ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

Message sharing by using linear & bilinear transformations

B. Kumaraswamy Achary, V. Vasu , K. Ramakrishna Prasad
Department of Mathematics, S.V.University

Abstract: In this paper we use linear and bilinear transformations to share the message secretly.

Key words: **Linear Transformation, Bilinear transformation, encryption, decryption, modular.**

I. INTRODUCTION

An encryption scheme or cryptosystem is a tuple (P, C, K, E, D) with the following properties.

- P is a set. It is called the plaintext space. Its elements are called plaintext.
- C is a set. It is called the cipher text space. Its elements are called cipher text.
- K is a set. It is called the key space. Its elements are called keys.

Linear transformation [1]:

This linear transformation based on the fact that every transformation having inverse. Linear transformation generally denoted by L. $x'=a_1x+b_1y$, $y'=a_2x+b_2y$

Which in matrix notation is $\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$

$$x' = l_1x + m_1y + n_1z$$

Similarly the relation of the type $y' = l_2x + m_2y + n_2z$

$$z' = l_3x + m_3y + n_3z$$

Which in matrix notation is $\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \begin{bmatrix} l_1 & m_1 & n_1 \\ l_2 & m_2 & n_2 \\ l_3 & m_3 & n_3 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix}$

In general, the relation y=AX, where

$$Y = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \dots \\ y_n \end{bmatrix}; A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}; X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \dots \\ x_n \end{bmatrix}$$

Gives linear transformation in n variables, $x_1,x_2 \dots x_n$ to the variables $y_1,y_2 \dots y_n$. i.e. the transformation of the vector X to the vector Y.

Step 3: Form the nx1 column vector X having the numerical values as its entries.

Step 4: Get each cipher vector Y by multiplying A by X. and comment each entry of the cipher text vector to its letter in alphabet.

The encryption process of this method is Y=AX, where Y is column vector of the numerical value of cipher text, X is column vector of the numerical value of plain text matrix 'A' is the key of the process.

Decryption process for linear transformation

The decryption which is the process of converting cipher text into plain text, could also be summarized in the following steps:

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

Step 1:Get inverse of matrix A, say A^{-1}.
Step 2: Change each cipher text to its numerical values.
Step 3: Put each cipher text in nx1 column vector say X.
Step 4: Get each plaintext vector by multiplying A^{-1} with Y. therefore $X=A^{-1}Y$.

Example 1:

Encode the message good by using linear transformation technique, where matrix $A=\begin{bmatrix}4 & 2\\ 3 & 1\end{bmatrix}$

Sol: first use the table below to convert letters in the message to their numerical values.

G	O	O	D
20	12	12	23

$$A=\begin{bmatrix}4 & 2\\ 3 & 1\end{bmatrix},$$

$$A^{-1}=\frac{1}{ad-bc}\begin{bmatrix}d & -b\\ -c & a\end{bmatrix}$$

$$=\frac{1}{-2}\begin{bmatrix}1 & -2\\ -3 & 4\end{bmatrix}$$

$$=\begin{bmatrix}-\frac{1}{2} & 1\\ \frac{3}{2} & -2\end{bmatrix}$$

$$C_1=\begin{bmatrix}-\frac{1}{2} & 1\\ \frac{3}{2} & -2\end{bmatrix}\begin{bmatrix}20\\ 12\end{bmatrix}=\begin{bmatrix}-10+12\\ 30-24\end{bmatrix}=\begin{bmatrix}2\\ 6\end{bmatrix}=\begin{bmatrix}Y\\ V\end{bmatrix}$$

$$C_2=\begin{bmatrix}-\frac{1}{2} & 1\\ \frac{3}{2} & -2\end{bmatrix}\begin{bmatrix}12\\ 23\end{bmatrix}=\begin{bmatrix}-6+23\\ 18-46\end{bmatrix}=\begin{bmatrix}17\\ -28\end{bmatrix}=\begin{bmatrix}17\\ 4\end{bmatrix}=\begin{bmatrix}J\\ W\end{bmatrix}$$

=[YVJW]

Therefore GOOD is converted into YVJW

Example 2: Encode the message ALLWAYS. Using linear transformation technique for the given matrix $A=\begin{bmatrix}3 & 1\\ 4 & 2\end{bmatrix}$

Sol: first convert given encode message which contains alphabets to numerical values.

A	L	L	W	A	Y	S
26	15	15	4	26	2	8

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

$$A=\begin{bmatrix}3 & 1\\ 4 & 2\end{bmatrix}$$

$$A^{-1}=\frac{1}{ad-bc}\begin{bmatrix}d & -b\\ -c & a\end{bmatrix}$$

$$=\frac{1}{6-4}\begin{bmatrix}2 & -1\\ -4 & 3\end{bmatrix}$$

$$=\begin{bmatrix}1 & -\frac{1}{2}\\ -2 & \frac{3}{2}\end{bmatrix}$$

Put '0' for the space between words if remained.

$$C_1=\begin{bmatrix}1 & -\frac{1}{2}\\ -2 & \frac{3}{2}\end{bmatrix}\begin{bmatrix}26\\ 15\end{bmatrix}=\begin{bmatrix}26-\frac{15}{2}\\ -52+\frac{45}{2}\end{bmatrix}=\begin{bmatrix}\frac{52-15}{2}\\ \frac{-104+45}{2}\end{bmatrix}=\begin{bmatrix}\frac{37}{2}\\ -\frac{59}{2}\end{bmatrix}=\begin{bmatrix}19\\ -30\end{bmatrix}=\begin{bmatrix}19\\ 8\end{bmatrix}=\begin{bmatrix}J\\ S\end{bmatrix}$$

$$C_2=\begin{bmatrix}1 & -\frac{1}{2}\\ -2 & \frac{3}{2}\end{bmatrix}\begin{bmatrix}15\\ 4\end{bmatrix}=\begin{bmatrix}15-2\\ -30+6\end{bmatrix}=\begin{bmatrix}13\\ -24\end{bmatrix}=\begin{bmatrix}13\\ 4\end{bmatrix}=\begin{bmatrix}N\\ W\end{bmatrix}$$

$$C_3=\begin{bmatrix}1 & -\frac{1}{2}\\ -2 & \frac{3}{2}\end{bmatrix}\begin{bmatrix}26\\ 2\end{bmatrix}=\begin{bmatrix}26-1\\ -52+3\end{bmatrix}=\begin{bmatrix}25\\ -49\end{bmatrix}=\begin{bmatrix}25\\ 3\end{bmatrix}=\begin{bmatrix}B\\ X\end{bmatrix}$$

$$C_4=\begin{bmatrix}1 & -\frac{1}{2}\\ -2 & \frac{3}{2}\end{bmatrix}\begin{bmatrix}8\\ 0\end{bmatrix}=\begin{bmatrix}8\\ -16\end{bmatrix}=\begin{bmatrix}8\\ -20\end{bmatrix}=\begin{bmatrix}S\\ G\end{bmatrix}$$

Therefore the encoded message becomes

19	8	13	4	25	3	8	20
J	S	N	W	B	X	S	G

Example 3: Decode the message RAEYWEN by using linear transformation technique to the matrix

Sol: First convert the message into its numerical value. Put zeros for the space between the word whenever required.

R	A	E	Y	W	E	N
9	26	22	2	4	22	13

$$P_1=\begin{bmatrix}3 & 2 & 1\\ 4 & 5 & 6\\ 2 & 7 & 1\end{bmatrix}=\begin{bmatrix}9\\ 26\\ 22\end{bmatrix}=\begin{bmatrix}27+52+22\\ 36+130+132\\ 18+182+22\end{bmatrix}=\begin{bmatrix}101\\ 298\\ 222\end{bmatrix}=\begin{bmatrix}3\\ 14\\ 12\end{bmatrix}=\begin{bmatrix}X\\ M\\ O\end{bmatrix}$$

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

$$P_2=\begin{bmatrix}3&2&1\\4&5&6\\2&7&1\end{bmatrix}\begin{bmatrix}2\\4\\22\end{bmatrix}=\begin{bmatrix}6+8+22\\8+20+132\\4+28+22\end{bmatrix}=\begin{bmatrix}36\\160\\54\end{bmatrix}=\begin{bmatrix}16\\22\\24\end{bmatrix}=\begin{bmatrix}K\\E\\C\end{bmatrix}$$

$$P_3=\begin{bmatrix}3&2&1\\4&5&6\\2&7&1\end{bmatrix}\begin{bmatrix}13\\0\\0\end{bmatrix}=\begin{bmatrix}39\\52\\26\end{bmatrix}=\begin{bmatrix}12\\26\\26\end{bmatrix}=\begin{bmatrix}O\\A\\A\end{bmatrix}$$

Therefore the decode message is X M O K E C O A A

The encryption process for linear transformation:

In fact we can summarized the encryption, which is the process of converting plain text into cipher text in the following steps.

Step 1: Choose a transformation Y=AX where X,Y,A are the matrices and also A is invertible nxn matrix, where n have may be depends on the length of the message that needs to be encrypted.

Step 2: Change each plain text to its numerical values by using following table

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

II. BI-LINEAR TRANSFORMATION TO SHARE THE MESSAGES SECRETRELY

Definition 1:

The transformation of the form $y=\frac{ax+b}{cx+d}$ where a,b,c,d are constants and ad-bc≠0 is known as the bi-linear transformation[19].

Definition 2: Inverse of Bi-linear transformation:

The transformation $x=\frac{-dy+b}{cy-a}$ is known as inverse of bi-linear transformation, which is also bi-linear.

Message sharing:

The following steps are required to share message using bi-linear transformation.

Step 1: First choose the constants namely a,b,c,d

Step 2: Convert given message into its numerical values using the table

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

Step 3: Convert cipher text into plain text

Step 4: Assign numerical values to that message.

Step 5: Inverse transformation is used to convert the plain text into cipher text.

Example 4: Encode the message BOOK by using bi-linear transformation $Y=\frac{2x+3}{4x+5}(\mathrm{mod}\,26)$

Sol: First use the table below to convert letter in the message to their numerical values.

B	O	O	K
6	19	19	15

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

$$C_1 = \frac{2(6)+3}{4(6)+5}(\text{mod } 26) = \frac{15}{29}(\text{mod } 26) = 1$$

$$C_2 = \frac{2(19)+3}{4(19)+5}(\text{mod } 26) = \frac{41}{81}(\text{mod } 26) = 0$$

$$C_3 = \frac{2(19)+3}{4(19)+5}(\text{mod } 26) = \frac{41}{81}(\text{mod } 26) = 0$$

$$C_4 = \frac{2(15)+3}{4(15)+5}(\text{mod } 26) = \frac{33}{65}(\text{mod } 26) = 1$$

Therefore the encoded message is 1 0 0 1

W V V W

Now the converted encoded message = WVVW

Example 5: Encode the message MUMMY using bilinear transformation $Y = \frac{5x+3}{2x+1} \text{mod } 26$

Sol: First convert the message letters into their corresponding numerical values by using the table.

M	U	M	M	Y
17	25	17	17	3

$$C_1 = \frac{5(17)+3}{2(17)+1} \text{mod } 26 = \frac{88}{35} \text{mod } 26 = 3$$

$$C_2 = \frac{5(25)+3}{2(25)+1} \text{mod } 26 = \frac{128}{51} \text{mod } 26 = 2$$

$$C_3 = \frac{5(17)+3}{2(17)+1} \text{mod } 26 = \frac{88}{35} \text{mod } 26 = 3$$

$$C_4 = \frac{5(17)+3}{2(17)+1} \text{mod } 26 = \frac{88}{35} \text{mod } 26 = 3$$

$$C_5 = \frac{5(3)+3}{2(3)+1} \text{mod } 26 = \frac{18}{7} \text{mod } 26 = 3$$

The encoded message 3 2 3 3 3

Y X Y Y Y

Example 6: Decode message ENOHP using inverse bi-linear transformation $X = \frac{7y+2}{3y-4} \text{mod } 26$

Sol:

First convert the message into its numerical values by using the table as,

E	N	O	H	P
9	18	19	12	20

$$P_1 = \frac{7(9)+2}{3(9)-4} \text{mod } 26 = \frac{65}{23} \text{mod } 26 = 3$$

$$P_2 = \frac{7(18)+2}{3(18)-4} \text{mod } 26 = \frac{128}{50} \text{mod } 26 = 2$$

$$P_3 = \frac{7(19)+2}{3(19)-4} \text{mod } 26 = \frac{135}{53} \text{mod } 26 = 3$$

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 2, March 2016

$$P_4 = \frac{7(12)+2}{3(12)-4} \bmod 26 = \frac{86}{32} \bmod 26 = 3$$

$$P_5 = \frac{7(20)+2}{3(20)-4} \bmod 26 = \frac{142}{56} \bmod 26 = 2$$

$\therefore$ The decoded message is 3 2 3 3 2
Y X Y Y X

Example 7:

Decode message THGIN by using inverse bi-linear transformation $X = \frac{9y+6}{y-7} \bmod 26$

Sol :

First convert the message into its numerical values by using the table as,

T H G I N
24 12 11 13 18

$$P_1 = \frac{9(24)+6}{24-7} \bmod 26 = \frac{222}{17} \bmod 26 = 13$$

$$P_2 = \frac{9(12)+6}{12-7} \bmod 26 = \frac{114}{5} \bmod 26 = 23$$

$$P_3 = \frac{9(11)+6}{11-7} \bmod 26 = \frac{105}{4} \bmod 26 = 0$$

$$P_4 = \frac{9(13)+6}{13-7} \bmod 26 = \frac{123}{6} \bmod 26 = 21$$

$$P_5 = \frac{9(18)+6}{18-7} \bmod 26 = \frac{168}{11} \bmod 26 = 15$$

$\therefore$ The decoded message is 13 23 0 21 15
I S V Q K

REFERENCES

[1] H.Dobbertin. Cryptanalysis of MD4. Journal of Cryptology, 11(4):253-271, 1998.

[2] Complex analysis by silver men.

[3] Probability & statics, S. Chand company ltd. http//: info@schand group.com.

[4] J.Black and P.Rogaway. A block cipher mode of operation for parallelizable message authentication. In advances in cryptology- Euro crypt 02, volume 2332 of LNCS, Pages 384-397. Springer- Verlag, 2002.

[5] O.Goldreich, Modern cryptography, probabilistic proofs and pseudo randomness. Springer-verlag, Newyork, 1999.