PAPER • OPEN ACCESS

DIFFERENCE MODULO LABELING

View the article online for updates and enhancements.

DIFFERENCE MODULO LABELING

S. Rekha[*], V. Maheswari[**]

[*]Research Scholar and [**]Associate Professor

Department of Mathematics,

Vels Institute of Science Technology & Advanced Studies (VISTAS) Pallavaram, Chennai-117, Tamil Nadu-India.

Email:[*]rekhamccmcc@gmail.com [**]maheswari.sbs@velsuniv.ac.in

Abstract-- In this paper, We prove that cycle C_n is a difference modulo labeled graph. We investigate the graph P_n^2 and $C_3^{(t)}$ is a difference modulo labeling. Here, the formulated edge labeling is considered as plaintext and with the help of affine cipher, we investigate a method of encryption and decryption of a message for the system of secured communication.

Keywords: Cycle graph, affine cipher, encipher, decipher, and plaintext

2010 Mathematical subject classification Number: 05C78.

1. Introduction

"Secured" word is primarily important in all fields, especially for secured communication in digital network areas. Graph labeling is the advanced research area which used in science and technology. For the purpose of protective data transfer between the two persons, we define difference modulo labeling. By Douglas Stinson [3], affine cipher is otherwise called as mono alphabetic substitution cipher. We gained the knowledge of graph theory and cryptography by Natalia Tokareva [4]. In this article we investigate difference modulo labeling in cycle C_n, the graph P_n^2 and $C_3^{(t)}$. Also by using affine cipher we encrypt and decrypt the message for highly secured communications.

Definition 1.1: Affine cipher is similar to shift cipher. In encryption, each and every letter in plaintext will be converted as cipher text and decryption is the multiplicative inverse of mod n

Cipher Text 1.2: It is the encoded message which is displayed for the third person.

Encryption 1.3: Encryption is nothing but converting the plaintext into a coded message.

Decryption 1.4: It is the reverse process of encryption to convert the coded message into plaintext.

Main Definition 1.5 Difference Modulo Labeling: A graph $G = (V, E)$ is said to be a Difference Modulo Labeled Graph, if there exist $F: V(G) \to \{1, 2 \dots p + q\}$ and for each induced edge,

$$F^*(e) = \begin{cases} \left\lfloor \dfrac{|u_i - u_j|}{2} \right\rfloor & \text{if } |u_i - u_j| \text{ is even} \\[3mm] \left\lceil \dfrac{|u_i - u_j| + 1}{2} \right\rceil & \text{if } |u_i - u_j| \text{ is odd} \end{cases}$$

Theorem 1.6: A Cycle C_n is difference modulo labeling when n = 12.

Proof: Let us consider a cycle graph C_n with n vertices $V = (V_1, V_2, \dots V_n)$ and m edges $E = (e_1, e_2, \dots e_m).$

Define vertex label as $V{:}(C_n) \rightarrow \{1, 2 \ldots p + q\}$ by $F(u_n) = n$ and $F(u_i)$ is the divisor's of n,

Where $n = p + q \;\; (1 \leq i < n)$.

The divisor of vertex label for n=12 is,

$u_1 = 1$, $u_2 = 2$, $u_3 = 3$, $u_4 = 4$, $u_5 = 6$, $u_6 = 12$

Then by definition (1.5), the resulting edge values are

$e(u_1u_2) = e(u_2u_3) = e(u_3u_4) = e(u_4u_5) = 1$, $e(u_5u_6) = 3$ and $e(u_6u_1) = 6$.

Hence Cycle C_n is difference modulo labeling.

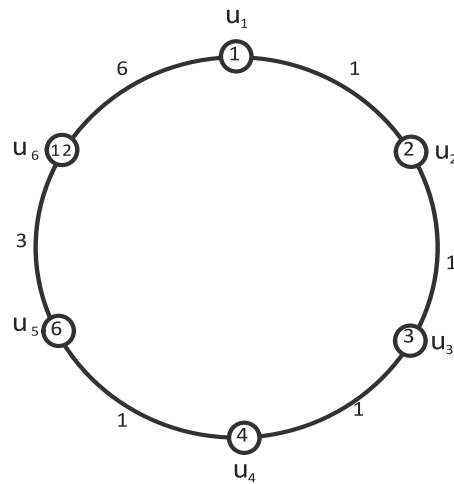Example 1.6.1 The difference modulo labeling of cycle C_{12} is given below.

Figure: 1

Fig.1: labeling of cycle

Procedure for coding and decoding:

- Let us take the appropriate Cycle graph C_n. The plaintext values are taken from the vertices u_iu_j.
- We define the vertices as $F{:} \; V(G) \rightarrow \{1, 2, \ldots p + q\}$ and fix the edge value by Difference Modulo Labeling
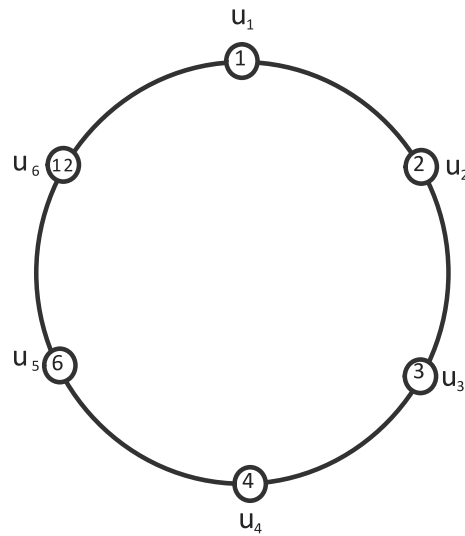
Figure: 2

Fig.2: Modulo Labeling

- Here, we consider edge label as the actual plain text.
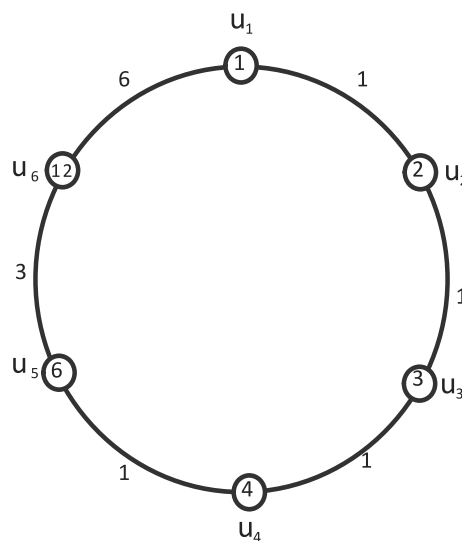

Figure: 3

Fig.3: edge label as the actual plain text

- Convert the letters A to Z into a number like A » 0, B » 1,………Z » 25.

Illustration: (Encryption)

Step: 1 Let us fix the vertices by Difference Modulo Labeling.

Step: 2 Let plaintext is formulated as P=$\left\{ \left\lceil \frac{|u_i - u_j|}{2} \right\rceil \quad \text{if } |u_i - u_j| \text{ is even} \right.$

$$\left. \frac{|u_i - u_j| + 1}{2} \right\} \text{ if } |u_i - u_j| \text{ is odd}$$

Plain Text:

1	1	1	1	3	6
B	B	B	B	D	G

Step: 3 Fix the edge labels as 1 1 1 1 3 6 and the corresponding plaintext is BBBBDG

Step: 4 Cipher text $C(X) = R(P) + N \bmod n$. Let R must be relatively prime number of n and N be the multiple of n, where $R = 5, N = 3, n = 12$ and P is the plain text ($P = X$). Substitute each value of plaintext in cipher text formula,

$$C(1) = 5\,(1) + 3 \bmod 12 = 8$$
$$C(1) = 5\,(1) + 3 \bmod 12 = 8$$
$$C(1) = 5\,(1) + 3 \bmod 12 = 8$$
$$C(1) = 5\,(1) + 3 \bmod 12 = 8$$
$$C(3) = 5\,(3) + 3 \bmod 12 = 6$$
$$C(6) = 5\,(6) + 3 \bmod 12 = 9$$

Cipher Text:

8	8	8	8	6	9
I	I	I	I	G	J

Decryption:

Decryption is the inverse method of encryption. Here, we are finding the multiplicative inverse of modulo n.

$D(X) = R^{-1}\,(C(X) - N) \bmod n$, where $R^{-1} = 5, N = 3$ and $C(X)$ is the cipher text.

Decipher Text:

8	8	8	8	6	9
B	B	B	B	D	G

Therefore our Plaintext is BBBBDG

    Cipher text is IIIIGJ

    Decipher text is BBBBDG.

Theorem 1.7: The graph P_n^2 is difference modulo labeling when n = 8.

Proof: Let us consider a graph P_n^2 with n vertices $V = (V_1, V_2, \ldots \ldots V_n)$ and m edges

$E = (e_1, e_2, \ldots \ldots e_m)$.

Define vertex label as $V: (P_n^2) \rightarrow \{1, 2 \ldots p + q\}$ by $F(u_n) = n$ and $F(u_i)$ is the divisor's

Of $n = p + q \ (1 \le i < n)$.

The divisor of vertex label for n = 8 is,

$u_1 = 1$, $u_2 = 2$, $u_3 = 4$, $u_4 = 8$.

By definition (1.5), the resulting edge values are,

$e(u_1u_2) = e(u_2u_3) = 1$, and $e(u_3u_4) = e(u_1u_3) = 2$.

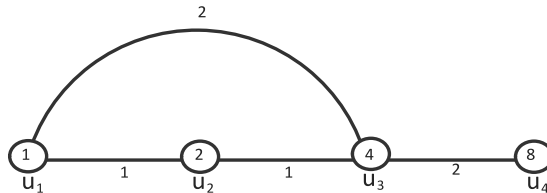Hence P_n^2 is difference modulo labeling.

Example 1.7.1:

Figure: 4

Fig.4: modulo labeling.

Procedure for coding and decoding:

- Let us take the appropriate graph P_n^2 . The plaintext values are taken from the vertices.
- We define the vertices as $F : V(G) \rightarrow \{1, 2, \dots p + q\}$ and fix the edge value by Difference Modulo Labeling.
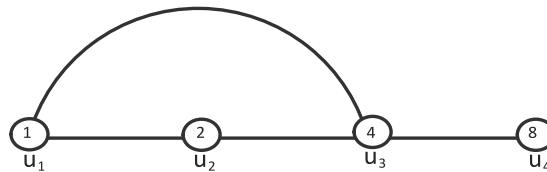

Figure: 5

Fig.5: modulo labeling.

- Here, we consider edge label as the actual plain text.
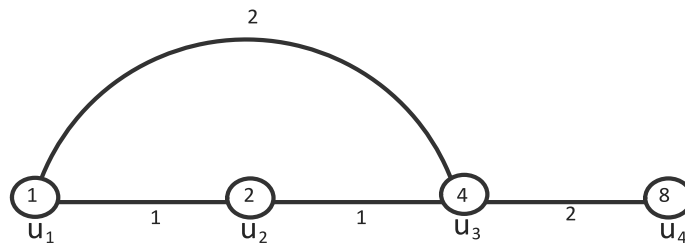
Figure: 6

Fig.6: modulo labeling.

- Convert the letters A to Z into a number like A » 0, B » 1,………Z » 25.

Illustration: (Encryption)

Step: 1 Let us fix the vertices by Difference Modulo Labeling.

Step: 2 Let plain text is formulated as P=
$$\begin{cases} \dfrac{|u_i - u_j|}{2} & \text{if } |u_i - u_j| \text{ is even} \\[2ex] \dfrac{|u_i - u_j| + 1}{2} & \text{if } |u_i - u_j| \text{ is odd} \end{cases}$$

Plain Text:

1	1	2	2
B	B	C	C

Step: 3 Fix the edge labels as 1 1 2 2 and the corresponding plaintext is BBCC

Step: 4 Cipher text $\boldsymbol{C(X) = R(P) + N \bmod n}$. Let R must be relatively prime number of n and N be the multiple of n, where $R = 5, N = 2, n = 8$ and P is the plain text $(P = X)$. Substitute each value of plaintext in cipher text formula,

$$C(1) = 5\,(1) + 2\,mod\,8 = 7$$
$$C(1) = 5\,(1) + 2\,mod\,8 = 7$$
$$C(2) = 5\,(2) + 2\,mod\,8 = 4$$
$$C(2) = 5\,(2) + 2\,mod\,8 = 4$$

Cipher Text:

7	7	4	4
H	H	E	E

Decryption:

Decryption is the inverse method of encryption. Here, we are finding the multiplicative inverse of modulo n. $\boldsymbol{D(X) = R^{-1}\,(C(X) - N)\bmod n}$, where $R^{-1} = 5, N = 2, n = 8$ and $C(X)$ is the cipher text.

Decipher Text:

1	1	2	2
B	B	C	C

Therefore our Plaintext is BBCC

          Cipher text is HHEE

        Decipher text is BBCC.

Theorem 1.8:

The graph $C_3^{(t)}$ is difference modulo labeling when n= 24.

Proof: Let us consider a graph $C_3^{(t)}$ with n vertices V= $(V_1, V_2\,,……V_n)$ and m edges

$E = (e_1, e_2, … … e_m)$.

Define vertex label as $V\,(C_3^{(t)}) \rightarrow \{1, 2\,…p + q\}$ by $F(u_n) = n$ and $F(u_i)$ is the divisor's of

n = p + q $(1 \leq i < n)$.

The divisor of vertex label for n = 24 is,

$u_1 = 1$, $u_2 = 2$, $u_3 = 3$, $u_4 = 4$, $u_5 = 6$, $u_6 = 8$, $u_7 = 12$, $u_7 = 24$

By definition (1.5) the resulting edge values are,

$e(u_1u_2) = e(u_2u_3) = e(u_3u_4) = e(u_4u_5) = e(u_5u_6) = e(u_2u_4) = 1$,

$e(u_6u_7) = e(u_4u_6) = 2$,

$e(u_7u_8) = 6$,

$e(u_8u_1) = 12$,

$e(u_2u_6) = 3$,

$e(u_4u_8) = 10$ and $e(u_6u_8) = 8$.

Therefore $C_3^{(24)}$ is a difference modulo labeled graph.

Example 1.8.1: Difference modulo labeling of graph $C_3^{(t)}$ is given below.
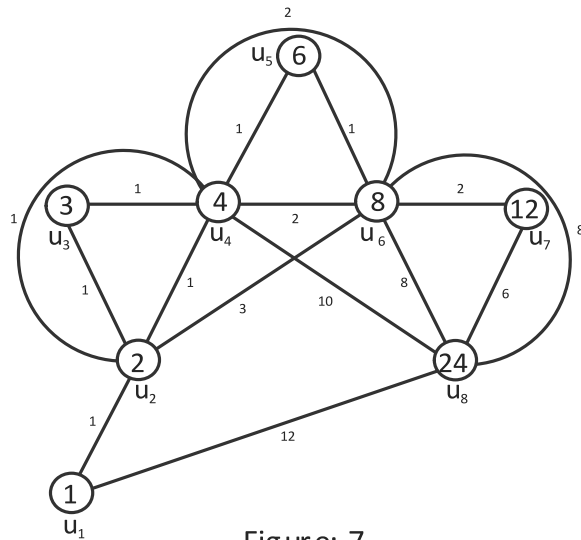

Figure: 7

Procedure for coding and decoding:

- Let us take the appropriate graph $C_3^{(t)}$. The plaintext values are taken from the vertices.
- We define the vertices as $F : V(G) \rightarrow \{1, 2, \dots p + q\}$ and fix the edge value by Difference Modulo Labeling.
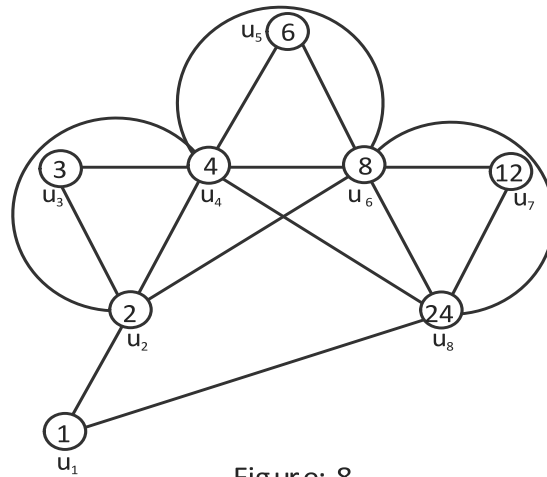
Figure: 8

- Here, we consider edge label as the actual plain text.

Figure: 9

- Convert the letters A to Z into a number like A » 0, B » 1,………Z » 25.

Illustration: (Encryption)

Step: 1 Let us fix the vertices by Difference Modulo Labeling.

Step: 2 Let plain text is formulated as P=
$$\begin{cases} \dfrac{||u_i - u_j|}{2} & \text{if } |u_i - u_j| \text{ is even} \\[2mm] \dfrac{|u_i - u_j| + 1}{2} & \text{if } |u_i - u_j| \text{ is odd} \end{cases}$$

Plain Text:

1	1	1	1	1	1	2	2	6	8	3	10	12	1	2	8
B	B	B	B	B	B	C	C	G	I	D	K	M	B	C	I

Step: 3 Fix the edge labels as 1 1 1 1 1 1 2 2 6 8 3 10 12 1 2 8 and the corresponding plaintext is BBBBBBCCGIDKMBCI.

Step: 4 Cipher text $C(X) = R(P) + N \, mod \, n.$ Let R must be relatively prime number of n and N be the multiple of n, where $R = 5, N = 4, n = 24$ and P is the plain text ($P = X$). Substitute each value of plaintext in cipher text formula,

$$C(1) = 5(1) + 4 \, mod \, 24 = 9$$
$$C(1) = 5(1) + 4 \, mod \, 24 = 9$$
$$C(1) = 5(1) + 4 \, mod \, 24 = 9$$
$$C(1) = 5(1) + 4 \, mod \, 24 = 9$$
$$C(1) = 5(1) + 4 \, mod \, 24 = 9$$
$$C(1) = 5(1) + 4 \, mod \, 24 = 9$$
$$C(2) = 5(2) + 4 \, mod \, 24 = 14$$
$$C(2) = 5(2) + 4 \, mod \, 24 = 14$$
$$C(6) = 5(6) + 4 \, mod \, 24 = 10$$
$$C(8) = 5(8) + 4 \, mod \, 24 = 20$$
$$C(3) = 5(3) + 4 \, mod \, 24 = 19$$
$$C(10) = 5(10) + 4 \, mod \, 24 = 6$$
$$C(12) = 5(12) + 4 \, mod \, 24 = 16$$
$$C(1) = 5(1) + 4 \, mod \, 24 = 9$$
$$C(2) = 5(2) + 4 \, mod \, 24 = 14$$
$$C(8) = 5(8) + 4 \, mod \, 24 = 20$$

Cipher Text:

9	9	9	9	9	9	14	14	10	20	19	6	16	9	14	20
J	J	J	J	J	J	O	O	K	U	T	G	Q	J	O	U

Decryption:

Decryption is the inverse method of encryption. Here, we are finding the multiplicative inverse of modulo n.

$D(X) = R^{-1} (C(X) - N) mod \, n$, where $R^{-1} = 5, N = 3$ and $C(X)$ is the cipher text.

Decipher Text:

1	1	1	1	1	1	2	2	6	8	3	10	12	1	2	8
B	B	B	B	B	B	C	C	G	I	D	K	M	B	C	I

Therefore our Plaintext is BBBBBBCCGIDKMBCI

Cipher text is JJJJJJOOKUTGQJOU

Decipher text BBBBBBCCGIDKMBCI.

Application 1.9:

- Affine cipher is mainly used in Digital network areas to keep the confidential mails or messages highly secured.
- By using Difference Modulo Labeling, the decryption of the message or data is cannot be able to identify by the third person or any open networks.
- It will be helpful in many industries to keep the payroll data's of employee or employers secured.

2.   Conclusion

In this paper, We have prove Difference Modulo Labeling for finite undirected graphs to keep the message or data secured by coding and decoding, because in many industries the communication signals are openly available. In further research work, we generalize this function to keep the message even more secured.

3.   References:

[1] F.Harary, Graph Theory, Addison Wesley, Reading. 1969.
[2] J.Gallian, A Dynamic Survey of Graph Labelling, The Electronic Journal of Combinatorics, 6 (2010), #DS6.
[3] Douglas Stinson, Cryptography Theory and Practice, CRC Press.
[4] Connections between graph theory and cryptography Natalia Tokareva G2C2: Graphs and Groups, Cycles and Coverings September, 2426, 2014. Novosibirsk, Russia.
[5] NHK K. ISMAIL*,"Estimation Of Reliability Of D Flip-Flops Using Mc Analysis",
Journal of VLSI Circuits And Systems 1 (01), 10-12,2019
[6] Mv Ngo Tien HoA,High Speed And Reliable Double Edge Triggered D- Flip-Flop For Memory Applications",*Journal of VLSI Circuits And Systems,* 1 (01), 13-17,2019