PAPER • OPEN ACCESS

Degree sequence in message transfer

View the article online for updates and enhancements.

Degree sequence in message transfer

M Yamuna

Department of Mathematics, School of Advanced Sciences, VIT University, Vellore-632014, India.

E-mail: myamuna@vit.ac.in

Abstract. Message encryption is always an issue in current communication scenario. Methods are being devised using various domains. Graphs satisfy numerous unique properties which can be used for message transfer. In this paper, I propose a message encryption method based on degree sequence of graphs.

1. Introduction
Safe transmission of message is always a problem of interest. Many methods are proposed and some of them used also. Graph theory is now in use for message transmission. In [1] the regular PCBC method is improved using music notes and graph theory. In [2] planar graphs are used in data encryption. In [3] binary string is encrypted using rigid very excellent graphs. A new parallel cryptography technique that uses DNA molecular structure, one – time – pad scheme with DNA hybridization technique which promises tominimizes the time complexity was proposed in [4]. In [5] a method of encryption using 7 bit periodic table is determined and discussed. In this paper, I propose a message encryption method based on degree sequence of graphs.

2. Preliminary note
In this section i have given some results for comfortable reading of the article.
Graph
A graph is an ordered pair G = (V, E) compromising a set V of vertices together with a set E of edges. A vertex is in general represented by a small shaded circle and an edge is a line drawn between two vertices [6].
Simple graph
A graph G with outself loops and parallel edges is called a simple graph [7]. G_1 [8] represents a simple graph and G_2 a multiple graph [9] in Snapshot – 1.
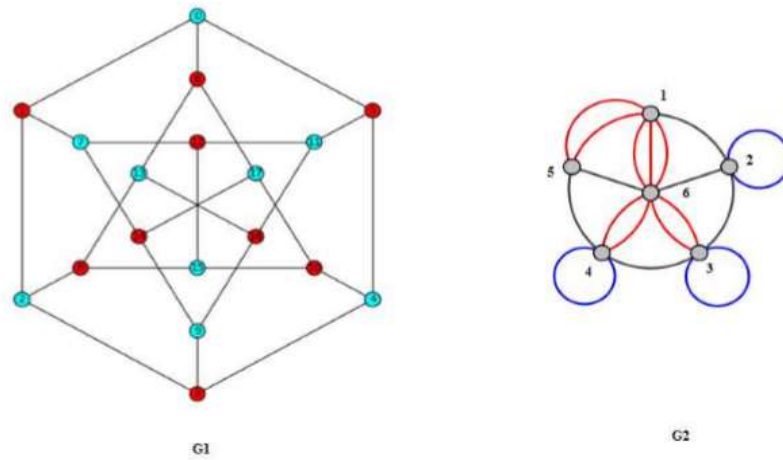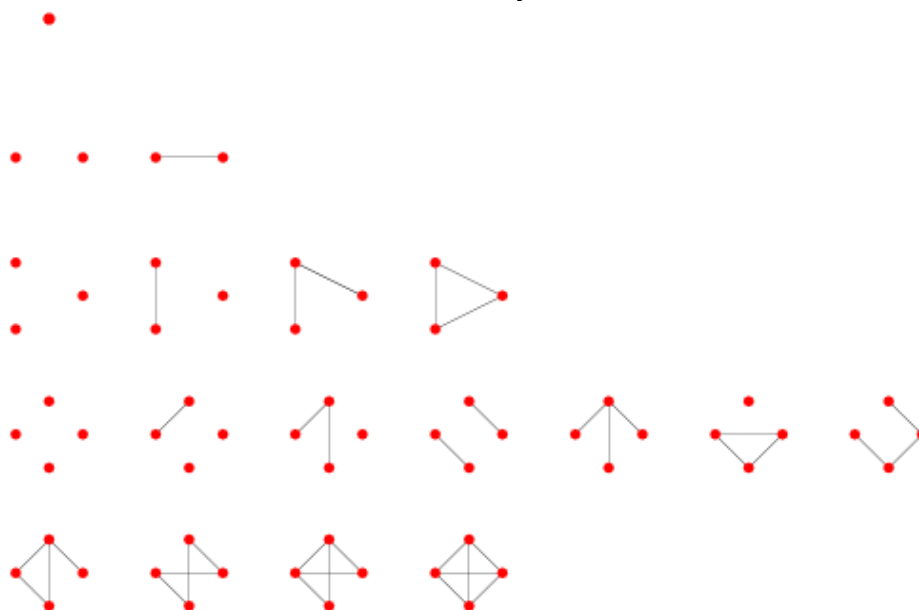
Snapshot – 1.

Degree

The number of edges incident on any vertex v, with self loops counted twice is called the degree of vertex v, denoted by deg(v). The maximum degree of a graph G is denoted by Δ (G), and the minimum degree of a graph is denoted by δ (G). The degree of all the vertices in G1 in Snapshot – 1 is 3. 6, 5, 6, 6, 4, 9 are the degree of vertices 1, 2, 3, 4, 5 in G_2 in Snapshot – 2 [10].

Materials and method

In graph theory given any integer greater than or equal to 1, there are many possible nonisomorphic graphs. Snapshot – 2 [11] gives the number of possible graphs with n = 1, 2, 3, 4 vertices. These graphs are unique and are not isomorphic. The distinct properties satisfied by these graph can be used for message transfer. In this paper I use the property that these graphs have unique degree sequence.

3. Proposed scheme

The number of characters for transferring any message is initially decided. We then choose a value of the integer which has graphs equal to atleast the number of characters. Alphabets along with blank space is used for any common message. This means that the number of characters is 27. We cannot choose the value of n = 1, 2, 3, or 4 because we have only 11

Snapshot – 2.

graphs with 4 vertices. We have 34 graphs with 5 vertices. So we can use any integer greater than or equal to 5. For our proposed method we shall choose the number of vertices n = 6. All possible graphs with n = 6 vertices is seen in Snapshot – 3 [12].

There are 156 graphs and this would be a comfortable number for any message transfer.

3.1. Degree sequence

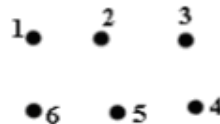Consider any random graph. For our purpose we consider graphs with six vertices. We assign labels to these six vertices uniformly as in Fig. 1.

Figure 1.

We then assign the degree sequence of the graph starting from vertex one clockwise.
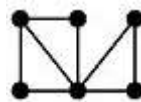
Figure 2.

For example the degree sequence of the graph seen in Fig. 1 is 000000. That is each graph
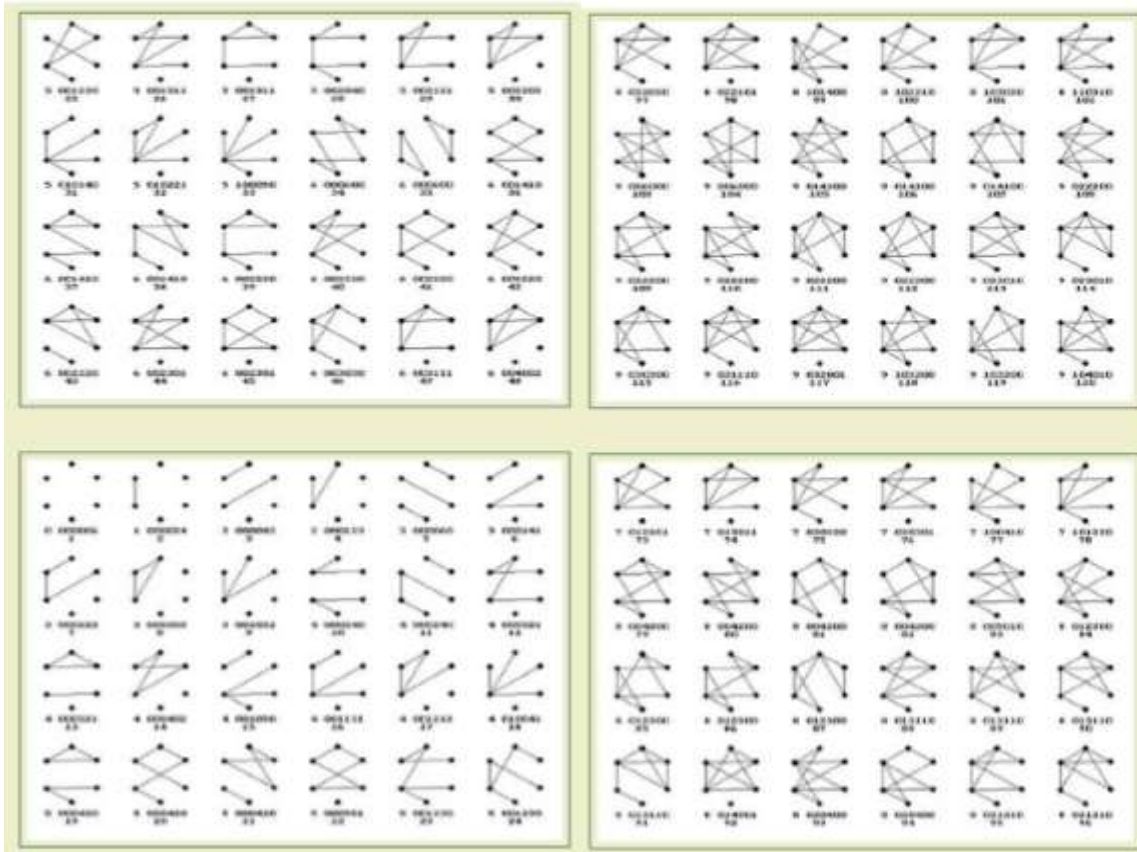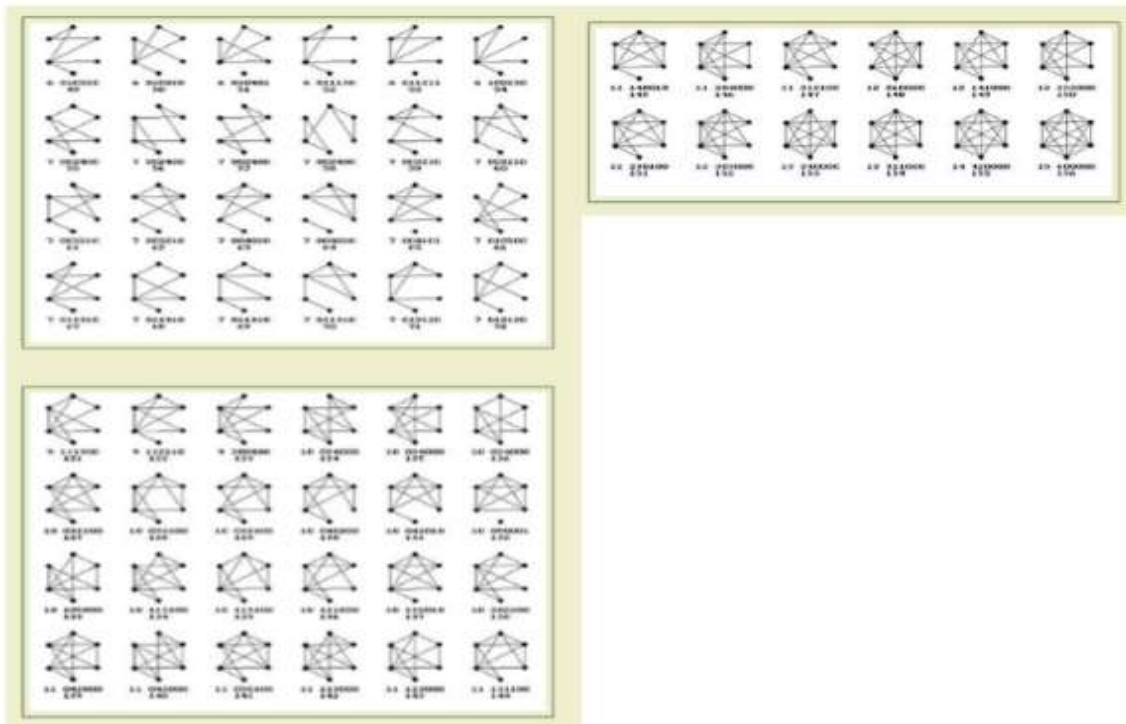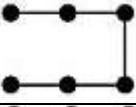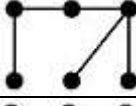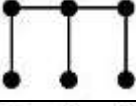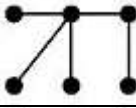
Snapshot – 3.
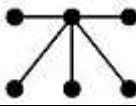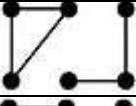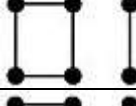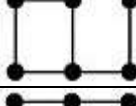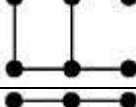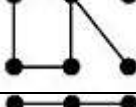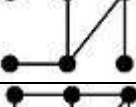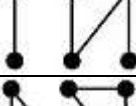
represents a degree sequence of length six. The degree sequence of the graph seen in Fig. 2 is 322252.

3.2. Construction of degree sequence graph

1. Choose an integer m which is equal to the number of characters in the message to be transferred.
2. Choose graphs with n vertices so that the possible number of graphs is atleast m with n vertices.
3. Assign any random graph to each character.
4. Finally assign the degree sequence of this graph to the characters as discussed in Section 3. 1.

Table – 1 [13] provides a sample for regular text encryption.

S. No	Graph	Degree Sequence
A		111111
B		211211
C		211111
D		311111
E		132231

F		122221
G		223111
H		222111
I		132111
J		151111
K		221211
L		221113
M		221122
N		221232
O		231132
P		241122
Q		323121
R		221213
S		133131
T		233121
U		222222
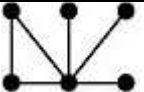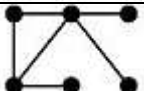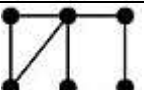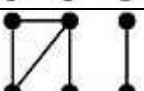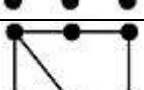
V		211152
W		241113
X		242112
Y		231123
Z		233112
Blank space		322221

Table – 1.

3.3. Encryption algorithm

Let m be the length of the message S to be encrypted.

Let the message to be encrypted be **ENCRYPTION.** In this case m = 10.

Step 1 Choose an integer n so that the possible number of graphs is atleast m with n vertices.

Step 2 Construct a degree sequence table as explained in Section 3. 2.

Step 3 Obtain a degree sequence S1 by converting each character into its corresponding degree sequence using Table – 1.

For our example S1 is

E   NC   R   Y   P   T   I   O   N
132231221232211111221213231123241122233121132111 231132 221232

Step 4 Concatenate string S1 to generate a sequence M.

M for our example is **132231221232211111221213231123241122233121132111231132221232**

Step 5 Send M to the receiver.

We can decrypt any message by reversing the procedure.

Suppose the received message is

311111132231110000101011111110110011011011010001101010111010

Divide the string into segments of length k = 6 to generate

311111132231110000 101011111110110011011011010001101010111010

Using Table – 1 the message received is **DECRYPTION**.

4. Conclusion

Graph degree sequence is used for message transfer. The proposed method is safe as

- It is tough to guess that degree sequence is used.
- There are 156 graphs possible with 6 vertices. So, there are $156C_6$ ways of choosing graphs which is a huge number. This means that even a guess of the sequence as degree sequence will still be tough to decrypt
- As the size of n increases the possibility of decryption is almost impossible.

So this proposed method can be used for safe transfer of any message.

References

[1]   Yamuna M et al 2013 *International Journal of Engineering and Technology***5** 2920 – 25.
[2]   Yamuna M and Elakkiya A 2015 International Journal of Advance Research in Science and Engineering **3** 1600 – 06 .
[3]   Yamuna M 2014 The International Journal of Computer Science and Applications **2** 11 – 15.
[4]   Sabari Pramanik and Sanjit Kumar Setua20 – 22 December 2012*7th International Conference on Electrical and Computer Engineering*, Dhaka, Bangladesh.
[5]   Venkata Krishna Pavan Kalubandhi and Yamuna M 2014 *Internationl Journal of Pharma Tech Research* **6** 990 – 995.
[6]   http://en.wikipedia.org/wiki/Graph_theory.
[7]   http://mathworld.wolfram.com/SimpleGraph.html.
[8]   http://www.sagemath.org/doc/reference/graphs/sage/graphs/graph.html.
[9]   http://en.wikipedia.org/wiki/Glossary_of_graph_theory.
[10]   http://en.wikipedia.org/wiki/Degree_%28graph_theory%29.
[11]   http://mathworld.wolfram.com/SimpleGraph.html.
[12]   file:///D:/New%20Folder/GKC's%20Favourite%20The%20156%20Graphs%20with%20 Six%20Vertices.html.
[13]   http://wiki.smp.uq.edu.au/G-designs/index.php/Graphs_with_six_vertices.