International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 04 | Apr -2017 www.irjet.net p-ISSN: 2395-0072

A Survey Paper on Playfair Cipher and its Variants

R.Deepthi[1]

[1]*Assistant Professor,Dept. Of CSE, Malla Reddy Engineering College for Women, Hyderabad.*

Abstract - Playfair cipher is the form of block cipher which has no limit on the number of characters in a message it can do, but it operates on block of characters encrypting and decrypting two characters at a time cipher. In this, the plain text digrams are converted to cipher text digrams and vice versa using a pre-shared key. This is achieved by performing several operations column wise row wise and by creating rectangular form. Even so the traditional 5 x 5 Playfair cipher supports twenty five uppercase alphabets only. To overcome this drawback, various authors have proposed extended Playfair cipher. This paper deals with the study of these variations proposed by different authors on the basis of some parameters.

Keywords: cryptography; encryption; decryption; Playfair; security

1.INTRODUCTION

In today's scenario, 'information' has become indispensable to both individuals and organizations. When any information is stored or transmitted by a message there should be some mechanism to protect that information from hackers a. 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. Even for static data, to prevent misuse of the data there should be some mechanism so that if a third party manages to get hold of the data he will not be able to find out the meaning of the data. Hence Cryptography plays an vital role in data communication in today's world.

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. Encryption is the idea of converting the real message into scramble message while decryption is just the opposite of it.

There are two ways of performing it one is substitution and another is transposition technique. Substitution is the way of substituting any alphabet, number; special characters at the place of plaintext .techniques which constitute it are playfair cipher, hill cipher, caeser cipher.

Transposition is the way of changing the position of given plaintext to get ciphertext technique which constitute this is rail fence cipher in which the plaintext is placed as a rail fence and read as row wise .likewise no extra alphabet, number is added in it.

Playfair cipher is the most popular polyalphabetic 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

Playfair cipher is the polygraphic subsititution. In traditional Playfair the position of I=J are incorporated into one square since English alphabets consist of 26 letters but in Playfair a matrix of five * five grid is made that is twenty five letters can only be embedded including keyword. To combat this, various authors have proposed extended Playfair cipher. For instance, if we select **puzzle** as the confidential keyword the matrix is shown in Table 1[1].

Table 1. Original Playfair 5 x 5 Matrix

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

Then the message is wrecked up into digrams or groups of two letters. Each letter can only be used once so further use of a letter is ignored leftover spaces are filled with the rest of the letters of the alphabet .The substitution occurs depending on the following three principles.

1. Just in case both the letters are in the same row, replace them with the letter on the right of the letter. If the letter is at the start, go to the next letter.
2. Just in case both the letters are in the same column, replace them with the letter below them. If the letter is at the top, go to the bottom of the column and use the letter to replace with top letter.
3. If neither of the alphabets lies in the same column nor same row, imagine creating a rectangle form and write the corners alphabets.

Just in case of secret writing the alternative is finished with the cipher text and that we retreat to the plain text. If we tend to take ballon as the plaintext and puzzle because the confidential keyword, the corresponding ciphertext will be as follows. In ballon it contains repeating letters so the letter X is to be inserted between the two repeated letters.

Initially the plaintext is reborn to capital and then variable into digrams mistreatment X as the artifact character. The digrams are going to be BA LX LO NX. For the primary digram B and A square measures within the same row. Mistreatment rule one we tend to get BC. Next we tend to take LX – they lie within the same column. Thence mistreatment rules two we tend to get DL. Consequent digram is LO that as before square measure neither within the same row or column. Thence mistreatment rule three we tend to get UR now the last diagram is NX that as before square measure neither lies in the identical row nor in a same column and then we tend to get RT. So the cipher text is BCDLURRT.

For decryption

1. Just in case both the letters are in the same row, replace them with the letter on the left of the letter. If the letter is at the start, go back to the end of the same row and just the letter to replace with start letter.
2. Just in case both the letters are in the same column, replace them with the letter above them. If the letter is at the top, go back to the bottom of the column and use the letter to replace with top letter.
3. If neither of the alphabets lies in the same column nor same row, imagine creating a rectangle form and write the corners alphabets.

plaintext	BA	LX	LO	NX
method	1	2	3	3
encryption	BC	DL	UR	RT
cipher text	BC	DL	UR	RT
method	4	5	6	6
decryption	BA	LX	LO	NX

Table 2. Playfair Encryption and Decryption

2.2 Drawbacks of Traditional Playfair Cipher

The original Playfair comprises of 5*5 grid in which 25 letters can be placed that to of uppercase so it cannot encrypt lowercase letters, whitespaces, different printable characters. Moreover one letter will be discarded due to 25 squares. This is the main downside so several new proposals have been discussed.

3. Variants of Playfair Cipher

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 Man *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

4. Parameters to be Analyzed

4.1 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.

4.2 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.

4.3 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.

5. Ease of Use

This section demonstrates a brief comparison of all the above variants of Playfair cipher.

Table 3. Comparative Analysis

Srivastava & Gupta [8]	64!	4096	0.016
Verma *et al.* [9]	64!	4096	0.016
Chand & Bhattacharyya [10]	36!	1296	0.028
Dhenakaran & Ilayaraja [11]	256!	65536	0.004
Hans *et al.* [12]	26!*24*24	Difficult	Difficult

6. Conclusion

This paper focuses on the study of original Playfair cipher and the other existing variants. It compares all these schemes on the basis of

key domain size for brute force attack

no. of digrams need to be searched for ciphertext only attack and

The probability of occurrence of an element for frequency analysis attack.

It has been found that all the existing work related to variants of Playfair cipher missed one of the most important security parameter. No one has discussed avalanche effect. Our future work will be to propose an improved Playfair cipher that will be better than the other related variants based on the avalanche effect also.

REFERENCES

[1] 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.

[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 Cryptographic 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

BIOGRAPHIES

R.Deepthi ,Working as an Assitant Professor of CSE department in Malla Reddy Engineering College for Women, Hyderabad. Pursuing PhD in Sri Satya Sai university, Bhopal. Madya Pradesh.