3D - Playfair Cipher with Message Integrity using MD5

Alok Kumar Chaturvedi
CSE Department, LNCT College Bhopal

Vikram Rajput
CSE Department, LNCT College Bhopal

Vineet Richarya
CSE Department, LNCT College Bhopal

ABSTRACT
In growing digital world, Cryptography plays an important role to secure confidential information. The objective of the paper is to implement encryption and message digest of information. 3D (6X4X4) - Playfair cipher is multiple letter encryption cipher. In this, tri-graphs of plaintext are treated as single units and converted into corresponding cipher text tri-graphs. 3D (6X4X4) -Playfair cipher supports all 52 alphabets (upper and lower case), 10 digits and 34 special characters. The theme of research is to furnish security to data which contains alphabets numerals and special characters during transmission that's why message-digest algorithm are introduced and applied on the cipher text of 3D-Playfair cipher with a random key. 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, Encryption, Decryption, Classical Playfair, Plain Text, Ciphertext, Trigraph, Message-digest algorithm (MD5).

1. INTRODUCTION
This paper based on two steps securing the message first the plaintext encryption using 3D- Playfair algorithm and generate cipher text. In the second step you create digital signature again cipher text using MD5 algorithm for integrity of the message during transmission.

Message digests are designed to protect the integrity of a piece of data or media to detect changes and alterations to any part of a message. MD5 message-digest algorithm takes as input a message of arbitrary length and produces as output a 128-bit "fingerprint" or "message digest" of the input. They are a type of cryptography utilizing hash values that can notify the copyright owner of any modifications applied to their work. [4][5]

This algorithm can accept the plaintext containing Alphabets (Capital and small letters), Numbers and special symbols.

To understand distinctly you divided model in to two viewpoints Encryption at sender side and Decryption at receiving end.

2. LITERATURE SURVEY
2.1 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 is based on three algorithms, Key matrix generation, Encryption on the sender side and Decryption at the receiving end.[1][2][3]

Key Matrix Generation:

3D Playfair cipher store key in to 4X4X4 matrix that is used to Encrypt plain text into cipher text and decrypt cipher text into plain. Keyword storing in table is based on some simple rule are as follows:

- Enter the secret key which is combination of numerals, alphabets and special symbols like: alok.chaturvedi04@gmail.com, chaturvedi_mtech@2014lnct.
- Extract final keyword by removing the duplicate letters of key. Ex: alok.chturvedi04@gm, chaturvedi_m@2014ln.
- Arrange the keyword in 4 X 4 X 4 matrix floor by floor, row-wise: left to right and then top-to-bottom.
- 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 keyword.

For the secret CHATURVEDI_MTECH@2014LNCT, keyword will be CHATURVEDI_M@2014LN and Key-Matrix will be:

Table 2: Sequence of letter

Floor 1			
C	H	A	T
U	R	V	E

Floor 2			
4	L	N	3
5	6	7	8

D	I	_	M
@	2	0	1

9	B	F	G
J	K	O	P

Floor 3			
Q	S	W	X
Y	Z	!	“
#	$	%	&
‘	(	)	*

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

Encryption and Decryption

To encryption first you have to divide message into group of 3-3 letter. If last pair is having only one or two letter then add filler X,Z or X to complete trigraph.

Encryption and decryption are performed with the help of table as follows:

Table 3: Encryption table

Plain text	Plain text			Cipher text
	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

Table 4: Decryption table

Cipher text	Cipher text			Plain text
	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

Example of encryption for 3D Playfair with

Key: CHATURVEDI_M@2014LN is:

*Plaintext:*M.TECH@THESIS

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

Cipher text: [T1 RTC 2CT ZTI SS”

Limitations

1. 3D (4X4X4) method is case insensitive.
2. Message integrity are not involve in this concept

2.2 Message Digest Algorithm (Md5)

MD5 message-digest algorithm takes as input a message of random length and produces as output a 128-bit "message digest" of the input. It is assumed that it is computationally speculative to produce two messages having the same message digest, or to create any message having a given pre-specified target message digest. The MD5algorithm is used for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key. [6][7]

MD5 is an algorithm that is used to verify data reliability through the formation of a 128-bit message digest from data input that is claimed to be as inimitable to that specific data as a fingerprint is to the specific individual. MD5, which was developed by Professor Ronald L. Rivest of MIT, is planned for use with digital signature applications, which require that large files must be compacted by a secure method before being encrypted with a secret key, under a public key cryptosystem. MD5 is currently a standard, Internet Engineering Task Force (IETF) Request for Comments (RFC) 1321. According to the standard, it is "computationally infeasible" that any two data that have been input to the MD5 algorithm could have as the output the same message digest, or that a false message could be created through anxiety of the message digest. MD5 is the third message digest algorithm created by Rivest. All three (the others are MD2 and MD4) have similar structures, but MD2 was optimized for 8-bit machines, in contrast with the two later formulas, which are enhance for 32-bit machines. The MD5 algorithm is an expansion of MD4, which the decisive review found to be fast, but possibly not completely secure. In comparison, MD5 is not quite as fast as the MD4 algorithm, but offers much more assurance of data security. [1][6][7]

Using an MD5 checksum you can do exactly that- verify the integrity of data. This can be used in a number of different situations and in any number of different ways, but it is a simple and effective way to verify large amounts of data.

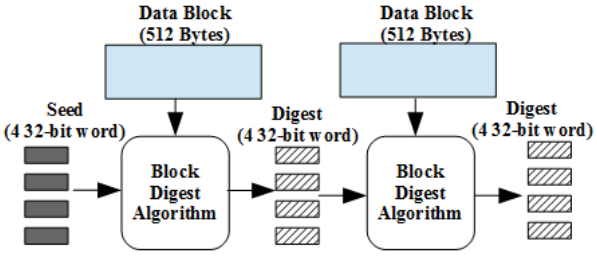

Fig. 1 MD5

The goal of this would be to identify data which needs to be backed up, and then create a MD5 checksum. With this done the data can be copied into place and the MD5 checksum can be reviewed so as to verify the data was copied without incident. Now the data is verified and redundant so you know that you have a safe backup of it.[6][7]

Many older techniques that based on 16 or 32 bit *cyclical redundancy codes* (CRC) to verify correct transmission in data communication protocols, but these short codes of MD5, while sufficient to detect the kind of transmission errors for which they were intended, are insufficiently secure for applications such as electronic commerce and verification of security related software distributions.

Limitation:

1. Message digest is one way encryption algorithm.
2. Authentication technique are not applicable in MD5

3. PRAPOSED METHOD

In modern networking world there is one new approach to securing your date from intruders. That model shows how to wrap up information in single unit which overcome to limitation of simple 3D playfair and Message digest algorithm.

A. Encryption at sender side

That will work in following steps;

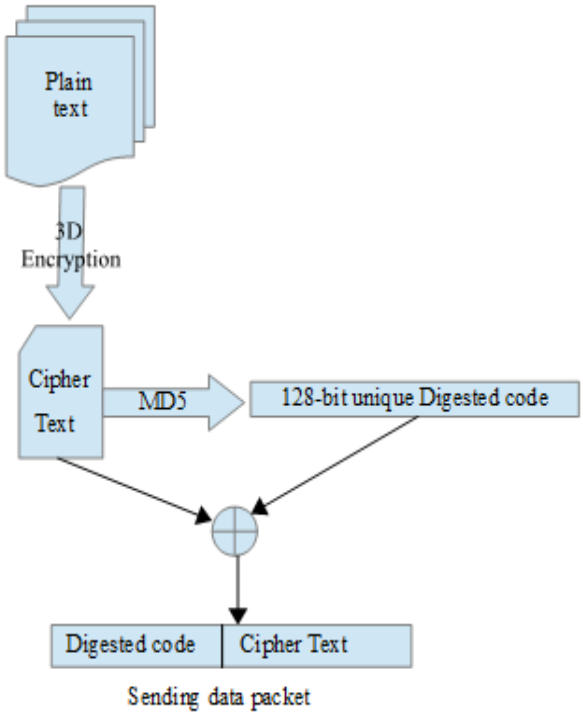

Fig. 2. Flow chart at sender side

1. Encrypt plaintext using 3D (6X4X4) Playfair algorithm.[1][2][3]. 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 6 X 4 X 4 matrix to store 52 alphabets (lower and upper case), 10 numerals and 34 special symbols. These letters are arranged in 6 X 4 X 4 matrix based on secret key. By assuming a null key the 6 X 4 X 4 matrix will be arrange as following (Sequence of 96 characters):
   - Selecting key which is combination of alphabets in upper and lower cases, some numeric value and special characters
   - Removing repeating characters from key.
   - Entering key in existing matrix (Table 3) and form key matrix.
   - Convert plain text with the help of encryption table

Table 5: Sequence of letter in base matrix

Floor 1			
0	1	2	3
4	5	6	7

Floor 2			
g	h	i	j
k	l	m	n

8	9	a	b
c	d	e	f

o	p	q	r
s	t	u	v

Floor 3			
w	x	y	z
A	B	C	D
E	F	G	H
I	J	K	L

Floor 4			
M	N	O	P
Q	R	S	T
U	V	W	X
Y	Z	!	“

Floor 5			
#	$	%	&
‘	(	)	*
+	,	-	.
/	:	;	<

Floor 6			
=	>	?	@
[	]	^	_
|	`	~	{
}	\	á	Ù

1. Digest of cipher text adopting MD5 to generate 128-bit digested code.[6][7]

- *Append padding bits*:

The message is "padded" so that its length is to 448, modulo 512. That is, the message is extended so that it is just 64 bits cloistered of being a multiple of 512 bits long.

- *Append length*:

A 64-bit representation of b (the length of the original message before the padding bits were added) is added to the result of the earlier step. In the unlikely event where b is greater than 2^{64}, then only the low-order 64 bits of b are used. (These bits are added as two 32-bit words and added low-order word first in accordance with the earlier conventions.)

At this point of time the resulting message (after padding with bits and with b - original message) has a length that is an exact multiple of 512 bits. At the same time,length of this message is an exact multiple of 16 (32-bit)words. Let M[0 N-1] denote the words of the resulting message, where N is a multiple of 16.

- *Initialize MD Buffer*:

algorithm perform on a 128-bit state, split into four 32-bit words, designate A, B, C, and D. These are initialized to certain fixed constants

- *Process Message in 16-Word Blocks*:

The main algorithm then uses each 512-bit message block in turn to change the state. The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations based on a non-linear function F, modular addition, and left rotation. Figure 1 illustrates one operation within a round. There are four possible functions F; a different one is used in each round:

$$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$$

$$G(B,C,D) = (B \wedge D) \vee (\mathrm{C} \wedge \neg D)$$

$$H(B,C,D) = B \oplus C \oplus D$$

$$I(B,C,D) = C \oplus (B \vee \neg \mathrm{D})$$

⊕, ∧, ∨, ¬ represent the XOR, AND, OR and NOT operations respectively.

- Output

2. Forming data packet which contains both digested code and encryption message as shown in fig.2.

B. Decryption at Receiving End

Data packet will be transmitted to the receiver over internet. Message will decrypt in following steps :

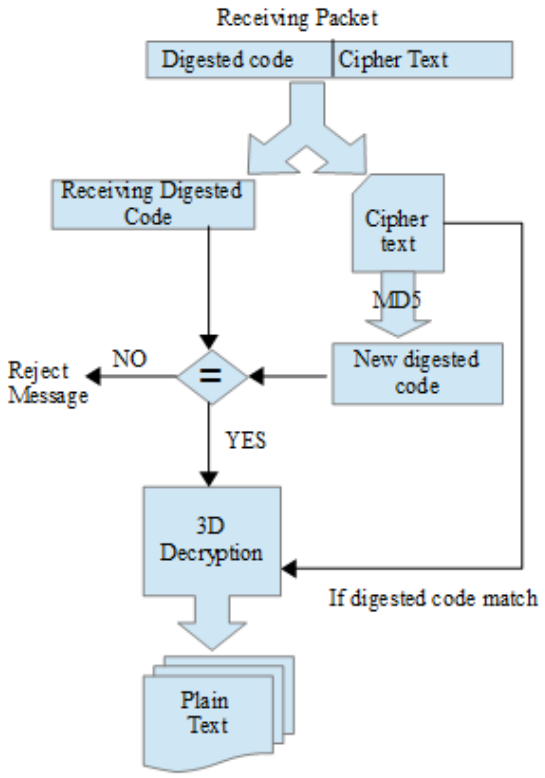

Fig.3. Flow chart at Receiver End

- Receiver will separate cipher text and digest message.
- Receiver also generates MD5 checksum of cipher text.
- Compare with received digested code to the new generated MD5 checksum
- If both digested code matches then decrypt this cipher text using the same key used by the sender and decryption table
- Otherwise send error message to sender.

4. WORKING EXAMPLE

A. Sender side

Playfair encryption starts from generating key matrix from existing base matrix as table 3. Selecting key is combination of alphabet, special symbol and number. Removing repeated character before entering in matrix.

For the secret MTech_CHATURVEDI@2014LNCT, keyword will be MTech_CHAURVEDI@2014LN and Key-Matrix will be:

Table 6: Sequence of letter in Key matrix

Floor 1			
M	T	e	c
h	_	C	H
A	U	R	V
E	D	I	@

Floor 2			
2	0	1	4
L	N	3	5
6	7	8	9
a	b	d	f

Floor 3			
g	i	j	k
l	m	n	o
p	q	r	s
t	u	v	w

Floor 4			
x	y	z	B
F	G	J	K
O	P	Q	S
W	X	Y	Z

Floor 5			
!	“	#	$
%	&	‘	(
)	*	+	,
-	.	/	:

Floor 6			
;	<	=	>
?	[	]	^
|	`	~	{
}	\	á	Ù

To encryption first you have to divide message into group of 3-3 letter. If last pair is having only one or two letter then add filler X,Z or X to complete trigraph.

Example of encryption for 3D Playfair with

Plaintext: alok.MTECH@THESIS

Trigraph :{alo}, {k.M}, {TEC}, {H@T}, {HES}, {ISX}

Encryption- (According to Table 3)

Encryption of **alo**

Plain text	Plain text			Cipher text
	a	l	o	
a	Row	Column	Floor	t
l	Floor	Row	Column	5
o	Column	Floor	Row	l

Encryption of **k.M**

Plain text	Plain text			Cipher text
	k	.	M	
k	Row	Column	Floor	T
.	Floor	Row	Column	t
M	Column	Floor	Row	$

Encryption of **TEC**

Plain text	Plain text			Cipher text
	T	E	C	
T	Row	Column	Floor	M
E	Floor	Row	Column	I
C	Column	Floor	Row	_

Encryption of **H@T**

Plain text	Plain text			Cipher text
	H	@	T	
H	Row	Column	Floor	H
@	Floor	Row	Column	D
T	Column	Floor	Row	c

Encryption of **HES**

Plain text	Plain text			Cipher text
	H	E	S	
H	Row	Column	Floor	F
E	Floor	Row	Column	@
S	Column	Floor	Row	V

Encryption of **ISX**

Plain text	Plain text			Cipher text
	I	S	X	
I	Row	Column	Floor	Ù
S	Floor	Row	Column	U
X	Column	Floor	Row	J

Cipher text: t5lTt$MI_HDcF@V ÙUJ

MD5 Checksum of cipher text:

3b60e2aeed11a34f1918338fc9199a2e

Cipher text append with MD5 checksum make data packet that has to be sent

Sending data:

3b60e2aeed11a34f1918338fc9199a2et5lTt$MI_HDcF@VÙUJ

A. Receiving Side :

Receiving data:

3b60e2aeed11a34f1918338fc9199a2et5lTt$MI_HDcF@VÙUJ

Receiving digested code:

3b60e2aeed11a34f1918338fc9199a2e

Cipher text: t5lTt$MI_HDcF@V ÙUJ

Decryption of **t5l**

Cipher text	Cipher text			Plain text
	t	5	l	
t	Row	Floor	Column	a
5	Column	Row	Floor	l
l	Floor	Column	Row	o

Decryption of **Tt$**

Cipher text	Cipher text			Plain text
	T	t	$	
T	Row	Floor	Column	k
t	Column	Row	Floor	.
$	Floor	Column	Row	M

Decryption of **MI_**

Cipher text	Cipher text			Plain text
	M	I	_	
M	Row	Floor	Column	T
I	Column	Row	Floor	E
_	Floor	Column	Row	C

Decryption of **HDc**

Cipher text	Cipher text			Plain text
	H	D	c	
H	Row	Floor	Column	H
D	Column	Row	Floor	@
c	Floor	Column	Row	T

Decryption of **F@V**

Cipher text	Cipher text			Plain text
	F	@	V	
F	Row	Floor	Column	H
@	Column	Row	Floor	I
V	Floor	Column	Row	S

Decryption of **ÙUJ**

Cipher text	Cipher text			Plain text
	Ù	U	J	
Ù	Row	Floor	Column	I
U	Column	Row	Floor	S
J	Floor	Column	Row	X

Plaintext: alok.MTECH@THESIS

5. PROPERTIES

3D (6X4X4) - Playfair Cipher with Message Integrity using MD5 holds below properties for its strength over simple 3D Playfair cipher:

1. Simple 3D Playfair cipher is case sensitive whereas 3D (6X4X4)-Playfair cipher supports all 52 alphabets (upper and lower case), 10 digits and 34 special characters. Whereas simple 3D playfair support 26 alphabets, 10 numerals and 28 special symbols.
2. In the simple 3D-Playfair cipher, the attacker has to search in 64 X 16 X 4 = 4096 trigraph. Whereas in new algorithm the search would be in 96 X 16 X 6 = 9216 trigraph.
3. 3D playfair along with MD5 secures integrity of the message over network transmission. Whereas simple 3D playfair are not providing this feature.

6. CRYPTANALYSIS

- *Brute Force Attack:*

Brute force is a trial and error method used by application programs to decode encrypted information. [15][16]

In the proposed system you use 6 X 4 X 4 matrix for encryption and decryption purpose. So attackers will get 96 X 16 X 6 = 9216 trigraph for brute force attack.

- *Frequency Analysis:*

Frequency analysis is the study of the frequency of letters or groups of letters in a ciphertext.[15][16]

Frequency analysis is based on, that how frequently certain letters and pattern of letter occur frequently in any given written language. The probability of occurrence of a character in 3D-Playfair matrix is 1/16 * 1/4 = 1/64 = 0.0156. Whereas the probability of occurrence of a character in proposed method is 1/16 * 1/6 = 1/64 = 0.01041.

- *Confusion and diffusion:*

Confusion means that the key does not narrate in a simple way to the ciphertext. In particular, each character of the ciphertext should depend on several parts of the key. Diffusion means that if you alter a character of the plaintext, then numerous characters of the ciphertext should change, and similarly, if you modify a character of the ciphertext, then some characters of the plaintext should change.[15][16]

- *Integrity*:

Integrity means information must not be changed and to ensure that you take a step so that data cannot be altered by unauthorized people.

In this method you apply 3D playfair and MD5.Message digested method check purity of the data whereas simple 3D playfair cipher are not concern about message integrity.

7. CONCLUSION

The proposed technique increases the security which is examined by different cryptanalysis techniques such as brute force attack, frequency analysis, confusion-diffusion etc. And the technique proved to be not vulnerable against these attacks.

This cipher is not susceptible to security attacks, by using trigraph and 6 X 4 X 4 matrix it provides high rate of confusion and diffusion, there is 96 X 16 X 4 = 9216 possible trigraph 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 this method is 1/16 * 1/6 = 1/96 = 0.0104.

Hence here you can conclude proposed method is a significant improvement over 3-D playfair cipher and can be used in applications where resources like bandwidth and memory are limited.

8. REFERENCES

[1] 3D - Playfair cipher with additional bitwise operation Amandeep Kaur, Harsh Kumar Verma and Ravindra Kumar Singh Control Computing Communication & Materials (ICCCCM), 2013 International Conference on Year: 2013

[2] 3D (6 X 4 X 4) - Playfair Cipher Nitin, Shubha Jain Department of Computer Science & Engineering, Kanpur Institute of Technology, Kanpur, India Year: 2014

[3] Amandeep Kaur, Harsh Kumar Verma and Ravindra Kumar Singh. Article: 3D (4 X 4 X 4) - Playfair Cipher. International Journal of Computer Applications 51(2):36-38, August 2012.

[4] Rivest, R., "The MD5 Message-Digest Algorithm," RFC-1321, MIT LCS and RSA Data Security, Inc., April 1992.

[5] Ming Hu, Yan Wang, "MD5-Based Error Detection", Circuits, Communications and Systems, 2009. PACCS '09. Pacific-Asia Conference on Year: 2009

[6] Schneier B, 1994. The blowfish encryption algorithm. Dr. Dobbs J., 19: 38-40

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

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

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

[10] P. Murali, and G. Senthilkumar, Modified version of Playfair Cipher using linear feedback shift register, International Journal of Computer Science and Network Security, vol. 8, no. 12, 2008.

[11] S. S. Srivastava, N. Gupta and R.jaiswal"Modified Version of Playfair Cipher by using 8x8 Matrixand Random Number Generation" in Proceedings of IEEE3rd International Conference on Computer Modeling andSimulation (ICCMS 2011), Mumbai, pages 615-617,January, 2011.

[12] V.U.K. Sastry, N. Ravi Shankar and S. DurgaBhavan" *A Blending of A Generalized Playfair Cipher and A Modified Hill Cipher*",2011.

[13] B. Schnier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed., John Wiley and Sons, 1996.

[14] E. Biham and A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard," Springer Verlag, 1993. ISBN 0-387-97930-1.

[15] W. Stallings, Cryptography and Network Security Principles and Practice. Second edition, Pearson Education.

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