MODIFIED CYCLIC_PLAYFAIR CIPHER WITH CIPHER BLOCK CHAINING

MANTOO KUMAR GUPTA[1], RAJEEV KUMAR DAS[2]

[1]M.Tech Student, Computer Science and Engineering
[2]HOD, Computer Science and Engineering
Bhabha College of Engineering, RKDF University, Bhopal, M.P.

ABSTRACT: This paper deals with a new solution approach to overcome the shortcomings of the Playfair algorithm. In this paper, the presented Cyclic_Playfair encryption mechanism makes the cryptanalysis complex. The encrypted text obtained is almost unreadable. The proposed Cyclic_Playfair algorithm is implemented and number of tests is performed to prove its efficiency. Finally, it has been analyzed on the basis of avalanche effect.

Keywords-Patient Avalanche; Brute force; CBC; Cipher; Cryptanalysis; Encryption; Playfair

I. INTRODUCTION

Playfair cipher is the most preferred polyalphabetic cipher [1]. The initial Playfair includes of 5*5 grid during which simply 25 uppercase English alphabets are encrypted or decrypted. But, it fails to encrypt lowercase letters, different printable characters, white spaces, etc. In addition to that, one letter i.e. ‘J’ has to be discarded because of 25 squares. In order to solve this issue, numerous authors have proposed their improved Playfair cipher. Nevertheless, none of them have analyzed their proposed modified scheme on the basis of avalanche effect. All the above issues have been the motivating factor for the present research work i.e. to propose Cyclic_Playfair encryption mechanism so that it makes the cryptanalysis complex. The encrypted text obtained is almost unreadable. The proposed Cyclic_Playfair algorithm is implemented and number of tests is performed to prove its efficiency. Finally, it has been analyzed on the basis of avalanche effect.

II. RELATED WORK

In the variation projected by Packirisamy Murali and Gandhidoss Senthilkumar [2] the new rule adds several advantageous over the conventional Playfair cipher. The quantity of random sequences mapped to plaintext within the table is set by what percentage bits square measure sorted.

In the variation projected by Babu et al. [3], the extensive play truthful rule is predicated on the utilization of a half-dozen X half-dozen matrix of letters created employing a keyword. The matrix is made by picking up the alphabetic character of the keyword from leftmost to rightmost and from high to bottom, and therefore the filling within the remaining matrix with the left over letters in alphabetical order and digits in ascension from zero to nine. During this they need not counted I/J collectively letter instead they're inserting each I and J in 2 totally different cells so as to avoid the paradox to the user at the time of decoding.

In the variation projected by knife Shakti Srivastava, Nitin Gupta [4] the five x five matrix has been replaced by eight x eight matrix and thence it'd be mistreatment sixty four grids. The projected system not solely encrypts the alphabets however conjointly the numerals and special characters. It conjointly shows area between words wherever needed. The system uses totally different blocks for various alphabet, numerals and symbols. within the projected System, | is employed at the time of coding to produce area between 2 words, ^ is employed for stuffing between 2 alphabets if they're perennial during a try and ^ will be accustomed place at the top to urge the last alphabet in try if the whole length at comes bent on be odd. At the time of secret writing | are going to be replaced by place of 1 alphabet and therefore the image ^ are going to be discarded. Rules for encryption and decipherment are same.

In the variation proposed by Agrawal et al. [5], the frequency of every alphabet in the plaintext is calculated. The two letters with the smallest amount frequency square measure combined rather than combining I and J. The five x five matrix is made by inserting the keyword while not duplication of letters, the combined letters and finally the opposite letters. The rule is as follows.

- Enter the key for coding.
- Enter the text to be encrypted.
- Calculate the frequency of every alphabet within the text or phrase to be encrypted. The frequency has been calculated so as to provide a substitution matrix with the assistance of that coding and secret writing is going to be done. They need thought of the smallest amount 2 least frequency alphabets for combining and forming the substitution matrix. Doing this reduces the redundancy to a good extent because the letters or an alphabet that have either occurred within the text or their frequency of prevalence is least thereby reducing the probabilities of ambiguity to a good scale.
- Once calculative the frequency of every alphabet the array is sorted in ascending order to search out the 2 least occurring alphabets.
- Once sorting the 2 least occurring alphabets from the frequency array square measure combined within the substitution matrix.
- Once this, the encryption and decipherment is finished.

Alam et al. [6] delineated a coding technique that provides security and privacy by encrypting the message at the sender facet and decrypting it at the receiver facet. It has changed playfair cipher, 5x5 matrix to m x n matrix playfair cipher within which 2 symbols "*" and "#" square measure accustomed create it safer. The most factor is that it helps to encipher or rewrite plain text written in any language.

A DNA and Amino Acid-Based Implementation [7] modifies the Playfair cipher significantly by introducing DNA-based amino acid structures to the core of the ciphering process. The proposed work treats the plaintext as a binary stream. Each and every pair of bits of the binary stream is replaced with either A, C, G or T, which are the abbreviated forms of the four bases of DNA namely- Adenine, Cytosine, Guanine and Thymine respectively. The proposed algorithm is quite time consuming because of its lengthy procedure and requirement of multiple read / write operations. Additionally 8-bit ASCII is converted to codons or triplets of bit-pairs, so remaining offsets are to be taken care of. The proposed modification actually treats the plaintext file as binary data stream and thus enriches the character set and actually solves the problem of limited character support. Another major problem of the traditional playfair is the predictability of the cipher by using frequency testing of character occurrences.

A Framework based on Probability analysis of Character occurrence [8] is a new approach which keeps track of the frequency of occurrences of each and every character in English language and replaces the every next occurrence of the character with a character of least frequency of use. It the new word becomes a meaning word replace with the next character of least frequency. The modified algorithm is efficient than the original Playfair and can handle spaces, repetitive characters more efficiently but still lacks in the number of supported character set. Playfair using LFSR [9] proposes an efficient way to generate unpredictable different random number sequences from Linear Feedback Shift Register. The random sequence can be varied by varying logic functions and taps based on key. The proposal is more focused on a cost efficient hardware based implementation. Though the use of random numbers increases the strength of the cipher but it does not supersedes the probability of breaking it on the basis of the frequency test.

Integration of Encryption Techniques [10] suggested a blending of both classical encryption and modern encryption techniques. The hybrid technique of blended Playfair and Vigenere cipher with the structural aspects of DES and SDES to some extends deals with some drawbacks of classical techniques. The proposed hybrid technique results in better avalanche effect than the individual ciphers and thus provides better security. In the design of an algorithm with high Avalanche Effect the positive measures of the classical cryptographic algorithms, like-scrambling of bits, use of a larger (64bits or more) key are used to obtain a high Avalanche Effect. The algorithm splits the actual plaintext message into black of 64-bits (8-alphabets) and applies Playfair cipher. Then, on the resulting ciphertext intensive scrambling and thereafter is further ciphered using Vigenere. The cipher bits are further XOR-scrambled M times using a 16×16 S-Box. Further the bits are split into 16-bit blocks and XOR-ed internally.

Recently, Dhenakaran and M. Ilayaraja [11] projected extended Playfair cipher. This Playfair algorithmic program is predicated on the employment of 16x16 matrix of characters made employing a keyword. The matrix is made by filling the characters of keyword from left to right and from high to bottom. After this, fill the remaining characters in ascending order from 0 to 255. Hans et al. [12] used random variety generator for swap patterns in order that key'schanged once more and once more up to fifty the troubles (max).Randomization adds a lot of security. Swapped patterns sequence is of eight digits containing decimal numbers 1-4, like 12342314 this can be indiscriminately generated and tells sequence of swapping of rows and columns of key matrix.

Siddqui et al. [13] proposed modified Playfair cipher with 9*7 matrixes eradicates the limitation of original Playfair cipher with 5*5 matrixes and is further enhanced by using crossover and mutation genetic operators. The modified Playfair cipher supports all 26 alphabets, in both uppercase and lowercase and accommodates numeric digits 0-9.

III. PROPOSED ALGORITHM

To encrypt a message, the message is broken into digraphs (groups of 2 letters) and then mapped them out on the key table. Then following protocols are applied to each pair of letters in the plaintext:

1. If both alphabets lies on the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue.
2. If the alphabets lie on the same row of the table, they are to be interchanged with the letters immediate right of them respectively.
3. If the alphabets lie on the same column of the table, they are to be interchanged with the letters just below them respectively.
4. If the alphabets lie not on the same row or column, exchange them with the letters on the same row respectively but of the column of the other keeping the order of the pair intact.
5. After encryption of the first digraph, pick the output and re-construct the key matrix which will be utilized to encrypt another digraph.
6. Take another diagraph and repeat the steps from 1 to 5.

To decrypt a message, the message is broke into digraphs (groups of 2 letters) and then mapped them out on the key table. Then following protocols are applied to each pair of letters in the plaintext:

1. If the alphabets lies on the same row of the table, they are to be shuffled with the letters immediate left of them respectively.
2. If the alphabets lie on the same column of the table, they are to be interchanged with the letters immediately above them respectively.
3. If the alphabets do not lies on the same row or column, interchange them with the alphabets on the same row respectively but of the column of the other keeping the order of the pair intact.
4. After decrypting first digraph, pick the first digraph and re-construct the key matrix. It will be used to decrypt another digraph.

IV. RESULT ANALYSIS AND DISCUSSION

Result Analysis On The Basis Of Ciphertext Only Attack

The proposed Cyclic_Playfair has been implemented using 8 x 8 matrix. However, it could also be implemented using 16 x 16 matrix (one can use any ascii code). To launch a ciphertext only attack, the number of digraphs the attacker has to search would be 224 x 224 i.e. 50176 in the modified cipher instead of 26 x 26 i.e. 676 digraphs in the traditional cipher.

Result Analysis On The Basis Of Brute Force Attack

The size of key domain the traditional Playfair cipher was 25! (Factorial 25). However, in the modified Cyclic_Playfair cipher it is 256! (Factorial 256).

Table 1: Comparison of various variants of Playfair Cipher with Cyclic_Playfair

Playfair Ciphers	Size of key domain	Number of digrams required to be searched	Probability of occurrence of an element	Avalanche effect with change of only one character
Original	25!	676	0.038	Max. 02 Min. 01
Babu et al. [3]	36!	1296	0.028	Max. 02 Min. 01
Srivastava & Gupta [7]	64!	4096	0.016	Max. 02 Min. 01
Srivastava & Gupta [8]	64!	4096	0.016	Max. 02 Min. 01
Verma et al. [9]	64!	4096	0.016	Max. 02 Min. 01
Chand & Bhattacharyya [10]	36!	1296	0.028	Max. 02 Min. 01
Hans et al. [12]	26!*24*24	Difficult	Difficult	Max. 02 Min. 01
Siddiqui et al. [13]	21*23!	16384	0.008	-
Proposed Cyclic_Playfair	256!	65536	0.0039	Max. N*

* N means length of message but depends on the position of changed character

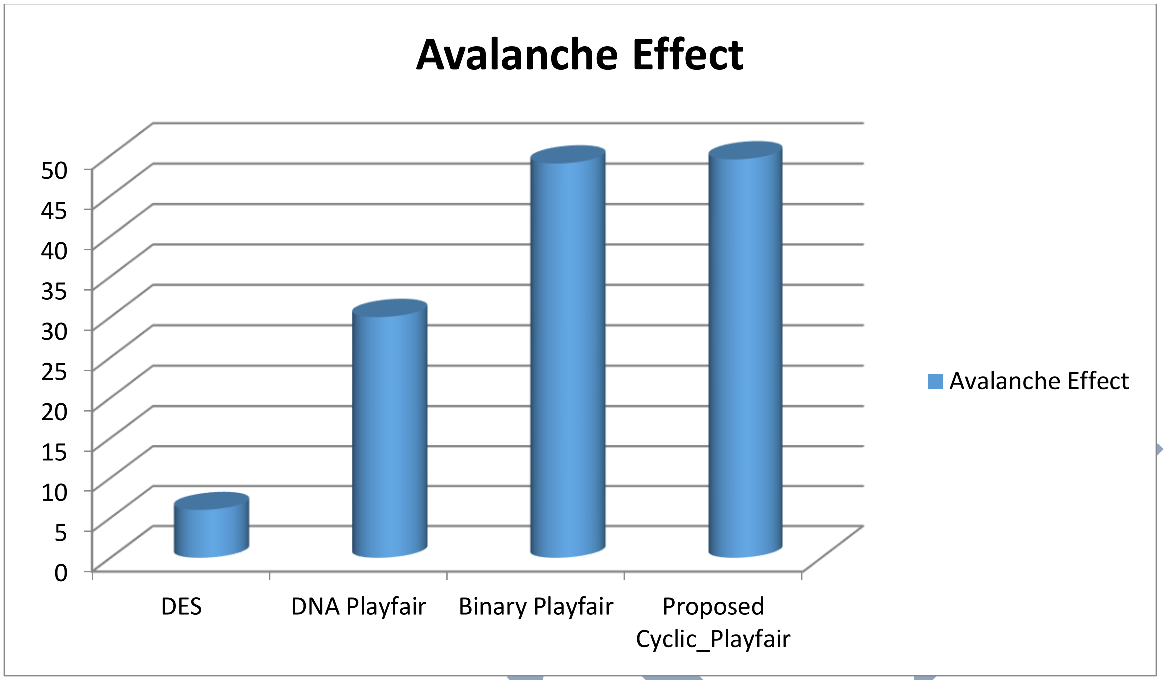

Figure 1: Comparison based on Avalanche Effect

Figure 1 shows the avalanche effect for different security algorithms by changing first character in the plaintext only. After analyzing we can conclude that DES exhibits only 6, DNA Playfair displays only 30, binary playfair reveals 49% characters changed in the output. However, our proposed Cyclic_Playfair shows change in 49.507% character in the output by changing only the first character in the plaintext.

V. CONCLUSION

The present paper compares all the existing variants of Playfair cipher found in the literature on the basis of Size of key domain

- Number of digrams required to be searched and
- The probability of occurrence of an element.

It has been found that no one has discussed avalanche effect in the existing literature. The proposed Cyclic_Playfair uses the encrypted digraph in order to re-construct the key matrix. It can be clearly seen that by the change of any character in the input, the difference will be reflected in the next coming ciphertext digraphs. If more number of characters is changed in the input then the output will be more different.

The proposed Cyclic_Playfair uses 16×16 key matrix. Still, many characters and symbols are left to be included. In future, one can extend it to include all printable characters for better results. It will not only give better avalanche but also increases key domain size and complex ciphertext only attack.

REFERENCE

[1] Behrouz A. Forouzan, Cryptography & Network Security, McGraw- Hill, Inc., New York, NY, 2007.

[2] 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.

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

[4] Shiv Shakti Srivastava, Nitin Gupta “A Novel Approach to Security using Extended Playfair Cipher”, International Journal of Computer Applications (0975 – 8887) Volume 20– No.6, April 2011.

[5] Gaurav Agrawal, Saurabh Singh, Manu 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 Issue 3 [2011] 10-16

[6] Alam, A., Ullah, S., Wahid, I., & Khalid, S. (2011). Universal Playfair Cipher Using MXN Matrix. International Journal of Advanced Computer Science, 1(3).

[7] Srivastava, S. S., & Gupta, N. (2011, June). Security aspects of the Extended Playfair cipher. In Communication Systems and Network Technologies (CSNT), 2011 International Conference on (pp. 144-147). IEEE.

[8] Srivastava, S. S., & Gupta, N. (2011). Rajaram jaiswal “Modified Version of Playfair Cipher by using 8x8 Matrix and Random Number Generation” in Proceedings of IEEE 3rd International Conference on Computer Modeling and Simulation (ICCMS 2011).

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

[10] Nisarga Chand, Subhajit 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) Volume 3, Issue 1, January 2014, 478-484.

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

[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.

[13] Mohammad Sadiq Nisar Siddiqui, Siddhartha Sankar Biswas, Parul Agarwal, “Genetic Extension of Playfair Cipher Using Modified Matrix,” International Journal of Computer & Mathematical Sciences (IJCMS), Volume 6, Issue 6, 2017, Page 25-30.