International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 5, May-2014, pp: (468-473), Impact Factor: 1.252, Available online at: www.erpublications.com

3D (6 X 4 X 4) - Playfair Cipher

Nitin[1], Shubha Jain[2]
[1,2]Department of Computer Science & Engineering, Kanpur Institute of Technology, Kanpur, India

Abstract: The role of Cryptography in today's digital world is significant. It secures information mathematically by mangling message with key. The privacy of intended sender and receiver information is protected from eavesdropper. The objective of the paper is playfair cipher. The existing methods of playfair cipher are studied. The restrictions of earlier works a playfair cipher using 5X5 matrix, 7X4 matrix, 6X6 and 4 X 4 X 4 matrix are overcome in the proposed work. The proposed method plays a 6X4X4 matrix giving strength to playfair cipher. The proposed work is an enhancement to the existing algorithms that uses 4X4X4 matrix to pick cipher characters. It makes use of alphabets both lower and uppercase characters, number and special characters for constructing the contents of the matrix.

Keywords: 3D Playfair Cipher, keys, Encryption, Decryption, Plaintext, Ciphertext.

Introduction

The Playfair cipher or Playfair square is a manual symmetric encryption technique and was the first literal digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair who promoted the use of the cipher [1]. The technique encrypts pairs of letters. The cryptanalysis of the Playfair cipher is also aided by the fact that a diagram and its reverse will encrypt in a similar fashion. That is, if AB encrypts to XY, then BA will encrypt to YX. So by looking for words that begin and end in reversed diagrams, one can try to compare them with plaintext words that are similar. To eliminate this loophole this proposed cipher does work on trigraph rather than digraphs This algorithm can accept the Plaintext containing Alphabets (capital letters and small letters), Numbers and Special characters.

3D- Playfair Cipher

3D- Playfair cipher is the multiple letter encryption cipher, which encrypts a trigraph of plaintext into 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. These letters are arranged in 4 X 4 X 4 matrix based on secret key. By assuming a null key the 4 X 4 X 4 matrix will be arrange as following (Sequence of 64 characters)[1].

Table 1: Sequence of letters in 3D (4 X 4 X 4) Playfair matrix

Floor 1			
0	1	2	3
4	5	6	7
8	9	A	B
C	D	E	F

Floor 2			
G	H	I	J
K	L	M	N
O	P	Q	R
S	T	U	V

Floor 3			
W	X	Y	Z
!	"	#	$
%	&	'	(
)	*	+	,

Floor 4			
-	.	/	:
;	<	=	>
?	@	[	\
]	^	_	|

3D PLAY CIPHER (6 X 4 X 4)

3D- Playfair cipher is the multiple letter encryption cipher, which encrypts a plaintext into corresponding cipher text. For that purpose it requires a 6 X 4 X 4 matrix to store 52 alphabets (lower case and upper case), 10 numerals and 34 special symbols. These letters are arranged in 6 X 4 X 4 matrix based on two secret keys. By assuming both of keys are null than the 4X 4X6 matrix will be arrange as following (Sequence of 96 characters).

0	1	2	3
4	5	6	7
8	9	a	b
c	d	e	f

g	h	i	j
k	l	m	n
o	p	q	r
s	t	u	v

w	x	y	z
A	B	C	D
E	F	G	H
I	J	K	L

M	N	O	P
Q	R	S	T
U	V	W	X
Y	Z	?	/

`	~	!	@
#	$	%	^
&	*	(	)
_	-	+	=

{	}	[	]
:	;	‘	“
<	,	>	.
|	\	π	×

3D-Playfair cipher has mainly 3 algorithms, Keys-Matrix Generation, Encryption and Decryption. These are described below:

I. Key-Matrix Generation:

In 3D (6 X 4 X 4) - Playfair Cipher, We use 2 keys to generate (6 X 4 X 4) matrix (table). First key is a string (set of characters) for inserting the characters into matrix and second key is set of numbers which is used to insert the character of first key in right position. Sizes of both keys are same. Second key show the value of I in matrix(I X J X K).

a. insert the size of key.
b. Enter the value of first key (set of character).
c. Enter the value of second key (only numbers).
d. Insert the charters into matrix using both keys.
e. Insert k1[i] into matrix[k2[i], J, K] (no character will be repeat or repeated character do ignore after using one time).

Example- k1= {nitinCHAUHAN@1990}
K2= {02312123101023210}
Insert k1[i] into matrix[k2[i], J , K]

Insert k1[0]= n	into matrix[k2[0], J, K]=matrix[0,0,0]	matrix[0,0,0]={n}
Insert k1[1]= i	into matrix[k2[1], J, K]=matrix[2,0,0]	matrix[2,0,0]={i}
Insert k1[2]= t	into matrix[k2[2], J, K]=matrix[3,0,0]	matrix[3,0,0]={t}
Insert k1[3]= i	ignore i because it is repeat	
Insert k1[4]= n	ignore n because it is repeat	
Insert k1[5]= C	into matrix[k2[5], J, K]=matrix[1,0,0]	matrix[1,0,0]={C}
Insert k1[6]= H	into matrix[k2[6], J, K]=matrix[2,0,1]	matrix[2,0,1]={H}
Insert k1[7]= A	into matrix[k2[7], J, K]=matrix[3,0,1]	matrix[3,0,1]={A}
Insert k1[8]= U	into matrix[k2[8], J, K]=matrix[0,0,1]	matrix[0,0,1]={U}
Insert k1[9]= H	ignore H because it is repeat	
Insert k1[10]= A	ignore A because it is repeat	
Insert k1[11]= N	into matrix[k2[11], J, K]=matrix[0,0,2]	matrix[0,0,2]={N}
Insert k1[12]= @	into matrix[k2[12], J, K]=matrix[2,0,2]	matrix[0,0,0]={@}
Insert k1[13]= 1	into matrix[k2[13], J, K]=matrix[3,0,2]	matrix[3,0,2]={1}
Insert k1[14]= 9	into matrix[k2[14], J, K]=matrix[2,0,3]	matrix[2,0,3]={9}
Insert k1[15]= 9	ignore 9 because it is repeat	
Insert k1[16]= 0	into matrix[k2[16], J, K]=matrix[0,0,3]	matrix[0,0,3]={0}

n	U	N	0
2	3	4	5
6	7	8	a
b	c	d	e

C	f	g	h
j	k	l	m
o	p	q	r
s	u	v	w

i	H	@	9
x	y	z	B
D	E	F	G
I	J	K	L

t	A	1	M
O	P	Q	R
S	T	V	W
X	Y	Z	?

/	`	~	!
#	$	%	^
&	*	(	)
_	-	+	=

{	}	[	]
:	;	‘	“
<	,	>	.
|	\	π	×

II. Encryption

To encrypt a message, one would break the message into groups of 2 letters. We take 2 letters for encryption and find out the position of these letters. Then apply encryption technique on this letters.

a. Take 2 letters for encryption char1 and char2.
b. Find out the position of these letters [a, b, c] and [p, q, r] in matrix.
c. For Encrypt, the letters replace by other letters. Other letters are find out by this method-

[a, b, c] <= [(a + p) mod 6, (b + q) mod 4, (c + r) mod 4]

[p, q, r] <= [(a + p) mod 6, (b + q) mod 4, (c + r) mod 4]

char1 and char2 are replace by the element of matrix[a, b, c] and matrix[p, q, r].

2.2 Decryption

To decrypt a message, one would break the message into groups of 2 letters. We take 2 letters for decryption and find out the position of these letters. Then apply decryption technique on this letters.

a. Take 2 letters for decryption char1 and char2.
b. Find out the position of these letters [a, b, c] and [p, q, r] in matrix.
c. For decrypt, the letters replace by other letters. Other letters are find out by this method-

[p, q, r] <= [(p - a) mod 6, (q - b) mod 4, (r - c) mod 4]

[a, b, c] <= [(a - p) mod 6, (b - q) mod 4, (c - r) mod 4]

char1 and char2 are replace by the element of matrix[a, b, c] and matrix[p, q, r].

ANALYSIS OF PROPOSED METHOD

We take 2 keys for matrix generation.

k1= {nitinCHAUHAN@1990}
K2= {02312123101023210}

Where k1 and k2 are keys.

Generated matrix is:

n	U	N	0
2	3	4	5
6	7	8	A
b	c	d	E

C	f	g	h
j	k	l	m
o	p	q	r
s	u	v	w

i	H	@	9
X	y	z	B
D	E	F	G
I	J	K	L

t	A	1	M
O	P	Q	R
S	T	V	W
X	Y	Z	?

/	`	~	!
#	$	%	^
&	*	(	)
_	-	+	=

{	}	[	]
:	;	‘	“
<	,	>	.
|	\	π	×

Encryption of massage with use generated matrix-

Plaintext: kit.KANPUR

Group of letters: {ki}, {t.}, {KA}, {NP}, {UR}

Encryption –

PLAINETEXT ELEMENTS	CO-ORDINATE	ENCRYPTION METHOD		CIPHERTEXT ELEMENTS
		[a, b, c] <= [(a + p) mod 6, (b + q) mod 4, (c + r) mod 4]	[p, q, r] <= [(a + p) mod 6, (b + q) mod 4, (c + r) mod 4]	
{ki}	[1,1,1],[2,0,0]	[3,1,1]	[5,1,1]	{P;}
{t.}	[3,0,0],[5,2,3]	[2,2,3]	[1,0,2]	{Bg}
{KA}	[2,3,2],[3,0,1]	[5,3,3]	[2,3,0]	{XD}
{NP}	[0,0,2],[3,1,1]	[3,1,3]	[0,2,0]	{R6}
{UR}	[0,0,1],[3,1,3]	[3,1,0]	[0,2,3]	{Oa}

Cipher text: P;BgXDR60a

Cipher text will be transmitted to the receiver over internet. Receiver will decrypt this ciphertext using the same keys used by the sender

Encryption of massage with using matrix-

Encryption –

CIPHERTEXT ELEMENTS	CO-ORDINATE	DECRYPTION METHOD		CIPHERTEXT ELEMENTS
		[p, q, r] <= [(p - a) mod 6, (q - b) mod 4, (r - c) mod 4]	[a, b, c] <= [(a - p) mod 6, (b - q) mod 4, (c - r) mod 4]	
{P;}	[3,1,1] [5,1,1]	[2,0,0]	[1,1,1]	{ki}
{Bg}	[2,2,3] [1,0,2]	[5,2,3]	[3,0,0]	{t.}
{XD}	[5,3,3] [2,3,0]	[3,0,1]	[2,3,2]	{KA}
{R6}	[3,1,3] [0,2,0]	[3,1,1]	[0,0,2]	{NP}
{Oa}	[3,1,0] [0,2,3]	[3,1,3]	[0,0,1]	{UR}

Plaintext: kit.KANPUR

PROPERTIES OF 3D-PLAYFAIR CIPHER

3D(6×4×4)- Playfair cipher holds these properties for its strength over classical Playfair cipher-

1. 3D-Playfair cipher shows a great advancement over the alphabetic ciphers.
2. Like classical Playfair cipher, 3D-Playfair cipher is case sensitive.
3. It removes the drawback of diagram & its reverse encryption attack (Chosen Plaintext Attack). For example of plaintext "**RE**CEIV**ER**" or "**DE**PART**ED**" it is too easy to determine the actual structure of Playfair cipher. By using 3D-Playfair Cipher eliminates this security loophole of classical Playfair cipher.
4. Classical Playfair cipher supports only 25 English alphabets but 3D-Playfair cipher supports all 52 alphabets (both lower case and upper case), 10 numerals and 34 frequently used special symbols.

SECURITY ASPECTS OF CIPHER

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 [6].

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 [6].
In the proposed system we use 6 X 4 X 4 matrix for encryption and decryption purpose. So attackers will get 96 X 24 X 4 = 9216 element for brute force attack.

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 [3], [7]. In 3D-Playfair cipher 6 X 4 X 4 matrix provides better confusion ratio. As it works with trigraph so any ciphertext letter could be determined by combination of three letters, it ensures the high diffusion rate comparing to classical Playfair cipher in which combination of two letters could determines the ciphertext letter.

CONCLUSION

3D-Playfair cipher is a symmetric encryption technique which is rich enough to encrypt all alphabets, numerals and most commonly used special symbols. 6 X 4 X 4 matrix it provides high rate of confusion and diffusion rate, there is 96 X 24 X 4 = 9216 possible elements so it is too hard for applying brute force attack on it. It works on 96 characters so the probability of occurrence of a character in 3D-Playfair matrix is 1/24 * 1/4 = 1/96. After the text edit has been

completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

References

[1]. Amandeep Kaur, Harsh Kumar Verma, Ravindra Kumar Singh, Internatinal Journal of Computer Applications, August 2012.
[2]. William Stallings, Cryptography and Network Security Principles and Practice. Second edition, Pearson Education.
[3]. Schnier B, Applied cryptography: protocols, algorithms and source code in C. New York: John Wiley and sons, 1996.
[4]. Menezes AJ, Oorschot PCV, Vanstone SA, Handbook of applied cryptography. Boca Raton, Florida, USA: CRC Press; 1997.
[5]. Johannes A.Buchmann, Introduction to Cryptography. Second Edition, Springer –Verlag NY, LLC, 2001.
[6]. Behrouz A. Forouzan, Cryptography and Network Security. Special Indian Edition, The McGraw- Hill companies, New Delhi, 2007.
[7]. Dhiren R.Patel, Information Security Theory and Practice. First Edition, Prentice-Hall of India Private Limited, 2008.
[8]. Keith Harrison, Bill Munro and Tim Spiller, Security through uncertainty. P Laboratories, February, 2007.