Journal of Physics: Conference Series

PAPER • OPEN ACCESS

Privacy Preserving Message using Padovan Sequence

To cite this article: D A Angel Sherin *et al* 2021 *J. Phys.: Conf. Ser.* **1964** 022026

View the article online for updates and enhancements.

Privacy Preserving Message using Padovan Sequence

D A Angel Sherin[1]**, V Maheswari**[1*] and **V Balaji**[2]
[1]Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies, Chennai – 600 117, Tamilnadu, India.
[2] Department of Mathematics, Sacred Heart College, Tirupattur – 635 601, Tamilnadu, India.
Corresponding Author: *maheswari.sbs@velsuniv.ac.in

Abstract. An evolution of wireless technology created tremendous change in this era. Large quantities of messages are registered, altered and transmitted through wireless or network cable by fixed devices. Privacy of the transmitted message is a main concern in networks. A diversified encryption algorithm has been suggested in these years to preserve the message. We take the cyclic graph and label the edges with the Padovan sequence. The computation of the closed trail matrix is applied in matrix inversion algorithms to get the cipher text. The usage of the symmetric key is applied in the encryption and decryption process. This paper proposes matrix inversion algorithms to transfer the message from sender to receiver. And also we applied SageMath algorithm for drawing the cyclic graphs. The result shows that the proposed algorithm gives enhanced security and efficiency when correlated with existing algorithms.

Keywords. Edge Injective Labeling, Cyclic graph, Padovan sequence, Matrix inversion, closed trail matrix.
2010 Mathematical subject classification Number: 05C78.

1. Introduction

TheInternet plays a major role in this era. Every second, large volumes of messages are transmitted among the devices. Considering the preservation of transmitted messages has endured a main area of concern. This functionality becomes very challenging since there is a rise of intruders and hackers. In the time of years, plenty of cryptographic algorithms have been used to protect the privacy of transmitted messages. The stability of the algorithms depended on the techniques used for controlling, implementing and sharing the secret keys. Secret keys are divided into symmetric and asymmetric keys. Symmetric algorithms mean using the same key for both encryption and decryption. The stability of this algorithm depends on how the key is transmitted between the sender and receiver in a secure manner. Asymmetric algorithm means two different keys inclusive of public and private keys. The private key is not transmitted but the public key is shared between the sender and the receiver.

Acyclic graph is considered and vertices are numbered using function volume. Edge labeling iscomputed using edge injective labeling such that it forms a Padovan sequence. Encryption and decryption process is done using matrix inversion. This paper proposes a closed trail matrix inversion algorithm that reforms the security features of symmetric keys. Since we transmit the message using edge injective labeling on the cyclic graph it is safe and secure from intruders.

Related Works

Researchers like[1][2] S.UmaMaheswari discussed graceful labeling on different paths using Padovan sequence and also she gave even graceful labeling on different paths using Padovan sequence, [3] K.Karthika, investigated data encryption using circuit matrix. [4] ShubhamAgarwal, Anand Singh Uniyal, encoded and decoded message using prime weighted graph. Getting inspired by the above research work we encoded the message using closed trail matrix inversion on cyclic graphs.

2. Preliminaries

Definition 2.1:
A cyclic graph is a graph which contains any cycle graph that is vertex can be traversed back to itself.

Definition 2.2:(Edge Injective Labeling EIL)
Let G(V,E) be a graph with injection vertex set of function volume $n^2 + k$, where n=0,1,2,3… and k=0,1,2,…. which results to Padovan sequence of induced edge set

$$\left\{ \begin{array}{ll} y = 3X - 1; & if\ 1 \leq y \leq 26 \\ y = (3X - 1) mod\ 26; & if\ y \geq 26 \\ y = (3X - 1) mod\ 26 = 0; & Exclude\ the\ case \end{array} \right\}$$

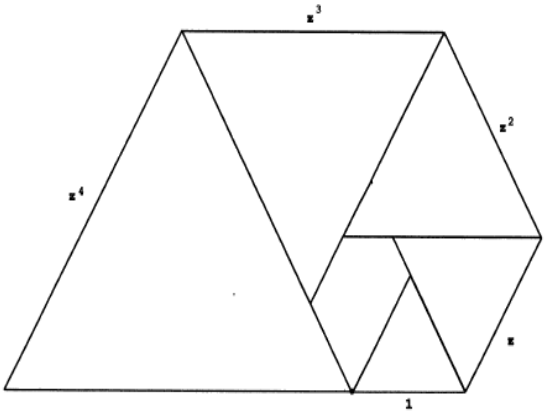
where X is the sum of $u + v$ vertices.

Closed trail 2.3:
In a graph, two trails are said to be edge disjoint if they have no common edge. A set of cycles T of a graph G is called a closed trail if the cycles T_p, $T_q \in$ T, have no edges in common.

Matrix 2.4:
Matrix is a set of numbers form a group and placed in order of rows and columns n x n. Here matrix is formed using the closed trail in cyclic graph T_p, $T_q \in$ T.

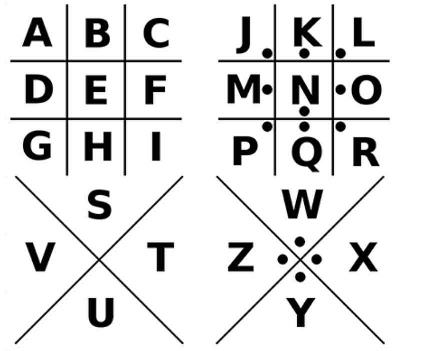
Inversion Matrix 2.5:
Let T be a square matrix with determinant of $T \neq 0$ then there exists a matrix τ which is called the Inverse of the matrix.

Padovan Sequence 2.6:
The Padovan sequence is derived from Dutch Architect Hans Van Der Laan in 1994 by Richard Padovan. A Padovan sequence is like a Fibonnaci sequence with the same recurrence relation.
A Padovan sequence is a series of integers P(n) defined with the initial values P(0)=P(1)=P(2)=1.The recurrence relation of the Padovan sequence is P(n)=P(n-2)+P(n-3). A helix of equal-sided triangle with lateral length forms a Padovan sequence.



Pigpen Cipher 2.7:

The Pigpen Cipher is a method of replacing the letter by the symbols. It is similar to a substitution cipher. The origin of the Pigpen cipher is unknown but it was used by a certain group of people called Freemasons in the 18th century.The encryption process of Pigpen cipher is unique. Each alphabetic letter has a different designed symbol. From the below cipher chart we can design the letter.The decryption process is the converse of the encryption process. Using the cipher chart we locate the image depicted in the ciphertext. Now we replace the letter by that part of the cipher chart.



Pigpen cipher chart

3. Preliminaries

In this section, we briefly describe the cryptosystem of. For symbolic consistency, we flexibly use the following notations. Encryption process is evaluated using edge injective labeling, closed trail and matrix inversion.

SageMath Algorithm 3.1:

The implementation of the cyclic graph is drawn using SageMath application. SageMath is an open-source mathematics software system. This system is licensed under the GPL. It was developed on top of many existing open-source packages NumPy, SciPy, matplotlib, FLINT, R and many more. SageMath has developed to visualize the drawings in Mathematics. SageMath is used to create 2-D, 3-D graphics and animated plots. It also contains interactive tools to dynamically visualize the impact of parameters on calculations.

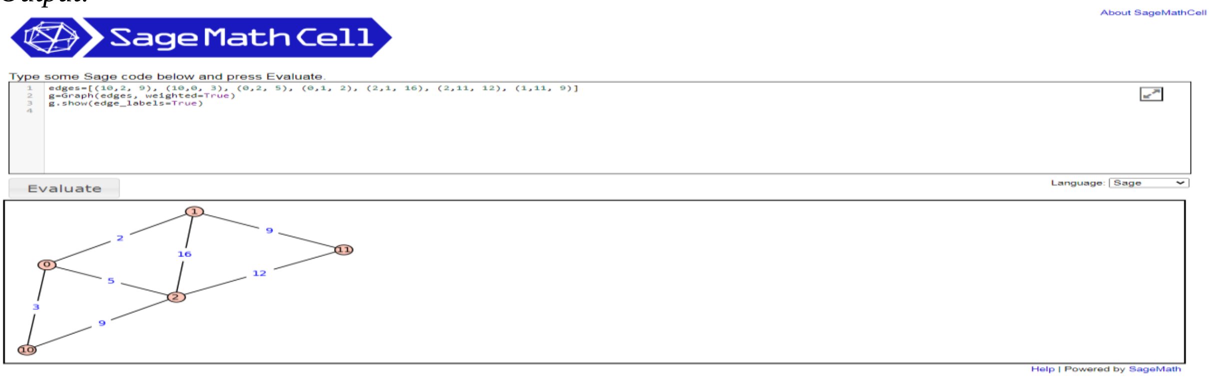
SageMath Algorithm for Graph1 3.1.1:

We have used www.sagecell.sagemath.org to code the graph and we capture the output.

Coding:

```
H=Graph({10:[2,0], 2:[0,1], 11:[2,1], 0:[2,1], 1:[2,11]})
Sage: plot(H)
edges=[(10,2, 9), (10,0, 3), (0,2, 5),  (0,1, 2),  (2,1, 16), (2,11, 12), (1,11, 9)]
g=Graph(edges, weighted=True)
g.show(edge_labels=True)
```

Output:



Type some Sage code below and press Evaluate.

```
edges=[(10,2, 9), (10,0, 3), (0,2, 5), (0,1, 2), (2,1, 16), (2,11, 12), (1,11, 9)]
g=Graph(edges, weighted=True)
g.show(edge_labels=True)
```

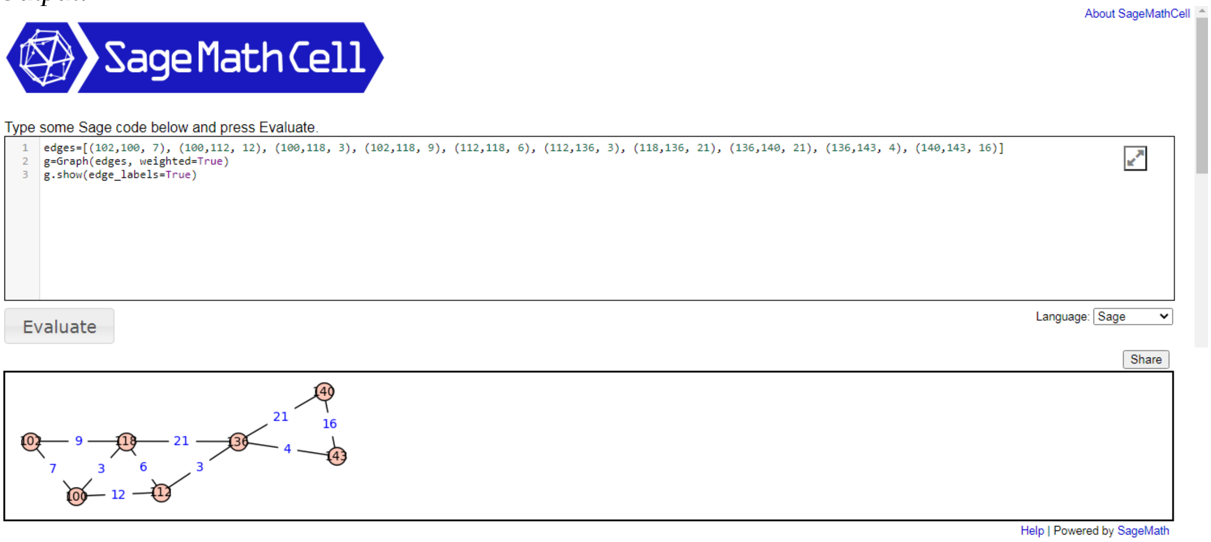
SageMath Algorithm for Graph2 3.1.2:

We have used www.sagecell.sagemath.org to code the graph and we capture the output.

Coding:

```
edges=[(100,102, 7), (100,112, 12), (100,118, 3), (102,118, 9), (112,118, 6), (112,136, 3), (118,136, 21), (136,140, 21), (136,143, 4), (140,143, 16)]
g=Graph(edges, weighted=True)
g.show(edge_labels=True)
```

Output:



Type some Sage code below and press Evaluate.

```
edges=[(102,100, 7), (100,112, 12), (100,118, 3), (102,118, 9), (112,118, 6), (112,136, 3), (118,136, 21), (136,140, 21), (136,143, 4), (140,143, 16)]
g=Graph(edges, weighted=True)
g.show(edge_labels=True)
```

Language: Sage

Encryption Table 3.2:

Encryption table is assigning numbers to the alphabet.

A B C D Z
↓ ↓ ↓ ↓ … ↓
1 2 3 4 26

We can expand the number of characters constantly depending upon the essential of the message to be encrypted.

Encryption Algorithm 3.2:

Let G be a graph cyclic graph with vertices $V(G)) \to n^2 + k$ where n= 0, 1, 1, 3, 3 and k= 0, 0, 1, 1, 2. Let F$_i$ be the corresponding induced edge injective labels given by the definition 2.2. The induced edge labels entries are Padovan sequence P(q)=P(q-2)+P(q-3). Let T be the $q \times i$ matrix formed by a closed trail of cyclic graphs. Therefore

$$T = \begin{pmatrix} F_1 \\ F_2 \\ \vdots \\ \vdots \\ F_i \end{pmatrix} \text{where} F_{1=} \{ f_1, f_2 \cdots\cdots f_q \}$$

We write the values of F$_i$ in row wise, where F$_i$ denotes an each closed trail in a cyclic graph. The formation of matrix depends upon the $q = i$, if $q \neq i$ then we make the matrix to be equal by removing the number of rows or columns. The removed rows or columns are denoted by ψ .

Matrix Inversion 3.3.1:

In an ordinary number say $pq = 1$ then we can obtain $q = \frac{1}{p}$ when q≠0. Also we can write as $q = p^{-1}$ or $pp^{-1} = p^{-1}p = 1$. Likewise matrix inverse is also similar to the division operation in ordinary numbers. Suppose the matrix product is an identity matrix $PQ = 1$. If matrix Q exists, (i.e is nonsingular) then that matrix is particularly written as $Q = P^{-1}$ or $PP^{-1} = I = P^{-1}P$. Matrix inversion exists only for a square matrix.

1. Multiply f_1 by the determinant of the 2×2 matrix by leaving the first row and column. Repeat the same calculation for f_2 and f_3. Then sum them up by placing minus in front of the f_3.

$$T = \begin{pmatrix} f_1 & f_2 & f_3 \\ f_2 & f_4 & f_5 \\ f_5 & f_6 & f_7 \end{pmatrix}$$

$$\left[f_1 \times \begin{vmatrix} f_4 & f_5 \\ f_6 & f_7 \end{vmatrix} \right] - \left[f_2 \times \begin{vmatrix} f_2 & f_5 \\ f_5 & f_7 \end{vmatrix} \right] + \left[f_3 \times \begin{vmatrix} f_2 & f_4 \\ f_5 & f_6 \end{vmatrix} \right]$$

2. To create Minors of matrix, first consider each element of the matrix
   (a) Ignore the values on the current row and column
   (b) Calculate the determinant of the remaining values
   (c) Look the checker board for the signs

$$\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$$

$$\text{Adjoint of } T = \begin{pmatrix} F_1 \\ F_2 \\ \vdots \\ \vdots \\ F_i \end{pmatrix}$$

3. Divide the each element by the determinant of matrix

Algorithm for ψ 3.3.2:

The removed rows or columns of T are encrypted Pigpen cipher. We take each number and look up for the encryption table to find the corresponding alphabet. Then the alphabet is converted into symbols by the Pigpen cipher chart.

Pigpen cipher chart contains two grids in identical shape and form but one pair of grids is distinguished by the placement of dots within each cell. The cipher is employed by representing each plaintext letter with the cell surrounding geometrical shapes.

Decryption Algorithm 3.4:

The receiver gets the matrix and symbols as the message and a clue will be given. The symbols will be decrypted using Pigpen cipher charts. For matrix we will calculate the product of given matrix and identity matrix.

4. Results

Theorem 4.1:
A cyclic graph which admits EIL forms a Padovan sequence.
Proof:
Let us consider $f : V(G)) \rightarrow n^2 + k$ be the vertices where n= 0, 1, 1, 3, 3 and k= 0, 0, 1, 1, 2.
Let F be the corresponding induced edge injective labels given by

$$\left\{\begin{array}{ll} y = 3X - 1; & if\ 1 \leq y \leq 26 \\ y = (3X - 1) mod\ 26; & if\ y \geq 26 \\ y = (3X - 1) mod\ 26 = 0; & Exclude\ the\ case \end{array}\right\}$$

This is edge injective label form Padovan sequence.

Example 4.2:
Let us take a suitable cyclic graph of Figure 1. The vertices are numbered using a certain function volume $n^2 + k$ where n=0, 1, 1, 3, 3 and k=0, 0, 1, 1, 2.We fix an edge value by edge injective labeling with the formation of the Padovan sequence. Now consider the edge label as the Message.
Edge Labels:3 5 9 5 2 16 16 12 9
Corresponding to the encryption table convert the edge labels into Message.
Message D= CEIEBPPLI

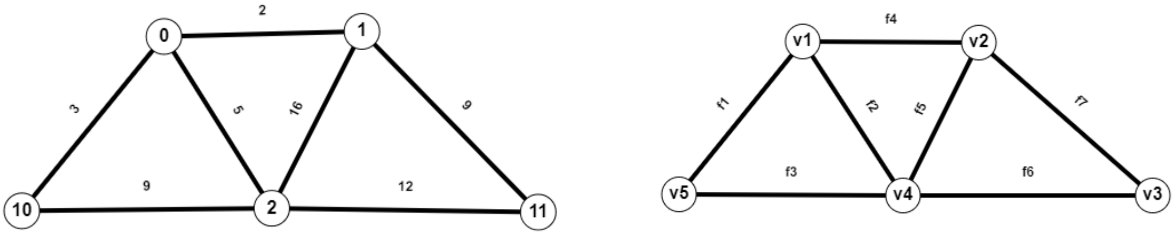


Figure1

Encryption Process 4.2.1:
Now choose the partition created by the closed trail T = { { T₁ }, { T₂ }, { T₃ } }, where

T_1 = { f_1, f_2, f_3 }, T_2 = { f_2, f_6, f_7 } and T_3= { f_4, f_5, f_6 }. We arrange the matrix T= $\begin{pmatrix} T_1 \\ T_2 \\ T_3 \end{pmatrix}$

$$T = \begin{pmatrix} f_1 & f_2 & f_3 \\ f_2 & f_4 & f_5 \\ f_5 & f_6 & f_7 \end{pmatrix} T = \begin{pmatrix} 3 & 5 & 9 \\ 5 & 2 & 16 \\ 16 & 12 & 9 \end{pmatrix}$$

After forming the matrix T. Find $|T| \neq 0$ if it is equal to zero we traverse the matrix by interchanging T_1, T_2, T_3.

$|T| = 758$

$$Adjoint\ of\ T = \begin{pmatrix} -174 & 63 & 62 \\ 211 & -117 & -3 \\ 28 & 44 & -19 \end{pmatrix}$$

$$S = T^{-1} = \frac{Adjo\text{int}\,T}{|T|}$$

$$S = \begin{pmatrix} \frac{-174}{758} & \frac{63}{758} & \frac{62}{758} \\ \frac{211}{758} & \frac{-117}{758} & \frac{-3}{758} \\ \frac{28}{758} & \frac{44}{758} & \frac{-19}{758} \end{pmatrix} \text{ Encrypted message}$$

Decryption Process4.2.2:

The receiver gets the matrix

Clue: Rectangular box

$$S = \begin{pmatrix} \frac{-174}{758} & \frac{63}{758} & \frac{62}{758} \\ \frac{211}{758} & \frac{-117}{758} & \frac{-3}{758} \\ \frac{28}{758} & \frac{44}{758} & \frac{-19}{758} \end{pmatrix} \qquad T=I \times T^{-1}=I \times S$$

$$T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} \frac{-174}{758} & \frac{63}{758} & \frac{62}{758} \\ \frac{211}{758} & \frac{-117}{758} & \frac{-3}{758} \\ \frac{28}{758} & \frac{44}{758} & \frac{-19}{758} \end{pmatrix}$$

Therefore we get the original matrix

$$T = \begin{pmatrix} 3 & 5 & 9 \\ 5 & 2 & 16 \\ 16 & 12 & 9 \end{pmatrix}$$

Now arrange the numbers in the row order 3 5 9 5 2 16 16 12 9

Message is **CEIEBPPLI**

Theorem 4.3:

A cyclic graph which admits EIL forms a Padovan sequence.

Proof:

Let us consider $f : V(G)) \rightarrow n^2 + k$ be the vertices where n= 10, 10, 10, 10, 11, 11, 11 and k= 0, 18, 2, 12, 15, 19, 22.

Let F be the corresponding induced edge injective labels given by

$$\left\{ \begin{array}{ll} y = 3X - 1; & if\ 1 \leq y \leq 26 \\ y = (3X - 1) mod\ 26; & if\ y \geq 26 \\ y = (3X - 1) mod\ 26 = 0; & Exclude\ the\ case \end{array} \right\}$$

This edge injective label forms a Padovan sequence.

Example 4.4:

Let us take a suitable cyclic graph of Figure 2. The vertices are numbered using a certain function volume $n^2 + k$ where n= 10, 10, 10, 10, 11, 11, 11 and k= 0, 18, 2, 12, 15, 19, 22. We fix an edge value by edge injective labeling with the formation of the Padovan sequence. Now consider the edge label as the Message.

Edge Labels: 3 7 9 3 12 6 6 21 3 21 16 4

Corresponding to the encryption table convert the edge labels into Message.

Message D= CGICLFFUCUPD

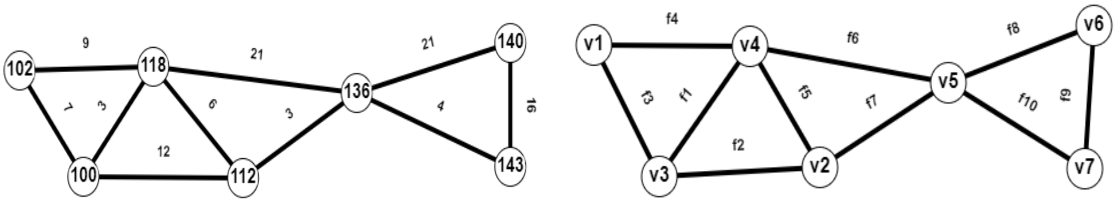


Figure 2

Encryption Process4.4.1:
Now choose the partition created by the closed trail T = { { T$_1$ }, { T$_2$ }, { T$_3$ }, { T$_4$ } }, where T$_1$ = { f$_1$, f$_3$, f$_4$ }, T$_2$ = { f$_1$, f$_2$, f$_5$ } T$_3$={ f$_5$, f$_6$, f$_7$ } and T$_4$= { f$_8$, f$_9$, f$_{10}$ }. We arrange the matrix

$$T=\begin{pmatrix}T_1\\T_2\\T_3\\T_4\end{pmatrix} \quad T=\begin{pmatrix}f_1 & f_3 & f_4\\ f_1 & f_2 & f_5\\ f_5 & f_6 & f_7\\ f_8 & f_9 & f_{10}\end{pmatrix} \quad T=\begin{pmatrix}3 & 7 & 9\\ 3 & 12 & 6\\ 6 & 21 & 3\\ 21 & 16 & 4\end{pmatrix}$$

Since the matrix is 4 x 3, we take 3 x 3 for Inversion matrix computation and the last row will be encrypted using Pigpen cipher. Now find $|T|\neq 0$ if it is equal to zero we traverse the matrix by interchanging T$_1$, T$_2$, T$_3$.

$|T|=-162$

$$Adjoint\ of\ T=\begin{pmatrix}-90 & 168 & -66\\ 27 & -45 & 9\\ -9 & -21 & 15\end{pmatrix}$$

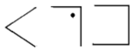
$$S=T^{-1}=\frac{Adjo\mathrm{int}\,T}{|T|}$$

$$S=\begin{pmatrix}\frac{5}{9} & \frac{-28}{27} & \frac{11}{27}\\ \frac{-1}{6} & \frac{5}{18} & \frac{-1}{18}\\ \frac{1}{18} & \frac{7}{54} & \frac{-5}{54}\end{pmatrix}$$

Encrypted message is a combination of matrix and Pigpen cipher.

$$S=\begin{pmatrix}\frac{5}{9} & \frac{-28}{27} & \frac{11}{27}\\ \frac{-1}{6} & \frac{5}{18} & \frac{-1}{18}\\ \frac{1}{18} & \frac{7}{54} & \frac{-5}{54}\end{pmatrix}$$ < ⏋̇ ⊐

Decryption Process 4.4.2:
The receiver gets the matrix

$$S = \begin{pmatrix} \frac{1}{41} & \frac{11}{123} & \frac{-2}{41} \\ \frac{-11}{82} & \frac{1}{123} & \frac{25}{246} \\ \frac{25}{82} & \frac{-2}{41} & \frac{-9}{82} \end{pmatrix}$$ and 

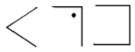
Clue: Rectangular box with animal chart
T=I x T^{-1}= I x S

$$T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \times \begin{pmatrix} \frac{1}{41} & \frac{11}{123} & \frac{-2}{41} \\ \frac{-11}{82} & \frac{1}{123} & \frac{25}{246} \\ \frac{25}{82} & \frac{-2}{41} & \frac{-9}{82} \end{pmatrix}$$

Therefore we get the original matrix

$$T = \begin{pmatrix} 3 & 9 & 7 \\ 12 & 9 & 3 \\ 3 & 21 & 9 \end{pmatrix}$$

Now arrange the numbers in the row order 3 7 9 3 12 6 6 21 3 21 16 4
Last row of the matrix is determined by Pigpen cipher chart



The above symbol represents the alphabets U P D
The original message is **CGICLFFUCUPD**

5. Conclusion

In this paper, we have investigated data encryption using the concepts of graph theory. We have used three major concepts: Edge injective labeling – closed trail – Inversion matrix. Initially, we have labeled the edges by edge injective labeling. Further the labels are converted into messages using an encryption chart. We have generated the matrix using the concepts of graph theory closed trail. We recommended this method for data transforming since it possesses high concealment of data encryption.

6. Application

Cyclic graphs are widely used for the analysis in biological networks. The number of components of the system and their interactions is distinguished as a network in graphical representation. To detect biological components like protein interaction and molecular properties we use cyclic graphs. In operation research the network flow is calculated using directed cyclic graphs. The network flow model, series of water pipes fitting, Kirchhoff‟s current law, ecology, food web, information theory, thermo dynamics, Robert Ulanowicz works under the principle of directed cyclic graph.

References

[1] Uma Maheswari S2013*IJMA* –**4**, p-4
[2] Uma Maheswari S 2013 *IJMA* –**4**, p-10
[3] Karthika K 2019*International Journal of Scientific and technology Research***8**
[4] ShubhamAgarwal, and Anand Singh Uniyal 2015 *International journal of Pure and applied Mathematics***105**

[5] SandhyaMaitra, Manish Bansal, and Preety Gupta 2014 *International journal of Computer Science and mobile computing***3**

[6] Jay Grossman 2008 *Rivier Academic journal***4**

[7] Angel Sherin D A, and Maheswari V 2019 *The International Journal of Recent Technology and Engineering***8**

[8] Angel Sherin D A, and Maheswari V 2019 *The International Journal of analytical and modal analysis***11**, P-167

[9] Ponraj R 2004 *Studies in Labelings of Graphs* Ph.D. thesis

[10] Rekha S, and Maheswari V 2019 *Journal of Physics: Conference Series***1362**

[11] Joseph Pugliano, and BrandsonSehestedt 2017 *Cryptography: Matrices and Encryption*

[12] Angel Sherin D A, and Maheswari V 2019 *Journal of Physics: Conference Series***1362**