An Approach of Graph Theory for Solving Cryptographic Problem

Srilekha Chowdhury[1], Promita Ghosh[2] , Mayurakshi Jana[3]
Department of Computer Science
Bijoy Krishna Girls' College, Howrah
5/3, Mahatma Gandhi Rd, Howrah, West Bengal 711101, India
srilekhachowdhury199@gmail.com[1] ; ghoshpromita16@gmail.com[2] ; mayurakshi.jana@rediffmail.com[3]

***Abstract*: Graph theory is rapidly moving into the main stream of research because of its applications in diverse fields such as coding theory, communication networks etc. In particular researchers are exploring the concepts of graph theory that can be used in different areas of Cryptography. Various paper based on graph theory applications have been studied and we explore the usage of Graph theory in Cryptography has been proposed here.**

***Keywords*: Graph, Simple graph, Adjacency Matrix, Incidence Matrix, Euler graph. Hamiltonian graph, Encryption, Decryption, Plain text, Cipher text, Cryptography.**

I. INTRODUCTION

Cryptography is the science of secret writing with the goal of hiding the meaning of a message. It has long been the art of spies and soldiers. Nowadays, it is used everyday by billions of people for securing electronic mail and payment transactions. The science of cryptography touches on many other disciplines, both within mathematics and computer science and in engineering. In mathematics, cryptology uses, and touches on, algebra, number theory, graph and lattice theory, algebraic geometry and probability and statistics. Analysis of cryptographic security leads to using theoretical computer science especially complexity theory. The actual implementation of crypto systems, and the hard work of carrying out security analysis for specific cryptosystems falls into engineering and practical computer science and computing. In this paper we have discussed and proposed an encryption-decryption algorithm using Euler graphs.

II. PRELIMINARIES

Graph:

Conceptually, a graph is formed by vertices and edges connecting the vertices. Formally, a graph is a pair of sets (V,E), where V is the set of vertices and E is the set of edges, formed by pairs of vertices[1].

Simple graph:

A graph in which each edge connects two different vertices and where no two edges connect the same pair of vertices is called a simple graph[1].

Adjacency matrix:

Let V = (V, E) be a graph with V = a set of vertices, E = a set of edges without including parallel edges. The adjacency matrix of G is an (NxN) symmetric binary matrix X = [xij] defined over the ring of integers such that

$$xij = 1, if\ ViVj\ \in E$$
$$0, otherwise$$

It is used to represent whether a pair of vertices in a given graph are connected or not. An adjacency matrix is used to represent a finite graph. An element in the adjacency matrix is represented by xij where i

represents the row and j represents the column in the adjacency matrix whose intersection is the element x_{ij} [1].

Incidence matrix:

Let G be a graph with N vertices, M edges and without self-loops. The incidence matrix A of G is an (NxM) matrix A = $[a_{ij}]$ whose N rows correspond to the N vertices and the M columns correspond to M edges such that

a_{ij} = 1, if jth edge M_j is incident on ith vertex
0, otherwise[1].$aij = 1,$ if jth edge Mj is incident on ith vertex
$= 0,$ otherwise[1].

Euler graph:

An Eulerian cycle, Eulerian circuit or Euler tour in an undirected graph is a cycle that uses each edge exactly once. If such a cycle exists, the graph is called Eulerian or unicursal. The term"Eulerian graph" is also sometimes used in a weaker sense to denote a graph where every vertex has even degree.

Hamiltonian Graph:

A Hamiltonian path or traceable path is a path that visits each vertex of the graph exactly once. A graph that contains a Hamiltonian path is called a traceable graph. A graph is Hamiltonian-connected if for every pair of vertices there is a Hamiltonian path between the two vertices [1].

Encryption:

The process of converting information or data into a code, especially to prevent unauthorized access [9].

Decryption:

The process of converting information or data into a code, especially to prevent unauthorized access [9].

Plain text:

It is the message or information that the sender wishes to send to the receiver [9].

Cipher text:

It is the encrypted or encoded message that contains the plain text in an unreadable format [9].

XOR:

In computer science, the simple XOR cipher is a type of additive cipher, an encryption algorithm that operates according to the following principles:

1. A XOR 0 = A,
2. A XOR A = 0,
3. (A XOR B) XOR C = A XOR (B XOR C),
4. (B XOR A) XOR A = B XOR 0 = B

This operation is sometimes called modulus 2 addition (or subtraction, which is identical). With this logic, a string of text can be encrypted by applying the bit wise XOR operator to every character using a given key. To decrypt the output, merely reapplying the XOR function with the key will remove the cipher[9].

III. PROCEDURE TO CHECK EULER GRAPH

For a graph G(V,E) , form the incidence matrix M. Then count the number of non zero elements that is 1,s in each and every row. If the count is even then the graph G is Euler otherwise G is not Euler[1].

IV. PROPOSED ENCODING SYSTEMS

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. Convert each and every alphabet into its equivalent uppercase.
2. Take ASCII value of each uppercase alphabets.

3. Convert the ASCII values into binary format.
4. After the binary format of each ASCII is achieved, they are XOR ed with the binary equivalent of 32.
5. Store the resultant XOR ed binary equivalent in an array M[i].
6. Count k= the number of 1,s in the binary equivalent from the array M[i].
7. Form an adjacency matrix A = (a_{ij}) with the count k, where a_{ij} denotes the element in the ith row and jth column of the matrix. The count represents the number of vertices of the simple graph . So the principal diagonal elements of the matrix are 0. This adjacency matrix is symmetric,
so $a_{ij} = a_{ij}$.
8. Now count the number of 0,s following the 1 for every element in the array and put aij = aj i = number of 0,s + 1. For example if 10 is in the array the a_j i = 2, if 1000 is in the array then a_j i = 4.
9. The above process is repeated till the Hamiltonian circuit tracing reaches the end vertex.
10. Upon reaching the last element of the array as 1 that is the binary stream ends with a 1, then make a_{1j} = 1 where j = k.
11. If the binary stream ends with a 1 and is followed by L number of 0,s , then put a_{1k} = L + 1.
12. The adjacency matrix is sent to the receiver[1] [2]3][4].

V. PROPOSED DECODING TECHNIQUE

1. The adjacency matrix is received.
2. The elements of the adjacency 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 alo
ng the maindiagonal. 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 Encoding system are applied backwards[5] [6] [8].

VI. RESULT

Let our plain text be GRAPH. Convert each alphabet in the plain text into binary strings. Then XOR each alphabet with 32 bit binary string. We get the following

Alphabet	ASCII Code	Binary Number	XORed
G	71	1000111	1100111
R	82	1010010	1110010
A	65	1000001	1100001
P	80	1010000	1110000
H	72	1001000	1101000

Using encryption algorithm and Euler graph, the adjacency matrix of each alphabet is constructed and shown below:

For the alphabet G, there are five 1, s , therefore the graph for the alphabet G has 5 vertices and hence its adjacency matrix is of 5*5 order which is given below.

$$G = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 3 & 0 & 0 \\ 1 & 3 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Similarly for the other alphabets, we get

$$R = \begin{pmatrix} 0 & 1 & 0 & 2 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 3 \\ 2 & 0 & 3 & 0 \end{pmatrix}, A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 5 \\ 1 & 5 & 0 \end{pmatrix}, P = \begin{pmatrix} 1 & 0 & 5 \\ 1 & 0 & 1 \\ 5 & 1 & 0 \end{pmatrix}, H = \begin{pmatrix} 0 & 1 & 4 \\ 1 & 0 & 2 \\ 4 & 2 & 0 \end{pmatrix}$$

All these matrices are sent to the receiver one by one.

For the first matrix the receiver receives [1 3 1 1 1]

For the second matrix the receiver receives [1 1 3 2]

For the 3rd matrix the he receives [1 5 1]

For the 4th matrix the he receives [1 1 5]

For the 5th matrix the he receives [1 2 4] .

By expanding these matrices the receiver gets

13111 = 1100111 115 = 1110000

1132 = 1110010 124 = 1101000

151 = 1100001

Using encoding technique in reverse order

1100111 gives G 1110000 gives P

1110010 gives R 1101000 gives H

1100001 gives A

Hence the receiver receives the plain text which was originally sent by the sender.

VI. CONCLUSION

The cryptography is an algorithm which provides secure communication. In this paper we proposed a technique where each character of the data will be encrypted into an Euler Graph. Hamiltonian Circuit is used as key to secure the data. Thus, decryption is practically incomprehensible unless the Hamiltonian circuit and the encoding plan is known. In this technique, the complexity and the uncertainty of the

decryption and interpretation of the actual message is very high and difficult as each graph represents a character of the message. This algorithm ensures the safety of the data[7].

REFERENCES

[1]. Narsingh Deo, Graph Theory with Applications to Engineering and Computer Science, Prentice Hall, 2010.

[2] 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.

[3] F.Amounas. 2015. "Enhanced Elliptic Curve Encryption Approach of Amazigh alphabet with Braille representation", International Journal of Computer Science and Network Solutions, vol 3, No 8, pp. 1-9.

[4] 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.

[5] 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.

[6] 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.

[7] Connections between graph theory and cryptography Natalia Tokareva G2C2: Graphs and Groups, Cycles and Coverings September, 2426, 2014. Novosibirsk, Russia.

[8] Rishi Pal Singh, Vandana , Application of Graph Theory in Computer Science and Engineerin International Journal of Computer Applications (0975 8887) Volume 104 No.1, October 2014.

[9] N.Koblitz, Algebraic Aspects of Cryptography, Springer-Verlag, Berlin 1998.