Secure Cryptosystem based on Braiding/Entanglement of Pauli 3/2 Matrices

D. Sravana Kumar
Reader in Physics
Dr.V.S.Krishna Government Degree college
Visakhapatnam

P. Sirisha
Faculty in Mathematics
Indian Maritime University
Visakhapatnam

Ch. Suneetha
Assistant Professor in Mathematics
GITAM University
Visakhapatnam

ABSTRACT
As the internet is the basic means of communication nowadays,secure transmission of the sensitive information to the genuine recipient has become a Herculean task. Cryptography is an essential tool for protecting information in computer systems. This paper presents a novel encryption scheme using Braiding/Entanglement of Pauli Spin 3/2 matrices.

Keywords
Braiding/Entanglement, Encryption and Decryption

1. INTRODUCTION
Hill cipher was invented in 1929 by Lester S. Hill [1]. It is a famous Polygram and classical ciphering algorithm based on matrix transformation. Hill cipher is a block cipher 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 3/2 matrices.

1.1 Pauli Spin 3/2 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-3/2 matrices are

$$S_x = \frac{1}{2}\begin{bmatrix} 0 & \sqrt{3} & 0 & 0 \\ \sqrt{3} & 0 & 2 & 0 \\ 0 & 2 & 0 & \sqrt{3} \\ 0 & 0 & \sqrt{3} & 0 \end{bmatrix}$$

$$S_y = \frac{1}{2i}\begin{bmatrix} 0 & 0 & 0 & 0 \\ -\sqrt{3} & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 0 & 0 & -\sqrt{3} & 0 \end{bmatrix}$$

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

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 = $\begin{bmatrix} a_{11} & a_{12} \\ a_{13} & a_{14} \end{bmatrix}$

b = $\begin{bmatrix} b_{11} & b_{12} \\ b_{13} & b_{14} \end{bmatrix}$, c = $\begin{bmatrix} c_{11} & c_{12} \\ c_{13} & c_{14} \end{bmatrix}$, d = $\begin{bmatrix} d_{11} & d_{12} \\ d_{13} & d_{14} \end{bmatrix}$ are four non-singular matrices of order 2x2 then these four non-singular matrices are braided/entangled to get higher order 4x4 matrices as

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

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

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

D = $\begin{bmatrix} c & b \\ a & d \end{bmatrix} = \begin{bmatrix} c_{11} & b_{12} & b_{11} & b_{12} \\ c_{21} & c_{22} & b_{21} & b_{22} \\ a_{11} & a_{12} & d_{11} & d_{12} \\ a_{21} & a_{22} & d_{21} & d_{22} \end{bmatrix}$ 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 above set of Pauli Spin 3/2 matrices with some elementary transformations are reduced to the matrices

b = $\begin{bmatrix} 0 & 3 & 0 & 0 \\ 3 & 0 & 2 & 0 \\ 0 & 2 & 0 & 3 \\ 0 & 0 & 3 & 0 \end{bmatrix}$

c = $\begin{bmatrix} 0 & -3 & 0 & 0 \\ 3 & 0 & -2 & 0 \\ 0 & 2 & 0 & -3 \\ 0 & 0 & 3 & 0 \end{bmatrix}$

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

These three matrices which were derived from Pauli spin 3/2 matrices along with the identity matrix (I 4x4 = a) are braided or entangled in different possible ways to get a set B of 16 non singular matrices.

$$B_{01}=\begin{bmatrix} a & b \\ c & d \end{bmatrix}=\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 & 0 & 3 \\ 0 & 0 & 0 & 1 & 0 & 0 & 3 & 0 \\ 0 & -3 & 0 & 0 & 3 & 0 & 0 & 0 \\ 3 & 0 & -2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & -3 & 0 & 0 & -1 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & -3 \end{bmatrix}$$

$$B_{02}=\begin{bmatrix} a & d \\ b & c \end{bmatrix}=\begin{bmatrix} 1 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -3 \\ 0 & 3 & 0 & 0 & 0 & -3 & 0 & 0 \\ 3 & 0 & 2 & 0 & 3 & 0 & -2 & 0 \\ 0 & 2 & 0 & 3 & 0 & 2 & 0 & -3 \\ 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 \end{bmatrix}$$

$$B_{03}=\begin{bmatrix} a & c \\ b & d \end{bmatrix}=\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & -3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & -2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 & 0 & -3 \\ 0 & 0 & 0 & 1 & 0 & 0 & 3 & 0 \\ 0 & 3 & 0 & 0 & 3 & 0 & 0 & 0 \\ 3 & 0 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & 3 & 0 & 0 & -1 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & -3 \end{bmatrix}$$

$$B_{04}=\begin{bmatrix} a & d \\ c & b \end{bmatrix}=\begin{bmatrix} 1 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -3 \\ 0 & -3 & 0 & 0 & 0 & 3 & 0 & 0 \\ 3 & 0 & -2 & 0 & 3 & 0 & 2 & 0 \\ 0 & 2 & 0 & -3 & 0 & 2 & 0 & 3 \\ 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 \end{bmatrix}$$

$$B_{05}=\begin{bmatrix} b & c \\ d & a \end{bmatrix}=\begin{bmatrix} 0 & 3 & 0 & 0 & 0 & -3 & 0 & 0 \\ 3 & 0 & 2 & 0 & 3 & 0 & -2 & 0 \\ 0 & 2 & 0 & 3 & 0 & 2 & 0 & -3 \\ 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 \\ 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -3 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$B_{06}=\begin{bmatrix} b & c \\ a & d \end{bmatrix}=\begin{bmatrix} 0 & 3 & 0 & 0 & 0 & -3 & 0 & 0 \\ 3 & 0 & 2 & 0 & 3 & 0 & -2 & 0 \\ 0 & 2 & 0 & 3 & 0 & 2 & 0 & -3 \\ 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 \\ 1 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -3 \end{bmatrix}$$

$$B_{07} = \begin{bmatrix} b & d \\ a & c \end{bmatrix} = \begin{bmatrix} 0 & 3 & 0 & 0 & 3 & 0 & 0 & 0 \\ 3 & 0 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & 3 & 0 & 0 & -1 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & -3 \\ 1 & 0 & 0 & 0 & 0 & -3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & -2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 & 0 & -3 \\ 0 & 0 & 0 & 1 & 0 & 0 & 3 & 0 \end{bmatrix} B_{08}=$$

$$\begin{bmatrix} b & a \\ d & c \end{bmatrix} = \begin{bmatrix} 0 & 3 & 0 & 0 & 1 & 0 & 0 & 0 \\ 3 & 0 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & 3 & 0 & 0 & 1 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 & 0 & -3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & -2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 & 0 & -3 \\ 0 & 0 & 0 & -3 & 0 & 0 & 3 & 0 \end{bmatrix}$$

$$B_{09} = \begin{bmatrix} c & d \\ a & b \end{bmatrix} = \begin{bmatrix} 0 & -3 & 0 & 0 & 3 & 0 & 0 & 0 \\ 3 & 0 & -2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & -3 & 0 & 0 & -1 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & -3 \\ 1 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 & 0 & 3 \\ 0 & 0 & 0 & 1 & 0 & 0 & 3 & 0 \end{bmatrix}$$

$$B_{10} = \begin{bmatrix} c & a \\ d & b \end{bmatrix} = \begin{bmatrix} 0 & -3 & 0 & 0 & 1 & 0 & 0 & 0 \\ 3 & 0 & -2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & -3 & 0 & 0 & 1 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 1 \\ 3 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 & 0 & 3 \\ 0 & 0 & 0 & -3 & 0 & 0 & 3 & 0 \end{bmatrix}$$

$$B_{11} = \begin{bmatrix} c & b \\ a & d \end{bmatrix} = \begin{bmatrix} 0 & -3 & 0 & 0 & 0 & 3 & 0 & 0 \\ 3 & 0 & -2 & 0 & 3 & 0 & 2 & 0 \\ 0 & 2 & 0 & -3 & 0 & 2 & 0 & 3 \\ 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 \\ 1 & 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -3 \end{bmatrix}$$

$$B_{12} = \begin{bmatrix} c & b \\ d & a \end{bmatrix} = \begin{bmatrix} 0 & -3 & 0 & 0 & 0 & 3 & 0 & 0 \\ 3 & 0 & -2 & 0 & 3 & 0 & 2 & 0 \\ 0 & 2 & 0 & -3 & 0 & 2 & 0 & 3 \\ 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 \\ 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -3 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$B_{13} = \begin{bmatrix} d & a \\ b & c \end{bmatrix} = \begin{bmatrix} 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -3 & 0 & 0 & 0 & 1 \\ 0 & 3 & 0 & 0 & 0 & -3 & 0 & 0 \\ 3 & 0 & 2 & 0 & 3 & 0 & -2 & 0 \\ 0 & 2 & 0 & 3 & 0 & 2 & 0 & -3 \\ 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 \end{bmatrix}$$

$$B_{14} = \begin{bmatrix} d & a \\ c & b \end{bmatrix} = \begin{bmatrix} 3 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -3 & 0 & 0 & 0 & 1 \\ 0 & -3 & 0 & 0 & 0 & 3 & 0 & 0 \\ 3 & 0 & -2 & 0 & 3 & 0 & 2 & 0 \\ 0 & 2 & 0 & -3 & 0 & 2 & 0 & 3 \\ 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 \end{bmatrix}$$

$$B_{15} = \begin{bmatrix} d & b \\ c & a \end{bmatrix} = \begin{bmatrix} 3 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & 2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 & 0 & 3 \\ 0 & 0 & 0 & -3 & 0 & 0 & 3 & 0 \\ 0 & -3 & 0 & 0 & 1 & 0 & 0 & 0 \\ 3 & 0 & -2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & -3 & 0 & 0 & 1 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$B_{16} = \begin{bmatrix} d & c \\ b & a \end{bmatrix} = \begin{bmatrix} 3 & 0 & 0 & 0 & 0 & -3 & 0 & 0 \\ 0 & 1 & 0 & 0 & 3 & 0 & -2 & 0 \\ 0 & 0 & -1 & 0 & 0 & 2 & 0 & -3 \\ 0 & 0 & 0 & -3 & 0 & 0 & 3 & 0 \\ 0 & 3 & 0 & 0 & 1 & 0 & 0 & 0 \\ 3 & 0 & 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 2 & 0 & 3 & 0 & 0 & 1 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

2.1 Encryption

Step 1: The text message is divided into data

blocks of 64 characters each. All the 64characters are coded to decimal equivalents using ASCII table and are written as 8x8 matrix called the message matrix M.

Step 2:Any two matrices say Blm and Bno from the set B of non singular matrices are selected at random. Then the product of these two matrices raised to the powers pq, rs is computed which is represented as the encoding matrix A.

$$A = B_{lm}^{pq} * B_{no}^{rs}$$

The Subscript lm of the first matrix, the power pq to which it is raised and the subscript no of the second matrix, the power rs to which it is raised

[l m p q n o r s] successively constitute the secret key. The sender 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= M x At then it is adjusted to mod 256

C = mod(E,256)

Step 4: All the elements of the matrix C along with the power‘t’ are coded to the text characters using the ASCII code table which is the cipher text C.

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

Example: when 1,116 is adjusted to mod 256 the integer part is 4 and the residue part is 92. 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 receiver in public channel.

2.2 Encryption of the secret key

Before communicating the message, the sender and the receiver agree upon to use a non-singular 8x8matrix S to encrypt and decrypt the secret key. The secret key [l m p q n o r s] 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 ×8 matrix. This 1 × 8 matrix is multiplied with the 8x8 matrix S to obtain the 1x8 matrix KE. This KE is the encrypted secret key and it is sent in public channel to the receiver.

2.3 Decryption

The receiver after receiving the cipher text C, cipher string I and the encrypted secret key KE 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 KE the receiver multiplies the 1x8 matrix KE with the inverse of the agreed upon 8x8 matrix S. Then the elements of the resulting 1x8 matrix are 8421 BCD encoded and gray decoded. Finally the result is 8421 BCD decoded to get secret key K. Using the secret key [l m p q n o r s] the receiver computes the encoding matrix A.

$$A = B_{lm}^{pq} * B_{no}^{rs}$$

Step 1:- All the characters of the cipher text C are coded to the decimal equivalents using ASCII code table excluding the last numeral and are written as 8x8 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 8x8 matrix I.

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

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.

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

3.1 Encryption

Step 1: Suppose Alice wants to send the message CONGRATULATIONS to Bob. Alice converts this message to decimal equivalents using ASCII code table. The text message in the present example has 15 characters. The remaining characters are filled at random. These decimal numbers are arranged in the form of 8x8 matrix M

$$M = \begin{bmatrix} 67 & 79 & 78 & 71 & 82 & 65 & 84 & 85 \\ 76 & 65 & 84 & 73 & 79 & 78 & 83 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \end{bmatrix}$$

Step 2:Two matrices B01 and B02 are selected at random from the set B of matrices. The product of these two matrices B01 and B02 are raised to the power 05 and 06is the encoding matrix A.

$$A = B_{01}^{05} * B_{02}^{06} =$$

$$\begin{bmatrix} 1029952 & -252288 & -371808 & -1142208 & 1616736 & -1712736 & -1382976 & 835488 \\ 1405056 & -603392 & 229952 & 878688 & 1109856 & 1316704 & -1999712 & -1514304 \\ 603552 & -90880 & 505472 & 293952 & 672192 & 151328 & -399776 & -351264 \\ -163584 & 83424 & -94656 & -322496 & -26208 & -496320 & 242976 & 417120 \\ 1426176 & -640320 & 511008 & 1733760 & 753120 & 2600544 & -2051520 & -2452896 \\ 34752 & 25152 & 252672 & 207072 & 8352 & 193632 & 162912 & -138816 \\ 406944 & -236736 & 10944 & 21504 & 385344 & 118368 & -530208 & -162144 \\ 1893312 & -545568 & -1540608 & -3064320 & 3211488 & -4242624 & -3131040 & 2297952 \end{bmatrix}$$

The subscripts of these matrices along with the powers [0 1 0 5 0 2 0 6] constitute the secret key K.

Step 3:The message matrix M is multiplied with the encoding matrix A raised to the power 3. E=M*A3 and E is adjusted to mod 256

C= mod (E,256)=

$$\begin{bmatrix} 224 & 160 & 128 & 192 & 192 & 192 & 64 & 128 \\ 224 & 32 & 0 & 192 & 128 & 224 & 0 & 224 \\ 128 & 128 & 224 & 0 & 32 & 128 & 64 & 128 \\ 128 & 128 & 224 & 0 & 32 & 128 & 64 & 128 \\ 128 & 128 & 224 & 0 & 32 & 128 & 64 & 128 \\ 128 & 128 & 224 & 0 & 32 & 128 & 64 & 128 \\ 128 & 128 & 224 & 0 & 32 & 128 & 64 & 128 \\ 128 & 128 & 224 & 0 & 32 & 128 & 64 & 128 \end{bmatrix}$$

Step 4:

All the elements of the matrix C along with the power 3 are coded to the text characters using the ASCII code table which is the cipher text C **.à (non breaking space)€ÀÀÀ@€à(space)(Null char) À€à(Null char)à€€à (Null char)(Space)€@€ €€à(Null char)(Space)€@€ €€à(Null char)(Space)€@€€€à(Null char)(Space)€@€ €€à(Null char)(Space)€@€ €€à(Null char)(Space)€@€(ETX)**

This cipher text C along with the cipher string I whose last number is 3 is communicated to Bob in a public channel.

3.2 Encryption of the secret key

Before communicating the messages Alice and Bob agree upon to use the 8x8 non singular matrix S.

K= [0 1 0 5 0 2 0 6]
K is 8421BCD encoded to get K1.
K_1=[0000 0001 0000 0101 0000 0010 0000 0110]
K_1 is gray coded to get k2
K_2=[0000 0001 1000 0111 1000 0011 0000 0101]

K2 is 8421BCD decoded to get K3

K_3=[0 1 8 7 8 3 0 5]
K_3 is multiplied with S to get encrypted key KE
K_E = K3*S = [71 77 94 152 98 161 83 81]
K_E = [71 77 94 152 98 161 83 81] 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 = [71 77 94 152 98 161 83 81]
K_3 = KE * Inv(s) =[0 1 8 7 8 3 0 5]
K_3 is 8421 BCD encoded to get K2
K_2 =[0000 0001 1000 0111 1000 0011 0000 0101]
K_2 is gray decoded to get k1
K_1=[0000 0001 0000 0101 0000 0010 0000 0110]
Finally it is 8421 BCD decoded to get decrypted key K
K=[0 1 0 5 0 2 0 6]

Step 1:Using the secret key Bob selects the matrices B01 and B02 from the set of B of matrices. He computes the product of these two matrices raised to the power 05 and 06 in the correct order.

$$A = B_{01}^{05} * B_{02}^{06} =$$

$$\begin{bmatrix} 1029952 & -252288 & -371808 & -1142208 & 1616736 & -1712736 & -1382976 & 835488 \\ 1405056 & -603392 & 229952 & 878688 & 1109856 & 1316704 & -1999712 & -1514304 \\ 603552 & -90880 & 505472 & 293952 & 672192 & 151328 & -399776 & -351264 \\ -163584 & 83424 & -94656 & -322496 & -26208 & -496320 & 242976 & 417120 \\ 1426176 & -640320 & 511008 & 1733760 & 753120 & 2600544 & -2051520 & -2452896 \\ 34752 & 25152 & 252672 & 207072 & 8352 & 193632 & 162912 & -138816 \\ 406944 & -236736 & 10944 & 21504 & 385344 & 118368 & -530208 & -162144 \\ 1893312 & -545568 & -1540608 & -3064320 & 3211488 & -4242624 & -3131040 & 2297952 \end{bmatrix}$$

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 8x8 matrix, the cipher matrix C.

Step 3:-The String I of integers received along with the cipher text in public is converted 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 3 to get the matrix M.

$$M = D * Inv[A^3]$$

$$M=\begin{bmatrix} 67 & 79 & 78 & 71 & 82 & 65 & 84 & 85 \\ 76 & 65 & 84 & 73 & 79 & 78 & 83 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \\ 46 & 46 & 46 & 46 & 46 & 46 & 46 & 46 \end{bmatrix}$$

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

4. CRYPTANALYSIS AND CONCLUSIONS

The original message contains only 15 characters but the size of the block here is 64. 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 Blm and Bno belonging to the set B. Hence the size of the key [13] space is 16x15 = 132. If we alter the algorithm such that A is the product of 'q' matrices belonging to the set B, then the size of the key space will be 16 x 15 x ……. x (16+1-q). 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

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

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.