An Improved Encryption Process using One-Time Pad Together With Graph Labeling

Jaya Shruthy V. N., V. Maheswari

***Abstract:** In this Research paper we discuss the encryption technique of secret messages using One -Time Pad encryption technique accompanied with Graph Labeling. Theoretically the One - Time Pads (OTPs) are recognized as the truly unbreakable Ciphers as messages are encrypted with unique keys based on randomness thereby paving no way to "Crack the Code" when applied properly. Though OTPs have their own limitations the efficiency of this Cipher can be improved by maintaining the utmost secrecy of the ciphering key and destroying it immediately after its implementation. To add a feather to its features the encryption procedure through One -Time Pads can be further enhanced by joining hands with Graph labeling Technique. The resulting Ciphertext is represented as a Cipher Graph which is passed over to the receiver. We apply Harmonious labeling technique to this Cipher graph which together with the clue reveals the Ciphertext and the corresponding decryption yields the plaintext back. Thus cryptography clubbed with Graph Labeling technique provides absolute security of message transmission*

***Keywords:** Encryption, Plaincode, Decryption, One-time Pad, Harmonious Labeling, Cipher key, Cipher Graph, Fan Graph, Cycle Graph, Friendship Graph, Cipher Clue.*

I. INTRODUCTION

Cryptography is the method of protecting and concealing communications by making use of codes so that only the intended persons can read and process it. In today's world cryptography finds its place in many field especially for transactions of payment, electronic mail etc. Cryptography touches on many disciplines including Mathematics, Engineering and Computer Science. Graph labeling is the assignment of integers to the vertices or edges or both subject to certain conditions. Few Research work combining Graph Theory with Cryptography are in progress which will definitely prove to be an indispensable tool for many innovations and ideas in the near future. In this paper we promote we establish encryption using One-Time Pad Cipher which is considered as the Unbreakable Cipher or True Cipher together with Graph labeling. We present our Ciphertext after encryption in the form of a Cipher Graph and for this we consider Harmonious labeling Technique and with the aid of Cipher clue the receiver is able to retrieve back the plaintext.

II. LITERATURE REVIEW

In paper [3], [4] and [5] Harmonious labeling techniques on various Graph structures and some of their properties have been studied. [6], [7] and [8] showcases new methodology and researches involved in encryption techniques using One-Time Pads, its uses, drawbacks etc. For some basic terminologies on Graph labeling we refer [1]. In [2] our work on double encryption process using Graph labeling through enhanced Vigenere Cipher Technique encouraged us to carry out some more research in this area with slight variations and our current work is one among them. Further from [9] the idea of introduction of Cipher Graphs to transmit secret message to the receiver has greatly motivated our current work in connection with Graph Labeling.

III. DEFINITIONS

A. Encryption

The process of converting the intended message called the plaintext into some secret form called the Ciphertext by making use of cryptographic techniques so that only authorized persons able to access it.

B. Plaincode

The process of transforming the plaintext into a non-readable form using some cryptographic technique to maintain its secrecy before actual encryption process is termed as the plaincode.

C. Decryption

The reverse mechanism of converting Ciphertext back to plaintext is called decryption.

D. Cipher Key

The key which is used to perform encryption and its corresponding decryption is called Cipher key.

E. Cipher Graph

The Ciphertext is passed to the receiver in the form of a Graph Structure called Cipher Graph.

F. Harmonious Labeling

Let G be a graph with q edges. A function g defined by g (uv = e) = (g(u) + g(v)) mod q is called Harmonious if g:V→{0,1,2,….q-1}is injective and g: E→{0,1,2,….q}.

Revised Manuscript Received on December 05, 2019.
***** Correspondence Author

Jaya Shruthy V. N., Department of Mathematics. Vels Institute of Science, Technology and Advanced Sciences (VISTAS), Pallavaram ,Chennai -117, Tamilnadu, India. Email: jayashruthy12@gmail.com

V. Maheswari, Department of Mathematics. Vels Institute of Science, Technology and Advanced Sciences (VISTAS), Pallavaram ,Chennai -117, Tamilnadu, India. Email:maheswari.sbs@velsuniv.ac.in

G. Friendship Graph

A friendship Graph F_n is a graph obtained by connecting n triangles to a common vertex.

H. Fan Graph

The fan Graph is a graph obtained by connecting all the vertices of P_n to a central vertex and contains n +1 vertices and 2n -1 edges denoted by $f_n = P_n + K_{1.}$

I. Cycle Graph

The Cycle Graph C_n with n vertices is a graph structure in which the number of edges equals the number of vertices and every vertices has two edges incident with it.

J. Cipher Clue

It is the clue provided to the receiver to determine the Ciphertext from the Cipher graph.

IV. PLAN OF WORK

The plan of work is as follows. We first encrypt our plaintext by adopt any of the two techniques of One –Time Pad encryption namely

(i) Using Conversion table

(ii) Using Code book

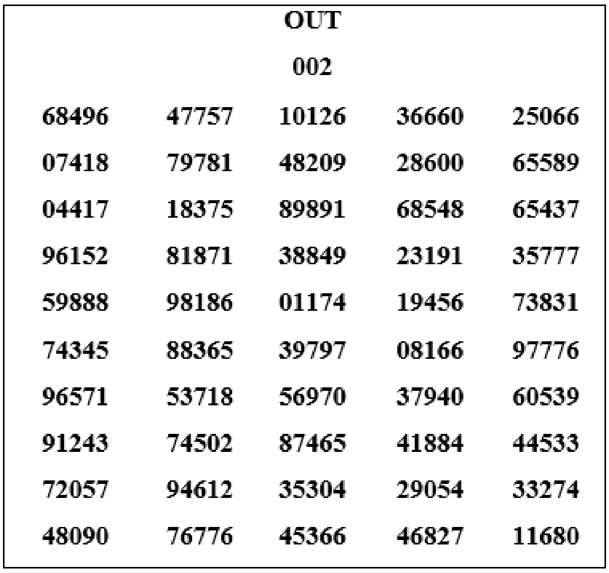
The resulting Ciphertext is then represented in the form of a Cipher Graph. We make use of Harmonious Labeling to the Cipher Graph along with a clue to identify our Ciphertext which on decryption yields the required plaintext.

V.THE ONE –TIME PAD

The one time pad was originally described by Frank Miller in the year 1882 but its reinvention credit goes to Gilbert Vernam and Joseph Mauborgne. One - time pad encryption is a simple yet perfect methodology to obtain security of message transmission. It is a Symmetric Key Encryption technique and the key used for performing One- Time encryption is termed as One-Time Pad. Two identical One Time Pads called the IN pad and OUT pad comprise a One-Time Pad set which can be either a single sheet, an entire strip of paper tape or a booklet consisting of truly random digits. The receiver possesses the IN pad and the sender the OUT pad respectively. The One Time Pad abbreviated as OTP is an encryption process in which every plaintext character is combined with a character generated from a random key stream to produce the Ciphertext characters. In Mathematical terms it can be recognized as an equation with two unknowns which is unsolvable.

The main idea on which One-Time Pad functions is that both the sender and the receiver have the same pre-defined key at their disposal which is wiped out instantly after its usage. The plaintext characters are added to the elements of OTP using modulo addition 10 creating Ciphertext that has no connection with the plaintext. The encryption key should comprises of truly random numbers and must be of the same length as the plaintext.

Table -I: Example of a One –Time Pad Out Sheet which has to be destroyed after use



		OUT		
		002		
68496	47757	10126	36660	25066
07418	79781	48209	28600	65589
04417	18375	89891	68548	65437
96152	81871	38849	23191	35777
59888	98186	01174	19456	73831
74345	88365	39797	08166	97776
96571	53718	56970	37940	60539
91243	74502	87465	41884	44533
72057	94612	35304	29054	33274
48090	76776	45366	46827	11680

The Golden rules to be adhered to while applying One -Time Pad Technique are as follows

(i) Only two copies of One - Time Pad should exist which should be immediately destroyed after use.

(ii) The OTP should consist of a series of truly random digits.

(iii) The OTP key should be of the same length as the plaintext or if possible longer than the plaintext.

(iv) New sheets of OTP should be used for encryption of new messages to avoid the risk of simultaneous use of repeated OTPs.

An OTP sheet consists of 5 - digit numbers arranged in rows and columns taken from the Table of random numbers and the top of the sheet contains the Serial number of the OTP sheet.

IV. TABLE OF RANDOM NUMBER

A random number table is a series of 5 – digit number from 0 to 9 randomly distributed in rows and columns. These random numbers are placed in such a way that they have no relation with either the predecessor or the successor numbers in the table. There are various methods for generating random numbers. A typical random number table may extend upto 4 or 5 pages.

V. THE CODE BOOK

The code book is an optional way of converting the plaintext into plaincode thereby reducing the transmission time considerably in case of long plaintext messages. It can be used with or without the aid of encryption through Standard Conversion table detailed below. The receiver should also possess same copy of code book. We can also create our own code book according to the plaintext content which is sent to the receiver before handed. We can assume space to be 99 and also give values for symbols or letters if required.

Table - II: An example of a Code -book

Code - Letters 884-UNABLE TO	Code -Letters 521 - FIX	Code -Letters 801 -TODAY
208- COORDINATE	574 - ROOM	999- BY ORDER
321- AT MEETING	602 -REPORT	686-RECEIVE
673 -FUNCTION	442 - NEED	985-COME
498 - FIND	794 -SUPPORT	1101-EVENING
514- MONEY	110 - GET	1472 -AND

VI. CONVERSION OF PLAINTEXT TO PLAINCODE

Before starting the encryption process the receiver must be informed well in advance which One – Time Pad is used. The plaintext must be converted into a series of digits called the Plain code by using a Checkerboard. There are various Checkerboards available for conversion of plaintext but we use the checkerboard which is optimized for English Language. 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 -III: The Standard English character -to- digits Conversion Table

CODE 0	A 1	E 2	I 3	N 4	O 5	T 6	Conversion Table – 1 English		
B 70	C 71	D 72	F 73	G 74	H 75	J 76	K 77	L 78	M 79
P 80	Q 81	R 82	S 83	U 84	V 85	W 86	X 87	Y 88	Z 89
FIG 90	(.) 91	(;) 92	(') 93	( ) 94	(+) 95	(-) 96	(=) 97	REQ 98	SPC 99

Table-III provides the character -to -digits conversion table of the English alphabets where **CODE 99 (SPC**) refers to space, **CODE 98 (REQ)** indicates question mark and numeric values are represented three times and are preceded and succeeded by the **CODE 90 (FIG).**

VII. OTP ENCRYPTION

The plaincode as such does not provide message security and we have to process it through the encryption process by adding the

Table IV: OTP Encryption of Plaincode to Ciphertext

Plaincode	KEYID	73383	75997	5879	5559	3499	85378	78190	77790
OTP key	68496	47757	10126	36660	25066	7418	79781	48209	28600
Ciphertex t	68496	10030	85013	31439	20515	807	54059	16399	95390

Have to process it through the encryption process by adding the

Plaincode with the cipher key (OTP Key) and applying mod10.The plaincode is then divided into groups of five. The OTP Key by choice

from the table of random numbers is then chosen depending on the plaincode digits. The first group of the OTP Key serves as the key indicator indicating which One –Time Pad sheet is used. This first group should not be added with the plaincode but as it only serves for the purpose of identification. Before encryption the plaincode is then

divided into groups of five. The last group of the plaincode is completed by adding full stops (.) if necessary. Thus our plaincode gets converted to Ciphertext by the addition of plaincode digits with the OTP Key digits by Modulo 10.

VIII. CIPHER GRAPH

We represent our Ciphertext in the form of Cipher Graph from which the receiver determines the Edge labels using the labeling scheme adopted. With the help of Cipher clue the Ciphertext is determined from some of the edge labels which on decryption gives the plaintext. The Cipher Graphs which we present here are a combination of two Graph structures admitting Harmonic labeling. We can also present any number of Graph structures as combination graphs. Here our combination graphs includes Graph Structures namely Cycle Graph, Friendship Graph, Fan Graph admitting Harmonious labeling from [3].Different Graph structures for a variety of labeling technique can also be tried upon.

IX. CIPHER CLUE

The Cipher clue is used to identify the Ciphertext from the edge labels which is provided to the receiver along with Cipher Key. It contains vital information which includes certain abbreviations or hints regarding the graph structures used, vertex (edge) connectivity etc.

X. OTP DECRYPTION

The OTP decryption is the reverse of encryption process in which the ciphertext is subtracted from the OTP Key using mod 10 to obtain the plaintext. As the resulting plaintext is divided into groups of 5 the identification of the original message becomes quite confusing. To avoid this confusion if the resulting numeric values are within the range of 1 to 6 count it as a single entry whereas if the digit exceeds 6 consider it as double digit entry together with the next immediate digit.

Also numeric values are represented three times preceded and succeeded with 90 and 99 indicates space between the words.

XI. ILLUSTRATION- 1

A. One -Time Pad Encryption Using Conversion Table

Let our **Plaintext: FISH BOX 5 IN VILLA 7**

Converting the Plaintext to Plaincode using Table -III we get **Plaincode: 7338375 99 70587 90 555 90 34 99 85378781 90 777 90**

Here 73 indicates **F**, 3 indicates **I**, 83 indicates **S**, 75 indicates **H**, 99 refers to **space** and numeric value **5** is written as **90 555 90** and so.

We divide the plaincode into groups of five for encryption as follows and adding the Plaincode with OTP Key using Modulo 10 we arrive

at the Ciphertext which is sent to the receiver in the form of Cipher Graph

B. Representation of Ciphertext as Cipher Graph

From the Cipher Graph the receiver determines the Ciphertext with the help of Cipher Clue which on decryption yields the plaintext. Our Cipher Graph is a combination of Cycle Graph and Friendship Graph

to which the receiver applies Harmonious Labeling (Cipher key) to find the edge labels. From [3] it follows that both **C_{11}** and **F_4** are Harmonious.

C_{11} F_4

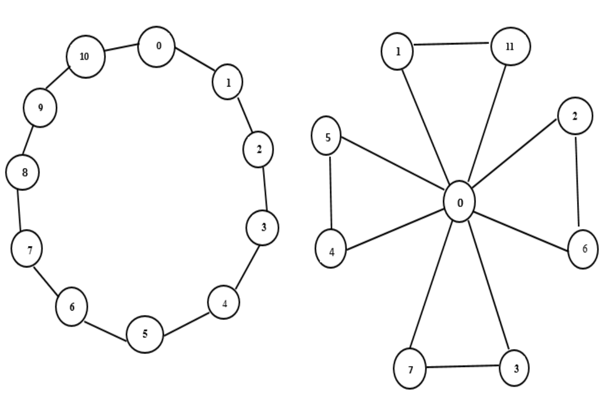
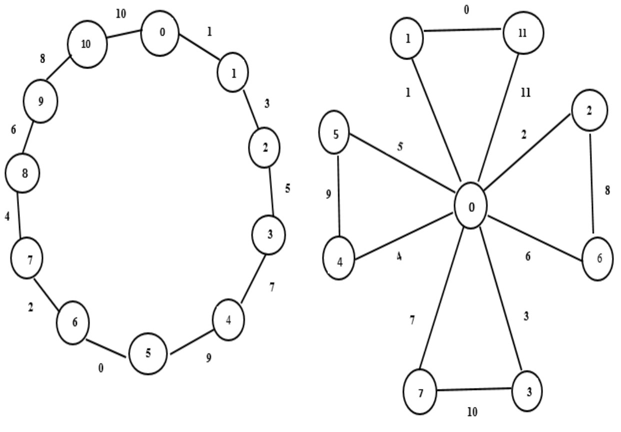


Figure 1: Combination of C_{11} and F_4 as Cipher graph message to the receiver

C. Cipher key



C_{11} F_4

Figure 2: Finding the Edge Labels for the Cipher Graph using Harmonious labeling

Our Cipher key is Harmonious labeling together with the clue to determine the Ciphertext. Any other labeling technique for different Graph structures also serve as the Cipher key.

D. Cipher Clue

With the help of Cipher Clue provided, the receiver determines the Ciphertext from the Cipher Graph.

Table V: Cipher Clue

$F^{0,6}C^{9,10}F^{0,4}C^{4,5}F^{0,6}$	$C^{0,1}F^{1,11}C^{5,6}F^{0,3}C^{5,6}$	$F^{2,6}C^{2,3}F^{1,11}C^{0,1}F^{0,3}$
$C^{1,2}F^{0,1}C^{7,8}F^{0,3}C^{4,5}$	$F^{0,2}C^{5,6}F^{0,5}C^{0,1}F^{0,5}$	$C^{5,6}F^{1,11}C^{9,10}F^{1,11}C^{4,3}$
$F^{0,5}C^{7,8}F^{1,11}C^{2,3}F^{4,5}$	$C^{0,1}F^{0,6}C^{1,2}F^{4,5}C^{4,5}$	$F^{4,5}C^{2,3}F^{0,3}C^{4,5}F^{1,11}$

Here $C^{i,j}$ stands for Cycle and $F^{i,j}$ stands for Fan where (i, j) determines the edge label joining i and j for using Harmonious labeling Technique.

Thus the Ciphertext corresponding to the edge labels are as follows:

Table VI: Conversion of Cipher clue to Ciphertext

68496	10030	85013	31439	20515
00807	54059	16399	95390	

E. One – time Pad Decryption

Subtracting the Ciphertext from the OTP Key using Modulo 10 we get the Plaincode.

Table VII: OTP decryption of Ciphertext to plaincode

Ciphertext:	68496	10030	85013	31439	20515	00807	54059	16399	95390
OTP key	68496	47757	10126	36660	25066	07418	79781	48209	28600
Plaincode	KEYID	73383	75997	05879	05559	03499	85378	78190	77790

Converting the Plaincode to Plaintext using Table 3 we get back our plaintext.

Here the first Plaincode value is 7 (greater than 6) and hence it has to be counted as a double digit 73 (along with the next digit 3) and it refers to **F,** the next digit is3 (less than 6) counted as a single digit indicating **I,** 99 refers to **space** , 90 555 90 refers to numeric value **5** and so on.

Thus our **Plaintext** is **FISH BOX 5 IN VILLA 7**

XII. ILLUSTRATION – 2

A. One -Time Pad Encryption using Code Book

Let our **Plaintext: UNABLE TO RECEIVE MONEY AND COORDINATE SUPPORT**

Converting the Plaintext to Plaincode using Code book values from Table II we get

Plaincode: 884 99 686 99 514 99 1472 99 208 99 794

Here 884 refers to **UNABLE TO,** 99 refers to **space,** 686refers to **RECEIVE** and so on.

We divide the plaincode into groups of five as follows and adding the Plaincode with OTP Key using Modulo 10 we arrive at the Ciphertext.

Table VIII: OTP Encryption of Plaincode to Ciphertext

Plaincode	KEYID	88499	68699	51499	14729	92089	97949
OTP key	*	92904	19478	62743	75792	95310	31348
Ciphertext	*	70393	77067	13132	89411	87399	28287

Here * denotes the first group of the OTP sheet which is known to the receiver. This Ciphertext is sent to the receiver in the form of Cipher Graph. The receiver identifies the Ciphertext with the clue which on decryption gives the plaintext.

B. Representation of Ciphertext as Cipher Graph

Fan Graph f_8 and Friendship Graph $F_4$are harmonious by [2].Our Cipher Graph is a combination of Fan Graph and Friendship Graph is the Cipher message to which the receiver applies Harmonious Labeling to find the edge labels with the help of Cipher clue

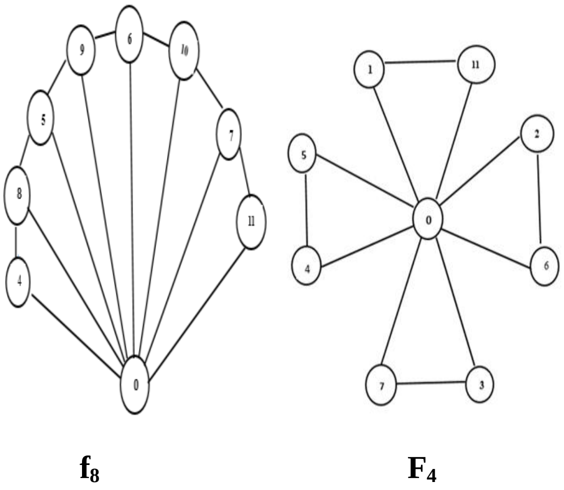


Figure 3: Combination of f8 and F4 as Cipher graph message to the receiver

C. Cipher Key

Our Cipher key is Harmonious labeling together with the clue to determine the Ciphertext. Using Harmonious Labeling we find the edge labels for the Cipher Graph.

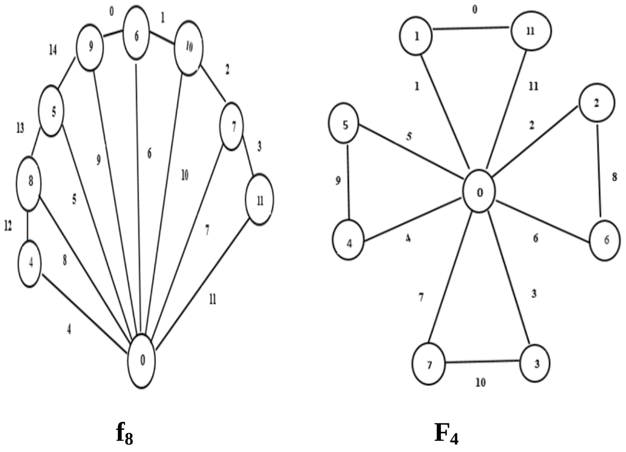


Figure 4: Finding the Edge Labels for the Cipher Graph using Harmonious Labeling

D. Cipher Clue to the receiver

With the help of Cipher Clue provided to the receiver we determine the ciphertext.

Table IX: Showing Cipher Clue

*	$f^{0,7}F^{1,11}f^{7,11}F^{5,4}f^{7,11}$	$F^{0,7}f^{0,7}F^{1,11}f^{0,6}F^{0,7}$	$f^{6,10}F^{0,3}f^{6,10}F^{0,3}f^{10,7}$	$F^{2,6}f^{0,9}F^{0,4}f^{6,10}F^{0,1}$
	$f^{0,8}F^{0,7}f^{7,11}F^{5,4}f^{0,9}$	$F^{0,2}f^{0,8}F^{0,2}f^{0,8}F^{0,7}$		

Here $f^{i,j}$ stands for Fan Graph and $F^{i,j}$ stands for Friendship Graph where (i, j) determines the edge label joining i and j using Harmonious Labeling.Thus from the edge labels the ciphertext obtained is as follows

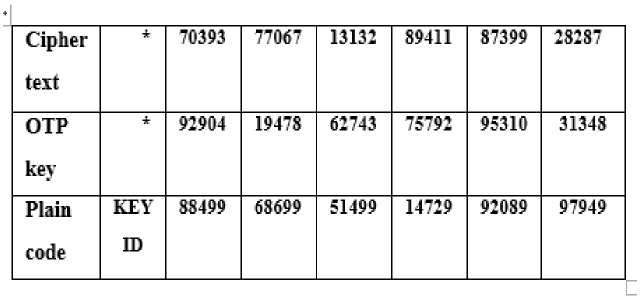
Table X: OTP Decryption of Ciphertext to plaincode

*	70393	77067	13132	89411	87399	28287

E. One - time Pad Decryption

The plaincode is obtained by subtracting the Ciphertext from the OTP Key using Modulo 10.

Table XI: OTP Decryption of Ciphertext to plaincode



Cipher text	*	70393	77067	13132	89411	87399	28287
OTP key	*	92904	19478	62743	75792	95310	31348
Plain code	KEY ID	88499	68699	51499	14729	92089	97949

Converting the Plaincode to Plaintext using Table. II we get back our required plaintext.

As our code book consists of 3 digits and 4 digit code for each letter we identify our plaintext by easily splitting the 3 or 4 digits separated by space 99.

Thus we get our required **Plaintext: UNABLE TO RECEIVE MONEY AND COORDINATE SUPPORT**

XIV. CONCLUSION

In this paper an entirely different encryption concept making use of Graph Labeling technique has been emphasized. Thus OTP Encryption combined together with Graph labeling ensures both data security as well as the usage of Code Book reduces the computational time to a desired extent thereby attaining the chief goal of Cryptography. A lot of research can be pursued from the above suggested methodology by admitting various Graph labeling techniques to different Graph forms thereby promoting secure message transactions.

REFERENCES

1. J. A. Gallian, “A Dynamic Survey of Graph Labeling”, Electronic Journal of Combinatorics (2018).
2. V.N. Jaya Shruthy, V.Maheswari, “Double Encryption, Decryption Process Graph Labeling through Enhanced Vigenere Cipher”, Journal of Physics: Conference Series, 1362 (2019)012023.
3. Dushyant Tanna, “Harmonious Labeling of certain Graphs”, International Journal of Advanced Engineering Research and Studies/II/IV/July – September 2013, 46-48.
4. R.L. Graham and N.J.A Sloane, “On Additive Bases and Harmonious Graphs”,SIAM, J.Alg,Disc.Meth.1,(1980), 382- 404.
5. P.Selvaraju, P.Balaganesan, J.Renuka, M.L.Suresh, “Harmonious and vertex Graceful Labeling on path and Star related Graphs”, International Journal of Pure and Applied Mathematics, Vol.93, No.4, 2014, 501-509.
6. Sumathi.R, N.R. Raajan, “A Secured approach for cryptography using multilevel encryption”, International Journal of Pure and Applied Mathematics, Vol.119, No.12, 2018, 16613-16621.
7. Dirk Rijmenants, “The Complete Guide to Secure Communication with the One- time Pad Cipher”, Cipher Machines and Cryptology,2009-2018,Ed.7.5-June 11,2018.
8. Shachi Sharma, Vinita Gupta ,“Encryption and Decryption using One -time pad algorithm in MAC Layer”, International Journal of Innovative Research in Science , Engineering and Technology ,Vol-2, Issue 6,June 2013,2248-2250.
9. Devipriya.M, Sasikala.G, “A new technique for One Time Pad Security scheme with complement method”, International Journal of Advanced Research in Computer Science and Software Engineering,Vol-5, Issue 6,June 2015,220 -223.
10. Jaya Shruthy V.N, V.Maheswari, “A Hybrid Perspective of Symmetric Encryption through Labeling for Union of Two Star Graphs”, International Journal of Analytical and Experimental Modal Analysis, Volume XI, ISSN NO.0886-9367, October 2019,104 -114.

AUTHORS PROFILE

V.N. Jaya Shruthy, Research Scholar, Department of Mathematics, Vels Institute of Science , Technology and Advanced Sciences (VISTAS), Pallavaram , Chennai -117,Tamilnadu,India .She continues her career in Sindhi Arts and Science College, Chennai as an Assistant Professor in Mathematics since 2012 to till date. She has ten years of Teaching Experience. Her Research interests are Graph Labeling and Cryptography. She has published research articles in both National and International journals. She is currently pursuing her Ph.D. Under the Guidance of **Dr. V. Maheswari** in VISTAS, Chennai.

Dr. V. Maheswari She is working at Vels Institute of Science, Technology& Advanced Studies (VISTAS) Chennai since 2017 to till date. She completed M.Sc., M.Phil., in Mathematics and her Ph.D. in (Graph Theory) Mathematics in Manone Maniyam Sundranar University, Tirunelveli. She has sixteen years of Teaching experience. Her research interests are Graph Labeling, 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.