Playfair, The Substitution Cipher: A Review

Mantoo Kumar Gupta
MTech Scholar
Computer Science & Engineering
Bhabha College of Engineering, Bhopal

Rajeev Kumar Das
Assistant Professor
Dept. of Computer Science & Engineering
Bhabha College of Engineering, Bhopal

Abstract— **Playfair Cipher is one of the techniques which encrypts and decrypts a given data and keeps it isolated from several threats. The initial digraph substitution cipher is the playfair cipher. This was introduced by charles wheatstone in 1854, but was mentioned after Lord Playfair who elevated the use of the cipher instead of enciphering the single letter likewise in simple substitution. This paper presents review of existing Playfair ciphers with few variants of it.**

Keywords—Avalanche; Brute force; CBC; Cipher; Cryptanalysis; Encryption; Playfair

I. INTRODUCTION

The most common and mind haunting question that comes to someone's mind while communicating through any platform is, how to maintain confidentiality while sharing any information .As the people have become computer savvy protection of information in transit across the network has emerged with the enormous data exchange over the network . Since this need has been felt on several occasions, different encrypting and decrypting techniques have been evolved to serve the purpose.

Playfair Cipher is one of the techniques which encrypts and decrypts a given data and keeps it isolated from several threats. The initial digraph substitution cipher is the playfair cipher. This was introduced by charles wheatstone in 1854, but was mentioned after Lord Playfair who elevated the use of the cipher instead of enciphering the single letter likewise in simple substitution.

Playfair Cipher works on the principle of "Polygraphic substitution" which starts with a "key" which could be any combination of alphabets, numbers or both. To start the encryption a grid needs to be prepared, which is a square matrix which contains the key to encrypt the data as well the characters that are participating to convey the message. The rows of the grid are mainly formed by the "key" which is preprocessed by removing any word which has been repeated in key followed by the other characters. In the grid the word "I" and "J" occupies the same position. Even the word which is already mentioned in "key" is not further used in the grid. Once the grid is formed, encryption starts with help of it. First the white spaces are trimmed throughout the message and same letters of the message are separated by the letter "X". Now two letters are taken at a time and their position on grid is observed carefully as based upon the different conditions the letter pair is substituted with other letters. If the pair falls in same row then they are substituted with letter on their right, if they fall at end of the row then the letter at the extreme opposite end taken as the substitution. If the pair falls in the same row then they are substituted with the letter which falls exactly below them and if any of the two letters falls at the end of the column they are substituted by the extreme end letter. If the pair occupies in different rows or a column in the grid then imaginary rectangles is drawn which contains the pair as its corners and letters are substituted by the letter present opposite to them in that rectangle.

The decryption follows the same methodology but in reverse fashion. So to decrypt any coded message two letters are taken at a time. Based upon the different conditions the letter pair is substituted with other letters. If the pair falls in same row then they are substituted with letter on their left, if they fall at end of the row then the letter at the extreme opposite end taken as the substitution, and so on.

II. LITERATURE SURVEY

Extended Playfair Algorithm [1] proposed a use of a larger key matrix of size 6×6. This approach provides space for 36 characters, which include 26-alphabets of English language and all the 10-decimal numbers (0-9). But it needs more character support in order to be able to work over a large range of text file. They also proposed the use of transposition ciphers to preserve the frequency distribution of single letters to destroy the diagram and higher order distribution. Various Security Aspects of the Extended Playfair Algorithm [2] which uses a key matrix of size 8×8 and provides character support for any letter (even multilingual character),

number (of any base), symbol and any type of media file has been analyzed. The proposed 8×8 Playfair cipher can be said to be safe from Brute Force Attack, as the attacker has to find in a 64×64 = 4096 digraphs. Also the use of a 7-bit Linear Feedback Shift Register to generate pseudorandom numbers allows a key space of 2^7. So the altogether $64\times64\times2^7 = 2^{19}$ is quite a huge alternative to search for the proper key. Increasing the key size also reduces the chances to break the cipher by Frequency Analysis.

The Universal Playfair Cipher [3] uses dynamic key matrix of size m×n to accommodate any set of alphabets of any language. The proposal introduces use of two special symbols- * and #. The symbol * is inserted if there is a repetition of characters in the plaintext pair and # is added after any odd length words. Initially the total number of characters "k" of a natural language is determined (26 for English, 40 for Urdu), the size of the matrix is identified such that- m×n = k+2. Playfair key matrix is formed based on the Password / Key and the plaintext is encrypted word by word adding the symbols * or # where necessary. Modified Playfair involving Interweaving and Iteration [4] generalized and modified the Playfair cipher into a block cipher. The proposed work focuses on the use of ASCII values in playfair. The use of 7-bit ASCII values increases the character support to 128characters. The formidable task of finding the substitution in all the cases makes the brute force attack almost impossible. The use of numerous iterative substitution and interweaving steps also makes it resistance of known plaintext attacks. The time requirement of the proposed algorithm is quite high for its complex iterative procedures. And thus can be proven less effective in case of encryption / decryption of large files.

Modified Playfair for a Large Block Plaintext [5] is a technique which further modified the proposal to reduce the time complexity for the cases of encryption / decryption of large block of plaintext, by increasing the size of the plaintext matrix P_{ij} to n×m. The use of a larger block size of plaintext further reduces the possibilities of brute force attack. The time requirement of this proposed work is substantially low from the previous one as it applying iterative substitution and interweaving on a larger block size. These interweaving and iteration actually leads to lots of confusion and diffusion. Play Color Cipher [6] addresses the problem in a completely different way by generating a Block Cipher using Color Substitution. The binary values of 7-bit ASCII codes are used along with the corresponding colors of ARGB color model. The proposed "Play Color Cipher" substitutes each character of the plaintext with a color block from an 18 decillions of colors. This proposed work uses ARGB color model with 256 color shades for each one, thus limiting the maximum color address to 4294967296. But still, the proposed algorithm with 8-but ASCII support focus on the encryption of a character to corresponding color, limiting the scope to English language only. However some small changes in the proposed algorithm can also make it compatible to multilingual characters.

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. There are some drawback in classical techinque due to the hybrid technique which

blend the playfair and vigenere cipher with the structural aspect of DES and SDES. 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 [11] 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 [12] 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. [13] 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 enhanced and illustrate the sequence of swapping of columns and rows of key matrix.

III. Parameters Used to Analyze Playfair Cipher

A. Brute Force Attack

In cryptography, a brute-force attack, or thoroughgoing key search, could be a strategy which will be used against any encrypted information. Such AN attack may be utilized once it's unfeasible to require advantage of different impuissance in an encoding system (if any occurs) that may build the task easier. It involves consistently checking all potential keys till the proper keys are found. Within the worst case, this may involve traversing the complete search area.

B. Ciphertext Solely Attack

A ciphertext-only attack or legendary ciphertext attack is AN attack model for cryptology wherever the wrongdoer is assumed to possess access solely to a group of ciphertexts. The attack is totally winning if the corresponding plaintexts is deduced, or maybe higher, the key. The flexibility to get any info in any respect concerning the underlying plaintext remains thought-about a hit. For instance, if a soul is causing ciphertext incessantly to keep up traffic-flow security, it'd be terribly helpful to be ready to distinguish real messages from nulls. Even creating AN advised guess of the existence of real messages would facilitate traffic analysis. One in every of the strategies to launch a ciphertext solely attack could be a applied math technique like frequency analysis.

C. Avalanche Effect

In cryptography, the avalanche result refers to a fascinating property of science algorithms. Avalanche result is obvious if, once an input is modified slightly the output changes considerably. A little modification in either the key or the plaintext ought to cause a forceful modification within the ciphertext. If a cipher doesn't exhibit the avalanche result to a big degree, then it's poor organization, and therefore a decipherer will build predictions concerning the input, being given solely the output. This might be adequate to part or fully break the algorithmic program. Thus, the avalanche result could be a fascinating condition from the purpose of read of the designer of the science algorithmic program or device.

IV. Conclusion

The original Playfair cipher uses a digraph substitution technique to encrypt/decrypt alphabets based on a reference 5×5 key matrix, which is formed from the given key. The algorithm is strictly restricted to “English Alphabet”, that to either in uppercase or in lowercase character. No numbers, punctuations are supported. Several modification attempts focuses on elimination of several limitations. Some increases the character-set of the key matrix, some uses the ASCII values and others incorporated randomness. But these modifications stand strong in their own purposes. The overall limitations of the cipher were not eliminated by these individual modifications.

References

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

[2] 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.

[3] R.S. Bhadoria,D.Sahu and M. Dixit,”Proficient Routing in Wireless Sensor Networks through Grid Based Protocol”,International Journal of Communication Systems and Networks,vol.. 1,no. 2,(2012),pp. 104-109.

[4] K. Ravindra Babu,S. Uday Kumar,A. Vinay Babu.I.V.N.S Aditya and P. Komuraiah, “An Extension to Traditional Playfair Cryptograhic

Method".International Journal of Computer Applications(0975-8887) vol.17, no.5,(2011) March.

[5] 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.

[6] 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

[7] Shiv Shakti Srivastava and Nitin Gupta, "Security aspects of the Extended Playfair cipher", International Conference on Communication Systems and Network Technologies, 2011, Page 144-147.

[8] Aftab Alam, Sehat Ullah, Ishtiaq Wahid and Shah Kalid, "Universal Playfair Cipher Using M×N Matrix", International Journal of Advanced Computer Science, Vol. 1, No. 3, September 2011, Page 113-117

[9] V. Umakanta Sastry, N. Ravi Shankar and S. Durga Bhabani, "A Modified Playfair Cipher Involving Interweaving and Iteration", International Journal of Computer Theory and Engineering, Vol. 1, No. 5, December 2009, Page 597-601.

[10] V. Umakanta Sastry, N. Ravi Shankar and S. Durga Bhabani, "A Modified Playfair for a Large Block of Plaintext", International Journal of Computer Theory and Engineering, Vol. 1, No. 5, December 2009, Page 592-556.

[11] Lt. Ravindra Babu Kallam, Dr. S. Udaya Kumar and Dr. M. Thirupathi Reddy, "A Block Cipher Generation Using Color Substitution", 2010 International Journal of Computer Applications (0975 - 8887), Vol.1 – No. 28, 2010, Page 25-27.

[12] Mona Sabry, Mohamed Hashem, Taymoor Nazmy and Mohamed Essam Khalifa, "A DNA and Amino Acids-Based Implementation of Playfair Cipher", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 3, 2010, Page 129-136.

[13] Uttam Kr. Mondal, Satyendra Nath Mandal and J. Pal Choudhury, "A Framework for the Development Playfair Cipher Considering Probability of Occurrence of Characters in English Literature", 2009 International Journal of Computer Science and Network Security, Vol. 8, No. 8, August 2008.

[14] Packirisamy Murali and Gandhidoss Senthil kumar "Modified Version of Playfair Cipher using Linear Feedback Shift Register", 2009 International Conference on Information Management an Engineering, 2009, Page 488-490.

[15] Fauzan Saeed and Mustafa Rashid, "Integrating Classical Encryption with Modern Technique",IJCSNS International Journal of Computer 280 Science and2010, Page 280-285.