Implementation of Modified Playfair CBC Algorithm

Priyanka Goyal
Dept. of Computer Science & Engineering
ITM Group of Institutions
Gwalior, India

Gaurav Sharma
Dept. of Computer Science & Engineering
ITM Group of Institutions
Gwalior, India

Shivpratap Singh Kushwah
Dept. of Computer Science & Engineering
ITM Group of Institutions
Gwalior, India

***Abstract*—These days, Information Security is the most summon aspects in the web and network application due to their swiftly origination. Therefore, secure exchanged data over the internet is vital. In this context, cryptography is used that converts information from its normal form into an unreadable form by using encryption techniques. This paper deals with a new solution approach to overcome the shortcomings of the Playfair algorithm. In this paper, the presented PlayfairCBC encryption mechanism makes the cryptanalysis complex. The encrypted text obtained is almost unreadable. The proposed PlayfairCBC algorithm is implemented and number of tests is performed to prove its efficiency. Finally, it has been analyzed on the basis of avalanche effect.**

Keywords—Avalanche; Brute force; CBC; Cipher; Cryptanalysis; Encryption; Playfair

I. INTRODUCTION

Cryptography word comes from Greek which means “secret writing” [1]. It refers to the science and art of transforming messages in such a way that makes it secure and immune to attacks. Its fundamental objective is to allow two individuals to communicate in such a way that an adversary cannot understand what is being communicated. It is the study of mathematical techniques associated with information security. To achieve the security goals, cryptography involves three distinct mechanisms: symmetric key cryptosystem (sometimes called symmetric key cryptography, secret key cryptography or private key cryptography), asymmetric key cryptosystem (sometimes called asymmetric key cryptography or public key cryptography) and hash functions. Cryptology is the science of cryptography and cryptanalysis. Cryptanalysis, “code breaking”, is the science of attacking cryptographic systems and gain access to the entire data of encrypted messages, also when the cryptographic key is unknown.

II. LITERATURE SURVEY

In this section, we will discuss existing modified Playfair ciphers. Basu and Ray [2] proposed their modified 10 x 9 matrix playfair cipher which contains almost all the printable characters i.e. uppercase and lowercase alphabets, numbers, punctuation marks and special characters. In the variation projected by Packirisamy Murali and Gandhidoss Senthilkumar [3], the authors propose new rules which has numerous benefits as compare to traditional Playfair cipher. In the variation projected by Man et al. [4] and in the variation projected by Srivastava and Gupta [5], the 5*5 matrix has been replaced by 8*8 matrix. Srivastava et al. [6] thought of diagrams within the plaintext as single. Totally different variety of cipher attacks and non-vulnerability of recent cipher has been mentioned. A few contributions were also noticeable [7-11].

A Framework based on Probability analysis of Character occurrence [12] is anew approach which keeps track of the frequency of occurrences of each and every character in English language and substitutes the every next occurrence of the character with a character of least frequency of use. It the new word becomes a meaning word replace with the next character of least frequency. The modified algorithm is efficient than the original Playfair and can handle spaces, repetitive characters more efficiently but still lacks in the number of supported character set.

A DNA and Amino Acid-Based Implementation [13] modifies the Playfair cipher significantly by introducing DNA-based amino acid structures to the core of the ciphering process. The proposed work treats the plaintext as a binary stream. Each and every pair of bits of the binary stream is replaced with either A, C, G or T, which are the abbreviated forms of the four bases of DNA namely- Adenine, Cytosine, Guanine and Thymine respectively. The proposed algorithm is quite time consuming because of its lengthy procedure and requirement of multiple read / write operations. Additionally 8-bit ASCII is converted to codons or triplets of bit-pairs, so remaining offsets are to be taken care of. The proposed modification actually treats the plaintext file as binary data stream and thus enriches the character set and actually solves the problem of limited character support.

A. Lahiri [14] also proposed binary Playfair algorithm. It uses a reduced 4×4 key matrix to encrypt each bytes of the plaintext file. Moreover, Salman Khan [15] surveyed and analyzed numerous Playfair ciphers with different matrix sizes. These matrices are 9 x 9, 10 x 10, and 11 x 11. Kumar and Rana [16] propose 6X6 Polybius square which includes both the alphabets and numbers leads to secured communication. Further, Kumar et al. [17] proposes a 10X10 hybrid Polybius and Playfair cipher to hold the 95 printable characters of ASCII character set. Blum-Blum Shub generator is used to generate key matrix.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 06, June-2016

III. PROPOSED PLAYFAIRCBC ALGORITHM

In Playfair cipher, the alphabets are arranged in a key matrix of size 5*5 based on secret key. In our proposed PlayfairCBC algorithm, we can implement any matrix size. As its name suggests, our proposed algorithm uses output in a chain to construct the key matrix. Its overall architecture is as follows:

To fill-in the key matrix table, the alphabets of the keyword (dropping any duplicate letters) are placed in serial order and the leftover spaces are filled with the remaining letters of the alphabet in a well ordered manner.

A. Encryption

To encrypt a message, the message is broken into digraphs (groups of 2 letters) and then mapped them out on the key table. Then following protocols are employed to each matching set of letters in the plaintext:

1. When both alphabets lie on the identical (and pair is left with one letter only), add an "X" after the first letter then encrypt the recently developed pair and proceed with.
2. When the alphabets repose on the same row of the table, they are to be interchanged with the letters immediate right of them respectively.
3. When the alphabets repose on the same column of the table, they are to be interchanged with the letters just below them respectively.
4. When the alphabets repose not on the same row or column, exchange them with the letters on the identical row respectively but of the column of the other keeping the order of the matching set unflawed.
5. After encryption of the first digraph,pick the output and reorganize the key matrix which will be utilized to encrypt another digraph.
6. Take another diagraph and redo the steps from 1 to 5.

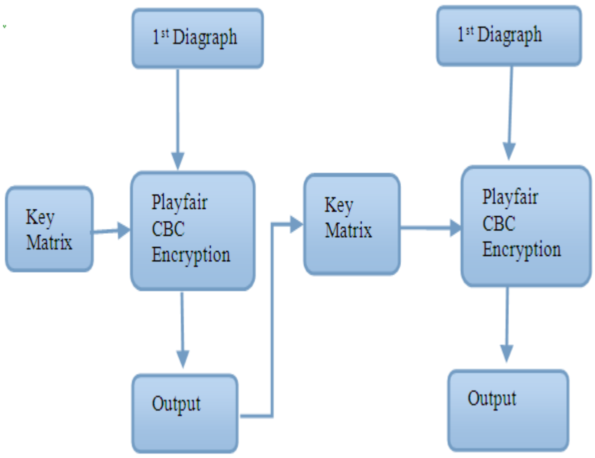

Fig. 1. Architecture of Encryption Process

B. Decryption

To decrypt a message, the message is broken into digraphs (groups of 2 letters) and then mapped them out on the key table. Then following protocols are employed to each matching set of alphabet in the plaintext:

1. When the alphabets repose on the same row of the table, they are to be shuffled with the letters immediate left of them respectively.
2. When the alphabets repose on the same column of the table, they are to be interchanged with the letters immediately above them respectively.
3. When the alphabets does not repose on the same row or column, interchange them with the alphabets on the same row respectively but of the column of the other keeping the order of the matching set unflawed.
4. After decrypting first digraph, pick the first digraph and reorganize the key matrix. It will be used to decrypt another digraph.

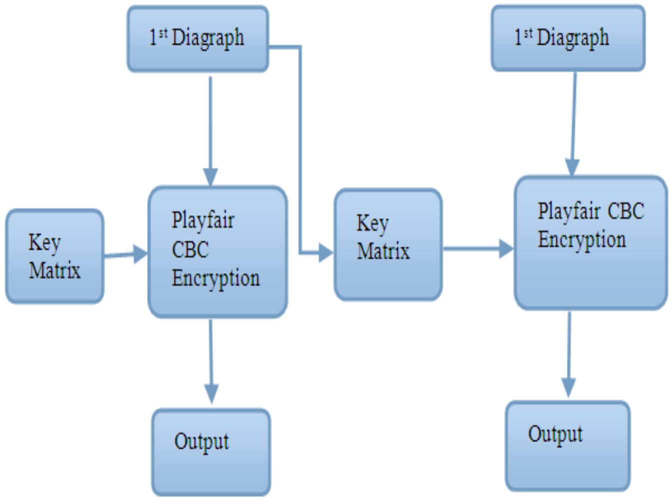

Fig. 2. Architecture of Decryption Process

IV. ILLUSTRATION OF THE PROPOSED PLAYFAIR CIPHER

In this section, our proposed Playfair cipher is demonstrates with the help of an example.

Enter the key (shared):

JAVA123$

Key Matrix for 8*8 Playfair Cipher is

J	A	V	1	2	3	$	!
"	#	%	&	'	(	)	*
+	,	-	.	/	0	4	5
6	7	8	9	:	;	<	=
>	?	@	B	C	D	E	F
G	H	I	K	L	M	N	O
P	Q	R	S	T	U	W	X
Y	Z	[	\	]	^	_	`

Consider the following plaintext.

MEET ME AT 05:00 PM TODAY

First, we have to separate it into di-grams.

ME ET ME AT 05 :0 0P MT OD AY
Encrypt first di-gram

ME **ND**

Now, the key matrix will change as per the ciphertext.

N	D	J	A	V	1	2	3
$	!	"	#	%	&	'	(
)	*	+	,	-	.	/	0
4	5	6	7	8	9	:	;
<	=	>	?	@	B	C	E
F	G	H	I	K	L	M	O
P	Q	R	S	T	U	W	X
Y	Z	[	\	]	^	_	`

Take another di-gram

ME ET **ND** @X

Now, the key matrix will change as per the ciphertext.

@	X	N	D	J	A	V	1
2	3	$	!	"	#	%	&
'	(	)	*	+	,	-	.
/	0	4	5	6	7	8	9
:	;	<	=	>	?	B	C
E	F	G	H	I	K	L	M
O	P	Q	R	S	T	U	W
Y	Z	[	\	]	^	_	`

Take another di-gram

ME ET ME **ND @X** LM

Now, the key matrix will change as per the ciphertext.

L	M	@	X	N	D	J	A
V	1	2	3	$	!	"	#
%	&	'	(	)	*	+	,
-	.	/	0	4	5	6	7
8	9	:	;	<	=	>	?
B	C	E	F	G	H	I	K
O	P	Q	R	S	T	U	W
Y	Z	[	\	]	^	_	`

In this way, our algorithm will proceed.

C. Benefits of Modified Playfair Cipher (PlayfairCBC)

Unlike the traditional Playfair cipher the modified playfair cipher can handle all the printable characters. It includes uppercase and lowercase alphabets, numerical, punctuation marks and special characters. Both keyword and plaintext can contain one or more sentences.

V. RESULT ANALYSIS AND DISCUSSION

A. Result Analysis based on Avalanche Effect

This section presents output of the implementation of our proposed algorithm. The avalanche effect has been analyzed by altering only one character (1st character) in the plaintext.

Actual Plaintext
PLAYFAIR CIPHER

Enter the key:
JAVA 123

Key Matrix for 8*8 Playfair Cipher is

J	A	V		1	2	3	!
"	#	$	%	&	'	(	)
*	+	,	-	.	/	0	4
5	6	7	8	9	:	;	<
=	>	?	@	B	C	D	E
F	G	H	I	K	L	M	N
O	P	Q	R	S	T	U	W
X	Y	Z	[	\	]	^	_

Enter Your Choice:
1.Encrypt (8*8 Playfair)
2.Decrypt (8*8 Playfair)
3.Encrypt (8*8 PlayfairCBC)
4.Decrypt (8*8 PlayfairCBC)
5.Avalanche in 8*8 Playfair
6.Avalanche in 8*8 PlayfairCBC
7.Go to Main Options

5

For Avalanche Effect, Enter Text to be Encrypted (8*8 Playfair):

KLAYFAIR CIPHER

After adding dummy character

KLAYFAIR CIPHERX
Encrypted text (8*8): LM#AGJR[2@GRN?O[

Avalanche Effect in Traditional 8*8 Playfair is: 2

Binary value:
10011001001101100011100000110001111001010101001010110111100101000000100011110100101001110111111100
11111011011

Difference in bits = 4

Enter Your Choice:
1.Encrypt (8*8 Playfair)
2.Decrypt (8*8 Playfair)
3.Encrypt (8*8 PlayfairCBC)
4.Decrypt (8*8 PlayfairCBC)
5.Avalanche in 8*8 Playfair
6.Avalanche in 8*8 PlayfairCBC
7.Go to Main Options

6

For Avalanche Effect, Enter Text to be Encrypted (8*8 PlayfairCBC):

Key Matrix for 8*8 Playfair Cipher is

J	A	V		1	2	3	!
"	#	$	%	&	'	(	)
*	+	,	-	.	/	0	4
5	6	7	8	9	:	;	<
=	>	?	@	B	C	D	E
F	G	H	I	K	L	M	N
O	P	Q	R	S	T	U	W
X	Y	Z	[	\	]	^	_

KLAYFAIR CIPHER

After adding dummy character

KLAYFAIR CIPHERX

Encrypted text (CBC 8*8): LM

L	M	J	A	V		1	2
3	!	"	#	$	%	&	'
(	)	*	+	,	-	.	/
0	4	5	6	7	8	9	:
;	<	=	>	?	@	B	C
D	E	F	G	H	I	K	N
O	P	Q	R	S	T	U	W
X	Y	Z	[	\	]	^	_

Encrypted text (CBC 8*8): LMM[

M	[	L	J	A	V		1
2	3	!	"	#	$	%	&
'	(	)	*	+	,	-	.
/	0	4	5	6	7	8	9
:	;	<	=	>	?	@	B
C	D	E	F	G	H	I	K
N	O	P	Q	R	S	T	U
W	X	Y	Z	\	]	^	_

Encrypted text (CBC 8*8): LMM[GJ

G	J	M	[	L	A	V	
1	2	3	!	"	#	$	%
&	'	(	)	*	+	,	-
.	/	0	4	5	6	7	8
9	:	;	<	=	>	?	@
B	C	D	E	F	H	I	K
N	O	P	Q	R	S	T	U
W	X	Y	Z	\	]	^	_

Encrypted text (CBC 8*8): LMM[GJFT

F	T	G	J	M	[	L	A
V		1	2	3	!	"	#
$	%	&	'	(	)	*	+
,	-	.	/	0	4	5	6
7	8	9	:	;	<	=	>
?	@	B	C	D	E	H	I
K	N	O	P	Q	R	S	U
W	X	Y	Z	\	]	^	_

Encrypted text (CBC 8*8): LMM[GJFT2@

2	@	F	T	G	J	M	[
L	A	V		1	3	!	"
#	$	%	&	'	(	)	*
+	,	-	.	/	0	4	5
6	7	8	9	:	;	<	=
>	?	B	C	D	E	H	I
K	N	O	P	Q	R	S	U
W	X	Y	Z	\	]	^	_

Encrypted text (CBC 8*8): LMM[GJFT2@CU

C	U	2	@	F	T	G	J
M	[	L	A	V		1	3
!	"	#	$	%	&	'	(
)	*	+	,	-	.	/	0
4	5	6	7	8	9	:	;
<	=	>	?	B	D	E	H
I	K	N	O	P	Q	R	S
W	X	Y	Z	\	]	^	_

Encrypted text (CBC 8*8): LMM[GJFT2@CU<H

<	H	C	U	2	@	F	T
G	J	M	[	L	A	V	
1	3	!	"	#	$	%	&
'	(	)	*	+	,	-	.
/	0	4	5	6	7	8	9
:	;	=	>	?	B	D	E
I	K	N	O	P	Q	R	S
W	X	Y	Z	\	]	^	_

Encrypted text (CBC 8*8): LMM[GJFT2@CU<HK^

K	^	<	H	C	U	2	@
F	T	G	J	M	[	L	A
V		1	3	!	"	#	$
%	&	'	(	)	*	+	,
-	.	/	0	4	5	6	7
8	9	:	;	=	>	?	B
D	E	I	N	O	P	Q	R
S	W	X	Y	Z	\	]	_

Encrypted text (CBC 8*8):LMM[GJFT2@CU<HK^

Avalanche Effect in 8*8 PlayfairCBC is: 12
Binary value:
1001100100110110011011011011100011110010101000110
1010100110010100000010000111010101111100100100010
010111011110

Difference in bits = 29

Similarly, if we take longer plaintext then the result will be more fascinating. Consider another example.

Actual Plaintext
CRYPTOGRAPHY A WORD WITH GREXEK ORIGIN MEANS SECRET WRITING.

Enter the key:
JAVA 123

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 06, June-2016

Key Matrix for 8*8 Playfair Cipher is

J	A	V		1	2	3	!
"	#	$	%	&	'	(	)
*	+	,	-	.	/	0	4
5	6	7	8	9	:	;	<
=	>	?	@	B	C	D	E
F	G	H	I	K	L	M	N
O	P	Q	R	S	T	U	W
X	Y	Z	[	\	]	^	_

For Avalanche Effect, Enter Text to be Encrypted (8*8 PlayfairCBC):

KRYPTOGRAPHY A WORD WITH GREXEK ORIGIN MEANS SECRET WRITING.

Encrypted text (CBC 8*8): ISZOMVFT2KLX1 V AHGH_KFAFH[@2DG1ZUM23BLB]I]'A#:EP#OXYW3 K]RV9

Avalanche Effect in 8*8 PlayfairCBC is: 56
Binary value:
1001001101001110110101001111100110110101101000110
1010100110010100101110011001011000110001100000101
0110100000100000110010001000111100100010111111100
1011100011010000011000110100100010110111000000110
0101000100100011111000110110101010101100110111001
0110011100001010011001000010101110110010011011101
1001111000001100011111010100010110100001000111001
1111011000101100110101111100111001011101110110100
101010110111001

Difference in bits = 201

It can be clearly seen that by the change of only 1 character in the input, the avalanche effect is 56 or 201 (49.507 %) in number of bits. If more number of characters is changed in the input then the output will be more different.

B. Result Analysis based onCiphertext Only Attack

Our Proposed PlayfairCBC can also be implemented using 16 x 16 matrix also. To launch a ciphertext only attack, the number of di-grams the attacker has to search would be 256 x 256 i.e. 65536 in the modified cipher instead of 26 x 26 i.e. 676 di-grams in the traditional cipher.

C. Result Analysis based on Brute Force Attack

The worst case may involve traversing the complete search area. The size of key domain in the modified cipher would be 256! (Factorial 256) instead of 25! (Factorial 25) for the traditional Playfair cipher.

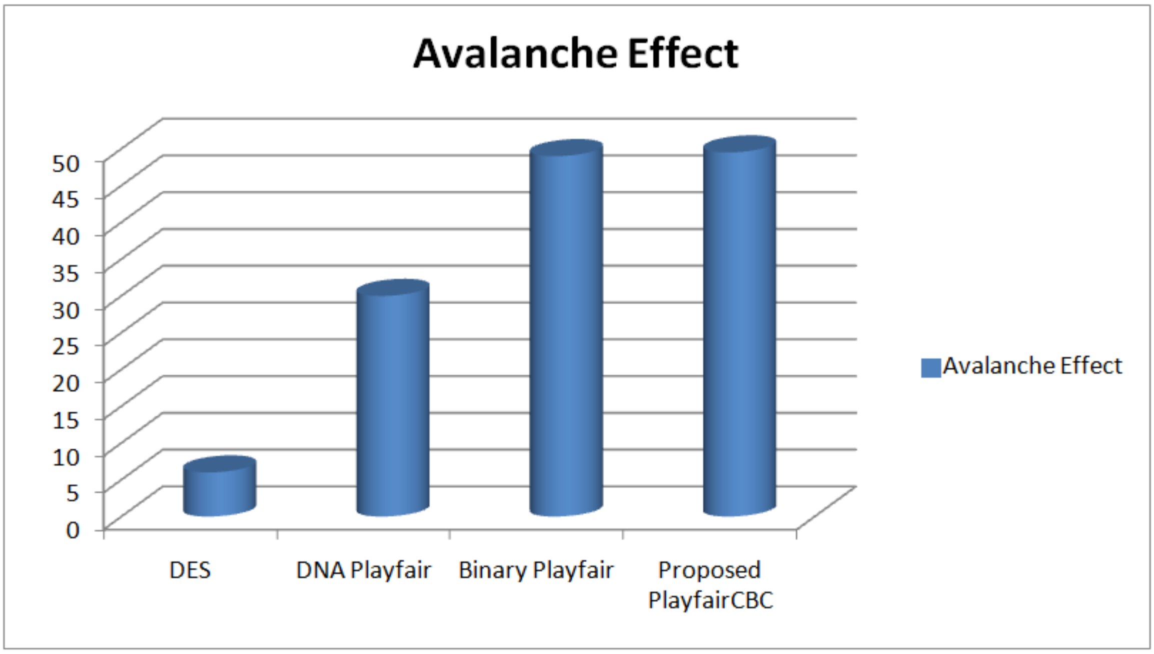

Figure 1. Comparison based on Avalanche Effect

VI. CONCLUSION

The original Playfair cipher uses a digraph substitution technique to encrypt/decrypt alphabets based on a reference 5×5 key matrix, which is formed from the given key. The algorithm is strictly restricted to “English Alphabet”, that to either in uppercase or in lowercase character. No numbers, punctuations are supported. Several modification attempts focuses on elimination of several limitations. Some increases the character-set of the key matrix, some uses the ASCII values and others incorporated randomness. But these modifications stand strong in their own purposes. The overall limitations of the cipher were not eliminated by these individual modifications.

The proposed PlayfairCBC uses the encrypted digraph in order to re-construct the key matrix. It can be clearly seen that by the change of only 1 character in the input, the avalanche effect is 56 or 201 (49.507 %) in number of bits. If more number of characters is changed in the input then the output will be more different.

REFERENCES

[1] B. A. Forouzan, “Cryptography and network security,” Tata McGraw-Hill, Special Indian Edition, 2007.

[2] Sanjay Basu and Utpal Kumar Ray “Modified Playfair Cipher using Rectangular Matrix”, International Journal of Computer Applications (0975 – 8887) Volume 46– No.9, May 2012.

[3] Packirisamy Murali and Gandhidoss Senthilkumar “Modified Version of Playfair Cipher using Linear Feedback Shift Register”, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008.

[4] Ravindra Babu K, S. Uday Kumar, A. Vinay Babu, I.V.N.S Aditya , P. Komuraiah, “An Extension to Traditional Playfair Cryptographic Method”, International Journal of Computer Applications (0975 – 8887) Volume 17, No.5, March 2011.

[5] Shiv Shakti Srivastava, Nitin Gupta “A Novel Approach to Security using Extended Playfair Cipher”, International Journal of Computer Applications (0975 – 8887) Volume 20– No.6, April 2011.

[6] Srivastava, S. S., & Gupta, N. (2011, June). Security aspects of the Extended Playfair cipher. In Communication Systems and Network Technologies (CSNT), 2011 International Conference on (pp. 144-147). IEEE.

[7] Srivastava, S. S., & Gupta, N. (2011). Rajaram jaiswal “Modified Version of Playfair Cipher by using 8x8 Matrix and Random Number Generation” in Proceedings of IEEE 3rd International Conference on Computer Modeling and Simulation (ICCMS 2011).

[8] Verma, V., Kaur, D., Singh, R. K., & Kaur, A. (2013, August).3D-Playfair cipher with additional bitwise operation. In Control Computing Communication & Materials (ICCCCM), 2013 International Conference on (pp. 1-6). IEEE.

[9] Nisarga Chand, Subhajit Bhattacharyya, “A Novel Approach for Encryption of Text Messages Using PLAY-FAIR Cipher 6 by 6 Matrix with Four Iteration Steps”, International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 1, January 2014, 478-484.

[10] S. S. Dhenakaran and M. Ilayaraja, “Extension of Playfair Cipher using 16X16 Matrix”, International Journal of Computer Applications (0975 – 888) Volume 48– No.7, June 2012.

[11] Swati Hans, Rahul Johari, Vishakha Gautam, “An Extended PlayFair Cipher using Rotation and Random Swap patterns,” 5th IEEE International Conference on Computer and Communication Technology, 2014.

[12] Uttam Kr. Mondal, Satyendra Nath Mandal and J. Pal Choudhury “A Framework for the Development Playfair Cipher Considering Probability of Occurrence of Characters in English Literature”, 2009 International Journal of Computer Science and Network Security, Vol. 8, No. 8, August 2008.

[13] Mona Sabry, Mohamed Hashem, Taymoor Nazmy and Mohamed Essam Khalifa, “A DNA and Amino Acids-Based Implementation of Playfair Cipher”, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 8, No. 3, 2010, Page 129-136.

[14] A. Lahiri, “Design and Implementation of an Enhanced Binary Playfair Algorithm using a 4×4 Key Matrix,” Thesis Dissertation, Jadhavpur University, 2012.

[15] Salman A. Khan, “Design and Analysis of Playfair Ciphers with Different Matrix Sizes,” International Journal of Computing and Network Technology, Vol. 3, No. 3, 2015, Page 117-122.

[16] Puneet Kumar and Shashi B. Rana, “Development of Modified Polybius Technique for Data Security,” Vol. 5, No. 2, 2015, Page 227-229.

[17] Chandan Kumar, Sandip Dutta and Soubhik Chakraborty, “A Hybrid Polybius-Playfair Music Cipher,” International Journal of Multimedia and Ubiquitous Engineering, Vol.10, No.8, 2015, Page 187-198.