An enriched cryptosystem based Polybius cipher using graph labeling techniques

Cite as: AIP Conference Proceedings **2516**, 210049 (2022); https://doi.org/10.1063/5.0108508
Published Online: 30 November 2022

B. Deepa and V. Maheswari

An Enriched Cryptosystem Based Polybius Cipher Using Graph Labeling Techniques

B. Deepa [b] and V. Maheswari [a]

Department of Mathematics, Vels Institute of Science, Technology and Advanced Studies
Chennai -600117, India.
[a] Corresponding author: maheswari.sbs@velsuniv.ac.in
[b] balaraman.deepa@gmail.com

Abstract. Cryptography is a concept to protect information and communication from adversaries through the use of codes. Graph theory is ultimately the study of graphs. In this paper we are using cryptographic technique together with graph labeling to protect our message being hacked by any adversaries as well as safeguarding the communication. This paper proposes an enriched technique of coding a message based on Polybius cipher and permutation cipher for the regular graph using product edge labeling techniques. The resulting cipher text is forwarded to the receiver in a structure of cipher graph which admits our proposed edge labeling. The receiver, thus decrypts the edge labels using secret keys shared by the sender. Here we make use of symmetric key cryptosystem as we perform both encryption and decryption using the same key. The main advantage of symmetric cryptosystem is that it is effective and fast for a huge collection of data.

Keywords: Encryption, Decryption, Polybius cipher, Permutation Cipher, Product edge Labeling, Regular graph.

AMS Subject classification MSC (2010) No: 05C78

INTRODUCTION

Here we make use of a combination of Polybius and Permutation cipher to perform our encryption process. Thus the resulting ciphertext using Polybius square cipher is re-encrypted using permutation cipher, after which we proceed product edge labeling technique to pass the encrypted message to the receiver in a form Cipher Graph. Here we deal with symmetric key cryptosystem for the process of encryption and decryption.

LITERATURE SURVEY

For basic definitions of graph structures and various graph labeling techniques we refer J.A. Gallian [1] and F. Harary [2]. On paper, [3], [4], [5], [6] and [7] encryption scheme through Polybius Cipher have been studied. We refer Falih Aldosray, [8] for Better Security Enhancement using permutation Cipher. [9], [10] and [11] showcases Encryption and Decryption techniques using various graphs through product edge labeling techniques, Inspired by [2], [3], [5] & [9] we present an enriched technique of coding a message based on Polybius square and Permutation cipher for the graph using product edge labeling techniques.

PRELIMINARIES

Definitions

Polybius square cipher

In Cryptography, The Polybius square cipher is a table in which each character is expressed by its row and column.

2nd International Conference on Mathematical Techniques and Applications
AIP Conf. Proc. 2516, 210049-1–210049-8; https://doi.org/10.1063/5.0108508
Published by AIP Publishing. 978-0-7354-4234-4/$30.00

Encryption

Encryption is a technique that transforms a text or file into an unreadable format.

Decryption

Decryption is the technique that transforms an encoded text into readable format.

Regular graph

A regular graph is a graph in which every pair of vertices has the same degree.

K regular graph

A K regular graph is a graph in which every pair vertex has the degree K.

POLYBIUS SQUARE CIPHER

A Polybius square is a table used to convert plain text characters into numeric sequences, it's also known as the Polybius checkerboard invented in second century B.C by Ancient Greeks Cleoxenus and Democleitus. This Polybius square consists of 26 English alphabets into the 25 cells, I and j sharing its position in a single cell.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

FIGURE 1. Polybius square cipher

PROPOSED POLYBIUS SQUARE CIPHER

In our proposed methodology, the traditional Polybius square matrix was stretched into a 5*8 square matrix consisting of 5 rows and 8 columns. These include lower case alphabets, numbers and punctuation marks. In this Polybius square table all the characters are arranged in a random manner. Each character represented as a couple of numeric values (row and column). Thus "e" represented as "21" and "t" is "25" and so on.

TABLE. 1 Polybius Square 5x8 matrix

	0	1	2	3	4	5	6	7
0	0	5	b	k	q	s	v	g
1	1	6	&	7	i	"	o	,
2	?	e	d	l	f	t	2	c
3	9	8	h	r	n	j	y	x
4	4	3	w	p	m	u	z	.

PERMUTATION CIPHER

Permutation cipher is a branch of Discrete Mathematics which is also known as transposition cipher. A reordering of the member into a sequence or ordered set. We can also state as "combination of groups" or "arrangement of blocks".

THEOREM

Any K regular Graph is a product labelled Graph.

Proof:

Let k be the regular Graph with different vertices $v_1, v_2, v_3, \ldots v_n$.

Consider f: $V(k) \rightarrow 3N$ by $f(u_i) = 3i$ for all $i = 1,2, \ldots . n$.

Define an edge labeling by $f(uv) = (f(u) \times f(v)) \bmod 26$

Therefore the product of edge labeling are distinct.

Hence the function f provides a product of edge labeling for the graph K.

Flowchart for Encryption and Decryption Process

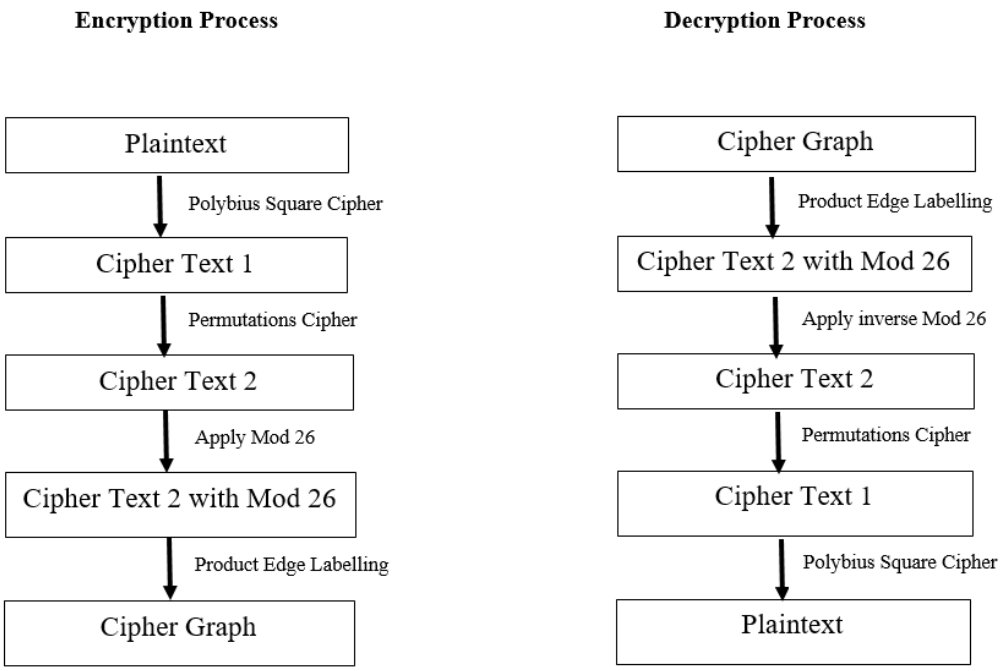

FIGURE 2. Flow chart

ILLUSTRATION

Encryption Process

Step: 1

Let us consider our Plain text to be “9 & 1 where did you come from?”

Step: 2

Our Plain text is going to process in the table 1.

Now each character of Plaintext identified in the Polybius square 5x8 table, the first letter of our Plaintext “9” is encoded as “31”, the second letter “&” is encoded as “12”. By continuing this process, we can get the pair values for our message, which is assembled in rows and columns.

TABLE 2. Pair value of plaintext

Plaintext	9	&	1	w	h	e	r	e	d	i	d	y	o	u	c	o	m	e	f	r	o	m	?
Row	3	1	1	4	3	2	3	2	2	1	2	3	1	4	2	1	4	2	2	3	1	4	2
Column	1	2	0	2	7	1	3	1	2	4	2	6	6	5	7	6	4	1	4	3	6	4	0

The pair value of plain text thus obtained from Polybius Square cipher will give us ciphertext 1 which going to process in the next stage of encryption as a plaintext 1.

Step: 3

We will encode it [table 2] using a permutation cipher that splits the plaintext 1 into 6-letter blocks. In that each block has 4 columns, but the last one is not having a 4 columns instead of padding a block we take it a block as it is same.

TABLE 3. Two letter blocks

Block 1					Block 2					Block 3					Block 4					Block 5					Block 6		
3	1	1	4		3	2	3	2		2	1	2	3		1	4	2	1		4	2	2	3		1	4	2
1	2	0	2		2	1	3	1		2	4	2	6		6	5	7	6		4	1	4	3		6	4	0

Here we are reordering the letter of blocks as stated in the following permutation cipher,

$$\begin{bmatrix} 1 & 3 & 5 & 2 & 4 & 6 \\ 3 & 5 & 2 & 4 & 6 & 1 \end{bmatrix}$$

We get,

TABLE 4. Ciphertext 2

Block 6				Block 5				Block 1				Block 2				Block 3				Block 4			
1	4	2		4	1	2	3	3	1	1	4	3	1	3	1	2	1	2	3	1	4	2	1
6	4	0		4	3	4	3	1	2	0	2	2	3	3	3	2	4	2	6	6	5	7	6

The letters in Block 1 moves 3, the letters in Block 2 moves to 4, the letters in Block 3 moves to 5, the letters in Block 4 moves to 6, the letters in Block 6 moves to 1. Then the permutation is applied to all the blocks we arrange the row and column value as a couple of numeric values, it is written off in a row. So the Ciphertext 2 is as shown in table 5.

TABLE 5. Pair value of Ciphertext 2

16	44	20	44	21	24	33	31	12	10	42	32	21	33	21	22	14	22	36	16	45	27	16

Step: 4

The ciphertext 2 is then altered by taking mod 26 are as follows

TABLE 6. Ciphertext 2 with mod 26

16	18	20	18	21	24	7	5	12	10	16	6	21	7	21	22	14	22	10	16	19	1	16

Finally, our encrypted plaintext 1 presented in the form of cipher graph using product edge labeling which is send to the receiver with key.

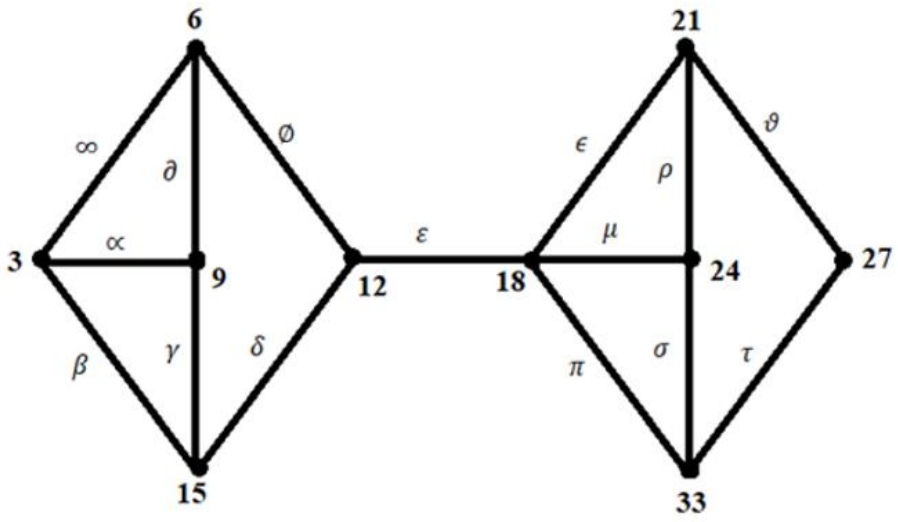

FIGURE 3. Cipher Graph

Clues

The message, which includes both letter and number.

Key 1: Use product edge labeling formula to find the labels by using the formula

$\big(f(u) \times f(v)\big) \bmod 26$. Further the receiver has to assign the labels in the order of

$$\mu, \infty, \emptyset, \infty, \vartheta, \delta, \tau, \gamma, \sigma, \rho, \mu, \varepsilon, \vartheta, \tau, \vartheta, \pi, \epsilon, \pi, \rho, \mu, \beta, \alpha, \mu$$

Key 2: Use Permutation order

1	3	5	2	4	6
3	5	2	4	6	1

Key3: A pair of numerical value represents its rows and columns.

Decryption Process

Step: 1

The message is deciphered by applying the inverse process of encryption techniques, here we make use of Product edge labeling formula $\big(f(u) \times f(v)\big) \bmod 26$ for finding edge labels.

We get,

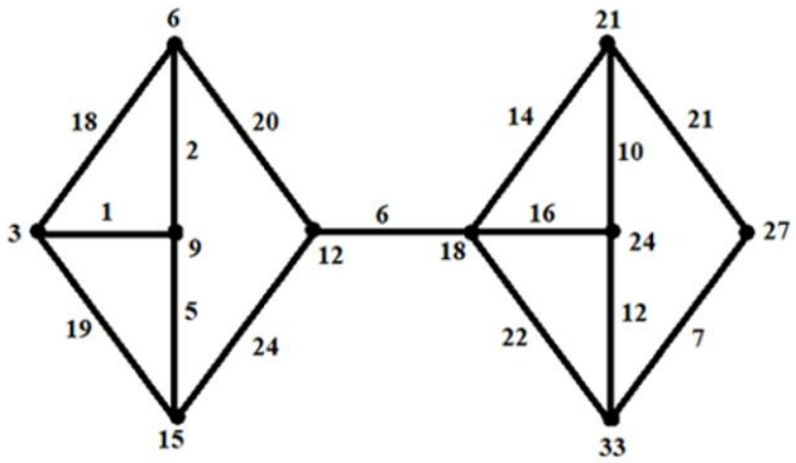

FIGURE 4. Regular graph on 10 vertices

Further great arrangements of labels as stated in clue 1, which give us our plaintext 2,

TABLE 7. Plaintext 2

16	18	20	18	21	24	7	5	12	10	16	6	21	7	21	22	14	22	10	16	19	1	16

Step: 2

By taking inverse mod 26 to each pair value of Plaintext 2, we get

TABLE 8. Plaintext 2 with inverse mod 26

16	44	20	44	21	24	33	31	12	10	42	32	21	33	21	22	14	22	36	16	45	27	16

The numeric value written off into rows and columns,

TABLE 9. Blocks of plaintext 2

Block 6				Block 5				Block 1				Block 2				Block 3				Block 4			
1	4	2		4	1	2	3	3	1	1	4	3	1	3	1	2	1	2	3	1	4	2	1
6	4	0		4	3	4	3	1	2	0	2	2	3	3	3	2	4	2	6	6	5	7	6

Step: 3

By making use of a permutation cipher as stated in clue 2, which yield our plaintext 1.

TABLE 10. Blocks of plaintext 1

Block 1				Block 2				Block 3				Block 4				Block 5				Block 6		
3	1	1	4	3	2	3	2	2	1	2	3	1	4	2	1	4	2	2	3	1	4	2
1	2	0	2	2	1	3	1	2	4	2	6	6	5	7	6	4	1	4	3	6	4	0

Step: 4

Finally, our plaintext 1 going to process in Polybius square table 1. Now we look at a couple of numeric values in the square table 1. So “31” stands for the plaintext letter “8” and “12” stands for “&”. Continuing in this way we obtain the plaintext message “9 and 1 where did you come from?”

Hence our required Plain text is **“9 & 1 where did you come from?”**.

CONCLUSION

The proposed crypto technique of coding a message based on Polybius square cipher and Permutation cipher for the 3 regular graph with 10 vertices using Product edge labeling techniques for message transaction is complex and more secure. As a future work, plan to encode a message with different combination of ciphers with various kinds of labeling to improve integrity and security.

REFERENCES

1. J.A. Gallian, A Dynamic Survey of Graph Labeling, *Electronic Journal of Combinatorics* (2018).
2. F. Harary, Graph Theory, *Addison – Wesley*, (1969).
3. T. S. Kondo, L. J. Mselle, *IJCA* 30-33, (2013).
4. Puneet Kumar, Dr. S. B. Rana, *IJIET*, 227-229, (2015).
5. J. C. T. Arroyo, A. R. L. Reyes and A. J. P. Delima, *IJACSA*, 108-115, (2020).
6. G.Manikandan, P.Rajendiran, R.Balakrishnan and S.Thangaselvan, *IJPAM*, 13317-13324, (2018).
7. Moumita Maity,*IJTRE*, 1117-1119, (2014).
8. Falih Aldosray, *JECET*, 104-107, (2019).
9. B.Deepa and V.Maheswari, *IJAEMA*, 8-15 (2019).
10. B.Deepa, V.Maheswari and V. Balaji, *IJEAT*, 206-212 (2019).
11. B.Deepa and V.Maheswari, *IJRTE*, 33-36 (2019).