DOI: 10.24996/ijs.2021.62.9.36

Iraqi Journal of Science

ISSN: 0067-2904

Playfair with Multi Strata Encryption

Raghad K. Salih*, Madeha Sh. Yousif

Department of Applied Sciences, University of Technology, Baghdad, Iraq

Received: 12/1/2021 Accepted: 21/5/2021

Abstract

Playfair cipher is a substitution scheme. The classical playfair scheme has a limited matrix size (5×5) containing only uppercase letters, so it is prone to hackers and cryptanalysis. To increase the resistance of playfair cipher, a new encipherment and decipherment method is proposed in this work, which depends on the permutation and its inverse, respectively. In addition, a modified (10×10) key matrix is utilized, which includes capital and small Alphabets, numbers, and 38 special characters collected from ASCII codes. In the proposed method, both substitution and transposition schemes are used, where the first stratum of the cipher is a substitution by using (10×10) key matrix and the second stratum is a transposition by using permutation key which provides multi strata resistance to brute force and other cryptanalysis attacks. A comparison between the traditional playfair scheme and the proposed method demonstrates that the encoded text is hard to recognize by cryptanalysts, which improves the security of the encryption process.

Keywords: Playfair, substitution, transposition and multi strata.

تشفير البلي فير متعدد الطبقات

رغد كاظم صالح* ، مديحة شلتاغ يوسف

قسم العلوم التطبيقية، الجامعة التكنولوجية، بغداد، العراق

الخلاصة

تشفير البلي فير التقليدي هو احد أنواع أنظمة التشفير التعويضية يكون بشكل مصفوفة محددة الحجم (5 × 5) مكونة من حروف هجائية كبيرة فقط. ولذلك النص المشفر يكون ضعيف امام قراصنة الشفرة وعلم تحليل الشفرة لزيادة مقاومة تشفير البلي فير تم اقتراح طريقة جديدة للتشفير وفك الشفرة بالاعتماد على التبديل و معكوسه مع مصفوفة مفتاح مطورة ذات حجم (10 × 10) تتضمن جميع الحروف الهجائية الكبيرة والصغيرة , ارقام و 38 رمز جمعت من رموز ASCII. في الطريقة المقترحة تم استخدام التشفير التعويضي والانتقالي معا حيث ان الطبقة الاولى من التشفير تعويضية باستخدام مصفوفة المفتاح (10 × 10) اما الطبقة الثانية انتقالية باستخدام مفتاح التبديل والذي يوفر طبقات متعددة من الحماية لمقاومة هجمات البحث الشامل وعلم تحليل الشفرة. كذلك يقدم البحث مقارنة ما بين الطريقة التقليدية والطريقة المقترحة والتي تبين صعوبة معرفة محلل الشفرة للنص المشفر مما يعمل على تحسين أمان عملية التشفير.

1. Introduction

The playfair system is one type of the symmetric cryptosystems. The (5×5) playfair matrix is generated by arranging the letters of the given key in a row by row or column by column way. Taking

*Email: Raghad.k.Salih@uotechnology.edu.iq into consideration to discard the repeated characters, the remaining places in the matrix are filled by the unused letters alphabetically [1,2]. To scale down, the letter 'Q' is omitted, or 'I' and 'J' are treated as a single alphabet. Now, to encrypt the sent text, the message must be divided into digraphs (groups of 2 letters) to be mapped with the key matrix. If the last diagraph is single, a ‘Z’ is appended to complete it. To cover every pair of letters in the plaintext, the following four rules must be applied [3,4,5]:

- For the group of two similar letters, an uncommon letter is added after the first letter. However, the new pair is encrypted, and then continues.
- If the two letters appear in the same row of the key matrix, each one is substituted by the letter in its immediate right. It should be rotated to the left key matrix if necessary.
- If the two letters appear in the same column of the key matrix, each one is replaced by the letter below it. It should be cycled to the top key matrix if necessary.
- Otherwise, the rectangle is created where the two alphabets are two opposite corners. Then each alphabet replaced with the alphabet that forms the other corner of the rectangle that lies on the same row as that alphabet.

This paper is building up an encryption scheme which is able to encrypt any text message safely. A high level firewall must be provided for the protection of networks and confidential information from being hacked. For this purpose, we need to create strong and secure encryption and decryption technique. This paper is designed as follows. Section 2 is focused on some previous work. The proposed method is presented in Section 3. Section 4 discusses some experimental work and the security analysis of the suggested method in terms of some attacks. Finally, Section 5 concludes the paper.

2. Related Work

In 2015, Zakariyau [6] used a 17×17 playfair key matrix that has a maximum key length of 289 characters. This size of key yields 83521 keys, making it very hard for eavesdroppers to obtain the sent text.

In 2016, Subramaniyam [7] utilized 7× 9 DES system to improve the playfair and increase its security to withstand some well-known attacks. Rajeswari *et al*. [8] expanded playfair ciphers and studied the avalanche effect as a measure for the security of the cryptographic algorithm. Hence, it is an alternative to playfair for protecting the encrypted data. Veetil [9] extended the traditional playfair method using genetic algorithm. The two main operators of genetic algorithm ‘Crossover’ and ‘Mutation’ were used for the extension to give security and affectivity by two layers of protection.

In 2017, Singhet *et al*. [10] introduced a modified version of playfair cipher based on random number generator combined with Vigenere cipher. Siddiqui *et al*. [11] extended the classical playfair cipher using modified matrix with 9×7 dimension, which eradicates the limitation of the original playfair cipher with 5×5 matrices and is further enhanced by using crossover and mutation genetic operators. Saman *et al*. [12] modified the original 5×5 playfair cipher to a 6×10 matrix cipher to accommodate all the characters of the Hindi language, the numerical digits, and the special characters, and to overcome the limitation of the original playfair cipher.

In 2019, Yousif *et al*. [13] expanding the key's matrix of the classical playfair scheme from (5×5) to $(n\times n,\ n>10)$. Using the permutation operation to the key matrix that adds more security layers to the encryption process.

3. The Proposed method

The suggested algorithm has two keys. The first key (k_1) is a keyword which is filling the initial cells of (10×10) key matrix, with eliminating the repetitive occurrence of any alphabet. The unfilled position of the (10×10) key matrix will be filled with the rest of capital letters, small letters, numbers (0,1,…,9) and 38 characters, collected from ASCII codes, that have not been part of the secret key.

In the classical playfair cipher, the cipher text obtained via the encryption process, which is discussed in section 1, is sent as a resulting cipher text. In the proposed approach, (k_2) is used as another key which represents the permutation operation, to give another stratum of security to the cipher text, as described in the following algorithm.

The Encryption Algorithm

Input:

- k_1, k_2,p (the Plaintext).

Output:

- Ciphertext (C)

1: Create a (10 × 10) key matrix as shown above.

2: Partition the given plaintext into pairs; if the numbers of letters are odd then the character '*' is added to form the last pair.

3: For the pair of the same letter, one of them is replaced by the character (^).

4: Apply the rule of palyfair as described in (section 1) to encipher each pair in step 3 and procure the cipher text C_1 .

5: Put the ciphertext C1 into a matrix that has columns identical to the length of permutation k2.

6: Rearrange the columns of the matrix in step 5 by using the second key (k_2) to procure the cipher text C_2.

7: Write the cipher text C_2 in step 6 in a row after row way to procure the final cipher text C.

The Decryption Algorithm

In the decryption, the key (k_1) and the inverse permutation key k_2^{-1}, are used to obtain the original plaintext, as follows:

Input

- k_1
- k_2
- The ciphertext C.

Output

- The plaintext P.

1: Construct (10×10) key matrix as shown previously.

2: Find the inverse permutation key k_2^{-1}.

3: Read the cipher text C.

4: Put the cipher text C in a matrix that has columns identical to the length of k_2. The matrix is filled in row by row way.

5: Rearrange the columns of the matrix in step 4 by using k_2^{-1} in step 2 to obtain the first plaintext P_1.

6: Write the plaintext P_1 in a row by row way.

7: Divide the plaintext P_1 into pairs of characters.

8: Make the same procedure applied in the playfair encryption, but in an inverse manner, to procure the original plaintext P.

4. Experimental results

Let k_1=University of Technology, then the modified playfair key generation matrix (10 × 10) is described as in Table-1 below.

Table 1-The (10 × 10) playfair matrix

U	**n**	**i**	**v**	**e**	**r**	**S**	**t**	**y**	**o**
f	**T**	**c**	**h**	**l**	**g**	**A**	**B**	**C**	**D**
E	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**
O	**P**	**Q**	**R**	**S**	**V**	**W**	**X**	**Y**	**Z**
a	**b**	**d**	**j**	**k**	**m**	**P**	**q**	**u**	**w**
x	**z**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
8	**9**	**!**	**"**	**#**	**$**	**%**	**&**	**‘**	**(**
)	*	+	**,**	**-**	**.**	/	**:**	**;**	<
=	>	**?**	**@**	**[**	\	**]**	^	**_**	**{**
|	**}**	~	∩	≡	±	≥	≤	≈	∪

Take the plaintext (P) = My gmail is farahana@gmail.com and the permutation key $k_2 = \begin{bmatrix} 1\ 2\ 3\ 4 \\ 3\ 1\ 4\ 2 \end{bmatrix}$.
When the encryption algorithm is applied, we can get these results:
The digraphs of plaintext are: My gm ai li sf ar ah an a@ gm ai l. co m*.
Hence, the first cipher text is:

C_1= YCJ3dUceUAmUfjbUj=J3dUg-Dyb.

By putting the cipher text C_1 in (7×4) matrix and applying the key k_2 to it to procure c_2, the final cipher text is:

C= JY3CcdeUmUUAbfUjJj3=gd-UbD.y,

as shown in Tables- 2 and 3, respectively.

Table 2-The (7×4) matrix

C_1=

Y	C	J	3
d	U	c	e
U	A	m	U
f	j	b	U
j	=	J	3
d	U	g	-
D	y	b	.

Table 3-The (7×4) matrix with rearranged columns by using k2

C_2=

J	Y	3	C
c	d	e	U
m	U	U	A
b	f	U	j
J	j	3	=
g	d	-	U
b	D	.	y

The decryption process is the reverse of the encryption. By applying the decryption algorithm, the following results are obtained:
We wrote the cipher text C in a (7×4) matrix in a row-by-row way, as shown in Table- 4, then used the inverse permutation key $k_2^{-1} = [3\ 1\ 4\ 2]^{-1} = \begin{bmatrix} 1\ 2\ 3\ 4 \\ 2\ 4\ 1\ 3 \end{bmatrix}$ to construct the matrix P_1, as shown in Table-5.

Table 4- The (7×4) matrix

J	Y	3	C
c	d	e	U
m	U	U	A
b	f	U	j
J	j	3	=
g	d	-	U
b	D	.	y

Table 5-The matrix P1 by using k_2^(-1)

$P_1 =$

Y	C	J	3
d	U	c	e
U	A	m	U
f	j	b	U
j	=	J	3
d	U	g	-
D	y	b	.

Hence, by writing the matrix P_1 in a row by row way, we can get the final plaintext P as described below:

P_1 = YCJ3dUceUAmUfjbUj=J3dUg-Dyb.

So, the digraph of P_1 is YC J3 dU ce UA mU fj bU j= J3 dU g- Dy b.

By using the key matrix in Table-2, the final plaintext is:

P= My gm ai li sf ar ah an a@ gm ai l. co m*

= My gmail is farahana@gmail.com

5. Security Analysis

The suggested algorithm improves the traditional playfair layout to increase the firewall against hackers and cipher analysis attacks for the following reasons:

- The classical playfair applied a (5×5) matrix as a key, where the letters ‘I’ and ‘J’ are considered as one character. However, this will cause a confusion at the decryption process. This defect is corrected in the suggested algorithm by expanding the traditional key matrix to (10×10), making the encryption safer and without confusion.
- By the classical playfair, the substitution as a one layers of encryption is involved. Whereas, by the proposed method, two encryption strata are applied, one is the substitution based on the playfair matrix and the second is the transposition based on the permutation key. These two strata contribute to increase the security of the cryptosystem.
- The second key (k_2) rearranges the characters of the cipher text to make it complicated for the hacker to decrypt via cryptanalysis (see the example in section 4). The cipher text of the traditional playfair cipher of the repeated word ***gmail*** is similar (*J3dUc* and *J3dUg*), whereas in the suggested method, the cipher of the repeated word ***gmail*** is not obvious due to re-changing the order of characters of the cipher text by using the key k_2.
- In the classical playfair, the key matrix holds 25 characters, where I and J are treated as a single character. This causes a confusion at decipher, and the crypto analyzer has to search $(25\times 25 = 625)$ diagrams to find the plaintext, whereas the appearance probability of a character is 1/25=0.04. In the suggested algorithm, all the alphabet characters are used and the crypto analyzer has to search $(100\times 100 = 10000)$ diagrams to find the plaintext. Moreover, It uses 100 characters where the occurrence probability of a character is 1/100=0.01. This leads to harder cryptanalysis and more resistance against hackers.

6. Conclusions

In this paper, vulnerabilities were noticed in a playfair cipher and attempts were made to correct them. The suggested algorithm improves the security of classical playfair encryption. Plain text undergoes in two levels of encryption, namely the substitution by playfair cipher and the transposition by permutation key. In the decryption process, the permutation inverse is applied. The suggested technique uses a (10×10) playfair matrix rather than a (5×5) matrix, which provides additional security benefits.

References

1. Mahdi, G. S. **2011**. A modification of TEA block cipher algorithm for data security (MTEA). *Eng & Tech. Journal*, **29**(5): 822-832.
2. Rahma, M. S. and Hassan, S. A. **2010**. Kangaroo a proposed stream cipher algorithm. *Eng. & Tech. Journal*, **28**(3): 537-551.

3. Ghazi, A.A. and Ali, F.H. **2018**. Robust and Efficient Dynamic Stream Cipher Cryptosystem. *Iraqi journal of science,* **59**(2C): 1105-1114.

4. Salman, S.A. and Hussin, A. **2019**. The Minimum Cost for the Vascular Network using linear programming based its path graph. *Iraqi journal of science*, **60**(4): 859-867.

5. Habeeb, S., and Shakeer, E. **2013**. Proposal to Generate a Various Key from Image for Various Encryption Methods. *Eng & Tech. Journal,* **31**(1): 107-114.

6. Zakariyau, Y. B., Muhammad, L. J., Garba, A. and Mohammed, I.A. **2015**. 17×17 matrix playfair cipher technique for securing confidential information. *African Journal of Computing & Ict*, **8**(2): 1-4.

7. Subramaniyam, C. S. **2016**. Playfair using DES algorithm 7 by 9 matrix and color substitution. *International Journal of Computer Applications,* **150**(6): 1-5.

8. Rajeswari, S., Ramya, N, and Saranya, K. **2016**. Avalanche effect based variants of playfair cipher for data security. International Conference on Explorations and Innovations in Engineering & Technology, Issn: 2348 – 8387, pp. 1-5.

9. Veetil, A. T. **2016**. Playfair extended using genetic operators. *International Journal of Advanced Engineering Research and Applications*. **1**(11): 1-5.

10. Singh, S. and Dixit, A. **2017**. An approach for enhancing the security of playfair cipher. *Imperial Journal Of Interdisciplinary Research*, **3**(6): 1-5.

11. Siddiqui, M. S. N., Biswas, S. S. and Agarwal, P. **2017**. Genetic extension of playfair cipher using modified matrix. *International Journal of Computer & Mathematical Sciences,* **6**(6): 1-6.

12. Saman, Md., Nafis ,T., Siddiqui, M.S.N. and Biswas , S. S. **2017**. Addendum of playfair cipher in Hindi. *Advances in Computational Sciences and Technology*, **10**(5): 1-8.

13. Yousif, M. S., Salih, R. K., & Alsaidi, N. M. G. **2019**. A new modified playfair cipher. In AIP Conference Proceedings, Vol. 2086, No. 1, p. 030047. AIP Publishing LLC.