International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-1S, October 2019

Creating Ciphertext and Decipher using Graph Labeling Techniques

B. Deepa, V. Maheswari, V. Balaji

Abstract: ***In this paper, we design plaintext through product edge labeling for a Cyclegraph. The edge labels thus obtained is further processed through Caesar cipher method. The ciphertext thus obtained is subjected to Bifid Cipherfor which we apply matrix multiplication. The decryption is performed usingInverse matrix multiplication and subsequent application of Bifid cipher and Caesar Cipher yields our plaintext. This methodology is considered highly efficient and secure as it combines Cryptographic technique together with Graph Labeling thereby making it difficult for any Adversary to hack the plaintext. We investigate the above technique using Non- singular square matrices.***

Keywords: Plaintext, Ciphertext, Encryption, Decryption, Bifid cipher, Rotation letters, Inverse matrix, Cycle Graphs. AMS subject classification MSC (2010) No: 05C78

I. INTRODUCTION

Dinesh Goyal, Naveen Hemrajani, Kritika Paliwal introduced the concept GPH Algorithm: Improved CBC improved BIFID cipher Symmetric Key Algorithm[1], and also [2],[3]etc.

Inspired by this work, we introduce a methodology of forming a plaintext by applying product labelingfor a given $C_n^{(t)}$ – Cycle graph G and then converting the plaintext to ciphertext by using Caesar and Bifid cipher method.

In traditional Caesar cipher the plaintext letters are shifted to a certain number of places down the alphabet. A Caesar Cipher is a simple form of Substitution Cipher were merely the letters are substituted in the place of original letters. But here we start numbering the alphabets beginning with the alphabet u, v,w …a, b……. s, t and we assign the value 1 to u, 2 to v…… and so on.

The Bifid cipher is considered a more secure cipher because it breaks the message apart into two separate streams and then recombines them. Bifid is a cipher technique which combines the Polybius square with transposition and uses fractionation to achieve diffusion. It was invented by Felix Delastelle a Frenchman who invented several ciphers including the bifid, trifid, and four-square ciphers. Keys for the Bifid cipher consist of a 26 letter 'key square'. To encode a message, the letters are written in column wise "uvwxy", then the plaintext is figured out the row and column for each letter.

A. Definition

Cryptography is passing confidential message from sender to the recipient, the conversion of information from a cryptic state to readable state. The originator of an encrypted message shares the decoding technique only with intended recipients to preclude access from the attacker.

B. Definition

A square matrix K, with a determinant not equal to zero, then there exists an inverse matrix of

$$\boldsymbol{K} = \frac{(\textbf{adjoint K})}{(\textbf{determinant K})}.$$

C. Definition

In cryptography readable material is known as plaintext.

D. Definition

Encrypting the message into an unreadable format is called Ciphertext.

E. Definition

A Graph G (V, E) is said to be product labeled graph, if$\mathbf{f}: \mathbf{V}(\mathbf{G}) \rightarrow \mathbf{3N}$ is an one-one mapping such that the resultant edge labels

are $\mathbf{f}^*(\mathbf{e} = \mathbf{uv}) = (\mathbf{u} \times \mathbf{v}) \bmod 26$.

F. Definition

C_n^t Graph

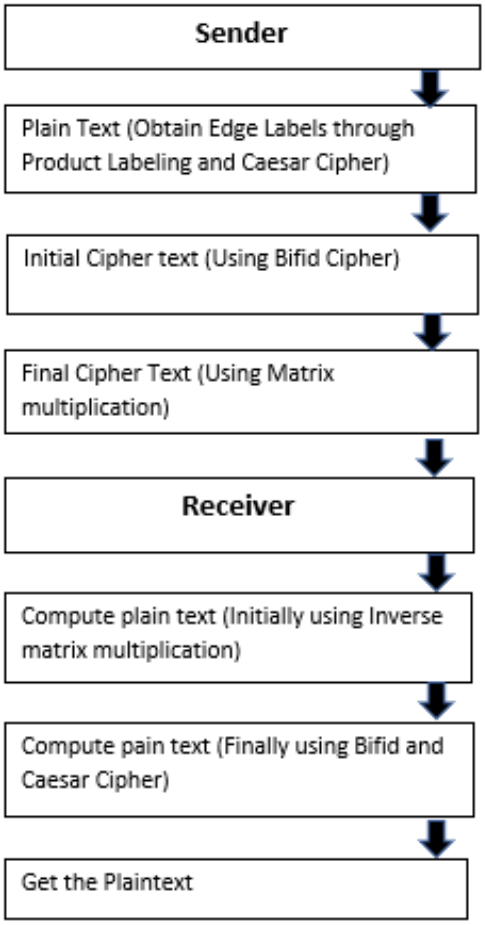
The cycle graph with *n* number of vertices connected in a closed chain is known as $C_n^{(t)}$ Graph.

Kolam is an artistic creation. It is a ubiquitous art form predominant
in South India, while also seen in a few places in northern India and South East
Asia. Kolam holds a rich tradition of cultural and medicinal significance.
Kolams are generated using kolam grammar
Kolam is an artistic creation. It is a ubiquitous art form predominant
in South India, while also seen in a few places in northern India and South East

Manuscript published on 30 October 2019.
***** Correspondence Author (s)
B. Deepa, Research Scholar, Department of Mathematics, Vels Institute ofScience, Technology&Advanced Studies(VISTAS)Chennai-117, Tamilnadu-India
V. Maheswari, Associate Professor, Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Chennai-117, Tamilnadu-India
V. Balaji, Assistant Professor, Department of Mathematics, SacredHeart College (Autonomous), Tirupattur, Vellore-635601, Tamilnadu-India.

Asia. Kolam holds a rich tradition of cultural and medicinal significance.
Kolams are generated using kolam grammar
Kolam is an artistic creation. It is a ubiquitous art form predominant
in South India, while also seen in a few places in northern India and South East
Asia. Kolam holds a rich tradition of cultural and medicinal significance.
Kolams are generated using kolam grammar
Kolam is an artistic creation. It is a ubiquitous art form predominant
in South India, while also seen in a few places in northern India and South East
Asia. Kolam holds a rich tradition of cultural and medicinal significance.
Kolams are generated using kolam grammar

II. OUTLINE OF ENCRYPTION AND DECRYPTION TECHNIQUE



III. METHODOLOGY

TO ENCIPHER

Step1: Draw a Cycles graph $\mathbf{G} = (\mathbf{V}, \mathbf{E})$ with vertices $\mathbf{V} = \{\mathbf{v_1}, \mathbf{v_2}, \mathbf{v_3}, \ldots . \mathbf{v_n}\}$ and edges $\mathbf{E} = \{\mathbf{e_1}, \mathbf{e_2}, \mathbf{e_3}, \ldots . \mathbf{e_{n-1}}\}$.

Step2: Obtain the Edge labels bydefinition through Caesar cipher.

Step 3: Use bifid cipher to encipher our plaintext message.

Step 4: A matrix multiplication to get our cipher text message.

To Decipher

Step 1: The receiver will decipher the message by using inverse matric multiplication and bifid cipher.

Step 2: Thus, the receiver will get a plaintext through which Caesar Cipher.

IV. THEOREM

Any Cycle graph is a product labeled Graph.

Proof: Let $\mathbf{C_n}$ be the Cycle graph with different vertices $\mathbf{v_1}, \mathbf{v_2}, \mathbf{v_3}, \ldots\ldots, \mathbf{v_n}$

Consider f: $\mathbf{V}(\mathbf{k_n}) \rightarrow$ 3N by f($\mathbf{u_i}$) = 3i for all i=1, 2…n

Then by definition f*(e=uv) = $(\boldsymbol{u} \times \boldsymbol{v})$ mod 26 the edge labels

are 18,2,4,24,10, 2……...etc.

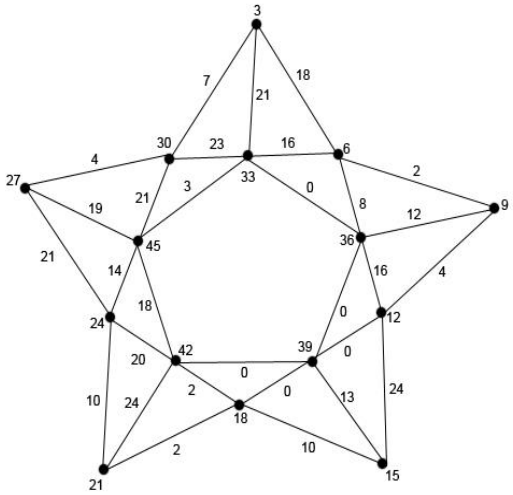


Fig a:C_n^t Graph with p vertices and2p edges

For the above CycleGraph, we apply product edge labeling and making use of Caesar cipher with additive key 6, obtained the edge labels thus obtained forms our initial Ciphertext.In the overall thirty edges we are using the some of the edges only rest of edges are known as the jumped edges.

Table I: Additive 6 Caesar Cipher

u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Now let's we explain the process by illustrations,

V. ILLUSTRATION:

let our Plaintext be:go abroad for job

Table II: Conversion of Plaintext using Additive 6 Caesar Cipher

13	21	7	8	24	21	7	10	12	21	24	16	21	8
g	o	a	b	r	o	a	d	f	o	r	j	o	b

Thus, the plaintext is converted into ciphertext which is our initial plaintext.
BIFID CIPHER

Now here we are going to use the Bifid Cipher technique which is invented by Felix Blessed Virgin Delastelle in 1840-1902. In the Bifid cipher we use square matrix of order 5 by 5 where each matrix element has a corresponding row and column entity.

	1	2	3	4	5
1	u	z	e	j	o
2	v	a	f	k	p
3	w	b	g	l	q
4	x	c	h	m	r
5	y	d	i	n	s, t

Fig.b Bifid Cipher

So, for our Plain text: go abroad for job
The corresponding row and column entity are as follows,
Row Value:3 1 2 3 4 1 2 5 2 1 4 1 1 3 Column Value: 3 5 2 2 5 5 2 2 3 5 5 4 5 2
Notice just how the letter "g" has the value of 33. "o" is 15 meanwhile it is found in row 1, column 5. s and t share theposition of (5,5) in the matrix above. After the message has been written out, with row and column values written as shown above, we encode the converted edge labels using matrix multiplication.

VI. ENCODING OF EDGE LABELING

We consider a 3 x10 matrix and the labels are written into three number blocks and to complete the matrix we add null values at the end

Table III:

3	1	2	3	4	1	2	5	2	1
4	1	1	3	3	5	2	2	5	5
2	2	3	5	5	4	5	2	0	0

Let us consider a key matrix $K = \begin{pmatrix} 7 & 2 & 1 \\ 0 & 3 & -1 \\ -3 & 4 & -2 \end{pmatrix}$

Now we use the key matrix multiplication to encrypt message. The key matrix should be selected such that its inverse exits.

$$kp = \begin{pmatrix} 7 & 2 & 1 \\ 0 & 3 & -1 \\ -3 & 4 & -2 \end{pmatrix} \begin{pmatrix} 3 & 1 & 2 & 3 & 4 & 1 & 2 & 5 & 2 & 1 \\ 4 & 1 & 1 & 3 & 3 & 5 & 2 & 2 & 5 & 5 \\ 2 & 2 & 3 & 5 & 5 & 4 & 5 & 2 & 0 & 0 \end{pmatrix} mod\ 26$$

$$= \begin{pmatrix} 5 & 11 & 19 & 6 & 13 & 21 & 23 & 15 & 24 & 17 \\ 10 & 1 & 0 & 4 & 4 & 11 & 1 & 4 & 15 & 15 \\ 3 & 23 & 18 & 19 & 16 & 9 & 18 & 15 & 14 & 17 \end{pmatrix}$$

5	11	19	6	13	21	23	15	24	17
10	1	0	4	4	11	1	4	15	15
3	23	18	19	16	9	18	15	14	17

Now, the receiver will decipher the message by using inverse matrix multiplication and Bifid Cipher

VII. DECODING OF EDGE LABELING

To decrypt the message to the original one, we use the inverse of key matrix such

that $\mathbf{K^{-1}} = \begin{pmatrix} -2 & 8 & -5 \\ 3 & -11 & 7 \\ 9 & -34 & 21 \end{pmatrix}$ Now multiplying the inverse matrix with column matrices which generated from matrix operations $k^{-1}C$ (mod26).

u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Thus

$$K^{-1}C = \begin{pmatrix} -2 & 8 & -5 \\ 3 & -11 & 7 \\ 9 & -34 & 21 \end{pmatrix} \begin{pmatrix} 5 & 11 & 19 & 6 & 13 & 21 & 23 & 15 & 24 & 17 \\ 10 & 1 & 0 & 4 & 4 & 11 & 1 & 4 & 15 & 15 \\ 3 & 23 & 18 & 19 & 16 & 9 & 18 & 15 & 14 & 17 \end{pmatrix} mod26$$

$$= \begin{pmatrix} 3 & 1 & 2 & 3 & 4 & 1 & 2 & 5 & 2 & 1 \\ 4 & 1 & 1 & 3 & 3 & 5 & 2 & 2 & 5 & 5 \\ 2 & 2 & 3 & 5 & 5 & 4 & 5 & 2 & 0 & 0 \end{pmatrix}$$

Converting the above matrix in the form of table we get,

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

3	1	2	3	4	1	2	5	2	1	4	1	1	3	3
5	2	2	5	5	2	2	3	5	5	4	5	2	0	0

Rewriting the above text in the form of rows and columns
Row Value:3 1 2 3 4 1 2 5 2 1 4 1 1 3
Column Value: 3 5 2 2 5 5 2 2 3 5 5 4 5 2

Using Bifid Cipher, the corresponding row and column values are noted down. Our plaintext is recovered after the decryption using additive 6 Caesar Cipher technique

BIFID CIPHER:

	1	2	3	4	5
1	u	z	e	j	o
2	v	a	f	k	p
3	w	b	g	l	q
4	x	c	h	m	r
5	y	d	i	n	s, t

Fig.c Bifid Cipher

Caesar cipher decryption

Then the decrypted message is

"go abroad forjob".

VIII. ILLUSTRATION

Table V: Additive 6 Caesar Cipher

u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Now let's we explain the process by illustrations, let our Plaintext be: a man had good wool bag

Table VI: Conversion of Plaintext using Additive 6 Caesar Cipher

a	m	a	n	h	a	d	g	o	o	d	w	o	o	l	b	a	g
7	19	7	20	14	7	10	13	21	21	10	3	21	21	18	8	7	13

Thus, the plaintext is converted into ciphertext which is our initial plaintext.

BIFID CIPHER

Now here we are going to use the Bifid

Cipher technique

	1	2	3	4	5
1	u	z	e	j	o
2	v	a	f	k	p
3	w	b	g	l	q
4	x	c	h	m	r
5	y	d	i	n	s, t

Fig.d Bifid Cipher

So, for our Plain text: "a man had good wool bag"

The corresponding row and column entity are as follows,

Row Value: 2 4 2 5 4 2 5 3 1 1 5 3 1 1 3 3 2 3

Column: Value: 2 4 2 4 3 2 2 3 5 5 2 1 5 5 4 2 2 3

the letter "a" has the value of 22. "m" has the value of 44, it is found in row 4, column 4 in the matrix above. After the message has been written out, with row and column values written as shown above, we encode the converted edge labels using matrix multiplication.

IX. ENCODING OF EDGE LABELING

We consider a 3 x12 matrix and the labels are written intothree number blocks and to complete the matrix we add null values at the end

TableVII:

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

Let us consider a key matrix $K = \begin{pmatrix} \mathbf{7} & \mathbf{2} & \mathbf{1} \\ \mathbf{0} & \mathbf{3} & \mathbf{-1} \\ \mathbf{-3} & \mathbf{4} & \mathbf{-2} \end{pmatrix}$

Now we use the key matrix multiplication to encrypt message. The key matrix should be selected such that its inverse exits.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

$$kp = \begin{pmatrix} 7 & 2 & 1 \\ 0 & 3 & -1 \\ -3 & 4 & -2 \end{pmatrix} \begin{pmatrix} 2 & 4 & 2 & 5 & 4 & 2 & 5 & 3 & 1 & 1 & 5 & 3 \\ 1 & 1 & 3 & 3 & 2 & 3 & 2 & 4 & 2 & 4 & 3 & 2 \\ 2 & 3 & 5 & 5 & 2 & 1 & 5 & 5 & 4 & 2 & 2 & 3 \end{pmatrix} mod\ 26$$

$$c = \begin{pmatrix} 18 & 7 & 25 & 20 & 8 & 21 & 18 & 8 & 15 & 17 & 17 & 2 \\ 1 & 0 & 4 & 4 & 4 & 8 & 1 & 7 & 2 & 10 & 7 & 3 \\ 20 & 12 & 22 & 13 & 18 & 4 & 9 & 23 & 23 & 9 & 19 & 19 \end{pmatrix}$$

The ciphertext thus obtained is arranged in the following table

Table VIII: FINAL CIPHERTEXT

18	7	25	20	8	21	18	8	15	17	17	2
1	0	4	4	4	8	1	7	2	10	7	3
20	12	22	13	18	4	9	23	23	9	19	19

Now, the receiver will decipher the message by usinginverse matrix multiplication and Bifid Cipher

X. DECODING OF EDGE LABELING

To decrypt the message to the original one, we use the inverse of key matrix such

that $\mathbf{K^{-1}} = \begin{pmatrix} \mathbf{-2} & \mathbf{8} & \mathbf{-5} \\ \mathbf{3} & \mathbf{-11} & \mathbf{7} \\ \mathbf{9} & \mathbf{-34} & \mathbf{21} \end{pmatrix}$ Now multiplying the inverse matrix with column matrices which generated from matrix operations k^{-1} C (mod 26). Thus

$$k^{-1}c = \begin{pmatrix} -2 & 8 & -5 \\ 3 & -11 & 7 \\ 9 & -34 & 21 \end{pmatrix} \begin{pmatrix} 18 & 7 & 25 & 20 & 8 & 21 & 18 & 8 & 15 & 17 & 17 & 2 \\ 1 & 0 & 4 & 4 & 4 & 8 & 1 & 7 & 2 & 10 & 7 & 3 \\ 20 & 12 & 22 & 13 & 18 & 4 & 9 & 23 & 23 & 9 & 19 & 19 \end{pmatrix} mod\ 26$$

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

Converting the above matrix in the form of table we get,

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

Rewriting the above text in the form of rows and columns

Row Value: 2 4 2 5 4 2 5 3 1 1 5 3 1 1 3 3 2 3

Column: Value: 2 4 2 4 3 2 2 3 5 5 2 1 5 5 4 2 2 3

BIFID CIPHER:

u	V	w	X	Y	Z	a	b	c	d	e	F	g	h	i	j	k	l	m	n	o	p	Q	r	s	t
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

	1	2	3	4	5
1	u	z	e	j	O
2	v	a	f	k	P
3	w	b	g	l	Q
4	x	c	h	m	R
5	y	d	i	n	s, t

Fig.e Bifid Cipher

Caesar cipher decryption Using Bifid Cipher, the corresponding row and column values are noted down. Our plaintext is recovered after the decryption using additive 6 Caesar Cipher technique. Then the decrypted message is “a man had good wool bag”.

XI. CONCLUSION

In this paper we have illustrated a new method called Product mod labeling to create edge labels. For making the encryption and decryption of plaintext we use Cipher techniques namely Caesar, Bifid Cipher with usage of matrix multiplication technique. The messages made by this process are difficult to hack by any intruder. we can also extend our work further by applying various Graph labelings to create secret messages with different cryptographic procedures along with matrix applications. Also, Further work can be developed by improving the edge labels to maintain secrecy.

APPLICATION

Modular Arithmetic is the main process used in encoding and decoding the messages. The concept of RSA in computer science is implemented using modulo property. Chinese remainder modulo function are used to create crypto systems. Cryptography is used in digital transfer of message through signature, verifying the authentication while signing in any application, integrity of transmitting data in banking sector and electronic money transfer.

REFERENCES

1. Dinesh Goyal, Naveen Hemrajani, Kritika Paliwal “GPH Algorithm: Improved CBC improved BIFID cipher Symmetric Key Algorithm,International Journal of Communication and Computer Technologies
2. Volume 01 – No.60 Issue: 07 Aug 2013, ISSN NUMBER: 2278-9723 David Kahn, The codebreakers: The story of secret writing, Revised ed.1996. ISBN 0-684-83130-9.
3. Lester S. Hill, Concerning Certain Linear Transformation Apparatus of Cryptography, The American Mathematical Monthly Vol.38,1931, pp.135-154.
4. Lester S. Hill, Cryptography in a Algebraic Alphabet, The American Mathematical Monthly Vol.36, June-July 1929, pp.306-312.
5. Jan CA. Van Dev Lubbe, Basic Methods of Cryptography, Cambridge University Press, United Kingdom (2002).
6. Chris Christensen, Caesar Ciphers, Spring 2010, HNR 304.
7. J. Basker Babujee, V. Vishnupriya, encrypting number using pair labeling in path graph, IJPAM: Volume 114, No.2 (2017)

AUTHORS PROFILE

B. Deepa, Research Scholar, Department of Mathematics, Vels Institute of Science, Technology &Advanced Studies (VISTAS), Pallavaram, Chennai-117, Tamilnadu, India. She continues her career in Sindhi Arts and Science College as an Assistant professor in Department of Mathematics since2013. She has also Guest Lectured in Department of Mathematics at Indira Gandhi Engineering College, Chengalpattu. Tamilnadu. Interesting area in Mathematics is Graph theory, Cryptography. She is now pursuing her Ph.D. in VISTAS ,Chennai.

Dr.VMaheswari She is working at Vels Institute of Science, Technology&AdvancedStudies (VISTAS) Chennai since 2017 to till date. She completedM.Sc.,M.Phil.,in Mathematics and her Ph.D. in (Graph Theory)Mathematics in ManoneManiyam Sundranar University,Tirunelveli. She has sixteen years of Teaching experience. Her research interests are Graph Labelings,Cryptography, she has published more than 15 research articles in both National and International journals. She has guided 3MPhil Scholars and is guiding 5Ph.D scholars.

Dr.V. Balaji,was born and brought up at Rajapalayam, Virudhunagar District,Tamilnadu,India.He completedM.Sc. and M.Phil. Mathematics in ANJAC College (Autonomous) Sivakasi, Virudhunagar District. He did his Ph.D. in (Graph Theory) Mathematics in ManoneManiyam Sundranar University, Tirunelveli. He has 23years of Teaching experience. He has experience both from Arts and Science; and as well as Engineering colleges. Since 2010 he is teaching at Sacred Heart Arts and Science College(Autonomous).His area of interest in Mathematics are Graph Theory and its applications. He has guided more than 5MPhil Scholars. He has completed a Minor Project from University Grants Commission.