International Journal of Mathematical Archive-13(8), 2022, 8-12
Available online through www.ijma.info ISSN 2229 – 5046

SECURITY USING K_6 GRAPH

UMA DIXIT*

**Department of Mathematics,
Osmania University, Hyderabad-500007, Telangana, India.**

(Received On: 28-07-22; Revised & Accepted On: 28-08-22)

ABSTRACT

Along with number theory, which is the fundamental source for cryptography, graph theory is currently a dominant academic subject. Graph theory has numerous applications in domains such as network security, coding theory, and the security of communication networks. In this paper, we use techniques of mathematical ideas and concepts of graphs and look at the principles of encryption and decryption. We have used MATLAB for calculations.

Keywords: *Complete Graph; Encryption; Decryption; Cryptography; Hamiltonian cycle.*

AMS Mathematics Subject Classification (2020):*68R10, 15A09.*

1. INTRODUCTION

In this digital age, data transfer and security are concerns. Cryptography is required to provide confidentiality and authenticity in a variety of applications, including securely communicating. The method of hiding and rendering a message unreadable to all but a select group of communication partners known as legitimate users is described as cryptography. Historically, details of the idea of securing messages are given in [4].

As technology progressed, the area of cryptography had to develop unique security ideas to suit the demands of changing technologies. As a result, cryptographers increased the criterion for cryptographic protocols to include not only hiding messages but also authenticating their source and ensuring that they were not counterfeited in transit. This prompted cryptographers to develop a key exchange protocol that would function in tandem with the cryptographic algorithm [1]. Diffie and Martin [2, 3], discussed how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems. The cryptographic algorithm's functional output was determined by keys, which described how an original message was changed into an encrypted message and vice versa. As a result, the secrecy of the key should ensure that cryptographic techniques are secure.

Discrete mathematics and modern encryption are inextricably linked. The development of various encryption schemes has been greatly aided by graph theory [5]. It is an example of a field that has been successfully merged in order to produce more powerful cryptography algorithms. Encryption makes heavy use of graph theory. The various researchers in different directions have given new methods of securing data using graph theory [6, 7, 8].

The relationship between cryptographic methods and graph theory is discussed in this work. We employ a selective encryption approach with a message-specific key using the complete graph K_6.

2. PRELIMINARIES

We require the following definitions for our discussion.

2.1 Definition A graph $G = (V, E)$ consists V, a non empty set of vertices and E, a set of edges.

2.2 Definition 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. Graphs that may have multiple edges connecting the same vertices are called multi graphs. Edges that connect a vertex to itself are called loops.

***Corresponding Author: Uma Dixit*,
Department of Mathematics, Osmania University, Hyderabad-500007, Telangana, India.***

2.3 Definition A directed graph (or digraph) consists of a nonempty set of vertices V and a set of directed edge E. Each directed edge is associated with an ordered pair of vertices. The directed edge associated with the ordered pair(u, v)is said to start at u and end at v .

2.4 Definition Two vertices u and v in an undirected graph G are called adjacent(or neighbors)in G if u and v are endpoints of an edge of G .

2.5 Definition The complete graph on n vertices, denoted by k_n is the simple graph that contains exactly one edge between each pair of distinct vertices.

2.6 Definition A Hamiltonian cycle (also called *Hamiltonian circuit*, *vertex tour* or *graph cycle*) is a cycle that visits each vertex exactly once (except for the starting vertex, which is visited once at the start and once again at the end).

The remaining part of this paper is devoted to a consideration of intractable problems arising from graph theory, with cryptography as the foundation. MatLab has been used for calculations.

3. MAIN RESULTS

To begin, we use graph edges to represent the given text or data. A data character is represented by each edge. Neighboring graph edges will now represent every neighboring character in the text.

For example, we'll encrypt the data we're delivering to the receiver on the other end, say **G R A P H**. By converting each letter as a graph edge, we can now convert this text into a Hamiltonian cycle.

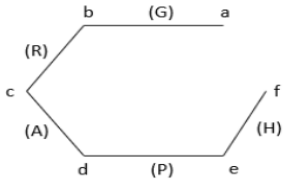

Figure-1

We also employ the encoding table which is widely utilised by most researchers, to label each edge. The labelled Graph is given in *Fig*.2

Table 1 : Encoding table

Character	A	B	C	D	-	-	-	-	-	W	X	Y	Z
Code	1	2	3	4						23	24	25	26
Character	0	1	2	3	4	5	6	7	8	9	Space	,	.
Code	27	28	29	30	31	32	33	34	35	36	37	38	39

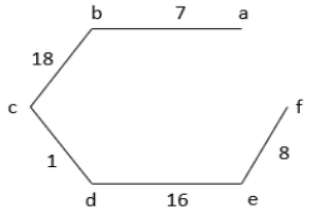

Figure-2

The adjacency matrix of the Hamiltonian cycle in *Fig*.2, denoted by M is

$$M = \begin{array}{c} \\ \boldsymbol{a} \\ \boldsymbol{b} \\ \boldsymbol{c} \\ \boldsymbol{d} \\ \boldsymbol{e} \\ \boldsymbol{f} \end{array} \begin{array}{c} \begin{array}{cccccc} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{c} & \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \end{array} \\ \begin{bmatrix} 0 & 7 & 0 & 0 & 0 & 0 \\ 7 & 0 & 18 & 0 & 0 & 0 \\ 0 & 18 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 16 & 0 \\ 0 & 0 & 0 & 16 & 0 & 8 \\ 0 & 0 & 0 & 0 & 8 & 0 \end{bmatrix} \end{array}$$

We now construct a Complete Graph K_6, and assign false labels to the remaining edges as can be seen in *Fig*. 3

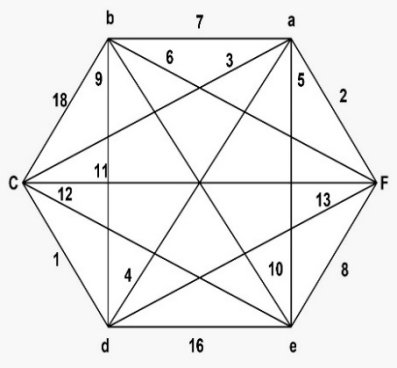

Figure-3

Let N be the adjacency matrix of the Complete graph K_6 in *Fig*.3

$$N = \begin{array}{c} \\ \boldsymbol{a} \\ \boldsymbol{b} \\ \boldsymbol{c} \\ \boldsymbol{d} \\ \boldsymbol{e} \\ \boldsymbol{f} \end{array} \begin{array}{c} \begin{array}{cccccc} \boldsymbol{a} & \boldsymbol{b} & \boldsymbol{c} & \boldsymbol{d} & \boldsymbol{e} & \boldsymbol{f} \end{array} \\ \begin{bmatrix} 0 & 7 & 3 & 4 & 5 & 2 \\ 7 & 0 & 18 & 9 & 10 & 6 \\ 3 & 18 & 0 & 1 & 12 & 11 \\ 4 & 9 & 1 & 0 & 16 & 13 \\ 5 & 10 & 12 & 16 & 0 & 8 \\ 2 & 6 & 11 & 13 & 8 & 0 \end{bmatrix} \end{array}$$

We also choose a Lower triangular Key Matrix, $X = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$

Let P = M*N, and the result using MATLAB is shown in below image.

```
P = M*N

P = 6×6

    49     0   126    63    70    42
    54   373    21    46   251   212
   130     9   325   162   196   121
    83   178   192   257    12   139
    80   192   104   104   320   208
    40    80    96   128     0    64
```

We then calculate Q = P*X and the result is posted below.

```
Q = P*X

Q = 6×6

   350   301   301   175   112    42
   957   903   530   509   463   212
   943   813   804   479   317   121
   861   778   600   408   151   139
  1008   928   736   632   528   208
   408   368   288   192    64    64
```

The encrypted data is being sent to the recipient as row-wise in the following way.

350 301 301 175 112 42 957 903 530 509 463 212 943 813 804 479 317 121 861 778 600 408 151 139 861 778 600 408 151 139 1008 928 736 632 528 208 408 368 288 192 64 64 0 7 3 4 5 2 7 0 18 9 10 6 3 18 0 1 12 11 4 9 1 0 16 13 5 10 12 16 0 8 2 6 11 13 8 0

Decryption Process:

The matrix Q and N are received. We now calculate $Z = X^{-1}$

```
Z = inv(X)

Z = 6×6

     1     0     0     0     0     0
    -1     1     0     0     0     0
     0    -1     1     0     0     0
     0     0    -1     1     0     0
     0     0     0    -1     1     0
     0     0     0     0    -1     1
```

and then find Q*Z , which will yield (P*X) * X^{-1} = P (= Y)

The calculation of Q*Z is posted below and it is easily seen that we get Q*Z = Y

```
Y = Q*Z

Y = 6×6

    49     0   126    63    78    42
    54   373    21    46   251   212
   130     9   325   162   196   121
    83   178   192   257    12   139
    80   192   184   184   328   208
    40    80    96   128     0    64
```

From the data N received we calculate $S = N^{-1}$ and when we multiply P * S, it must yield P * S = (M * N)* N^{-1} = M

```
S = inv(N)

S = 6×6

   -0.9753   -0.0013    0.3568   -0.1250   -0.0426    0.3261
   -0.0013    0.0156    0.1101   -0.0913   -0.0144   -0.0012
    0.3568    0.1101   -0.0463   -0.0605   -0.0099   -0.1703
   -0.1250   -0.0913   -0.0605    0.0812    0.0509    0.1206
   -0.0426   -0.0144   -0.0099    0.0509   -0.0477    0.0826
    0.3261   -0.0012   -0.1703    0.1206    0.0826   -0.1880

M = P*S

M = 6×6

    0.0000    7.0000   -0.0000    0.0000    0.0000   -0.0000
    7.0000   -0.0000   18.0000    0.0000    0.0000    0.0000
    0.0000   18.0000   -0.0000    1.0000    0.0000   -0.0000
    0.0000    0.0000    1.0000    0.0000   16.0000   -0.0000
    0.0000   -0.0000    0.0000   16.0000    0.0000    8.0000
    0.0000    0.0000    0.0000    0.0000    8.0000    0.0000
```

After decryption process, we have got M, where

$$M = \begin{bmatrix} 0 & 7 & 0 & 0 & 0 & 0 \\ 7 & 0 & 18 & 0 & 0 & 0 \\ 0 & 18 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 16 & 0 \\ 0 & 0 & 0 & 16 & 0 & 8 \\ 0 & 0 & 0 & 0 & 8 & 0 \end{bmatrix}$$

and from which we can get a Hamiltonian cycle.

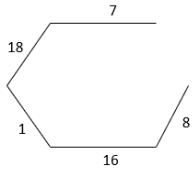

Figure-4: Decrypted Graph

which gives us the data 7, 18, 1, 16, 8 after which we use Encoding Table 1 and get 7 = G, 18 = R, 1 = A, 16 = P, 8 = H. and therefore decrypted data is **G R A P H**.

4. CONCLUSION

we have adapted a graph theory approach in which Hamiltonian cycle was used first and then converted it to Complete graph and using adjacency matrix the data is made more secure and not easy for interrupting data in transit. In this way we could make more secure data during transmission. Though there is a matrix key used, unless the graph is known in the end, the data cannot be decrypted, making it more secure way of transmitting the text.

REFERENCES

1. A. V. Aho, J. E. Hopcroft, and J. D. Ullman, The Design and Analysis of Computer Algorithms. Reading, MA.: AddisonWesley, 1974.
2. Diffie, Whitfield, and Martin Hellman. New directions in cryptography. Information Theory, IEEE Transactions on 22, no. 6 (1976): 644-654.
3. W. Diffie and M. E. Hellman, "Multiuser cryptographic techniques," presented at National Computer Conference, New York, June 7-10, 1976.
4. D. Kahn, The Codebreakers, The Story of Secret Writing. New York: Macmillan, 1967.
5. Narsingh Deo (2004), "Graph Theory with Applications to Engineering and Computer Science", Prentice-Hall, Inc. ISBN: 9788120301450.
6. S. G. Shirinivas, S. Vetrivel, Dr. N.M.Elango," Applications of Graph Theory in Computer Science :An Overview", International Journal of Engineering Science and Technology, Vol. 2(9), pp. 4610-4621, 2010.
7. Srilekha C, Promita G, Mayurakshi J, An Approach of Graph Theory for Solving Cryptographic Problem, BKGC SCHOLARS, Vol. 1 Issue. 2, PP. 64 – 68; 2020
8. Wijesiri and perera, Encryption and Decryption Algorithms in symmetric key cryptography using graph theory, Psychology(Savannah, Ga.) 58(1):3420-3427;2021

Source of support: Nil, Conflict of interest: None Declared.