Modified Playfair Cipher using Rectangular Matrix

Sanjay Basu
Department of Information Technology
Jadavpur University
Kolkata, India

Utpal Kumar Ray
Department of Information Technology
Jadavpur University
Kolkata, India

ABSTRACT
One of the well known polyalphabetic ciphers is the Playfair cipher. In this cipher digrams or groups of 2 letters in the plain text is converted to cipher text digrams during encryption using a key. Similarly during decryption cipher text digrams are converted to plain text digrams using the same key. However the original 5 x 5 Playfair cipher can support only 25 uppercase alphabets. To overcome this drawback we propose a rectangular matrix having 10 columns and 9 rows which can support almost all the printable characters including white space. This paper analyses the original Playfair cipher, the different variations that have been proposed and the modified Playfair cipher that we propose. Cryptanalysis is done to show that the proposed cipher is a strong one.

Keywords
Playfair cipher, Polyalphabetic cipher, Special symbols, cryptanalysis, rectangular matrix

1. INTRODUCTION
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 – 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.

2. EXISTING PLAYFAIR CIPHER
The traditional Playfair cipher [3] [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. For example if we choose **DUPLICATE** as the secret keyword the matrix is given in Table I.

Table I: Traditional Playfair 5 x 5 matrix

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

The message is then broken up with digrams or groups of 2 letters. In case of duplication of letters in a digram 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.

1. In case letters of a digram are 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.

2. 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.

3. 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.

If we take balloon as the plaintext and duplicate as the secret keyword the ciphertext can be derived as follows. First the plaintext is converted to uppercase and then broken up into digrams using X as the padding character. The digrams will be BA LX LO ON. For the first digram B and A are in the same row. Using rule 1 we get CT. Next we take LX – they are neither in the same row or column. Hence using rule 3 we get PY. The next digram is LO which as before are neither in the same row or column. Hence using rule 3 we get UR. The last digram is ON which are in the same row and so we get QO. Thus the cipher text is CTPYURQO.

3. VARIATIONS OF PLAYFAIR CIPHER
n 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 this system 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 x 5 matrix is formed by inserting the keyword without duplication of letters, the combined letters and lastly the other letters.

In the variation proposed by Packirisamy Murali and Gandhidoss Senthilkumar [8] random numbers are mapped to secret key of Playfair cipher method and corresponding numbers will be transmitted to the recipient instead of alphabetical letter. This method rapidly increases security of the transmission over an unsecured channel.

In the variation proposed by Harinandan Tunga, Soumen Mukherjee [9] multiple array of structure has been used to store the information about the spaces and the other to store the information about whether an 'X' has appeared in the alphabet matrix. Secondly the key table has been extended from 5 X 5 matrix to 16 X 16 matrix form. Finally, the 16 X 16 algorithm has been modified so that it can incorporate shifting of rows and columns of the 16 X 16 matrix to ensure that the encrypted text contains any ASCII ranging between 0 – 255.

In the variation proposed by V. Umakanta Sastry, N. Ravi Shankar, and S. Durga Bhavani [10] it is assumed that the characters of the plain text belong to the set of ASCII characters denoted by the codes 0 to 127. A substitution table is constructed in an appropriate manner and the rules 1 to 3 are modified suitably for encryption and decryption. Further, interweaving is introduced and iteration which will lead to a lot of confusion and diffusion.

4. LIMITATIONS OF ORIGINAL 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.

In a monoalphabetic 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 digrams. Although the frequency analysis is much more difficult than in monoalphabetic cipher still using modern computational techniques the attacker can decipher the cipher text.

To overcome the drawbacks we propose a modified cipher which uses a 10 x 9 matrix which will contain almost all the printable characters.

5. MODIFIED PLAYFAIR CIPHER

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 Table II.

Table II: Modified Playfair 10 x 9 matrix

D	u	p	l	i	c	a	t	e	b
d	f	g	h	j	k	m	n	o	q
r	s	v	w	x	y	z	A	B	C
E	F	G	H	I	J	K	L	M	N
O	P	Q	R	S	T	U	V	W	X
Y	Z	0	1	2	3	4	5	6	7
8	9		,	.	/	;	'	[	]
<	>	?	:	{	}	-	=	!	@
#	$	%	^	&	*	(	)	_	+

Lowercase as well as uppercase alphabets along with numbers and other printable characters can be handled. Single or multiple sentences can be encrypted and decrypted keeping the case, punctuation marks, special characters and white space intact (white space is part of the character set which we are using). The keyword can be a word or single or multiple sentences (maximum non-duplicate character count can be 90).

In case of duplicate letters in a digram and odd number of characters we use ^ as the padding character during encryption. During decryption all instances of ^ are deleted and we get back the original plain text. The logic of substitution is same as the traditional Playfair cipher.

6. ENCRYPTION USING MODIFIED CIPHER

Let us take the plaintext as **This is a plain text.** Breaking up the plaintext into digrams we get the following digrams and hence the ciphertext.

Th We see that they are neither in the same row or column. Hence using rule 3 we get **Rk**.

is They are neither in the same row or column and thus using rule 3 we get **ux**.

<space>i They are neither in the same row or column. Using rule 3 we get **.p**

s<space> They are neither in the same row or column and using rule 3 we get **v9**

a<space> They are neither in the same row or column. Using rule 3 we get **p;**

pl They are in the same row. Using rule 1 we get **li**

ai They are in the same row. Using rule 1 we get **tc**

n<space> They are neither in the same row or column. Using rule 3 we get **g'**

te They are in the same row. Using rule 1 we get **eb**

xt They are neither in the same row or column. Using rule 3 we get **Ai**

.^ They are neither in the same row or column. Using rule 3 we get **,&**

Thus the ciphertext will be **Rkux.pv9p;litcg'ebAi,&**

7. DECRYPTION USING MODIFIED ALGORITHM

In case of decryption rules 1 and 2 have to be reversed. Breaking up the cipher text into digrams we get the following digrams and hence the plaintext.

Rk They are neither in the same row or column. Using rule 3 we get **Th**
ux They are neither in the same row or column. Using rule 3 we get **is**
.p They are neither in the same row or column. Using rule 3 we get **<space>i**
v9 They are neither in the same row or column. Using rule 3 we get **s<space>**
p; They are neither in the same row or column. Using rule 3 we get **a<space>**
li They are in the same row. Using reverse of rule 1 we get **pl**
tc They are in the same row. Using reverse of rule 1 we get **ai**
g' They are neither in the same row or column. Using rule 3 we get **n<space>**
eb They are in the same row. Using reverse of rule 1 we get **te**
Ai They are neither in the same row or column. Using rule 3 we get **xt**
,& They are neither in the same row or column. Using rule 3 we get **.^**

Since ^ is to be deleted the plain text which we get is as follows.
This is a plain text.

8. CRYPTANALYSIS OF MODIFIED CIPHER

The various types of cryptanalytic attacks are as follows.
1. Brute force attack
2. Ciphertext only attack
3. Chosen plaintext/ciphertext attack

1. Brute force attack
The size of the key domain is 90! (factorial 90). Thus brute force attack will be very difficult for the modified Playfair cipher.

2. Ciphertext only attack
The frequencies of digrams are preserved in the cipher text (to some extent). The cryptanalyst can launch a cipher-text only attack. However the number of digrams to be searched would be 90 x 90 = 8100.

3. Chosen plaintext/ciphertext attack
Obtaining the key is relatively straightforward if both plaintext and ciphertext are known.

9. CONCLUSION

In this paper we have analyzed the merits and demerits of the original Playfair cipher. We then looked at the variations that have been proposed. Then we discussed the modified Playfair cipher which we proposed. By doing cryptanalysis we showed that this modified cipher is stronger than the original Playfair cipher.

As far as future scope of work is concerned, the 10 x 9 matrix which is being formed after taking the keyword is formed with a certain sequence of the different printable characters (small letters then capital letters then numerical and then the other printable characters). If we take small letters, capital letters, numerical and other printable characters as four different groups the sequence of the groups can change the 10 X 9 matrix with the same keyword. This should make cryptanalysis more difficult. This can be tried out and the results can be analyzed.

10. ACKNOWLEDGEMENT

The first author would like to thank Jadavpur University authorities for giving him the chance to undertake such a work. He also wishes to thank the second author for the guidance provided to him.

11. REFERENCES

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

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

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

[4] Atul Kahate, Cryptography and Network Security, 2nd Ed., Tata McGraw-Hill Publishing Company Limited, New Delhi.

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

[6] Shiv Shakti Srivastava, 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] Packirisamy Murali and Gandhidoss Senthilkumar "Modified Version of Playfair Cipher using Linear Feedback Shift Register", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008

[9] Harinandan Tunga, Soumen Mukherjee "A New Modified Playfair Algorithm Based On Frequency Analysis", International Journal of Emerging Technology and Advanced Engineering, (ISSN 2250-2459, Volume 2, Issue 1, January 2012)

[10] V. Umakanta Sastry, N. Ravi Shankar, and S. Durga Bhavani "A Modified Playfair Cipher Involving Interweaving and Iteration", International Journal of Computer Theory and Engineering, Vol. 1, No. 5, December, 2009 1793-8201