

A Reinforced System For The Playfair Cipher By Incorporating Dominator Coloring In Latin Square Graphs*

Karthika Ravichandran[†], Mohanapriya Nagaraj[‡]

Received 1 March 2024

Abstract

The art of secret communication has endured through the ages, dating back to ancient times. There has consistently been a need to protect shared information to prevent any unauthorized access. A number of classical ciphers were developed and employed over time, but they eventually fell short in terms of data security. Hence, there remained a necessity to address the shortcomings of classical ciphers, which, in turn, paved the way for the development of modern ciphers. While numerous encryption algorithms are continuously under development and scrutiny, the knowledge of classical algorithms should not go unnoticed. An essential adjustment to an existing algorithm might provide greater strength than newer alternatives. With this idea under consideration, we present an enhanced version of the traditional Playfair cipher, utilizing the concept of dominator coloring of Latin square graphs.

1 Introduction

Cryptography does indeed trace its roots back to ancient times [8]. Cryptography is the practice of confidential communication, where the information to be conveyed is encrypted using specific algorithms, referred to as ciphers. In this process, the key or rules necessary for decrypting the exchanged cipher text are exclusively known to the sender and the receiver. Undoubtedly, secret communication remains a vital necessity in this digitalized era, especially as every piece of data shared globally is readily accessible through cloud technologies and are more vulnerable to unauthorized access. A great number of classical ciphers have been introduced and utilized over the centuries [11] but their security was eventually compromised by technological and human advancements. As traditional ciphers gradually lost their effectiveness, cryptographers faced persistent pressure to enhance the security of cryptographic systems, ultimately leading to the development of modern ciphers. Yet, an excessive introduction of modern ciphers can become overwhelming, and some may go unnoticed. The mere development of new algorithms might not fully address this issue. Thus, incorporating certain additional algorithms and essential modifications to the existing ciphers can surprisingly yield a noteworthy cryptographic solution. Among the several classical ciphers that exist, the Playfair Cipher serves as the focus of our research proposal. It is distinguished as the first literal digraph substitution cipher.

Computational techniques in mathematics have paved the way for its integration into the field of cryptography. Notably, renowned mathematicians and graph theorists have introduced several effective encryption procedures in [12, 1, 13]. The combination of Graph Theory and Linear Algebra has the strength to become a vital tool in encryption systems. In Graph Theory, the concept of graph coloring has showcased its versatility, finding applications across a diverse range of domains [4]. Dominator Coloring has been explored for its potential influence in specific optimization domains. Several innovations have employed the ideas of domination number and dominator chromatic number, leading to intriguing applications [10]. Likewise, there has been an increasing research interest in the concept of Latin Squares and their applications in recent years. In this article, the concept of Latin Square Graphs in combination with Dominator Coloring [2] has been considered under study and its utilization to enhance an established encryption algorithm is presented.

*Mathematics Subject Classifications: 05B15, 05C15, 05C90, 11C20.

[†]Department of Mathematics, Kongunadu Arts and Science College, Coimbatore-641 029, Tamil Nadu, India

[‡]Department of Mathematics, Kongunadu Arts and Science College, Coimbatore-641 029, Tamil Nadu, India

2 Preliminaries

A brief outline of necessary definitions and preliminaries is provided in this section. A Graph [6] $\mathcal{G} = \{V, E, I_G\}$ is an ordered triplet where V represents the set of nodes called vertices, E represents the set of links called edges and I is the incidence relation of a vertex and an edge. Properly assigning colors to each vertex in a graph such that adjacent vertices do not have the same color is referred to as Proper Graph Coloring [3] and the minimum number of colors required for this is known as the chromatic number. A subset S of the vertex set V is referred to as a dominating set of a graph \mathcal{G} if every vertex in $V \setminus S$ is adjacent to at least a vertex in S . The domination number $\gamma(\mathcal{G})$ is the minimum cardinality of a dominating set in \mathcal{G} . Dominator coloring [5] of a graph \mathcal{G} is one of the proper colorings in which each vertex is said to be in the closed neighbourhood of all the vertices of atleast one color class. The minimum number of colors required for a dominator coloring is known as the dominator chromatic number denoted by $\chi_d(\mathcal{G})$.

A Latin Square [7] can be defined as an $n \times n$ array where each element from the set $\{0, 1, 2, \dots, n-1\}$ appears exactly once in both a row and a column. The Latin square graph [9] of a Latin square \mathcal{L} is the simple graph $\Gamma(\mathcal{L})$ whose vertices are the cells of \mathcal{L} , and where two cells (r, c, s) and (r', c', s') are adjacent if (exactly) one of the equations $r = r'$, $c = c'$, $s = s'$ is satisfied. Accordingly, each edge of $\Gamma(\mathcal{L})$ is called, respectively, a row edge, a column edge or a symbol edge.


3 Dominator Coloring of the Latin Square Graph of $(\mathbb{Z}_5, +)$

In this section, the dominator coloring is employed for the latin square graph for the group $(\mathbb{Z}_5, +)$ and the respective dominator chromatic number is found.

Theorem 1 *The dominator chromatic number of the latin square graph of the group $(\mathbb{Z}_5, +)$ is*

$$\chi_d(\Gamma(L(\mathbb{Z}_5, +))) = 9.$$

Proof. By the definition, the latin square is formed in accordance with the Cayley table of the group $(+\mathbb{Z}_5)$. The cayley table for this group $(\mathbb{Z}_5, +)$ and the respective latin square graph are given in Figures 1 and 2. Now, the proof of the theorem proceeds through the provided steps. In this graph, there are 5 cliques (K_5)



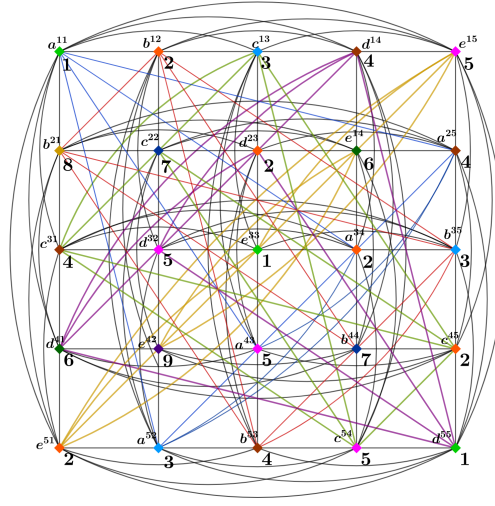
$+\mathbb{Z}_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$+\mathbb{Z}_5$	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

Figure 1: Cayley Table of $+\mathbb{Z}_5$.

each in row-adjacency, column-adjacency and symbol-adjacency.

- Commence the color assignment with a numerical sequence of 1, 2, 3, 4, 5 for the vertices in the first row.
- Assign the fifth row with the coloring sequence 2, 3, 4, 5, 1, ensuring the preservation of the proper coloring scheme.
- Given the graph's order of 5×5 , the possibility to reuse these colors remains available if required.

Figure 2: Dominator Coloring of $\Gamma(L(\mathbb{Z}_5, +))$.

- Carefully employ the used colors to color the column 3 and column 5 as per the formula $[(n-2) \& n]$, while upholding the proper coloring algorithm. Column 3 will be labeled as 3, 2, 1, 5, 4, and column 5 will be labeled as 5, 4, 3, 2, 1.
- Among the remaining nine vertices, there is the option to reuse any three colors from the set 1-5 for three vertices, with the choice of vertices and colors being contingent on maintaining proper coloring.
- Selecting the third row while considering dominator coloring is the most favorable choice. So, the assignment for third row will be 4, 5, 1, 2, 3.
- Now, the three remaining vertices in the second and fourth rows must be colored using new colors.
 - The vertices e^{24} and d^{41} are colored with the color 6.
 - The vertices c^{22} and b^{44} are colored with the color 7.
 - The vertex b^{21} is colored with the color 8.
 - The vertex e^{42} is colored with the color 9.
- This assignment preserves the dominating property as well.

■

4 Application in Strengthening a Cryptographic System

The dominator coloring of Latin square graph of the group $(\mathbb{Z}_5, +)$ introduces an intriguing application in the field of cryptography. Specifically, it offers an excellent approach to enhance an established cipher. The reason for selecting this cipher is its compatibility with the structure of a 5×5 grid.

4.1 Playfair Cipher - An Overview

The Playfair Cipher was initially devised by Charles Wheatstone in 1854. However, it is commonly associated with Lyon Playfair, who popularized its use. This technique is recognized as the first digraph substitution cipher, wherein pairs of characters (digraphs) are encrypted. To initiate this method, both

the sender and the receiver must first agree on a common key word. Subsequently, the keyword table is generated, which consists of a 5×5 square grid containing the keyword at the beginning. Repeated letters in the keyword are disregarded. For the sake of grid convenience, the letters 'I' and 'J' are placed within the same cell, as accommodating all 26 alphabets within the 25 cells would be impossible. After filling the grid with the keyword, the remaining letters are entered subsequently. For example, if the chosen keyword is 'LATIN' then the corresponding keyword table is given in Figure 3.

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

Figure 3: Keyword Table.

4.1.1 Encryption Rules:

The encryption process commences by dividing the plain text into bigrams, and these bigrams are subsequently replaced with the corresponding cipher text from the key table. Letters that are left unpaired, are supplemented with a filler letter, typically 'X' or 'Z'. The encryption is governed by four distinct conditions.

- If both letters in a bigram are situated within the same row of the key table, we replace the first letter with the immediate right character as the cipher.
- If both letters in a bigram reside within the same column of the key table, we replace the first letter with the immediate character below it as the cipher.
- If both letters in a bigram are identical, we insert a filler letter between them.
- If both letters in a bigram are located in different rows and columns, we replace them with the letters at the point of intersection within the key table.

The decryption procedure is essentially the inverse of the encryption.

4.2 Proposed Methodology to Enhance the Playfair Cipher

Playfair Cipher method proves considerably more resistant to decryption through frequency analysis, as compared to simpler substitution methods. However, despite its complexity, it remains susceptible to decoding. With repeated analysis of frequency, a significant amount of English language text could eventually be deciphered. Therefore, we introduce a revised set of encryption rules that incorporate mathematical and graph theoretical computations. This approach is expected to boost up the security of the existing cipher mechanism, resulting in an exceptionally strong encryption protocol.

4.3 Revised Encryption Algorithm

The alphabets along with their indices are provided in the Table 1 below.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Table 1: Alphabets and Indices.

The encryption process follows the given steps:

1. Construct a 5×5 table that includes all the letters of the alphabet, where 'I' and 'J' occupy a shared cell.
2. Create an index table for the alphabetical grid. Note this as a matrix 'A'.
3. Swap the first row of the matrix A with the $(n-1)^{th}$ row, i.e., 4^{th} row, as the domination number of an 5×5 Latin square is 4. Name the modified matrix as 'B'.
4. Next, generate another matrix 'C' that signifies the coloring sequence of the rows and columns employed in the graph described in Figure 2.
5. Calculate matrix 'D' by multiplying 'B' and 'C'.
6. Consider only the first row and replace each entry with the result of that entry modulo 26.
7. If any index is repeated in the revised row, rewrite the repeated index using the formula ($repeated\ value = value + 9(mod\ 26)$).
8. Repeat Step 7 until there are no repeating indices.
9. Determine the alphabets corresponding to the obtained indices and fix these five letters as the keyword.
10. Create a keyword table using the keyword obtained in the preceding step.
11. Construct a matrix 'E' with the respective indices of the keyword table.
12. Replace the entries of the matrix 'E' with " $entry + 9(mod\ 26)$ ", since the dominator chromatic number, $\chi_d(\Gamma(L(\mathbb{Z}_5, +))) = 9$. Denote the resulting matrix as 'K'.
13. The alphabetical table corresponding to the matrix 'K' is the Encrypted Keyword Table.
14. Now, perform the encryption of the Plain Text using the rules mentioned in section 4.1.1.
15. The resulting bigrams are assembled together which forms the Cipher Text.
16. Share the Cipher Text, $\gamma(L(\mathbb{Z}_5, +))$, $\chi_d(\Gamma(L(\mathbb{Z}_5, +)))$, matrix C and the steps 1–12 with the recipient to discover the encrypted keyword table.

4.4 Decryption Algorithm

1. Receive the shared values and matrices.
2. Discover the encrypted keyword table by following the rules provided by the sender.
3. With the keyword table in hand, execute the decryption process of the Cipher Text following the rules of the Playfair Cipher as elucidated in section 4.1.1.
4. The resulting bigrams assembled together, with the fillers removed, if any, is the deciphered plain text.

4.5 Illustration

Suppose that the plain text ‘DOMINATOR COLORING’ has to be encrypted.

ENCRYPTION:

Step 1: The alphabets are put in a 5×5 grid as follows:

$$\begin{bmatrix} A & B & C & D & E \\ F & G & H & I/J & K \\ L & M & N & O & P \\ Q & R & S & T & U \\ V & W & X & Y & Z \end{bmatrix}.$$

Step 2: The corresponding index table of the above displayed grid is represented as a matrix ‘A’.

$$A = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 11 \\ 12 & 13 & 14 & 15 & 16 \\ 17 & 18 & 19 & 20 & 21 \\ 22 & 23 & 24 & 25 & 26 \end{bmatrix}.$$

Here, the index corresponding to the letter ‘J’ is ignored for calculation purposes.

Step 3: $B = \text{row } 1 \leftrightarrow \text{row } 4 \text{ in } A$.

$$B = \begin{bmatrix} 17 & 18 & 19 & 20 & 21 \\ 6 & 7 & 8 & 9 & 11 \\ 12 & 13 & 14 & 15 & 16 \\ 1 & 2 & 3 & 4 & 5 \\ 22 & 23 & 24 & 25 & 26 \end{bmatrix}.$$

Step 4: The assignment sequence from the dominator coloring of the latin square graph, depicted in Figure 2, can be demonstrated as another matrix C as provided below.

$$C = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 8 & 7 & 2 & 6 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 6 & 9 & 5 & 7 & 2 \\ 2 & 3 & 4 & 5 & 1 \end{bmatrix}.$$

Step 5: Computing $D = BC$.

$$D = \begin{bmatrix} 17 & 18 & 19 & 20 & 21 \\ 6 & 7 & 8 & 9 & 11 \\ 12 & 13 & 14 & 15 & 16 \\ 1 & 2 & 3 & 4 & 5 \\ 22 & 23 & 24 & 25 & 26 \end{bmatrix} \times \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 8 & 7 & 2 & 6 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 6 & 9 & 5 & 7 & 2 \\ 2 & 3 & 4 & 5 & 1 \end{bmatrix} = \begin{bmatrix} 399 & 498 & 290 & 459 & 275 \\ 170 & 215 & 129 & 200 & 111 \\ 294 & 368 & 215 & 339 & 200 \\ 63 & 82 & 50 & 75 & 35 \\ 504 & 628 & 365 & 579 & 350 \end{bmatrix}.$$

Step 6: Replacing each entry of the first row of D with the value of that entry modulo 26. Here,

$$399(\bmod 26) = 9, \quad 498(\bmod 26) = 4, \quad 290(\bmod 26) = 4, \quad 459(\bmod 26) = 17, \quad 275(\bmod 26) = 15.$$

Hence, the first row of D is revised as:

$$[399 \quad 498 \quad 290 \quad 459 \quad 275] = [9 \quad 4 \quad 4 \quad 17 \quad 15].$$

Step 7: The value 4 is repeated in the revised row. So replacing it with $value + 9(\text{mod } 26)$ yields $4 + 9(\text{mod } 26) = 13$.

$$[9 \ 4 \ 4 \ 17 \ 15] = [9 \ 4 \ 13 \ 17 \ 15].$$

Step 8: There are no more repeated indices, so we proceed to the next step.

Step 9: The corresponding alphabets of these indices are obtained from Table 1. Therefore,

$$[9 \ 4 \ 13 \ 17 \ 15] = [I \ D \ M \ Q \ O].$$

Hence, the keyword obtained is 'IDMQO'.

Step 10: The keyword table is generated as follows:

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

Step 11: The respective indices of the entries in the keyword table are formed as a matrix 'E'.

$$E = \begin{bmatrix} 9/10 & 4 & 13 & 17 & 15 \\ 1 & 2 & 3 & 5 & 6 \\ 7 & 8 & 11 & 12 & 14 \\ 16 & 18 & 19 & 20 & 21 \\ 22 & 23 & 24 & 25 & 26 \end{bmatrix}.$$

Step 12: Replacing all the entries of matrix 'E' with $entry + 9(\text{mod } 26)$, we get the matrix 'K'.

$$K = \begin{bmatrix} 18/19 & 13 & 22 & 26 & 24 \\ 10 & 11 & 12 & 14 & 15 \\ 16 & 17 & 20 & 21 & 23 \\ 25 & 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 & 9 \end{bmatrix}.$$

Step 13: The respective alphabetical table of the matrix K is the Encrypted Keyword Table, which is shown in Figure 4.

Step 14: The plain text 'DOMINATOR COLORING' is now ready to be encrypted using the playfair rules.

The bigrams are (D,O), (M,I), (N,A), (T,O), (R,C), (O,L), (O,R), (I,N), (G,Z). Note that the last letter G has no pair, so the filler letter 'Z' is used.

Pair 01 - (D,O): The letters D and O appear in the same column of the keyword table. Hence, the immediate characters I and W respectively below these letters are the cipher letters.

$$(D,O) \rightarrow (I,W).$$

Pair 02 - (M,I): The letters M and I appear in different rows and columns of the keyword table. Hence, the letters X and F at the intersection of M and I are the cipher letters.

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

Figure 4: Encrypted Keyword Table.

$$(M,I) \rightarrow (X,F).$$

Pair 03 - (N,A): The letters N and A appear in different rows and columns of the keyword table. So, the letters K and C at the intersection of N and A are the cipher letters.

$$(N,A) \rightarrow (K,C).$$

Pair 04 - (T,O): The letters T and O appear in different rows and columns of the keyword table. So, the letters W and L at the intersection of T and O are the cipher letters.

$$(T,O) \rightarrow (W,L).$$

Pair 05 - (R,C): The letters R and C appear in different rows and columns of the keyword table. Hence, the letters Z and Y at the intersection of R and C are the cipher letters.

$$(R,C) \rightarrow (Z,Y).$$

Pair 06 - (O,L): The letters O and L appear in the same row of the keyword table. Hence, the immediate characters J and N respectively to the right of these letters are the cipher letters.

$$(O,L) \rightarrow (J,N).$$

Pair 07 - (O,R): The letters O and R appear in different rows and columns of the keyword table. Hence, the letters J and X at the intersection of O and R are the cipher letters.

$$(O,R) \rightarrow (J,X).$$

Pair 08 - (I,N): The letters I and N appear in different rows and columns of the keyword table. Hence, the letters H and O at the intersection of I and N are the cipher letters.

$$(I,N) \rightarrow (H,O).$$

Pair 09 - (G,Z): The letters G and Z appear in different rows and columns of the keyword table. Hence, the letters H and V at the intersection of G and Z are the cipher letters.

$$(G,Z) \rightarrow (H,V).$$

$$\begin{array}{c}
(D,O), (M,I), (N,A), (T,O), (R,C), (O,L), (O,R), (I,N), (G,Z) \\
\downarrow \\
(I,W), (X,F), (K,C), (W,L), (Z,Y), (J,N), (J,X), (H,O), (H,V)
\end{array}$$

So the Cipher Text is obtained as:

IWXFKCWLZYJNJXHOHV.

The cipher text can be deciphered in a similar manner to discover the plain text.

5 Conclusion

The proposed mechanism significantly enhances the encryption level for an existing algorithm, thereby reinforcing the security of the classical cipher. The matrix operations conducted during encryption can be executed rapidly using software tools like MATLAB or Python. In this Playfair Cipher method, merely exchanging the keyword and executing the encryption could be vulnerable to decryption since the keyword is typically not confidential. Besides, the sender and receiver agreeing on a potentially guessable alphabetical word as a key could be of a pathway for the intruders to easily break in. Therefore, establishing a set of rules for the systematic generation of a keyword and re-encrypting the keyword table can significantly enhance reliability, as the recipient would need to carry out an encryption to uncover the key. Furthermore, the keyword generated will be sufficiently random, making it extremely challenging for anyone to deduce or guess. Thus, these additional concepts from Mathematics and Graph Theory prove to be highly valuable in providing a greater security support to the Playfair Cipher method. To sum up, the combination of Latin squares and dominator coloring, with minimal programming involved, has the potential to significantly enhance encryption procedures, reducing the time required while ensuring a high level of security.

References

- [1] W. M. Al Etaiwi, Encryption algorithm using graph theory, *Journal of Scientific Research & Reports*, 3(2014), 2519–2527.
- [2] S. Arumugam, K. R. Chandrasekar, N. Misra, G. Philip and S. Saurabh, Algorithmic aspects of dominator colorings in graphs, *Lecture Notes in Comput. Sci.*, 7056(2011), 19–30.
- [3] J. A. Bondy and U. S. R. Murty, *Graph Theory*, Graduate texts in mathematics. Vol. 244, Springer Science and Media, 2008.
- [4] J. A. Bondy and U. S. R. Murthy, *Graph Theory with Applications*, North-Holland, New York, 1982.
- [5] R. M. Gera, On dominator colorings in graphs, *Graph Theory Notes of New York*, 52(2007), 25–30.
- [6] F. Harary, *Graph Theory*, Addison-Wesley Publishing Co., Reading, Mass.-Menlo Park, Calif.-London, 1969.
- [7] A. D. Keedwell and J. Denes, *Latin Squares and Their Applications*, Second edition, Elsevier.
- [8] N. Koblitz, *A Course in Number Theory and Cryptography*, 2nd edition, Springer-Verlag, New York, 1994.
- [9] B. Pahlavsay, E. Palezzato and M. Torielli, Domination for latin square graphs, *Graphs Combin.*, 37(2021), 971–985.
- [10] M. A. Rajan, K. Ch. Das, V. Lokesha and I. N. Cangul, On some properties of coprime Labelled graphs, *Turkish Journal of Analysis and Number Theory*, 7(2019) 77–84.
- [11] S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, First edition, Fourth Estate and Doubleday, 1999.

- [12] V. A. Ustimenko, On graph-based cryptography and symbolic computations, *Serdica J. Comput.*, 1(2007), 131–156.
- [13] M. Yamuna, M. Gogia, A. Sikka and M. J. H. Khan, Encryption using graph theory and linear algebra, *International Journal of Computer Application*, 5(2012), 102–107.