Int. J. Math. And Appl., 6(1)(2018), 25–28. (Special Issue)
ISSN: 2347-1557
Available Online: http://ijmaa.in/

International Journal of Mathematics And its Applications

Role of Matrices in Cryptography

S. Prabhavathi[1,*] and T. Chandrapushpam[1]

1 Department of Mathematics, Vivekanandha Arts and Science College for Women, Sankari, Tamil Nadu, India.

Abstract: Modern Cryptography exists at the intersection of the disciplines of Mathematics, Computer Science, Electrical Engineering and Communication Science. It is heavily based on mathematical theory and Computer Science practice. One discipline that is being applied in Cryptography is Linear Algebra in specific, Matrices. This paper attempts how to derive the role of matrices in Cryptography in day to day life.

Keywords: Matrices, Inverse Matrices, Congruence,Encryption,Decryption, Plaintext, Cipher text.

Accepted on: 13th April 2018

1. Introduction

Cryptography is a study of Science of secret writing [1]. Also defines Cryptography as the study of Mathematical techniques related to the concept of message security such as confidentiality, integrity of data, authentication of entry and data origin authentication [2]. The study of Cryptography consist of two parts: Encryption and Decryption. Data that can be read and understandable easily is called Plaintext. The process of hiding the information of the plaintext is called Encryption which results in unreadable text called cipher text. The process of converting cipher text to its original is called Decryption [3].

2. Mathematical Concepts (Product of Matrices)

Theorem 2.1. *A text message of strings of some length size L can be converted in to 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 numeral and zeros [4].*

2.1. Methodology

Encryption:

(1). Convert the plain data into numerical by giving A to 1,B to 2,C to 3 and so on.

(2). Place the numerical in to matrix M of order $mn \geq L$.

(3). Multiply the matrix M with a non-singular matrix A to get the encoded matrix X.

(4). Convert the resultant, the encrypted message matrix in to a text message of length L and that will be send to the receiver.

* *E-mail: sprabhakannan2005@gmail.com*

Decryption:

(1). Receiver can form a matrix with the encrypted message.

(2). Multiply the encoded matrix X with A^{-1} to get back the message matrix M.

Example 2.2. *Consider the message to be sent*

K I N G O F A R T S

11 9 14 7 15 6 1 18 20 19

Arrange these numbers in to a matrix M.

$$M = \begin{bmatrix} 11 & 9 & 14 \\ 7 & 0 & 15 \\ 6 & 0 & 1 \\ 18 & 20 & 19 \end{bmatrix}$$

Consider the non-singular matrix $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix}$ *as an encryption key, such that* $A^{-1} = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix}$ *exists. We perform the product of matrix MA which is the encoded matrix. Now*

$$X = MA = \begin{bmatrix} 11 & 9 & 14 \\ 7 & 0 & 15 \\ 6 & 0 & 1 \\ 18 & 20 & 19 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} = \begin{bmatrix} 81 & 115 & 69 \\ 82 & 104 & 61 \\ 11 & 18 & 18 \\ 113 & 170 & 134 \end{bmatrix}$$

The encoded message to be sent is

81 115 69 8 2 104 21 11 18 18 113 170 134

The encoded message to be sent is

81 115 69 82 104 21 11 18 18 113 170 134

The receiver can multiply the encoded matrix by $A^{(-1)}$ *to get back the original message.*

$$M = A^{(-1)} = \begin{bmatrix} 81 & 115 & 69 \\ 82 & 104 & 61 \\ 11 & 18 & 18 \\ 113 & 170 & 134 \end{bmatrix} \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 11 & 9 & 14 \\ 7 & 0 & 15 \\ 6 & 0 & 1 \\ 18 & 20 & 19 \end{bmatrix}.$$

The decoded message is

11 9 14 7 0 15 6 0 1 18 20 19

By changing the numerals to alphabet we get the original message **KING OF ARTS**.

2.2. Congruence Modulo Method

Definition 2.3. *Let m be a positive integer, we say that a is congruent to $b(mod\ m)$ if $m(a-b)$ where a and b are integers i.e., $a = b + km$ and $k \in z$, we write $a \equiv b(mod\ m)$. The relation $a \equiv b(mod\ m)$ is called Congruence relation, the number m is the modulus of congruence [5].*

Theorem 2.4. *Let $m \geq 0$,we say that a and b are congruent modulo m, denoted $a \equiv b(mod\ m)$ if a and b leaves the same remainder when divided by m. The number m is the modulus of congruence. The notation $a \neq b(mod\ m)$ means that they are not congruent [6].*

Definition 2.5. *Inverse of an integer a to modulo m is $a^{(-1)}$ such that $[a.a]^{(-1)} \equiv 1(mod\ m)$,where $a^{(-1)}$ is called inverse of a.*

Example 2.6. *As there are 26 letters in alphabet, we are taking matrix modulo 26.Giving A to 0,B to 1,C to 2 and so on. The encoded matrix can be formed by multiplying a non singular matrix by the corresponding column vectors. Consider the plain text*

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

KING OF ARTS

Splitting the plaintext into successive letters of three as follows.

$$K\ I\ N\ G\_\ O\ F\ \_\ A\ R\ T\ S$$

Assigning numerical value to each letters from the above table, and arrange them as 3×1 matrix we get

$$KIN = \begin{bmatrix} 11 \\ 9 \\ 14 \end{bmatrix}\ G-O = \begin{bmatrix} 7 \\ 0 \\ 15 \end{bmatrix}\ F-A = \begin{bmatrix} 6 \\ 0 \\ 1 \end{bmatrix}\ RTS = \begin{bmatrix} 18 \\ 20 \\ 19 \end{bmatrix}$$

Consider the key matrix $A = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix}$ *and* $A^{-1} = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix}$. *To get the column vector corresponding to cipher text, multiply the key matrix by the corresponding column vectors of the plaintext.*

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \begin{bmatrix} 11 \\ 9 \\ 14 \end{bmatrix} mod\ 26 = \begin{bmatrix} 19 \\ 13 \\ 5 \end{bmatrix} \Rightarrow TNF \quad \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \begin{bmatrix} 7 \\ 0 \\ 15 \end{bmatrix} mod\ 26 = \begin{bmatrix} 0 \\ 8 \\ 9 \end{bmatrix} \Rightarrow AIJ$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \begin{bmatrix} 6 \\ 0 \\ 1 \end{bmatrix} mod\ 26 = \begin{bmatrix} 9 \\ 4 \\ 4 \end{bmatrix} \Rightarrow JEE$$

$$\begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \begin{bmatrix} 18 \\ 20 \\ 19 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} 11 \\ 18 \\ 2 \end{bmatrix} \Rightarrow LSC$$

The encrypted message to be sent is

TNFAIJJEELSC

The receiver can decrypt the encrypted message by multiply the inverse of the key matrix A.

$$\begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} \begin{bmatrix} T \\ N \\ F \end{bmatrix} \text{ mod 26} = \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} \begin{bmatrix} 19 \\ 13 \\ 5 \end{bmatrix} \text{ mod 26} = \begin{bmatrix} 11 \\ 9 \\ 14 \end{bmatrix} \Rightarrow KIN$$

$$\begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} \begin{bmatrix} A \\ I \\ J \end{bmatrix} \text{ mod 26} = \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 8 \\ 9 \end{bmatrix} \text{ mod 26} = \begin{bmatrix} 7 \\ 0 \\ 15 \end{bmatrix} \Rightarrow G_0$$

$$\begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} \begin{bmatrix} J \\ E \\ E \end{bmatrix} \text{ mod 26} = \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} \begin{bmatrix} 9 \\ 4 \\ 4 \end{bmatrix} \text{ mod 26} = \begin{bmatrix} 6 \\ 0 \\ 1 \end{bmatrix} \Rightarrow F_A$$

$$\begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} \begin{bmatrix} L \\ S \\ C \end{bmatrix} \text{ mod 26} = \begin{bmatrix} 2 & 18 & 5 \\ 20 & 11 & 22 \\ 21 & 4 & 1 \end{bmatrix} \begin{bmatrix} 11 \\ 18 \\ 2 \end{bmatrix} \text{ mod 26} = \begin{bmatrix} 18 \\ 20 \\ 19 \end{bmatrix} \Rightarrow RTS$$

Finally the cipher text **TNFAIJJEELSC** *is decrypted to the original message.*

3. conclusion

This paper provides the methods of sending messages secretly. As both methods are using mathematical techniques they are considered to be best methods. To decrypt the encoded message the key matrix and congruence modulo must be known between the sender and the receiver, the sending messages can be kept secretly from others.

References

[1] www.synopsys.com. C.J.R.Berges,

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

[3] S.Wolfram, *Cryptography with cellular automata*, in advances in Cryptography-Crypto 85, Spring-Verlaglecture notes in Computer Science 218(1986), 429-432.

[4] Koblitz, *Algebraic aspects of Cryptography*, Springer-Velag, Berlin Heidelberg, New York.

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

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