International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

CRYPTOGRAPHY – A GRAPH THEORY APPROACH

Uma Dixit
Assistant Professor, Department of Mathematics
University Post Graduate College, Osmania University
Secunderabad-500003 (Telangana), India.

Abstract: Transfer of data and its safety is an issue in this information world. Public key cryptography is indispensable to ensure both confidentiality and authenticity in numerous applications which comprises of securely communicating. Graph theory is now being a dominant research area along with number theory, which is primary source for cryptography. Graph theory has various applications in different fields like network security, coding theory, communication networks and their security etc. In particular, concept of graph theory is being used in areas of cryptography in various ways. In this paper, we use some methods of encryption using graphs and mathematical ideas and highlight the principles of public key cryptography
Keywords: Public key, cryptography, graphs, encryption, network security.

I. INTRODUCTION

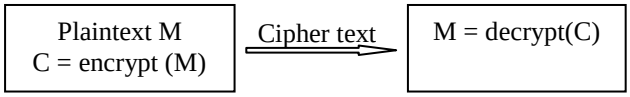
Cryptography is defined to be the way of making a message obscure and unintelligible to everyone except to a subgroup of communication parties known as legitimate users. The mindset of cryptographers was focused on developing ways to merely hide messages while in transit. The development of technology stimulated the field of cryptography to introduce new principles of security to serve the obligation of evolved technologies. This led cryptographers to expand the requirements of cryptographic protocols to not only hide messages, but also to develop a way to authenticate the source of messages and ensure that the message had not been counterfeited while in transit.

Furthermore, advances in cryptographic analysis broadened over time so that the range of their applications could be utilized by a large number of people exchanging messages. This stimulated cryptographers to find a key exchange methodology to work in conjunction with the cryptographic algorithm. The role of keys was to determine the functional output of the cryptographic algorithm; it specified the transformation of an original message to an encrypted message and vice versa. Consequently, security of cryptographic algorithms should rely on secrecy of the key.

Definition (**Kerckhoff's principle**): It states that the description of cryptographic protocols should be a public knowledge and its security must rely solely on a secret key and randomization procedures.
Kerckhoffs principle is an imperative rule in modern day cryptographic algorithms.

Encryption and Decryption: Encryption is a process in which plain text data is converted into an unintelligible or unreadable text called cipher text and decryption is the process of transforming data that has been rendered unreadable back to its normal form.

The whole idea of cryptography is:



Public vs. Private Cryptography: Current cryptographic protocols are classified into two categories; Private-key (symmetric) and public-key (asymmetric) cryptography. The classification is mainly based on the key form used in the protocol. In private-key cryptography, only one key is used to convert the message into an unintelligible form and all parties involved in the communication keep this key secret. The private key needs to be exchanged via a secured communication channel. Since both parties use the same key, there is no way to guarantee authenticity and the origin of exchanged messages. Private-key cryptography serves a variety of applications such as files and passwords protection. However, a problem of key exchange arises when many parties intend to elaborate in a communication such that none of them has met before hand or a secure communication channel does not exist. Using this protocol requires the creation of approximately n^2 keys if n parties want to securely communicate with each other.

RSA was the first practical protocol standard to solve this problem[4]. The RSA algorithm is a form of public-key cryptography and differs from private-key cryptography by using two keys; one is made public and the other is kept private to encrypt and decrypt respectively. These two parts of the key pair are always related in some mathematical sense. As for using them, the owner of such a key pair may publish their public key, but it is crucial that they keep the private key only to themselves. Here, it suffices to create n keys, generated such that each party generates and publishes a public key, which is used to encrypt messages by other parties destined to become key owners. It is also important to note that the public-key scheme guarantees authenticity and origin since a key can belong to only one party involved in the communication. For more details, we refer to the standard literature [1,2].

These days, public-key cryptography is indispensable to ensure both confidentiality and authenticity in numerous applications which comprise securely communicating via mobile phone or email or digitally signing documents. For all public-key systems, such as RSA, mathematically challenging and technically involved methods are employed.

Connections to graph theory: Modern cryptography is highly connected with discrete mathematics. Graph theory has a great contribution in the development of various encryption techniques. It is one such field which is being successfully integrated to provide stronger cryptographic algorithms. Graph theory is extensively used in encryption.

In this paper we discuss connection between cryptographic method and graph theory. In particular, we use selective encryption mechanism using message specific key and spanning tree concept of graph theory.

II. PRELIMINARIES

We require few definitions in graphical terminology:

Graph : A graph is an ordered pair G = (V, E) consisting set V of vertices or nodes together with a set E of edges or links, which are 2 – elements subset of V (that is an edge is related with two vertices, and the relation is represented as an unordered pair of the vertices with respect to the particular edge).

Order and Size of graph : The number of vertices in graph is called order and number of edges is called size of graph.

Weighted graph : Weighted graph is a graph in which each branch is given a numerical weight. A weighted graph is therefore a special type of labeled graph in which the labels are numbers.

Simple graph : A simple graph, is an unweighted, undirected graph containing no graph loops or multiple edges.

Complete graph : A simple nondirected graph with n mutually adjacent vertices is called a complete graph on n vertices.

Cycle graph : A cycle graph of order n is a connected graph whose edges form a cycle of length n.

Planar or plain graph : It is a graph that can be embedded in the plane, i.e., it can be drawn on the plane in such a way that its edges intersect only at their endpoints.

Minimal spanning tree : A spanning tree T of a graph G is a sub graph containing all the vertices of G. It is a minimal set of edges that connects all the vertices of G without creating any cycles or loops. Out of all the spanning trees of G, the minimum spanning tree is one with least weight.

One Wayness in Public Key Cryptography:

The central requirement for an operational public-key cryptographic system is a one-way function; it is the security core in the development and implementation of public-key cryptographic protocols. A one-way function is a function : $M \rightarrow C$ that is easy to compute for every given input M, however, it is computationally infeasible to reverse the computation. Thus, it is hard to reconstruct the input of the function given the output C and the function f.

For cryptographic purposes, the one-wayness must involve a trapdoor element such that it can be reversed if legitimate users obtain the trapdoor [6].

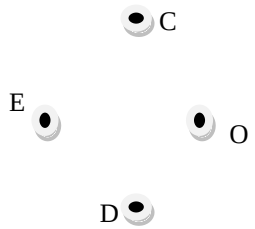
A one-way trapdoor function is constructed in such a way that it is easy to compute for any given input, but practically infeasible to construct given input from output with zero knowledge of the trapdoor (i.e., the trapdoor serves as a secret key to compute the function backward).

The remainder of this paper is a discussion of intractable problem from graph theory keeping cryptography as the base.

III. PROPOSED APPLICATION

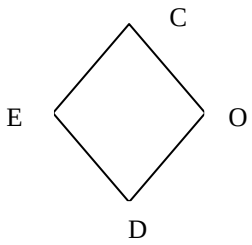
Firstly we represent the given text or data as vertices of the graph. Every vertices represent a character of the data. Now every adjacent character in the given text will be represented by adjacent vertices in the graph.

Example : We will encrypt the text or data, say C O D E, which we will be sending to the receiver on the other end. Now we change this text into graph by converting each letter to vertices of graph.



Graph 1: Conversion of letter to vertex

Then we link each two characters which are in sequence to form a Cycle Graph.



Graph 2: Cycle Graph

Further we label each edge by using the encoding table, which is followed by most researchers.

Table 1 : Encoding table

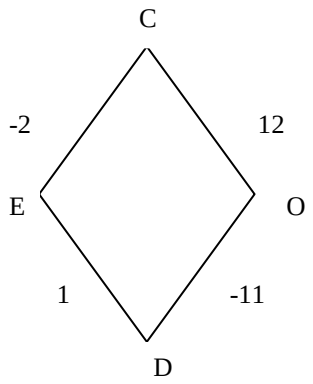
A	B	C	D	-	-	-	-	W	X	Y	Z
1	2	3	4					23	24	25	26

The label on each edge represents the distance between the connected two vertices from the encoding table. So the edge connecting vertex C with vertex O has a label which is distance between the two characters in the encoding table.

distance = code (O) – code (C)
= 15 - 4
= 12

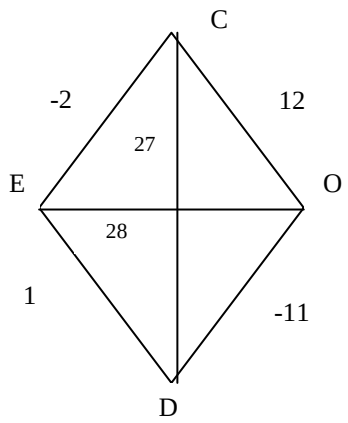
Similarly we can deduce the distances of other edges . Then we label the graph containing all the plain text letters and we get

International Journal of Advance Research in Science and Engineering
Vol. No.6, Special Issue (01), September 2017, BVCNSCS 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354



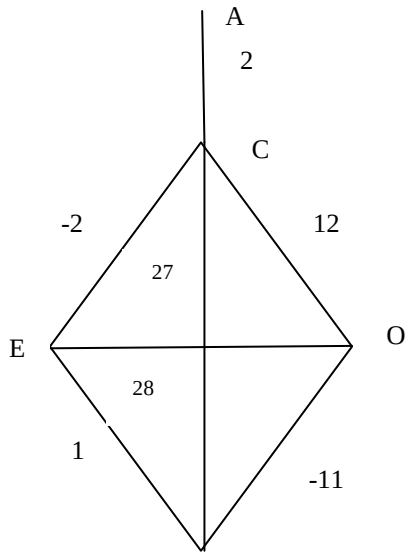
Graph 3: Weighted Graph

Such a graph is also called a weighted graph. We have now added the edges to form a complete graph and further we then give a label in sequence of our encoding table moving ahead of maximum number of the table which is 26. Therefore we can add 27, 28 and so on.



Graph 4: Complete plain Graph

Then add a special character before the first text character in the encoding table and this points to the first letter of text. Say A is special character, then we get

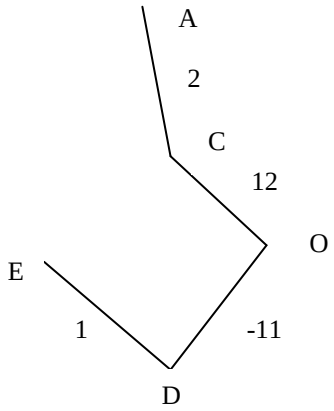


Graph 5 : Complete plain Graph with special character

Now represent the above graph in the form of a distance matrix.

$$X_1 = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 \\ 2 & 0 & 12 & 27 & -2 \\ 0 & 12 & 0 & -11 & 28 \\ 0 & 27 & -11 & 0 & 1 \\ 0 & -2 & 28 & 1 & 0 \end{bmatrix}$$

We now construct a minimal spanning tree of Graph 5 .



Graph 6: Minimal spanning tree

Then the distance matrix is

$$X_2 = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 \\ 2 & 0 & 12 & 0 & 0 \\ 0 & 12 & 0 & -11 & 0 \\ 0 & 0 & -11 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Encryption Process :

Now we store the character order in the diagonal instead of zeroes as follows:

Table 2 :

character	order
A	0
C	1
O	2
D	3
E	4

Then the modified X_2 is

$$\begin{bmatrix} 0 & 2 & 0 & 0 & 0 \\ 2 & 1 & 12 & 0 & 0 \\ 0 & 12 & 2 & -11 & 0 \\ 0 & 0 & -11 & 3 & 1 \\ 0 & 0 & 0 & 1 & 4 \end{bmatrix}$$

Now we get a matrix $X_3 = X_1X_2$

$$X_3 = \begin{bmatrix} 4 & 2 & 24 & 0 & 0 \\ 0 & 148 & -273 & -53 & 19 \\ 24 & 12 & 265 & -5 & 101 \\ 54 & -105 & 302 & 122 & 4 \\ -4 & 334 & 21 & -305 & 1 \end{bmatrix}$$

Then use a Public Key P_K to encrypt X_3.

Let $P_K = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$, so that the cipher text

$$C_t = P_KX_3 = \begin{bmatrix} 78 & 391 & 339 & -241 & 125 \\ 74 & 389 & 315 & -241 & 125 \\ 74 & 241 & 588 & -188 & 106 \\ 50 & 229 & 523 & -183 & 5 \\ -4 & 334 & 21 & -305 & 1 \end{bmatrix}$$

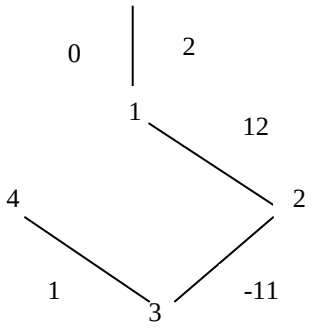
We now send the encrypted data C_t to the receiver.
78 391 339 -241 125 74 389 315 -241 125 74 241 588 -188 106 50 229 523 -183 5 -4 334 21 -305 1

Decryption Process :

On the receiver side, X_3 is got from multiplying the cipher text received with the inverse of shared Key P_k^{-1},
$X_3 = C_t P_k^{-1}$
Then calculate X_2 by multiplying X_3 by X_1^{-1}

Therefore $X_2 = X_3 X_1^{-1} = \begin{bmatrix} 0 & 2 & 0 & 0 & 0 \\ 2 & 1 & 12 & 0 & 0 \\ 0 & 12 & 2 & -11 & 0 \\ 0 & 0 & -11 & 3 & 1 \\ 0 & 0 & 0 & 1 & 4 \end{bmatrix}$

Then X_2 represents the below Graph 7, regardless of the diagonal, we use it to retrieve the original text.



Graph 7: Decrypted Graph

We suppose that the vertex 0 is A, and by using encoding table

Vertex 1 = code (A) + 2 = 3, which is character C
Vertex 2 = code (C) + 12 = 15, which is character O
Vertex 3 = code (O) - 11 = 4, which is character D
Vertex 4 = code (D) + 1 = 5, which is character E

Which gives us the original text **C O D E**

IV. REFERENCES

[1] Diffie, Whitfield, and Martin Hellman. New directions in cryptography. Information Theory, IEEE Transactions on 22, no. 6 (1976): 644-654.
[2] Bellare, Mihir, and Shafi Goldwasser. Lecture notes on cryptography. (2008).
[3] Goldreich,Oded. Foundations of cryptography.(1998): 3.
[4] Merkle, Ralph Charles. Secrecy, authentication, and public key systems. (1979).
[4] Yan, Song Y. Computational number theory and modern cryptography. John Wiley & Sons, 2012.
[5] 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; 2012
[6] Ustimenko VA. On graph-based cryptography and symbolic computations, Serdica. Journal of Computing. 2007;131-156.
[7] Paszkiewicz A, et al. Proposals of graph based ciphers, theory and implementations. Research Gate; 2001.
[8] Steve Lu, Rafail Ostrovsky. Daniel Manchala. Visual Cryptography on Graphs, CiteSeerx, COCOON. 2008;225-234.
[9] J.A. Bondy and U.S.R Murty ,"Graph Theory with Application", Macmillan Press Ltd, First Edition 1976.
[10] Narsingh Deo (2004), "Graph Theory with Applications toEngineering and Computer Science", Prentice- Hall, Inc. ISBN: 9788120301450.