Playfair using DES Algorithm, 7 by 9 Matrix and Colour Substitution

C. S. Subramaniyam
Dept of CSE,
Alpha College of Engineering,Chennai.

ABSTRACT
In this paper the playfair cipher is handled in a new way from the normal way of encrypting the plain text with alphabet only.In this paper encrypting the plain text with the help of colours is discussed.Traditionally encrypting the text elements is done by the use of the text only,but here new encryption techinique by using the colours is used.

In this paper two different things that is the difference in the normal playfair techinique,and the other is that encrypting with the colours which makes the decryption by the hackers some more difficult.Then the other thing is that we are implementing the DES techinique in playfair to make it more difficult for the hacker to decrypt.Through this method we can encrypt both the uppercase and lowercase letters with case sensitive patterns and also the numeric datas.First use the colour substitution for the plain text and then the encryption takes place with the help of colours.

Keywords
playfair;coloursubstitution;DESalgorithm;encryption;decryption

1. INTRODUCTION
Cryptography is the science of using mathematics to encrypt and decrypt data. It enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient. There are various encryption techniques in today's world. Symmetric key cryptography technique is very useful for encryption process. In symmetric key cryptography, sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Symmetric key cryptography is also called the private key cryptography. Playfair cipher is one of the popular symmetric encryption methods.

The first recorded description of the Playfair cipher was in a document signed by Wheatstone on 26 March 1854. However Lord Playfair promoted the use of this cipher and hence it is called Playfair Cipher. It was used by the British in the Second Boer War and in World War I. It was also used by the Australians and Germans during World War II. Playfair is reasonably easy to use and was used to handle important but non-critical secrets. By the time the enemy cryptanalysts could break the message, the information would be useless to them. Between February 1941 and September 1945 the Government of New Zealand used it for communication between New Zealand, the Chatham Islands and the Pacific Islands.

The techinique of encryption and decryption is in the form of colours.There are many techinique used for the encryption among those techiniques playfair is considered as the best techinique.In this paper work to improve the techinique in a more better way is done,for improving this techinique the use of the colour substitution techinique.Two keys are used for the encryption. one is for forming the key1 playfair table and the other is for the key2 playfair table . use two type of tables one is for the colour substitution of the alphabets and the other table is for the playfair table which consist of the colours. This paper is going to deal the data with colours completely.

The organization of the paper can be summarized as: The existing playfair algorithm using 5 x 5 matrix explained in Section-II. Limitations of existing playfair cipher discussed

in Section-III, Extended 7 by 9 playfair cipher algorithm explained in Section-IV. Rules for encryption in Section-V. Rules for decryption in SectionVI. Working procedures are discussed in Section-VII. Example worked are discussed in Section VIII. Advantages of proposed algorithm are discussed in Section XI. Disadvantages of proposed algorithm are discussed in Section X. Conclusions are explained in Section-XI.

2. EXISTING PLAYFAIR ALGORITHM USING 5 X 5 MATRIX
The traditional Playfair cipher uses 25 uppercase alphabets. A secret keyword is chosen and the 5 x 5 matrix is built up by placing the keyword without any duplication of letters from left to right and from top to bottom. The other letters of the alphabet are then placed in the matrix. For example if we choose "PLAYFAIREXAMPLE" as the secret keyword the matrix is given in Table 1.

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

In this algorithm, the letters I & J are counted as one character. It is seen that the rules of encryption applies a pair of plaintext characters. So, it needs always even number of characters in plaintext message. In case, the message counts odd number of characters a spare letter X is added at the end of the plaintext message. Further repeating plaintext letters in the same pair are separated with a filler letter, such as X, so that the words COMMUNICATE would be treated as CO MX MU NI CA TE.

Rules:

1. Plain text letters that fall in the same row of the matrix are replaced by the letter to the right, with the first element of the row circularly following the last. For example RE is encrypted as EX.
2. Plain text letters that fall in the same column are replaced by the letter beneath, with the top element

of the row circularly following in the last. For example, RC is encrypted as CN.

3. Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, OH becomes SD, and FD becomes AH.

3. LIMITATIONS OF EXISTING PLAYFAIR CIPHER

The main drawback of the traditional Playfair cipher is that the plain text can consist of 25 uppercase letters only. One letter has to be omitted and cannot be reconstructed after decryption. Also lowercase letters and numbers cannot be handled by the traditional cipher. This means that complete sentences cannot be handled by this cipher.

A spare letter X is added when the plaintext word consists of odd number of character. In the decryption process this X is ignored. X is a valid character and creates confusion because it could be a part of plaintext, so we cannot simply remove X in decryption process.

X is used a filler letter while repeating letter falls in the same pair are separated.

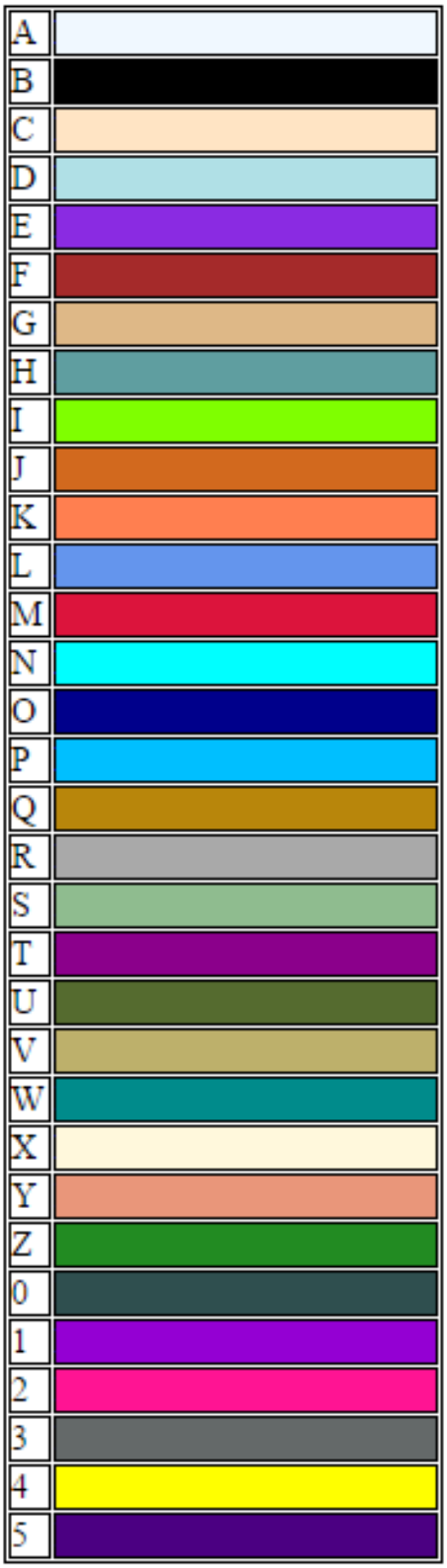
In a mono alphabetic cipher the attacker has to search in 26 letters only. Playfair cipher being a polyalphabetic cipher the attacker has to search in 26 x 26 = 676 diagrams. Although the frequency analysis is much more difficult than in mono alphabetic cipher still using modern computational techniques the attacker can decipher the cipher text.

To overcome the drawbacks of the existing playfair we modified the playfair cipher with 7x9 matrix which includes all the upper and lower case letters and the numeric values.

4. EXTENDED PLAYFAIR WITH 7x9 MATRIX

To overcome the drawbacks of traditional playfair cipher algorithm introduction of a new techinique with 7x9 matrix is made.This matrix is filled with the colours representing the alphabets in upper case,lower case and the numbers,so that encryption of both the alphanumeric values with case sensitive manner is possible.This table is filled from the left to right and top to bottom.In this table first the colours representing the keyword characters are placed first followed by the upper case letters without repetation followed by the numbers followed by the lower case letters.First this play fair is mainly based on the colour substitution table which consist of the colours for the respective alphabets and the numbers. This is the primary table to fill the colours in the playfair table.One additional ”*” symbol is also added to it to separate the repeating characters.

4.1 Colour Substitution Table



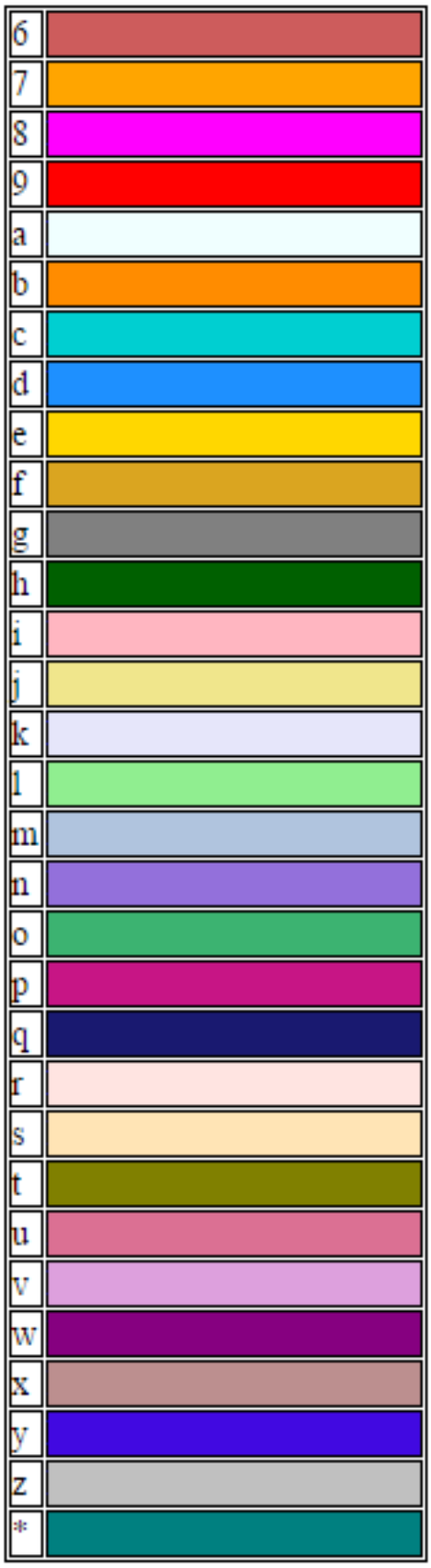
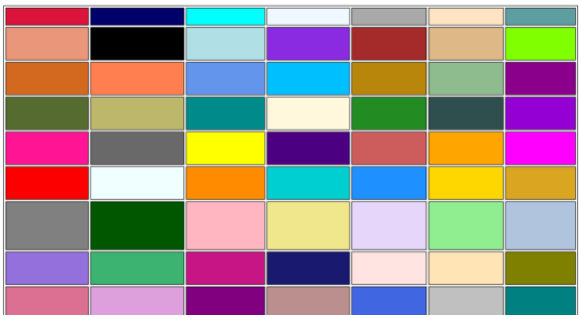


Table For Key K1

By using the above table the plain text is substituted with the colours and the plain text is converted as the colours. After the colour substitution by using the above table the plain text are divided into pair of colours without repeating letters in the same pair then the matrix is constructed by using the keyword k1. Let us consider the keyword k1 as MONARCHY. The colours corresponding to the keyword is filled in the table first followed by the colours of upper case letters followed by colours of numbers followed by the colours of the lower case letters. The table with the keyword MONARCHY is shown below:

Keyword:MONARCHY

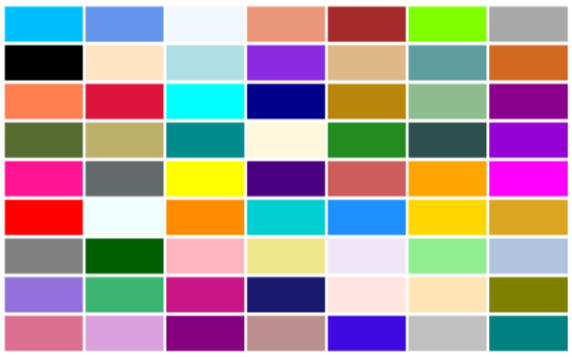


The above given playfair table is divided into four quadrants and the fourth column and fifth row are collectively known as middle plus. No encryption or decryption is required for the colour which present in this middle plus sign cells. By using this five divisions the encryption is handled.

Table for Key K2

This table is used for the decryption process with the second key k2. And the table with the key k2 is formed .with this table the encryption,decryption algorithm is applied in the decryption ,encryption process respectively.The table with the keyword playfair is shown below:

Keyword:PLAYFAIR



This table is also used in then same way as specified for the above table but it works with the different keyword. The rules for encryption and decryption algorithm is shown below:

5. RULES FOR ENCRYPTION

- Repeating plain text colours are separated by the colour of the * inbetween the two same colours in a pair.
- Two plain text colours that falls in the same quadrant are each replaced by the colours to the down
- Two plain text colours that falls in the same top side but in the different quadrant are replaced by the colour to the right.

- Two plain text colours that falls in the same bottom side but in the different quadrant are replaced by the colour to the left.
- Two plain text colours that falls in the different quadrant are replaced by the colour to the top.
- Two plain colours that falls in the middle plus are replaced by the same colour.
- If one plain text colour falls in the quadrant and the other falls in the middle plus then replace the plain text colour in the quadrant by the colour to its top and the plain text colour that falls in the middle plus is replaced by the same colour.

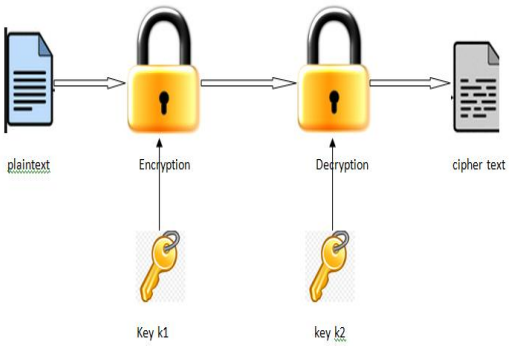
6. RULES FOR DECRYPTION

- Two colours that falls in the same quadrant are replaced by the colour to the top.
- Two colours that falls in the top side but different quadrant are replaced by the colour to the left.
- Two colours that falls in the bottom side but in the different quadrant are replaced by the colour to the right.
- Two colours that falls in the different quadrant are replaced by the colour to the bottom.
- Two colours that falls in the middle plus are not replaced.
- If one colour falls in the quadrant and the other falls in the middle plus then replace the colour in the quadrant by the colour to the top and the colour that falls in the middle plus is replaced by the same colour.
- After the decryption remove the colour corresponding to the * is removed from the decrypted colour.

7. WORKING PROCEDURE

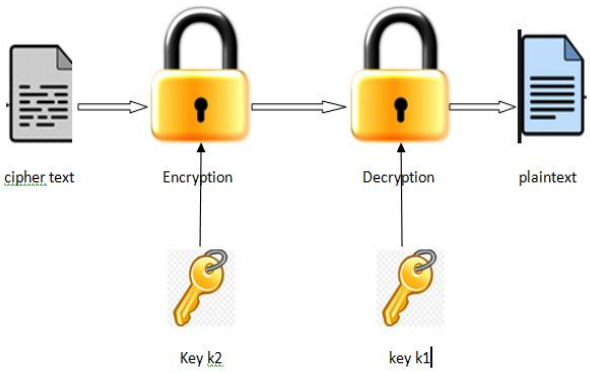
- The plain text is replaced by the colours by using the colour substitution table.
- After the colour substitution you will get the plain text colours.
- Then split the colours into a pair of colours.If two colours appear in the same pair introduce the colour of the * between these colours. If there is only one colour present in the pair then add the colour of the * at the last.
- while encrypting the plain text is given with two keys one is for constructing the Encryption table and the other is for constructing Decryption table
- Now construct the Encryption table with the given keyword k1and encrypt the plain text colours with the encryption rules.
- Then construct the Decryption table with the given keyword k2 and decrypt the plain text colours with the encryption rules
- The resulting colour is the encrypted colour this colour is sent to the receiver.
- In the receiver end the receiver gets the encrypted colour with the two keys.
- With the keys the receiver construct the Encryption and Decryption table
- Then first perform encryption by using the keyword k2, then perform decryption by using key k1.
- At last the colour corresponding to * is removed and the colour is converted into the text to get the plain text sent by the sender.

Encryption



(a)Encryption process

Decryption:



(b)Decryption process

8. EXAMPLE

Plain text:Balloon

Keyword k1:MONARCHY

Keyword k2:PLAYFAIR

Encryption:
STEP 1:
Convert the plain text into colours.

STEP 2:
Split the colours into pairs.

STEP 3:
Introduce the colour of * in between the repeating colours.

STEP 4:
Again split the colours into pairs

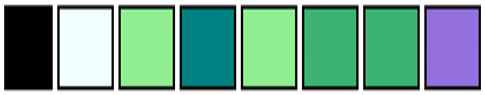
STEP 5:
Encryption (Iteration 1)

Decryption(Iteration 2)

Decryption:
STEP 1:

Encryption(iteration1)

STEP 2:
Decryption(iteration2)



STEP 3:
Remove the colour representing *

STEP 4:
After reverse colour substitution

Plain text:Balloon

9. ADVANTAGES OF PROPOSED ALGORITHM

1. There is no chance to cryptanalyze.
2. Overcomes the limitation of simple Playfair square cipher.
3. Easy to perform substitution
4. The algorithm uses the colour which is difficult to decrypt by the hacker

10. DISADVANTAGE OF PROPOSED ALGORITHM

1. It makes use of two keys.
2. It is difficult to implement.
3. The receiver must follow the same colour substitution table .
4. If the key k1 and k2 are same it directly specify the plaintext.

11. CONCLUSION

In this paper the way how to improve security of play fair square Cipher to make it more secure and strong by Its implementation with substitution and transposition techniques is discussed. This playfair cipher can be used in the transmission of the messages such as e-mails and the messages in the mobile applications.

12. ACKNOWLEDGMENT

Author would like to give sincere gratitude especially to Mrs. Sukanya sargunar and Mr.Santhakumar.T (Asst Prof CSE) for their guidance and support to pursue this work.

13. REFERENCES

[1] Stallings, W. (2006). Cryptography and Network Security: Principles and Practice(4th ed.). Prentice Hall: New York

[2] Stallings, W. (2004). Cryptography and Network Security – Principles and Practices(3rd ed.). Pearson Education: Boston

[3] Stallings, W. (2003), Cryptography and Network Security, (3rd ed.). Pearson Education:Boston

[4] A. Aftab Alam, B. Shah Khalid, and C. Muhammad Salam," A Modified Version of Playfair Cipher Using 7×4 Matrix", International Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013.

[5] Sombir Singh* Sunil K. Maakar Dr.Sudesh Kumar," Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques", Volume 3, Issue 6, June 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[6] Yahaya Bala Zakariyau, Zirra Peter Buba and Gregory Maksha Wajiga," Securing Message Transactions through Modified Playfair Cipher Technique", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 12, December 2015.

[7] Subhajit Bhattacharyya, Nisarga Chand and Subham Chakraborty,"A Modified Encryption Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3, Issue 2, February 2014.

[8] Monika Arora, Anish Sandiliya and Jawad Ahmad Dar," Modified Encryption Technique by Triple Substitution on Playfair Square Cipher Using 6 By 6 Matrix with Five Iteration Steps", International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 4, 2015.

[9] en.wikipedia.org/wiki/Playfair_cipher

[10] en.wikipedia.org/wiki/Cryptography