International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 2 ǁ 2022 ǁ PP. 21-24

Survey on 3D-Playfair Encrypted Message Verification Technology based on MD5

Shalvi Bhambure, Prof. Sagar Mane
Computer Department, NBN Sinhgad School of Engineering Pune

Abstract— *Now a days the transmission of information has become much more convenient for everyone, but the risk of data being attacked,*
stolen and tampered encourages to build highly data security algorithms and methods. However, for maintaining one of the pillars of CIA triad i.e., integrity Alok et al. author of this paper proposed 3D-Playfair Cipher with Message Integrity using MD5. This review paper uses 3D-Playfair encryption for the encryption purpose.
Basically, simple 3D-playfair encryption cannot guarantee the integrity of data during transmission, so in this paper the author proposes combination of 3D-playfair with MD5 to ensure the integrity of the data. But still there are doubts about the credibility of the data source, so author uses XOR calculation methods for further verification of credibility of the data.
Key words: *3D Playfair, MD5, XOR*

Date of Submission: 02-02-2022 Date of acceptance: 16-02-2022

I. INTRODUCTION

This technology includes three steps-
In the first step, original message is converted into 3D Playfair Cipher. 3D Playfair has size 4X4X4 and contains 64 characters containing 26 letters, 10 digits and 28 special symbols.
In the second step, on cipher code MD5 algorithm is applied and the combined summary code is sent to receiver; receiver first separates plane message from source and compare it with summary code by applying MD5 on it.
In third step, to ensure correctness and integrity of sent message XOR of 3D Playfair and MD5 and this verification code sent to receiver to achieve verification of source code.

II. MANUSCRIPTS

A. 3D Playfair cipher

3D Playfair cipher is a multiletter cipher which accepts 3 letters plain text and encrypts it into 3 letters password. 3D-playfair has size 4X4X4 as it contains 4 floors containing each of it contains 4 rows and 4 columns. 64 characters are arranged on four floors in manner of 10 digits, 26 letters and 28 special symbols respectively.
Sequence of characters in basic matrix is as follows-

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 contains three stages-
1. key matrix creation
2. message encryption

3. message decryption

1.Key Matrix Creation
For key matrix generation, while entering characters in matrix duplicate characters in input key must be omitted. Hence to get final key characters should written in table in top to bottom arrangement from left to right.
Example
Key - WXYZ@YMAIL.COM

Floor 1			
W	X	Y	Z
@	M	A	I
L	.	C	O
0	1	2	3

Floor 2			
4	5	6	7
8	9	B	D
E	F	G	H
J	K	N	P

Floor 3			
Q	R	S	T
U	V	!	“
#	$	%	&
	(	)	*

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

For message encryption, plaintext message is divided in set of groups of three characters. If any group contains only two or one character then it contains X or XY as replacement characters respectively.

2.Message Encryption
To encrypt message following table method is used

Three-Letter Set In Plaintext	Three-Letter Set In Plaintext			Three-Letter Set In Cipher
	First Letter	Second Letter	Third Letter	
First Letter	Row	Column	Floor	First Letter
Second Letter	Floor	Row	Column	Second Letter
Third Letter	Column	Floor	Row	Third Letter

If plaintext message is PASSWORD, then it converted into set of three characters as {PAS}{SWO}{RDX}. As third group contains only two letters third letter get replaced by X.

3.Message Decryption
For message decryption, following table method is used

Three-Letter Set In Cipher	Three-Letter Set In Cipher			Three-Letter Set In Plaintext
	First Letter	Second Letter	Third Letter	
First Letter	Row	Floor	Column	First Letter
Second Letter	Column	Row	Floor	Second Letter
Third Letter	Floor	Column	Row	Third Letter

B. Message Digest Algorithm 5(MD5)
MD5 is a message digest algorithm which takes input of any length and convert it into 128-bit hash code. MD5 algorithm is a cryptographic algorithm which has following properties-
1) Irreversibility- From digest code one cannot get original message.
2) Same message there will have same hash code for all the time.
3) Two different messages would not have same hash code.

MD5 algorithm have following stages-
1. Append padding bits
2. Append length bits
3. Initialize MD buffer
4. Process for each 512-bit block
5. Getting digested message

1.Append padding bits
In this, padding bits are added to original message so that total number of bits must be 64-bit less than any exact multiple of 512.

2.Append length bits
In this, length bits are added to original message using mod 2^{64} to original message. Hence exact 512-bit message created by adding padding bits and length bits.

3.Initialize MD Buffer
For initializing MD Buffer 512-bit created message is divided into N multiple 512-bit blocks; each block contains 4 buffers A, B, C and D of size 32 bits.
each has standard names A – 01234567
B – 89abcdef
C – fedcba98
D – 76543210
Each 512-bit block contains 4 rounds. Every round has one compression function and 16 operations are applied in one round.
Compression functions of MD5 algorithm is as follows

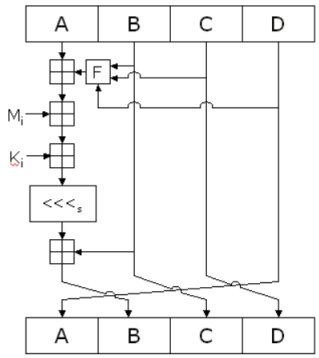
$$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D) \quad (1)$$

$$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D) \quad (2)$$

$$H(B,C,D) = B \oplus C \oplus D \quad (3)$$

$$I(B,C,D) = C \oplus (B \vee \neg D) \quad (4)$$

4.Process for each 512-bit block



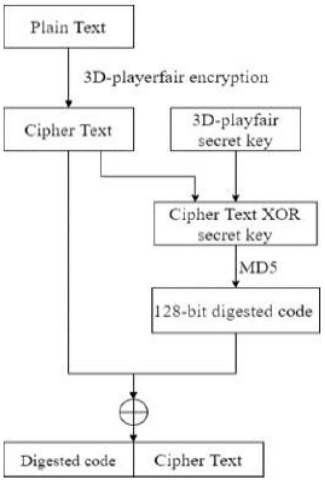
This algorithm fetches input from B, C, D buffer and passes it to C, D, A respectively. Input in buffer A is added to output of corresponding compression function(which uses inputs in buffer B, C, D). Further original message input M_i added it; Later, constant value K_i are added to achieved output. By left shifting of orininal bits by s will give desire output for first round.

5.Getting digested output
By repeating above same procesure for all rounds and for all 512-bit blocks till the last N block, this algorithm will give digested code as a output.

C. Message integrity over 3D Playfair cipher using MD5

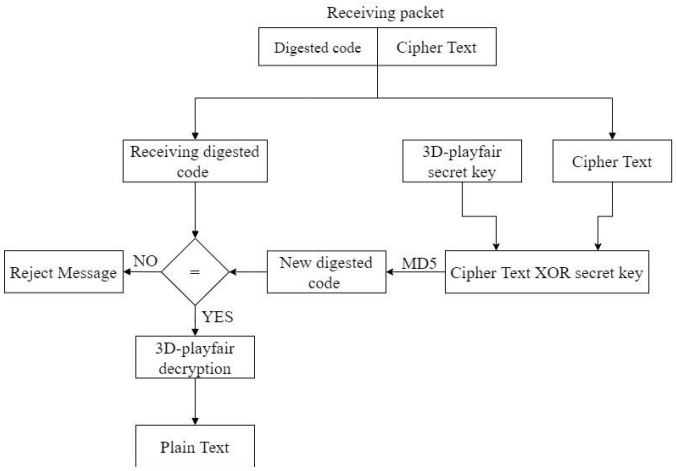
Before this technology, for message encryption 3D Playfair secret key would not get used. So, there were more chances that cipher text get tampered and send incorrect data to the receiver.
To achieve integrity, in this technology 3D Playfair secret key is used to generate verification code.

Sender end
At receiver end for message encryption; plain text is converted to the cipher text using 3D Playfair encryption. Cipher text get XOR with 3D Playfair secret key, MD5 algorithm is applied on its output. Further 128-bit digested code get XOR with cipher text and this packet sent to receiver end.



Receiver end

At receiver end digested code is considered as validation code. After receiving packet of data digested code and cipher code get separated. Again, XOR operation applied on cipher text and 3D Playfair secrete key. After applying MD5 on it if new digested code equals to received digested code that is validation code, then cipher code gets decrypted to get plain text else rejection message sent to receiver.



CONCLUSION

XOR computation of 3D Playfair key with cipher gives verify source data and application of MD5 algorithm verifies integrity of data. This technology verifies whether transmitted data is tampered or not and gives guarantee about integrity of transmitted data.

References

[1]. Alok Kumar Chaturvedi, Vikram Rajput, Vineet Richarya,"3DPlayfair Cipher with Message Integrity using MD5," International Journal of Computer Applications Vol. 148, No. 9, pp.6-12, August

[2]. Amandeep Kaur, Harsh Kumar Verma, Ravindra Kumar Singh,"3D(4X4X4)-Playfair Cipher," International Journal of Computer Applications Vol. 51, No. 2, pp.36-38, August 2012.

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

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

[5]. MD5 https://www.itread01.com/content/1548845464.html