International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

# Design and Analysis of Modified Playfair Square Cipher Algorithm Using 6 By 6 Matrix with Five Iteration Steps and its Implementation in C/C++

**Monika Arora[1], Anish Sandiliya[2]**

[1]Research Scholar, Department of Computer Science and Engineering
NNSS, Samalkha Group of Institutions, Kurukshetra University Kurukshetra, Haryana, India

Assistant Professor, Department of Computer Science and Engineering
NNSS, Samalkha Group of Institutions, Kurukshetra University Kurukshetra, Haryana, India

**Abstract:** ***An ad-hoc network generally consists of nodes, on which sensors are embedded to provide security measures. The main challenge of these sensors is to provide security of data and also to work effectively within a limitation of power and memory. This paper is a step toward developing an encryption system which can encrypt any text messages securely. Cryptography is an art and science of converting original message into no readable form. There are two techniques for converting data into no readable form. Transposition technique, Substitution technique. In recent years there is drastic progress in Internet world. Sensitive information can be shared through internet but this information sharing is susceptible to certain attacks. Cryptography was introduced to solve this problem. Cryptography is art for achieving security by encoding the plain text message to cipher text. Substitution and transposition are techniques for encoding. When Caesar cipher substitution, Rail fence cipher and Columnar Transposition Cipher techniques are used individually, cipher text obtained is easy to crack. This Paper will present a perspective on combination of techniques like substitution and transposition with play fair square cipher to enhance its security. Play fair 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. To enhance its security we combine it with transposition and substitution cipher techniques, to minimize attacks on it(Cryptanalyst), by performing double substitution and transposition Techniques. There are two main disadvantages of traditional play fair cipher matrix. First one is we have to compromise between I and J and second one is we cannot include numeric values in this matrix. This matrix consists of alphabets A to Z and numeric values 0 to 9.Here we use Five Iteration steps to make strong encrypted message.***

**Keywords:** Caesar cipher**,** Play fair cipher, key, columnar transposition, cryptography, cryptanalysis, C/C++

## 1. Introduction

This modern era is dominated by paperless offices-mail messages-cash transactions and virtual departmental stores. Due to this there is a great need of interchanging of data through internet. The dramatic rise of internet has opened the possibilities that no one had imagined. We can connect to any person, any organization or any computer, no matters how far we are from them. Internet cannot be used only for browsing purpose. Sensitive information like banking transactions, credit card information and confidential data can be shared through internet. But still we are left with a difficult job of protecting network from variety of attacks. With the lots of efforts, network support staff came up with solution to our problem named "Cryptography". Cryptography is the art of achieving security by encoding the data into unreadable form. Data that can be read and understood without any difficulty is called plain text or clear text. The method of encoding Plain text in such a way as to hide its content is called encryption. Encrypting plain text results in unreadable gibberish called cipher text. You use Encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting cipher text to its original plain text is called decryption. There are two primary ways in which plaintext can b codified to corresponding Cipher text: Substitution and Transposition. A Substitution technique is one in which the letters of Plain text are replaced by other letters or by numbers(Caesar Cipher, Hill Cipher, Mon alphabetic cipher etc).A Transposition technique is one in which the letters of the message are rearranged or permuted. (Rail Fence method, Columnar method etc.).The columnar transposition cipher is a fairly simple, easy to implement cipher. It is a transposition cipher that follows a simple rule for mixing up the characters in the plaintext to form the cipher text. Although weak on its own, it can be combined with other ciphers, such as a substitution cipher, the combination of which can be more difficult to break than either cipher on it's own. Play fair cipher is one of the popular symmetric encryption methods. The first recorded description of the Play fair cipher was in a document signed by Wheatstone on 26 March 1854. However Lord Play fair promoted the use of this cipher and hence it is called Play fair 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.


Licensed Under Creative Commons Attribution CC BY

## 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 | 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:

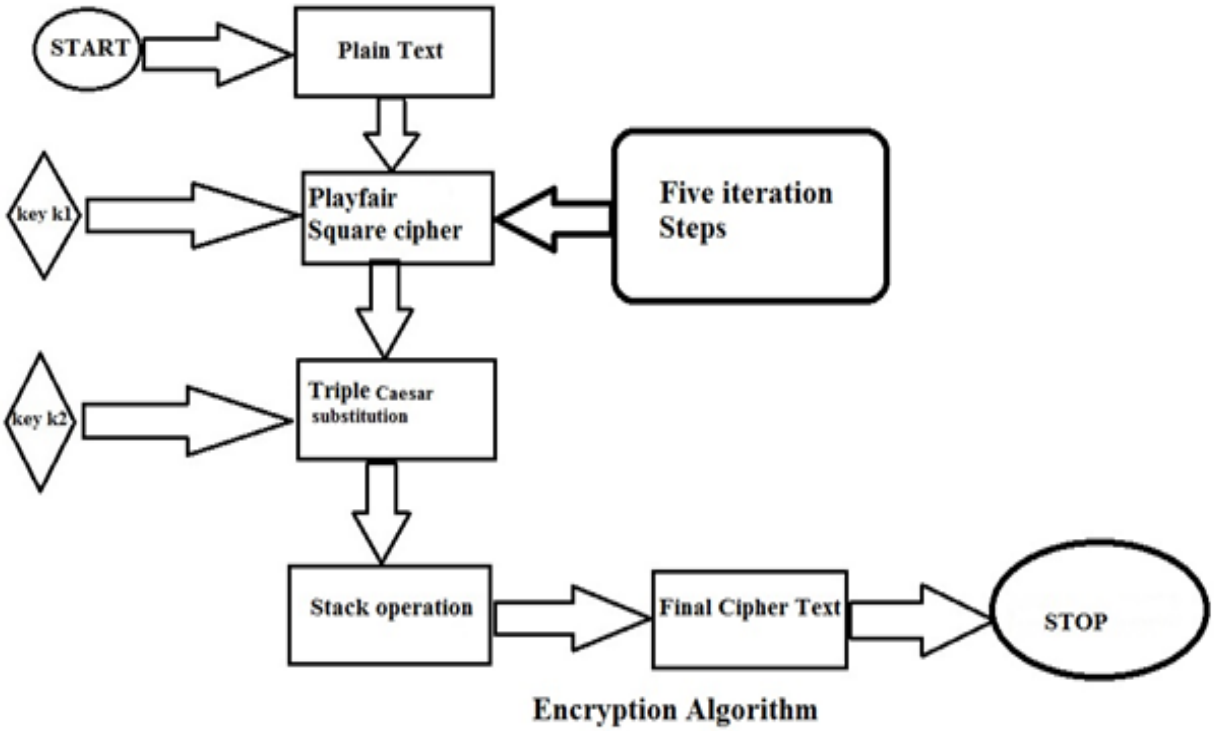
1) Plain text letters that fall in the same row of the matrix are replaced by the letter to the right, with the first element of the row circularly following the last. For example RE is encrypted as EX.
2) Plain text letters that fall in the same column are replaced by the letter beneath, with the top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

### 2.1 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, white space, numbers and other printable characters cannot be handled by the traditional cipher. This means that complete sentences cannot be handled by this cipher. Space between two words in the plaintext is not considered as one character. 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. So performing double substitution and transposition on playfair cipher will considerably increases its security.

## 3. Proposed Work

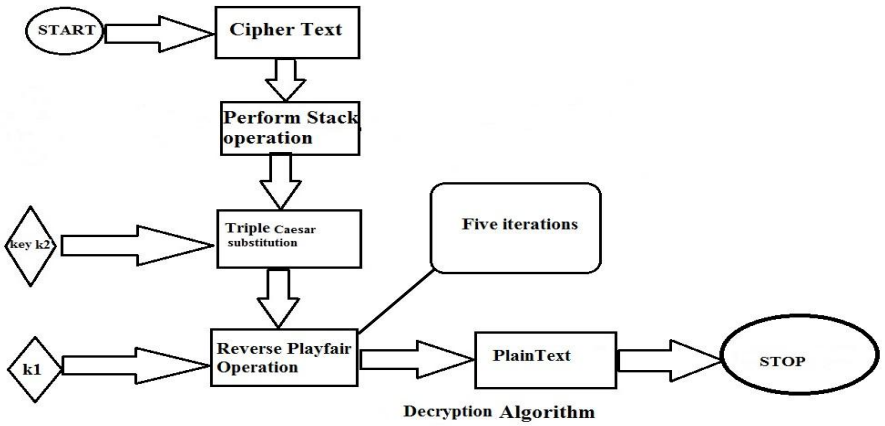
### 3.1Block diagram for Encryption Algorithm




Encryption Algorithm


Licensed Under Creative Commons Attribution CC BY

### 3.2 Block diagram for decryption algorithm



Decryption Algorithm

**Extended 6 by 6 Playfair Cipher Algorithm Using Five Iteration Steps**

This extended play fair algorithm is based on the use of a 6x6 matrix of letters constructed using a keyword. The matrix is constructed by filling in the letters of the keyword from left to right and from top to bottom, and the filling in the remainder of the matrix with the remaining letters in alphabetic order and digits in ascending order form 0 to 9.the digits 0 to 9 can be placed next cells of the alphabet z in the ascending order. In this we have not counted I/J as one letter instead we are placing both I and J in two different cells in order to avoid the ambiguity to the user at the time of decipherment. This algorithm can allow the plaintext containing of alpha numeric values, hence the user can easily encrypt alpha numeric values efficiently. The plain text containing contact numbers, date of birth, house numbers and other numerical values can easily and efficiently encrypted using this algorithm.

Here we have used five reserved keywords: COMPUTER, MONARCHY, PLAYFAIR, ENCRYPTION AND DIAMONDS. Five 6 by 6 matrices are shown below

**Keyword: Computer**

| C | O | M | P | U | T |
|---|---|---|---|---|---|
| E | R | A | B | D | F |
| G | H | I | J | K | L |
| N | Q | S | V | W | X |
| Y | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

**Keyword: Monarchy**

| M | O | N | A | R | C |
|---|---|---|---|---|---|
| H | Y | B | D | E | F |
| G | I | J | K | L | P |
| Q | S | T | U | V | W |
| X | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

**Keyword: Playfair**

| P | L | A | Y | F | I |
|---|---|---|---|---|---|
| R | B | C | D | E | G |
| H | J | K | M | N | O |
| Q | S | T | U | V | W |
| X | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

**Keyword: Encryption**

| E | N | C | R | Y | P |
|---|---|---|---|---|---|
| T | I | O | A | B | D |
| F | G | H | J | K | L |
| M | Q | S | U | V | W |
| X | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

**Keyword: Diamonds**

| D | I | A | M | O | N |
|---|---|---|---|---|---|
| S | B | C | E | F | G |
| H | J | K | L | P | Q |
| R | T | U | V | W | X |
| Y | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

### 3.3 Algorithm

**Encryption**

1) Take Plain text as input from user.
2) if any space or punctuations occurs, then it should be automatically removed from the input message.
3) After that we check any double occurrence, and add “X” automatically in between these two characters.
4) After removing the unwanted space and punctuations we get a modified message that is called the digraph message.
5) Next we encrypt this diagraph message with the keyword: “COMPUTER”
6) After that corresponding four iteration steps introduced with four different keywords:”MONARCHY”, ”PLAYFAIR”, ”ENCRYPTION” and “DIAMONDS”.
7) During encryption process if any two character occurs same row or column and any one of the character occurs at last column(for same row character) or at the last row(for same column character) then in the encrypted message they becomes first column character(for same row character) or first row character(for same column character).
8) Next we perform Triple Substitution using Key K1.
9) Finally we perform stack operation on step 8.
10) The cipher text obtained above is our final cipher text.

**Decryption**

1) Take the cipher text you want to decrypt from user.
2) Perform Triple substitution on Above step using Key K1.
3) Perform Stack operation on Step 2
4) Next we decrypt the last encrypted message with the


Licensed Under Creative Commons Attribution CC BY

keywords:"DIAMONDS". And repeat the same decryption process four times with four different keywords: ENCRYPTION", PLAYFAIR", MONARCHY", and "COMPUTER" respectively.

5) During decryption process if any two character occurs same row or same coloumn and any one of the character occurs at the first coloumn(for same row character) or at the first row(for same coloumn character), then in the encrypted message it becomes last column character(for same row character)or last row character(for same coloumn character).
6) Finally we recover the orginal text message which we give at the outset

## 4. Example

### 4.1 Encryption

1) Let the plain text is SAMALKHA ENGINEERING COLLEGE.
2) Now Write The Plain Text as :**SA MA LK HA EN GI NE ER IN GC OL LE GE.**
3) Using Five Keywords Encrypt the Above Digraphs, as shown.

**Key Word : Computer**

| C | O | M | P | U | T |
|---|---|---|---|---|---|
| E | R | A | B | D | F |
| G | H | I | J | K | L |
| N | Q | S | V | W | X |
| Y | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

**CT1:0IAIGLIRGYHJYGRAGSNETHGFNG**

**Keyword: Monarchy**

| M | O | N | A | R | C |
|---|---|---|---|---|---|
| H | Y | B | D | E | F |
| G | I | J | K | L | P |
| Q | S | T | U | V | W |
| X | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

**CT2:ZJOKIPLOIHBGHICRIQRBQBPHMJ**

**Keyword: Playfair**

| P | L | A | Y | F | I |
|---|---|---|---|---|---|
| R | B | C | D | E | G |
| H | J | K | M | N | O |
| Q | S | T | U | V | W |
| X | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

**CT3:5SHMPLIJPOCROPDBPWBCSRRQNK**

**Keyword: Encryption**

| E | N | C | R | Y | P |
|---|---|---|---|---|---|
| T | I | O | A | B | D |
| F | G | H | J | K | L |
| M | Q | S | U | V | W |
| X | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

**CT4:6QFSDWAGCDRYDCTDD3OYUCNUYG**

**Keyword: Diamonds**

| D | I | A | M | O | N |
|---|---|---|---|---|---|
| S | B | C | E | F | G |
| H | J | K | L | P | Q |
| R | T | U | V | W | X |
| Y | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

**CT5:9KGBORNCSAY4ASRINYD20KAXH3**

**Final Cipher Text is**
**CT5:9KGBORNCSAY4ASRINYD20KAXH3**

4. Perform Substitution on CT5 Using Key K1=2, three times
**CT5:9KGBORNCSAY4ASRINYD20KAXH3**we get
**CT6:1MIDQTPEUCA6CUTKPAF42MCZJ5**
**CT7:3OKFSVRGWEC8EWVMRCH64OEBL7**
**CT8:5QMHUXTIYGE0GYXOTEJ86QGDN9**
**5.**Reverse the text obtained in above Step 4(CT8), as
**CT9:9NDGQ68JETOXYG0EGYITXUHMQ5**
**6.**Output of Step 5 is our Required Cipher text.

### 5.2. *Decryption*

**1.**Take Cipher Text from user, let it be
**CT9:9NDGQ68JETOXYG0EGYITXUHMQ5**

**2.**Perform reverse substitution using key k2=2 3 times, we get
**CT8:5QMHUXTIYGE0GYXOTEJ86QGDN9**
**CT7:3OKFSVRGWEC8EWVMRCH64OEBL7**
**CT6:1MIDQTPEUCA6CUTKPAF42MCZJ5**
**CT5:9KGBORNCSAY4ASRINYD20KAXH3**

**3.**Using Five Keywords Encrypt the Above Digraphs CT5, as shown.

**KEYWORD: DIAMONDS**
**CT5: 9KGBORNCSAY4ASRINYD20KAXH3**

| D | I | A | M | O | N |
|---|---|---|---|---|---|
| S | B | C | E | F | G |
| H | J | K | L | P | Q |
| R | T | U | V | W | X |
| Y | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

**CT4:6QFSDWAGCDRYDCTDD3OYUCNUYG**

**KEYWORD: ENCRYPTION**

| E | N | C | R | Y | P |
|---|---|---|---|---|---|
| T | I | O | A | B | D |
| F | G | H | J | K | L |
| M | Q | S | U | V | W |
| X | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

**CT3:5SHMPLIJPOCROPDBPWBCSRRQNK**

**KEYWORD: PLAYFAIR**

| P | L | A | Y | F | I |
|---|---|---|---|---|---|
| R | B | C | D | E | G |
| H | J | K | M | N | O |
| Q | S | T | U | V | W |
| X | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |


Licensed Under Creative Commons Attribution CC BY

**CT2:ZJOKIPLOIHBGHICRIQRBQBPHMJ**

**KEYWORD: MONARCHY**

| | | | | | |
|---|---|---|---|---|---|
| **M** | **O** | **N** | **A** | **R** | **C** |
| **H** | **Y** | B | D | E | F |
| G | I | J | K | L | P |
| Q | S | T | U | V | W |
| X | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

**CT1:0IAIGLIRGYHJYGRAGSNETHGFNG.**

**KEY WORD: COMPUTER**

| | | | | | |
|---|---|---|---|---|---|
| **C** | **O** | **M** | **P** | **U** | **T** |
| **E** | **R** | A | B | D | F |
| G | H | I | J | K | L |
| N | Q | S | V | W | X |
| Y | Z | 0 | 1 | 2 | 3 |
| 4 | 5 | 6 | 7 | 8 | 9 |

**4.**Now Write The Plain Text as :**SA MA LK HA EN GI NE ER IN GC OL LE GE.**

SAMALKHA ENGINEERING COLLEGE.

## 5. Advantages of Proposed Algorithm

**1.** Diverse cipher text
If we scrutinize at the Algorithm we can notice at every Stage we are getting diverse cipher text, thus more trouble to cryptanalyst.
**2.** Brute force attack on it is impossible
**3.** There is no chance to cryptanalyze.
**4.**Overcomes the limitation of simple Playfair square cipher.
**5.** Easy to perform substitution

## 6. Disadvantage of Proposed Algorithm

**1.** It makes use of two keys.
**2.** difficult to implement.

## 7. Implementation in Turbo C/C++

**(A).Encryption algorithm**

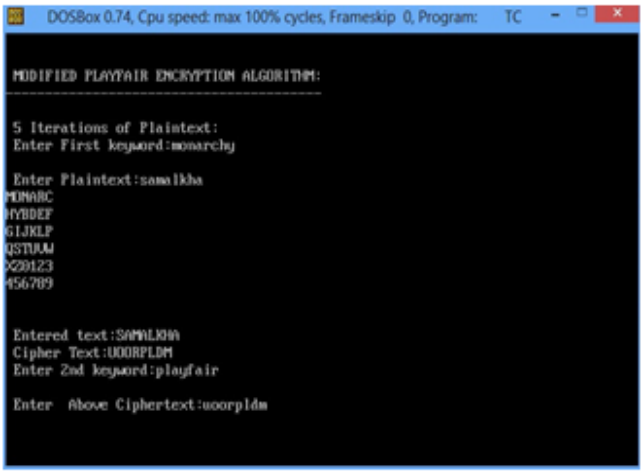



**Figure 1**

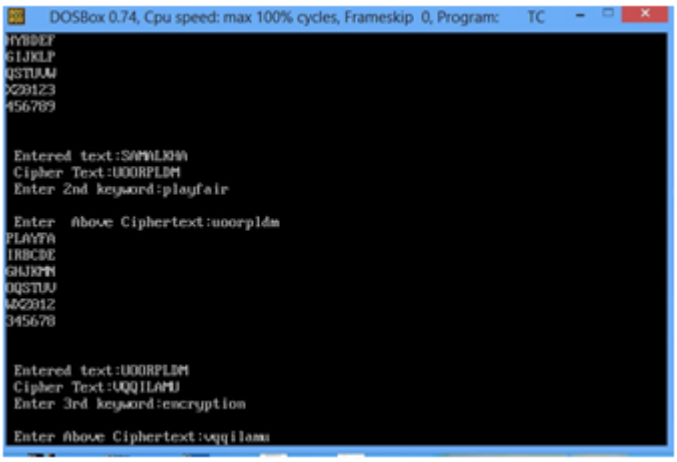



**Figure 2**

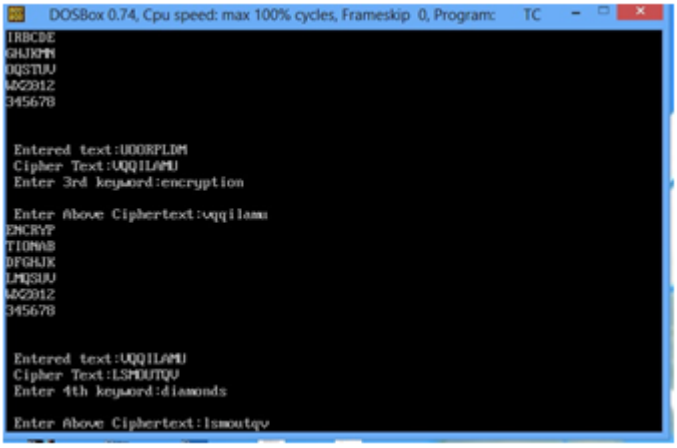



**Figure 3**

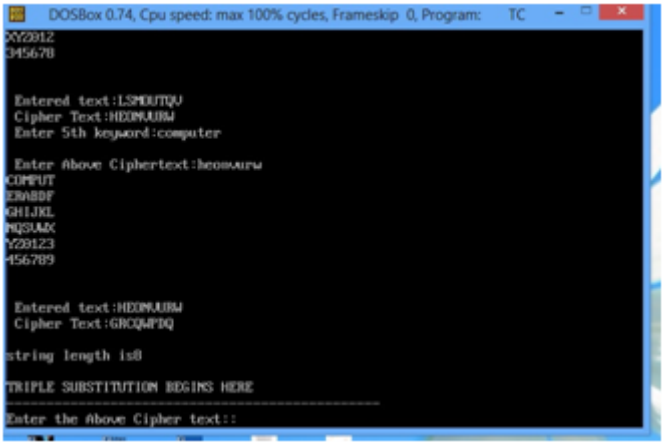



**Figure 4**

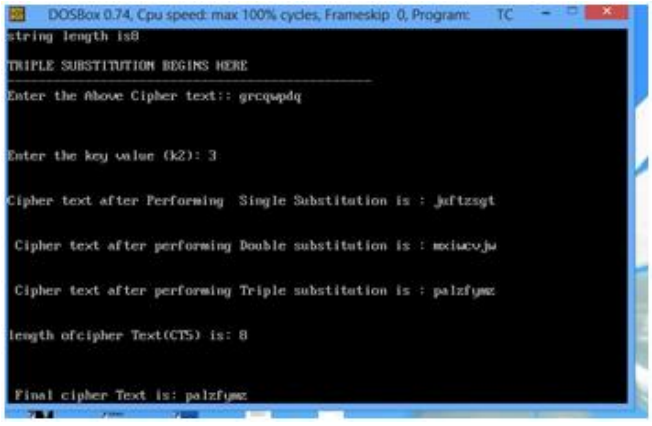



**Figure 5**


Licensed Under Creative Commons Attribution CC BY

**(B) Decryption Algorithm**

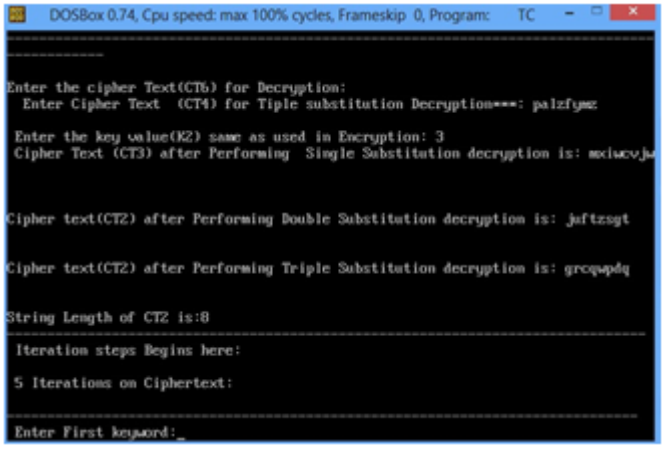



**Figure 6**

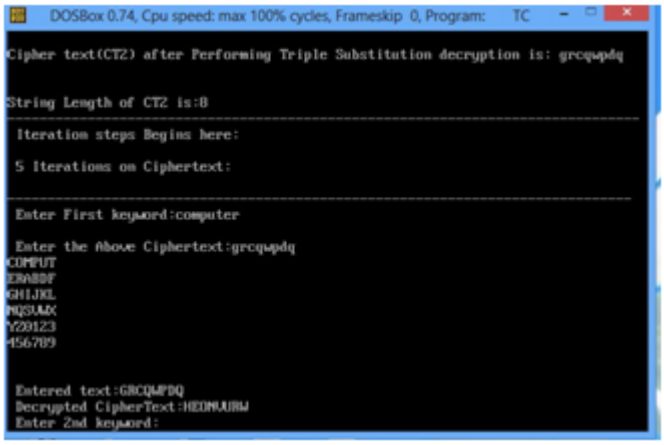



**Figure 7**

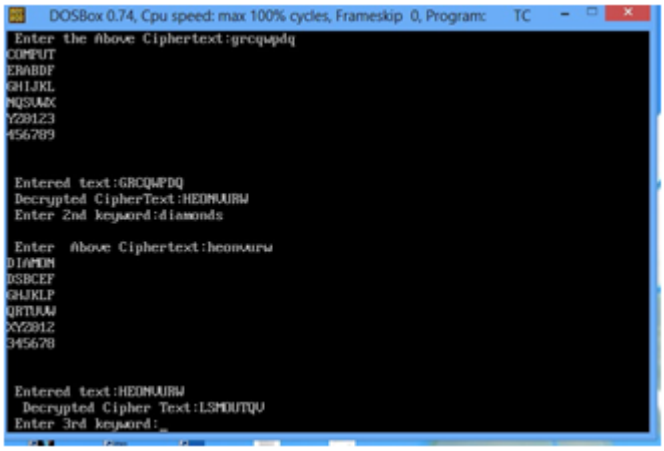



**Figure 8**

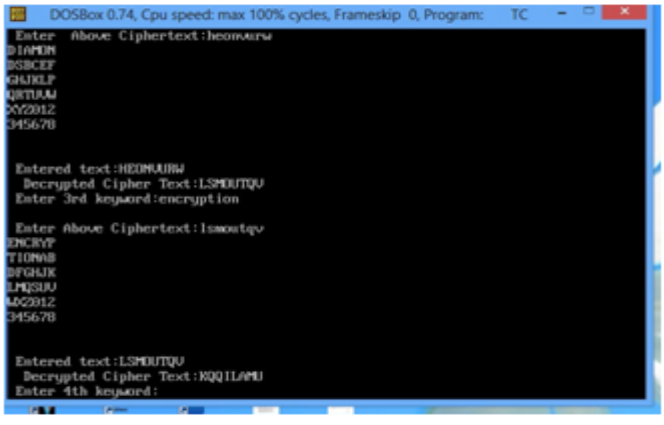



**Figure 9**

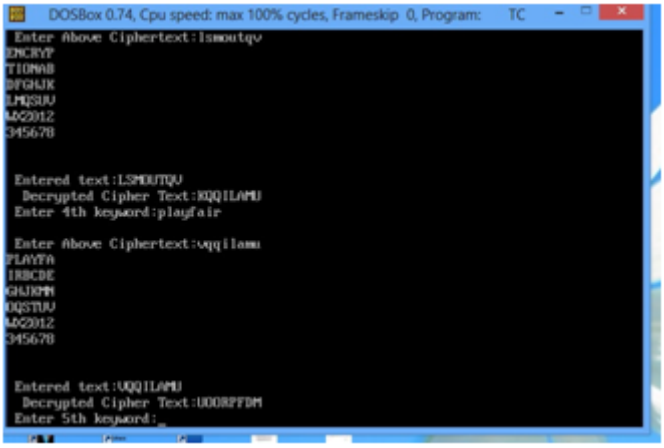



**Figure 10**

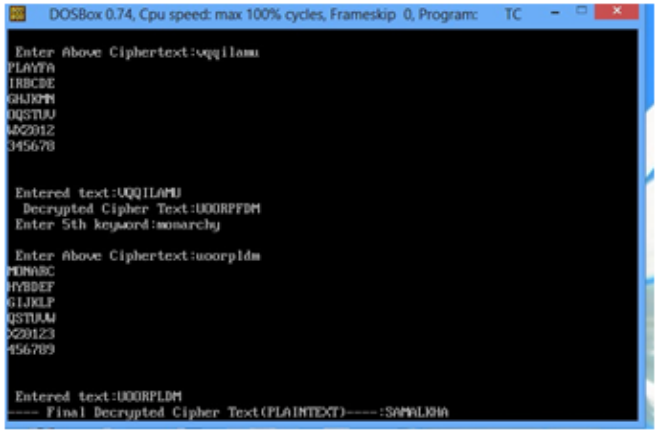



**Figure 11**

## 8. Conclusion

In this paper we have presented how to modify security of play fair square Cipher to make it more secure and strong by Its implementation with substitution and transposition techniques. I we have analyzed the merits and demerits of the original play fair cipher. Then we discussed the modified play fair cipher using double substitution and transposition cipher. Finally the proposed algorithm works successfully.

## 9. Acknowledgment

Author would like to give sincere gratitude especially to Mr. Anish, (Astt Prof CSE) for his guidance and support to pursue this work.

## References

[1] Jawad ahmad dar, *"Humanizing the Security of Rail Fence Cipher Using Double Transposition and Substitution Techniques*, International *Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Volume 3 Issue 9, September 2014*
[2] Atul Kahate (2009), *Cryptography and Network Security*, second edition, McGraw-Hill
[3] William Stalling *"Network Security Essentials(Applications and Standards)*", Pearson Education, 2004
[4] practicalcryptography.com/ciphers/rail-fence-cipher/


Licensed Under Creative Commons Attribution CC BY

[5] Charles P.Pfleeger "Security in Computing", 4th edition, Pearson Education
[6] Neal R. Wagner *"The Laws of Cryptography: Perfect Cryptography: The One-Time Pad "*
[7] jawad ahmad dar, sandeep Sharma" Implementation of One Time Pad cipher with Rail Fence and Simple Columnar Transposition Cipher, for Achieving Data security,, International *Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Volume 3 Issue 11, November 2014*
[8] jawad ahmad dar, Enhancing the data security of simple columnar transposition cipher by Caesar cipher and Rail fence cipher technique. International Journal of Computer Science & Engineering Technology (IJCSET), ISSN : 2229-3345 Vol. 5 No. 11 Nov 2014

## Author Profile

**Monika Arora** is currently in final year **M- TECH** Computer science and Engineering from **Kurukshetra University, Kurukshetra**, Her interested areas of research are Neural Networks, Mobile computing, Network security, and Algorithms.


Licensed Under Creative Commons Attribution CC BY