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

Amandeep Kaur, Harsh Kumar Verma, Ravindra Kumar Singh
Department of Computer Science and Engineering
Dr. B. R. Ambedkar National Institute of Technology, Jalandhar (India)

ABSTRACT

The theme of this research is to provide security for the data that contains alphabets numerals and special characters during its transmission. However because of the drawbacks inherent in the classical Playfair cipher which adversely affects the security, this research proposed 3D-Playfair Cipher (4 X 4 X 4 Playfair cipher) which works on trigraph rather than using digraph which eliminates the fact that a diagram and its reverse will encrypt in a similar fashion. 3D-Playfair cipher supports all 26 alphabets {A-Z}, 10 digits {0-9} and 28 special characters { **! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ |** } which eliminate the limitation of classical Playfair in which "i" and "j" both character cannot appear at the same time. 3D-Playfair enhances the security by increasing complexity. Various types of cryptography attacks have been taken under consideration for original Playfair cipher but not vulnerable for this proposed cipher.

Keywords-*3D* Playfair cipher, trigraph

1. 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 (*digraphs*) [2]. 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 [3, 4]. 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.

With the assumption, the characters of the plaintext belong to the set of ASCII characters, 64 characters among ASCII character set is considered for the cipher. For choosing 64 characters among 128, it selected 26 alphabets, 10 numerals and 28 most commonly used special characters of ASCII charter set. 3D-Playfair cipher is a case insensitive cipher, so it requires only 26 alphabets (only upper case) rather than 52 alphabets (including lower and upper case both). Here, our interest is to eliminate the security loopholes and provide a cipher which is not vulnerable to any cryptanalytic attack.

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):

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

1.1 Key-Matrix Generation

3D-Playfair Cipher makes use of 4 X 4 X 4 matrix (table), which is used to store a keyword that becomes the key for encryption and decryption. Storing keyword into 4 X 4 X 4 matrix is based on some simple rules, as below.

1. Enter the secret (password) which may contain numerals, alphabets and special symbols like: aman2012nitj@gmail.com, ravindra_1987_singh@nitj.ac.in, cipher, 29101989 etc.
2. Find out the keyword by dropping the duplicate letters of key. Ex: amn201itj@g.com, ravind_1987sgh@tj.c, cipher, 29108 for above keys.
3. Arrange the keyword in 4 X 4 X 4 matrix floor by floor, row-wise: left to right and then top-to-bottom.
4. Fill the remaining spaces in the matrix with the rest of numerals (0-9), alphabets (A-Z), special symbols that were not the part of our keyword.

For the secret FRIENDS4EVER@NITJ_2012.CSE, keyword will be FRIENDS4V@TJ_201.C and Key-Matrix will be:

Table 2: 3D (4 X 4 X 4) Playfair matrix based on secret key FRIENDS4V@TJ_201.C

Floor 1			
F	R	I	E
N	D	S	4
V	@	T	J
_	2	0	1

Floor 2			
.	C	3	5
6	7	8	9
A	B	G	H
K	J	M	O

Floor 3			
P	Q	U	W
X	Y	Z	!
"	#	$	%
&	'	(	)

Floor 4			
*	+	,	-
/	:	;	<
=	>	?	[
\	]	^	|

1.2 Encryption

To encrypt a message, one would break the message into trigraph (groups of 3 letters). If any two letters are the same or only one letter is left, add two filler letter *X* and *Z* after the first letter in the trigraph. And if any two letter is left, add a filler x after the second letter. So that *BALLOON* would be treated as {BAL}, {LOX}, {ONX}, and *HELLOWORLDS* would be treated as {HEL}, {LOW}, {ORL}, {DSX} and *MASTI_M.TECH @NITJ.2012* would be treated as {MAS}, {TI_}, {M.T}, {ECH}, {@NI}, {TJ.}, {201}, {2XZ}.

A letter in the trigraph will be replaced by the letter that will lay on the same row of the letter and the column of the next letter and at the floor of next-to-next letter in circular fashion. This approach can be better understand by the following diagram

Table 3: Encryption Process of 3D (4 X 4 X 4) Playfair matrix

Plain Text Trigraph	Plain Text Trigraph			Cipher Text Trigraph
	1st Letter	2nd Letter	3rd letter	
1st Letter	Row	Column	Floor	1st Letter
2nd Letter	Floor	Row	Column	2nd Letter
3rd letter	Column	Floor	Row	3rd letter

Circular fashion means if we consider 1st letter for encryption then 2nd letter will be the next letter and 3rd letter will be the next-to-next letter and if we consider 2nd letter for encryption then 3rd letter will be the next letter and 1st letter will be the next-to-next letter and if we consider 3rd letter for encryption then 1st letter will be the next letter and 2nd letter will be the next-to-next letter.

1.3 Decryption

A letter in the trigraph will be replaced by the letter that will lay on the same row of the letter and at the floor of the next letter and the column of next-to-next letter in circular fashion. This approach can be better understand by the following diagram

Table 4: Decryption Process of 3D (4 X 4 X 4) Playfair matrix

Cipher Text Trigraph	Cipher Text Trigraph			Plain Text Trigraph
	1st Letter	2nd Letter	3rd letter	
1st Letter	Row	Floor	Column	1st Letter
2nd Letter	Column	Row	Floor	2nd Letter
3rd letter	Floor	Column	Row	3rd letter

Remove the filler letter from the trigraph (Dropping any extra X and Z that don't make sense in the final message when finished) to find out the actual text (plaintext).

2. ANALYSIS OF PROPOSED METHOD

Example of encryption for 3D- Playfair with key FRIENDS4V@TJ_201.C is:

Plaintext: M.TECH@THESIS

Trigraph: {M.T}, {ECH}, {@TH}, {ESI}, {SXZ}

Encryption- (According to Table 2)

Table 5: Encryption of M.T

Plain Text Trigraph	Plain Text Trigraph			Cipher Text Trigraph
	M	.	T	
M	Row	Column	Floor	_
.	Floor	Row	Column	3
T	Column	Floor	Row	G

Table 6: Encryption of ECH

Plain Text Trigraph	Plain Text Trigraph			Cipher Text Trigraph
	E	C	H	
E	Row	Column	Floor	C
C	Floor	Row	Column	E
H	Column	Floor	Row	H

Table 7: Encryption of @TH

Plain Text Trigraph	Plain Text Trigraph			Cipher Text Trigraph
	@	T	H	
@	Row	Column	Floor	G
T	Floor	Row	Column	J
H	Column	Floor	Row	@

Table 8: Encryption of ESI

Plain Text Trigraph	Plain Text Trigraph			Cipher Text Trigraph
	E	S	I	
E	Row	Column	Floor	I
S	Floor	Row	Column	S
I	Column	Floor	Row	E

Table 9: Encryption of SXZ

Plain Text Trigraph	Plain Text Trigraph			Cipher Text Trigraph
	S	X	Z	
S	Row	Column	Floor	X
X	Floor	Row	Column	S
Z	Column	Floor	Row	Z

Ciphertext: _3GCEHGJ@ISEXSZ

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

Decryption-(According to Table 2)

Table 10: Decryption of _3G

Cipher Text Trigraph	Cipher Text Trigraph			Plain Text Trigraph
	_	3	G	
_	Row	Floor	Column	M
3	Column	Row	Floor	.
G	Floor	Column	Row	T

Table 11: Decryption of CEH

Cipher Text Trigraph	Cipher Text Trigraph			Plain Text Trigraph
	C	E	H	
C	Row	Floor	Column	E
E	Column	Row	Floor	C
H	Floor	Column	Row	H

Table 12: Decryption of GJ@

Cipher Text Trigraph	Cipher Text Trigraph			Plain Text Trigraph
	G	J	@	
G	Row	Floor	Column	@
J	Column	Row	Floor	T
@	Floor	Column	Row	H

Table 13: Decryption of ISE

Cipher Text Trigraph	Cipher Text Trigraph			Plain Text Trigraph
	I	S	E	
I	Row	Floor	Column	E
S	Column	Row	Floor	S
E	Floor	Column	Row	I

Table 14: Decryption of XSZ

Cipher Text Trigraph	Cipher Text Trigraph			Plain Text Trigraph
	X	S	Z	
X	Row	Floor	Column	S
S	Column	Row	Floor	X
Z	Floor	Column	Row	Z

Trigraph: {M.T}, {ECH}, {@TH}, {ESI}, {SXZ}

Plaintext: M.TECH@THESIS

3. PROPERTIES OF 3D-PLAYFAIR CIPHER

3D-Playfair cipher holds these properties for its strength over classical Playfair cipher-

1. 3D-Playfair cipher shows a great advancement over the monoalphabetic ciphers.
2. Like classical Playfair cipher, 3D-Playfair cipher is not case sensitive.
3. It uses Trigraph rather than using digraph, so the length of plaintext may be even or odd. That's why it is very hard to determine the actual length of plaintext.
4. 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 Trigraph 3D-Playfair Cipher eliminates this security loophole of classical Playfair cipher.
5. Classical Playfair cipher supports only 25 English alphabets but 3D-Playfair cipher supports all 26 alphabets (including "i" and "j" both), 10 numerals and 28 frequently used special symbols.
6. The identification of trigrams is more difficult than individual letters or digraphs. 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.

4. 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 [5].

4.1Brute Force Attack

A brute force attack systematically attempts every possible key. It is most often used in a known plaintext or ciphertext-only attack [5].

In the proposed system we use 4 X 4 X 4 matrix for encryption and decryption purpose. So attackers will get 64 X 16 X 4 = 4096 trigraph for brute force attack instead of having 26*26 digrams.

4.2Frequency Analysis

Frequency analysis is the study of the frequency of letters or groups of letters in a ciphertext [6]. Frequency analysis is based on the fact that, in any given stretch of written language, certain letters and combinations of letters occur with varying frequencies. Moreover, there is a characteristic distribution of letters that is roughly the same for almost all samples of that language [7].

The probability of occurrence of any particular character in classical Playfair matrix is 1/26 = 0.0384.Whereas the probability of occurrence of a character in 3D-Playfair matrix is 1/16 * 1/4 = 1/64 = 0.0156.

4.3Confusion 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 [2], [6].

In 3D-Playfair cipher 4 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.

5. CONCLUSION

3D-Playfair cipher is a symmetric encryption technique which is rich enough to encrypt all alphabets, numerals and most commonly used special symbols. It uses trigraph rather than using digraph to eliminate the fact fact that a diagram and its reverse will encrypt in a similar fashion. This cipher is not vulnerable to security attacks, by using trigraph and 4 X 4 X 4 matrix it provides high rate of confusion and diffusion rate, there is 64 X 16 X 4 = 4096 possible trigraph so it is too hard for applying brute force attack on it. It works on 64 characters so the probability of occurrence of a character in 3D-Playfair matrix is 1/16 * 1/4 = 1/64 = 0.0156.

6. REFERENCES

[1]. William Stallings, Cryptography and Network Security Principles and Practice. Second edition, Pearson Education.

[2]. Schnier B, Applied cryptography: protocols, algorithms and source code in C. New York: John Wiley and sons, 1996.

[3]. Menezes AJ, Oorschot PCV, Vanstone SA, Handbook of applied cryptography. Boca Raton, Florida, USA: CRC Press; 1997.

[4]. Johannes A.Buchmann, Introduction to Cryptography. Second Edition, Springer –Verlag NY, LLC, 2001.

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

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

[7]. Keith Harrison, Bill Munro and Tim Spiller, Security through uncertainty. *P* Laboratories, February, 2007.