Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

A Survey Paper on Different Modification of Playfair Cipher

Mohammed Haris
Dept of Computer Science
Jamia Hamdard University
New Delhi, India

Bhavya Alankar
Dept of Computer Science
Jamia Hamdard University
New Delhi, India

Abstract: Working of Playfair cipher depends on the characters that are first grouped in blocks and later substituted. We can add as many as block of messages but the size should be defined as 2 alphabets per block, known as diagraphs.Playfair cipher operates on block of characters encrypting and decrypting two characters at a time. In this cipher, the plain text digraphs are converted to cipher text digraphs and the cipher text digraphs are converted to decrypted text digraphs using a shared key known to both the encrypter and decrypter. Due to the traditional 5 x 5 matrix used in Playfair cipher it supports twenty five uppercase alphabets only. To overcome the drawbacks and limitations, various authors have proposed their modifications of Playfair cipher. The paper contains different variants of Playfair cipher proposed by different scholars on the basis of their respected parameters.

Keywords: Cryptography, Decryption, Encryption, Playfair Cipher, Security, Substitution, Symmetric Key.

1. INTRODUCTION

In today's scenario, 'information' has become indispensable to both individuals and organizations. There is always a threat that when information is transmitted the information can land up in wrong hands so a mechanism should be placed in order to protect that information. If information reaches the unauthorized person they might arise a lot of complications. Hence there is a need to hide the data so that a third person or irrelevant person cannot extract the exact message. As the growth and development of technology is increasing, the concern for the safety and security of data is increasing equally. We need to share the data in encrypted form on open communication channels to ensure its security. The norm of cryptography mainly focuses on the methodology with which a message is transformed into a covert form and then shared over public communication channels in order to maintain the confidentiality of the message. The process of encryption and decryption mechanism is completely done by Cryptography. Cryptology is the combination of cryptography and cryptanalysis where crypto has arrived from the Greek word kryptos means something hidden not revealed. Cryptography is numerical approach for impregnable communication in the front of third parties (called adversaries) over the large network.

The basic principle of the Cryptography lies in the fact that the original message is ciphered at the dispatcher's end, then transmitting that ciphered message over a secure channel and then finally being deciphered to obtain the original message over receiver's end.

Encryption and Decryption focuses on the security of the data. In Cryptography, the plaintext is the original message that the sender wants to transmit. Cipher text is the message which is obtained after the encryption is done using a key.

Encryption is the creation of the cipher text from the plaintext using a key. The value of the key is unique, only the authorized user has the permission to encrypt and decrypt the message. Decryption simply is the opposite of encryption where the plaintext is restored or recovered from given cipher text using the same keys.

Cryptographic algorithms are divided into two types: Symmetric key Cryptography and Asymmetric key Cryptography. In the symmetric key encryption, only one key is used for both encryption and decryption process. Symmetric algorithm does not require too much of computing power and it needs high speed to encrypt the message. In the asymmetric key encryption, more than one key is used for both encryption and decryption process. Asymmetric algorithm requires computing power and it even works with low speed to encrypt the message. We may further classify ciphers on the basis of techniques used in Algorithms: Substitution Cipher/ Transposition Cipher: In Substitution cipher each letter of the message is systematically replaced with another letter. The characters of plaintext are replaced by letters, numbers or symbols. While as in Transposition cipher, mapping is done using variety of permutation with the plaintext letters, where the plaintext characters are repositioned in regular pattern to form the cipher text.

Playfair cipher is the most popular poly-alphabetic cipher. Although, the original 5 x 5 Playfair cipher supports only 25 uppercase alphabets of the English language. In order to handle this problem, various authors have proposed extended Playfair cipher. This paper deals with the study of these variations proposed by different authors.

2. LITERATURE SURVEY

2.1 Traditional Playfair Cipher

In order for Playfair Cipher to work we need to choose a keyword for encryption and decryption key.

There is one simple rule for this that no letter should be repeated in the key.We take 'KEYWORD' as our key.

Now we need to create a 5 x 5 matrix table and the rules for it are:

1)Remove the letter J
2)Insert the desired keyword in the table
3)Followed the rest of the alphabets

Table 1. This is how the table looks

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

Now there are some rules for the preparation of your message before encryption which are:

- All the letters must be split into pairs
- Separate all the duplicate letters by putting 'X'
- If there is an odd letters at the end of the message,insert letter 'X'
- Ignore all the spaces

Now lets suppose we want to encrypt the message called "SECRET MESSAGE"
Following above rules we get:
SE CR ET ME SX SA GE

Encoding:

For encoding insert each pair into a separate table
1)If the pair is in the same column

- Move each letter down One
- Upon reaching the end of the table,wrap around to the start

2)If the pair is in the same Row

- Move each letter right one
- Upon reaching the end of the table,wrap around

3)If the pair forms a rectangle

- Swap the letters with the ones on the end of the rectangle

Putting into practice the above rules we get:
SE – NO
CR- RD
ET- KU
ME-NK
SX-QZ
SA-PC
GE-DN

Encryption- "NORDKUNKQZPCND"

Decoding

Now for the decoding we do the exact opposite using the previous made table.

2.2 Drawbacks of Traditional Playfair Cipher

Most basic disadvantage of this cipher is that it has a five into five matrix that can store on 25 uppercase characters due to which it is unable to store that are lowercased,whitespaces and other different characters.To Overcome these issues of the traditional Playfair Cipher several authors has proposed different solution to this problem.

3. Variants of Playfair Cipher

Ravindra Babu K, S. Uday Kumar, A. Vinay Babu, I.V.N.S Aditya , P. Komuraiah [1] proposed an advancement of playfair cipher in which the 5 by 5 matrix is replaced by a 6 by 6 matrix to accommodate all the uppercase alphabets as well as numeric digits. However lowercase alphabets, other printable characters and same letters in a digraph cannot be handled.

Shiv Shakti Srivastava and Nitin Gupta[2] proposed an advancement of playfair cipher in which the 5 by 5 matrix is replaced by a 8 by 8 matrix to accommodate all the uppercase alphabets as well as numeric digits and few symbols. They also suggested converting the cipher text to their respective ASCII values and perform LFSR on its 7 bit binary equivalent to obtain final cipher text. However lowercase alphabets still cannot be handled and encryption and decryption process takes more time due to LFSR.

Sanjay Basu and Utpal Kumar Ray [3] proposed an advancement of playfair cipher in which the 5 by 5 matrix is replaced by a 10 by 9 matrix to accommodate all the uppercase alphabets, lowercase alphabets, numeric digits, other symbols as well as white space. However by including the white space the cipher becomes weak as it becomes easier for the cryptanalyst to decipher the cipher text

P. Murali and G. Senthilkumar [4] proposed an advancement of playfair cipher in which the original 5 by 5 matrix is still used but they have coupled it with a random number generator method. They suggested converting the cipher text obtained from playfair ciper to their respective ASCII values and perform LFSR on its 7 bit binary equivalent to obtain final cipher text. However the limitations that were existing in original playfair cipher still persist.

G. Agrawal, S. Singh and M. Agarwal [5] proposed an advancement of playfair cipher in which the original 5 by 5 matrix is still used but they have coupled it with a technique to check the frequency of alphabets in the plaintext. They suggested combining the 2 alphabets with least frequency in forming the matrix rather than combining "I" and "J". However the limitations that were existing in original playfair cipher still persist.

Aftab Alam, ,Shah Khalidand , Muhammad Salam [6] proposed an advancement of playfair cipher in which the 5 by 5 matrix is replaced by a 7 by 4 matrix to accommodate all the uppercase alphabets as well as two special symbols. However lowercase alphabets as well as numeric digits cannot be handled.

Ouday Nidhal Ameen Hanosh and BaraaWasfi Salim [7] proposed an advancement of playfair cipher in which the 5 by 5 matrix is replaced by an 11 by 11 matrix tosupports all 26 alphabets in both upper case letters as well as lower case letters, all the numeric digits, special characters and the extended special characters.They also suggested settingthe cipher text of playfair cipher as input to the complete procedure of a cascade LFSR to get final cipher text.However by including the white space the cipher becomes weak as it becomes easier for the cryptanalyst to decipher the cipher text and encryption and decryption process takes more time due to LFSR.

V. Verma, D. Kaur, R. K. Singh and A. Kaur [8] proposed an advancement of playfair cipher in which the 5 by 5 matrix is replaced by a 4 by 4 by 4 three dimensional matrix to accommodate 64 characters that includes all the uppercase 26 alphabets, 10 numeric digits and 28 special symbols. However lowercase alphabets cannot be handled and the diagraph formed consists of three characters.

V. Verma, D. Kaur, R. K. Singh and A. Kaur [9] proposed an advancement of playfair cipher in which the 5 by 5 matrix is replaced by a 4 by 4 by 4 three dimensional matrix

to accommodate 64 characters that includes all the uppercase 26 alphabets, 10 numeric digits and 28 special symbols. They also suggested converting the cipher text to their respective ASCII values and perform LFSR on its 7 bit binary equivalent to obtain final cipher text. However lowercase alphabets cannot be handled and the diagraph formed consists of three characters.

N. Chand and S. Bhattacharyya [10] proposed an advancement of playfair cipher in which the 5 by 5 matrix is replaced by a 6 by 6 matrix to accommodate all the uppercase alphabets as well as numeric digits. They also suggested applying four rounds of playfair cipher to obtain final cipher text where output of one cipher acts as input for other and also use different keyword for each matrix. However lowercase alphabets, other printable characters and sameletters in a digraph cannot be handled.

S.S.Dhenakaran and M. Ilayaraja [11] proposed an advancement of playfair cipher in which the 5 by 5 matrix is replaced by a 16 by 16 matrix to accommodate all the possible ASCII characters in ascending order of their values (0-255). However by increasing the size of matrix by huge amount the time taken to construct key matrix and substituting characters from it increases and including the white space the cipher becomes weak as it becomes easier for the cryptanalyst to decipher the cipher text.

Swati Hans, Rahul Johari, Vishakha Gautam [12] proposed an advancement of playfair cipher in which the original 5 by 5 matrix is still used but they have coupled it with a random pattern generator method. They suggested swapping the order of rows and columnsusing patterns sequence of ten digits containing decimal numbers 1-5, like 1234525314 which can be sequence of swapping of rows and columns of key matrix. However the limitations that were existing in original playfair cipher still persist.

4. PARAMETERS TO BE ANALYZED

A cryptanalyst tries a range of cryptanalytic attacks to break a cryptographic algorithm. The commonly practiced cryptanalytic attacks are as follows.

1. Brute force attack
   In cryptography, a brute-force attack is a strategy which is used against every encryption algorithm. It involves consistently checking all potential keys till the proper keys are found.
2. Cipher text only attack
   A cipher text-only attack is an attack model in cryptology when the cryptanalyst has access to a group of cipher texts only.
3. Frequency analysis attack
   A Frequency analysis attack is based on the average, the probability of occurrence of any particular element in the cipher text instead of an element in plaintext.
4. Avalanche effect
   The phenomenon in cryptography when if small change is made in plain text say 1 bit has a huge change in cipher text like around half of the bits of total bits in cipher text is known as avalanche effect.

5. CONCLUSION

This paper focused on scrutinizing the distinctiveness, benefits and limitations of the original Playfair cipher and its proposed variants. It compares all these schemes on the basis of various cryptanalytic attacks, the limitations on acceptable characters as input, the problem of filler character and the integrity of plaintext.

It has been found that all the existing proposed variants of Playfair cipher missed one of the most important security parameter. No one has addressed the issue of maintaining the integrity of plain text and only a few of them have taken the avalanche effect into consideration. Our future work will be to propose an improved Playfair cipher that will be better than the proposed variants thus far and focus on maintaining the integrity of plain text.

REFERENCES

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

[2] S. S. Srivastava and N. Gupta, “A Novel Approach to Security using Extended Playfair Cipher”, International Journal of Computer Applications (0975 – 8887), vol. 20, no. 6, (2011) April.

[3] S. Basu and U. K. Ray, “Modified Playfair Cipher using Rectangular Matrix”, International Journal of Computer Applications (0975 – 8887), vol. 46, no. 9, (2012) May.

[4] P. Murali and G. Senthilkumar, “Modified Version of Playfair Cipher using Linear Feedback Shift Register”, IJCSNS International Journal of Computer Science and Network Security, vol. 8, no. 12, (2008) December.

[5] G. Agrawal, S. Singh and M. 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, no. 3, (2011), pp. 10-16

[6] A. Alam, S. Ullah, I. Wahid and S. Khalid, “Universal Playfair Cipher Using MXN Matrix”, International Journal of Advanced Computer Science, vol. 1, no. 3, (2011).

[7] Ouday Nidhal Ameen Hanosh and BaraaWasfi Salim, “11 × 11 Playfair Cipher based on a Cascade of LFSRs”. IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 1, PP 29-35, May-Jun. 2013.

[8] Kaur A.; Verma H. K.; Singh R. K., 3D (4 X 4 X 4) - Playfair Cipher, International Journal of Computer Applications, 51 (2), pp. 36-38, 2012.

[9] V. Verma, D. Kaur, R. K. Singh and A. Kaur, “3D- Playfair cipher with additional bitwise operation”, In Control Computing Communication & Materials (ICCCCM), 2013 International Conference on IEEE, (2013), August, pp. 1-6.

[10] N. Chand and S. Bhattacharyya, “A Novel Approach for Encryption of Text Messages Using PLAY-FAIR Cipher 6 by 6 Matrix with Four Iteration Steps”, International Journal of Engineering Science and Innovative Technology (IJESIT), vol. 3, no. 1, (2014) January, pp. 478-484.

[11] S. S. Dhenakaran and M. Ilayaraja, “Extension of Playfair Cipher using 16X16 Matrix”, International Journal of Computer Applications (0975 – 888), vol. 48, no. 7, (2012) June.

[12] Swati Hans, Rahul Johari, Vishakha Gautam, “An Extended PlayFair Cipher using Rotation and Random Swap patterns,” 5th IEEE International Conference on Computer and Communication Technology, (2014).