A hybrid fusion of symmetric encryption techniques with graph labeling

Cite as: AIP Conference Proceedings **2516**, 210050 (2022); https://doi.org/10.1063/5.0108509
Published Online: 30 November 2022

V. N. Jaya Shruthy and V. Maheswari

A Hybrid Fusion of Symmetric Encryption Techniques with Graph Labeling

V. N. Jaya Shruthy [b] and V. Maheswari [a]

Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies
Chennai - 600117, India.
[a]*Corresponding Author: maheswari.sbs@velsuniv.ac.in*
[b]*jayashruthy12@gmail.com*

Abstract. Cryptography is the science of using codes for secure transmission of information enabling the intended recipient alone to process its content thereby preventing the invention of any adversaries. The assignment of integers to the nodes and edges of graph adopting certain conditions is Graph theory. In today's world both Cryptography and Graph theory are considered inseparables in the field of promoting secure digital transactions. We here display a Hybrid fusion of two famous symmetric techniques namely Further Enhanced Cyclic Vigenere cipher and One - time pad Cipher to generate a hybrid Ciphertext passed over to the recipient as a Cipher graph. The former is a polyalphabetic Substitution Cipher whereas the latter is a Stream Cipher. To facilitate this we embrace Graceful labeling and the recipient is advance is provided with Cipher clue pertaining to Graph labeling,Trace keys and decryption key to discover the hybrid Ciphertext, original Ciphertext and eventually the required plaintext from the Cipher graph.

KEYWORDS. Further Enhanced Cyclic Vigenere Cipher, One time Pad Cipher, Superstar Tree, Graceful labeling.

2010 Mathematical Subject Classification number: 05C78

INTRODUCTION

A hybrid is a blend of two or more methodology of same or different kind to produce an offspring inheriting the qualities and properties of the parent methodologies. In symmetric encryption the same pre-defined key is shared by both the receiver and the sender for performing encryption and corresponding decryption respectively. The methodology portrayed here is a combination of Symmetric encryption namely Further Enhanced Cyclic Vigenere cipher, a substitution Cipher and One time Pad Ciphers, stream Cipher respectively. In our proposed work we explore a homo hybrid encryption process fusing the above said symmetric methodologies joining hands with Graceful labeling for enhancing data security and transfer.

LITERATURE REVIEW

The graphs considered here are finite, simple and connected. J.A. Gallian in [1] provides an insight about various labeling techniques introduced. R.C.Read in [2] details ideas on applications of Graph Theory associated with Cryptography. F.Harary [3] provides basic definitions and notations in Graph theory. From G.Uma Maheswari, G.Margaret Joan Jebarani and V.Balaji [4], coding of two star graph using Super Mean Labeling is visualized. S. Somasundaram and R. Ponraj [5] details Mean labelings of various graph. In [6] we have portrayed double encryption and decryption of secret messages using Enhanced Vigenere Cipher. In [7] we have discussed encryption using one time Pad using Graph labeling. A great source of inspiration on hybrid encryption using graph labeling is derived from our work in [8, 9]. In [9] hybrid combination of substitution and transposition ciphers both symmetric key cryptographies using two varied labeling techniques has been discussed. Indeed, our current work on combination of symmetric and asymmetric key cryptosystem is an extension of idea portrayed in it. Aized Amin Soofi, Irfan Riyaz, Umair Rasheed [10] introduces Enhanced Vigenere Cipher for security of data. Quist-Aphetsi Kester [11] and O.E.Omolara, A.I.Oludare and S.E. Abdulahi [12] details hybrid combination of various ciphers for promoting data security. R. Uma and N. Murugesan [13] showcases on graceful labeling and some of their subgraphs.

PRELIMINARIES

Definitions

Encryption

The conversion of original message into some secret form called ciphertext making use of cryptographic techniques is called encryption. The reverse process is decryption.

Plaincode

Before actual encryption the plaintext is disguised into plaincode using Cryptographic technique.

Cipher Graph

The Ciphertext is forwarded as a Graph Structure called Cipher Graph to the receiver.

Cipher Clue

The key for determining the ciphertext sequence from Cipher graph is called Cipher clue.

Graceful Labeling

Let G be a graph with n edges. A bijection g: V(T)→ {0,1, 2, ….., n} such that when each edge is assigned the label $|g(u) - g(v)|$the edge label sets is equal to$\{1,2,3,\ldots..n\}$ is called a graceful labeling of G.

Trace key

The key which traces ciphertext from the hybrid ciphertext is called the trace key.

Hybrid Encryption Algorithm

The algorithm details the steps to be performed for hybrid encryption. We assume the parent encryption techniques to be Encryption technique I and Encryption technique II abbreviated as ET- I and ET - II and the resulting Hybrid Ciphertext as HC.

Step 1. Process the given Plaintext through ET - I. Here ET - I is our Symmetric Encryption technique namely FECV Cipher. The ciphertext obtained is CT - I.

Step 2. Process the ciphertext CT - I obtained from ET - I through ET - II. Here ET - II is our symmetric Encryption technique namely One- time pad. The resulting ciphertext obtained is CT - II.

Step 3. The Resulting Hybrid ciphertext HC is obtained as a zig - zag combination of CT - I elements $e_{i,k}$ and CT - II elements $d_{j,k}$ using the relation using the relation $e_{i,2n-1}\, d_{j,2n}$ where i = 1; j = 2 ; k = 1, 2,…..n recursively.

Step 4. Represent the resulting Hybrid ciphertext HC as a Cipher graph adopting the prescribed labeling to the receiver. Here we use Graceful Labeling.

Step 5. The cipher text is identified from Hybrid ciphertext HC with the aid of trace key which in turn undergoes decryption yielding the required plaintext.

Plan of Work

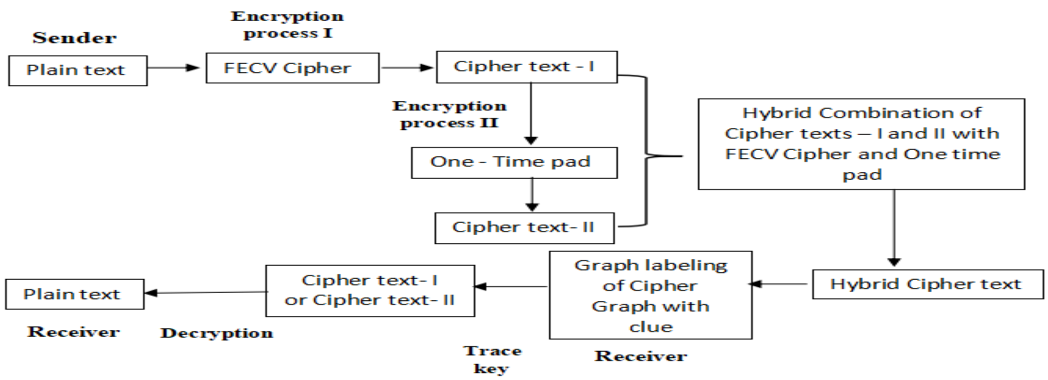


FIGURE 1. Plan of Work

FURTHER ENHANCED CYCLIC VIGENERE CIPHER (FECV Cipher)

The Vigenere Cipher is a poly alphabetic substitution cipher which uses a table of alphabets called the v square to encrypt plaintext using a series of interwoven Caesar Ciphers with the aid of key. Enhanced Vigenere Cipher depicted in [10] is an extension of this Cipher and we in [7] have followed a cyclic pattern and further enhanced its properties to suit its nomenclature Further Enhanced Cyclic Vigenere Cipher abbreviated as FECV Cipher. In [7] FECV Cipher with ten Reference Tables implementing cyclic encryption pattern with P_i (plaintext) and C_i (Ciphertext) values follows from i^{th} reference table and its corresponding K_i (key value) follows it +1 th reference table and we proceed likewise. Encryption Formula for Further Enhanced Cyclic Vigenere Cipher for plaintext encryption is $C_i\,[t_i] = (P_i\,[t_i] + K_i\,[t_{i+1}])\ (\text{mod } 26)$ where i = 1 to 10. The corresponding Decryption Formula for obtaining plaintext from ciphertext using FECV Cipher is as follows $P_i\,[t_i] = (C_i\,[t_i] - K_i\,[t_{i+1}])\ (\text{mod } 26)$ where i = 1 to 10.

TABLE 1. FECV Cipher table

Ref. tab no.	0	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
t_1	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
t_2	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
t_3	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
t_4	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
t_5	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
t_6	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
t_7	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
t_8	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
t_9	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
t_{10}	t	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

Encryption Formula for Further Enhanced Cyclic Vigenere Cipher for plaintext encryption is $C_i [t_i] = (P_i [t_i] + K_i [t_{i+1}])$ (mod 26) where i = 1 to 10. The corresponding Decryption Formula for obtaining plaintext from ciphertext using FECV Cipher is as follows $P_i [t_i] = (C_i [t_i] - K_i [t_{i+1}])$ (mod 26) where i = 1 to 10.

One -Time Pads

Miller in 1882 introduced the One - Time pad which was further improved by Gilbert Vernam and Joseph Mauborgne provides an ideal methodology to promote secure data transmission.

TABLE 2. Example of One -Time Pad Out Sheet which has to be destroyed after use

OUT 001			
61424	20419	86546	00517
90222	27993	04952	66762
50349	71146	97668	86523
85676	10005	08216	25906
024291	19761	15370	43882
90519	61988	40164	15815
20631	88967	19660	89624
89990	78733	16447	27932

A One - Time Pad consists of single sheet or booklet containing truly random digits which is bestowed as a IN Pad to the receiver and an OUT Pad from the sender. For OTP encryption the ciphertext letters are generated by combining each plaincode generated from plaintext with a random key stream using addition modulo 10. For general rules and description one can refer [7].

Generation of Plaincode from plaintext

Before the encryption process the receiver is handed over in advance the One - Time Pad to be used. Mere conversion of the plaintext into plaincode alone does not provide any message security and the plaincode has to undergo proper encryption process to guarantee ultimate security.

TABLE 3. Alphabet -to- digits Conversion Table

Character	a	b	c	d	e	f	g	h	i	j	k	l	m
Digit Entry	26	01	25	02	24	03	23	04	22	05	21	06	20

n	o	p	q	r	s	t	u	v	w	x	y	z
07	19	08	18	09	17	10	16	11	15	12	14	13

OTP Encryption

The plaincode as such does not provide message security and we have to process it through the encryption process. The plaincode is converted to ciphertext by adding the plaincode digits with the OTP Key digits by Modulo 10.

ILLUSTRATION

Encryption Process I - FECV Cipher

Let our Plaintext be**: earth is our treasure** and let keyword be **save water**.

TABLE 4. FECV Ciphertext obtained from Encryption process 1

Plain text (P_i)	e (3)	a (23)	r (12)	t (12)	h (24)	i (23)	s (5)	o (25)	u (3)	r (24)	t (18)	r (14)	e (25)	a (19)	s (9)	u (9)	r (4)	e (15)
Key (K_i)	s (15)	a (21)	v (14)	e (21)	w (11)	a (13)	t (4)	e (13)	r (24)	s (17)	a (23)	v (16)	e (23)	w (13)	a (15)	t (6)	e (15)	r (0)
$P_i + K_i$ (mod 26) (Ref. Table)	t_1+t_2 = 18 (mod 26) =18	t_2+t_3 = 44 (mod 26) =18	t_3+t_4 = 26 (mod 26) = 0	t_4+t_5 = 33 (mod 26) = 7	t_5+t_6 = 35 (mod 26) = 9	t_6+t_7 = 36 (mod 26) = 10	t_7+t_8 = 9 (mod 26) = 9	t_8+t_9 = 38 (mod 26) = 12	t_9+t_{10} = 27 (mod 26) =1	$t_{10}+t_1$ = 41 (mod 26) =15	t_1+t_2 = 41 (mod 26) =15	t_2+t_3 = 30 (mod 26) = 4	t_3+t_4 = 48 (mod 26) = 22	t_4+t_5 = 32 (mod 26) = 6	t_5+t_6 = 24 (mod 26) = 24	t_6+t_7 = 15 (mod 26) = 15	t_7+t_8 = 19 (mod 26 = 19	t_8+t_9 = 15 (mod 26) = 15
C_i (Ref. Table)	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{10}	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8
FECV Cipher	t	v	f	o	s	v	w	b	s	i	q	h	b	n	h	a	g	e

From "Table 4", the FECV ciphertext I is obtained as**: tvfosvwbsiqhbnhage** by applying $C_i [t_i] = (P_i [t_i] + K_i [t_{i+1}])$ (mod 26).

Encryption Process II using One - Time Pad

For Encryption process II using One - Time pad this ciphertext I**: tvfosvwbsiqhbnhage** becomes our plaintext. We convert this plaintext**: tvfosvwbsiqhbnhage** to plaincode before our Encryption process with random digits using addition modulo 10 to produce the ciphertext II. The corresponding plaincode using "Table 3" is given by **10 11 03 19 17 11 15 01 17 22 18 04 01 20 04 26 23 24.** Here we take the 5 - digit random numbers from "Table 2" in groups of two and add with the corresponding two-digit plaincode as depicted in "Table 6". The first value of OTP key in "Table 5" indicates the OTP sheet. Thus, the ciphertext II is obtained as **03 52 91 74 53 11 66 70 19 44 35 93 31 69 56 82 99 49.**

TABLE 5. Ciphertext II obtained from one time pad cipher

Plaincode	**KEYID**	10	11	03	19	17	11	15	01	17	22	18	04	01	20	04	26	23	24
OTP key	61424	20	41	98	65	46	00	51	79	02	22	27	99	30	49	52	66	76	25
Ciphertext	61424	03	52	91	74	53	11	66	70	19	44	35	93	31	69	56	82	99	49

Hybrid Production

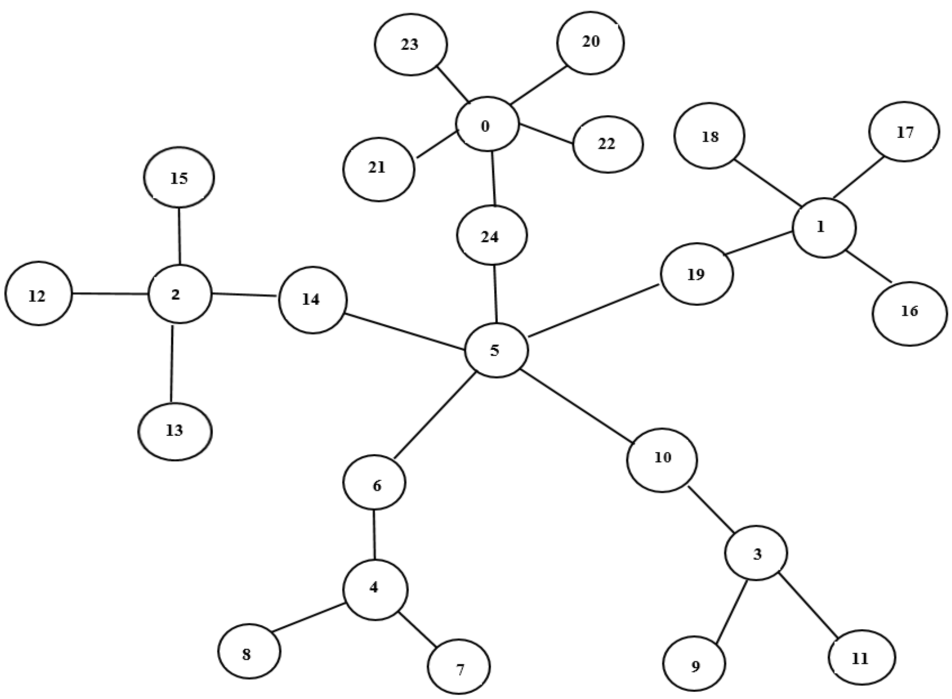
Our hybrid is now a fusion of FECV Ciphertext and One time pad Cipher in a zig – zag pattern using the relation $e_{i,2n-1}\, d_{j,2n}$ where i = 1; j = 2 ; n = 1, 2,…..13 recursively. The hybrid ciphertext is obtained as **18 52 00 74 09 11 09 70 01 44 15 93 22 69 24 82 19 49** as shown in "Table 6".

TABLE 6. Hybrid Ciphertext

FECV Cipher ($e_{i,k}$)	18	18	00	07	09	10	09	12	01	15	15	04	22	06	24	15	19	15
One time pad Cipher ($d_{i,k}$)	03	52	91	74	**53**	11	66	70	19	44	35	93	31	69	56	82	99	49
Hybrid Ciphertext	18	52	00	74	09	11	09	70	01	44	15	93	22	69	24	82	19	49

Cipher graph - Message to the receiver

The hybrid Ciphertext is forwarded to the receiver as a Cipher graph which the receiver in turn guesses with the aid of clue provided.



Cipher clue : E(1,19) E(5,10) E(4,6) V_0 V_0 E(3,10) E(4,8) V_0E(5,14) E(2,13) V_0 E(5,14) E(3,10)V_0 E(5,6) E(4,8) E(4,8) E(1,16) E(5,14) E(4,7)E(0,22) E(3,9) E(5,14) E(0,24) E(3,11) E(4,6) E(5,24) E(4,8) E(5,14)

FIGURE 2. Cipher graph - Superstar Tree forwarded to the receiver

The receiver applies graceful labeling to the Superstar tree in “Fig.2” and determines the edge labeling with the above clue provided. Only a few edges labels are utilized and the remaining edges are considered dummy which is purposely done in order to confuse any intruder. The final Superstar graph with their corresponding edges is depicted in “Fig.3”.

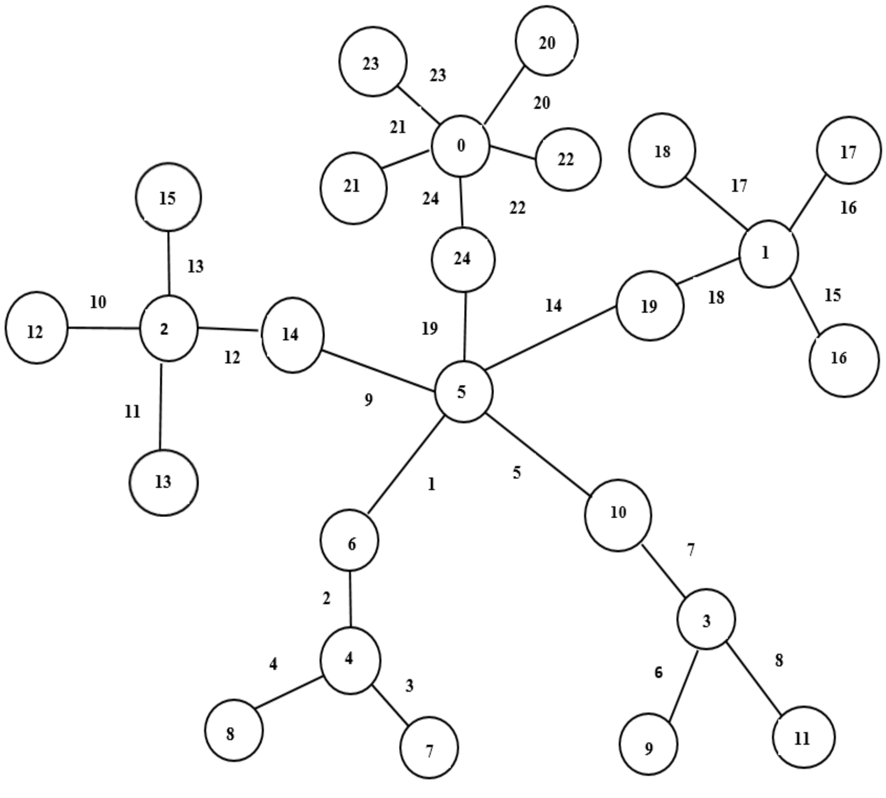


FIGURE 3. Superstar tree showing edge labels through Graceful Labeling

Identification of hybrid Ciphertext

Here E (i,j) denotes the edge labels connecting the vertices (i, j) and v_i refers to the i^{th} vertex .Using Graceful labeling the hybrid ciphertext sequence in blocks of two are : **18 52 00 74 09 11 09 70 01 44 15 93 00 69 24 82 19 49.**

Trace key I

The ciphertext I is obtained from hybrid ciphertext by making use of Trace key I: **- 18 - 07 - 10 - 12 - 15 - 04 - 06 - 15 -15**. By making use of **Trace key II: 03 - 91 - 53 - 66 - 19 - 35 - 31- 56 - 99 -** we can also use track **Ciphertext II: 03 52 91 74 53 11 66 70 19 44 35 93 31 69 56 82 99 49.**

TABLE 7. Extraction of Ciphertext from Hybrid text

Hybrid Ciphertext	18	52	00	74	09	11	09	70	01	44	15	93	22	69	24	82	19	49
Trace key I	-	18	-	07	-	10	-	12	-	15	-	04	-	06	-	15	-	15
Ciphertext I	18	18	00	07	09	10	09	12	01	15	15	04	22	06	24	15	19	15

FECV Decryption

The ciphertext I subjected to FECV decryption using **$P_i [t_i] = (C_i [t_i] - K_i [t_{i+1}])$ (mod 26)** where i = 1 to 10 yields the original plaintext***:* earth is our treasure.**

TABLE 8. Decryption using FECV Cipher

FECV Cipher (C_i)	t (18)	v (18)	f (0)	o (7)	s (9)	v (10)	w (9)	b (12)	s (1)	i (15)	q (15)	h (4)	b (22)	n (6)	h (24)	a (15)	g (19)	e (15)
Key (K_i)	s (15)	a (21)	v (14)	e (21)	w (11)	a (13)	t (4)	e (13)	r (24)	s (17)	a (23)	v (16)	e (23)	w (13)	a (15)	t (6)	e (15)	r (0)
$C_i - K_i$ (mod 26) (Ref. Table)	$t_1 - t_2$ (mod 26) = 3	$t_2 - t_3$ (mod 26) = 23	$t_3 - t_4$ (mod 26) = 12	$t_4 - t_5$ (mod 26) = 12	$t_5 - t_6$ (mod 26) = 24	$t_6 - t_7$ (mod 26) = 23	$t_7 - t_8$ (mod 26) = 5	$t_8 - t_9$ (mod 26) = 25	$t_9 - t_{10}$ (mod 26) = 3	$t_{10} - t_1$ (mod 26) = 24	$t_1 - t_2$ (mod 26) = 18	$t_2 - t_3$ (mod 26) = 14	$t_3 - t_4$ (mod 26) = 25	$t_4 - t_5$ (mod 26) = 19	$t_5 - t_6$ (mod 26) = 9	$t_6 - t_7$ (mod 26) = 9	$t_7 - t_8$ (mod 26) = 4	$t_8 - t_9$ (mod 26) = 15
C_i (Ref. Table)	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{10}	t_1	t_2	t_3	t_4	t_5	t_6	t_7	t_8
Plaintext (P_i)	e	a	r	t	h	i	s	o	u	r	t	r	e	a	s	u	r	e

CONCLUSION

Thus, a hybrid encryption methodology using FECV Cipher and One- Time pad along with graph labeling technique has been presented here. Further studies can be carried on this versatile schema of encryption detailed above using other labeling techniques which certainly ensures confidentiality, non - repudiation, reliable and secure transfer of data which is the need of the hour.

REFERENCES

1. J. A. Gallian, *E - JC*, 18 (2016), #DS6.
2. R.C. Read, *Computer Math Application,* 34, (1997), pp.121- 127.
3. F. Harary, Graph Theory, *Addison - Wesley, Reading*, Massachusetts (1969).
4. G. Uma Maheswari, G. Margaret Joan Jebarani and V. Balaji, *Applied Mathematics and Scientific Computing* (2019), pp.469- 478.
5. S. Somasundaram and R. Ponraj,*National Academy of Science letters*, 26,(2003),pp.210 -213.
6. V.N. Jaya Shruthy and V. Maheswari, *IJRTE*, 8, (2019), pp.76 - 81.
7. V.N. Jaya Shruthy and V. Maheswari, *JPCS*, 1362 (2019) 012023, (2019), pp.1-7.
8. V.N. Jaya Shruthy and V. Maheswari, *IJAEMA*, XI, ISSN NO.0886 – 9367 (2019).
9. V.N. Jaya Shruthy and V. Maheswari, *TWMS J. of Appl. and Eng. Math.*,11, (2021), pp.154 -163.
10. Aized Amin Soofi, Irfan Riyaz, Umair Rasheed, *IJSR*, 5, Issue 03, ISSN 2277- 8616 (2016).
11. Quist-Aphetsi Kester, *IJATER*, Vol 3, Issue 1 (2013), pp.141-147.
12. O.E. Omolara, A.I. Oludare and S.E. Abdulahi, *IISTE*, 5 (2014), pp.34-46.
13. R. Uma, N. Murugesan, *Asian Journal of Current Engineering and Maths*, 6, (2012), pp.367-370.