Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 6, Issue 07, July -2019

An Enhanced Play Fair Cipher Cryptography Technique for Data Security

Dr.B.Rebecca Jeyavadhanam

Associate Professor
Department of Computer Applications
SRM Institute of Science and Technology
Kattankulathur, Tamilnadu, India

Abstract— *The theme of this research work is to design and develop a very strong cryptographic technique which will be used to provide the security for the alphanumeric characters, special characters and number when we transmit over the network. However, this cryptographic technique very well addresses the problems that were faced by the classical play fair and 3D Play fair technique is used in the present study. In this paper, an enhanced approach has been done to overcome the problem in existing traditional playfair technique. In this work, there are 4 characters used at the same time and make them as a pair and then it will be considered them for the encryption. As we had the problem in the classical play like using i and j as same character here we eliminate this problem and then we also eliminate the problem of 3D play fair which will use only certain limited character sets for encryption and that is not case sensitive. But in our proposed method, we have taken into consideration of all the 256 ASCII characters for encryption and are also very complex algorithm when compared to previous replacement techniques.*

Keywords—*Advanced play fair, advanced play fair encryption, ASCII , 3D play fairer placement algorithms.*

I. INTRODUCTION

The best know multiple-letter encryption cipher is the Playfair, which treats digrams in the plain text as single units and translate into cipher text. This cipher was actually invented by British scientist Sir Charles Wheatstone in 1854, but it bears the name of his friend Baron Play-fair of St. Andrews, who championed the cipher at the British foreign office [1]. It had the drawback that a digraph and its reverse will encrypt in the same fashion. i.e., if A and B are plain text that produces X and Y , then B and A will produce Y and X. Keeping in mind that all the characters are ASCII characters which we use in general for the data transmission and almost all the alphabets both upper case and lower case are used widely along with numerals and special characters, here we are considering 256 ASCII character which includes the extended ASCII values also for framing the secret key word matrix and then for obtaining the encrypted messages. Here, the main concern is to create a encryption algorithm which uses the substitution technique and considers all the ASCII characters for encryption and decryption.

II. PROPOSED WORK

This paper proposes an advanced play fair which is a multiple letter encryption technique based on the substitution mechanism which will consider 4 characters of plain text to convert them in corresponding cipher text of 4 characters. To achieve this type of encryption we are need to have 4 X 4 bigger matrixes like structure again which will have in each cell of a 4 X 4 matrix. Hence, each small 4 X 4 matrix will have 16 characters and then we have similarly 16 such matrix which all together form 256 characters. First we will consider the alphabets (upper case(26) first then lower case(26)) and then numerals(10) and then the ASCII character in the ordered fashion. In previous play fair cipher techniques we usually had key matrix generation, encryption algorithms and decryption algorithms which will be discussed below in detail. The main contribution in this research is finding the new encryption algorithm which is based on replacement technique and the introduction of all the 256 character in that process for more confusion. Again we are going to use Radix 64 algorithm for transmitting the data via network so that most the readable format is alone sent.

2.1. Key matrix generation

This is very simple Key Matrix Generation as we had in classical Play fair techniques. Here the cube which get is made used for the encryption purposes and also for decryption. Here first we will be concentrating on diagonal of the bigger matrix, first we will fill them only.

The matrix generation is as follows:

1. First we have to accept the secret keyword which we will be containing combination of alphabets, numeric and then special characters. Like, HeisMulti-Talented, Don'tWasteit, Believeitornot etc.,

2. Then we have to make the presence each character one time and dropping out the duplicating ones like HeisMult-Tand, Don'tWasei, Belivtorn.

For example: Plain Text : HeisMult-Tand

H	e	i	s	M	u	l	t	-	T	a	n	d
48	65	69	73	4D	75	6C	74	2D	54	97	6E	64

3. Arrange them in the first row and first column, then arrange in second row and second column for next matrix, and then make it for 3rd matrix and 4th matrix and so on.

4. Then we have fill the remaining spaces in the matrix First we will be taking the first column to fill in order, after we finish we will go for second and then third so on.

5. While we are filling we have to use the Hexadecimal values only.

2.2. Encryption

The encryption which we are doing in this type is two step process. In the first step we will be considering the 4 character and will find the cipher text for them which is told in detail below, during the separation of this 4 letters if we find anything two letters to be similar then we will be introducing X between them. Then if any characters are left free we will be adding X, Z and finally _ to make them as a pair of 4 characters. And then using Base 64 algorithm again we will be converting them into plain text which can be displayed in the text editor application. Steps involved in the encryption process are as follows. Consider the plain text. Divide them and group them as 4 in a group Then we have to find the cipher text of the each four character using the below table. See that it is in circular fashion. First letter will be having 2nd as next letter and then 3rd and next to next and 4th letter as final letter. While for 2nd letter, 3rd as next, and 4th as next to next and 1st as the final letter. And it will be going on for all the letters.

Table 1. Encryption process of extended play fair

Plain Text	Plain Text of the poly character				Cipher Text
	1st Letter	2nd Letter	3rd Letter	4th Letter	
1st Letter	Row	Column	Matrix Row	Matrix Column	1st Letter
2nd Letter	Matrix Column	Row	Column	Matrix Row	2nd Letter
3rd Letter	Matrix Row	Matrix Column	Row	Column	3rd Letter
4th Letter	Column	Matrix Row	Matrix Column	Row	4th Letter

After we get the cipher letter hexadecimal values we then have to find the binary value for each and every hexadecimal we have got. Then for those binary values we have to make them as 6 bits as we have in base 64 algorithm. The base 64 algorithm uses A-Z in sequence manner and then followed by a-z and then 0-9 then + and / as the 64 character. The final result of cipher will be any one of these. Then we have to find the corresponding printable character and make it as the final cipher and save them in the note pad so that we can send it through network.

2.3. Decryption

The Decryption involves almost the similar step of the encryption where we also have 2 step. First is to make use of Radix 64 algorithm and find out the binary values of each and every character we have received. Then we will divide them into 8 bits and then we will be finding the hexadecimal values. It is reverse process of encryption. The detailed steps is as follows. The first step is to receive the cipher text from the network which is made as readable in the notepad. Then convert them into 6 bit binary values according to the Radix 64 table. Make them as 8 bit binary values. Convert them to hexadecimal values which we will be using to get the cipher text.

Table II. Decryption process of extended play fair

Cipher Text	Cipher Text				Plain Text
	1st Letter	2nd Letter	3rd Letter	4th Letter	
1st Letter	Row	Matrix Column	Matrix Row	Column	1st Letter
2nd Letter	Column	Row	Matrix Column	Matrix Row	2nd Letter
3rd Letter	Matrix Row	Cube Column	Row	Column	3rd Letter
4th Letter	Matrix Column	Matrix Row	Column	Row	4th Letter

Then as in encryption we have separate them into 4 characters so that we use them for getting plain text ASCII hexadecimal values. Then method which we will be using for this is shown in the below table. Then after we get the values we will have to compare with the ASCII table and make them to normal plain text as we had before encryption. Then if we find any unwanted additional X or Z or _ in the middle of the message of at the end of the message we just have to remove them.

2.4. Analysis of the proposed extended play fair cipher

Here is the example with the key "HeisMult-Tand"
Plain text is: God is great
Poly Char: {God }, {is g}, {reat}
Hexadecimal values: {47 6F 64 20}, {69 73 20 67} , { 72 65, 61 74}

Table III. Key matrix generation

	Column 1				Column 2			
Row 1	48	65	69	73	3C	3D	3E	3F
	4D	75	6C	74	40	5B	5C	5D
	2D	54	61	6E	5E	5F	60	7B
	64	41	42	43	7C	7D	7E	7F
Row 2	01	02	03	04	44	45	46	47
	5	6	7	8	49	4A	4B	4C
	9	A	B	C	4E	4F	50	51
	D	E	F	10	52	53	55	56
Row 3	11	12	13	14	80	81	82	83
	15	16	17	18	84	85	86	87
	19	1A	1B	1C	88	89	8A	8B
	1D	1E	1F	20	8C	8D	8E	8F
Row 4	21	22	23	24	90	91	92	93
	25	26	27	28	94	95	96	97
	29	2A	2B	2C	98	99	9A	9B
	2E	2F	3A	3B	9C	9D	9E	9F

	Column 3				Column 4			
Row 1	A0	A1	A2	A3	D0	D1	D2	D3
	A4	A5	A6	A7	D4	D5	D6	D7
	A8	A9	AA	AB	D8	D9	DA	DB
	AC	AD	AE	AF	DC	DD	DE	DF

Row 2	B0	B1	B2	B3	E0	E1	E2	E3
	B4	B5	B6	B7	E4	E5	E6	E7
	B8	B9	BA	BB	E8	E9	EA	EB
	BC	BD	BE	BF	EC	ED	EE	EF
Row 3	57	58	59	5A	F0	F1	F2	F3
	62	63	66	67	F4	F5	F6	F7
	68	6A	6B	6D	F8	F9	FA	FB
	6F	70	71	72	FC	FD	FE	FF
Row 4	C0	C1	C2	C3	76	77	78	79
	C4	C5	C6	C7	7A	30	31	32
	C8	C9	CA	CB	33	34	35	36
	CC	CD	CE	CF	37	38	39	00

2.5. Encryption

Table IV. Encryption of 47 6F 64 20

Plain Text	Plain Text of the poly character				Cipher Text
	47	6F	64	20	
47	Row	Column	Matrix Row	Matrix Column	48
6F	Matrix Column	Row	Column	Matrix Row	8C
64	Matrix Row	Matrix Column	Row	Column	BF
20	Column	Matrix Row	Matrix Column	Row	20

Table V. Encryption of 69 73 20 67

Plain Text	Plain Text of the poly character				Cipher Text
	69	73	20	67	
69	Row	Column	Matrix Row	Matrix Column	5A
73	Matrix Column	Row	Column	Matrix Row	14
20	Matrix Row	Matrix Column	Row	Column	43
67	Column	Matrix Row	Matrix Column	Row	6C

Table V. Encryption of 72 65 61 74

Plain Text	Plain Text of the poly character				Cipher Text
	72	65	61	74	
72	Row	Column	Matrix Row	Matrix Column	41
65	Matrix Column	Row	Column	Matrix Row	A2
61	Matrix Row	Matrix Column	Row	Column	1C
71	Column	Matrix Row	Matrix Column	Row	74

The resultant hexadecimal cipher value is 48 8C BF 20 5A 14 43 6C 41 A2 1C 74 Binary value for above in 8 bit is 01001000100011001011111100100000010110100001010001 00001101101100010000011010001000111000011101000 Encoding the binary value using Radix 64 Algorithms [3].

MDEwMDEwMDAxMDAwMTEwMDEwMTExMTExMDAxMDAwMDAwMTAxMTAxMDAwMDEwMTAwMDEwMDAwMTEwMTEwMTEwMDAxMDAwMDAxMTAxMDAwMTAwMDAx MTEwMDAxMTEwMTAw is the cipher text which will be sent through the network.

2.6. Decryption

Cipher text:
MDEwMDEwMDAxMDAwMTEwMDEwMTExMTExMDAxMDAwMDAwMTAxMTAxMDAwMDEwMTAwMDEwMDAwMTEwMTEwMTEwMDAxMDAwMDAxMTAxMDAwMTAwMD AxMTEwMDAxMTEwMTAw

Decoding of cipher text using Radix 64 Converter
01001000100011001011111100100000010110100001010001
00100001101101100010000011010001000 001110001110100
The resultant hexadecimal cipher value is 48 8C BF 20 5A 14 43 6C 41 A2 1C 74

Table VI. Decryption of 48 8c bf 20

Cipher Text	Cipher Text				Plain Text
	48	8C	8F	20	
48	Row	Matrix Column	Matrix Row	Column	47
8C	Column	Row	Matrix Column	Matrix Row	6f
BF	Matrix Row	Cube Column	Row	Column	64
20	Matrix Column	Matrix Row	Matrix Column	Row	20

Table VII. Decryption of 5a 14 43 6c

Cipher Text	Cipher Text				Plain Text
	5A	14	43	6C	
5A	Row	Matrix Column	Matrix Row	Column	69
14	Column	Row	Matrix Column	Matrix Row	73
43	Matrix Row	Cube Column	Row	Column	20
6C	Matrix Column	Matrix Row	Column	Row	67

Table VIII. Decryption of 41 a2 1c 74

Cipher Text	Cipher Text				Plain Text
	41	A2	1C	74	
41	Row	Matrix Column	Matrix Row	Column	72
A2	Column	Row	Matrix Column	Matrix Row	65
1C	Matrix Row	Cube Column	Row	Column	61
74	Matrix Column	Matrix Row	Column	Row	74

The final plain text hexadecimal value is 47 6F 64 20 69 73 20 67 72 65 61 74 .On comparing the above hexadecimal values with the ASCII values we get the result as “God is great” which is our plain text. Since we have used every spacing and letters correctly we did not get any extra characters in the final plain text. If any space found, it is needed to remove them off.

III. PROPERTIES OF CUBIC PLAY FAIR

The proposed cubic play fair cipher have lot of advantages when we compare it to the classical play fair cipher and the 3D play fair cipher which are as follows:

1. Extended Play fair can be considered as the greatest achievement in the monoalphbetic ciphers and in substitution techniques.

2. This is highly case sensitive and so it is hard to determine the encrypted message and we will have the proper correct message encrypted without leaving anything.

3. Classical Play fair cipher consider only 25 characters where we will make i and j as single character and in 3D play fair we use only 64 characters but in cubic play fair we will be using all the 256 characters as what we have in algorithms like AES, MD5 and so on.

4. The identification of the key matrix is very difficult when compared to previous key matrix. In the monoalphabetic cipher, the attacker searches in 26 letters only while in classical Playfair cipher an attacker has to search in 26 X 26 = 676 digraphs. But by using the 3D- Playfair cipher, the attacker has to search in 64 X 16 X 4 = 4096 trigraph [2]. But here we will be having 256 X 64 X 16 X 4 = 1048576 polygraph.

IV. SECURITY ASPECTS OF EXTENDED PLAY FAIR

Security is main aspects for any encryption algorithm while time complexity and space complexity also play roles in the selection of any cryptographic algorithms but security is the sole parameter. So some security aspects are discussed here [4].

4.1. Brute force attack

A brute force attack systematically attempts every possible key. It is most often used in a known plaintext or ciphertext only attack [4]. In our proposed system we are using 16 4 X 4 matrix for encryption and decryption purposes so we will be having 1048576 polygraph instead of 4096 trigraph from the 3D play fair cipher[2].

4.2. Frequency Analysis

It refers to the study of the frequency of each and every character depending upon their occurrence in the context. The frequency of letters in text messages has often been studied for use in cryptography, and frequency analysis in particular. An exact analysis of this is not possible, as each person writes slightly differently; however, an approximate ordering of english letters by frequency of use is ETAOIN SHRDL UCMFG YPWBV KXJQZ [5]. The probability of occurrence of the particular letter in the 3D playfair cipher techniques is 1/4*1/4*1/4= 1/64= 0.0156 [2] but where as in extended play fair cipher technique it is 1/4*1/4*1/16= 1/256= 0.00390625.

4.3. Confusion and diffusion

Confusion involves making the statistical relation between plaintext and ciphertext as complex as possible. Diffusion refers to the property that the redundancy in the statistics of the plaintext is dissipated in the statistics of the ciphertext [6]. Extended play fair cipher is most secured when compared to previous techniques on play fair. It is using 4 characters at a same time to give one character so finding the character is not that much easy task.

V. CONCLUSION

The extended Play fair cipher is the symmetric encryption technique which is using all the alphabets, numerals, special characters and also non printable characters for encryption and decryption process leads confusions to the attackers.. It is eliminating the limitation which we had in the 3D play fair like restriction to case sensitivity, special characters and then limitation of including all the ASCII character. But here we have made the approach where we can easily add all the ASCII character sets; there is no restriction of the case sensitivity also. This work will be extended to generate an efficient algorithm to enhance the network security.

REFERENCES

[1] William Stallings, Cryptography and Network Security Principles and Practices, Fourth edition.

[2] Amandeep Kaur, Harsh Kumar Verma, Ravindra Kumar Singh , "Internatinal Journal of Computer Applications", (0975 – 8887) Volume 51– No.2, August 2012 1048576 .

[3] Radix 64 Converter-http://www.oktay.de/decode/ base64.htm.

[4] Behrouz A. Forouzan, Cryptography and Network Security. Special Indian Edition, The McGraw- Hill companies, New Delhi, 2007.

[5] English Character frequency table-http://www.cryptograms.org/letter-frequencies.php.

[6] Dhiren R.Patel, Information Security Theory and Practice. First Edition, Prentice-Hall of India Private Limited, 2008.

[7] Bhowmick, Anirban, Anand Vardhan Lal, and Nitish Ranjan. "Enhanced 6x6 Playfair Cipher using Double Myszkowski Transposition." International Journal of Engineering Research and Technology. Vol. 4. No. 07, July-2015. IJERT, 2015.

[8] Negi, Ashish, et al. "Cryptography Playfair Cipher using Linear Feedback Shift Register." IOSR Journal of Engineering 2.5 (2012): 1212-1216.

[9] Kumar, Vinod, et al. "Modified Version of Playfair Cipher Using Linear Feedback Shift Register and Transpose Matrix Concept'." International Journal of Innovative Technology and Exploring Engineering (IJITEE) 3 (2013).

[10] Behrouz A. Forouzan. Cryptography and Network Security, Special Indian Edition 2007, The McGraw- Hill companies, New Delhi.

[11] Bhattacharyya, Subhajit, Nisarga Chand, and Subham Chakraborty. "A Modified Encryption Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps.

[12] Dhenakaran, S. S., and M. Ilayaraja. "Extension of Playfair Cipher using 16X16 Matrix." International Journal of Computer Applications 48.7 (2012).

[13] Basu, Sanjay, and Utpal Kumar Ray. "Modified Playfair Cipher using Rectangular Matrix." IJCA (0975-8887) Volume (2012)

[14] Alam, A. Aftab, B. Shah Khalid, and C. Muhammad Salam. "A Modified Version of Playfair Cipher Using 7? 4 Matrix." International Journal of Computer Theory and Engineering 5.4 (2013): 626.

[15] Kaur, Amandeep, Harsh Kumar Verma, and Ravindra Kumar Singh. "6 X 6 Playfair Cipher using LFSR based Unique Random Number Generator." International Journal of Computer Applications 51.2 (2012).

[16] Murali, Packirisamy, and Gandhidoss Senthilkumar. "Modified version of playfair cipher using linear feedback shift register." Information Management and Engineering, 2009. ICIME'09. International Conference on. IEEE, 2009. 6/7/2017.

