Discussions

Illustration 2.1 The message which we are going to send to the receiver is

"LET US MAKE IT SIMPLE INDEPENDENTLY."

Now let us convert the message into numbers ,

12 5 20 27 21 19 27 13 1 11 5 27 9 20
27 19 9 13 16 12 5 27 9 14 4 5 16 5 14 4 5
14 20 12 25 28

Setting these numbers into a matrix form R as,

$$R = \begin{bmatrix} 12 & 5 & 20 \\ 27 & 21 & 19 \\ 27 & 13 & 1 \\ 11 & 5 & 27 \\ 9 & 20 & 27 \\ 19 & 9 & 13 \\ 16 & 12 & 5 \\ 27 & 9 & 14 \\ 4 & 5 & 16 \\ 5 & 14 & 4 \\ 5 & 14 & 20 \\ 12 & 25 & 28 \end{bmatrix}$$

Now let us assume a non singular matrix T as,

$$T = \begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix} \text{ as an encryption key then } T^{-1} \text{ is}$$

$$\begin{bmatrix} -24 & 20 & -5 \\ 18 & -15 & 4 \\ 5 & -4 & 1 \end{bmatrix}. \text{ We now multiplied matrix } R \text{ with}$$

a non singular matrix T to get the encoded matrix Q .

$$Q = RT = \begin{bmatrix} 12 & 5 & 20 \\ 27 & 21 & 19 \\ 27 & 13 & 1 \\ 11 & 5 & 27 \\ 9 & 20 & 27 \\ 19 & 9 & 13 \\ 16 & 12 & 5 \\ 27 & 9 & 14 \\ 4 & 5 & 16 \\ 5 & 14 & 4 \\ 5 & 14 & 20 \\ 12 & 25 & 28 \end{bmatrix} \begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix}$$

$$Q = \begin{bmatrix} 82 & 85 & 90 \\ 126 & 97 & 261 \\ 56 & 17 & 213 \\ 102 & 113 & 85 \\ 130 & 128 & 165 \\ 76 & 61 & 149 \\ 55 & 32 & 152 \\ 87 & 65 & 189 \\ 62 & 69 & 50 \\ 45 & 30 & 109 \\ 93 & 94 & 109 \\ 146 & 137 & 210 \end{bmatrix}$$

The encoded message to be sent is

82 85 90 126 97 261 56 17 213 102 113 85 130
128 165 76 61 149 55 32 152 87 65 189 62 69
50 45 30 109 93 94 109 146 137 210

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

$$R = RTT^{-1} = \begin{bmatrix} 82 & 85 & 90 \\ 126 & 97 & 261 \\ 56 & 17 & 213 \\ 102 & 113 & 85 \\ 130 & 128 & 165 \\ 76 & 61 & 149 \\ 55 & 32 & 152 \\ 87 & 65 & 189 \\ 62 & 69 & 50 \\ 45 & 30 & 109 \\ 93 & 94 & 109 \\ 146 & 137 & 210 \end{bmatrix} \begin{bmatrix} -24 & 20 & -5 \\ 18 & -15 & 4 \\ 5 & -4 & 1 \end{bmatrix}$$

Therefore, the decoded message is,

12 5 20 27 21 19 27 13 1 11 5 27 9 20 27 19 9
13 16 12 5 27 9 14 4 5 16 5 14 4 5 14 20 12
25 28

Hence, we received the original plaintext by changing the numbers into alphabets. We get the original message as "LET US MAKE IT SIMPLE INDEPENDENTLY."

NOTE: We have used Matlab for matrix multiplication.

3. Congruence Modulo Method

Definition 3.1 Let g be a positive integer, we say that m is congruent to $n \pmod{g}$ if $g \mid (m-n)$ where m and n are integers i.e., $m = n + sg$ and $s \in \mathbb{Z}$, we write $m \equiv n \pmod{g}$ is called congruence relation, the number g is the modulus of congruence.[1], [4]

Definition 3.2 Inverse of an integer l to modulo g is l^{-1} such that $[l.l]^{-1} \equiv 1 \pmod{g}$, where l^{-1} is called inverse of l .

4. Results and discussions

Illustration 4.1 First we are going to assign numbers from 1 to 26 to the 26 alphabets starting from A to Z. Since we are going to use congruence method so let us take matrix modulo 28. Consider the message that as plain text is
"LET US MAKE IT SIMPLE INDEPENDENTLY."

Alphabet	A	B	C	D	E	F	G
Number	1	2	3	4	5	6	7
	-27	-26	-25	-24	-23	-22	-21
Alphabet	H	I	J	K	L	M	N
Number	8	9	10	11	12	13	14
	-20	-19	-18	-17	-16	-15	-14
Alphabet	O	P	Q	R	S	T	U
Number	15	16	17	18	19	20	21
	-13	-12	-11	-10	-9	-8	-7
Alphabet	V	W	X	Y	Z	spacebar	DOT
Number	22	23	24	25	26	27	0
	-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 3×1 matrix.

$$LET = \begin{bmatrix} 12 \\ 5 \\ 20 \end{bmatrix}; US = \begin{bmatrix} 27 \\ 21 \\ 19 \end{bmatrix}; MA = \begin{bmatrix} 27 \\ 13 \\ 1 \end{bmatrix}; KE = \begin{bmatrix} 11 \\ 5 \\ 27 \end{bmatrix};$$

$$IT = \begin{bmatrix} 9 \\ 20 \\ 27 \end{bmatrix}; SIM = \begin{bmatrix} 19 \\ 9 \\ 13 \end{bmatrix}; PLE = \begin{bmatrix} 16 \\ 12 \\ 5 \end{bmatrix}; IN = \begin{bmatrix} 27 \\ 9 \\ 14 \end{bmatrix};$$

$$DEP = \begin{bmatrix} 4 \\ 5 \\ 16 \end{bmatrix}; END = \begin{bmatrix} 5 \\ 14 \\ 4 \end{bmatrix}; ENT = \begin{bmatrix} 5 \\ 14 \\ 20 \end{bmatrix};$$

$$LY = \begin{bmatrix} 12 \\ 25 \\ 0 \end{bmatrix} \text{ Let the key matrix } T = \begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix}$$

$$\text{and } T^{-1} = \begin{bmatrix} -24 & 20 & -5 \\ 18 & -15 & 4 \\ 5 & -4 & 1 \end{bmatrix}$$

$$T^{-1} = \begin{bmatrix} -24 & 20 & -5 \\ 18 & -15 & 4 \\ 5 & -4 & 1 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix}$$

Now we multiplied the column vector corresponding to key matrix,

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \\ 20 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 112 \\ 149 \\ 56 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 0 \\ 9 \\ 0 \end{bmatrix} = \begin{bmatrix} \cdot \\ I \\ \cdot \end{bmatrix} = .I.$$

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix} \begin{bmatrix} 27 \\ 21 \\ 19 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 122 \\ 189 \\ 165 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 10 \\ 21 \\ 25 \end{bmatrix}$$

$$= \begin{bmatrix} J \\ U \\ Y \end{bmatrix} = .UY$$

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix} \begin{bmatrix} 27 \\ 13 \\ 1 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 32 \\ 73 \\ 133 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 4 \\ 17 \\ 21 \end{bmatrix}$$

$$= \begin{bmatrix} D \\ Q \\ U \end{bmatrix} = DQU$$

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix} \begin{bmatrix} 11 \\ 5 \\ 27 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 146 \\ 189 \\ 53 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 6 \\ 21 \\ 25 \end{bmatrix}$$

$$= \begin{bmatrix} F \\ U \\ Y \end{bmatrix} = FUY$$

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix} \begin{bmatrix} 9 \\ 20 \\ 27 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 144 \\ 200 \\ 107 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 4 \\ 4 \\ 23 \end{bmatrix}$$

$$= \begin{bmatrix} D \\ D \\ W \end{bmatrix} = DDW$$

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix} \begin{bmatrix} 19 \\ 9 \\ 13 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 84 \\ 125 \\ 93 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 0 \\ 13 \\ 9 \end{bmatrix}$$

$$= \begin{bmatrix} \cdot \\ M \\ I \end{bmatrix} = .MI$$

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix} \begin{bmatrix} 16 \\ 12 \\ 5 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 41 \\ 74 \\ 96 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 13 \\ 18 \\ 12 \end{bmatrix}$$

$$= \begin{bmatrix} M \\ R \\ L \end{bmatrix} = MRL$$

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix} \begin{bmatrix} 27 \\ 9 \\ 14 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 97 \\ 147 \\ 117 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 13 \\ 7 \\ 5 \end{bmatrix}$$

$$= \begin{bmatrix} M \\ G \\ E \end{bmatrix} = MGE$$

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix} \begin{bmatrix} 4 \\ 5 \\ 16 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 84 \\ 109 \\ 32 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 0 \\ 25 \\ 4 \end{bmatrix}$$

$$= \begin{bmatrix} \cdot \\ Y \\ D \end{bmatrix} = .YD$$

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix} \begin{bmatrix} 5 \\ 14 \\ 4 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 25 \\ 48 \\ 71 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 25 \\ 20 \\ 15 \end{bmatrix}$$

$$= \begin{bmatrix} Y \\ T \\ O \end{bmatrix} = YTO$$

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix} \begin{bmatrix} 5 \\ 14 \\ 20 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 105 \\ 144 \\ 71 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 21 \\ 4 \\ 15 \end{bmatrix}$$

$$= \begin{bmatrix} U \\ D \\ O \end{bmatrix} = UDO$$

$$\begin{bmatrix} 1 & 0 & 5 \\ 2 & 1 & 6 \\ 3 & 4 & 0 \end{bmatrix} \begin{bmatrix} 12 \\ 25 \\ 0 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 12 \\ 49 \\ 136 \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 12 \\ 21 \\ 24 \end{bmatrix}$$

$$= \begin{bmatrix} L \\ U \\ X \end{bmatrix} = LUX$$

Hence the message to be sent is,
**"I.JUYDQUFUYDDW.MIMRLMGE.YDYTO
 UDOLUX"**

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

$$\begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} . \\ I \\ . \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 9 \\ 0 \end{bmatrix} \text{mod}(28) \\ = \begin{bmatrix} 12 \\ 5 \\ 20 \end{bmatrix} = LET$$

$$\begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} J \\ U \\ Y \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} 10 \\ 21 \\ 25 \end{bmatrix} \text{mod}(28) \\ = \begin{bmatrix} 27 \\ 21 \\ 19 \end{bmatrix} = US$$

$$\begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} D \\ Q \\ U \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} 4 \\ 17 \\ 21 \end{bmatrix} \text{mod}(28) \\ = \begin{bmatrix} 27 \\ 13 \\ 1 \end{bmatrix} = MA$$

$$\begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} F \\ U \\ Y \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} 6 \\ 21 \\ 25 \end{bmatrix} \text{mod}(28) \\ = \begin{bmatrix} 11 \\ 5 \\ 27 \end{bmatrix} = KE$$

$$\begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} D \\ D \\ W \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} 4 \\ 4 \\ 23 \end{bmatrix} \text{mod}(28) \\ = \begin{bmatrix} 9 \\ 20 \\ 27 \end{bmatrix} = IT$$

$$\begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} . \\ M \\ I \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 13 \\ 9 \end{bmatrix} \text{mod}(28) \\ = \begin{bmatrix} 19 \\ 9 \\ 13 \end{bmatrix} = SIM$$

$$\begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} M \\ R \\ L \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} 13 \\ 18 \\ 12 \end{bmatrix} \text{mod}(28) \\ = \begin{bmatrix} 16 \\ 12 \\ 5 \end{bmatrix} = PLE$$

$$\begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} M \\ G \\ E \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} 13 \\ 7 \\ 5 \end{bmatrix} \text{mod}(28) \\ = \begin{bmatrix} 27 \\ 9 \\ 14 \end{bmatrix} = IN$$

$$\begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} . \\ Y \\ D \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 25 \\ 4 \end{bmatrix} \text{mod}(28) \\ = \begin{bmatrix} 4 \\ 5 \\ 16 \end{bmatrix} = DEP$$

$$\begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} Y \\ T \\ O \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} 25 \\ 21 \\ 15 \end{bmatrix} \text{mod}(28) \\ = \begin{bmatrix} 5 \\ 14 \\ 4 \end{bmatrix} = END$$

$$\begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} U \\ D \\ O \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} 21 \\ 4 \\ 15 \end{bmatrix} \text{mod}(28) \\ = \begin{bmatrix} 5 \\ 14 \\ 20 \end{bmatrix} = ENT$$

$$\begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} L \\ U \\ X \end{bmatrix} \text{mod}(28) = \begin{bmatrix} 4 & 20 & 23 \\ 18 & 13 & 4 \\ 5 & 24 & 1 \end{bmatrix} \begin{bmatrix} 12 \\ 21 \\ 24 \end{bmatrix} \text{mod}(28) \\ = \begin{bmatrix} 12 \\ 25 \\ 0 \end{bmatrix} = LY.$$

Finally, we decrypyted the original message **"LET US
 MAKE IT SIMPLE INDEPENDENTLY."**

5. 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.

Acknowledgment

The corresponding author (Dr.V.Balaji) for financial assistance No.FMRP5766/15(SERO/UGC).

References

- [1] W. Edwin Clark, Elementary Number Theory, University of South Florida (2002).
- [2] Koblitz, Algebraic aspects of Cryptography, Springer-Verlag, Berlin Heidelberg, Newyork.
- [3] A. Menzes, P. Van oorschot and S. Vanstoe, Hand book of applied Cryptography, CRC Press, (1997).
- [4] P. Shanmugam and C. Loganathan, Involuntary Matrix in Cryptography, IJRRAS, 6(4)(2011).
- [5] L.Vinothkumar and V.Balaji, Encryption and Decryption Technique Using Matrix Theory, Journal of computational Mathematics, vol.3, Issue-2.2019;1-7.