ISSN: 0975-766X
CODEN: IJPTFI
Available Online through ***Research Article***
www.ijptonline.com

A GRAPH BASED MESSAGE ENCRYPTION ALGORITHM

Ananya, Avishek Dutta, Prabhjot Singh Sandhu, R. Thandeeswaran
School of Information Technology and Engineering. VIT University, Vellore, India.
Email: rthandeeswaran@vit.ac.in

Received on 25-10-2016 *Accepted on 02-11-2016*

Abstract: Throughout the hundreds of years, the craft of planning conventions and measures have been created to manage the issues of data security. There are various applications of Graph Theory in about every field. Its major contribution is in the field of Cryptography. The need of secure communication of messages is nothing new. It has been present since ages. Ciphers can be replaced by graphs for secret communication. The complexity of graph algorithms makes it hard for the eavesdroppers to decrypt the encrypted message. An algorithm has been proposed in this paper to decide if a graph is an Euler graph. The message will be encrypted into an Euler Graph by the proposed encryption technique. An Hamiltonian circuit will be traced out from the encrypted graph. Apart from that another algorithm has been proposed for encrypting a text message with Euler Graph and the Hamiltonian circuit as the key. The complexity and the uncertainty of the decryption and interpretation of the actual message is very high and difficult as each graph carries a single character of the message. This ensures the safety of the proposed algorithm.

Keywords: Adjacency Matrix, Cryptography, Encryption, Decryption, Euler Graph, Hamiltonian circuit.

I. Introduction

Cryptography is the ancient science of writing message in encoded form. With the increasing sense of privacy and the need of secure transportation of important message, cryptography has evolved with time. The main intention of cryptography is to hide the secret message or make it unreadable from the eavesdropper. Graphs can be utilized to display numerous sorts of relations and procedures in physical, biological, social and data frameworks. Numerous functional issues can be spoken to by Graphs.

Accentuating their application to true frameworks, the term Graph Theory is some of the time characterized to mean a diagram in which qualities (e.g. names) are connected with the nodes as well as edges. Graph theory had been variedly used for the purpose of cryptography. [1] Discusses various connections between graph theory and cryptography. In this paper we have discussed and proposed an encryption-decryption algorithm using Euler graphs.

II. Methods

We will discuss the basic properties of the graph in this section that are required to make a concrete support to our assumptions and propositions.

1. Graph

Graphs in Graph Theory are the structures to model connect objects pairwise. In computer science and mathematics, a ”graph” is built up of “nodes” also called “vertices”.

The paths joining them are called “edges”. There are directed and undirected graphs. A directed graph means there exists a fixed direction from one node to another. Whereas an undirected graph means there is no directed edge between nodes.

2. Euler Graph

An Eulerian path or trail in Graph Theory is a path in the graph which visits all the edges exactly once. Likewise, an Eulerian cycle or circuit is an Eulerian path which loops (starts and ends) on the same vertex. In graph theory an Eulerian graph is a graph where every vertex has even degree.

3. Hamiltonian Graph

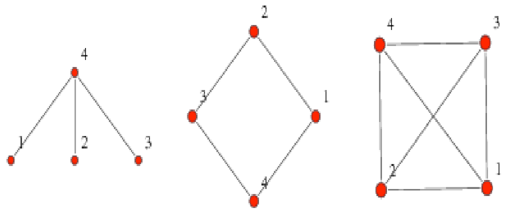
A Hamiltonian path in Graph theory is a path that visits each vertex exactly once. It is same in both directed and undirected graphs. An acyclic Hamiltonian path is called a Hamiltonian circuit.

4. Incidence Matrix

An incidence matrix or also called as adjacency matrix is way of representing the graph in a matrix format with the nodes or vertices as the rows and columns. To be more exact, for a given graph G which has n vertices, the incidence matrix is a n x n matrix.

In this matrix the non-diagonal entries a_{ij} represents the number of edges from vertex i to vertex j. aii or the diagonal entries are left as 1 or 2 based on whether the graph is directed or undirected. In undirected graphs the loops are counted twice [6]. We refer to [8] for properties of graph.

The following snapshot provides the graphs with their corresponding incidence matrix.



$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

III. Proposed Algorithm of Euler Graph

- In graph G let V denotes the number of vertices or nodes and E denotes the number of edges.
- The incidence matrix is developed based on the algorithm. It is denoted as M[p,q].
- The number of non-zero elements M[p,q]=1 are counted in each and every row.

```
If count = even then
        Graph G is Euler
Else
        Graph G is not Euler
```

IV. Proposed Encryption Technique

The message that the user wants to send, will be encrypted into an Euler Graph by the proposed encryption technique. An Hamiltonian circuit will be traced out from the encrypted graph. This will be used as a key for decryption.

1. Each and every alphabet at-first is converted to equivalent uppercase.

2. ASCII value of each uppercase alphabets are taken.

3. The decimal ASCII values are now converted into binary format.

4. After the binary format of each ASCII is achieved, they are XORed with the binary equivalent of 32.

5. The resultant XORed binary equivalent is stored in an array M[p].

6. The number of 1’s in the binary equivalent i.e. in M[i] is counted.

7. An incidence matrix or adjacency matrix A[p,q] is created with count(M[p]=1). The count represents the number of vertices.

8. A simple graph is created by making A[p,q]=0 for each A[p,q] where p=q.

9. To make the adjacency matrix symmetric, we make A[p,q]=1 as well as A[q,p]=1 for every M[p]=1 and M[i+1]!=0.

10. Count the number of 0's following the 1 for every M[p]=1 and M[p+1]=0 and put A[p,q] and A[q,p] = count(number of 0's)+1. For example, if M[p]= 10, then A[p,q]=A[q,p] = 2, if M[p….]= 1000, then A[p,q]=A[q,p] = 4.

11. The above process is repeated till the Hamiltonian circuit tracing reaches the end vertex.

12. Upon reaching the last element of M[p] =1 i.e. the binary stream ends with a 1, then make A[p,0]=A[0,q]=1.

13. If the binary stream ends with a 1 and is followed by a number of 0's i.e. the last element of M[p] !=1 that is, then put A[p,0]=A[0,q] = count(number of 0's) + 1.

14. The adjacency matrix is sent to the receiver.

V. Proposed Decryption Technique

1. The adjacency matrix is received.

2. The elements of the incidence matrix are stored in a temporary array Z[p].

3. We will traverse and take into consideration either the upper triangular matrix or the lower triangular matrix along the main diagonal. This is because of the symmetric nature of the adjacency matrix.

4. To build the binary stream, the elements of the Z[p] are expanded.

5. To get back the original message, the operations used in the encryption are applied backwards.

VI. Result

Let we sent to a message "ANANYA". With the use of encoding chart, we convert each alphabets into binary strings and XOR each alphabet with 32 bit binary string.

A = 65 = 1100001

N = 78 = 1101110

A = 65 = 1100001

N = 78 = 1101110

Y = 89 =1111001

A = 65 =1100001

Using Encryption algorithm and Euler Graph, the representation of adjacency matrix of each alphabet is shown here:

$$A = \begin{matrix} 0 & 1 & 1 \\ 1 & 0 & 5 \\ 1 & 5 & 0 \end{matrix} \qquad N = \begin{matrix} 0 & 1 & 0 & 0 & 2 \\ 1 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 2 & 0 & 0 & 1 & 0 \end{matrix}$$

$$A = \begin{matrix} 0 & 1 & 1 \\ 1 & 0 & 5 \\ 1 & 5 & 0 \end{matrix} \qquad N = \begin{matrix} 0 & 1 & 0 & 0 & 2 \\ 1 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 2 & 0 & 0 & 1 & 0 \end{matrix}$$

$$Y = \begin{matrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 3 \\ 1 & 0 & 0 & 3 & 0 \end{matrix} \qquad A = \begin{matrix} 0 & 1 & 1 \\ 1 & 0 & 5 \\ 1 & 5 & 0 \end{matrix}$$

All these matrices are send to the receiver one by one. When the receiver receives matrices, he will decode the data using these matrices.

For the first matrix, he receives [1 5 1]. For 2nd [1 2 1 1 2]. [1 5 1], [1 2 1 1 2], [1 1 1 3 1] and [1 5 1] for 3rd 4th 5th 6th respectively.

On expansion of each, he gets

151 = 1100001

12112 = 1101110

151 = 1100001

12112 = 1101110

11131 = 1111001

Using encoding technique in reverse order

1100001 gives “A”

1101110 gives “N”

1100001 gives “A”

1101110 gives “N”

1111001 gives “Y”

1100001 gives “A”

Hence, Receiver receives the message which was originally sent by the sender.

VII. Conclusion

The field of cryptography is changing and evolving on daily basis. In this paper we proposed a technique where each character of the message to be sent is encrypted into an Euler Graph. Hamiltonian Circuit is used as key to secure the message. Thus, decryption is practically incomprehensible unless the Hamiltonian circuit and the encoding plan is known.

In the above proposed technique, the complexity and the uncertainty of the decryption and interpretation of the actual message is very high and difficult as each graph carries a single character of the message. This ensures the safety of the proposed algorithm.

VIII. References

1. Connections between graph theory and cryptography.
2. http://en.wikipedia.org/wiki/Graph_theory.
3. http://en.wikipedia.org/wiki/Eulerian_path.
4. http://en.wikipedia.org/wiki/Hamiltonian_path.
5. http://mathworld.wolfram.com/AdjacencyMatrix.html.
6. http://en.wikipedia.org/wiki/Adjacency_matrix.
7. Narsingh Deo, Graph Theory with Applications to Engineering and Computer Science, Prentice Hall, 2010.
8. N. Jeyanthi, Hena M, Mogan Kumar P C, **2013 "**Credit Based Methodology to Detect and Discriminate DDoS Attack from Flash Crowd in a Cloud Computing Environment", International Journal of Network Security & Its Applications, Vol.5, No.5, Sep. 2013, pp.129-138**.**
9. Siva Kishore.B, Siva Theja Reddy.J, N.Jeyanthi, **2013**, "Three Phase Power Management Algorithms for Green Cloud Computing ", International Journal of Applied Engineering Research Vol. 8, No.14, pp. 1725-1736.
10. N. Jeyanthi, R. Thandeeswaran, J. Vinithra, 2014, "RQA Based Approach to Detect and Prevent DDoS Attacks in VoIP Networks", Cybernetics and Information Technologies, Vol.14, No.1, pp. 11-24.
11. K. Brindha, N. Jeyanthi, "Secured Document Sharing Using Visual Cryptography in Cloud Data Storage", Cybernetics and Information Technologies, Vol.15, No.4, pp.111-123, December, 2015.

12. Jay Ghiya, Mayur Date and N. Jeyanthi, Artificial Bee Colony Based Load Balancing in Cloud Computing, International Journal of Control Theory and Applications, Vol.9, No.17, 2016, pp. 8593-8598.

13. Mahantesh Gawannavar, Payal Mandulkar, R. Thandeeswaran, N. Jeyanthi, “Office in cloud: Approach to Authentication and Authorization”, Recent Advances in Communications and Networking Technology, Bentham sciences, Vol.4, No.1, 2015, pp.49-55.

14. N. Jeyanthi, Hena Shabeeb, R. Thandeeswaran, M A Saleem Durai, 2014, “RESCUE: Three Phase Authentication to Detect and Prevent DDoS attacks in Cloud Computing Environment”, International Journal of Engineering, Transaction B: Applications, Vol.27, No.8,August, pp.1137-1146.

15. Amrutha, R. Thandeeswaran, N. Jeyanthi, 2014, “Cloud based VoIP Application in Aircraft Data Networks”, International Journal of Grid Distribution Computing, Vol.7, No.6 (2014) December, pp.11- 18.