IOP Conf. Series: Materials Science and Engineering **263** (2017) 042120 doi:10.1088/1757-899X/263/4/042120

Data transfer using complete bipartite graph

V M Chandrasekaran[1], B Praba[2], A Manimaran[1] and G Kailash[3]
[1]Department of Mathematics, School of Advanced Sciences, VIT University, Vellore-632014, India
[2]SSN College of Engineering, Kalavakkam, Chennai - 603110
[3]School of Computer Science and Engineering, VIT University, Vellore-632014, India

E-mail: marans2011@gmail.com

Abstract. Information exchange extent is an estimation of the amount of information sent between two focuses on a framework in a given time period. It is an extremely significant perception in present world. There are many ways of message passing in the present situations. Some of them are through encryption, decryption, by using complete bipartite graph. In this paper, we recommend a method for communication using messages through encryption of a complete bipartite graph.

1. Introduction

Encryption is a procedure of transforming the data in such a method that only the accessed persons can read it. Decryption is the method of altering encrypted information so that it is comprehensible again. A cryptographic algorithm is a mathematical function used for encryption or decryption additionally called as cipher, in most extreme cases, two interrelated functions are enlisted, one for encoding and the other for decoding.

By means of recent cryptography, the capability to keep encrypted data secret is not only grounded on cryptographic algorithm, but on numeral called key, which must be used to provide encrypted result or to decrypt formerly encrypted result. Decryption through the correct key is modest, whereas decryption without the correct key is intolerable for all real-world purposes.

Graph theory is widely used for Encryption Algorithms. Communication is one of the basic necessities in today's world. Due to the rapid development of network and multimedia technologies, security of the messages communicated has a very key importance and require a secure framework for transfer purpose. Guo et al.[1] introduced the expansion of pixel in visual cryptograph scheme in 2017. Rathore and Jain [2] introduced a new visual cryptography using mosaic and spread spectrum water marking in 2017. Also in the same year, Yang et al.[3] described the concept of enhanced password processing scheme based on visual cryptography. One of the greatest challenges posing in today's techniques is the static cryptographic code, as mentioned by authors Manimaran et al. [6] in 2015. Also in the same year the authors Manish et al. [7] mentioned that in encryption structure, the note or data (referred to as plaintext) is encrypted by means of an encryption algorithm, spinning it into an unreadable cipher text. Encryption is the most active way to attain data security. This procedure accomplishes a powerful part sequestered from everything the substance of the message, in light of the fact that the first data must be recuperated through the portrayal procedure [8]. There are several ways to transfer the data in secure and reliable mode, one such way to secure the information in communication is using cryptography. Cryptography refers to the science of transfiguring messages to

make them secure and invulnerable to hacking or outbreaks. In 1999, Zimmerman [12] described about cryptography in detail. The authors Chandrasekaran et al. [5], discussed about cryptography concept using pair of dice in 2015. They considered sample space of two dice and converted binary to decimal and vice versa for giving the concepts in detail. The authors Yamuna et al. [11] provided the data transfer using bipartite graph in 2015.

In 2014, Vikas Agrawal et al. [10] provided how the process of encryption and decryption in case of symmetric key and public key cryptography using AES and DES algorithms and modified RSA algorithm for secure communication. Obaida [9] proposed a new approach for complex encrypting and decrypting of the data in 2013.

2. Preliminaries

Definition 2.1 [4]

A graph G = (V, E) consists of a set of objects $V = \{v_1, v_2, ...\}$ called vertices and $E = \{e_1, e_2, ...\}$ whose elements are called edges such that each edge e_k is identified with an unordered pair of vertices (v_i, v_j).

Definition 2.2 [4]

An edge to be related with a pair of vertices (v_i, v_i). It means that an edge containing the similar vertex as both its end vertices is termed as a self-loop.

Definition 2.3 [4]

In graph concept, multiple edges (similarly termed parallel edges), are two or additional edges that are incident to the similar two vertices.

Definition 2.4 [4]

A graph that has neither self-loop nor parallel edges is called simple graph.

Definition 2.5 [4]

A simple graph *G* is said to be complete if every pair of distinct vertices of *G* are adjacent.

Definition 2.6 [4]

A graph in which all vertices are of equal degree is called a regular graph.

Definition 2.7 [4]

A graph is bipartite if its vertex set can be partitioned into two nonempty subsets *X* and *Y* such that each edge of *G* has one end in *X* and the other in *Y*.

Definition 2.8 [4]

A simple bipartite graph $G(X, Y)$ is complete if each vertex of *X* is adjacent to all the vertices of *Y*.

3. Encryption and decryption algorithms

3.1. Encryption

Step1: First reflect the note to remain encrypted.

Step2: Translate each and every element into α, into its equivalent number value by means of table to produce β; such that the note encrypted should be in the form of a complete bipartite graph.

Step3: Construct the graph corresponding to the sequence β to generate a graph G. Also, for β, we obtain the vertex set, edge set and edge weights.

Step4: Send G in the direction of the receiver.

3.2. Decryption

Intended for decrypting we reverse the procedure

STEP5: When encrypted message is arranged as vertices according to their weights.

STEP6: Then generate a sequence for the vertices for decryption.

STEP7: According to that, picking the corresponding vertex labels we generate the sequence in ascending order.

4. Outcomes and deliberations

In this paper, we anticipated the encryption arrangement for transmission of the data through the complete bipartite graph.

4.1. Structure of Encryption Table

Initially, we choose the quantity of characters (*H*) mandatory for encrypting the message. In table, we can fix the number of rows and columns arbitrarily by taking attention that the number of compartments accessible inside the table is at least of the dimension of *H*. We just allocate the column numbers from $1,\ 2,\ldots.\ k$ and for rows $k+1,\ k+2,\ \ldots\ m$, where *k* = number of columns, *m* = number of rows. Suppose we are taking the numbers up to 6 for the columns and number up to 13 for rows which generally resembles the dice.

For a normal message the table consists of 26 characters with a blank space, but for this as size is more and also the characters are more we even take the special symbols for our construction of the table.

	1	2	3	4	5	6
7	A	B	C	D	E	F
8	G	H	I	J	K	L
9	M	N	O	P	Q	R
10	S	T	U	V	W	X
11	Y	Z	Space	!	@	#
12	$	%	^	&	*	(
13	)	=	+	?	-	:

Table -1

Now every element in each compartment receives a numerical value. The column number is characterized by the first element, lasting the row number. For example, via Table 1: A obtains value 17, U obtains value 310 and special character @ receives 511, = receives 213 etc.

4.2. Number of vertices, edges, and degrees in complete bipartite graphs

Since there are two sets *A* and *B* with r vertices and *s* vertices respectively then the figure of vertices $V(G)=r+s$, where $V(G)=A\cup B$.

Moreover, the quantity of edges in a complete bipartite graph is equivalent to $r\times s$ since *r* vertices in set *A* coordinate with *s* vertices in set *B* to shape every conceivable edge for a complete bipartite graph. Ultimately, if the set *A* has *r* vertices and the set *B* has *s* vertices then all vertices in *A* have degree *s*, and all vertices in B have degree *r*. This should bode well since every vertex in set *A* is associated with all *s* vertices in set *B*, and every vertex in set *B* interfaces with all *r* vertices in set *A*.

5. Encryption and Decryption Algorithm:

Let α: GM$KQ*LR(be the note on the way to be encrypted.

STEP 1: Convert every character individually in *α* into its matching number value via Table-1 to produce β; such that the note encrypted should be in the form of a complete bipartite graph.

β= 18 19 112 58 59 512 68 69 612

STEP 2: Try to construct the graph equivalent to the sequence β to produce a graph G.

Intended for β:

Vertex set = (1,5,6,8,9,12)

Edge set = ((1,8), (1,9), (1,12), (5,8), (5,9), (5,12), (6,8), (6,9), (6,12))
Edge weights = (24,20,18,26,44,66,74,38,84)

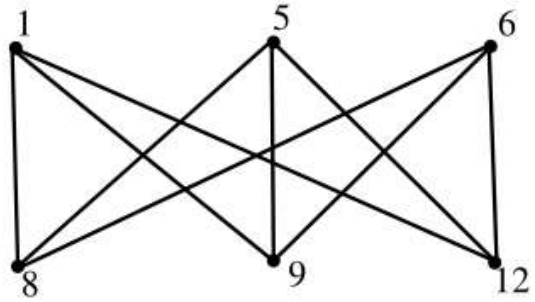

Figure 1.

STEP3: Guide G in the direction of the receiver

Intended for decryption the procedure should be reversed. Assume, the established graph which is seen in Fig. 2 i.e.

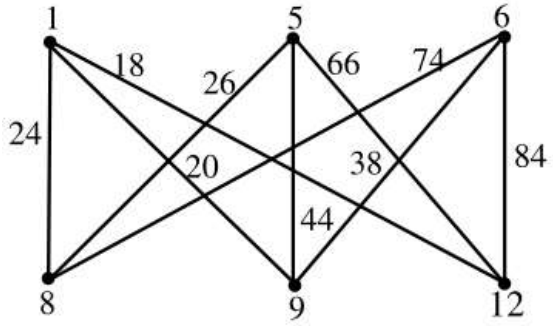

Figure 2.

Placing the edge weights in ascending order we produce the order for the decryption:

18 20 24 26 38 44 66 74 84

Pick the equivalent vertex tags from the graph, we produce the order

112 19 18 58 69 59 512 68 612

6. Conclusion

The numeral columns and rows can be constructed as per the above algorithm. We can build a graph with $1, 2\ldots, n$ number of columns. We can construct the tables as per the necessity of the graph. Several weighted graphs are obtainable in public field for numerous reasons. It is problematic to find the variance between a forged graph besides the graph which is encrypted. Accordingly the anticipated process is benign for encryption of any note through the complete bipartite graph.

References

[1] Guo T, Jiao J, Liu F and Wang W 2017 International Journal of Digital Crime and Forensics **9** 38-44
[2] Rathore A K and Jain A 2017 International Journal of Computer Applications **165** 1-5
[3] Yang D, Doh I and Chae K 2017 *International Conference on IEEE* 254-258
[4] Narsing Deo 2016 Graph theory with applications to engineering and computer science (USA, Courier Dover Publications)
[5] Chandrasekaran V M, Manimaran A and Akhil Ranjan 2015 *Int. J. Pharm Tech. Res.* **7** 85-89
[6] Manimaran A, Chandrasekaran V M and Archit 2015 *Int. J. Applied Eng. Res.* **10** 34068-34071
[7] Manimaran A, Chandrasekaran V M, Manish Gaur, Ayush Gupta and Pulkit Narwani 2015 *Int. J. Pharmacy and Technology* **7** 9774 – 9778
[8] Manimaran A, Chandrasekaran V M, Vivek Mallineni, Gangireddy Koushik Reddy and

Karthick P M 2015 *Int. J. Pharmacy and Technology* **7** 9904 – 9908
[9] Obaida Mohammad Awad Al-Hazaimeh 2013 *Int. J. Computer Networks & Comm.* **5** 95-103
[10] Vikas Agrawal, Shruti Agrawal and Rajesh Deshmukh 2014 *Int. J. Sci. Eng. Res.* **2** 1-3
[11] Yamuna M and Karthika K 2015 *Int. J.Advance Research in Science and Eng*. **4** 128-131
[12] Zimmerman P 1999 *An Introduction to Cryptography* (USA, Doubleday & Company)