Hiding a message using quintuple square and inspection of planar graph

Cite as: AIP Conference Proceedings **2385**, 130019 (2022); https://doi.org/10.1063/5.0070807
Published Online: 06 January 2022

D. A. Angel Sherin, V. Maheswari and V. Balaji

Hiding a Message using Quintuple Square and Inspection of Planar Graph

D. A. Angel Sherin[1, b)], V. Maheswari[1, a)] and V. Balaji[2, c)]

[1] *Department of Mathematics, Vels Institute of Science, Technology & Advanced Studies (VISTAS), Pallavaram, Chennai-117.*

[2] *PG and Research Department of Mathematics, Sacred Heart College, Tirupattur, Vellore Dt-635601.*

[a)]Corresponding author: maheswari.sbs@velsuniv.ac.
[b)]d.a.angelsherin@gmail.com
[c)]pulibala70@gmail.com

Abstract. *Cryptography plays a major role in hiding the data. It converts the plaintext into ciphertext in order to secure data. Ciphertext is a form of coding which should not reveal the secrecy. Quintuple Square is a 5x5 table grid with alphabets or symbols. This square table is used to get a ciphertext. Quintuple square encrypts the pairs of letters, which is hard to obtain the secret message. The recurrence of paired letters is 600 rather than the single letter in English alphabet. In this paper we encrypt the message using Playfair and Bifid Cipher. The message and transposition of Playfair is applied to get a planar graph with edge injective labeling and we confer the properties of planar graph.*

Keywords: Playfair, Bifid, Cipher, Planar Graph and Properties.

2010 Mathematics Subject Classification Number: 05C78

INTRODUCTION

Cryptography is a study of hiding a message from the brute force attack. Cryptography is interconnected with terms cryptanalysis and cryptology. Initially Cryptography was used in passing messages in British war. Slowly it made a greater impact when the world moved to adapt technology. All the old data is now converted into digital and saved in chips, so that it can be retrieved at any time and the storage space is less. A confidential message is passed to the receiver in cryptic forms. The conversion of a message into an unknown secret message is called cryptic form. Otherwise the conversion of messages into microdots, merging words with images and merging words in the form of audio are the examples of hiding the data.

Cryptography technique always focus into four objectives

1. Confidentiality
2. Integrity
3. Non-repudiation

International Conference on Advances in Materials, Computing and Communication Technologies
AIP Conf. Proc. 2385, 130019-1–130019-10; https://doi.org/10.1063/5.0070807
Published by AIP Publishing. 978-0-7354-4161-3/$30.00

4. Authentication

Strategy and algorithm combined to form crypto systems. The execution of crypto systems can be done by Mathematical procedures and computer programming. Password verification, digital signature, smart phones and SSL certificates works with the help of crypto systems (Fig. 1).

Cryptography divides into two main categories

1. Symmetric keys- Sender and receiver uses same keys to break the message
2. Asymmetric keys- Sender and receiver uses different keys to break the message

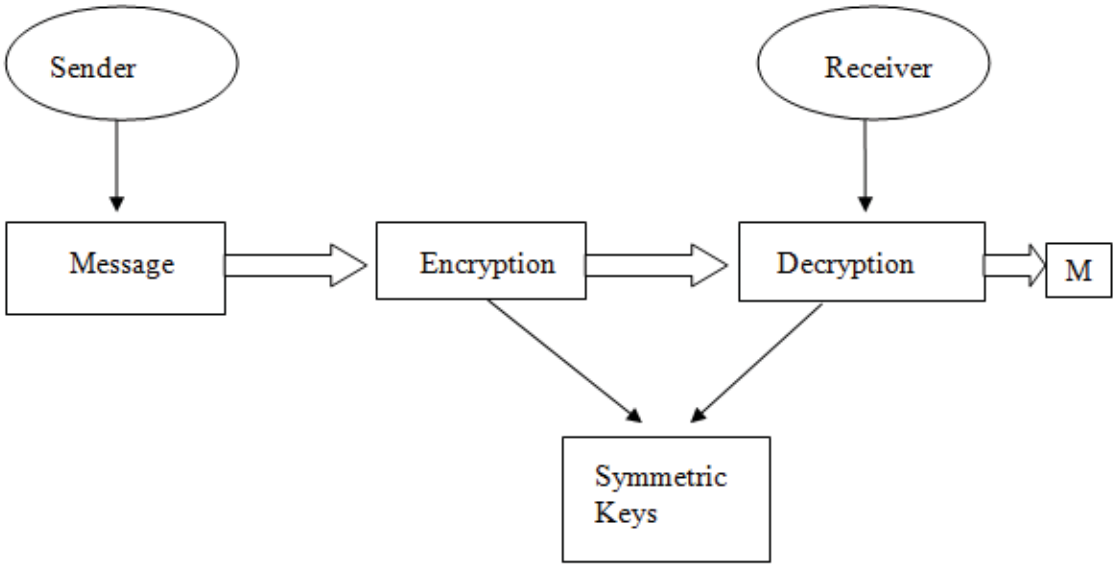

FIGURE 1. Symmetric key chart

In this research paper we are going to use two cipher techniques to reveal the message. Cipher is a system of rules to do encryption and decryption. Ciphers are categorized into six divisions. Among the six categories we execute two ciphers. One is a Bifid cipher and the other one is a Playfair cipher. Using the Playfair cipher method we form a set of equations. These equations are used to implement a planar graph and we use edge injective labeling to discuss some of the properties of it.

LITERATURE REVIEW

Yahiaalemami, MohamadAfendee Mohamed and SalehAtiewi [6] discussed various Cryptography techniques. DivyaChanana [7], investigated how cryptography plays a major role in cyber security. H.de.Fraysseix and P.Ossona de Mendez [1] talked about the connectivity of Planar graphs. MatheusP.Viana, EmanueleStrano, Patricia Bordin and Marc Barthelemy [2] linked the network with Planar graphs. Inspired by these works we create a graph using ciphers and labeled them with edge injective labeling.

BIFID CIPHER

Bifid Cipher is a cryptographic technique of converting plaintext into ciphertext. It contains Quintuple square with transposition. Fractional diffusion is used to get the ciphertext. Felix Delastelle, a Frenchman, found many ciphers including the bifid, trifid, and four-square ciphers.The first outcome of the bifid ciphertext is in the year 1985 as French Revue du Génie civil.He had named the cipher as cryptographie nouvelle. This type of ciphertext is mainly used by amateur cryptographers. This ciphertext is considered to be more secure because it divides the message into part of two separate streams and then reunites them. Quintuple stands for a 5x5 table of letters or symbols.

For this cipher technique we use the English alphabets in Quintuple square of merging the letter I and J into one cell. The numbering of each row and column is done by even numbers.

Encryption Algorithm

1. A message and a key will be given
2. Arrange the letters of key in row wise of 5x5 Quintuple square
3. Rest of the boxes are filled with left out alphabets
4. Number the outer box row and column wise with even numbers
5. Now find the corresponding row number and column number of each letter in message and write that in two separate lines
6. Select a certain interval of period as your key and separate the message
7. Now merge the values of rows and columns with interval period of key
8. From the final combined values take corresponding letter value from the Quintuple Square
9. We get a random ciphertext from the combined values

Illustration

Encryption

Message: Share the data of aircraft through transcripts.

Key: Cleft

Cleft means Bifid (divided the key into two equal parts)

2	4	6	8	10	
2	C	L	E	F	T
4	A	B	D	G	H
6	I/J	K	M	N	O
8	P	Q	R	S	U
10	V	W	X	Y	Z

S-88 H-410 A-42 R-86 E-26 T-210 H-410 E-26 D-46 A-42 T-210A-42

O-610 F-28 A-42 I-62 R-86 C-22 R-86 A-42 F-28 T-210T-210 H-410

R-86 O-610 U-810 G-48 H-410 T-210 R-86 A-42 N-68S-88 C-22 R-86

I-62 P-82 T-210 S-88

Row	8	4	4	8	2	2	4	2	4	4	2	4	6	2
Column	8	10	2	6	6	10	10	6	6	2	10	2	10	8
Row	4	6	8	2	8	4	2	2	2	4	8	6	8	4
Column	2	2	6	2	6	2	8	10	10	10	6	10	10	8
Row	4	2	8	4	6	8	2	8	6	8	2	8		
Column	10	10	6	2	8	8	2	6	2	2	10	8		

Now pair the consecutive numbers to get the encryption Ciphers

84/48/22/42/44/24/62/46/82/84/22/24/86/84/42/84/68/28/68/28/810/26/610/106/62/102/108/22/62/62/810/1010/

610/108/1010/62/88/26/22/108.

The above numbered values are matched with rows and columns in Quintuple square to get the ciphertext.

Ciphertext: QGCABLIDPQCLPQAQNFNFUEOXIVYCIIUZOYZISECY

Decryption

To decrypt a ciphertext the receiver counts the number of letters in encryption text and divided into two separate parts. The receiver finds the corresponding numerical value from the Quintuple Square and writes into separate parts. Then the receiver joins the separated parts to get a new numerical value and also finds the corresponding letter against the value. At last we get an original message.

Ciphertext: QGCABLIDPQCLPQAQNFNFUEOXIVYCIIUZOYZISECY

Key: Cleft

Total letters: 40 divided the ciphertext into two equal streams (20+20)

Ciphertext: QGCABLIDPQCLPQAQNFNF UEOXIVYCIIUZOYZISECY

Stream 1

Q G C A B L I D P Q C L P Q A Q N F N F

84 48 22 42 44 24 62 46 82 84 22 24 86 84 42 84 68 28 68 28

Stream 2

U E O X I V Y C I I U Z O Y Z

810 26 610 106 62 102 108 22 62 62 810 1010 610 108 1010

I S E C Y

62 88 26 22 108

Now write the numerical value of stream 1 below the stream 2.

84 48 22 42 44 24 62 46 82 84 22 24 86 84 42 84

810 26 610 106 62 102 108 22 62 62 810 1010 610 108 1010 62

68 28 68 28

88 26 22 108

Pair the numerical value in vertical wise as shown in arrow

88/410/42/86/26/210/410/26/46/42/210/42/610/28/42/62/86/22/86/42/28/210/210/410/86/

610/810/48/410/210/86/42/68/88/22/86/62/82/210/88

Now using Quintuple square we find the corresponding alphabets forthe paired numeric. Finally we get the original message.

S-88 H-410 A-42 R-86 E-26 T-210 H-410 E-26 D-46 A-42 T-210A-42

O-610 F-28 A-42 I-62 R-86 C-22 R-86 A-42 F-28 T-210T-210H-410

R-86 O-610 U-810 G-48 H-410 T-210 R-86 A-42 N-68S-88 C-22

R-86 I-62 P-82 T-210 S-88

Message: Share the data of aircraft through transcripts.

PLAY FAIR CIPHER

The Playfair cipher was invented by Charles Wheatstone in the year 1854 and further it was developed by Lord Playfair. This method was used by the British Military forces to maintain military secrecy during the second Boer war. In Playfair Cipher we encrypt the message into a digraph pattern.

Encryption Algorithm

1. The key is Quintuple of 5x5 grid with alphabets
2. The letter I and J will be written in one box
3. Arrange the letters of key in row wise of 5x5 Quintuple square
4. Rest of the boxes are filled with left out alphabets
5. Divide the message into pairs, if the last letter is single then add asterisk
6. If pair of letters are in the same column then move downward of each letter
7. If pair of letters are in the same row then move right of each letter
8. If pair of letters is in different place then draw the rectangular box including these letters and write the underneath corner letter against the pair of letters
9. If pair of letters contains asterisk then interchange the letter

Illustration

Encryption

Message: Send five soldiers to guard the North east gate.
Key: Quintuple (which means five)

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

Encrypted ciphertext

SE- OB ND- UG FI-OE VE-XP SO-KR LD-DM IE-EF RS-SK TO-IS

GU-DN AR-GY DT-HU HE-FB NO-IR RT-SN HE-FB AS-BR TG-NH

AT-BN E*-*E

Encoded message

OBUGOEXPKRDMEFSKISDNGYHUFBIRSNFBBRNHBN*E

Decryption Algorithm

1. Divide the encrypted message into pairs
2. If pair of letters are in the same column then move upward of each letter
3. If pair of letters is in the same row then move left of each letter
4. If pair of letters is in different place then draw the rectangular box including these letters and write the underneath corner letter against the pair of letters
5. If pair of letters contains asterisk then interchange the letter

Encoded message

OBUGOEXPKRDMEFSKISDNGYHUFBIRSNFBBRNHBN*E

Divide the encoded message

OB UG OE XP KR DM EF SK IS DN GY HU FB IR SN FB BR NH BN *E

Follow the above decoded algorithm and decode the message.

Decoded message

SEND FIVE SOLDIERS TO GUARD THE NORTH EAST GATE.

INSPECTION OF GRAPH PATTERN

Let us examine a new graph using message and Encrypted message.

S E N D F I V E S O L I D E R S T O G U A R D T H E

O B U G O E X P K R D M E F S K I S D N G Y H U F B

E N O R T H E A S T G A T E

I R S N F B BR N H B N * E

Formation of Equations

Write the message in one line and encrypted message in another line. Now we are going to relate the message with an encrypted message and we search for the letter cycle. If we find the letter cycle we stop relating and look for another letter. For example $S \to O \to R$

$D \to G \to H \to F$ $S \to O \to R$ $E \to B$ $I \to E \to P$ $U \to N \to I$ $U \to N \to I$
$O \to S \to K$ $N \to U$ $E \to F$ $G \to D$ $T \to I$ $A \to G$ $L \to D \to M$ $R \to Y$ $S \to R$ $A \to B$
$T \to N$

Ordering of Equations

Depending upon the number of letters in the equations we had given the ordered

$$D \to G \to H \to F \quad (1)$$
$$S \to O \to R \quad (2)$$
$$I \to E \to P \quad (3)$$
$$O \to S \to K \quad (4)$$
$$U \to N \to I \quad (5)$$
$$L \to D \to M \quad (6)$$

$$E \to B,\ N \to U,\ E \to F$$
$$G \to D, T \to I, A \to G \qquad (7)$$
$$R \to Y,\ S \to R,\ A \to B$$
$$T \to N$$

GRAPH IMPLEMENTATION

In equation (1) the first letter is D, now we are going to trace the same letter in all other equations. Whenever we find the same letter in the equation we are going to draw the vertices and label the vertex with equation number. We also join the vertices by edges.

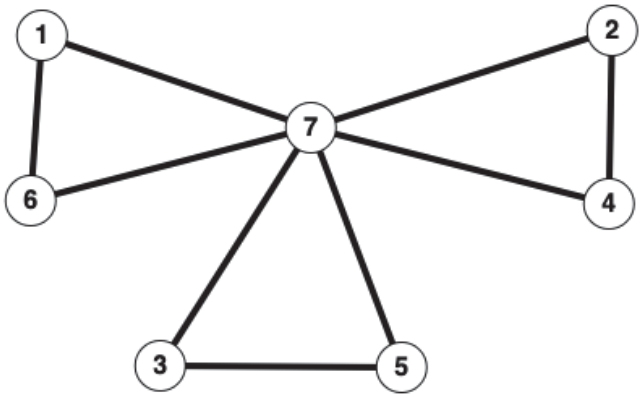

FIGURE 2. Traced graph

The traced graph (Fig. 2) is a planar graph with seven vertices and nine edges. We are going to impose Edge injective labeling on the edges of the Planar graph.

PRELIMINARIES

In this section we see the definition of the Planar graph with imposed edge injective labeling.

Definition Planar graph:

A graph which is embedded in a plane and its edges do not cross each other is called Planar graph.

Definition Edge Injective Labeling(EIL):

Let G(V,E) be a graph and let $f : V(G) \rightarrow \{1,2,3....26\}$ be an injective vertex set with the induced edge set as

$\begin{cases} y = 3x - 1; & if\ 1 \leq y \leq 26 \\ y = (3X - 1) mod 26; & if\ y \geq 26 \end{cases}$ where X is the sum of u+v of vertices.

Theorem

A graph which admits EIL is EIL Planar graph.

Proof:

Let v_1, v_2, v_3….v_7 be the distant vertices of a graph.
$F(v_1)=1$
$F(v_2)=2$

The corresponding induced edge injective labels are given by

$$\begin{cases} y = 3x - 1; & if\ 1 \leq y \leq 26 \\ y = (3X - 1) mod 26; & if\ y \geq 26 \end{cases}$$

Where $y=3(v_1+v_2)-1$.

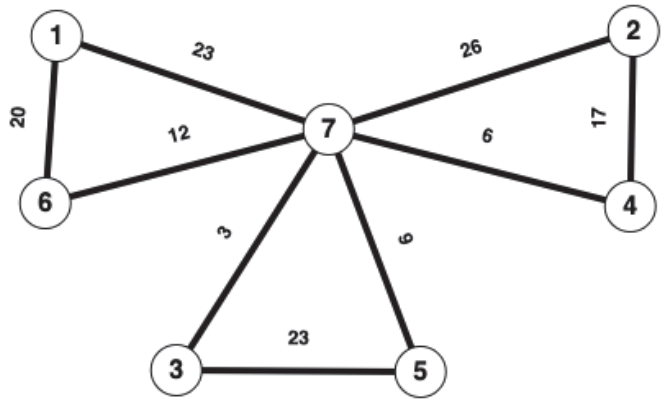

FIGURE 3. EIL Labeled

Since the graph is labeled using EIL, we conclude that graph is a planar graph.

CONCLUSION

The conversion of messages into ciphertext using Bifid Cipher and Playfair Cipher are safer. From the Playfair cipher we had introduced the comparison of equation methods to implement a graph. This graph may give any structure and we relate this structure with graph theory to obtain a graph name. We also elaborately discuss the graph and imposing EIL labels on them. In future, we apply different ciphers to enclose the confidentiality of the message.

APPLICATIONS

A cryptologist uses ciphers to secure the data in the form of a cryptic system. Micro circuitry and computer technology are developed using the ciphers. Internet, digital TV, digital communication and mobile phones depend on the ciphers for reliability and secrecy. Now every digital module uses this cipher system for security channels.

REFERENCES

1. H. Fraysseix and P. Ossona, Connectivity of Planar graphs, Journal of graph Algorithms and Applications, Volume 5, 2001.
2. M. P. Viana, E. Strano, P. Bordin and M. Barthelemy, The simplicity of Planar networks, Aigner, Scientific Reports DOI:10.1038/srep03495.
3. https://www.cs.yale.edu/lect25-09.pdf
4. T. Nishizeki and N. Chiba, Planar graphs: Theory and algorithms (Book)
5. F. J. Brandenburg, Recognizing IC-Planar and NIC-Planar graphs, Journal of graph Algorithms and Applications, Volume 22, 2018.
6. Yahiaalemami, M. Afendee, Mohamed and S. Atiewi, Research on Various Cryptography Techniques, International Journal of Recent Technology and Engineering, ISSN: 2277-3878.
7. D. Chanana, Research paper on Cyber security and Cryptography, International Journal of Innovative science and Research Technology, ISSN: 2456-2165.
8. K. Sunitha, C. D. Raj and A. Subramanian, Radio labeling of Hurdle graph and Biregular rooted trees. ISOR journal of Mathematics, e-ISSN:2278-5728, Volme-13,pp 37-44.
9. F. Harary, Graph Theory Book, Addison-Wesley, 1969.
10. D. A. A. Sherin, V. Maheswari, Encryption and decryption process using edge magic labeling Journal of Physics: Conference series, ISSN-1742-6596/1362/1/01/2024.
11. D. A. AngelSherin, V. Maheswari, Encoding the Graph using Instant Insanity puzzle and decoding with Hamiltonian cycle, The International Journal of analytical and modal analysis, ISSN-08869 - 9367. P.No: 167-175.
12. S. Rekha and V. Maheswari, Difference Modulo Labeling Journal of Physics: Conference Series, ISSN-1742-6596/1362/1/01/2049
13. G. U. Maheswari, G. M. J. Jebarani and V. Balaji, Coding through a two star and Super Mean Labeling. Applied Mathematics and Scientific Computing pp 469-478.