Advances and Applications in Mathematical Sciences
Volume 21, Issue 2, December 2021, Pages 531-537

A CRYPTOSYSTEM BASED ON THE ECCENTRIC SEQUENCE OF GRAPHS

K. DEEPIKA[1], S. MEENAKSHI[2] and M. HAJ MEERAL[3]

[1]Research Scholar
[2]Associate Professor
Department of Mathematics
Vels Institute of Science
Technology and Advanced Studies
Pallavaram, Chennai, 600 117, India
E-mail: maths1988@gmail.com
meenakshikarthikeyan@yahoo.co.in

[3]Assistant Professor
Department of Mathematics
The Quaide Milleth College for Men
(Affiliated to University of Madras)
Chennai-600100, Tamil Nadu, India
E-mail: hajmeeralmubarak@yahoo.com

Abstract

Let G be a graph with a vertex set V and edge set E. The eccentric sequence of the graph G is the list of eccentricities of vertices of graph arranged in a non decreasing order. The eccentricity of vertex v of G denoted as $e(v)$ is the distance of farthest vertex from v. The distance between two vertices u, v denoted as $d(u, v)$ is the length of the shortest $u-v$ path. In this paper, we have designed a cryptosystem to encrypt and decrypt messages based on the eccentric sequence of graphs.

1. Motivation and Main Results

The sequences in graph theory were mainly studied as sequences carry

2020 Mathematics Subject Classification: 05CXX, 05C12, 05C85.
Keywords: Graph, Distance between two vertices, Eccentricity, Eccentric sequence, Encryption, Decryption.
Received May 17, 2021; Accepted June 7, 2021

more information of graph parameters than a single numerical value. In other words, it is comparatively easier to handle sequences than a single value. There are various types of sequences that represent a graph [1]. Some of them are degree sequence, path degree sequence, eccentric sequence, status sequence, distance degree sequence of a graph. Various studies have been carried out in these sequences and the results thus obtained have been applied in many practical real life problems. The first type of sequence to be studied was the degree sequence based on the degrees of the vertices of the graphs. Many characterizations have been studied based on this type of sequence [2]. It is easy to compute a degree sequence of any given graph based on the degree of every vertex of that particular graph. But the converse is not that easy. That is, given a particular degree sequence, finding a graph that realizes the sequence is tricky. Many researchers have worked on this line to give existence and realization theorems for graphs. The first distance based sequence to be studied was the eccentric sequence of graphs. Based on the eccentricity of every vertex of the graph, its eccentric sequence is found out and various results have been computed. The major contribution in this study were due to Lesniak, Ostrand, Behzad and Simpson. Later Nandakumar studied the eccentric sequence of directed graphs.

In this paper we have proposed a method to encrypt and decrypt messages based on the eccentric sequence of graphs.

Message encryption is a major concern in communication field. From olden days onwards various methods have been employed to safely transmit a message. Some have been effective but some have been proved ineffective. In modern days, Encryption plays a vital role in the transfer of communication for security and trade which is done through internet. Graph theory, in particular, is now used for transferring of messages. For example, planar graphs are used in data encryption. Rigid, very excellent graphs are used to encrypt binary string. Also, Degree Sequence of graphs is used in transferring message [3], [4].

2. Preliminaries

Some prerequisites are given below for better understanding of the article.

Definition 2.1. A graph G is a set of points called nodes or vertices that are linked by a set of lines called edges. Usually, a graph is denoted as $G = (V, E)$ where V is the set of vertices and E is the set of edges.

Definition 2.2. For a graph G, let $\lceil u, v$ be two vertices. The distance between these two vertices is the length of the shortest $\lceil u - v$ path.

Definition 2.3. Eccentricity of a vertex $\lceil u \in G$ is the distance of the farthest vertex from $\lceil u$.

Definition 2.4. Listing or enumerating the eccentricities of every vertex of the graph G is the eccentric sequence of G.

Definition 2.5. The process of encoding a message or an information is known as Encryption. This is usually done in Cryptography where the original information known as the plain text is converted into an alternative form known as the cipher text.

Definition 2.6. The reverse process of Encryption is known as Decryption. It is the process of converting an encrypted information into its original plain text.

Objective of this paper

The objective or scheme of this paper is to encrypt a message based on the eccentric sequence of graphs. There are various random graphs in graph theory. Such random pairs of graphs are chosen to which Cartesian products are obtained and eccentric sequence along with the eccentricities of every vertex is applied to transfer a message to its encrypted form.

Proposed Method

- The first step is to decide the number of characters to be used in encryption process. Since we have chosen English language, the number of characters used will be 27 including the blank space.

- Let us take three pairs of graphs and find the cartesian product of these graphs such that the total number of vertices comes to 27 as there are 27 characters in our proposed method. Here we have considered three pairs of path graphs. Their cartesian products are found out.

• Let us name the cartesian product graphs as G_1, G_2 and G_3. The vertices of these graphs are assigned the characters as A to Z including the blank space.

• The eccentricity of every vertex A to Z including blank space is computed. The eccentric sequence of the graphs G_1, G_2 and G_3 is subsequently determined by listing the eccentricities of the vertices.

• To encrypt a message we write the corresponding eccentricity of every character from the cartesian product graphs G_1, G_2 and G_3.

• Also the eccentric sequence of the graph corresponding to the characters is also stated along with the number of repetitions of the eccentricities for the vertices.

3. Illustration

We take three pairs of path graphs and their corresponding cartesian products as follows

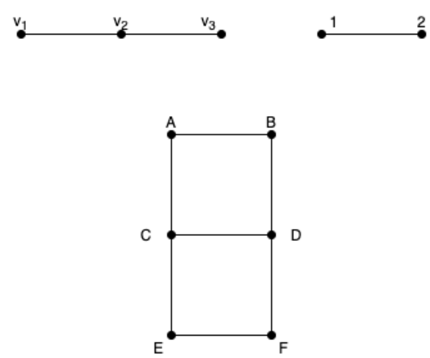

Figure (i). Graph G_1.

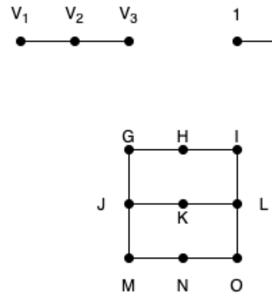

Figure (ii). Graph G_2.

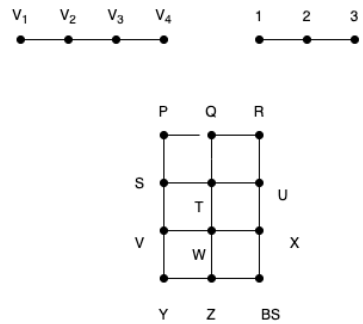

Figure (iii). Graph G_3.

We now find the eccentricities of every character (vertex). Also we compute the eccentric sequence of the cartesian product graphs G_1, G_2 and G_3.

The eccentric sequence of the graphs are $\{3, 3, 2, 2, 3, 3\}$ for G_1 $\{4, 3, 4, 3, 2, 3, 4, 3, 4\}$ for G_2 and $\{5, 4, 5, 4, 3, 4, 4, 3, 4, 5, 4, 5\}$ for G_3.

Also we note that eccentricities of some vertices are repeated. It is noted accordingly and we assign the eccentric sequence of the graphs G_1, G_2 and G_3 as 1, 2 and 3 respectively for convenience sake.

[['A' '1' '3' '1']   ['C' '1' '2' '1']

['B' '1' '3' '2']   ['D' '1' '2' '2']

['E' '1' '3' '3']   ['Q' '3' '4' '1']

['F' '1' '3' '4']   ['R' '3' '5' '2']

[‘G’ ‘2’ ‘4’ ‘1’]	[‘S’ ‘3’ ‘4’ ‘2’]
[‘H’ ‘2’ ‘3’ ‘1’]	[‘T’ ‘3’ ‘3’ ‘1’]
[‘I’ ‘2’ ‘4’ ‘2’]	[‘U’ ‘3’ ‘4’ ‘3’]
[‘J’ ‘2’ ‘3’ ‘2’]	[‘V’ ‘3’ ‘4’ ‘4’]
[‘K’ ‘2’ ‘2’ ‘1’]	[‘W’ ‘3’ ‘3’ ‘2’]
[‘L’ ‘2’ ‘3’ ‘3’]	[‘X’ ‘3’ ‘4’ ‘5’]
[‘M’ ‘2’ ‘4’ ‘3’]	[‘Y’ ‘3’ ‘5’ ‘3’]
[‘N’ ‘2’ ‘3’ ‘4’]	[‘Z’ ‘3’ ‘4’ ‘6’]
[‘O’ ‘2’ ‘4’ ‘4’]	[‘3’ ‘5’ ‘4’]]
[‘P’ ‘3’ ‘5’ ‘1’]	

From the above table, we can encrypt any message.

The first column shows the characters from A to Z including blank space. The second column shows the eccentric sequence of the corresponding graphs. The third column is the eccentricity of every character. The fourth column is the number of times the eccentricity is repeated.

Suppose we encrypt the message

“ALL IS WELL”

The generated encryption sequence for the given input string is:

[1 3 1 2 3 3 2 3 3 3 5 4 2 4 2 3 4 2 3 5 4 3 3 2 1 3 3 2 3 3 2 3 3]

The decoded string is

ALL IS WELL.

Thus the encryption and decryption is done based on the eccentricity and the eccentric sequence of graphs.

4. Conclusion

The process of encryption is safe in this proposed method as random graphs of any order can be chosen and the number of graphs chosen can also vary. Other than the encrypter and the decrypter, it will be difficult for an unauthorised person to guess these graphs. Also, the encryption is done based on the eccentric sequence of the Cartesian product of pairs of graphs which is again a challenge to make a guess. The characters that are assigned to each vertex in the graph can either be horizontal or vertical. This makes the above proposed method for a safe transmission of messages.

References

[1] P. Erdos and T. Gallai, Graphs with prescribed degrees of vertices, Matematikai Lapok (Hungarian) 11 (1960), 264-274.

[2] V. Havel, A remark on the existence of finite graphs, Casopis Pro Pestov an ı Matematiky (Czech) 80 (1955), 477-480.

[3] S. L. Hakimi, On realizability of a set of integers as degrees of the vertices of a linear graph, I, Journal of the Society for Industrial and Applied Mathematics 10 (1962), 496-506.

[4] M. Yamuna, A. Sankar, S. Ravichandran and V. Harish, Encryption of a Binary String using music notes and graph theory, International Journal of Engineering and Technology (IJET) 5 (2013), 2920-2925.