Journal of AL-Qadisiyah for computer science and mathematics Vol.9 No.2 Year 2017
ISSN (Print): 2074 – 0204 ISSN (Online): 2521 – 3504

Adaptive playfair cipher Crypto algorithm

Salam Abdulkhaleq Noaman

Department of computer science / faculty of education for pure science /
Diyala University / Iraq
salam_000@yahoo.com

Recived : 8\10\2017 **Revised : 23\10\2017** **Accepted : 30 \10\2017**

Abstract

A well known cryptographic techniques is Playfair Cryptography, it is considered one of the classical method. After the invention of different techniques, it is easy to break Playfair. This paper proposed some way for removal of the traditional Playfair drawbacks. The Adaptive playfair algorithm proposed in this paper, add more security and complexity to the classical playfair algorithm. In addition to the use of two keys in form of matrices to encrypt the message, the proposed method works depending on using the odd even positions for the every pairs of the letters. The odd pairs encrypt through the first matrix key and the even pairs encrypt by using the second matrix, then applying XOR function with the third key to the result. The resulting cipher text will be in binary form, the plain text obtained by run proposed step backwards.

Keyword: Double keys, playfair, m-138 cipher text only attack, frequency attack

1. Introduction

In many applications in the life, there is a need to transfer information from the sender to the receiver. When information is transmitted, care should be taken so that the information is not accessible to a third party. Cryptography is the science that refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. My consider the cryptography as the establishment of a large toolkit containing different techniques in security applications. [1]

There are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system: Symmetric Key Encryption and Asymmetric Key Encryption, the main difference between them is the relationship between the encryption and the decryption key. Practically it is impossible to decrypt the cipher text with the key that is unrelated to the encryption key. [2, 3]

Third party will try to obtain the plain text using several cryptanalysis systems. Cryptanalysis is the sister branch of cryptography and they both co-exist. It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic techniques to test their security strengths.[4,5,6]

2. Review Of Literature

In 2008, Packirisamy Murali and Gandhidoss Senthilkumar present a new approach for secure transmission of message by modified version of Playfair cipher combining with Random number generator methods. One of the simplest methods of random number generator methods called Linear Feedback Shift Register (LFSR) has been used. This approach mapped random numbers to secret key of Playfair cipher method and corresponding numbers will be transmitted to the recipient instead of alphabetical letter.[7]

In 2012, Harinandan Tunga , Soumen Mukherjee present used multiple array of structure to store the information about the spaces and the other to store the information about whether an ‘X’ has appeared in the alphabet matrix. Also a Password mechanism has supplied to increase the level of security. The key table extended from 5 X 5 matrix to 16 X 16 matrix form, and modified the previous 16 X 16 algorithm so that we 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.[8]

Also in 2012, Sanjay Basu and Utpal Kumar Ray present a modified playfair cipher using rectangular matrix In this method a 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. The original 5 x 5 Playfair cipher can support only 25 uppercase alphabets. To overcome this drawback, authors propose a rectangular matrix having 10 columns and 9 rows which can support almost all the printable characters including white space. [9]

In 2013, A. Aftab Alam, B. Shah Khalid, and C. Muhammad Salam present a paper deals with the modification of playfair cipher. The original 5×5 matrix playfair cipher is modified to 7×4 matrix playfair , added two symbols “*” and “#”in the matrix. The addition of these two symbols creates one-to-one correspondence between the plaintext and the ciphertext, which makes the encryption and decryption easy and unambiguous.[10]

In 2014, Harinandan Tunga and Arnab Saha Suggested a method to encrypt and decrypt a text using a secret password provided by the user. The encryption machine takes the password and source message as input and generates acipher text based on Modified Playfair Algorithm using dynamic rectangular matrix. The decryption machine takes the same password and the cipher text generated by the encryption engine as input to produce the original message.[11]

3. Existing Playfair Algorithm:

[12,13,14]

In this algorithm, an alphabets table of 5×5 grid is created as a key for encrypting the plaintext. Each of the 25 alphabets must be unique, since we have 26 letters in English alphabet, one letter (usually J) is omitted from the table. If the plaintext contains J, then it is replaced by I.

The sender and the receiver decide on a particular key. In a key table, the first characters (going left to right) in the table is the phrase, excluding the duplicate letters. The rest of the table will be filled with the remaining letters of the alphabet, in natural order.

To encrypt a message using Playfair Algorithm, first, a plaintext is split into pairs of two letters. If the message contains an odd number of letters, then a letter Z is added to the last letter, for example, the message “computing” will be written as - co mp ut in gz .

Depending on the location of each two letters in the matrix key, encryption will do according to the rules below:

- If both the letters are in the same column, take the letter below each one (going back to the top if at the bottom)
- If both letters are in the same row, take the letter to the right of each one (going back to the left if at the farthest right)
- If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

4. Adaptive Playfair algorithm

In addition to the general rules of original Playfair algorithm, the modified encryption phase is depending on applying the odd pairs of the message to the first key matrix and applying the even pairs of the message to the second key matrix. Then XOR function used to gather the result with another key (k3). Since XOR function deals with binary, the cipher text will be in binary form. Fig (1) show encryption phase diagram for the proposed method. In the decryption phase will implement the previous steps in reverse order.

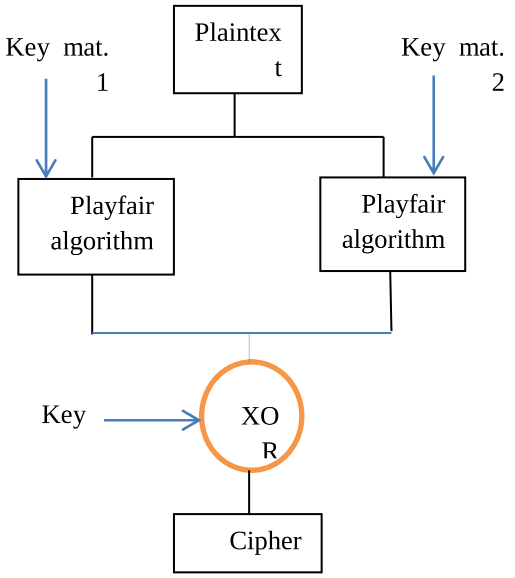


Fig (1): Encryption phase diagram

5. Methodology

5.1. Encryption phase

1- Using two different word as a keys (k1 & k2)
2- Using an integer number as a key (k3)
3- Using two matrices for encryption
4- Full the first matrix with the first key k1
5- Full the rest of alphabet in the matrix
6- Full the second matrix with the second key k2
7- Full the rest of alphabet in the matrix
8- Encrypt the message by using even odd position as follows : the odd pair of the letters encrypt with the first matrix , and the even pair of the letters encrypt with the second matrix by using the playfair algorithm
9- Perform the XOR function with key3 on the output in step 8 (in binary form)

5.2. Decryption phase

1- Perform the XOR function with key3 with the cipher text.
2- Using the k1& k2 to compose the two matrices
3- Using the first matrix to decrypt the odd pair of the letters
4- Using the second matrix to decrypt the even pair of the letters
5- After gathering the letters , the plaintext will obtain

6. Example

6.1. Encryption phase:

1- Plaintext = diyala university
2- K1= computer
3- K2=security
4- K3= 47

5- The first matrix is :

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

6- The second matrix is :

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

7- Encrypt the plain text as follows :
DI=FD
YA=AB
LA=QE
UN=CO
IV=DZ
ER=CS
SI=ZS
TY=YA

8- Gathering the result:
FDABQECODZCSZSYA

9- Perform the XOR function with key3:
- Convert the result in step 8 to the binary throw the Ascii code.
- Perfrming XOR function.

playfair text	Ascii code	Binay code	XOR	Cipher text
F	70	1000110		1101001
D	68	1000100		1101011
A	65	1000001		1101110
B	66	1000010		1101101
Q	81	1010001		1111110
E	69	1000101	Key 3	1101010
C	67	1000011		1101100
O	81	1010001	0101111	1111110
D	68	1000100		1101011
Z	90	1011010		1110101
C	67	1000011		1101100
S	83	1010011		1111100
Z	90	1011010		1110101
S	83	1010011		1111100
Y	89	1011001		1110110
A	65	1000001		1101110

6.2. Decryption phase

1- Perform the XOR function with key3 on the cipher text:

Cipher text	XOR	Binay code	Ascii code	playfair text
1101001		1000110	70	F
1101011		1000100	68	D
1101110		1000001	65	A
1101101		1000010	66	B
1111110		1010001	81	Q
1101010	Key 3	1000101	69	E
1101100		1000011	67	C
1111110	0101111	1010001	81	O
1101011		1000100	68	D
1110101		1011010	90	Z
1101100		1000011	67	C
1111100		1010011	83	S
1110101		1011010	90	Z
1111100		1010011	83	S
1110110		1011001	89	Y
1101110		1000001	65	A

2- Compose the two matrices by using the two keys as follows

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

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

3- Using playfair text obtain from step 1, Decrypt the ciphertext depending on the even odd positions of each double letters at once ,as follows
FD=DI
AB=YA
QE=LA
CO=UN
DZ=IV
CS=ER
ZS=SI
YA=TY

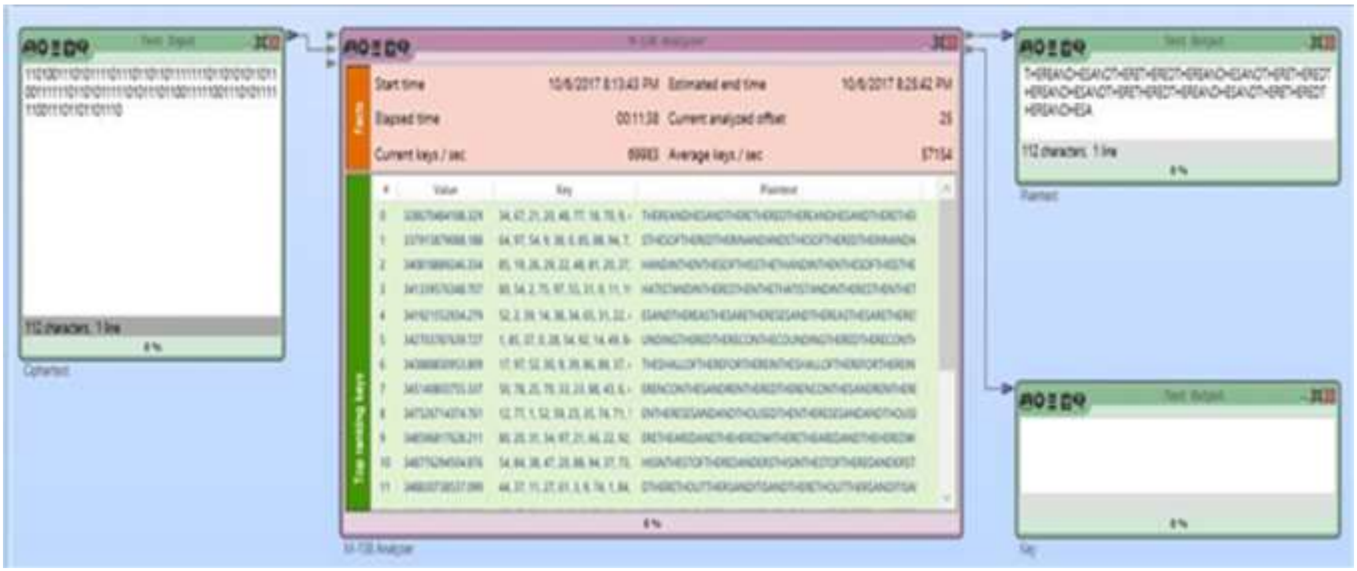
4- Plaintext= diyala university

7. Evaluation and discussion

Different types of cryptanalytic are used to evaluate the proposed method. Since the outputs of the proposed method binary format, appropriate cryptanalytic methods have been adopted like:

- m-138 cipher text only attack. [15]
- Autocorrelation. [16]
- Automatic XOR analysis. [17]

The result show the fail of applying m-138 cipher text only attack cryptanalysis to break the cipher text of the proposed method, since m-138 cipher text only attack could not guess the correct plain text. Fig (2) show the difficulty of the proposed method against the m-138 cipher text only attack. The left window represents the encrypted text and the right window is for the expected text.



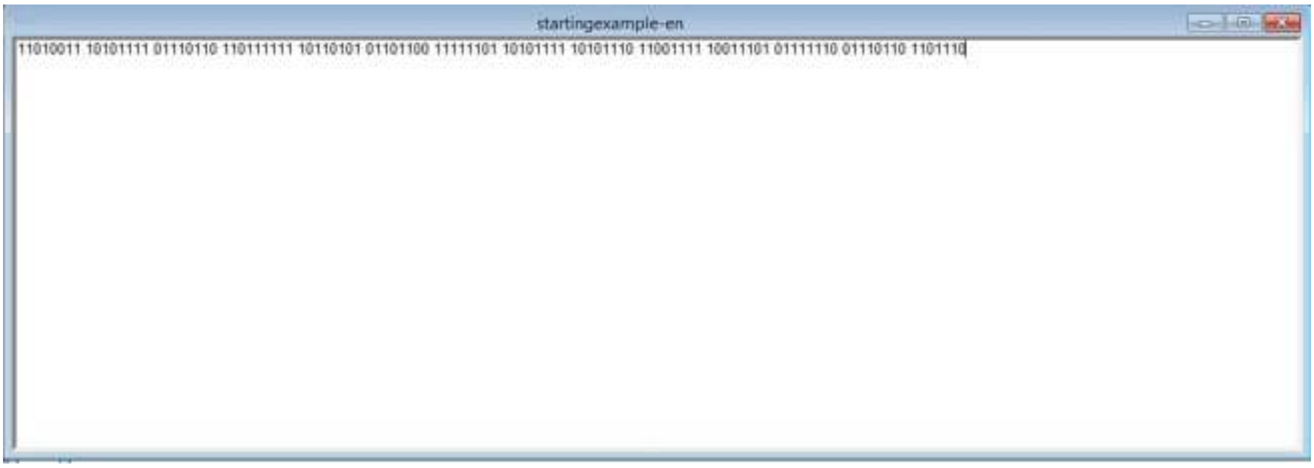
Start time 10/6/2017 8:13:43 PM Estimated end time 10/6/2017 8:25:42 PM
Elapsed time 00:11:38 Current analyzed offset 25
Current keys / sec 69983 Average keys / sec 57154

#	Value	Key	Plaintext
0	[illegible]	[illegible]	[illegible]
1	[illegible]	[illegible]	[illegible]
2	[illegible]	[illegible]	[illegible]
3	[illegible]	[illegible]	[illegible]
4	[illegible]	[illegible]	[illegible]
5	[illegible]	[illegible]	[illegible]
6	[illegible]	[illegible]	[illegible]
7	[illegible]	[illegible]	[illegible]
8	[illegible]	[illegible]	[illegible]
9	[illegible]	[illegible]	[illegible]
10	[illegible]	[illegible]	[illegible]
11	[illegible]	[illegible]	[illegible]

112 characters, 1 line

Fig.(2): Applied m-138 cipher text only attack to the proposed algorithm.

Fig (4) and fig (5) show the results of applying Autocorrelation attack and Automatic XOR analysis respectively in order to break the cipher text of the proposed method; obviously, it’s difficult to guess the plain text. A window containing encrypted text shown in fig.(3).



```
11010011 10101111 01110110 110111111 10110101 01101100 11111101 10101111 10101110 11001111 10011101 01111110 01110110 1101110
```

Fig.(3): A window containing encrypted text.

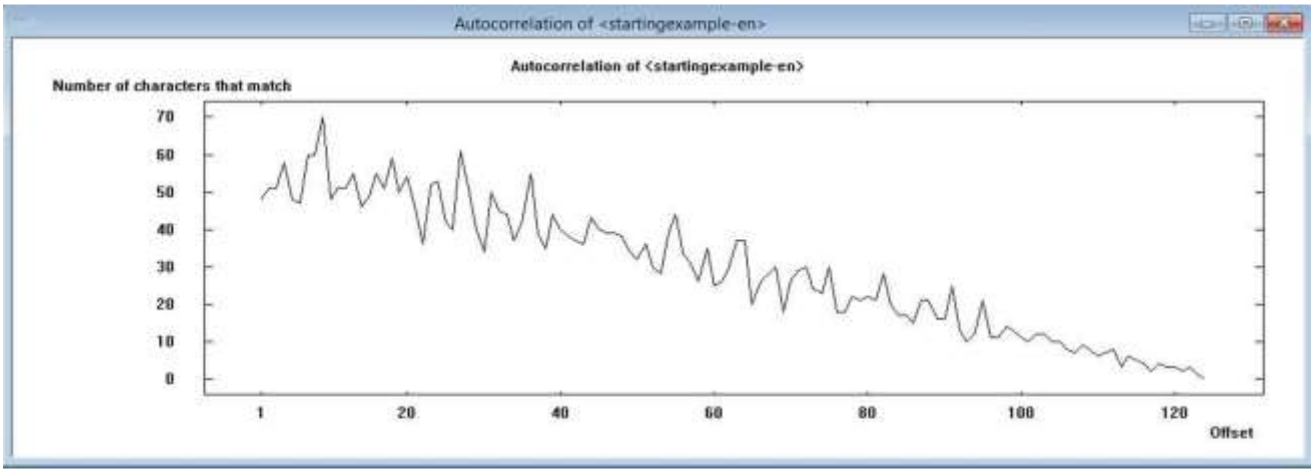
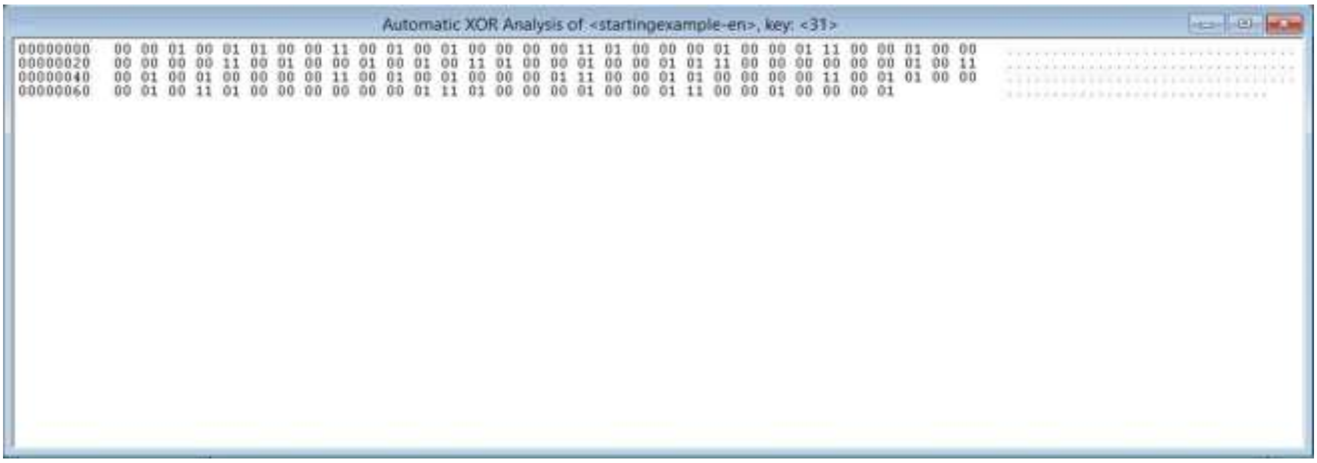


Fig.(4): Applied Correlation attack to the proposed algorithm. Very poor correlations between the characters make difficulty to guess the plain text.



```
00000000   00 00 01 00 01 01 00 00 11 00 01 00 01 00 00 00 00 11 01 00 00 00 01 00 00 01 11 00 00 01 00 00   ................................
00000020   00 00 00 00 11 00 01 00 00 01 00 01 00 11 01 00 00 01 00 00 01 01 11 00 00 00 00 00 00 01 00 11   ................................
00000040   00 01 00 01 00 00 00 00 11 00 01 00 01 00 00 00 01 11 00 00 01 01 00 00 00 00 11 00 01 01 00 00   ................................
00000060   00 01 00 11 01 00 00 00 00 00 00 01 11 01 00 00 00 01 00 00 01 11 00 00 01 00 00 00 01            .............................
```

Fig.(5): Applied Automatic XOR analysis to the proposed algorithm.

8. Conclusion

In this proposed algorithm attempted to implement adaptive Playfair cipher. Since the classical Playfair cipher method is not secure because it based on polyalphabetic cipher, It is relatively easy to break because it still leaves much of the structure and a few hundreds of letters of ciphertext are sufficient. The proposed algorithm rapidly increases security of the transmission over an unsecured channel. The additional new process in the proposed algorithm (using three keys, double alphabet for each key matrix, applying XOR function) added more complexity and more security to the original method, which make the method very difficult to break the cipher text by the attacker. The attacker couldn't guess the three keys correctly. The proposed method is more secure and difficulty than the classical Playfair algorithm.

9. References

[1] John Justin, M. and S. Manimurugan, A survey on various encryption techniques. International Journal of Soft Computing and Engineering (IJSCE) ISSN, 2012. 2231: p. 2307.

[2] Aruljothi, S. and M. Venkatesulu. Symmetric Key Cryptosystem Based on Randomized Block Cipher. in Future Information Technology (FutureTech), 2010 5th International Conference on. 2010. IEEE.

[3] Luciano, D. and G. Prichett, Cryptology: From Caesar ciphers to public-key cryptosystems. The College Mathematics Journal, 1987. 18(1): p. 2-17.

[4] Carter, B. and T. Magoc, Classical Ciphers and Cryptanalysis. space, 2007.

[5] Dhavare, A., R.M. Low, and M. Stamp, Efficient cryptanalysis of homophonic substitution ciphers. Cryptologia, 2013. 37(3): p. 250-281.

[6] Benjamin Rhew, Cryptanalyzing the Playfair Cipher Using Evolutionary Algorithms, December 9, 2003.

[7] 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.

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

[9] 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.

[10] A. Aftab Alam, B. Shah Khalid, and C. Muhammad Salam, A Modified Version of Playfair Cipher Using 7×4 Matrix. International Journal of Computer Theory and Engineering, Vol. 5, No. 4, August 2013.

[11] Harinandan Tunga and Arnab Saha, Novel Modified Playfair Cipher using a SquareMatrix. International Journal of Computer Applications (0975 – 8887) Volume 101– No.12, September 2014.

[12] Avinash Kak, Some Basic Vocabulary of Computer and Network Security and a Brief Review of Classical Encryption Techniques. Purdue University, 2017

[13] Nilesh Jadav,PlayFair Cipher in C# , Nov 16 2016, http://www.c-sharpcorner.com/article/playfair-cipher-in-c-sharp/

[14] Fauzan Saeed , Mustafa Rashid, Integrating Classical Encryption with Modern Technique. IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.5, May 2010

[15] Tsonka Baicheva, Miroslav Dimitrov, Cryptanalysis on Short Messages Encrypted with M-138 Cipher Machine. Second International Conference "Mathematics Days in Sofia" July 10–14, 2017, Sofia, Bulgaria

[16] C.S. Bruwer , Correlation attacks on stream ciphers using convolutional codes. University of Pretoria etd – Bruwer, C S (2005)

[17] Gavin Keighren and Graham Steel, Automatic Analysis of the Security of XOR-based Key Management Schemes. School of Informatics, University of Edinburgh, Scotland, 2017

خوارزمية تشفير بلايفير مطورة

سلام عبدالخالق نعمان

قسم علوم الحاسوب/كلية التربية للعلوم الصرفة/جامعة ديالى

salam_000@yahoo.com

المستخلص :

واحدة من تقنيات التشفير المعروفة هي بلايفير ، وتعتبر احدى الطرق الكلاسيكية. بعد اختراع تقنيات مختلفة، فمن السهل كسر شفرة بلايفير. في هذا البحث تم اقتراح طريقة لإزالة نقاط الضعف التقليدية لبلايفير. خوارزمية بلايفير المطورة المقترحة في هذا البحث اضافت المزيد من الأمن والتعقيد إلى خوارزمية بلايفير الكلاسيكية. فبالإضافة إلى استخدام مفتاحين في شكل المصفوفات لتشفير الرسالة، الأسلوب المقترح يعمل اعتمادا على استخدام مواقع حروف الرسالة (فردي ، وزجي) لكل زوج من الحروف. الأزواج الفردية تشفر من خلال مفتاح المصفوفة الأولى والأزواج ذات الترتيب الزوجي تشفير باستخدام المصفوفة الثانية، ثم تطبيق وظيفة (XOR) مع المفتاح الثالث على شفرة بلايفير. وسوف يكون النص المشفر الناتج بصيغة شفرة ثنائية (0,1)، ويتم استرجاع النص الصريح عن طريق تنفيذ الخطوات المقترحة بعكس الترتيب.

الكلمات: المفاتيحية: مفاتيح مزدوجة، بلايفير، هجوم م-138 ، هجوم التردد