IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 7, July 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

Enhanced Play Fair Cipher

Naveen KM[1],

[1] Department of Information Technology, Velammal Engineering College,
Chennai, Tamil Nadu, India.

Abstract

The theme of this research work is to design and develop a very strong cryptographic technique, which will be used to provide security for alphanumeric characters, special characters and numbers, when we transmit over the network. This cryptographic technique, very well addresses the problems that were faced by the classical play fair and 3D Play fair techniques and overcomes the problems we faced in those techniques. Here we will consider 4 characters at a time, group them and then use them for encryption. We have a problem in the classical play fair as it uses i and j as same character. Here we eliminate this problem and we also eliminate the problem with 3D play fair which will use only certain limited character sets for encryption and that is not case sensitive. In our proposed method, we take into consideration all the 256 ASCII characters for encryption and it is also a complex algorithm when compared to previous replacement techniques.

Keywords: Enhanced Play fair.

1. *Introduction*

The best know multiple-letter encryption cipher is the Playfair, which treats diagrams in plain text as a single unit and translates it into cipher text. This cipher was invented by the 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. 3D- Play-fair cipher is a multiple letter encryption cipher, which encrypts a trigraph of plain text into its corresponding cipher text trigraph. For that purpose it requires a 4 X 4 X 4 matrix to store 26 alphabets, 10 numerals and 28 special symbols [2].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 widely used along with numerals and special characters, here we are considering 256 ASCII characters which also includes the extended ASCII values for framing the secret key word matrix and then for obtaining the encrypted messages. Here our main concern is to create an encryption algorithm which uses the substitution technique and considers all the ASCII characters for encryption and decryption.

2. Enhanced Play Fair Cipher

Enhanced play fair is a multiple-letter encryption technique based on the substitution mechanism which will consider 3 characters of plain text to convert them in corresponding cipher text of 3 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. So each small 4 X 4 matrix will have 16 character and then we have similarly 16 such matrix which all together form 256 characters. In previous play fair cipher techniques we usually had key matrix generation, encryption 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.

2.1 Algorithm with an example

Let us consider the keyword to be Passion.

STEP 1: Transform the keyword into required form.

- Exclude the repetitive letters
- Exclude the space.

Note: Both caps and small letters are accepted.

Passion → Pasion

STEP 2: Convert the resultant keyword letters into their respective hexadecimal values.

P	a	s	i	o	n
50	61	73	69	6F	6E

→50 61 73 69 6F 6E

STEP 3: Key Matrix Generation:

Table 1: key Matrix Generation

Row /col	**Col1**	**Col2**	**Col3**	**Col4**
Row 1	50 61 73 69 6F 6E 00 01 02 03 04 05 06 07 08 09	6D 70 71 72 74 75 76 77 78 79 7A 7B 7C 7D 7E 7F	A0 A1 A2 A3 A4 A5 A6 A7 A8 A9 AA AB AC AD AE AF	D0 D1 D2 D3 D4 D5 D6 D7 D8 D9 DA DB DC DD DE DF
Row 2	3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49	0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19	B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 BA BB BC BD BE BF	E0 E1 E2 E3 E4 E5 E6 E7 E8 E9 EA EB EC ED EE EF
Row 3	4A 4B 4C 4D 4E 4F 51 52 53 54 55 56 57 58 59 5A	80 81 82 83 84 85 86 87 88 89 8A 8B 8C 8D 8E 8F	1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29	F0 F1 F2 F3 F4 F5 F6 F7 F8 F9 FA FB FC FD FE FF
Row 4	5B 5C 5D 5E 5F 60 62 63 64 65 66 67 68 6A 6B 6C	90 91 92 93 94 95 96 97 98 99 9A 9B 9C 9D 9E 9F	C0 C1 C2 C3 C4 C5 C6 C7 C8 C9 CA CB CC CD CE CF	2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39

The above key matrix is a 4*4 matrix each cell in this matrix contains another 4*4 sub matrix .This will lead to 16 units in each cell which will lead to a total of 256 units. These 256 units will have a range of hexadecimal values (00-FF).

STEP 3.1: Fill the diagonals of the matrix first using the hexadecimal values of keyword first and the rest with the remaining hexadecimal values.

STEP 3.2: Followed by the diagonal boxes we have to fill the columns accordingly. Fill the hexadecimal values in the 1st row 1st column and then 2nd row 2nd column and so on (ie) diagonal wise.

STEP 3.3: Now fill the remaining hexadecimal values excluding those we have filled previously from 1st empty space in a vertical fashion, continuously from 2nd column to 3rd and from 3rd column to 4th.The matrix thus obtained will be of the form as below. It will have 4 columns and 4 rows each box of the bigger matrix will have a separate 4*4 matrix in it which consist of 4 columns and 4 rows each.

STEP 4: Plain text encryption, Let us consider the plain text :"Decide the Destiny".

STEP 4.1: Split the text into groups of three. In accordance with plain text we can include space and special characters. Repeated letters are accepted in this case. If any letter is left single or double then use filler letters x or y in order to make it three.

Dec ide _th e_D est iny
Note: Here space is denoted as '_'

STEP 4.2: Convert into hexadecimal values

D e c i d e
44 65 63 69 64 65

_ t h e _ D
20 74 68 65 20 44

e s t i n y
65 73 74 69 65 79

Thus the hexadecimal value of the plain text will be given as
44 65 63 69 64 65 20 74 68 65 20 44 65 73 74 69 6E 79

STEP 4.3 : Now we would draw a separate table for each of the three hexadecimal letters. The encryption table will be of the below form.

Table 2: Encryption Table

PLAIN TEXT	PLAIN TEXT			CIPHER TEXT
	1st letter	2nd letter	3rd letter	
1st letter	ROW	COL	MATRIX	?
2nd letter	MATRIX	ROW	COL	?
3rd letter	COL	MATRIX	ROW	?

STEP 4.4 : The cipher text in the above table is generated by the following steps.

For the cipher text of the 1st letter:

- ✓ The row in which the 1st letter is present in its own matrix is assumed as 'k'.
- ✓ The column in which the 2nd letter is present in its own matrix is assumed as 'l'.
- ✓ We should consider the matrix in which the 3rd letter is present.
- ✓ Now the letter in the kth row lth column of the 3rd matrix will be the cipher value of 1st letter.

Similarly, for all the letters the cipher values are identified.

Table 3: Encryption table for 44,65,63.

PLAIN TEXT	PLAIN TEXT			CIPHER TEXT
	44	65	63	
44	ROW	COL	MATRIX	65
65	MATRIX	ROW	COL	45
63	COL	MATRIX	ROW	62

IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 7, July 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

Table 4: Encryption table for 69, 64, 65

PLAIN TEXT	PLAIN TEXT			CIPHER TEXT
	69	64	65	
69	ROW	COL	MATRIX	5B
64	MATRIX	ROW	COL	03
65	COL	MATRIX	ROW	67

Table 5: Encryption table for 20, 74, 68

PLAIN TEXT	PLAIN TEXT			CIPHER TEXT
	20	74	68	
20	ROW	COL	MATRIX	5F
74	MATRIX	ROW	COL	1E
68	COL	MATRIX	ROW	7E

Table 6: Encryption table for 65, 20, 44

PLAIN TEXT	PLAIN TEXT			CIPHER TEXT
	65	20	44	
65	ROW	COL	MATRIX	44
20	MATRIX	ROW	COL	62
44	COL	MATRIX	ROW	23

Table 7: Encryption table for 65, 73, 74

PLAIN TEXT	PLAIN TEXT			CIPHER TEXT
	65	73	74	
65	ROW	COL	MATRIX	7A
73	MATRIX	ROW	COL	5B
74	COL	MATRIX	ROW	6E

Table 8: Encryption table for 69,6E,79

PLAIN TEXT	PLAIN TEXT			CIPHER TEXT
	69	6E	79	
69	ROW	COL	MATRIX	70
6E	MATRIX	ROW	COL	6E
79	COL	MATRIX	ROW	05

Thus the cipher text (in the form of hexadecimal values) of the plain text is obtained as

65 45 62 5B 03 67 5F 1E 7E 44 62 23 7A 5B 6E 70 6E 05

The corresponding ASCII values for those hexadecimal values are obtained and listed.

65	45	62	5B	03	67	5F	1E	7E
e	E	b	[	ETX	g	_	RS	~

44	62	23	7A	5B	6E	70	6E	05
D	b	#	z	[	n	p	n	ENQ

Thus the resultant cipher text is

eEb[ETXg_RS~Db#z[npnENQ

where,

ETX→End of text.

RS → record separator.

ENQ → enquiry are some of the available keypad functions.

STEP 5: CIPHER TEXT DECRYPTION

Let us take the obtained cipher text: "eEb[ETXg_RS~Db#z[npnENQ".

STEP 5.1: Split the cipher text into groups of three.

eEb [ETXg _RS~ Db# z[n pnENQ

where,

ETX→End of text.

RS → record separator.

ENQ → enquiry are some of the available keypad functions.

STEP 5.2: Convert into hexadecimal values

e E b [ETX g
65 45 62 5B 03 67

_ RS ~ D b #
5F 1E 7E 44 62 23

z [n p n ENQ
7A 5B 6E 70 6E 05

Thus the hexa-decimal value of the cipher text will be given as

65 45 62 5B 03 67 5F 1E 7E 44 62 23 7A 5B 6E 70 6E 05

STEP 5.3: Now we would draw a separate table for each of the hexadecimal letters. The decryption table will be of the below form.

Table 9: Decryption Table

CIPHER TEXT	CIPHER TEXT			PLAIN TEXT
	1st letter	2nd letter	3rd letter	
1st letter	ROW	MATRIX	COL	?
2nd letter	COL	ROW	MATRIX	?
3rd letter	MATRIX	COL	ROW	?

STEP 5.4 : The plain text in the above table is generated by the following steps.

For the cipher text of the 1st letter:

The row in which the 1st letter is present in its own matrix is assumed as ‘k’.

The column in which the 3rd letter is present in its own matrix is assumed as ’l’.

We should consider the matrix in which the 2nd letter is present.

Now the letter in the kth row lth column of the 2nd letter matrix will be the plain text of 1st letter.

Similarly, for all the letters the plain text values are identified.

Table 10: Decryption table for 65, 42, 62

CIPHER TEXT	CIPHER TEXT			PLAIN TEXT
	65	45	62	
65	ROW	MATRIX	COL	44
45	COL	ROW	MATRIX	65
62	MATRIX	COL	ROW	63

Table 11: Decryption table for 5B, 03, 67

CIPHER TEXT	CIPHER TEXT			PLAIN TEXT
	5B	03	67	
5B	ROW	MATRIX	COL	69
03	COL	ROW	MATRIX	64
67	MATRIX	COL	ROW	65

Table 12: Decryption table for 5F, 1E, 7E

CIPHER TEXT	CIPHER TEXT			PLAIN TEXT
	5F	1E	7E	
5F	ROW	MATRIX	COL	20
1E	COL	ROW	MATRIX	74
7E	MATRIX	COL	ROW	68

Table 13: Decryption table for 44, 62, 23

CIPHER TEXT	CIPHER TEXT			PLAIN TEXT
	44	62	23	
44	ROW	MATRIX	COL	65
62	COL	ROW	MATRIX	20
23	MATRIX	COL	ROW	44

IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 7, July 2016
ISSN (Online) 2348 – 7968 | Impact Factor (2015) - 4.332
www.ijiset.com

Table 14: Decryption table for 7A, 5B, 6E

CIPHER TEXT	CIPHER TEXT			PLAIN TEXT
	7A	5B	6E	
7A	ROW	MATRIX	COL	65
5B	COL	ROW	MATRIX	73
6E	MATRIX	COL	ROW	74

Table 15: Decryption table for 70, 6E, 05

CIPHER TEXT	CIPHER TEXT			PLAIN TEXT
	70	6E	05	
70	ROW	MATRIX	COL	69
6E	COL	ROW	MATRIX	6E
05	MATRIX	COL	ROW	79

Thus the plain text (in the form of hexadecimal values) of the cipher text is obtained as

44 65 63 69 64 65 20 74 68 65 20 44 65 73 74 69 6E 79

The corresponding ASCII values for those hexadecimal values are obtained and listed.

44 65 63 69 64 65 20 74 68
D E C I D E _ T H

65 20 44 65 73 74 69 6E 79
E _ D E S T I N Y

Note: change back the underscore (_) as space.

Thus the resultant plain text is
“Decide the destiny”.

3. Properties of enhanced Play Fair

The proposed play fair cipher has lot of advantages when compared it to the classical play fair cipher and the 3D play fair cipher, which are as follows:

1. Cubic Play fair can be considered as the greatest achievement in the mono-alphabetic 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 correct message encrypted without missing out on anything.

3. Classical Play fair cipher considers only 25 characters where we will make ‘i’ and ‘j’ as a 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 we do in the algorithms like AES, MD5.

4. Security Aspects of the enhanced Play Fair

Security is one of the main aspects for any encryption algorithm. While time complexity and space complexity also play major roles in the selection of any cryptographic algorithm, security is the sole parameter. So some security aspects are discussed below [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 cipher text-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 different; however, an approximate ordering of English letters by frequency of use is ETAOIN SHRDL UCMFG YPWBV KXJQZ [5].

The probability of occurrence of a particular letter in the 3D play fair cipher techniques is 1/4*1/4*1/4= 1/64= 0.0156 [2].
Whereas, in enhanced play fair cipher technique it is 1/3*1/3*1/16=1/144=0.00694.

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]. The enhanced play fair cipher is most secured when compared to the previous techniques on play fair. It is uses 3 characters at the same time to give one character. So finding the character is not an easy task.

5. CONCLUSION

The Enhanced Play fair cipher is the symmetric encryption technique which uses all the alphabets, numerals, special characters and also non printable characters for encryption and decryption making the users to get more confused. It is eliminates 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 characters. Here we have made the approach where we can easily add all the ASCII character sets and there is no restriction in case sensitivity also.

REFERENCES

[1] William Stallings, Cryptography and Network Security Principles and Practices, Fourth edition, Pearson 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] DhirenR.Patel, Information Security Theory and Practice. First Edition, Prentice-Hall of IndiaPrivate Limited, 2008.