Avalanche Effect based Variants of Playfair Cipher for Data Security

[1]Rajeswari.S, [2]Ramya.N, [3]K.Saranya,
[12]Student, [3]Assistant Professor, Department of Computer Science and Engineering
Kumaraguru College of Technology, Coimbatore, India

Abstract

Cryptography is the technique of converting original message into non-readable form. It is further classified as Transposition technique and Substitution technique. One of the commonly used substitution technique is Playfair cipher. It is a form of block cipher which operates on block of characters, considering two characters at a time. One of the important considerations for measuring the strength of any cryptographic algorithm is its Avalanche effect, (i.e.) if an input is changed slightly, the output changes significantly. A good algorithm must have high Avalanche Effect. The traditional 5 x 5 Playfair cipher supports twenty five uppercase alphabets only. To overcome this drawback, extended Playfair ciphers were proposed. This paper deals with the study of these on the basis of Avalanche effect.

Keywords — *Cryptography, Substitution, Playfair Cipher, Avalanche effect.*

I. INTRODUCTION

In modern world, information is the biggest asset. When any information is stored or transmitted by a message there should be some mechanism to protect that information from unauthenticated third party who can be hackers. If information reaches the unauthorized person the security is totally lost. 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.

Cryptography is numerical approach for confidential communication over the large network. Encryption is the idea of converting the real message into scramble message while decryption is just the opposite of it as shown in Fig 1. 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.

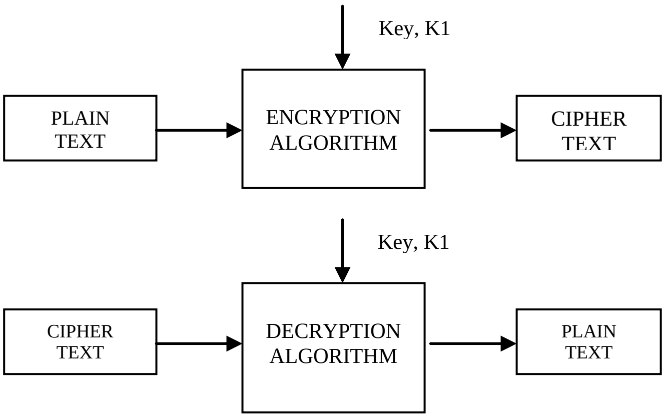

Fig 1.Encryption and Decryption Process

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 diagrams are converted to cipher text diagrams and vice versa using a pre-shared key. This is achieved by performing several operations column wise row wise and by creating rectangular form.

In order to apply an appropriate technique for a particular application it is required to know features like avalanche effect which is a desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the cipher text. In, particular a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher texts. In the existing technique producing avalanche effect can be raised using more specify operation and structure.

The Avalanche Effect is calculated as:

$$\text{Avalanche Effect} = \frac{\text{No of flipped bits in cipher text}}{\text{No of bits in cipher text}} \text{ X } 100\%$$

The paper is being organized as follows: the next section is about the working of traditional playfair Cipher and Section III discusses the variants of playfair cipher and section IV gives the comparative study results followed by the conclusion.

II. 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, the with the confidential keyword CRYPTO the matrix is shown in TABLE I.

Table I . Traditional Playfair Cipher

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

The message is split into 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.

The construction of 5x5 matrix using the keyword “CRYPTO” plus the uppercase alphabets satisfying the rules of prepare the table. The matrix is first filled by the keyword from left to right and the remaining cells are filled by the uppercase alphabets ignoring the letters of keyword.In this algorithm, the letters I & J are counted as one character. It is seen that the rules of encryption applies a pair of plaintext characters. So, it needs always even number of characters in plaintext message. In case, the message counts odd number of characters a spare letter X is added at the end of the plaintext message. Further repeating plaintext letters in the same pair are separated with a filler letter.

Initially the plaintext is reborn to capital and then variable into groups’ mistreatment X as the artifact character. The groups are going to be BA LX LO NX. Then the rules are applied and encryption is done. 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.

The drawbacks of Traditional Playfair Cipher is in which 25 letters can be placed only that as 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.

III. VARIANTS OF PLAYFAIR CIPHER

The traditional Cipher with few variations and features many ciphers were designed which are listed as follows:

Nisarga Chand et al,suggested a Novel Approach for Encryption of Text Messages Using Playfair Cipher 6 by 6 Matrix with Four Iteration Steps as in TABLE II.[13]

Table II . Playfair Cipher uing 6x6 Matrix

C	R	Y	P	T	O
A	B	D	E	F	G
H	I	J	K	L	M
N	Q	S	U	V	W
X	Z	0	1	2	3
4	5	6	7	8	9

In the four iteration steps, every time a keyword is used for encryption, thus the cryptanalyst will find it difficult to find the plain text. The main disadvantages of this matrix are that it cannot be used for numeric and also have to compromise between I and J. Here use this concept but extend the matrix dimension 6 by 6, so that can include numeric as well as I and J. To make the algorithm stronger here use four iteration steps instead of one. Since it takes place as four iteration every time a key word is used and encryption is done. This is done to have a high avalanche affect.

A.Aftab Alam et al, proposed a A Modified Version of Playfair Cipher Using 7×4 Matrix where the original 5X5 matrix playfair cipher is modified to 7x4 matrix playfair cipher in which two symbols “*” and “#” are included as in TABLE III. The addition of these two symbols in the matrix creates one-to-one correspondence between the plaintext and the ciphertext, which makes the encryption and decryption easy and unambiguous. The text is more unreadable when these symbols appear in the resulting ciphertext. Also this method can be extended to encrypt and decrypt the messages of any language by taking a proper size matrix.[14]

Table III. Playfair Cipher uing 7x4 matrix

C	R	Y	P
T	O	A	B
D	E	F	G
H	I	J	K
L	M	N	Q

S	U	V	W
X	Z	*	#

Nitin Gupta et al, have modified the Playfair cipher by using 8*8 matrix along with LFSR for random number generation as in TABLE IV. In the present paper, assume that the characters of the plaintext belong to the set of ASCII characters denoted by the codes 0 to 127. Here, the strength of the cipher enhances significantly and no cryptanalytic attack would be possible on account of the modifications. For this all the drawbacks are analysed and security loopholes and provide a new cipher which is a strong one.[2]

Table IV . Palyfair Cipher uing 8x8 with LFSR

S	H	I	V	@	A	K	T
B	C	D	E	F	G	J	L
M	N	O	P	Q	R	U	W
X	Y	Z	0	1	2	3	4
5	6	7	8	9	!	#	$
%	^	&	*	(	)	-	%
=	{	}	[	]	\	|	:
;	‘	.	<	>	/	.	?

Shiv Shakti Srivastava et al suggested extension for playfair cipher using 16*16.It secures information mathematically by mangling message using with key. The privacy information is protected from eavesdropper. The restrictions of earlier works a playfair cipher using 5x5 matrix,7x4 matrix and 6x6 matrix are overcome in the 16x16 matrix. The proposed work is an enchancement to the existing algorithms that uses 16x16 matrix to pick cipher characters. This algorithm can accept the plain text containing alphabets , numbers and special characters.so the user can easily encrypt combination of alphabets ,numbers, characters efficiently.it is concluded the selection of keyword can generate full of machine symbols in the cipher. the feature applications are different keys using encryption and decryption process .public key is used for encrypt process and private key used for decrypt process. The algorithm eliminates the repeated characters in keyword. Construct a matrix by filling the character of keyboard from left to right and top to bottom. Fill the remainder of matrix with the remaining characters from ASCII values 0 to 255.The repeating plaintext characters that are in the same pair the first character is replaced by the character to the right, with the first element of the row circularly following the last. The second character is replaced by the character to left, with the last element of the row circularly following the first. If a word consists of odd number of characters, it will add the character “null” to complete the pairs ,because “null” character cannot affect the plaintext at the time of decipherment.[2]

Harinandan Tunga1etal, came up with a new modified playfair algorithm based on frequency analysis (16*16) in which two private keys f variable length are chosen. According to the original Playfair Algorithm create the key table using the first key. Take the plain text from the user and internally break the input text into diagrams. If odd numbers of characters are present have to append a „¿‟. Let the secondary key be A1 of odd length. Now will define a key A2 from A1 by removing the last character from A1. Else A2=A1 The plain text is divided into a number of blocks. The blocks are created dynamically. The first block size will be e qual to length of the A2.The current block of interest will be stored in an array „PT‟. The plain text of size A2 is converted into modified plain text of size A2.For generating modified plaintext corresponding to blocks of plain text- (i) Take the primary key and the secondary key in two different arrays and also another array say M for storing the generated characters. (ii) Compare the character of the primary key with the The character of the secondary key.(Initially i=0). (iii) Take the greater one. Let it be „G‟. + 1 for secondary key and i=((i+1)%(primary key length)) for primary key. (x) Let the generated string be „S‟. (xi) Encrypt „S‟ using the current key table. Let it be „E‟. (xii) Now a virtual text „V‟ = ‟E‟.[3]

Subhajit bhattacharyya et al, proposed a modified encryption technique using playfair cipher 10 by 9 matrix with iteration steps as in TABLE V. It is new technique which includes a rectangular matrix having 10 columns and 9 rows and six iteration steps for encryption and decryption purpose. This 10x9 rectangular matrix as in Fig 2 ,includes all alphanumeric characters and some special characters. single common key used for encrypt and decrypt the message.[6]

Table V. Playfair Cipher uing 10x9 Matrix

D	u	p	l	i	C	a	T	e	2
9	b	d	f	g	H	j	K	m	n
o	q	r	s	v	W	x	Y	z	A
B	C	E	F	G	H	I	J	K	L
M	N	O	P	Q	R	S	T	U	V
W	X	Y	Z	0	1	3	4	5	6
7	8	~	.	.	/	;	“	\	|
<	>	?	(	(	}	-	=	!	@

Keyword:DuplicaTe

Sanjay Basuetal,suggested a Modified playfair cipher using rectangular matrix in which Two letters in the plaintext is converted to cipher text. during encryption using a key. Cipher text can converted into plain text using the same key.one letter has to be omitted and cannot be reconstructed after decryption. Also lowercase letters ,white space, numbers and other prim table characters cannot be handled by traditional cipher. Playfair cipher being a polyalphabetic cipher the attacker has to search in 26x26=676 diagrams. Although the frequency analysis is much more difficult than in monoalphabetic cipher still using modem computational techniques the attacker can decipher the cipher text.to overcome the drawbacks propose a modified cipher which uses a 10x9 matrix which will contain almost all the printable characters.

Zubair Iqbal et al,found a way to Enhance the security of playfair technique using excess 3 code (xs3)and ceasar cipher:It is showed that proposed technique is stronger than the original playfair cipher and provide better security to the plaintext and key as compared to original playfair technique.[12]

Table VI . Playfair Cipher uing Excess 3 Code

V	I	P	S	o	H
D	e	F	G	i	J
K	m	N	Q	r	T
U	w	X	Y	z	0
1	2	3	4	5	6
7	8	9	A	b	C

IV. COMPARATIVE STUDY AND FUTURE DIRECTIONS.

The plaintext ought to cause a forceful modification within the cipher text. 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.

Table VII. Comparison of Variants of Playfair cipher

Playfair	Matrix order	Key domain size	No of iteration	Avalanche effect
Original	5X5	25!	1	0.22
Nisarga Chand	6X6	36!	4	0.32
A. Aftab Alam	7X4	64!	2	0.11
Subhajit hattacharyya	10X9	128!	6	0.47
Shiv Shakthi Srivastava	8X8	64!	LFSR	0.55
Harinandan Tunga	16x16	256!	Multiple iterations	0.62
Zubair Iqbal	6X6	36!	1	0.25

There are various limitations' in each variants of cipher:

In 5x5, letters I and J are considered as one character.26 letters alone can take as keyword without duplicates. Space between two words in the plaintext is not considered as one character. It cannot use special characters and numbers. It only uppercase alphabets.

In 7x4 Matrix, 26 characters only can take as a keyword without any repetition The space between two words in the plaintext is not considered as one character. It cannot use numbers and special characters except * and #.It is not case sensitive. It ignores the symbols * and # at the time of decipherment. In 6x6 Matrix, it can only take 36 characters as a keyword without duplicates. Space between two words in plaintext is not considered as one character.The matrix cannot accept special character. It is not case sensitive.[10]

V. CONCLUSION

In this paper,the traditional Playfair cipher is discussed in brief and the other existing variants proposed earlier were compared on the basis of matrix order, Key domain size, no of iterations, Avalanche effect. It has been found that all the existing work related to variants of Playfair cipher did not concentrate on avalanche effect which is dealt as a parameter for comparision in this paper.The future works will be to propose an improved Play fair cipher with high avalanche effect compared to its variants.

REFERENCES

[1] Priyanka Goyal, Gaurav Sharma and Shivpratap Singh Kushwah, "A Survey Paper on Playfair Cipher and its Variants", Vol.3. ITM Group of Institutions, Gwalior, India, No.1 (2015), pp.1-6.

[2] Shiv Shakti Srivastava, Nitin Gupta, "A Novel Approach to Security using Extended Playfair Cipher", National Institute of Technology Hamirpur, India Volume 20– No.6, April 2011.

[3] Harinandan Tunga1, Soumen Mukherjee2, "A New Modified Playfair Algorithm Based On Frequency Analysis", Volume 2, Issue 1. Kolkata, West Bengal, India, January 2012.

[4] Fauzan Saeed, Mustafa Rashid, "Integrating Classical Encryption with Modern Technique ", VOL.10 No.5, Karachi, Pakistan, May 2010.

[5] K. Banupriya, Dr.G.Arutchelvan, "Improved playfair with multistage encryption and decryption", Volume 2, Issue 10, Vellore, Tamil Nadu, India, June-2015.

[6] Subhajit Bhattacharyya, Nisarga Chand, Subham Chakraborty, "A Modified Encryption Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps", Volume 3, Issue 2, India, February 2014.

[7] Nisarga Chand, Subhajit Bhattacharyya, "A Novel Approach for Encryption of Text Messages Using PLAY-FAIR Cipher 6 by 6 Matrix with Four Iteration Steps", Volume 3, Issue 1, January 2014.

[8] A. Aftab Alam, B. Shah Khalid, and C. Muhammad Salam, "A Modified Version of Playfair Cipher Using 7×4 Matrix ", Vol. 5, No. 4, August 2013.

[9] Vinod Kumar, Santosh kr Upadhyay, Satyam Kishore Mishra, Devesh Singh, "Modified Version of Playfair Cipher Using Linear Feedback Shift Register and Transpose Matrix Concept", Volume-3, Issue-1, June 2013.

[10] Sanjay Basu, Utpal Kumar Ray, "Modified Playfair Cipher using Rectangular Matrix", Volume 46– No.9, Kolkata, India, May 2012.

[11] Hadab Khalid Obayes, "Suggested Approach to Embedded Playfair Cipher Message in Digital Image", Vol. 3, Issue 5, Babylon University, Iraq, pp.710-714, Sep-Oct 2013.

[12] Zubair Iqbal, Bhumika Gupta, Kamal Kr. Gola, Prachi Gupta, "Enhanced the Security of Playfair Technique using Excess 3 Code (XS3) and Ceasar Cipher", Volume 103 – No 13, M.I.T, Moradabad, GB Pant Eng. College, October 2014.

[13] Nisargachand,subhajitBhattacharyya,"A Novel Approach for encryption of text messages using PLAYFAIR cipher 6 by 6 matrix with four iteration steps",volume 3,issue1,January 2014.

[14] A.Aftab Alam,B.Shah Khalid,C.Muhammad salam,"A modified version of Playfair Cipher using 7x4 matrix"volume.5,no.4,August 2013.

[15] Shiv Shakthi srivastava,Nitin Gupta,"A Novel Approach to security using extended Playfair Cipher",volume 20.No.6,Hamirpur,India,April 2011.