BULLETIN OF MATHEMATICS AND STATISTICS RESEARCH
A Peer Reviewed International Journal,
Contents available on www.bomsr.com
Vol.4. S1.2016; ISSN: 2348-0580
Email:editorbomsr@gmail.com
RADMAS– 2016

SECURE CRYPTOSYSTEM BASED ON BRAIDING/ENTANGLEMENT OF PAULI 5/2 MATRICES

P. SIRISHA[1], Ch. Suneetha[2]

[1]Faculty in Mathematics, Indian MaritimeUniversity, Visakhapatnam
sirinivas06@gmail.com

[2] Associate Professor in Mathematics, GIS, GITAM University, Visakhapatnam

Abstract

Cryptography is the art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible and then retransforming that message back to its original form. Secure transmission of the information to the genuine recipient has become a Herculean task .This paper presents a novel encryption scheme using Braiding/Entanglement of Pauli Spin 5/2 matrices.

Key Words: Braiding/Entanglement, Encryption and Decryption.

1. INTRODUCTION

The Hill cipher was invented in 1929 by Lester S. Hill [1]. based on matrix transformation that its attributes, including its cryptanalysis are described in some cryptographic textbooks [3]. The Hill cipher was invented in 1929 by Lester S. Hill [1,2]. It is a famous polygram and classical ciphering algorithm based on matrix transformation that its attributes, including its cryptanalysis are described in some cryptographic textbooks [3,4]. It is a famous Polygram and classical ciphering algorithm based on matrix transformation. Hill cipher is a blockcipher having diverse advantages such as concealing letter frequency, its simplicity because of using matrix multiplication and inversion for encryption and decryption and high speed. But it is vulnerable to known plain text attacks. Several researchers tried to improve the security of the Hill cipher. The present paper describes a novel encryption algorithm using braiding/entanglement technique with Pauli 5/2 matrices.

1.1 Pauli Spin 5/2 Matrices:

In Quantum Mechanics a very class of dynamical problems arises with central forces. These forces are derivable from a potential that depends on the distance (r) of the moving particle from a fixed point, the origin of the co-ordinate system (O). Since central forces produce no torque about the origin, the angular momentum L = rxp is constant of motion where p is a constant of motion the momentum of the particle. In addition to the dynamical variables x,y,z to describe the position of the vector there is another fourth variable σ, called the spin angular momentum variable required to describe the dynamical state of fundamental particles. In 1920's, in the study of the spectra of alkali atoms, some troublesome features were observed which could not be explained on the basis of orbital quantum properties [2]. The energy levels corresponding to the n, l and ml quantum numbers were found to be further split up. Uhlenbeck and Goudsmit [3,4] in 1925 attributed these difficulties due to the fact that the electron has an additional property of intrinsic angular momentum and magnetic momentum. Pauli was the first to propose a non-relativistic wave equation, which takes into account the intrinsic magnetic moment of the electron. To describe the electron spin he used spin ½ , spin 3/2, spin 5/2 matrices. The spin-5/2 matrices are

BULLETIN OF MATHEMATICS AND STATISTICS RESEARCH
A Peer Reviewed International Journal,
Contents available on www.bomsr.com
Vol.4. S1.2016; ISSN: 2348-0580
Email:editorbomsr@gmail.com
RADMAS– 2016

$$S_x=\frac{1}{2}\begin{bmatrix}0&\sqrt{5}&0&0&0&0\\ \sqrt{5}&0&\sqrt{8}&0&0&0\\ 0&\sqrt{8}&0&\sqrt{9}&0&0\\ 0&0&\sqrt{9}&0&\sqrt{8}&0\\ 0&0&0&\sqrt{8}&0&\sqrt{5}\\ 0&0&0&0&\sqrt{5}&0\end{bmatrix}$$

$$S_y=\frac{1}{2i}\begin{bmatrix}0&\sqrt{5}&0&0&0&0\\ -\sqrt{5}&0&\sqrt{8}&0&0&0\\ 0&-\sqrt{8}&0&\sqrt{9}&0&0\\ 0&0&-\sqrt{9}&0&\sqrt{8}&0\\ 0&0&0&-\sqrt{8}&0&\sqrt{5}\\ 0&0&0&0&-\sqrt{5}&0\end{bmatrix}$$

$$S_z=\frac{1}{2}\begin{bmatrix}5&0&0&0&0&0\\ 0&3&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&-1&0&0\\ 0&0&0&0&-3&0\\ 0&0&0&0&0&-5\end{bmatrix}$$

1.2 Braiding/Entanglement of Matrices: Entanglement [5] is a term used in quantum theory to describe the way that particles of energy/matter can become correlated to predictably interact with each other regardless of how far apart they are. Braiding/Entanglement of matrices is a technique of generating higher order non-singular matrices from simple lower order non-singular matrices.

For example if $a=\begin{bmatrix}a_{11}&a_{12}&a_{13}\\ a_{21}&a_{22}&a_{23}\\ a_{31}&a_{32}&a_{33}\end{bmatrix}$, $b=\begin{bmatrix}b_{11}&b_{12}&b_{13}\\ b_{21}&b_{22}&b_{23}\\ b_{31}&b_{32}&b_{33}\end{bmatrix}$, $c=\begin{bmatrix}c_{11}&c_{12}&c_{13}\\ c_{21}&c_{22}&c_{23}\\ c_{31}&c_{32}&c_{33}\end{bmatrix}$, $d=\begin{bmatrix}d_{11}&d_{12}&d_{13}\\ d_{21}&d_{22}&d_{23}\\ d_{31}&d_{32}&d_{33}\end{bmatrix}$ are four non-singular matrices of order 3x3 then these four non-singular matrices are braided/entangled to get higher order 6x6 matrices as

$$A=\begin{bmatrix}a&b\\ c&d\end{bmatrix}=\begin{bmatrix}a_{11}&a_{12}&a_{13}&b_{11}&b_{12}&b_{13}\\ a_{21}&a_{22}&a_{23}&b_{21}&b_{22}&b_{23}\\ a_{31}&a_{32}&a_{33}&b_{31}&b_{32}&b_{33}\\ d_{11}&d_{12}&d_{13}&c_{11}&c_{12}&c_{13}\\ d_{21}&d_{22}&d_{23}&c_{21}&c_{22}&c_{23}\\ d_{31}&d_{32}&d_{33}&c_{31}&c_{32}&c_{33}\end{bmatrix}$$

BULLETIN OF MATHEMATICS AND STATISTICS RESEARCH
A Peer Reviewed International Journal,
Contents available on www.bomsr.com
RADMAS– 2016
Vol.4. S1.2016; ISSN: 2348-0580
Email:editorbomsr@gmail.com

$$B=\begin{bmatrix} c & a \\ b & d \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & c_{13} & d_{11} & d_{12} & d_{13} \\ c_{21} & c_{22} & c_{23} & d_{21} & d_{22} & d_{23} \\ c_{31} & c_{32} & c_{33} & d_{31} & d_{32} & d_{33} \\ b_{11} & b_{12} & b_{13} & a_{11} & a_{12} & a_{13} \\ b_{21} & b_{22} & b_{23} & a_{21} & a_{22} & a_{23} \\ b_{31} & b_{32} & b_{33} & a_{31} & a_{32} & a_{33} \end{bmatrix}$$

$$C=\begin{bmatrix} b & c \\ a & d \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & b_{13} & c_{11} & c_{12} & c_{13} \\ b_{21} & b_{22} & b_{23} & c_{21} & c_{22} & c_{23} \\ b_{31} & b_{32} & b_{33} & c_{31} & c_{32} & c_{33} \\ a_{11} & a_{12} & a_{13} & d_{11} & d_{12} & d_{13} \\ a_{21} & a_{22} & a_{23} & d_{21} & d_{22} & d_{23} \\ a_{31} & a_{32} & a_{33} & d_{31} & d_{32} & d_{33} \end{bmatrix}$$

$$D = \begin{bmatrix} c & b \\ a & d \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & c_{13} & b_{11} & b_{12} & b_{13} \\ c_{21} & c_{22} & c_{23} & b_{21} & b_{22} & b_{23} \\ c_{31} & c_{32} & c_{33} & b_{31} & b_{32} & b_{33} \\ a_{11} & a_{12} & a_{13} & d_{11} & d_{12} & d_{13} \\ a_{21} & a_{22} & a_{23} & d_{21} & d_{22} & d_{23} \\ a_{31} & a_{32} & a_{33} & d_{31} & d_{32} & d_{33} \end{bmatrix}$$

and so on.

These matrices are further braided /entangled to get higher order 16x16 matrices like

$P = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ and so on. Non-Singular matrices from the set of these matrices can be selected for the process of encryption/decryption.

1.3 Literature on Golden Matrices: In the last decades the theory of Fibonacci numbers [6,7] was complemented by the theory of the so-called Fibonacci Q – matrix. Stakhov [8] developed a theory of the golden matrices that are a generalization of the matrix Q^n for continuous domain. He defined the golden matrices in the terms of the symmetrical hyperbolic Fibonacci functions. B.Vellainkann et.al. [9] used non-singular diagonal matrices of higher order, especially induced from quadratic forms in their encryption algorithm. Bibhudendra Acharya et.al. [10] used Hill Cipher for image encryption. Birendra Goswami [11]used matrices in cloud computing. Ayan Mahalanobis [12] used matrices in public key cryptography.

2. Proposed Method: The set of Pauli Spin 5/2 matrices with some elementary transformations are reduced to the matrices

BULLETIN OF MATHEMATICS AND STATISTICS RESEARCH
A Peer Reviewed International Journal,
Contents available on www.bomsr.com
RADMAS– 2016
Vol.4. S1.2016; ISSN: 2348-0580
Email:editorbomsr@gmail.com

$$b = \begin{bmatrix} 0 & 5 & 0 & 0 & 0 & 0 \\ 5 & 0 & 8 & 0 & 0 & 0 \\ 0 & 8 & 0 & 9 & 0 & 0 \\ 0 & 0 & 9 & 0 & 8 & 0 \\ 0 & 0 & 0 & 8 & 0 & 5 \\ 0 & 0 & 0 & 0 & 5 & 0 \end{bmatrix} \quad c = \begin{bmatrix} 0 & -5 & 0 & 0 & 0 & 0 \\ 5 & 0 & -8 & 0 & 0 & 0 \\ 0 & 8 & 0 & -9 & 0 & 0 \\ 0 & 0 & 9 & 0 & -8 & 0 \\ 0 & 0 & 0 & 8 & 0 & -5 \\ 0 & 0 & 0 & 0 & 5 & 0 \end{bmatrix}$$

$$d = \begin{bmatrix} 5 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -3 & 0 \\ 0 & 0 & 0 & 0 & 0 & -5 \end{bmatrix}$$

These three matrices derived from Pauli spin 5/2 matrices along with the identity matrix (I 6x6 = a) are braided or entangled in different possible ways to get a set B of 12nonsingular matrices.

$$B_{001} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 5 & 0 & 8 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 8 & 0 & 9 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 9 & 0 & 8 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 8 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 5 & 0 \\ 0 & -5 & 0 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 0 \\ 5 & 0 & -8 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 8 & 0 & -9 & 0 & -8 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 9 & 0 & 0 & -8 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 8 & 0 & -5 & 0 & 0 & 0 & 0 & -3 & 0 \\ 0 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & 0 & 0 & 0 & -5 \end{bmatrix}$$

And similarly other matrices are $B_{002} = \begin{bmatrix} a & b \\ d & c \end{bmatrix}$, $B_{003} = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$, $B_{004} = \begin{bmatrix} a & c \\ d & b \end{bmatrix}$

$B_{005} = \begin{bmatrix} b & a \\ c & d \end{bmatrix}$, $B_{006} = \begin{bmatrix} b & a \\ d & c \end{bmatrix}$, $B_{007} = \begin{bmatrix} b & d \\ a & c \end{bmatrix}$, $B_{008} = \begin{bmatrix} c & a \\ d & b \end{bmatrix}$, $B_{009} = \begin{bmatrix} c & b \\ a & d \end{bmatrix}$, $B_{010} = \begin{bmatrix} c & d \\ a & b \end{bmatrix}$, $B_{011} = \begin{bmatrix} d & b \\ c & a \end{bmatrix}$, $B_{012} = \begin{bmatrix} d & c \\ b & a \end{bmatrix}$

BULLETIN OF MATHEMATICS AND STATISTICS RESEARCH
A Peer Reviewed International Journal,
Contents available on www.bomsr.com
RADMAS– 2016
Vol.4. S1.2016; ISSN: 2348-0580
Email:editorbomsr@gmail.com

2.1. Encryption:

Step 1:The text message is divided into data blocks of 144 characters each. All the 144 characters are coded to decimal equivalents using ASCII table and are written as 12x12 matrix called the message matrix M.

Step 2: Any two matrices say B_{lmn} and B_{opq} from the set B are selected at random. Then the product of these two matrices raised to the powers rst, uvwis computed which is represented as the encoding matrix A.

A =$B_{lmn}^{rst} * B_{opq}^{uvw}$

The Subscript lmn of the first matrix, the power rst to which it is raised and the subscript opq of the second matrix, the power uvw to which it is raised [l m n r s t o p q u v w] successivelyconstitute the secret key. The Alice also encrypts the secret key and communicates to the receiver in a public channel.

Step 3:The message matrix M is multiplied with the encoded matrix A raised to the power't' and the resulting matrix is adjusted to mod 256 called the cipher matrix C.

E= MxA then it is adjusted to mod 256

C = mod (E, 256)

Step 4: All the elements of the matrix C along with the power 1 are coded to the text characters using the ASCII code table which isthe cipher text C.

The integer parts of the matrix E when adjusted to mod 256 is named as the integer matrix I.

Example: when 1,209 is adjusted to mod 256 the integer part is 4 and the residue part is 185.

All the elements of the integer matrix I along with the power to which the matrix A is raised are written successively as a string of numbers called the cipher string I.The cipher text C along with the cipher string I are communicated to the Bob in a public channel.

2.2 Encryption of the secret key:

Before communicating the message, the Alice and the Bob agree upon to use a non-singular 12x12matrix S to encrypt and decrypt the secret key. The secret key[l m n r s t o p q u v w] is first converted to weighted 8421 BCD code. The 8421 BCD code thus obtained is gray coded. Then it is 8421BCD decoded and written as 1 ×12 matrix. This 1 × 12 matrix is multiplied with the 12x12 matrix S which is already agreed by both the Alice and the BobSaythe 1x12matrix K_E. This K_E is the encrypted secret key and it is sent in public channel to the Bob.

2.3. Decryption:

TheBob after receiving the cipher text C, cipher string I and the encrypted secret key K_E first verifies that the corresponding numeral of the last character of the cipher text C is same as the last numeral in the string I.

2.4 Decryption of the secret key:

To obtain the secret key K from the encrypted key K_E the receiver multipliesthe 1x12 matrix $K_E$with the inverse of the agreed upon 12x12matrix S. Then the elements of the resulting 1x12 matrix are 8421BCD encoded and gray decoded.Finally the result is 8421 BCD decoded to get secret key K.

Using the secret key [l m n r s t o p q u v w] the receiver computes the encoding matrix A.

A =$B_{lmn}^{rst} * B_{opq}^{uvw}$

BULLETIN OF MATHEMATICS AND STATISTICS RESEARCH
A Peer Reviewed International Journal,
Contents available on www.bomsr.com
Vol.4. S1.2016; ISSN: 2348-0580
Email:editorbomsr@gmail.com
RADMAS– 2016

Step 1: All the characters of the cipher text C are coded to the decimal equivalentsusing ASCII code table excluding the last numeral and are written as 12x12 matrix say the cipher matrix C. All the elements of the cipher sting I of integers received along with the cipher text C excluding the last numeral are arranged in the form of 12x12 matrix I.

Step 2: Each element of the matrix I is multiplied with 256 and added to the corresponding element of cipher matrix C.

D = 276*I + C (or) Dij= 256Iij + Cij

where Dij, Iij and Cij are the elements of matrices D, I and C respectively.

Step 3: The matrix D is multiplied with inverse of the encoding matrix A raised to the power t to get the message matrix M.

$M = D*[inv\ (A)]^t$

Step 4: Then the numerals are coded to the text characters using ASCII code table which is the original message.

3.Example: Suppose Alice and Bob want to communicate with each other first they agree upon to use a non-singular 8x8 matrix S for encryption and decryption of the secret key.

$$S=\begin{bmatrix} 5 & 2 & 5 & 3 & 7 & 8 & 4 & 1 & 3 & 2 & 6 & 5 \\ 8 & 9 & 6 & 1 & 7 & 5 & 4 & 2 & 3 & 8 & 9 & 7 \\ 8 & 1 & 2 & 6 & 3 & 9 & 5 & 4 & 3 & 2 & 9 & 6 \\ 1 & 3 & 5 & 4 & 3 & 9 & 8 & 7 & 6 & 5 & 4 & 3 \\ 2 & 1 & 7 & 6 & 8 & 5 & 9 & 4 & 2 & 1 & 2 & 3 \\ 6 & 5 & 7 & 9 & 8 & 9 & 5 & 7 & 2 & 2 & 3 & 9 \\ 6 & 7 & 8 & 9 & 4 & 5 & 2 & 1 & 6 & 4 & 9 & 8 \\ 7 & 6 & 4 & 3 & 5 & 2 & 1 & 9 & 8 & 1 & 2 & 3 \\ 4 & 7 & 6 & 8 & 5 & 5 & 4 & 3 & 2 & 9 & 8 & 3 \\ 5 & 3 & 2 & 9 & 6 & 7 & 4 & 3 & 5 & 3 & 2 & 9 \\ 5 & 0 & 3 & 5 & 6 & 1 & 7 & 4 & 3 & 5 & 2 & 1 \\ 3 & 5 & 2 & 3 & 4 & 3 & 6 & 7 & 8 & 9 & 1 & 3 \end{bmatrix}$$

3.1. Encryption:

Step 1: Suppose Alice wants to send the message **DONT JUST WAIT FOR GOOD THINGS TO HAPPEN TO YOU WORK HARD TO ACHIEVE YOUR GOAL to** Bob. She converts this message to decimal equivalents using ASCII code table. The text message in the present example has 79 characters. The remaining characters are filled at random. These decimal numbers are arranged in the form of 12x12 matrix M

BULLETIN OF MATHEMATICS AND STATISTICS RESEARCH
A Peer Reviewed International Journal,
Contents available on www.bomsr.com
RADMAS– 2016
Vol.4. S1.2016; ISSN: 2348-0580
Email:editorbomsr@gmail.com

$$M = \begin{bmatrix} 68 & 79 & 78 & 84 & 32 & 74 & 85 & 83 & 84 & 32 & 87 & 65 \\ 73 & 84 & 32 & 70 & 79 & 82 & 32 & 71 & 79 & 79 & 68 & 32 \\ 84 & 72 & 73 & 78 & 71 & 83 & 32 & 84 & 79 & 32 & 72 & 65 \\ 80 & 80 & 69 & 78 & 32 & 84 & 79 & 32 & 89 & 79 & 85 & 32 \\ 87 & 79 & 82 & 75 & 32 & 72 & 65 & 82 & 68 & 32 & 84 & 79 \\ 32 & 65 & 67 & 72 & 73 & 69 & 86 & 69 & 32 & 89 & 79 & 85 \\ 82 & 32 & 71 & 79 & 65 & 76 & 83 & 42 & 42 & 42 & 42 & 42 \\ 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 \\ 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 \\ 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 \\ 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 \\ 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 \end{bmatrix}$$

Step 2:Two matrices B_{01} and B_{04} are selected at random from the set B of matrices. The product of these two matrices B_{01} and B_{04} are raised to the power 01 and is the encoding matrix A.

$$A= B_{001}^{001} * B_{004}^{001} = \begin{bmatrix} 1 & 15 & 0 & 0 & 0 & 0 & 25 & -5 & -40 & 0 & 0 & 0 \\ 25 & 1 & 8 & 0 & 0 & 0 & 5 & 39 & -8 & -72 & 0 & 0 \\ 0 & 24 & 1 & -9 & 0 & 0 & 40 & 8 & 17 & -9 & -72 & 0 \\ 0 & 0 & 9 & 1 & -24 & 0 & 0 & 72 & 9 & -17 & -8 & -40 \\ 0 & 0 & 0 & -8 & 1 & -25 & 0 & 0 & 72 & 8 & -39 & -5 \\ 0 & 0 & 0 & 0 & -15 & 1 & 0 & 0 & 0 & 40 & -39 & -5 \\ 25 & -5 & 0 & 0 & 0 & 0 & 25 & -25 & 40 & 0 & 0 & 0 \\ 5 & 9 & -8 & 0 & 0 & 0 & 15 & -89 & -24 & 72 & 0 & 0 \\ 0 & 8 & 1 & -9 & 0 & 0 & 40 & 8 & -145 & -9 & 72 & 0 \\ 0 & 0 & 9 & 1 & -8 & 0 & 0 & 72 & -9 & -145 & 8 & 40 \\ 0 & 0 & 0 & 8 & 9 & -5 & 0 & 0 & 72 & -24 & -89 & 15 \\ 0 & 0 & 0 & 0 & 5 & 25 & 0 & 0 & 0 & 40 & -25 & -25 \end{bmatrix}$$

The subscripts of these matrices along with the powers [00 100 4 0 0 1 0 0 1] constitute the secret key K.

Step 3: The message matrix M is multiplied with the encoding matrix A raised to the power 1. $E=M*A^1$ and E is adjusted to mod 256

BULLETIN OF MATHEMATICS AND STATISTICS RESEARCH
A Peer Reviewed International Journal,
Contents available on www.bomsr.com
RADMAS– 2016
Vol.4. S1.2016; ISSN: 2348-0580
Email:editorbomsr@gmail.com

C= mod (E, 256) =

$$\begin{bmatrix} 231 & 125 & 150 & 122 & 62 & 208 & 169 & 61 & 78 & 74 & 82 & 142 \\ 0 & 242 & 20 & 86 & 125 & 103 & 102 & 240 & 184 & 244 & 53 & 31 \\ 32 & 216 & 22 & 30 & 231 & 85 & 104 & 176 & 176 & 82 & 105 & 173 \\ 119 & 213 & 163 & 183 & 9 & 171 & 167 & 225 & 99 & 45 & 79 & 191 \\ 1 & 213 & 65 & 197 & 95 & 59 & 161 & 67 & 121 & 47 & 245 & 117 \\ 56 & 40 & 236 & 86 & 38 & 230 & 78 & 68 & 106 & 100 & 74 & 54 \\ 95 & 193 & 98 & 200 & 97 & 59 & 219 & 33 & 138 & 86 & 129 & 211 \\ 48 & 136 & 72 & 96 & 192 & 88 & 156 & 32 & 96 & 248 & 128 & 184 \\ 48 & 136 & 72 & 96 & 192 & 88 & 156 & 32 & 96 & 248 & 128 & 184 \\ 48 & 136 & 72 & 96 & 192 & 88 & 156 & 32 & 96 & 248 & 128 & 184 \\ 48 & 136 & 72 & 96 & 192 & 88 & 156 & 32 & 96 & 248 & 128 & 184 \\ 48 & 136 & 72 & 96 & 192 & 88 & 156 & 32 & 96 & 248 & 128 & 184 \end{bmatrix}$$

Step 4: All the elements of the matrix C along with the power 1
are coded to the text characters using the ASCII code table which is the cipher text C.
ç}z>Ð©=NJRŽ(NULLCHARACTER)òDC4V}gfð¸ô5US(SPACE)ØSYNRSçUh°°Ri-wÕ£·HT«§ác-O¿SOHÕAÅ_;¡Cy/õu8(ìV&æNDjdJ6_ÁbÈa;
Û!ŠVűÓ0ˆH`Xœ(SPACE)`ø€¸0ˆH`Xœ(SPACE)`ø€¸0ˆH`Xœ(SPACE)`ø€¸0ˆH`Xœ(SPACE)`ø€¸0ˆH`Xœ(SPACE)`ø€¸ SOH
This cipher text C along with the cipher string I whose last number is 1 is communicated to Bob in a public channel.

3.2Encryption of the secret key: Before communicating the messages Alice and Bob agree upon to use the 12x12nonsingular matrix S.

K= [0 0 1 0 0 1 00 4 0 0 1]

K is 8421BCD encoded to get K_1.

K_1= [0000 0000 0001 0000 0000 0001 0000 0004 0001]

K_1 is gray coded to get K_2

K_2= [0000 0000 0001 1000 0000 0001 1000 0000 0110 0000 0000 0001]

K_2 is 8421BCD decoded to get K_3

K_3=[0 0 1 8 0 1 8 0 6 0 0 1]

K_3 is multiplied with S to get encrypted key K_E

$K_E = K_3$*S=[97 133 151 170 101 163120 100121 139 165 124]

K_E = = [97 133 151 170 101 163120 100121 139 165 124]

is sent to Bob as encrypted secret key in a Public channel.

3.3. Decryption:

Before attempting for the decryption Bob verifies that the numeral corresponding to the last character in the cipher text C is same as the last numeral in the cipher string I.Bob starts the decryption process as follows. **Decryption of the secret key**:

K_E = [97 133 151 170 101 163120 100121 139 165 124]

BULLETIN OF MATHEMATICS AND STATISTICS RESEARCH
A Peer Reviewed International Journal,
Contents available on www.bomsr.com
RADMAS– 2016
Vol.4. S1.2016; ISSN: 2348-0580
Email:editorbomsr@gmail.com

K_3 = KE * Inv(s) =[0 0 1 8 0 1 8 0 6 0 0 1]

K_3 is 8421 BCD encoded to get K_2

K_2= [0000 0000 0001 1000 0000 00011000 0000 0110 00000000 0001]

K_2 is gray decoded to get K_1

K_1=[0000 0000 0001 0000 0000 0001 0000 0000 0100 0000 0000 0001]

Finally it is 8421 BCD decoded to get decrypted key K

K= [0 0 1 0 0 10 4 0 0 1]

Step 1:Using the secret key Bob selects the matrices B_{01} and B_{04} from the set of B of matrices.He computes the product of these two matrices raised to the power 001 and 001 in the correct order.

$$A= B_{001}^{001} * B_{004}^{001}= \begin{bmatrix} 1 & 15 & 0 & 0 & 0 & 0 & 25 & -5 & -40 & 0 & 0 & 0 \\ 25 & 1 & 8 & 0 & 0 & 0 & 5 & 39 & -8 & -72 & 0 & 0 \\ 0 & 24 & 1 & -9 & 0 & 0 & 40 & 8 & 17 & -9 & -72 & 0 \\ 0 & 0 & 9 & 1 & -24 & 0 & 0 & 72 & 9 & -17 & -8 & -40 \\ 0 & 0 & 0 & -8 & 1 & -25 & 0 & 0 & 72 & 8 & -39 & -5 \\ 0 & 0 & 0 & 0 & -15 & 1 & 0 & 0 & 0 & 40 & -39 & -5 \\ 25 & -5 & 0 & 0 & 0 & 0 & 25 & -25 & 40 & 0 & 0 & 0 \\ 5 & 9 & -8 & 0 & 0 & 0 & 15 & -89 & -24 & 72 & 0 & 0 \\ 0 & 8 & 1 & -9 & 0 & 0 & 40 & 8 & -145 & -9 & 72 & 0 \\ 0 & 0 & 9 & 1 & -8 & 0 & 0 & 72 & -9 & -145 & 8 & 40 \\ 0 & 0 & 0 & 8 & 9 & -5 & 0 & 0 & 72 & -24 & -89 & 15 \\ 0 & 0 & 0 & 0 & 5 & 25 & 0 & 0 & 0 & 40 & -25 & -25 \end{bmatrix}$$

Step 2: The cipher text C excluding the last character is coded to the decimal numbers using ASCII code table and all the numbers are written as 12x12 matrix, the cipher matrix C.

Step 3:The String I of integers received along with the cipher text in public is converting to 8x8 matrix I excluding the last numeral.

D=256*I+C is computed

Step 4:The matrix D is multiplied with the inverse of encoding matrix A raised to the power 1 to get the matrix M.

M = D * Inv[A^1]

$$M = \begin{bmatrix} 68 & 79 & 78 & 84 & 32 & 74 & 85 & 83 & 84 & 32 & 87 & 65 \\ 73 & 84 & 32 & 70 & 79 & 82 & 32 & 71 & 79 & 79 & 68 & 32 \\ 84 & 72 & 73 & 78 & 71 & 83 & 32 & 84 & 79 & 32 & 72 & 65 \\ 80 & 80 & 69 & 78 & 32 & 84 & 79 & 32 & 89 & 79 & 85 & 32 \\ 87 & 79 & 82 & 75 & 32 & 72 & 65 & 82 & 68 & 32 & 84 & 79 \\ 32 & 65 & 67 & 72 & 73 & 69 & 86 & 69 & 32 & 89 & 79 & 85 \\ 82 & 32 & 71 & 79 & 65 & 76 & 83 & 42 & 42 & 42 & 42 & 42 \\ 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 \\ 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 \\ 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 \\ 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 \\ 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 & 42 \end{bmatrix}$$

BULLETIN OF MATHEMATICS AND STATISTICS RESEARCH
A Peer Reviewed International Journal,
Contents available on www.bomsr.com
RADMAS– 2016
Vol.4. S1.2016; ISSN: 2348-0580
Email:editorbomsr@gmail.com

All the elements are coded to text characters using the ASCII code table which is the original message

DONT JUST WAIT FOR GOOD THINGS TO HAPPEN TO YOU WORK HARD TO ACHIEVE YOUR GOAL

4. Cryptanalysis and Conclusions:

The original message contains only 79 characters but the size of the block here is 144. So, the remaining characters are dummy which may be selected at random. Here same dummy character "." is selected to fill the remaining characters. But, in the cipher the same character is mapped to different characters. This shields the cipher against the security implications like chosen plain text attacks, chosen cipher text attacks, linear cryptanalysis and mono-alphabetic cryptanalysis. In the proposed algorithm encoding matrix A is the product of two matrices B_{lmn} and B_{opq} belonging to the set B. The size of key space can be increased by braiding the elements of the set B to form 16x16 non-singular matrices of the type

$\begin{bmatrix} B_{pq} & 0 \\ 0 & B_{rs} \end{bmatrix}$ or $\begin{bmatrix} B_{pq} & B_{rs} \\ 0 & B_{tu} \end{bmatrix}$ or $\begin{bmatrix} B_{pq} & 0 \\ B_{rs} & B_{tu} \end{bmatrix}$ and so on.

The encrypted secret key can be decrypted only by the authenticated receiver. i.e., who knows the matrix S. The procedure can be further improved to enhance the security level by selecting more matrices from the set B of matrices and raising each matrix to the power f(i,j) where the function f(i,j) is confidential between the communicating parties. So, the encryption algorithm presented here provides high level of security at relatively low computational overhead.

5. References

[1]. Lester Hill, "Concerning certain linear transformation apparatus of cryptography", The American Mathematical monthly, March 1931, pp 135-154.

[2]. Richard Liboff, "Introductory quantum mechanics, IV Edition, Addison Wesley, 2002.

[3]. J. J. Sakurai, "Modern quantum mechanics", Addidon Wesley, 1985.

[4]. Steward EG ,"Quantum mechanics: its early development and the road to entanglement", 2008,Imperial College Press. ISBN 978-1860949784.

[5]. Jaeger G, "Entanglement, information, and the interpretation of quantum mechanics", Heildelberg 2009: Springer, ISBN 978-3-540-92127-1.

[6]. Gould HW., "A history of the Fibonacci Q-matrix and a higher-dimensional problem, the Fibonacci quart." 1981(19),250-7.

[7]. Hoggat VE., "Fibonacci and Lucas numbers", Palo Alto, CA: Houghton-Mifflin, 1969.

[8]. Stakhov A.P. , "The golden matrices and a new kind of cryptography", Chaos, Solutions and Fractals, 2006.

[9]. B.Vellainkannan, Dr. V. Mohan, V. Gnanaraj "A Note on the application of Quadratic forms in Coding Theory with a note on Security", International Journal Computer Tech. Applications Vol 1(1) 78-87.

[10]. Bibhudendra Acharya , Saroj Kumar Panigrahy, Sarat Kumar Patra , and Ganapati Panda, "Image Encryption using Advanced Hill cipher Algorithm", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009.

[11]. Birendra Goswami, Dr.S.N.Singh "Enhancing Security in Cloud computing using Public Key Cryptography with Matrices" International Journal of Engineering Research and Applications

Vol. 2, Issue 4, July-August 2012, pp.339-344 339.

[12]. Ayan Mahalanobis, "Are Matrices Useful in Public-Key Cryptography?"International Mathematical Forum, Vol. 8, 2013, no. 39, 1939 - 1953 HIKARI Ltd, www.m-hikari.com http://dx.doi.org/10.12988/imf.2013.310187.

[13]. Asrjen K. Lenstra and Eric R. Verheul, "Selecting cryptographic key size", Journal of Cryptology, 2001, Volume-14, Number 4, pages 255-293.