Enhanced the Security of Playfair Technique using Excess 3 Code (XS3) and Ceasar Cipher

Zubair Iqbal
Asst. Prof., Dept. of CS & IT,
M.I.T, Moradabad

Bhumika Gupta
Asst. Prof., Dept. of CS&E,
GB Pant Eng. College

Kamal Kr. Gola
Lecturer in Dept. of CS&E.
T.M.U., Moradabad

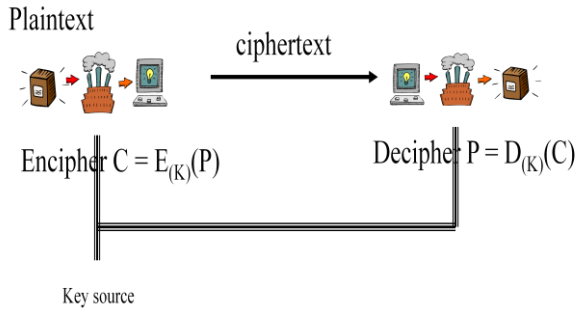
Prachi Gupta
Asst. Prof., Dept. of CS & IT,
M.I.T, Moradabad

ABSTRACT
The main purpose of our research is to provide security for the data that contains alphabets and integer values during the transmission, when data is transmitted form sender to receiver. As we know that playfair technique if best for multiple letter encryption, which treats the plain text as single units and translates these units into cipher text. It is highly difficult to the attacker to understand or to decrypt the cipher text. The existing playfair technique is based on the use of a 5 X 5 matrix of letters constructed using a keyword. This algorithm can only allow the text that contains alphabets only. But many algorithms have been proposed that allow text which contains alphabets, integers as well as special symbols using 6 * 6 matrix and 10 * 9 matrix etc. In playfair technique a groups of 2 letters in the plain text is converted to cipher text during encryption using a key. Similarly on other hand during decryption cipher text are converted to plain text using the same key. Some time it may be possible for the attacker to understand the plaintext. To overcome this problem we proposed an algorithm that extends the security of playfair technique using excess 3 code and ceasar cipher technique where first each alphabets and integer is converted into binary number and then its equivalent excess 3 code and after that with the help of key encryption process will be apply. In our proposed technique we are using 6 * 6 matrix which contain alphabets and integers only.

General Terms
SECURITY

Keywords
Playfair cipher, excess 3 code, ceasar cipher, Plaintext, cipher text, rectangular matrix, key, encryption, decryption, binary number.

1. INTRODUCTION
The Playfair cipher or Playfair square is a manual symmetric encryption technique and was the first literal digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair who promoted the use of the cipher. When information is transmitted from the sender to the receiver care should be taken so that the information is not accessible to a third party. One of the ways to protect information is the method of encryption and decryption whereby the sender encrypts the message with a secret key which is known only to the receiver. Once the receiver gets the message the message is decrypted using the same secret key. This type of encryption is known as symmetric encryption. Playfair cipher[1] is one of the well known symmetric encryption methods. The first recorded description of the Playfair cipher [2] 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 technique encrypts [3] pairs of letters (digraphs), instead of single letters as in the simple substitution cipher. The Play fair cipher uses a 5 by 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules was all that was required to create the 5 by 5 table and use the cipher.



2. TRADITIONAL PLAYFAIR CHIPER TECHNIQUE
This section briefly described the existing play fair cipher algorithm.

The existing play fair cipher algorithm is based on with use of 5 X 5 matrix of letters constructed using a keyword. The existing Playfair algorithm is based on the use of a 5 X 5 matrix of letters constructed using a keyword. The 5 X 5 matrix can only allow 25 characters, hence the letters I/J count as one. If we encrypt the plain text which is having the letter I/J and when we decrypt the ciphertext at the receive end, the receiver will be under ambiguity whether to consider I or J in his text, because the meaning can be changed with the change of the letters. This algorithm can only useful for the plain text containing of alphabets but it is failed for the plain text containing of alphanumeric values. That means the plain text that is to be encrypted can only have alphabets but should not contain digits or numbers. For example:

s	i/j	m	p	l
e	a	b	c	d
f	g	h	k	n
o	q	r	t	u
v	w	x	y	z

Key: simple

The traditional Playfair cipher [4] uses 25 uppercase alphabets with I=J or Q omitted. 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. The message is then broken a groups of 2 letters. In case of duplication of letters in a group one of the letters is used as padding and is placed between the letters. In case of odd number of characters the same padding is applied at the end. The substitution happens depending on the following three rules.

- In case of letters of in the same row the letters to the right of each letter are taken. Wrapping happens in case one of the letters is at the last column.
- In case of letters in the same column the letters to the bottom of each letter are taken. Again wrapping happens in case any letter is in the last row.
- In case the letters are neither in the same row or column a rectangle is made with the letters and the letters at the opposite corners are taken.

In case of decryption the reverse process is done with the cipher text and we get back the plain text

3. VARIATIONS OF PLAYFAIR CIPHER TECHNIQUE

In the variation proposed by Ravindra Babu K, S.Uday Kumar, A. Vinay Babu, I.V.N.S Aditya , P. Komuraiah [5] the 5 x 5 matrix has been replaced by 6 x 6 matrix. In proposed technique all the uppercase alphabets as well as numbers can be handled. However lowercase letters, white space and other printable characters cannot be handled.

In the variation proposed by Shiv Shakti Srivastava, Nitin Gupta [6] the 5 x 5 matrix has been replaced by 8 x 8 matrix. After converting plain text to cipher text using the 8 x 8 matrix, the characters are converted to the corresponding ASCII values in decimal and then to corresponding binary values of 7 bits. Linear Feedback Shift Register is then applied to get the final cipher text.

In the variation proposed by Gaurav Agrawal, Saurabh Singh, Manu Agarwal [7] the frequency of each alphabet in the text to be encrypted is calculated. The 2 letters with the least frequency are combined instead of combining I and J. The 5 x5 matrix is formed by inserting the keyword without duplication of letters, the combined letters and lastly the other letters.

In the variation proposed by Sanjay Basu and Utpal Kumar Ray [8] assumed a rectangular matrix having 10 columns and 9 rows which can support almost all the printable characters including white space. The 10 x 9 matrix contains almost all the printable characters. This includes lowercase and uppercase alphabets, punctuation marks, numbers and special characters. The order of placement of different groups of characters can also be done so that the matrix formed by using the same secret keyword depends on the order of placement. This means that the ciphertext will also depend on the order of placement of different groups of characters. The matrix with the secret keyword as Duplicate and a particular placement order is given.

In the variation proposed by Nisarga Chand and Subhajit Bhattacharyya [9] developed a new concept which includes 6 by 6 play fair cipher matrix. This matrix consists of alphabets A to Z and numeric values 0 to 9. In this paper they used four iteration steps to make strong encrypted message. In this experiment they have used four different keywords and with the help of these four keywords they encrypt and decrypt the text messages successfully. This extended play fair algorithm is based on the use of four 6 X 6 matrices of letters constructed using corresponding four keywords. 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.

4. PROPOSED TECHNIQUE

This section presents the algorithm that extends the security of playfair technique using excess 3 code and ceasar cipher.

4.1 Generation of Rectangular Matrix

- First place the alphabets of key in the matrix from left to right and top to bottom with no repeating alphabet.
- Fill all the entries of the matrix with remaining alphabets and integer values (0-9) with no repeating alphanumeric value.
- Convert all entries into its equivalent integer value according to the given matrix that will start from 0 to 35 for 0 to z.

Example Shown in Fig 3:

0	0	6	6						
1	1	7	7						
2	2	8	8						
3	3	9	9						
4	4								
5	5								
a	10	g	16	m	22	s	28	y	34
b	11	h	17	n	23	t	29	z	35
c	12	i	18	o	24	u	30		
d	13	j	19	p	25	v	31		
e	14	k	20	q	26	w	32		
f	15	l	21	r	27	x	33		

Fig 3:

- Convert all the entries of the matrix into the binary number.
- Convert each entry into the excess 3 code.
- Now convert all entries into its equivalent integer value. If any entry has value more than or equal to 36 then we will take a mod like (value mod 36).
- Again convert the all entries of the matrix into its equivalent alphabets or integer value according to the given matrix.

0	0	6	6						
1	1	7	7						
2	2	8	8						
3	3	9	9						
4	4								
5	5								
a	10	g	16	m	22	s	28	y	34
b	11	h	17	n	23	t	29	z	35
c	12	i	18	o	24	u	30		
d	13	j	19	p	25	v	31		
e	14	k	20	q	26	w	32		
f	15	l	21	r	27	x	33		

Fig 2: Speed verses end-to-end delay

4.2 Encryption and Decryption Process

4.3 Encryption

- First assign a numerical equivalent to each alphanumeric value according to the matrix that is given below.

0	0	6	6						
1	1	7	7						
2	2	8	8						
3	3	9	9						
4	4								
5	5								
a	10	g	16	m	22	s	28	y	34
b	11	h	17	n	23	t	29	z	35
c	12	i	18	o	24	u	30		
d	13	j	19	p	25	v	31		
e	14	k	20	q	26	w	32		
f	15	l	21	r	27	x	33		

- Now encrypt the key using Ceaser cipher technique. General additive cipher algorithm can be expressed as follows. For each alphanumeric value of key.

K1=E (k + n) mod 36

Where n takes on a value in the range 0 to 35. But in our case the value of n =3.

For example: Key is simple

K1= E (s+ 3) mod 36

= (28+3) mod 36=31 that is equal to v. similarly we find the encrypted key.

Thus encrypted key if vlpsoh

- Now instead of original key we send the encrypted key to the receiver.

4.4 Decryption

- First receiver receives the key and decrypts the key in the same manner using given formula.

K= (k1-3) mod 36

- After finding the original key, the generation of rectangular matrix will be start and after that follow the decryption process for the plaintext

5. ENCRYPTION AND DECRYPTION PROCESS FOR THE PLAINTEXT

- First the plaintext is broken into groups of 2 letters. In case of duplication of letters in a group one of the letters is used as padding and is placed between the letters.
- In case of odd number of characters the same padding is applied at the end. The substitution happens depending on the following three rules.
- In case of letters of in the same row the letters to the right of each letter are taken. Wrapping happens in case one of the letters is at the last column.
- In case of letters in the same column the letters to the bottom of each letter are taken. Again wrapping happens in case any letter is in the last row.
- In case the letters are neither in the same row or column a rectangle is made with the letters and the letters at the opposite corners are taken.

In case of decryption the opposite is done with the cipher text and we get back the plain text.

6. IMPLEMENTATION

Suppose we have 6 * 6 rectangular matrix. In given Example key is **simple** and plain text is **hello122**

6.1 At Sender Side

Step 1: First place the alphabets of key in the matrix from left to right and top to bottom with no repeating alphabet.

s	i	m	p	l	e
a	b	c	d	f	g
h	j	k	n	o	q
r	t	u	v	w	x
y	z	0	1	2	3
4	5	6	7	8	9

Step 2: Fill all the entries of the matrix with remaining alphabets and integer values with no repeating alphanumeric value.

Step 3: Convert all entries into its equivalent integer value.

0	0	6	6						
1	1	7	7						
2	2	8	8						
3	3	9	9						
4	4								
5	5								
a	10	g	16	m	22	s	28	y	34
b	11	h	17	n	23	t	29	z	35
c	12	i	18	o	24	u	30		
d	13	j	19	p	25	v	31		
e	14	k	20	q	26	w	32		
f	15	l	21	r	27	x	33		

Step 4: Convert all the entries of the matrix into the binary number. For example

0	000000	6	000110						
1	000001	7	000111						
2	000010	8	001000						
3	000011	9	001001						
4	000100								
5	000101								
a	001010	g	010000	m	010110	s	011100	y	10001
b	001011	h	010001	n	010111	t	011101	z	10001
c	001100	i	010010	o	011000	u	011110		
d	001101	j	010011	p	011001	v	011111		
e	001110	k	010100	q	011010	w	100000		
f	001111	l	010101	r	011011	x	100001		

Step 5: Convert each entries into the excess 3 code.

0	000011	6	001001						
1	000100	7	001010						
2	000101	8	001011						
3	000110	9	001100						
4	000111								
5	001000								
a	001101	g	010011	m	011001	s	011111	y	10
b	001110	h	010100	n	011010	t	100000	z	10
c	001111	i	010101	o	011011	u	100001		
d	010000	j	010110	p	011100	v	100010		
e	010001	k	010111	q	011101	w	100011		
f	010010	l	011000	r	011110	x	100100		

Step 6: Now convert all entries into its equivalent integer value. If any entry has value more than or equal to 36 then we will take a mod like **(value mod 36).**

0	3	6	9						
1	4	7	10						
2	5	8	11						
3	6	9	12						
4	7								
5	8								
a	13	g	19	m	25	s	31	y	37
b	14	h	20	n	26	t	32	z	38
c	15	i	21	o	27	u	33		
d	16	j	22	p	28	v	34		
e	17	k	23	q	29	w	35		
f	18	l	24	r	30	x	36		

0	3	6	9						
1	4	7	10						
2	5	8	11						
3	6	9	12						
4	7								
5	8								
a	13	g	19	m	25	s	31	y	1
b	14	h	20	n	26	t	32	z	2
c	15	i	21	o	27	u	33		
d	16	j	22	p	28	v	34		
e	17	k	23	q	29	w	35		
f	18	l	24	r	30	x	0		

Step 7: Now apply **Step 3 to Step 6** on an encryption matrix. Now coming matrix is used for encryption is given below.

v	l	p	s	o	h
d	e	f	g	i	j
k	m	n	q	r	t
u	w	x	y	z	0
1	2	3	4	5	6
7	8	9	a	b	c

Step 8: Now encrypt the message hello122

- First break the message into group of two.
  he lx lo 12 2x
- he encrypt by lj, lx encrypt by pw, lo encrypt by ph, 12 encrypt by 23, x2 encrypt by 3w

Step 9: Now encrypt the key using Ceaser cipher technique. General additive cipher algorithm can be expressed as follows. For each alphanumeric value of key.

$$K1=E\ (k + n)\ \text{mod}\ 36$$

Where n takes on a value in the range 0 to 35. But in our case the value of n =3.

For example. Key is simple

$$K1= E\ (s+ 3)\ \text{mod}\ 36$$

$$= (28+3)\ \text{mod}\ 36=31$$

That is equal to v. similarly we find the encrypted key.

Thus encrypted key if vlpsoh

Step 10: Now instead of original key sender send the encrypted key to the receiver.

6.2 At Receiver Side:

Step 1: First receiver receives the key and decrypts the key in the same manner using given formula.

$$K= (k1-3) \bmod 36$$

Step 2: After finding the original key, the generation of rectangular matrix will be start.

Step 3: Now the same process will be apply by the receiver for decryption.

7. CONCLUSION

In this paper we have analyzed the security of original Playfair cipher. We proposed a technique to extend the security of playfair technique. By doing implementation we showed that proposed technique is stronger than the original Playfair cipher and provide better security to the plaintext and key as compared to original playfair technique.

8. REFERENCES

[1] Behrouz A. Forouzan, Cryptography and Network Security. Special Indian Edition 2007, Tata McGrawHill Publishing Company Limited, New Delhi.

[2] Wikipedia (http://en.wikipedia.org/wiki/Playfair_cipher)

[3] C Nisarga Chand, Subhajit Bhattacharyya "A Novel Approach for Encryption of Text Messages Using PLAY -FAIR Cipher 6 by 6 Matrix with Four Iteration Steps".

[4] William Stallings, Cryptography and Network Security Principles and Practices, 4th Edition, Pearson Education.

[5] Ravindra Babu K, S. Uday Kumar, A. Vinay Babu, I.V.N.S Aditya , P. Komuraiah [3] An Extension to Traditional Playfair Cryptographic Method´ International Journal of Computer Applications (0975 ± 8887) Volume 17± No.5, March 2011.

[6] Shiv Shakti Srivastava and Nitin Gupta "A Novel Approach to Security using Extended Playfair Cipher" International Journal of Computer Applications (0975 ±8887) Volume 20± No.6, April 2011.

[7] Gaurav Agrawal, Saurabh Singh, Manu Agarwal An Enhanced and Secure Playfair Cipher by Introducing the Frequency of Letters in any Plain text´ Journal of Current Computer Science and Technology Vol. 1 Issue 3 [2011]10-16.

[8] Sanjay Basu and Utpal Kumar Ray"Modified Playfair Cipher using Rectangular Matrix" International Journal of Computer Applications (0975 ± 8887) Volume 46± No.9, May 2012.

[9] Nisarga Chand and Subhajit Bhattacharyya "A Novel Approach for Encryption of Text Messages Using PLAY -FAIR Cipher 6 by 6 Matrix with Four Iteration Steps" International Journal of Engineering Science and Innovative Technology (2319-5967) Volume 3, Issue 1, January 2014.