ISSN No. 0976-5697

Volume 5, No. 4, April 2014 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Improvement of Security in Playfair Cipher

Chinmoy Ghosh
Dept. of Computer Science & Engineering
Jalpaiguri Government Engineering College
Jalpaiguri, West Bengal, India
chinmoyslg@gmail.com

Satyendra Nath Mandal
Dept. of Information Technology
Kalyani Government Engineering College
Kalyani, Nadia, West Bengal, India
satyen_kgec@rediffmail.com

Abstract: There are many drawbacks inherent in the NXN Playfair cipher and the security level is not good. In this paper, a logical operation has been performed between key and output of Playfair algorithm. It has been observed that the drawback of the existing Playfair cipher has been improved using proposed method.

Keywords: Playfair Cipher, Plain Text, Key, Middle Text, Cipher Text, Effective Key**.**

I. INTRODAUCTION

Playfair is a one type of substitution cipher. In 1854, it was developed by Charles Wheatstone and promoted by Lord Playfair[1]. Playfair uses a 5x5 matrix which is filled by the key with no repeating letter followed by the remaining alphabet where I and J are placed in the same cell. The message is divided into digraphs for encoding. Any diagraph with repeating letters are separated by filler letter X. If the message consists of odd numbers of letter then also X is added to make it even. Each pair of plain text is replaced according to the four rules presented in [2]. Over the years, several methods like using 7x4 matrix[3], MXN matrix[4], 16x16 matrix[5] has been proposed to enhancement the security of the Playfair algorithm. In August, 2012, Amandeep Kaur and Harsh Kumar Verma[6] have proposed 3D (4X4X4Playfair cipher) which works on trigraph rather than using digraph. Ashish Negi, Jayveer Singh Farswan in their paper[7] they used Linear Feedback Shift Register (LFSR) for over 8x8 playfair cipher to make it more robust like the advanced ciphers available like AES and DES.

In this paper, 16x16 matrix has been taken to represent the key and other remaining characters. According the existing rules of Playfair cipher has been used to generate the cipher text. Here, this cipher text is known as middle text. Finally, the cipher has been generated by XOR operation between middle text and key. This type of work has not been applied in Playfair cipher. This is the reason of making this paper.

II. WEAKNESS OF EXISTING CIPHER

There are several weaknesses in the Playfair cipher; First of all, repeated plain diagram will create repeated cipher diagrams. Moreover, the pattern of a diagram followed by that same diagram reversed, like ‘er’ and ‘re’ in ‘aperture’, will also appear in the Cipher Text. These instances will often enable recognition of plain words in the Cipher Text, especially probable words or cribs. Once plaintext can be matched to Cipher Text, a section of the MxM square can be recovered.

The second weakness is that diagram frequency counts can lead to recognition of the most frequently occurring English diagrams. This helps to guess possible plain words and again helps to piece together the MxM square.

Thirdly the most frequently occurring Cipher Text letters are likely to be near the most frequent English letters=E=, =T=, =A= and =O= in the MxM square. This again helps in square reconstruction.

Another problem is the deviation of character when converting Plain Text to Cipher Text mainly when KEY is too short. In most of the cases character deviation in Cipher Text from Plain Text is 5 in case of 5x5 matrix, 6 in case of 6x6 matrix and 16 in case of 16x16 matrix.

III. PROPOSED METHOD

A. *Algorithm for Encryption:*

Input: Key and Plain Text.
Output: Cipher Text.
Methods:

Step 1.To read the keyword as “KEY” and the Plain Text as “PT”.

Step 2.To finds the Effective key (EK) after eliminating the repeated characters from the keyword.

Step 3.To construct a NXN matrix (M) by filling the character of keyword from left to right and top to bottom.

Step 4. To fill the reminder of matrix with the remaining characters.

Step 5. To divide the plaintext into pair of characters. Add the character “Null” or “X” based on the total number of character when there is an odd number of character in the message.

Step 6. To replace each pair “PQ” of PT by “XY” from M by using existing conversion process of Playfair algorithm and construct middle text (MT).

Step 7. To convert Middle text (MT) and Effective Key (EK) to their unsigned integer form.

Step 8. To perform bit-wise X-OR operation with the each value of middle text (MT)with the character of Effective key (EK) and store the value to an array C known as cipher text “CT”

B. Algorithm for Decription:

Decryption is the reverse process of the Encryption where at first the bit-wise X-OR operation is needed with the each value of Cipher text (MT) and the Effective key (EK) in order to get the Middle Text "MT". Then apply the existing Playfair decryption algorithm on MT to get the desired Plain Text PT.

IV. ILLUSTRATION WITH EXAMPLE

A. Encryption:

Consider the examples with the set of all characters of the range 0 to 255 as ASCII value.

Example 1:

Say Plain Text PT= Jalpaiguri 123%GEC
KEY=SILIGURI
Existing Playfair output or the middle text MT=
;n`|bjewyb!034FD
Final output or the encrypted cipher text CT=
h',;786>5%tb`}QB

Example 2:

Plain Text PT=Construct NXN matrix M with the KEY 345%
KEY=Chinmoy@!$
Middle text MT=hymrusx`zOYT@^us$qT-zoq pod"U9T'45G5
Cipher text
CT=
+□□□□ [?□1=t-1□3□UZ<w□□yWQK'J<W9HMuf□

Example 3:

Plain Text PT=ABAB2323BB$#()cdcdaskllk
KEY=Repeat Diagrams
Middle text MT= BCBC3434CC$)*dfdftlnnl
Cipher text CT= □&2"G□w]$1yW{O□□□F0i□□□

Example 4:

Plain Text PT=[1] David Shallcross, "The Playfair Cipher," (2008) Vinculum,
KEY=ISSN: 0157-759X.
Middle text MT= UXR =hyft7abmmd□btt(7^ifNRmbvibjtNEgx`bu8@)9)(0Ygod|e} e37
Cipher Text
CT=
□:XHSC*□9L$>*EBDE 5g1H□□ #XVYS_Cc|?V)1;□;7q□,□p□4!^\ULP□

Decryption

Cipher Text CT= □&2"G□w]$1yW{O□□□F0i□□□
Key=Repeat Diagrams
Middle Text=BCBC3434CC$)*dfdftlnnl
Plain Text=ABAB2323BB$#()cdcdaskllk

V. CONCLUSION

In this paper, one new has been proposed to enhance the security to the existing play fair cipher. Here the Effective key is X-ORed with the Middle Text to get the Encrypted Cipher Text. Since, the each character is unique in EK, the final output or the Cipher Text is fully different from the Plain Text. In example 3 we have given the PT of repeated characters but the CT is without the repeated key and hence improves security. The proposed method can be used in any types of (NXN) matrix which uses the Effective key (key without the repeating character) two times to improve the security in Playfair algorithm. To generalize our approach, more tests will be performed in future.

VI. REFERENCES

[1] David Shallcross, "The Playfair Cipher," (2008) *Vinculum*,vol. 45, no. 2, Pp. 4-6, 2008.

[2] Stallings W., "Cryptography and Network Security: Principles and Practice", 4th Edition, Prentice Hall, ISBN-10:0131873164, 2005.

[3] A. Alam, S. Khalid, & M. Salam, "A Modified Version of Playfair Cipher Using 7x4 Matrix," IEEE International Conference on Software and Computing Technology (ICSCT2010), vol. 2, pp. 36-38, October 17-19, 2010.

[4] Aftab Alam, Sehat Ullah, Ishtiaq Wahid, & Shah Khalid, "Universal Playfair Cipher Using MXN Matrix" International Journal of Advanced Computer Science, Vol. 1, No. 3, Pp. 113-117, Sep. 2011

[5] S.S.Dhenakaran, M. Ilayaraja, Extension of Playfair Cipher using 16X16 Matrix, IJCA, Volume 48– No.7, pp 38-40, June 2012.

[6] Amandeep Kaur, Harsh Kumar Verma, Ravindra Kumar Singh, "3D (4 X 4 X 4) - Playfair Cipher", IJCA, Volume 51– No.2, pp-36-38, August, 2012.

[7] Dr. Ashish Negi, Jayveer Singh Farswan, "Cryptography Playfair Cipher using Linear Feedback Shift Register", IOSR Journal of Engineering, Vol. 2(5) pp: 1212-1216, May. 2012.

[8] AtulKahate, "Cryptography and Network Security", New Delhi, Tata McGraw Hill Pvt. Ltd, 2008.

[9] Michael J. Cowan , "Breaking Short Playfair Ciphers with the Simulated Annealing Algorithm", Cryptologia, 32:1, 71-83, 2008.

[10] Behrouz A. Forouzan, D. Mukhopadhyay, "Cryptography & Network Security", New Delhi, Tata McGraw Hill Pvt. Ltd, 2013.

Short Bio Data for the Authors

Chinmoy Ghosh received his B.E (CSE) from North Bengal University and M.Tech (IT Courseware Engineering) from Jadavpur University. At present he is working as an Assistant Professor in the Dept. of Computer Science and Engineering at Jalpaiguri Govt. Engg. College, Jalpaiguri, West Bengal. His field of research areas includes cryptography & network Security, fuzzy logic, Image processing, Networking

SatyendraNathMandal received his B.Tech&M.Tech degrees in Computer Science & Engineering from University of Calcutta, West Bengal India. This author is AICTE Career Award for Young Teachers (CAYT) awarded from All India Council for Technical Education (AICTE) on 2010. He is now working as Assistant Professor in Department of Information Technology at Kalyani Govt. Engg. College, Kalyani, Nadia, West Bengal, India. His field of research areas includes cryptography & network Security, fuzzy logic, Artificial Neural Network, Genetic Algorithm etc. He has about 60 research papers in National and International conferences. His eleven research papers have been published in International journals.