Palestine Journal of Mathematics

Vol 14(Special Issue II)(2025) , 180–187

A GRAPH THEORETIC ENCRYPTION USING THE SELF-INVERTIBLE KEY MATRICES AND THE ADJACENCY MATRICES OF COMPLETE GRAPH

P. MOHAN, M.V.SURESH and C. PERIYASAMY

MSC 2010 Classifications: Primary 14G50; Secondary 05B20, 05C50.

Keywords and phrases: Adjacency Matrix, Complete graph, Graph Encryption, Hamiltonian circuit, Self-Invertible Matrix.

Corresponding Author:P. MOHAN

Abstract Message encryption techniques stand as the cornerstone of safeguarding our communications and information in today's digital landscape. The proliferation of internet usage and network communications has spurred the advancement of these techniques. Transmitting sensitive messages across vulnerable networks opens avenues for attacks, data theft, or unauthorized access. Cryptographic methods have played a pivotal role in mitigating such risks. Among them are Caesar Cipher, Atbash Cipher, Hill Cipher, and various symmetric enciphering techniques. This article delves into an encryption method utilizing a self invertible matrix, adjacency matrix, and the complete graph of the Hamiltonian circuit to create intricate ciphertext from provided message units. What sets this method apart is its reliance on a self invertible matrix as the key, ensuring the existence of its inverse without needing explicit computation. This simplifies the process of deciphering the ciphertext, reducing computational complexity significantly.

1 Introduction

Cryptography, a mathematical technique utilized to thwart hackers from accessing communications, data, and images, is pivotal in safeguarding sensitive information [10]. The original message, termed plain textual content, undergoes transformation into encrypted text or ciphertext [10]. Although the structure of alphabets is still present in both plain text and ciphertext, they no longer always use the same set of letters. Occasionally, strange characters, numbers, punctuation, and other symbols are added to communications in order to increase security and decrease susceptibility to theft or hacking. In order to efficiently encode message units, this work uses an encoded table. Concepts from graph theory have several applications in mathematics, es-

A	B	C	D	E	F	G	H	I	J	···	W	X	Y	Z		?	!
1	2	3	4	5	6	7	8	9	10	···	23	24	25	26	27	28	29

Table 1. Encoded Table for encoding the message units

pecially in cryptography [12]. Graph theory is widely used in cryptography [12]; many different methods rely on it. A lower triangular matrix served as the key for an encryption scheme using an exhaustive graph and the Hamiltonian route in [14]. In a manner similar to this, symmetric encryption methods disclosed in [12, 13] employed the uppermost triangular matrix as the key, utilising the complete graph and its corresponding MST (Minimum Spanning Tree). Reference [2] proposed an additional creative approach to encoding and decoding messages that uses graph labelling and the uppermost triangular matrix as the encryption key.[9] explained the connection between graph theory and cryptography, using an upper triangular matrix as the key.
Every one of the previously covered symmetric encryption methods, included the sender and the recipient exchanging a shared key—typically made up of triangular matrices of lower and upper —over a variety of communication routes. For cryptographic techniques to remain secure, this

key must be kept secret [9]; if intermediaries figure out the plan, breaking gets easier. There are many obstacles when sharing a shared key matrix via an unreliable link. We provide a novel approach that uses the corresponding adjacency matrix of a given graph and a self invertible matrix as the encryption and decryption keys, in order to overcome this and improve security.

This work proposes a technique for encrypting and decrypting plain text message units that combines a basic idea from graph theory with a self-invertible matrix [1, 5, 6, 7, 8] as the key matrix. This tactic aims to improve security while presenting a fresh and effective method. Decryption can be completed without computing the inverse of the key matrix when a self-invertible key matrix is employed. In this way, the message units serve as graph vertices, and the sender can ascertain the adjacency matrix of a complete graph for a Hamiltonian circuit. Both users produce the self-invertible key matrix, which is then multiplied by this adjacency matrix. The recipient receives the output across an insecure channel. The recipient interprets the first message by following the opposite process after receiving it. The structure of the paper is as follows: Section 2 provides an overview of the fundamentals of graph theory, while Section 3 discusses the construction of self-invertible matrices. . In Section 4, the newly suggested approach is explained, and in Section 5, its implementation is demonstrated. Section 6 concludes with findings and recommendations for more research.

2 An Overview of Graph Theory

In this section, our objective is to outline fundamental graph definitions.
Undirected/Directed Graphs: In an undirected graph, the set ab will be an edge connecting nodes a and b, therefore it links nodes a and b, which is equivalent to connecting nodes b and a, which are both identical. The graphs are not in any particular order, and neither is there any direction to them. For a directed graph, it's crucial to consider the graphs' directions and order.
Path: A path without repeating vertices is called a route. A path from a to b exists for every a and b in a graph called V if the graph is connected.
Hamiltonian Path: A path through a linked graph G that visits all vertices precisely once is known as a "Hamiltonian path.
Complete Graph: When one edge connects each pair of vertices in a graph, the graph is said to be complete.
Adjacency Matrix: Adjacency matrix refers to a matrix that is mostly dependent on the vertices of a certain network. $A = a_{ij} = \begin{cases} 1, & v_i = v_j \\ 0, & v_i \neq v_j \end{cases}$

3 The generation process of self-invertible key matrices

If $J = J^{-1}$, or $J \cdot J^{-1} = J^{-1} \cdot J = I$ then such a matrix J is called as a self invertible matrix, It was crafted through the utilization of the following:

Consider any arbitrary $\frac{n}{2} \times \frac{n}{2}$ matrix J_{22} (where n being selected based on the order of adjacency matrix). With J_{22} as a starting point, we can able to identify the other $\frac{n}{2} \times \frac{n}{2}$ matrices as follows,

$$J_{11} + J_{22} = 0, \implies J_{12} = I - J_{11}, J_{21} = I + J_{11}$$

After computing $J_{11}, J_{12}, J_{21}, J_{22}$ the self-invertible matrix J was created by

$$J = \begin{bmatrix} J_{11} & \vdots & J_{12} \\ \cdots & \vdots & \cdots \\ J_{21} & \vdots & J_{22} \end{bmatrix} = \begin{bmatrix} j_{11} & j_{12} & \cdots & \vdots & \cdots & \cdots & j_{1n} \\ j_{21} & j_{22} & \cdots & \vdots & \cdots & \cdots & j_{2n} \\ \cdots & \cdots & \ddots & \vdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \vdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \vdots & \ddots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \vdots & \cdots & \ddots & \cdots \\ j_{n1} & j_{n2} & \cdots & \vdots & \cdots & \cdots & j_{nn} \end{bmatrix}$$

4 The proposed cryptosystem

This section provides more details on the suggested approach, which makes use of the adjacency matrix, the complete graph of the undirected graph's Hamiltonian circuit, and the key matrix for encryption as a self-invertible matrix.

4.1 Methodology for the Suggested Encryption Approach:

The phases needed in the encryption process are as follows:
Level 1: To create a Hamiltonian circuit, join the successive letters in the given plaintext message units.
Level 2: Utilizing Table 1, convert the given message bits into the appropriate numerical values.
Level 3: Utilizing the created Hamiltonian circuit, create a complete graph.
Level 4: Prepend an additional character, such as 'A', before the first letter of the given plaintext to indicate the start of the original message.
Level 5: To find the weights of each edge, compute the numerical distance between neighboring vertices.
Level 6: Find the connected full graph's adjacency matrix.
Level 7: Create the self-invertible matrix using the given data and the steps described in Section 3.
Level 8: Encrypts the initial plaintext message by multiplying the newly created key matrix by the existing adjacency matrix. Through an unprotected channel, the end user can obtain these encrypted matrix of the plaintext message, the adjacency matrx's order, the matrix which aids to built the key matrix.

4.2 Methodology for the Suggested Decryption Approach:

The decryption process involves the following levels:
Level 1: The end user determines the sequence of matrices, the matrix that utilized to create the self invertible key matrix and the encoded matrix of the original message, after obtaining the encrypted data from the sender.
Level 2: The end user also creates the self invertible matrix by following the guidelines given in Section 3.
Level 3: The above created self-invertible matrix is multiplied with the encrypted matrix.
Level 4: After that, the receiver adds modulo 29 to the resultant matrix in order to calculate the matrix of adjacency.
Level 5: Entails the recipient reconstructing the entirety of the graph, encompassing both its nodes and weights, through retracing the graph.
Level 6: By summing the weights, the original message can be deduced. It's noted that vertex v1 corresponds to 'A', with a numerical equivalent of 1, and vertex v2 equals the value of v1 plus the weight e1, and so forth.

5 Example of implementation:

Assume that the Transmitter wishes to transmit the plaint text message "NOVEL" to the receiver using the method described in the aforementioned section and the key matrix described in Section 3.

5.1 User A (The sender):

The encrypting process involves the subsequent techniques:

At first, the sender (User A) converts the given plaintext message "NOVEL" into the vertices of a graph and forms a Hamiltonian circuit. Sequential letters of the given message are connected to create the vertices.

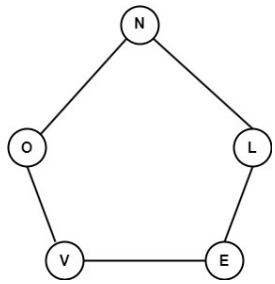

Figure 1. The Hamiltonian circuit of origina plaintext message

Using the furnished encoded table we obtain,

$$N \to 14, O \to 15, V \to 22, E \to 5, L \to 12$$

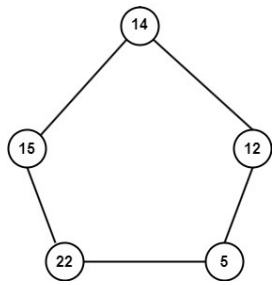

Figure 2. Encoded Hamiltonian circuit

Now to make this Hamiltonian circuit into a complete graph K_5 by connecting unpaired vertices of the Hamiltonian circuit.

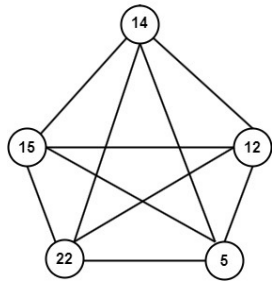

Figure 3. The Complete graph (K_5)

An additional character (typically 'A') was appended before the initial letter of the origina plaintextl message unit to indicate the starting point of the original plaintext message.

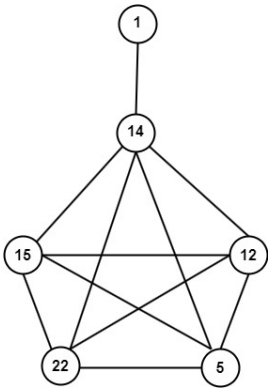

Figure 4. The Complete graph with a special character.

The numerical separation between the successive vertices is calculated, and modulo 29 is then applied to compute the weights of the graph's edges. $(e1 = \text{Code}N - \text{Code}A, e2 = \text{Code}O - \text{Code}N, \ldots)$

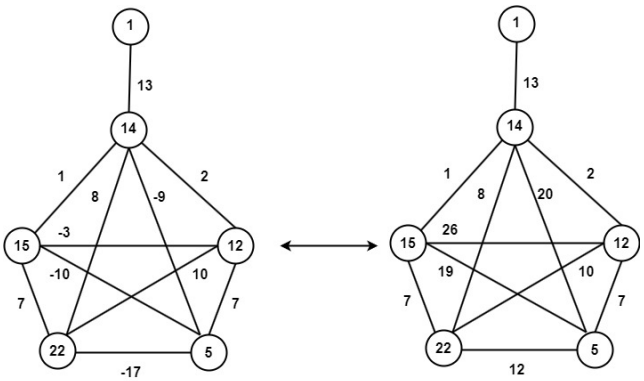

Figure 5. Complete graph K_5 with weights.

After computation, A was assigned to the adjacency matrix for the entire graph.

$$A = \begin{bmatrix} 0 & 13 & 0 & 0 & 0 & 0 \\ 13 & 0 & 1 & 8 & 20 & 2 \\ 0 & 1 & 0 & 7 & 19 & 26 \\ 0 & 8 & 7 & 0 & 12 & 10 \\ 0 & 20 & 19 & 12 & 0 & 7 \\ 0 & 2 & 26 & 10 & 7 & 0 \end{bmatrix}$$

Now, we generate the self invertible matrix $'G'$ using a $\frac{n}{2} \times \frac{n}{2}$ matrix G_{22}.

$$\text{Let } G_{22} = \begin{bmatrix} 1 & 4 & 1 \\ 9 & 9 & 6 \\ 1 & 2 & 3 \end{bmatrix} \text{ then } G_{11} = \begin{bmatrix} 28 & 25 & 28 \\ 20 & 20 & 23 \\ 28 & 27 & 26 \end{bmatrix}$$

$$G_{12} = I - G_{11} = \begin{bmatrix} 2 & 4 & 1 \\ 9 & 10 & 6 \\ 1 & 2 & 4 \end{bmatrix} \text{ and } G_{21} = I + G_{11} = \begin{bmatrix} 0 & 25 & 28 \\ 20 & 21 & 23 \\ 28 & 27 & 27 \end{bmatrix}$$

$$G = \begin{bmatrix} G_{11} & G_{12} \\ G_{21} & G_{22} \end{bmatrix} = \begin{bmatrix} 28 & 25 & 28 & 2 & 4 & 1 \\ 20 & 20 & 23 & 9 & 10 & 6 \\ 28 & 27 & 26 & 1 & 2 & 4 \\ 0 & 25 & 28 & 1 & 4 & 1 \\ 20 & 21 & 23 & 9 & 9 & 6 \\ 28 & 27 & 27 & 1 & 2 & 3 \end{bmatrix}$$

Ultimately, the encryption matrix resulted from the multiplication of matrices A and G.

$$C = A \cdot G = \begin{bmatrix} 0 & 13 & 0 & 0 & 0 & 0 \\ 13 & 0 & 1 & 8 & 20 & 2 \\ 0 & 1 & 0 & 7 & 19 & 26 \\ 0 & 8 & 7 & 0 & 12 & 10 \\ 0 & 20 & 19 & 12 & 0 & 7 \\ 0 & 2 & 26 & 10 & 7 & 0 \end{bmatrix} \cdot \begin{bmatrix} 28 & 25 & 28 & 2 & 4 & 1 \\ 20 & 20 & 23 & 9 & 10 & 6 \\ 28 & 27 & 26 & 1 & 2 & 4 \\ 0 & 25 & 28 & 1 & 4 & 1 \\ 20 & 21 & 23 & 9 & 9 & 6 \\ 28 & 27 & 27 & 1 & 2 & 3 \end{bmatrix}$$

$$C = \begin{bmatrix} 260 & 260 & 299 & 117 & 130 & 78 \\ 848 & 1026 & 1128 & 217 & 270 & 151 \\ 1128 & 1296 & 1358 & 213 & 261 & 205 \\ 876 & 871 & 912 & 197 & 222 & 178 \\ 1128 & 1402 & 1479 & 218 & 300 & 229 \\ 908 & 1139 & 1163 & 117 & 175 & 168 \end{bmatrix}$$

The encrypted matrix has the flexibility to be converted into either a row wise matrix or a column wise matrix format and transmitted to another user using various communication channels, specifying the matrix's order, the matrix which plays a crucial role in the computation of the self-invertible matrix.
[6, 260, 260, 299, 117, 130, 78, 848, 1026, 1128, 217, 270, 151, 1128, 1296, 1358, 213, 261, 205, 876, 871, 912, 197, 222, 178, 1128, 1402, 1479, 218, 300, 229, 908, 1139, 1163, 117, 175, 168; 1, 4, 1, 9, 9, 6, 1, 2, 3].

5.2 User B (The receiver):

The decryption procedure involves these steps: Upon reception, the recipient can identify the sequence of the adjacency matrix, the matrix used to create the key matrix, and the encrypted matrix.

$$C = \begin{bmatrix} 260 & 260 & 299 & 117 & 130 & 78 \\ 848 & 1026 & 1128 & 217 & 270 & 151 \\ 1128 & 1296 & 1358 & 213 & 261 & 205 \\ 876 & 871 & 912 & 197 & 222 & 178 \\ 1128 & 1402 & 1479 & 218 & 300 & 229 \\ 908 & 1139 & 1163 & 117 & 175 & 168 \end{bmatrix}$$

The self-invertible matrix is also being produced by the receiver in accordance with the method described in Section 3.

$$G = \begin{bmatrix} G_{11} & G_{12} \\ G_{21} & G_{22} \end{bmatrix} = \begin{bmatrix} 28 & 25 & 28 & 2 & 4 & 1 \\ 20 & 20 & 23 & 9 & 10 & 6 \\ 28 & 27 & 26 & 1 & 2 & 4 \\ 0 & 25 & 28 & 1 & 4 & 1 \\ 20 & 21 & 23 & 9 & 9 & 6 \\ 28 & 27 & 27 & 1 & 2 & 3 \end{bmatrix}$$

$$C \cdot G = \begin{bmatrix} 260 & 260 & 299 & 117 & 130 & 78 \\ 848 & 1026 & 1128 & 217 & 270 & 151 \\ 1128 & 1296 & 1358 & 213 & 261 & 205 \\ 876 & 871 & 912 & 197 & 222 & 178 \\ 1128 & 1402 & 1479 & 218 & 300 & 229 \\ 908 & 1139 & 1163 & 117 & 175 & 168 \end{bmatrix} \cdot \begin{bmatrix} 28 & 25 & 28 & 2 & 4 & 1 \\ 20 & 20 & 23 & 9 & 10 & 6 \\ 28 & 27 & 26 & 1 & 2 & 4 \\ 0 & 25 & 28 & 1 & 4 & 1 \\ 20 & 21 & 23 & 9 & 9 & 6 \\ 28 & 27 & 27 & 1 & 2 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 25636 & 27534 & 29406 & 4524 & 6032 & 4147 \\ 85476 & 87348 & 93033 & 14856 & 19508 & 13806 \\ 106488 & 107127 & 114202 & 18045 & 23799 & 16730 \\ 76908 & 78337 & 83701 & 12876 & 17180 & 11813 \\ 113448 & 114106 & 121471 & 19500 & 25520 & 18161 \\ 88972 & 88017 & 93696 & 15090 & 19729 & 14065 \end{bmatrix}$$

By applying addition modulo 29, the result is:
$25636(mod\ 29) = 0, 27534(mod\ 29) = 13, 29406(mod\ 29) = 0, \ldots, 14065(mod\ 29) = 0.$

$$C \cdot G = \begin{bmatrix} 0 & 13 & 0 & 0 & 0 & 0 \\ 13 & 0 & 1 & 8 & 20 & 2 \\ 0 & 1 & 0 & 7 & 19 & 26 \\ 0 & 8 & 7 & 0 & 12 & 10 \\ 0 & 20 & 19 & 12 & 0 & 7 \\ 0 & 2 & 26 & 10 & 7 & 0 \end{bmatrix} = A$$

A complete graph corresponding to the aforementioned adjacency matrix was created.

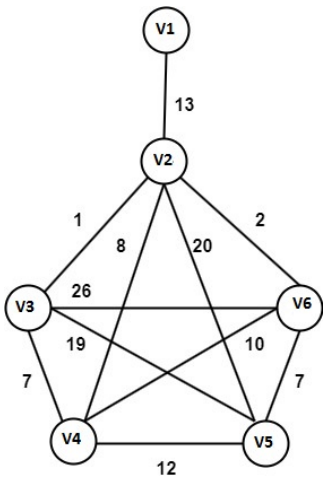

Figure 6. Complete graph K_5 of decoded adjacency.

The nodes of the aforementioned graph mentioned was created by combining the value of each vertex with its associated edge. Given that we include the character A at the start, the first vertex is fixed at 1, and the subsequent vertices follow accordingly, $v1 = 1$, so $v2 = 1 + 13 = 14, v3 = 14 + 1 = 15, v4 = 15 + 7 = 22, v5 = 22 + 12 = 34 = 5, v6 = 5 + 7 = 12, \ldots$

$\therefore$ The vertices are $14, 15, 22, 5, 12$.
$\therefore$ The original message is $14 \rightarrow N$,$15 \rightarrow O$, $22 \rightarrow V$, $5 \rightarrow E$, $12 \rightarrow L$ i.e., NOVEL.

6 Conclusion:

In today's landscape, safeguarding our information stands as a paramount concern. Various publications resort to encryption methods such as the Hill cipher and graphical techniques to address

this need. To bolster information security further, this paper introduces a novel cryptosystem encryption approach. By utilizing the principles of a Hamiltonian circuit, the adjacency matrix of a complete graph, and an even-ordered self-invertible matrix as the key matrix, this technique provides improved efficiency and resistance to intermediaries. Unlike traditional approaches, our proposed method simplifies encryption and decryption processes while fortifying security. Sharing just a $\frac{n}{2} \times \frac{n}{2}$ matrix helps in generating the key matrix, eliminating the need to calculate its inverse during decryption. This study relies solely on basic graph theory principles and encryption/decryption methods. Notably, the key matrix is specifically tailored to be of even order. Future iterations of this method aim to accommodate any ordered self-invertible matrices explore further complex graph theory concepts.

References

[1] Acharya, B., Rath, G.S., Patra, S.K., Panigrahy, S.K., *A Novel methods of generating self-invertible matrix for Hill Cipher Algorithm*, International Journal of Security(2007), pp.14-21.

[2] Amudha P, Jayapriya J, Gowri J, *An algorithmic approach for encryption using graph Labeling*, Journal of physcis,1770(1): 012072, (2021), pp. 375-384.

[3] Arumugam S, Ramachandran S, *Invitation to Graph theory*, Scitech Publications, (2015).

[4] Diffie, W., Hellman, M., *New directions in Cryptography*, IEEE Trans. Inf. Theory 22 (6), (1976), pp.644-654.

[5] Mohan. P, Rajendran. K, Rajesh. A, *An Encryption Technique using a Complete graph with a Self-invertible matrix*, Journal of Algebraic statistics, Volume 13. No 3, (2022), https://publishoa.com/index.php/journal/article/view/816, pp.1821-1826.

[6] Mohan P, Rajendran K, Rajesh A. *A Hamiltonian Path-Based Enciphering Technique with the use of a Self-Invertible Key Matrix,* Indian Journal of Science and Technology, 15(44) (2022), pp.2351-2355.

[7] Mohan P, Rajendran K, Rajesh A. *An encryption techniques using the adjacency matrices of certain graphs with a self-invertible key matrix,* E3 Web of conferences, Vol 376, 01108(2023).

[8] Mohan P, Rajendran K, Rajesh A. *Enhancing computational performance of minimal spanning tree of certain graphs based enciphering technique using self invertible key matrix*, Journal of Aeronautical Meterials, Vol.43(01) (2023), pp.359-371.

[9] Nandhini R, Maheswari V and Balaji V, *A Graph Theory Approach on Cryptography*, Journal of Computational Mathematics,2(1),(2018), pp.97-104.

[10] Neal Koblitz, *A course in Number Theory and Cryptography*, second edition, Springer.

[11] Saniah Sulaiman Zurina Mohd Hanpi, *Extensive analysis on Images Encryption using Hybrid Elliptic Curve Cryptosystem and Hill cipher*, Journal of Computer Science,17(3),(2021), pp.221-320.

[12] Uma Dixit, *Cryptography a Graph theory approach*, International journal of Advance Research in Science and Engineering,6(01),(2017), pp.218-221.

[13] Weal Mahmoud AI Etaiwi, *Encryption algorithm using Graph theory*, Journal of Scientific Research and Reports, 3(19), (2014), pp. 2519-2527.

[14] Yamuna M, Meenal Gogia, Ashish Sikka, Md. Jazib Hayat Khan, *Encryption Using Graph Theory and Linear Algebra*, International Journal of Computer Application, ISSN:2250-1797,Issue 2 Vol 5(2012), pp.102-107.

[15] Ziad E. Dawahdeh, Shahrul N. Yaakob, Rozmie Razif bin Othman, *A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher*, Journal of King Saud University - Computer and Information Sciences,30(3),(2018), pp.349-355.

Author information

P. MOHAN, Assistant Professor, Department of Mathematics, Faculty of Science and Humanities, SRMIST, Vadapalani., India.
E-mail: mohan14palani@gmail.com, mohanp2@srmist.edu.in

M.V.SURESH, Assistant Professor, Department of Mathematics, FSH, Panimalar Engineering College, Chennai, India.
E-mail: m.v.sureshpari@gmail.com

C. PERIYASAMY, Assistant Professor, Department of Mathematics, Faculty of Science and Humanities, SRMIST, Vadapalani., India.
E-mail: periyasamy.cps@gmail.com