TWMS J. App. and Eng. Math. V. 11, Special Issue, 2021, pp. 154-163

A HYBRID COMBINATION OF SUBSTITUTION AND TRANSPOSITION CIPHERS FOR EFFICIENT ENCRYPTION USING GRAPH LABELING

V. N. JAYA SHRUTHY[1], V. MAHESWARI[1], §

Abstract. In this study, we conceptualise a hybrid approach of plaintext encryption by making use of Substitution and Transposition cipher technique namely Playfair Cipher and Simple Columnar Transposition. Both the Ciphers are Symmetric Encryption Technique and the need for developing such a hybrid is to inherit the positive traits as well as restrict certain limitations of both the techniques to a considerable extent. The resulting hybrid text is further subjected to Graph Labeling Technique as the receiver receives the ciphertext in the form of a Graph structure together with a clue to determine the type of labeling used and the ciphertext sequence. Here we adopt two varied labeling techniques namely Simply Sequentially Additive labeling and Distance two labeling for some Tree related Graphs and the corresponding Decryption of the Cipher Graph yields the desired plaintext.

Keywords: Playfair Cipher, Simple Columnar transposition, Hybrid text, Simply Sequentially Additive labeling, Distance Two labeling, Cipher Graph.

AMS Subject Classification: 05C78.

1. Introduction

The science and art of transforming messages thereby making them immune to brute attack making use of encryption and decryption techniques is termed as Cryptography. Various forms of cryptography came soon after the widespread development of computer and telecommunications. Based on the types of keys used the Cryptographic algorithm are classified asSecret key cryptography and Public key Cryptography. Secret Key Cryptography also known as Symmetric encryption employs a single key for encryption and decryption whereas Public Key Cryptography also known as Asymmetric encryption uses different keys for both encryption and decryption. Symmetric encryption are further classified into substitution ciphers and transposition ciphers based on the encryption technique used.

As the name suggests a Substitution cipher substitutes or replaces the plaintext letters with other character, letters or symbols to form the Ciphertext whereas the transposition cipher rearranges or jumbles the position of the plaintext letters to form a Ciphertext.

[1] Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies, Chennai, 600117, India.
e-mail: jayashruthy12@gmail.com; ORCID: https://orcid.org/0000-0002-2265-1045.
e-mail: maheswari.sbs@velsuniv.ac.in; ORCID: https://orcid.org/0000-0002-7268-9420.

§ Manuscript received: October 14, 2019; accepted: April 02, 2020.
TWMS Journal of Applied and Engineering Mathematics, Vol.11, Special Issue © Işık University, Department of Mathematics 2021; all rights reserved.

In this paper we present a hybrid methodology of encrypting the plaintext by making use of both Substitution and Transposition Cipher technique. A Hybrid is a combination of two or more techniques blended to yield a further improved technique which encompasses the properties of the parent Cipher techniques. A hybrid which merges two or more methodology of same components or techniques with different features is termed as homogeneous hybrid and that which combines two entirely varied components or techniques with different features is a heterogeneous hybrid. The purpose for developing such a hybrid is to inherit the positive traits thereby restricting certain limitations of both the techniques considerably.In a substitution cipher letters with low frequency occurrence tends to reveal the plaintext wherein the letters close to the key might disclose the plaintext in case of transposition cipher.Here we deal with hetero hybrid as our plaintext is initially subjected to Playfair cipher which is a substitution cipher and the obtained Ciphertext is further processed through Simple Columnar transposition which is a transposition cipher. Thus the hybrid Ciphertext created is an amalgamation of a substitution and a transposition Cipher embracing their advantages and devouring major disadvantages.

An assignment of integers to the vertices or edges or both subject to certain conditions are called is termed as Graph Labeling. We discuss about two Graph labeling technique in our proposed work namely Simply Sequentially Additive Labeling (SSA Labeling) also known as 1- Sequentially Labeling and Distance two labeling for tree related Graph structures.

1.1. **Literature review.** Various modifications and advancements in Playfair Cipher techniques have been insighted in [1, 2, 4].The paper [3, 5] surveys Playfair Cipher and its variants. Columnar transposition technique with further improvements have been discussed in [10]. In [7] and [8] Simply Sequentially Additive labeling of some tree Graph structures have been discussed. [6] discusses Distance Two labeling of some cycle related Graphs. In [9] we have discussed about the Hybrid approach of Symmetric encryption using Super Mean Labeling and introduction of trace keys for easy decryption in place of traditional methods. Motivated by the work we now present a further improved hybrid methodology combining substitution and transposition ciphers for efficient encryption producing a Cipher Graph and also adopt trace key for easy decryption.

1.2. **Definitions.**

1.2.1. *Simply Sequentially Additive labelling.* A k- Sequentially Additive labeling f of a Graph $G(V, E)$ with vertex V and edge G is a bijection from $V \cup E$ to $\{k, k+1, k+2, \ldots k+|V \cup E|-1\}$ such that $f(xy) = f(x) + f(y)$ for $xy \in E$. The graph $G(V, E)$ is said to be Simply Sequentially additive if $k = 1$ or 1- Sequentially additive abbreviated as SSA labeling.

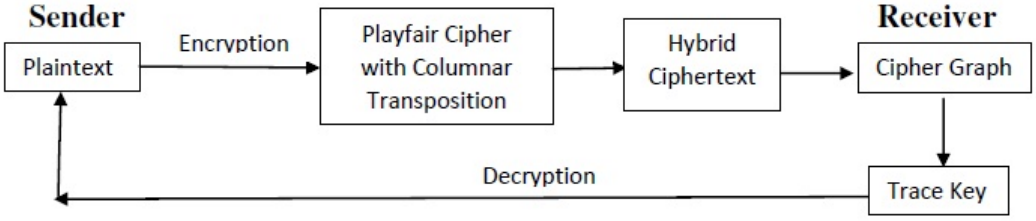
1.2.2. *Distance Two Labeling.* A Distance two labeling of a Graph G is a function f from the vertex set to the set of all non - negative integer such that $|f(x) - f(y)| \geq 2$ if $d(x, y) = 1$ and $|f(x) - f(y)| \geq 1$ if $d(x, y) = 2$ such that $d(x, y) + |f(x) - f(y)| \geq 3$.

1.2.3. *Trace Keys.* The keys which trace some data from the source key for easy decryption are called Trace Keys. They are used by the receiver for easy manipulation of the plaintext from the ciphertext.

1.2.4. *Tree.* A connected Acyclic Graph is a tree.

1.2.5. *Caterpillar.* A tree in which all the vertices are within distance 1 from the central path is a caterpillar.

1.3. **Plan of Work.**



1.4. **Encryption Process.**

1.4.1. *6 × 6 Playfair Cipher.* Playfair Cipher is a digraph Substitution Block Encryption Cipher technique which uses the same key for both encryption and decryption. The Playfair Cipher is a Block Cipher which encrypts several plaintext characters at a stretch creating a group of Ciphertext. It is termed a digraph as it operates on 2 characters at time for encryption and decryption.The cryptanalysis of Playfair Cipher is possible but much more difficult than normal Substitution Cipher because they make use of digraphs (pairs of letters) instead of monographs (single letter).The major advantage of Playfair Cipher is that the frequency analysis has to undergo $26 \times 26 = 676$ digraphs rather than 26 letters of the English alphabets as in the case of monoalphabetic or polyalphabetic substitution Ciphers.

1.4.2. *Methodology of 6 × 6 Playfair Cipher.* The traditional Playfair cipher is a 5×5 matrix and many variants have been introduced since its inception. In our work we adopt a 6×6 matrix consisting of English alphabets together with numbers 0 to 9. Our plaintext is an alphanumeric statement. The key should not exceed $6 \times 6 = 36$ words probably with no repeating characters. Let us illustrate the working of our 6×6 Playfair Cipher with an example as detailed.

The following rules have to be followed for key insertion and encryption of Playfair Cipher using 6×6 matrix

(1) The blank spaces has to be removed from the key and remove the repeating letters if any present in the key.
(2) Insert the key word at the beginning of the matrix followed by the set of the characters in 6×6 matrix not present in the key.
(3) Divide the plaintext into digraphs (pair of letters)such that it contains distinct characters and we adhere to the following steps for plaintext encryption

a. If the two characters of the digraph occupies the same row of the matrix then substitute them with the corresponding characters that are located on the right of them.
b. If the two characters of the digraph occupies the same column of the matrix then substitute them with the corresponding characters that are located below them.
c. If the two characters of the digraph does not occupy the same column or row of the matrix but occupies different positions of the matrix then replace the original characters by the corresponding characters that occurs diagonally opposite to them in the matrix enclosed by them.
d. The order of the characters in the digraph and ciphertext characters must be preserved.

1.4.3. *Simple Columnar Transposition.* The Columnar Transposition is an encryption methodology in which the Ciphertext is produced by rearranging the order or shuffling the plaintext characters following some pattern. Thus a permutation of plaintext characters is our Ciphertext. In Mathematical terms, the encryption is performed using an objective

function which determines the order of the characters and its corresponding inverse function performes the decryption. There are two types of Columnar Transposition namely Regular and Irregular Columnar transposition. In Regular Columnar Transposition the column lengths are equal or made equal by adding buffer character at the end of the plaintext. In Irregular Columnar Transposition the plaintext characters are filled as it without the insertion of Buffer Character at the end to make the column length balanced. Here we employ irregular Columnar Transposition without the inclusion of Buffer Characters. The transposition Cipher technique merely rearranges the order of the plaintext and hence is relatively easier to break when compared to their counterpart namely substitution Cipher. Hence our hybrid which is a combination of the two would indeed result in a very secure cipher technique. We use the Ciphertext obtained through Playfair as our plaintext for columnar transposition.

1.4.4. *Designing the Hybrid text.* We follow a Zig-Zag combination of Ciphertext characters of the Substitution and Transposition Ciphers namely Playfair and Columnar Transpositions Ciphers for designing our hybrid. Any other pattern of combination can also be implemented for effective designing of the hybrid. The hybrid is designed in such a way that repetition of ciphertext characters are minimized to make graph labeling technique more effective.

1.4.5. *Numbering of alphabets- Odd Multiples Numbered First.* We number the alphabets and numerals as per Odd Multiples Numbered First in which the odd positioned alphabets and numerals are numbered first in the order 1, 2, 3... after which the numbering is reversed to the even positioned alphabets.

Table 1. Odd Multiples Numbered First

a	b	c	d	e	f	g	h	i	j	k	l	m
1	36	2	35	3	34	4	33	5	32	6	31	7
n	o	p	q	r	s	t	u	v	w	x	y	z
30	8	29	9	28	10	27	11	26	12	25	13	24
0	1	2	3	4	5	6	7	8	9			
14	23	15	22	16	21	16	20	18	19			

1.4.6. *Message to the Receiver - Cipher Graph.* We now represent the hybrid text in the form a Graph which we call as a Cipher Graph. This Cipher Graph is sent to the receiver accompanied with a Clue to determine the Edge labels and the hybrid text sequence and Trace Key to determine the playfair Ciphertext.

1.5. **Illustration 1.**

1.5.1. *Playfair Cipher.* Let our Plaintext be: 123 plant a tree
Key: earth
Divide the plaintext into digraphs

1 2	3 p	1 a	n t	a t	r e	e x

Here "x" serves the duplicate character so that a digraph contains no repeating character and also as the buffer character to make the digraph complete. Our 6×6 Playfair cipher takes the following form

TABLE 2. 6 × 6 Playfair Cipher with alphabets and numerals

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

Hence the required ciphertext after Playfair encryption is

2	3	9	x	s	d	v	g	r	h	t	a	q	b

1.5.2. *Columnar Transposition.* We apply columnar transposition for our plaintext: 239xs-dvgrhtaqb

Let our Keyword be: end

The ordering of the alphabets for the keyword is 231.

Applying columnar transposition for the keyword

TABLE 3. Simple Columnar Transposition

e(2)	n(3)	d(1)
2	3	9
x	s	d
v	g	r
h	t	a
q	b	

Our ciphertext using Columnar transposition is 9dra2xvhq3sgtb

1.5.3. *Designing the Hybrid Text.*

TABLE 4. Hybrid text obtained through Playfair and columnar Transposition

Playfair Ciphertext	**2**	**3**	**9**	**x**	**s**	**d**	**v**	**g**	**r**	**h**	**t**	**a**	**q**	**b**
Columnar transposition Ciphertext	**9**	**d**	**r**	**a**	**2**	**x**	**v**	**h**	**q**	**3**	**s**	**g**	**t**	**b**
Hybrid Ciphertext	**2**	**d**	**9**	**a**	**s**	**x**	**v**	**h**	**r**	**3**	**t**	**g**	**q**	**b**

The Hybrid text is: 2d9asxvhr3tgqb

1.5.4. *Numbering the Alphabets.* For the Hybrid text: 2d9asxvhr3tgqb the corresponding numbering obtained through Odd multiples numbered first is 15, 35, 19, 1, 10, 25, 33, 28, 22, 27, 4, 9, 36. These numbers are to be guessed by receiver which is sent in the form of Cipher Graph to the receiver accompanied with a clue with the help of which the receiver the determines the hybrid text and eventually the plaintext.

1.5.5. *Cipher Message to the Receiver.* We consider a caterpillar Graph with a given set of vertices and determine the edge labels by applying Simply Sequentially Additive labeling to determine the hybrid text. Clue: SSAL with ($e_{2,4}$-1), ($e_{2,9}$), v_1, v_2, ($e_{2,1}$), ($e_{1,5}$), ($e_{1,6}$), ($e_{2,8}$), ($e_{2,6}$-1), ($e_{1,2}$), ($e_{1,7}$), $v_{1,3}$, ($e_{2,1}$-1), ($e_{2,10}$-1) where $e_{i,j}$ refers to the edge labels, $v_{i,j}$ denotes the vertices, v_1, v_2 denotes the vertex on the common path.

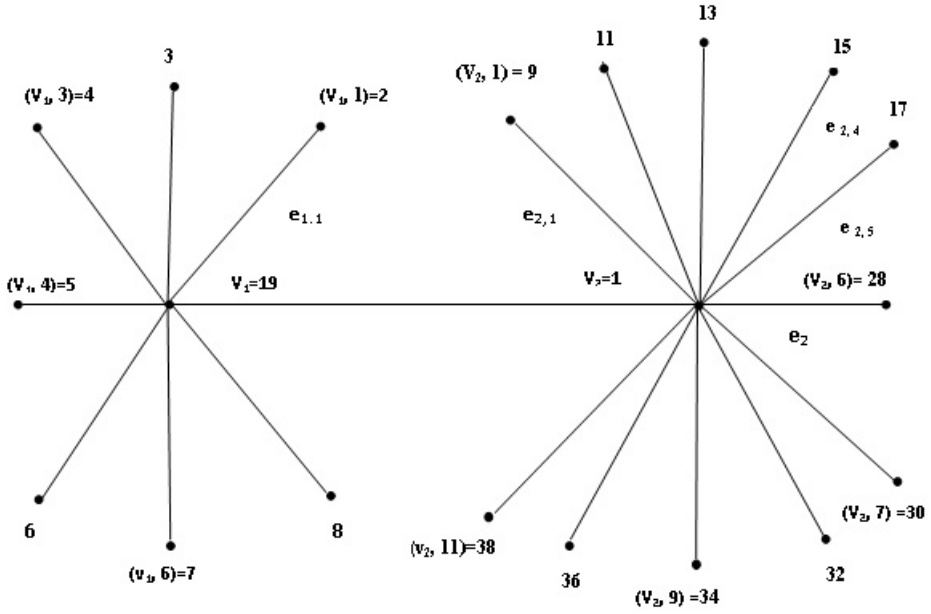


FIGURE 1. Cipher Graph to the Receiver - Caterpillar

The receiver identifies the edge labels using the clue SSAL which signifies Simply Sequentially Additive labeling $f(xy = e) = f(x) + f(y)$ and finds the ($e_{2,4}$-1), ($e_{2,9}$), v_1, v_2, ($e_{2,1}$), ($e_{1,5}$), ($e_{1,6}$), ($e_{2,8}$), ($e_{2,6}$-1), ($e_{1,2}$), ($e_{1,7}$), $v_{1,3}$, ($e_{2,1}$-1), ($e_{2,10}$-1) corresponding edge labels with the help of vertices given.

1.5.6. *Determination of edge labels by the receiver.* Our Cipher Graph adheres to SSA Labeling and not all the egde labels of the Cipher Graph are utilised but we only need to identify the specified labels in the given order. Using SSAL we identify the value for the edge labels as 15, 35, 19, 1, 10, 25, 26, 33, 28, 22, 27, 4, 9, 36 and their corresponding position as 2d9asxvhr3tgqb.

1.5.7. *Trace Key 1.* Applying Trace key technique using Trace key 1: - 3 - x - d - g - h - a - - as in [9] we get the playfair ciphertext as 239xsdvgrhtaqb. For more detailed explanation of trace key technique we refer [9]. The trace key reduces the burden of long decryption process. Deciphering the Cipher text without trace key technique can also be performed.

1.5.8. *Playfair decryption.* The decryption of the Playfair Ciphertext yields the original plaintext 123 plant a tree.

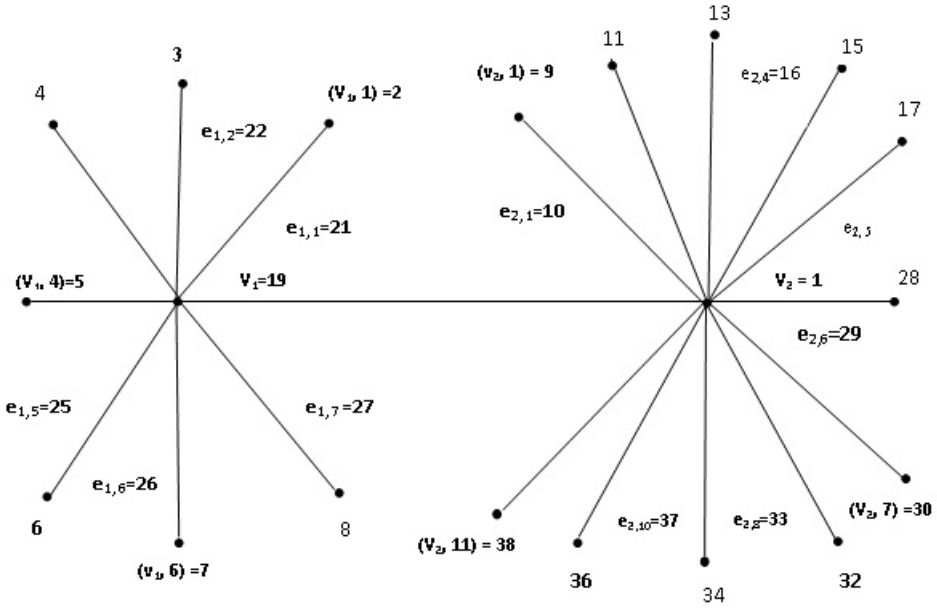


FIGURE 2. Cipher Graph with edge labels determined by the receiver

1.6. **Illustration 2.** We illustrate the plaintext encryption for our hybrid methodology using distance two labeling for a tree.

1.6.1. *6 × 6 Playfair Cipher.* Let our plaintext be rainbow49

The corresponding Digraph is:

r	a	i	n	b	o	w	4	9	x

Let us choose the Playfair Cipher Key to be: fineday

TABLE 5. Playfair Cipher

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

Encryption of the plaintext using Playfair Cipher yields our Ciphertext as : fwnelg9r34

1.6.2. *Columnar Transposition.* We now apply Columnar Transposition for the playfair ciphertext with Key: 132

The columnar Transposition Ciphertext in given by fe94ng3wlr.

1.6.3. *Producing the Hybrid.* We select the hybrid text in a zig-zag combination in such a way that no letters are repeated as follows

TABLE 6. Simple Columnar Transposition

1	3	2
f	w	n
e	l	g
9	r	3
4		

TABLE 7. Hybrid text obtained through Playfair and columnar Transposition

PlayfairCiphertext	**f**	**w**	**n**	**e**	**l**	**g**	**9**	**r**	**3**	**4**
Columnar transposition Ciphertext	**f**	**e**	**9**	**4**	**n**	**g**	**3**	**w**	**l**	**r**
Hybrid text	**f**	**e**	**n**	**4**	**l**	**g**	**9**	**w**	**3**	**r**

1.6.4. *Numbering the alphabets of the ciphertext.* Hybrid text value corresponding to Table 4

f	e	n	4	l	g	9	w	3	r
34	3	30	16	31	4	19	12	1	22

1.6.5. *Message to the receiver - Cipher Graph.* The Cipher Graph is sent to the receiver with the vertex labeling and the receiver's job is to find the edge labels and the order of the ciphertext sequence. Here we apply Distance two labeling which by definition implies function f from the vertex set to the set of all non-negative integer such that $|f(x) - f(y)| \geq 2$ if $d(x, y) = 1$ and $|f(x) - f(y)| \geq 1$ if $d(x, y) = 2$. This means that if $d(x, y) = 1$ which in our context refers to distance of the source node x from the adjacent vertex with unit distance apart has edge label greater than 2 i.e., $|f(x) - f(y)| \geq 2$ and if the distance of the source node from all the corresponding non adjacent vertex is 2 i.e., if $d(x, y) = 2$ then the edge label is greater than 1 such that $d(x, y) + |f(x) - f(y)| \geq 3$ in both the cases. Our source node here is 34 and 3 and 16 are the adjacent vertices with distance 1 unit apart whereas all other vertices from 34 are assigned distance 2 apart.

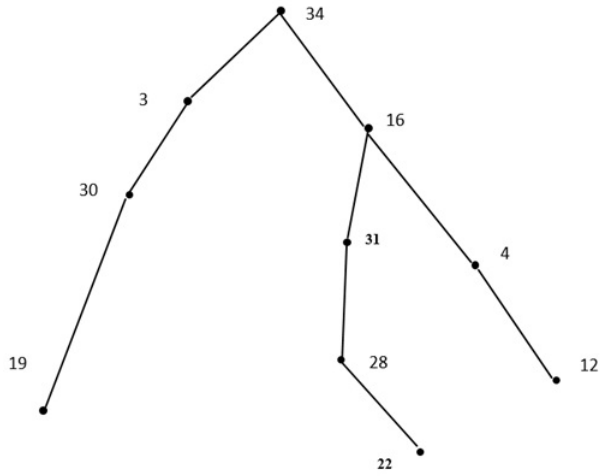


FIGURE 3. Cipher Graph - Tree

Clue: D2L decreasing from head to tail with trace key 2

From the the clue provided the receiver guesses the labeling type and calculates the edge values and determines the ciphertext.

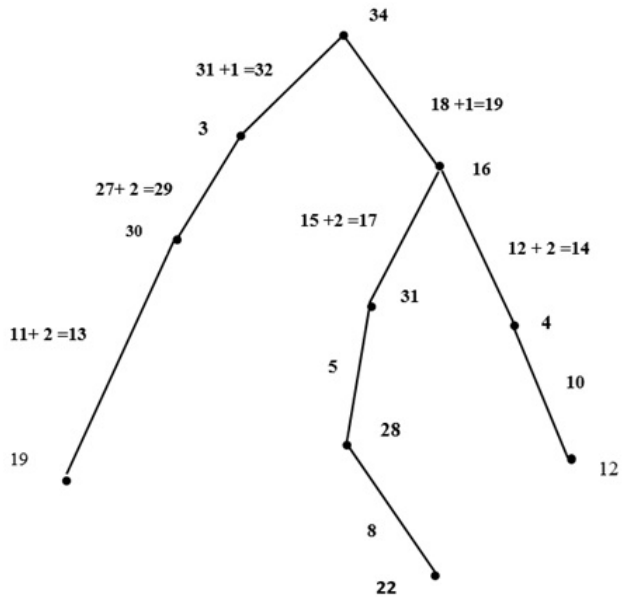


FIGURE 4. Cipher Graph with edge labels determined by the receiver

1.6.6. *Determination of the edge Labels by the receiver.* Using distance 2 labeling we get the ciphertext sequence based on the decreasing order of the edge labels starting from source node 34 as 32, 29, 19, 17, 14, 13, 9, 8, 5. The corresponding vertex labels from head (Source) to tail (terminal nodes) are 34, 3, 30, 16, 31, 4, 19, 12, 22, 28.
From Table 4 the receiver notes the hybrid text to be fen4lg9w3r

1.6.7. *Trace Key 2.* Applying Trace key technique using Trace key 2: - w - e - - - r - 4 as in [9] we get the Playfair ciphertext as fwnelg9r34. For more detailed explanation of trace key technique we refer [9]. The trace Key reduces the burden of long decryption process. Deciphering the Ciphertext without trace Key technique can also be performed.

1.6.8. *Playfair Decryption.* The decryption of the Playfair Ciphertext fwnelg9r34 yields the plaintext rainbow49x. As x is a buffer to complete the digraph omitting x the required plaintext is rainbow49.

2. Conclusion

Thus we have promoted a new hybrid approach of Encryption using Playfair Cipher and Columnar Transposition using two Graph labeling techniques thereby combining both Cryptography and Graph Labeling concept for Secure Communication. Further the introduction of Trace Keys for decryption paves a way to revolutionarize the age old decryption techniques. More labeling techniques with varied Ciphers can be adopted for further innovations.

References

[1] Aftab Alam, A., Shah Khalid, B., and Muhammad Salam, C. (2013), A Modified version of playfair Cipher using 7 × 4 matrix. International Journal of Computer Science and Engineering, 5(4).

[2] Gaurav Shrivastava, Manoj Chauhan and Manoj Dhawan, (2013), A Modified version of extended Playfair Cipher (8 × 8). International Journal of Engineering and Computer Science, 2(4), pp. 956-961.

[3] Deepthi, R., (2017), A Survey paper on Playfair cipher and its variants. International Research Journal of Engineering and Technolgy (IRJET), 4(4).

[4] Salman A. Khan, (2015), Design and Analysis of Playfair Ciphers with Different Matrix sizes. International Journal of Computing and Networking Technology, (3).

[5] Mohammed Haris and Bhavya Alankar, (2017), A survey paper on different modifications of Playfair cipher. International Journal of Advanced Research in Computer Science, 8(5).

[6] Baby Smitha, K. M. and Thirusangu, K., (2016), Distance two labeling Of Cycle related Graphs. International Journal of Pure and Applied Mathematical Sciences, 9(2), pp. 299-312.

[7] Manimekalai, K., Baskar Babujee, J. and Thirusangu, K., (2012), Simply Sequentially Additive Labeling of some special Trees. Applied Mathematical Sciences, 6(131), pp. 6501-6514.

[8] Bonge, D. W., Barkauskas, A. E. and Slater, P. J., (1983), Sequentially Additive Graphs. Discrete Mathematics, North-Holland Publishing Company, 44, pp. 235-241.

[9] Jaya Shruthy, V. N. and Maheswari, V., (2019), A Hybrid Perspective of Symmetric Encryption Through Graph Labeling for Union of Two Star Graphs. The International Journal of Analytical and Experimental Modal Analysis, XI(X).

[10] Gaurav Shrivastava, Ravindra Sharma and Manorama Chouhan, (2013), Using letters Frequency in Caesar Cipher with Double Columnar Transposition Technique. International Journal of Engineering Sciences & Research Technology.

V. N. Jaya Shruthy graduated from Madras University, Chennai, India, in 2005. She received her M.Sc and M.Phil Degree from Madras Universtiy in the year 2007 & 2009 respectively. She is pursuing PhD under the guidance of Dr. V. Maheswari, Department of Mathematics, Vels Institute of Science, Technology and Advanced Sciences (VISTAS), Chennai, India and has worked as assistant professor in mathematics, Sindhi Arts and Science College, Chennai since 2012. Her research interests are Graph Labeling and Cryptography.

Dr. V. Maheswari received her Master's degree in the year 2000 from MK University, India and PhD degree in 2016 from Manonmaniyam Sundaranar University, Tirunelveli, India. She did her PhD degree in the field of Graph Theory. She has worked as associate professor in Vels Institute of Science, Technology & Advanced Studies (VISTAS) Chennai since 2017 Her area of interest includes Graph Labeling and Cryptography.