

PAPER • OPEN ACCESS

An Efficient Cryptosystem Using Playfair Cipher Together With Graph Labeling Techniques

To cite this article: B Deepa *et al* 2021 *J. Phys.: Conf. Ser.* **1964** 022016

View the [article online](#) for updates and enhancements.

You may also like

- [A Hybrid Encryption and Decryption Algorithm using Caesar and Vigenere Cipher](#)
Camille Merlin S. Tan, Gerald P. Arada, Alexander C. Abad et al.
- [Application and Manual Encryption Process with The Combination Algorithm of One Time Pad and Vigenere Cipher](#)
Siti Julianita Siregar, Muhammad Zarlis and Zakarias Situmorang
- [Advanced hill cipher algorithm for security image data with the involutory key matrix](#)
Supiyanto and S A Mandowen

PRIME
PACIFIC RIM MEETING
ON ELECTROCHEMICAL
AND SOLID STATE SCIENCE

HONOLULU, HI
Oct 6-11, 2024

Abstract submission deadline:
April 12, 2024

Learn more and submit!

Joint Meeting of
The Electrochemical Society
•
The Electrochemical Society of Japan
•
Korea Electrochemical Society

An Efficient Cryptosystem Using Playfair Cipher Together With Graph Labeling Techniques

B Deepa¹, V Maheswari¹ and V Balaji²

¹Department of Mathematics, Vels Institute of Science, Technology and Advanced Studies, Chennai -600 117, Tamilnadu, India.

²Department of Mathematics, Sacred Heart College, Tirupattur 635 601, Tamilnadu, India.

Corresponding Author: maheswari.sbs@velsuniv.ac.in

Abstract. Cryptography is the branch of Discrete Mathematics which deals with the transmission of secret communications between intended parties without the knowledge of third party. Graph theory is the enchanting field of Mathematics that designate integers to edges and vertices through some established functions. In current scenario security of communication plays a crucial role in any telecommunication or network applications. In this paper we have proposed an efficient cryptosystem using play fair cipher together with graph labeling to safeguard our secret text from unauthorised persons. Here we employ the substitution cipher namely Play fair cipher for plaintext encryption and our encrypted text in the form of Cipher Graph is forwarded to the receiver which on application of graph labeling yields our plaintext. Thus a fusion of the techniques Cryptography with Graph labeling provides ultimate security for secure transmission of data or information at various levels.

Keywords: Cipher Graph, Cipher key, Cipher text, Graceful edge labeling, Permutation Cipher, Plaintext, Play fair Cipher

AMS Subject classification MSC (2010) No: 05C78

1. Introduction

In paper, [1], [2], [3], [4] Graph labeling techniques have been studied. We refer [5], [6],[7],[8] and [9] for Better Security Enhancement using Play fair Cipher. From [10] and [11] Permutation cipher techniques have been studied. [12], [13] and [14] showcases Encryption and Decryption techniques using various graphs, Inspired by [3],[4],[5],[7],[10],[11] & [12] we present an improved technique of coding a message based on Play fair Cipher and permutation for the graph using prime graceful labeling techniques. So here we make use of combination of Play fair and Permutation method to perform our encryption process after which we apply Graph labeling technique to pass the encrypted message to the receiver in a form Graph. Here we adopt symmetric key cryptosystem for the both process of encryption and decryption.

2. Definitions



Content from this work may be used under the terms of the [Creative Commons Attribution 3.0 licence](https://creativecommons.org/licenses/by/3.0/). Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.

Definition 2.1: Graceful labeling

G be a graph and $f: V \rightarrow (1,2,3, \dots, p)$ is an injective function. For each distinct edge $e=uv$, The induced edge labeling defined by $f(uv) = |f(u) - f(v)|$ for all $uv \in E$ is said to be Graceful labeling.

Definition 2.2: Graceful graph

A Graph which admits graceful labeling is said to be a graceful graph.

Definition 2.3: plaintext

A message in the form of readable is known as plaintext

Definition 2.4: Cipher Graph

An encrypted message presented in the form of Graph is known as Cipher Graph.

Definition 2.5: Permutation Cipher

In Mathematics, The rearrangement of columns within a block is known as Permutation Cipher.

3. Traditional Play Fair Cipher

Play fair cipher is the most popular symmetric polyalphabetic encryption technique. Instead of replacing single character in any kind of encryption process we can replace pair of character in play fair cipher encryption technique. It was invented in the year of 1854 by Charles Wheatstone but promoted and executed by Lord Play fair.

The Traditional Play fair cipher uses a 5*5 matrix containing a keyword as shown in the table 1. Which consists of 25 cells. Firstly, the spaces of cell filled with letters of keyword then the rest of cells filled with English alphabets in the order, I and J sharing its position. The keyword together with the conventions for filling in the 5*5 matrix establish the cipher key. Here the keyword is "GREAT"

Table: 1 Traditional Play fair Cipher

G	R	E	A	T
B	C	D	F	H
I/J	K	L	M	N
O	P	Q	S	U
V	W	X	Y	Z

4. Proposed Algorithm For Encryption And Decryption Process

Step: 1 Use a keyword "Mount" to generate Play Fair Cipher Matrix.

Step: 2 First take the message and Split it be a two letter block

Step: 3 Use the following Play Fair Cipher 8*8 matrix to encrypt message.

M	o	u	n	t	A	B	C
D	E	F	G	H	I	J	K
L	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	p	q	r	s	v
w	x	y	z	0	1	2	3
4	5	6	7	8	9	*	!

The Play fair encryption process has the following 4 rules.

Rule 1: If two letters are similar means we need to add on the letter “X” after the first letter.

Rule 2: In a Key table: 2 if two letters fall in the same row, Replace the two letters with their immediate right of their first letter.

Rule 3: In a Key table: 2 if two letters fall in the same column, Replace the two letters with their immediate bottom of their first letter.

Rule 4: In a key table: 2 if two letters neither fall on the same row or column, , we need to connect the two letters by draw a rectangular or square format in a key table and replace by its corner letters.

Step: 4 Apply Permutation cipher (reordering the each character of cipher text I) for the encrypted message (Cipher text I) to constitute cipher text II.

Step: 5 Use Play fair Cipher 8*8 matrix to relate numerical value for the cipher text II to get cipher text 3.

Step: 6 For each character of Cipher text II, apply Additive 6 Caesar cipher to produce Cipher text III.

Step: 7 Use Graceful labeling technique to represent cipher text III in the form of Cipher Graph.

Decryption process follows all the steps of reverse encryption process 4.1:

Step: 1 Use Graceful labeling technique to trace Plaintext III.

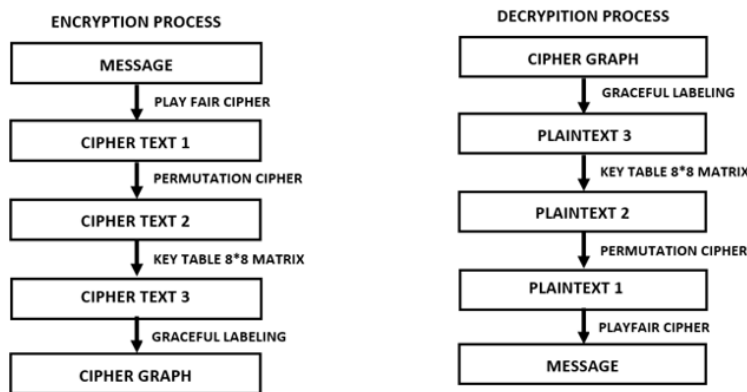
Step: 2 Use Play fair Cipher 8*8 matrix to relate to trace numerical value of Plaintext II.

Step: 3 Use Permutation cipher to trace Plaintext I.

Step: 4 Use Play fair Cipher 8*8 matrix to finally trace our message.

5. Outline of Encryption and Decryption Process

Fig: 1



6. Illustration 1

Encryption Process 6.1:

Let our Plaintext be “I like 5* Cadbury”.

Stage 1 Proposed Play Fair Cipher 6.2:

In our proposed methodology, the revised Play fair cipher utilized here is an 8*8 matrix which consists of keyword, upper and lower case of English alphabets, special characters and numerical values. We first insert the letter of the key word in the order followed by the remaining alphabets, numerical values, special characters in the order. Here the keyword is “Mount”.

Table: 2 Play fair Cipher 8*8 Matrix

M	o	u	n	t	A	B	C
D	E	F	G	H	I	J	K
L	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	p	q	r	s	v
w	x	y	z	0	1	2	3
4	5	6	7	8	9	*	!

To encrypt our plaintext, we first Split the plaintext be a two letter block

Table: 3 Two letter Block

I	l		i	k		e	5		*	C		a	d		b	u		r	y
---	---	--	---	---	--	---	---	--	---	---	--	---	---	--	---	---	--	---	---

Now, the two letter block processed in play fair cipher matrix table 2,

Thus the plaintext “I like 5* Cadbury” encrypted as shown in the below table: 4.

Table: 4 Cipher text 1

E	r		C	s		d	6		!	B		v	i		W	C		m	l
---	---	--	---	---	--	---	---	--	---	---	--	---	---	--	---	---	--	---	---

The plaintext processed in the play fair cipher will become our cipher text 1. Which is consider as a plaintext 1 to our next encryption process. Now we are going to use Permutation Cipher.

Stage 2 Permutation Cipher 6.3:

Permutation is a branch of Discrete Mathematics, is a rearrangement of the member into a sequence or ordered set. We can also referred as “linear order” or “arrangement of member”.

To encrypt our Plaintext 1, take the Plaintext 1 as a 2 letter 7 blocks,

$$\begin{pmatrix} E & c & d & ! & v & W & m \\ r & s & 6 & B & i & C & l \end{pmatrix}$$

Then greater arrangements of the letter blocks according to the following permutation cipher $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 5 & 4 & 7 & 2 & 6 \end{pmatrix}$.

The first 2 letter block moves to position 3, the second 2 letter block moves to position 1, the third 2 letter block moves to position 5, the fourth 2 letter block remains same in the position 4, the fifth 2 letter block moves to position 7, the sixth 2 letter block moves to position 2, the seventh 2 letter block moves to position 6. We get, $\begin{pmatrix} c & W & E & ! & d & m & v \\ s & C & r & B & 6 & l & i \end{pmatrix}$.

After the permutation is applied the plaintext 1 will becomes cipher text 2 as shown in the below table: 5.

Table: 5 Cipher text: 2

c	s		W	C		E	r		!	B		d	6		m	1		v	i
---	---	--	---	---	--	---	---	--	---	---	--	---	---	--	---	---	--	---	---

Further great use Play fair Cipher 8*8 matrix table 2, our cipher text 2 of “csWCer!Bd6m1vi” changed as numerical value as stated in table 6.

Table: 6 Cipher text 3

51	67	43	18	22	66	57	17	52	83	63	76	68	57
----	----	----	----	----	----	----	----	----	----	----	----	----	----

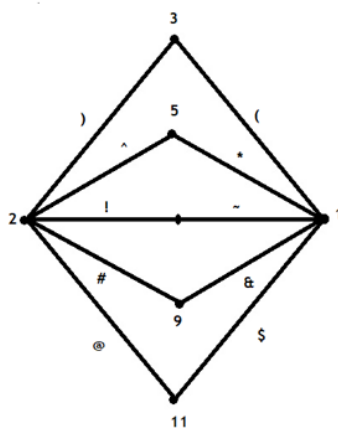
The pair of number that coordinates of each letter in the table: 2,(I.e.) 51 stands for row 5 and column 1 so letter c, 67 stands for row 6 and column 7 so letter s, and so on.

Table: 7 Row and Column value of Cipher text 3

Row	5	6	4	1	2	6	5	1	5	8	6	7	6	5
column	1	7	3	8	2	6	7	7	2	3	3	6	8	7

Here we divide the pair value by row and column to represent the numeric value in the cipher graph. Finally our row and column value of cipher text 3 presented in the form of Cipher Graph. Then the Cipher Graph is shared to the receiver along with the following clues.

Fig: 2 Cipher Graph



Clue6.4:

Key: 1 Use Graceful labeling formula to trace edges which the receiver make arrangements in the order of

Row	!	~	*)	(~	!)	!	&	~	#	~	!
Column)	#	^	&	(~	#	#	(^	^	~	&	#

Key: 2 Use Key table 8*8 matrix to know alphabetic value.

Key: 3 Use permutation cipher to make the arrangement of the block in the order

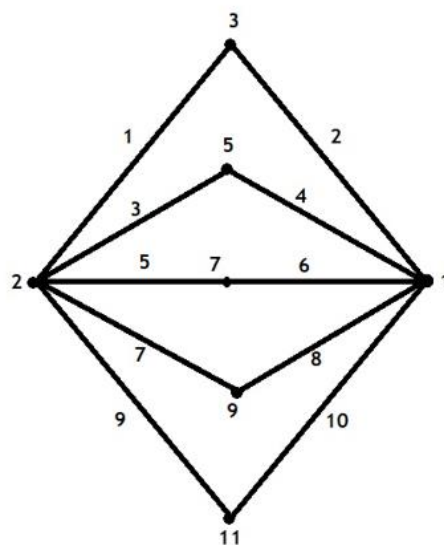
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 5 & 4 & 7 & 2 & 6 \end{pmatrix}$$

Key: 4 Use Play fair cipher to finally trace our message.

Decryption Process6.5:

The Decryption is the progress of transforming cipher text back to plaintext. For the above cipher Graph the receiver has to find the edges by applying the formula of Graceful Labeling thus obtained forms our Plaintext in the form of Graph.

Fig: 3 Shadow Graph



We obtain plaintext 3, further arrangements of edges in the order as stated in clue 1 as shown below table 8.

Table: 8 Row and Column value of Plaintext 3

Row	5	6	4	1	2	6	5	1	5	8	6	7	6	5
column	1	7	3	8	2	6	7	7	2	3	3	6	8	7

The row and column value combined as a pair of number, bylocating each pair value in the table 2, I.e. 51 stands for row 5 and column 1 so letter c, 67 stands for row 6 and column 7 so letter s, and repeating this similar process Which yield our Plaintext 2 as shown in the below table 9.

Table: 9 Plaintext 2

c	s		W	C		E	r		!	B		d	6		m	1		v	i
----------	----------	--	----------	----------	--	----------	----------	--	----------	----------	--	----------	----------	--	----------	----------	--	----------	----------

Rewriting the each block corresponding to permutation cipher stated in clue 3, we get Plaintext 1 as shown in the below table 10.

Table: 10 Plaintext 1

E	r		C	s		d	6		!	B		v	i		W	C		m	1
----------	----------	--	----------	----------	--	----------	----------	--	----------	----------	--	----------	----------	--	----------	----------	--	----------	----------

Further considering Play fair Cipher we get our Plaintext.

Finally, we reach our message is “I like 5* Cadbury”.

7.Illustration 2

Encryption Process 7.1:

Let us consider our Plaintext be “**Catch up!**” .

For the encryption process, we first divide the plaintext into two letter block as shown in table 11.

Table: 11 Two letter block

C	a		t	c		h	u		P	!
----------	----------	--	----------	----------	--	----------	----------	--	----------	----------

Now, the two letter block processed in play fair cipher matrix 9*9 as stated in the below table 12,

Table: 12 Play fair Cipher 9*9 matrix

W	o	n	d	e	r	A	B	C
D	E	F	G	H	I	J	K	L
M	N	O	P	Q	R	S	T	U
V	X	Y	Z	a	b	c	f	g
h	i	j	k	l	m	p	q	s
t	u	v	w	x	y	z	0	1
2	3	4	5	6	7	8	9	!
~	@	#	\$	%	^	&	*	(
)	{	}	[]	\	 	:	“

Thus the plaintext “**Catch up!**” encrypted as “**egzvits8**”. Now, we get our cipher text 1 in the form of two letter block as stated in below table 13.

Table: 13 Cipher text 1

e	g		z	v		i	t		s	8
----------	----------	--	----------	----------	--	----------	----------	--	----------	----------

The plaintext processed in the play fair cipher 9*9 matrix will become our cipher text 1. Which is taken as a plaintext 1 to our next encryption process of permutation cipher.

First, to encrypt our Plaintext 1, take the Plaintext 1 as a 2 letter 4 blocks,

$$\begin{pmatrix} e z i s \\ g v t 8 \end{pmatrix}$$

Then greater arrangements of the letter blocks according to the following permutation cipher

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

Weget,

$$\begin{pmatrix} z & i & s & e \\ v & t & g & \end{pmatrix}$$

The first block moves to position 4, the second block moves to position 1, the third block moves to position 2, the fourth block moves to position 3. Further the greater arrangements of plaintext 1 using permutation cipher will becomes cipher text 2 as shown in the below table 14.

Table: 14 Cipher text 2

z	v		i	t		s	g		e	g
----------	----------	--	----------	----------	--	----------	----------	--	----------	----------

Then cipher text 2 of “**zvits8eg**” value taken from the Play fair cipher 9*9 matrix table 12, as shown in table 15.

Table: 15 Cipher text 3

67	63	52	61	59	77	15	49
-----------	-----------	-----------	-----------	-----------	-----------	-----------	-----------

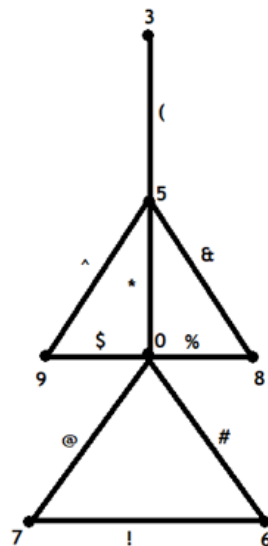
The pair value which indicates each letter in the table 12, I.e. 67 stands for row 6 and column 7 so letter z, 63 stands for row 6 and column 3 so letter v, and so on.

Table: 16 Row and Column value of Cipher text 3

Row	6	6	5	6	5	7	1	4
Column	7	3	2	1	9	7	5	9

Now, we split up the pair value by row and column to present in the cipher graph. Finally our row and column value of cipher text 3 presented in the form of Cipher Graph. Then the Cipher Graph send to the receiver with the following clues.

Fig: 4 Cipher Graph



Clue7.2:

Key: 1 Use Graceful labeling formula to trace edges which the receiver make arrangements in the

Row	#	#	*	#	*	@	!	^
Column	@	&	(!	\$	@	*	\$

order of

Key: 2Use Key table Play fair cipher 9*9 matrix to know alphabetic value.

Key: 3 Use permutation cipher to make the arrangement of the blocks in the order

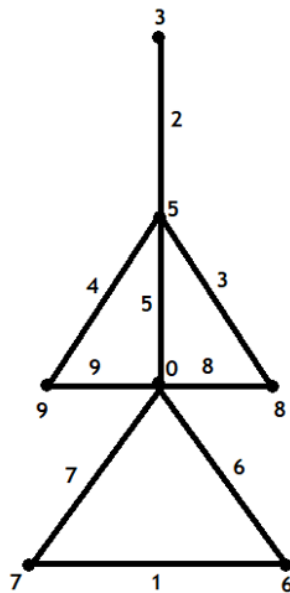
$$\begin{pmatrix} 1 & 3 & 4 & 2 \\ 4 & 2 & 3 & 1 \end{pmatrix}$$

Key: 4Use Play fair cipher to finally trace our message.

Decryption Process 7.3:

In Decryption process, first the receiver has to find the edges for the above Cipher Graph by applying the formula of Graceful Labeling thus obtained forms our Plaintext in the form of Graph as shown in below.

Fig 5: Tower Graph



Further arrangements of edges in the order as stated in clue 1, we obtain Plaintext 3 as shown in the below table 17.

Table: 17 Row and Column value of Plaintext 3

Row	6	6	5	6	5	7	1	4
Column	7	3	2	1	9	7	5	9

The row and column value combined as a pair of number, by locating each pair value in the table 12, I.e. 67 stands for row 6 and column 7 so letter z, 63 stands for row 6 and column 3 so letter v, and repeating this similar process Which yield our Plaintext 2 as shown in the below table 18.

Table: 18 Plaintext 2

z	v		i	t		s	8		e	g
----------	----------	--	----------	----------	--	----------	----------	--	----------	----------

Further greater arrangements of two letter block corresponding to permutation cipher stated in clue 3 will give us plaintext 1 as stated in the below table 19.

Table: 19 Plaintext 1

e	g		z	v		i	t		s	8
----------	----------	--	----------	----------	--	----------	----------	--	----------	----------

Further plaintext 1 processed in Play fair Cipher matrix 9*9 which yield our initial Plaintext.

Finally, we obtain our message is **“Catch up!”**.

8. Conclusion

Cryptography is a method of securing information and communication from malicious third parties. The modification of play fair cipher with different size matrix along with Graceful labeling techniques will give us more integrity and security to the communication. In future work we can try with further extension and modification of matrix size along with Some different labeling techniques.

References

- [1] J.A. Gallian, “A Dynamic Survey of Graph Labeling”, Electronic Journal of Combinatorics (2018)
- [2] F. Harary, “Graph Theory”, Addison – Wesley, Reading, 1969.
- [3] T.M. Selvarajan, R. Subramoniam, “Prime Graceful Labeling”, International Journal of Engineering and Technology, 7(4.36) (2018) 750-752.
- [4] Mohamed R.Zeen El Deen, “Edge even graceful labeling of some graphs”, Journal of the Egyptian Mathematical Society, (2019) 27:20.
- [5] Salman A. Khan, “Design and Analysis of Play fair Ciphers with Different Matrix Sizes”, International Journal of Computing and Network Technology, ISSN 2210-1519, Sept. 2015.
- [6] Md. AhnafTahmid Shakil Md. Rabiul Islam, “An Efficient Modification to Play fair Cipher”, UlabJournal of Science and Engineering, Vol. 5, No. 1, November 2014 (ISSN: 2079-4398).

- [7] R.Deepthi, "A Survey Paper on play fair Cipher and its Variants", International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395 -0056 Volume: 04 Issue: 04 Apr -2017 p-ISSN: 2395-0072
- [8] MaherinMizanMaha, MdMasuduzzaman February and AbhijitBhowmik "An Effective Modification of Play Fair Cipher with Performance Analysis using 6x6 Matrix", ICCA '20, January, 2020, Dhaka, Bangladesh.
- [9] S.Karthiga, T.Velmurugan "Enhancing Security in Cloud Computing using Play fair and Caesar Cipher in Substitution Techniques", IJITEE, ISSN:2278-3075, Volume 9 Issue-4, 2020.
- [10] Song Xiaomei, Changxiu Cheng and Zhou Chenghu, "Research on permutation generation algorithm based on sorting," The 2nd International Conference on Information Science and Engineering, Hangzhou, 2010, pp. 1-4, doi: 10.1109/ICISE.2010.5691730.
- [11] Falih A. M. Aldosray "Permutations and Combinations", Journal of Environmental Science, Computer Science and Engineering & Technology, JECET; March 2019- May 2019; Sec. C; Vol.8. No.2, 104-107. E-ISSN: 2278-179X, DOI: 10.24214/jecet.C.8.2.10407.
- [12] B.Deepa, Dr.V.Maheswari, V. Balaji "Creating Cipher text And Decipher Using Graph Labeling Techniques", International Journal of Engineering and Advanced Technology, ISSN: 2249 – 8958, Volume-9 Issue-1S, October 2019.
- [13] B.Deepa, Dr.V.Maheswari "Encoding and Decoding Using Graph Labeling", ISSN NO: 0886-9367, IJAEM.
- [14] B.Deepa, Dr.V.Maheswari "Ciphering and Deciphering Messages by Graph Labeling Techniques Through Multilevel Cryptosystem" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-4S5, December 2019.