Journal of AL-Qadisiyah for computer science and mathematics
Vol.6 No.2 Year 2014

Page 169-175

Enhancing the Security of Playfair Cipher by Stream Cipher

Fairouz Mushtaq Sher Ali
Department of Computer Science/ College of Education for Girls/ University of Kufa/ Najaf/ Iraq
Fairoozm.jaafar@uokufa.edu.iq

Recived :13\7\2014 Revised : 4\9\2014 Accepted :28\9\2014

ABSTRACT:

Cryptography is a science of converting clear message into secret message "nonreadable message",where message was encrypted at sender side then decrypted at receiver side. Playfair is an example of substitution cipher,it has various limitations, inthis paper we proposean advanced encryption algorithm which improves the security of Playfair method by combining it with modern cipher method like Stream cipher, Stream cipher relatively regards as unbreakable method, and bit oriented method (instead of character-oriented) where the Plaintext, Ciphertext and the Key are strings of bits.

When applying the proposed algorithm, we see that the mentioned above combination cipher has a high degree of security, where cipher based on just Playfair method is not secure. Also the proposed algorithm makesthe cryptanalysis more difficult.

Keywords
Information Security, Plaintext, Ciphertext, Key, Cipher, Substitution,Playfair,Stream cipher.

1. INTRODUCTION

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography[1].

Cryptography is a Greek word which means secret writing. Today this term refers to the science and art of transforming message to make them secure and immune to attacks[2]. For the purpose of security and privacy, we need to encrypt the message at the sender side and decrypt it at the receiver side. In cryptography the term Plaintext is used for the original message that is to be transformed. The message which has been transformed is called Cipher text. An encryption algorithm is a function that works with a key to transform the Plaintext into cipher text. Decryption algorithm works in the reverse order and convert the Ciphertext into Plaintext[1].

Symmetric and Asymmetric are the two types of encryption. In symmetric encryption techniques we use the same key for both encryption and decryption purpose[3].

Asymmetric-key encryption using public and private keys. The public key is announced to all members while the private key is kept secure by the user. The sender uses the public key of the receiver to encrypt the message. The receiver uses his own private key to decrypt the message[3].

In symmetric method, there are two techniques (substitution and transposition) are used as a classical methods. Substitution technique maps the Plaintext elements into cipher text elements. Substitution has further two types,Monoalphabetic and polyalphabetic cipher. In monoalphabetic the character in the Plaintext is changed to the same character in the Ciphertext. In polyalphabetic cipher a single character in the Plaintext is changed to many characters in the Ciphertext[2].

Permutation technique is one in which the Plaintext remains the same, but the order of characters is shuffled around to get the Ciphertext[4].

Also the symmetric ciphers can be divided into Stream ciphers and block ciphers, as a modern ciphers[2].

3. RELATED WORKS

There are different researches in computer and data security:

S.G.Srikantaswamy and H. D. Phaneendra (2011) attempts in their paper to identify that using different key values for encrypting consecutive characters of Plaintext hides the relationship between the Ciphertext and Plaintext, and makes the cryptanalysis still more complex[5].

Sonia Dhull and VinodSaroha(2013) applieda double columnar transposition method on One Time Pad in order to overcome limitations of One time Pad cipher and provide much more secure and strong cipher[6].

FauzanSaeed and Mustafa Rashid(2010) propose a new technique that emphasizes on improvingclassical encryption techniques by integrating modern cipher like DES and SDES with classical methodslikePlayfair and Vigenere cipher[7].

Next sections will explainPlayfair methodand Stream cipher, after that we will discuss our proposedcombination method.

3. PLAYFAIR CIPHER

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. The technique encrypts pairs of letters (digraphs), instead of single letters as in the simple substitution cipher. The Playfair is thus significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. Frequency analysis can still be undertaken, but on the 600 possible digraphs rather than the 26 possible monographs. The frequency analysis of digraphs is possible, but considerably more difficult –and it generally requires a much larger Ciphertext in order to be useful[8].

Playfair uses a 5x5 matrix, in which the key word is written first and the remaining cells of the matrix are filled with other letter of alphabets, while I and J are placed in the same cell. The message is divided into digraphs, in which repeating letters in the same pair are separated by filler letter X. in case of odd number of letters in the message a spare letter X is added with word to complete the pair[1]. Then the Plaintext is encoded according the following four rules[9]:

a) If the pair of Plaintext falls in the same row of the matrix are replaced by the character to the right, with the first element of the row circularly following left.

b) If the pair of Plaintext fall in the same column of the matrix are replaced by the characterbeneath, with the top element of the column circularly following in the last.

c) If the pair of Plaintext are same, the first character replaced by the character to the right. The second character replaced by the character to the left.

d) If the pair of Plaintext appears on the different row and column, each Plaintext character is replaced by the character that lies in its own row and column occupied by the other Plaintext character.

4. MODERN ENCRYPTION[2]:

The symmetric ciphers can be divided into Stream ciphers and Block ciphers.

1) Stream ciphers encrypt bits individually. This is achieved by adding a bit from a key stream to a Plaintext bit. There are synchronous Stream ciphers where the key stream depends only on the key, and asynchronous ones where the key stream also depends on the Ciphertext.

2) Block cipher is much more than just an encryption algorithm. It can be used as a versatile building block with which a diverse set of cryptographic mechanisms can be realized. For instance, we can use them for building different types of blockbased encryption schemes, and we can even use block ciphers for realizing Stream ciphers. The different ways of encryption are called *modes of operation*. Block ciphers can also be used for constructing hash functions, message authentication codes which are also known as MACs, or key establishment protocols. There are also other uses for block ciphers, e.g., as pseudo-random generators in addition to modes of operation.

5. PROPOSED TECHNIQUE:

Modern ciphers normally use a combination of (substitution with transposition) and some other complex transformations to create a Ciphertext from a Plaintext.

In our paperwe put emphasis onproposing a new combination method (Playfair with Stream cipher), becausecipher based on just Playfair method is not secure.

5.1 Structure of Encryption Algorithm

Below the briefly steps of this algorithm:

Step1: Start

Step2: Read the Keyword for playfair encryption

Step3: Entering the key word in 5X5 matrix(key may include capital and small letters) as follows:

i. eliminate the duplicate letters of key

ii. arrange the key word in 5X5 matrix row wise from left to write then top to bottom.

iii. fill the remaining cells in the matrix with rest of alphabets(A-Z)

Step4: Read the Plaintext

i. break the Plaintext into pairs of characters.

ii. if both letters are in the same pair then they are separated by filler letter X

iii. rearrange the Plaintext into pairs.

iv. if one letter is left in the end of message then add filler letter X after it

Step5: Apply the *first encryption*using playfair method to encipher each pair of letters:

i. if the pair of Plaintext appear on the same row of the matrix are replaced by the letters to the right(wrap around to the left side of the row if a letter in the original pair appears on right side of the row)

ii.if the pair of Plaintext appear on the same column of the matrix are replaced by the letters to the beneath(wrap around to the top side of the column if a letter in the original pair appears on bottom side of the column)

iii. if the pair of Plaintext did not fall on the same row or column, each letter is replacedby the letter on its own row and columnthat in use by the other Plaintext character.

Step6: Apply the*Second encryption*(Reencrypt the resulted Ciphertext using Stream cipher)

i.convert the character to Ascii value then to equivalent binary form

ii. encipherthe resulted Ciphertext (from step5)using $C=P\oplus Key$,the key also in binary form and can be generated by any binary keystream generator.

iii. convert the resulted binary number to equivalentAscii value

iv. convert these numbers to characters to obtain the final Ciphertext

Step7: End

5.2 Example

To clarify the proposed encryption algorithm, we will consider the following:

- Plaintext: *the professor is evil*

- Keyword(K): *science*

- Binary key (K_{Bin}): 0110010001111000011101110001

The Encryption results produced by the above Algorithm are explained in the following points**:**

1- *Initialize the key matrix as in the following table*

Table 1:Key matrix using the word***"science"***

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

2- *Initialize the Plaintext*

- Break the text into pairs ***theprofess or is evil***
- Separate between the pair ***ss*** by ***x*** ***theprofesxsor is evil***
- Re arrange the sentence as pairs of letters ***theprofesx so ri se vi l***
- The letter ***l*** is left in the end of message, add ***x*** to the end ***theprofesx so ri se vi lx***

3- *Apply palyfairEncryption*

- To encrypt the first pair ***th***, we see that the letter *t* and *h* are in different row and column, therefore they will be ciphered to ***mp***
- To encrypt the second pair ***ep***, we see the letter ***e*** and ***p*** are also in different row and column, therefore they will be ciphered to ***ts***
- To encrypt the fourth pair ***fe***, we see the letter ***f*** and ***e*** are in different row but in the bbbsame column, therefore they will be ciphered to ***mf***
- To encrypt the eighth pair ***se***, we see the letter ***s*** and ***e*** are in different column but in the same row, therefore they will be ciphered to ***cn***

And so on to other Plaintext***, Primary CipherText: mptslu mf vi hnxdcnsxri***

4-*Apply stream cipher encryption*to encipher the above resulted primary Ciphertext as in the following table:

Table 2: Enciphering using stream cipher

P_{char} →	M	P	T	S	L	U	M	F	V	I	H	N
$P_{ASCIIvalue}$	77	80	84	83	76	85	77	70	86	73	72	78
P_{binary} → Key_{bin} → ⊕	1001101 0110010	1010000 0011110	1010100 0001110	1010011 1110001	1001100 0110010	1010101 0011110	1001101 0001110	1000110 1110001	1010110 0110010	1001001 0011110	1001000 0001110	1001110 1110001
C_{binary} →	1111111	1001110	1011010	0100010	1111110	1001010	1000011	0110111	1100100	1010111	1000110	0111111
$C_{ASCIIvalue}$	127	78	90	34	126	74	67	55	100	87	70	63
C_{char} →	del	N	Z	"	~	J	C	7	d	W	F	?

P_{char} →	X	D	C	N	S	X	R	I
	88	68	67	78	83	88	82	73
P_{binary} → Key → ⊕	1011000 0110010	1000100 0011110	1000011 0001110	1001110 1110001	1010011 0110010	1011000 0011110	1010010 0001110	1001001 1110001
C_{binary} →	1101010	1011010	1001101	0111111	1100001	1000110	1011100	0111000
$C_{ASCIIvalue}$	106	90	77	63	97	70	92	56
C_{char} →	J	Z	M	?	A	F	\	8

Final Ciphertext**:** delN Z " ~ J C 7 d W F ? j Z M ? a F \ 8

6. COMPARISON WITH THE CONVENTIONAL COMBINATION METHODS

Most traditional combination ciphers combine substitution cipherswith transposition cipher. In this section we will give a brief comparison between traditional combination ciphers and our proposed technique.

The existing combination cipher is based on with use of classical ciphers only, i.e., combining Caesar cipher with rail fence cipher[4,10]. This type of cipher makes the detection and decryption processes are very easy cipher. Also, it is a very weak cipher to Cryptanalyze using frequency attack. Furthermore, in the classical cipher there is no using to random binary key. While in our proposed work we combined classical ciphers, i.e., Playfair method, with moderns ones, i.e., Stream cipher, makes the encryption and decryption processes very difficult in absence of a secret binary random key which improve the security of data.

7. CONCLUSION

Playfaircipher regard as simplest and weakestmethod that mean it is very easy to detect by intruder or attacker. To overcome the limitations of this method, we propose a new algorithm which includes combining Playfair substitution cipher with Stream cipher. We notice that when we encipher capital and small letters, the final Ciphertextmay be contains different characters not only letters, that meanproposed algorithm hides the relationship between the Ciphertext and Plaintext, and makes the cryptanalysis more difficult. On other hand the proposed combinationmethod enhance the security of Playfairmethod and make the detection process not easy, because the combined method(Stream cipher)relatively regards asunbreakable cipher.

8. FUTURE STEPS

The binary key value consider as an essential part in encryption process. In our work we use the same seven bits of key with each letter of Plaintext but the best thing is using different binary key values forEncrypting and Decryption process which help in hiding the correlation between the Ciphertext and plaintext, this make Ciphertext breaking processmore complex and the above algorithm more efficient.

9. REFERENCES

[1] W.Stalling. Network Security Essentials (Applications and Standards), *Pearson Education*, 2004.

[2] A.J.Menezes, P. C.Oorschot and S. A. Vanstone. HAND BOOK of APPLIED CRYPTOGRAPHY, *CRC Press*, 1996.

[3] C.Paar and J.Pelzl. Understanding Cryptography, *Springer-Verlag Berlin Heidelberg*.

[4] A. Singh,A. Nandal andS. Malik. Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security.*International Journal of Advanced Research in Computer Science and Software Engineering*,(2)12: 78-82,2012.

[5] H. D.Phaneendra andS.G.Srikantaswamy.A Cipher Design using the Combined Effect of Arithmetic and Logic Operations with Substitutions and Transposition Techniques.*International Journal of Computer Applications*, (29)8: 34-36,2011.

[6] V. Saroha andS. Dhull. Enhancing Security of One Time Pad Cipher by Double Columnar Transposition Method.*International Journal of Advanced Research in Computer Science and Software Engineering*, (3)3: 692-694, 2013.

[7] F. Saeed and M. Rashid. Integrating Classical Encryption with Modern Technique.*IJCSNS International Journal of Computer 280 Science and Network Security*, (10)5: 280-285,2010.

[8] A. Alam,S. Ullah, I. Wahid and S. Khalid.Universal Playfair Cipher Using MXN Matrix.*International Journal of Advance Computers Science*, (1)3: 113-117, 2011.

[9] S. S. Dhenakaran andM. Ilayaraja. Extension of Playfair Cipher using 16X16 Matrix.*International Journal of Computer Application*, (48)7: 37-41, 2012.

[10] A. Mishra.Enhancing security of Caesar cipher using different methods. *International Journal of Research in Engineering and Technology*, (2)9, 2013.

تحسين سرية طريقة بليفير بواسطة طريقة التشفير الانسيابي

فيروز مشتاق شير علي

جامعة الكوفة/كلية التربية للبنات/ قسم علوم الحاسبات

الخلاصة:

علم التشفير هو العلم الذي يعمل على تحويل الرسالة من نص واضح الى نص سري "غير قابل للقراءة" ، حيث ان الرسالة تشفر من قبل المرسل ثم تفك شفرتها من قبل المستقبل. تعد طريقة بليفر أحد طرق التشفير التعويضية والتي تحتوي على قيود ومحددات متنوعة. في هذا البحث اقترحنا خوارزمية تشفير متطورة والتي سوف تحسن من سرية طريقة بليفير وذلك كان بدمجها مع طريقة تشفير حديثة مثل طريقة التشفير الانسيابي، والتشفير الانسيابي نسبيا يعد من طرق التشفير غير القابلة للكسر، علاوة على ذلك فإن هذا النوع من طرق التشفير يستخدم النظام الثنائي بدل استخدام الرموز والحروف، حيث ان النص الصريح والنص المشفر والمفتاح هي عبارة عن خيط من الارقام الثنائية الصفر والواحد.

عند تطبيق الخوارزمية المقترحة فقد لاحظنا ان طريقة تشفير الدمج اعلاه تمتلك درجة عالية من السرية، حيث ان التشفير الذي يعتمد على طريقة بليفير وحدها يفتقر الى السرية. كذلك فإن الخوارزمية المقترحةجعلت عملية التحليل الاحصائي لكسر الشفرة أكثر تعقيدا