ISSN: 2456-8686, Volume 3, Issue 2, 2019:1-7
DOI : http://doi.org/10.26524/cm49

Journal of Computational Mathematica

Open Access

Encryption and Decryption Technique Using Matrix Theory

L. Vinothkumar[1*] and V. Balaji[2]
[1,2]Department of Mathematics, Sacred Heart College (Autonomous), Tirupattur, Tirupattur (Dt) - 635 601, Tamilnadu, S.India.

Abstract

Cryptography is a common discipline for mathematics, computer science and communication field. One main discipline which is applied in cryptography is mathematics, specifically matrix. This paper attempts to derive encryption and decryption technique using matrix theory

Key words: Encyption, Decryption, Matrix, Key Matrix.
AMS classification: 94A60, 94B27, 94B40

1. Introduction

Cryptography is a study of secret writing. The information needs to be secured from attack in this competitive world [3]. The process of encryption consists of an algorithm and a key. Data that can be read and understandable easily is called Plaintext. The key is the value independent of the plaintext. The process of converting cipher text to its original is called Decryption[6]. The algorithm will produce a different output depending on the specific key being used at the time. Once the ciphertext is produced, it may be transmitted upon reception, the ciphertext can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for decryption [5].

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 M 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*]drvinophd@gmail.com,[2]pulibala70@gmail.com

ISSN: 2456-8686, Volume 3, Issue 2, 2019:1-7
DOI : http://doi.org/10.26524/cm49

3. Algorithms

Encryption Algorithm :

- Encode the message in to numerals by giving $A\ as\ 1, B\ as\ 2$ and so on.
- Place the numerals in matrix M.
- Non singular matrix A is multiplied with matrix M to get the encoded message Y.
- Encrypted message is now converted into a plain text of length L and that will be send to the receiver.

Decryption Algorithm :

- Received message is converted into a matrix form.
- To get the original message, we have multiplied the encoded matrix Y with A^{-1}.

4. Worked Examples

Suppose the message to be sent is "**DUMCAKLANCRT**".

NOTE: We have used **Matlab** for matrix multiplication.

We now convert above message into numerals,

3 20 12 2 0 10 11 0 13 2 17 19

Arranging these numbers in Matrix M,

$$M = \begin{bmatrix} 3 & 20 & 12 \\ 2 & 0 & 10 \\ 11 & 0 & 13 \\ 2 & 17 & 19 \end{bmatrix}$$

Let the non singular matrix A as, $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix}$ as an encryption key, then

[1*]drvinophd@gmail.com,[2]pulibala70@gmail.com

ISSN: 2456-8686, Volume 3, Issue 2, 2019:1-7
DOI : http://doi.org/10.26524/cm49

$$A^{-1} = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix} \text{ exists.}$$

We now multiplied matrix M with a non singular matrix A to get the encoded matrix Y.

$$Y = MA = \begin{bmatrix} 3 & 20 & 12 \\ 2 & 0 & 10 \\ 11 & 0 & 13 \\ 2 & 17 & 19 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix}$$

$$Y = \begin{bmatrix} 63 & 98 & 89 \\ 52 & 64 & 6 \\ 76 & 100 & 33 \\ 97 & 135 & 74 \end{bmatrix}$$

The encoded message to be sent is

63 98 89 52 64 6 76 100 33 97 135 74

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

$$M = M.A.A^{-1} = \begin{bmatrix} 63 & 98 & 89 \\ 52 & 64 & 6 \\ 76 & 100 & 33 \\ 97 & 135 & 74 \end{bmatrix} \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix}$$

Therefore, the decoded message is,

3 20 12 2 0 10 11 0 13 2 17 19

[1*]drvinophd@gmail.com,[2]pulibala70@gmail.com

ISSN: 2456-8686, Volume 3, Issue 2, 2019:1-7
DOI : http://doi.org/10.26524/cm49

Hence, we received the original plaintext by changing the numerals into alphabets. We get the original message as **DUMCAKLANCRT**.

5. Congruence Modulo Method

Definition 5.1 Let m be a positive integer, we say that a is congruent to $b(modm)$ if $m(a-b)$ where a and b are integers i.e., $a = b + km$ and $k \in z$, we write $a \equiv b(modm)$ is called congruence relation, the number m is the modulus of congruence [1], [4].

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

6. Worked Examples

Assigning 26 alphabets in numerical numbers from 1 *to* 26. So, we have taken matrix modulo 26.
Consider the Plain text $DUMCAKLANCRT$.

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

Assigning numerals to the above words from the above tableau, and arranging them as 3×1 matrix,

$$DUM = \begin{bmatrix} 3 \\ 20 \\ 12 \end{bmatrix} \; ; \; CAK = \begin{bmatrix} 2 \\ 0 \\ 10 \end{bmatrix} \; ; \; LAN = \begin{bmatrix} 11 \\ 0 \\ 13 \end{bmatrix} ; \; CRT = \begin{bmatrix} 2 \\ 17 \\ 19 \end{bmatrix}$$

[1*]drvinophd@gmail.com,[2]pulibala70@gmail.com

ISSN: 2456-8686, Volume 3, Issue 2, 2019:1-7
DOI : http://doi.org/10.26524/cm49

Let the key matrix $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix}$

and $A^{-1} = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix}$

Now we multiplied the column vector corresponding to key matrix,

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \begin{bmatrix} 3 \\ 20 \\ 12 \end{bmatrix} mod(26) = \begin{bmatrix} 2 \\ 16 \\ 5 \end{bmatrix} = BQF$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \begin{bmatrix} 2 \\ 0 \\ 10 \end{bmatrix} mod(26) = \begin{bmatrix} 6 \\ 14 \\ 10 \end{bmatrix} = GOK$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \begin{bmatrix} 11 \\ 0 \\ 13 \end{bmatrix} mod(26) = \begin{bmatrix} 24 \\ 0 \\ 3 \end{bmatrix} = YAD$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \begin{bmatrix} 2 \\ 17 \\ 19 \end{bmatrix} mod(26) = \begin{bmatrix} 15 \\ 15 \\ 8 \end{bmatrix} = PPI$$

Hence the message to be sent is,

$$BQFGOKYADPPI$$

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

[1*]drvinophd@gmail.com,[2]pulibala70@gmail.com

ISSN: 2456-8686, Volume 3, Issue 2, 2019:1-7
DOI : http://doi.org/10.26524/cm49

$$\begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} \begin{bmatrix} B \\ Q \\ F \end{bmatrix} mod26 = \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 16 \\ 5 \end{bmatrix} = \begin{bmatrix} 3 \\ 20 \\ 12 \end{bmatrix} \Rightarrow DUM$$

$$\begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} \begin{bmatrix} G \\ O \\ K \end{bmatrix} mod26 = \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} \begin{bmatrix} 6 \\ 14 \\ 10 \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \\ 10 \end{bmatrix} \Rightarrow CAK$$

$$\begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} \begin{bmatrix} Y \\ A \\ D \end{bmatrix} mod26 = \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} \begin{bmatrix} 24 \\ 0 \\ 3 \end{bmatrix} = \begin{bmatrix} 11 \\ 0 \\ 13 \end{bmatrix} \Rightarrow LAN$$

$$\begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} \begin{bmatrix} P \\ P \\ I \end{bmatrix} mod26 = \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} \begin{bmatrix} 15 \\ 15 \\ 8 \end{bmatrix} = \begin{bmatrix} 2 \\ 17 \\ 19 \end{bmatrix} \Rightarrow CRT$$

Finally, we decrypyted the original message "$DUMCAKLANCRT$"

Conclusion

This paper provides the method for sending the messages very secretly. The key matrix and congruence modulo should be known between the receiver and the sender to decrypt the message more secretly...

References

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

[2] Koblitz K, Algebraic aspects of Cryptography, Berlin Heidelberg, New York, (1998).

[3] Menzes M, Vanoorschot V and Vanstoe S, Hand book of applied Cryptography, CRC Press, (1997).

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

[1*]drvinophd@gmail.com,[2]pulibala70@gmail.com

ISSN: 2456-8686, Volume 3, Issue 2, 2019:1-7
DOI : http://doi.org/10.26524/cm49

[5] Vinothkumar L and Balaji V, Encryption and Decryption technique using graph theory, International Journal of Research and Analytical Reviews, 6(2), 2019, 192-197.

[6] Wolfrom S, Cryptography with cellular automata in advances in cryptography-crypto, Spring-Verlaglecture notes in Computer Science, 218, 1986, 429-432.

[1*]drvinophd@gmail.com,[2]pulibala70@gmail.com