Word Encryption Using Prism Graph

P Yuvashanmuga sree[1], K Maheswari[2]

[1]Department of Mathematics, Assistant Professor of Mathematics, Sakthi College of Arts and Science for Women Oddanchatram, Palani Main Road, Dindigul-624 624.

[2]PG Scholar, Department of Mathematics, Sakthi College of Arts and Science for Women Oddanchatram, Palani Main Road, Dindigul-624 624.

Abstract

It is always a big task to communicate confidential and sensitive information without leaking it to social media or any third party. The study of cryptography helps in dealing with these issues. There are many mathematical concepts in cryptography for communicating and authenticating secrecy. This paper gives an application model of graph theory in cryptography. Prism graphs, edge labeling, and matrices are used to encrypt and decrypt a five-letter word.

1. Introduction

Cryptography [1] is a tool for converting a readable message to an unreadable one. Which is of two kinds of ways of using encryption and decryption keys. The first one is Symmetric Key cryptography, which uses the same key for encryption as well as decryption. The second one is the Public key of non-symmetric key cryptography, which uses different keys for encryption and decryption. In this digital world cryptography plays a main role in the safety and security of financial and personal information. Updating the security systems is necessary to research in our day-to-day life. This paper is a model of applying graph theory in cryptography in communicating a five-letter word.

$G(V, E)$ is a graph with a set of vertices V and a set of edges E. A graph is a connected graph if there is a path between every pair of vertices. A graph is a cycle if it's starting and ending vertices are the same. If there is an edge between every pair of vertices, then the graph is called a complete graph. Graph theory [8, 9] is one of the mathematics topics with many applications in science and technology. The application of graph theory in cryptography is elaborated in [2, 3, 4]. The application of graph theory in cryptography strengthens its robustness, as the knowledge of graph theory is very important for the decryption of any ciphertext [5, 1]. Beaula and Venugopal constructed a cryptosystem using a double vertex graph [12]. Dawn Song et al. [6] used an expander graph in authenticating long digital streams over lossy networks as the constant degree of the graph makes the authentication more efficient. [7] gives a method using the Cayley graph constructed from groups, to construct cryptosystems.

Venugopal et al. gave block encryption and decryption of a sentence using the decomposition of the Turan graph [10].

Any important secret document which has to be shared among people will be encrypted by a password. This encrypted document and the secret key to decrypt the document will be sent separately to the receiver. Mostly a single word is used as a password. In this paper, a new cryptosystem using the prism graph, edge labeling, and matrices has been proposed.

Definition 1.1: Cartesian Product of two graphs [11]
The *Cartesian product* $G_1 \times G_2$ of two graphs G_1 and G_2 is the simple graph with $V_1 \times V_2$ as its vertex set and two vertices (u_1, v_1) and (u_2, v_2) are adjacent in $G_1 \times G_2$ if and only if $u_1 = u_2$ and, v_1 is adjacent to v_2 in G_2, or u_1 is adjacent to u_2 in G_1 and $v_1 = v_2$. Ex: Prism $C_8 \times P_2$, the following Figure 1. Prism $C_8 \times P_2$ is an example of a Cartesian product of C_8 and P_2.

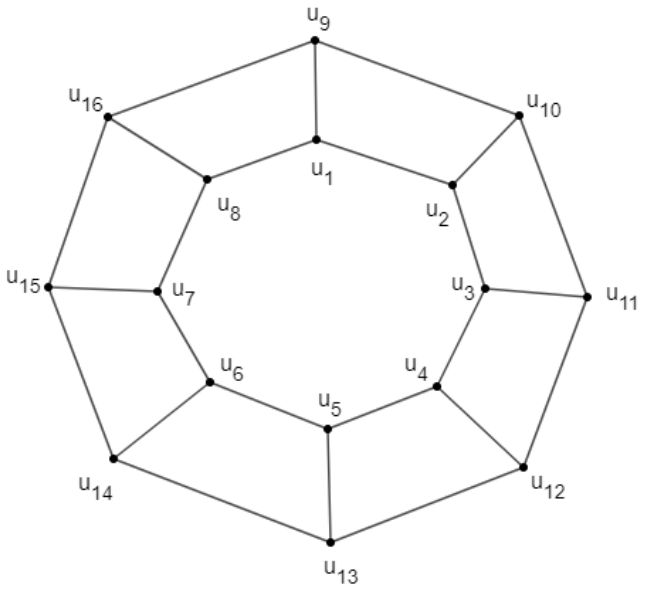

Figure 1: Prism $C_8 \times P_2$

2. Main Results:

In this section, we first introduce an encryption algorithm based on a prism graph $C_5 \times P_2$. This path is constructed from the given password. An illustration is given for this encryption algorithm by considering a password. Then a decryption algorithm is introduced to decrypt the encrypted word. We use the encoding table [1] given in Table I to convert any word to a number string.

Table I: Encoding table

Alphabet	A	B	C	D	E	F	G	H	I	J	K	L	M
Coding Number	2	4	6	8	10	12	14	16	18	20	22	24	26
Alphabet	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Coding Number	28	30	32	34	36	38	40	42	44	46	48	50	52

2.1. Edge labeling and Matrix formation:

The prism graph $C_5 \times P_2$ is labeled as given in Figure 2, which is listed as a matrix element as defined below, this matrix is named M.

$$M = \begin{pmatrix} a & b & c & d & e \\ f & g & h & i & j \\ k & l & m & n & o \end{pmatrix}.$$

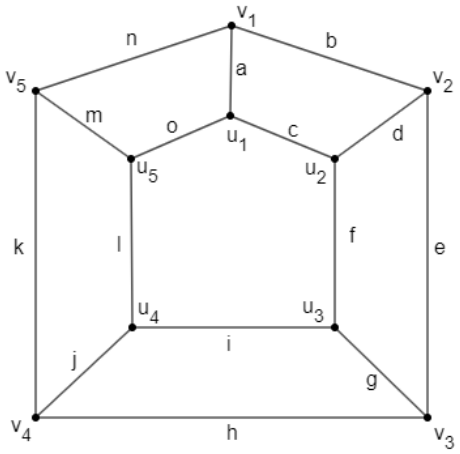

Figure 2. Edge labeled $C_5 \times P_2$

2.2. Key matrix:

A key matrix K is used as a symmetric key for encryption and decryption, which we have defined as follows.

$$K = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}$$

2.3. Encryption Algorithm:

Input: Alphabetical string of length 5
Output: Cipher text of length 15

Step 1: Convert the alphabetical string to a number string $N_5 = n_1, n_2, n_3, n_4, n_5$, using the encoding table - Table I.

Step 2: If the numbers are repeating, add 53 to the first repeating number, add 54 to the second repeating number 54, and add 55 to the third repeating number.

Step 3: Label these numbers to the edges $(u_i,\ v_i);\ 1 \leq i \leq 5$ of the graph $C_5 \times P_2$.

Step 4: Fill the remaining edges of $C_5 \times P_2$ with random numbers.

Step 5: Refer to Section 2.1 for the labeled graph, and form the matrix M.

Step 6: Add the key matrix K (defined in Section 2.2) to the matrix M and name the resulting matrix to be C.

Step 7: List the elements of the resulting matrix row by row to get the cipher text.

Encrypted message:

The encrypted message will be of the following form

Encrypted message = (First row of the matrix C, Second row of the matrix C, Third row of the matrix C).

2.4. ILLUSTRATION:

Input: **TREES**

Output: Cipher text of length 15

Step 1: Convert the plain text to a number string N_5= 40, 36, 10, 10, 38**,** using the encoding table - Table I.

Step 2: Add 53 to the second 10, which is a repeating number, therefore the resulting number string is 40, 36, 10, 63, 38.

Step 3: Labeling these numbers for the edges $(u_1, v_1), (u_2, v_2), (u_3, v_3), (u_4, v_4), (u_5, v_5)$ of $C_5 \times P_2$.

Step 4: Label the remaining edges of $C_5 \times P_2$ with random numbers. See Figure 3 for the resulting edge-labeled $C_5 \times P_2$.

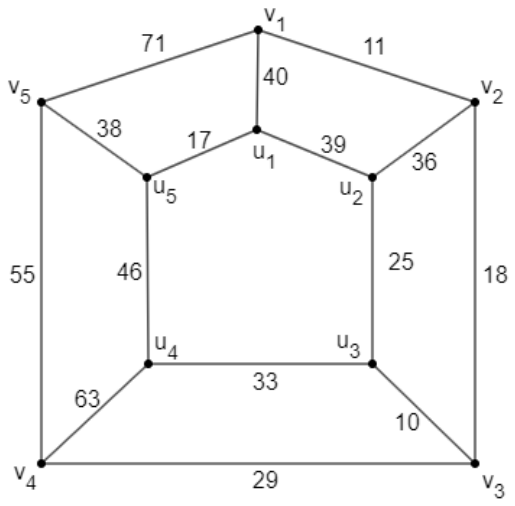

Figure 3: Edge-labeled $C_5 \times P_2$.

Step 5: The matric M of the edge-labeled $C_5 \times P_2$ as defined in Section 2.1

$$M = \begin{pmatrix} 40 & 11 & 39 & 36 & 18 \\ 25 & 10 & 29 & 33 & 63 \\ 55 & 46 & 38 & 71 & 17 \end{pmatrix}$$

Step 6: Add the key matrix K (defined in Section 2.2) to the matrix M and name the resulting matrix to be C.

$$C = \begin{pmatrix} 41 & 12 & 42 & 40 & 23 \\ 28 & 14 & 34 & 34 & 65 \\ 60 & 47 & 40 & 74 & 21 \end{pmatrix}$$

Step 7: Cipher text: {41, 12, 42, 40, 23, 28, 14, 34, 34, 65, 60, 47, 40, 74, 21}

Remark 1: The encrypted message can be decrypted by the receiver using the decryption algorithm**.**

Decryption Algorithm:

Step 1: Form a matrix of order 3×5 from the cipher text and name it C.
Step 2: Subtract the key matrix K from the matrix C and name the resulting matrix as M.
Step 3: Using M and Section 2.1 construct an edge-labeled prism graph $C_5 \times P_2$.
Step 4: List the edge labels $(u_1, v_1), (u_2, v_2), (u_3, v_3), (u_4, v_4), (u_5, v_5)$ of $C_5 \times P_2$ as a number string.
Step 5: If there is any number greater than 52, subtract 53 from the first greater number, subtract 54 from the second greater number, subtract 55 from the third greater number, and subtract 56 from the fourth greater number.
Step 6: Convert the resulting number string into an alphabetical string using the encoding table – Table I, which gives a plain text of length 5.

Conclusion:

In this paper, a prism graph used to encrypt a word was proposed. First, the given alphabetical string was encoded using the encoding table – Table I. The number string is labeled in the Prism graph then the graph is represented as a matrix as defined. These three stages make encryption stronger. Without the knowledge of graph theory, it is very difficult to hack and decrypt the encrypted plain text. This kind of encryption is used to communicate single words like passwords securely. This study can be extended to encrypt a sentence. This work can also be extended to other big graph structures of graphs to make the password more secure and strong.

References:

[1] William Stallings, "Cryptography and Network Security", Sixth Edition, Pearson Education Inc. 2014.

[2] P.L.K. Priyadarsini, "A survey of some applications of Graph theory in Cryptography" Journal of Discrete Mathematical Sciences and Cryptography, 2015 Vol.18 pp.209-217.

[3] M.Yamuna, Meenal Gogia, Ashish Sikka, Md. Jazib Hayat Khan "Encryption Using Graph Theory and Linear Algebra", International Journal of Computer Application, 2012, Vol.5, pp. 102-107.

[4] M. Yamuna, K. Karthika, "Data Transfer using Bipartite Graphs", International Journal of Advance Research in Science and Engineering, 2015, Vol.4, pp. 128-131.

[5] Wael Mahmoud Al Etaiwi, "Encryption Algorithm Using Graph Theory", Journal of Scientific Research and Reports", 2014, pp. 2519-2527.

[6] Dawn Song, David Zuckerman, and J.D. Tygar, "Expander Graphs for digital stream authentication and robust overlay networks", Proceedings of the 2002 IEEE

Symposium on Security and Privacy (S&P.02)

[7] Brian Cusack, Erin Chapman, "Using graphic methods to challenge cryptographic Performance", Proceedings of 14th Australian Information Security Management Conference, 5-6 December 2016, Edith Cowan University, Perth, Western Australia. pp.30-36.

[8] Harary F, "Graph Theory" Narosa Publishing House, 1988.

[9] Narsingh Deo, "Graph Theory with Applications to Engineering and Computer Science", Prentice-Hall, 1974.

[10] C Beaula, P Venugopal, B Praba, "Block encryption and decryption of a sentence using decomposition of the Turan graph", Journal of Mathematics, Vol. 2023, Article ID 7588535, 9 pages, 2023. https://doi.org/10.1155/2023/7588535.

[11] S Ramakrishnan, J Baskar Babujee, Degree distance of some Planar graphs, International Journal of Computing Algorithm, Volume 3, 54-57, 2014.

[12] C Beaula, P Venugopal, Cryptosystem using double vertex graph, Indian Journal of Science and Technology, Volume 13, (44), 4483-4489, 2020. Doi: 10.1745/IJST/v3i44.1699.