Indonesian Journal of Electrical Engineering and Computer Science
Vol. 6, No. 3, June 2017, pp. 695 ~ 703
DOI: 10.11591/ijeecs.v6.i3.pp695-703

New Approach of the Playfair's Cipher with a Numerical Value of the Keyword

Assia Merzoug*[1], Adda Ali Pacha[2], Naima Hadj Said[3]
[1]Laboratory of Coding and Security of Information, University Batna 2, 05 avenue Chahid Boukhlouf Batna 05000 Algeria
[2,3]University of Oran of Sciences and Technology, PoBox 1505 Oran M'Naouer 31000
*Corresponding author, e-mail: assia_merzoug@yahoo.fr

Abstract

At least during the last five years there has been an explosion of a public academic research in cryptography for Playfair's cipher. We were interested, and we have proposed a method to improve it, to make it safer and more efficient. We have oversized this encryption matrix by 7x7 coefficents and for its filling, we have combined two chaotic maps (the attractor Henon and logistics map). The attractor Henon of dimension 2, determines the intersection of the row and column of the new matrix playfair. The coefficients of this matrix are calculated from logistic map, each value is a single character of the alphabet used. The secret keyword is formed by the initial conditions of the chaotic attractors.

Keywords*: cryptography, playfair, polygram, chaos, attractor, henon, logistics map*

1. Introduction

Technological progress especially in the areas of telecommunications and computing has created a new form of information security (cryptography). Therefore, it is the way to safeguard the confidentiality of the information. This works is based on the Playfair cipher [1], which is to encrypt pairs of letters (digraphs), instead of single letters as in ciphers poly-alphabetic substitutions such as the Vigenère cipher, more prevalent in time. In recent years, there has been a public academic research in cryptography explosion on this cipher [2-14].

In this paper, we propose a new approach to the cipher of Playfair, with the combination of the concepts of chaos theory. The idea is to combine two chaotic maps, the attractor Henon and logistics map to construct the Playfair matrix. By Henon attractor that has dimension 2, we constructed this new matrix; the elements of this matrix are calculated from the logistic map. This value is a unique character of the Playfair matrix and the alphabet used. The secret keyword is formed by the initials conditions of chaotic attractors.

This paper is organized as follows: Section 2 description of the Playfair cipher. In Section 3, we introduce the concept of the chaos theory and we introduce the Hénon attractor and the logistical map. In Section 4, we propose a new approach to the cipher of Playfair. In Section 5, we analyze the results and we valid the proposal cipher. Section 6 concludes this paper.

2. Playfair Encryption

The Playfair cipher or Playfair square is a manual symmetric encryption method that was first used encryption technique of practice Polygram substitution. It was devised in 1854 by Charles Wheatstone (1802-1875), one of the pioneers of the electric telegraph, but bears the name of Lord Playfair who popularized its use. It was used by British forces during the Second Boer War and the First World War and by the Australians during the Second World War.

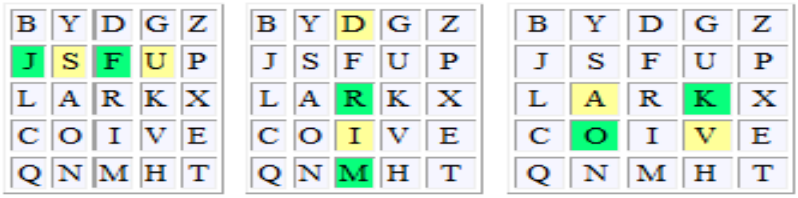
2.1. Encryption Method

Playfair cipher uses an array of 5x5 letters containing a keyword or phrase. The memorization of the keyword and 4 rules to follow are enough to use this encryption. Completethe table with the letters of the keyword (ignoring duplicates), and then supplement it

Received February 27, 2017; Revised May 5, 2017; Accepted May 22, 2017

with the ther letters of the alphabet in order (in omitting the letter Q or occupying the same space for the letters I and J depending on the version).

The key word can be written on-line, column or even on spiral. To form the encryption grids, using a secret keyword to create a messy alphabet with which filled the grid line by line. To encrypt a message, take the letters 2 by 2 (bigrams) and apply the following rules depending on the position of the letters in the table:



1. If two letters are identical (or if only one remains), put an "X" after the first letter. Encrypt the new pair thus constituted and continue with the next. In some variations, use 'Q' instead of 'X', but any letter will do the trick, between the two letters to eliminate this duplication
2. If the letters are on the same line of the table, replace them with those found immediately to their right (by looping on the left if the edge is reached), FJ will be replaced by US, VE by EC (Rule 1).
3. If the letters appear on the same column, replace them with those that are just below (by looping from the top if the bottom of the table is reached), BJ will be replaced by JL, RM by ID (Rule 2).
4. If not, replace the letters by them being on the same line, but in the opposite corner of the rectangle defined by the original pair. Example VA is OK, BI becomes DC, GO becomes YV. The first two letters are encrypted on the same line as the first clear letter (Rule 3).

2.2. Example of a Cipher Playfair

Assuming that the key is "playfair example", the table must be filled as follows, with omitting the letter Q:

P	L	A	Y	F
I	R	E	X	M
B	C	D	G	H
J	K	N	O	S
T	U	V	W	X

Encryption of the message *"Come to the window"*.
Plaintext: CO ME TO TH EW IN DO WX
Cryptogram: GK IX JW BX VX EJ GN TX

2.3. Decryption Method

To decrypt, use the inverse method with ignoring the 'X' or 'Q' that do not have their place in the final message, that is to say, taking the letters to the left in the case of the same line up in the case of a same column, and always in the case the corners of a rectangle.

2.4. Cryptanalysis

This encryption is significantly harder to break since the frequency analysis attacks usually used on simple substitution ciphers are not very effective on him.

The digraphs frequency analysis is still possible, but applied to $25^2 = 625$ possible digraphs rather than the 26 letters of the alphabet; it is considerably more difficult and requires a cipher text much longer to hope to be effective.

However, like most old ciphers, the Playfair cipher can be broken if we have enough samples. Get the key is relatively fast if one has knowledge of both the cipher text and plaintext (known plaintext attack). The use of chaos would complicate things.

3. Chaos Theory

There is no strict definition of chaos. However, we must admit the notion of an "unpredictable and erratic phenomenon" [15, 16, 17]. In addition, over the past twenty years, the term chaos is attributed to "erratic behaviors that are related to simple systems that can be governed by a small number of variables between which the relations describing their evolution can be written. These systems are while unpredictable deterministic. "Various authors state that chaos is "a long-term actually unpredictable behavior occurring in a dynamic system because of sensitivity to initial conditions (SIC)".

3.1. Sensitivity to Initial Conditions

Sensitivity to initial conditions (S.I.C) is a fundamental characteristic of dynamic systems. Here means that a system will react completely differently depending on the initial condition. This particular result in the fact of chaotic system, even if all its components are determined, is very unpredictable as sensitive to very small initial perturbations.

3.2. Attractor

Attractor describes a regime situation that can occur after disappearance of transient phenomena. Strange attractors are what we call chaos.

Among the most popular attractors in the discrete case, we find logistics map and Henon attractor [15], to study the dynamics of stars moving in galaxies. Henon discovered that the strange attractor of stellar orbits has the shape of banana (Figure 1).

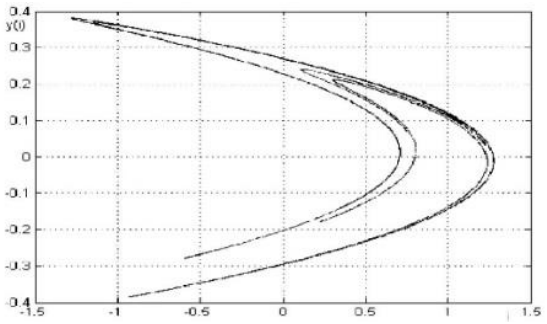


Figure 1. Attracteur de Henon

3.3. Henon Attractor

Chaotic attractor of Henon named like the French astronomer “Michel Henon” was presented first time in 1976 [16] and depending on two parameters a and b, based on the following equations:

$$X_{n+1} = \begin{cases} (Y_n + 1) - (a * X_n^2) \\ Y_{n+1} = b * X_n \end{cases} \quad (1)$$

The initial conditions are (x_0=1, y_0=1) with a = 1.4 and b = 0.3, these both values shows the chaotic behavior of Henon attractor.

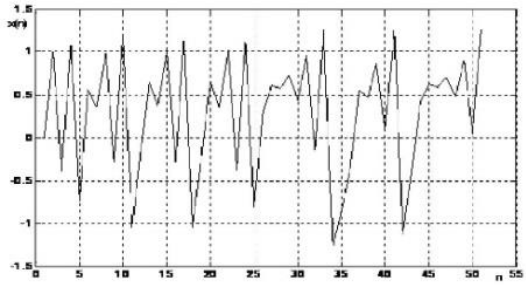


Figure 2A. Attractor for *x*

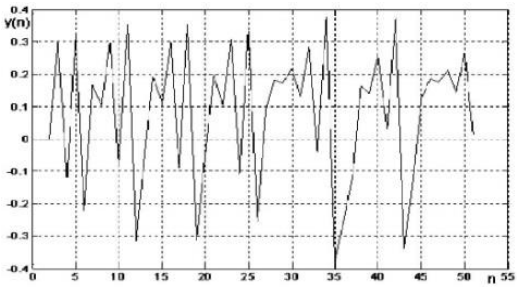


Figure 2B. Attractor for *y*

3.4. Logistic Map

Logistics map [17] is a well-known dynamic in non-linear systems theory, defined by equation (2):

$$y_{k+1} = r.x_k(1 - x_k) \quad (2)$$

It gives a perfect explanation of a dynamic system behavior. This system was developed by Prof. Pierre François Verhulst (1845) to measure the evolution of a population in limited environment, later used in 1976 by the biologist Robert May to study the evolution of insect population:

1. y_{k+1}: Generation in the future that is proportional to x_k.
2. x_k: Previous generation.
3. r: Positive constant incorporates all factors related to reproductive, successful overwintering eggs for example, etc.

In order to study this dynamic system and some asymptotic individuals' models, the first thing to do is to draw the parabolic graph $y = r.x(1 - x)$, and the diagonal $y = x$.The operation that we will follow to draw the iterative form y_{k+1}according to x_k is simply summarized as following:

1. Starting from an initial value x_0 of the x-axis, we reach the function with a vertical, the function takes the value$y_1 = r.x_0(1 - x_0)$
2. From horizontal $y_1 = r.x_0(1 - x_0)$ of the previous point, we join the line $y = x$,
3. We represent the abscissa of the intersection with the vertical line $x = x_0$, we have $y_1 = x_1$.
4. From the x_1 value of the x-axis, we reach the function with a vertical, the function takes the value $y_2 = r.x_1(1 - x_1)$, and so on.

We take $r = 3.9$ and, $x_0 = 0.01$ for logistics card, the previous operations for 100 iterations are represented in Figure 3.

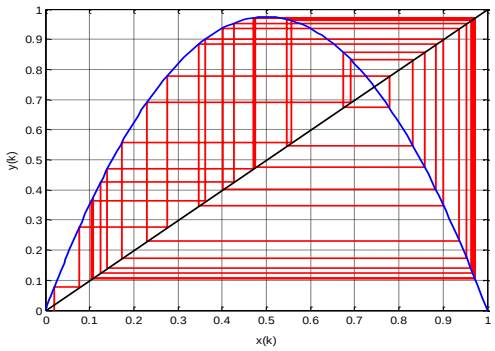


Figure 3A. Evolution of y_k in function of x_k

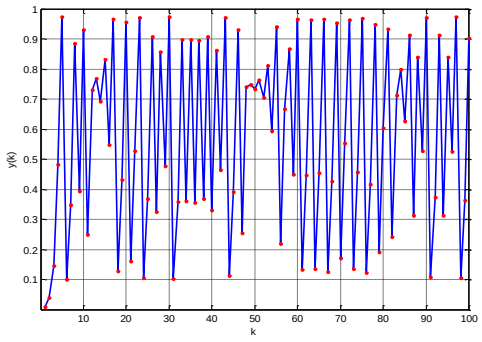


Figure 3B. Chaotic regime in function of k

4. Proposed Cryptosystem

First, we must know that we work in a set of characters that contains the alphabet increased by two characters (#, @) symbols of punctuation, and the decimal numbers and the basic calculation operators as follows:

a) The basic alphabet — 26 +2 : The alphabet is increased by two characters (#, @):

1. Typographical sign "#": the spider is often confused with the sharp "♯".
2. Typeface @: the at sign, a business.

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	#	@

b) Special symbols — 5 characters: dot, comma, question mark, and the open and closed parentheses.

.	,	?	(	)

c) Ciphers— 10 characters 0 to 9

0	1	2	3	4
5	6	7	8	9

d) Operators — 6 characters : the addition, subtraction, division, multiplication represented by *, equality and the percent sign:

+	-	/	*	=	%

We has (26 + 2 + 5 + 10 + 6) =49 characters, we put them in a 7x7 matrix of size, as follows:

Table 1. Basis Matrix of Playfair

	0	1	2	3	4	5	6
0	A	B	C	D	E	F	G
1	H	I	J	K	L	M	N
2	O	P	Q	R	S	T	U
3	V	W	X	Y	Z	#	@
4	.	,	?	(	)	0	1
5	2	3	4	5	6	7	8
6	9	+	-	/	*	=	%

There continues to be one relationship between the basis matrix Playfair, the modulo (49) and the character itself. Any character is represented by its value in the base matrix Playfair as follows:

$$\text{Character} \rightarrow \text{value (line *7 + column)} \quad (3)$$

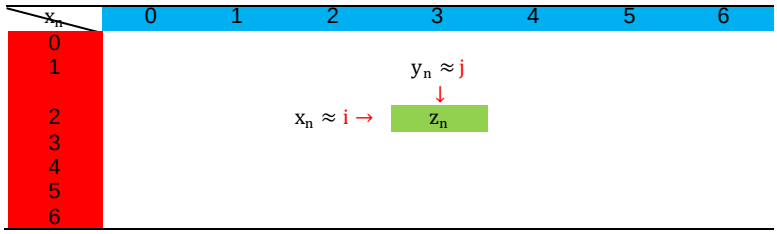
The idea is to fill the size of Playfair cipher matrix (7x7), lines and columns as follows:

- $Line\ i = mod(fix(x_n * 10^7), 7)$
- $Column\ j = mod(fix(y_n * 10^7), 7)$
- $Value(i,j) = mod(fix(z_n * 10^7), 49)$

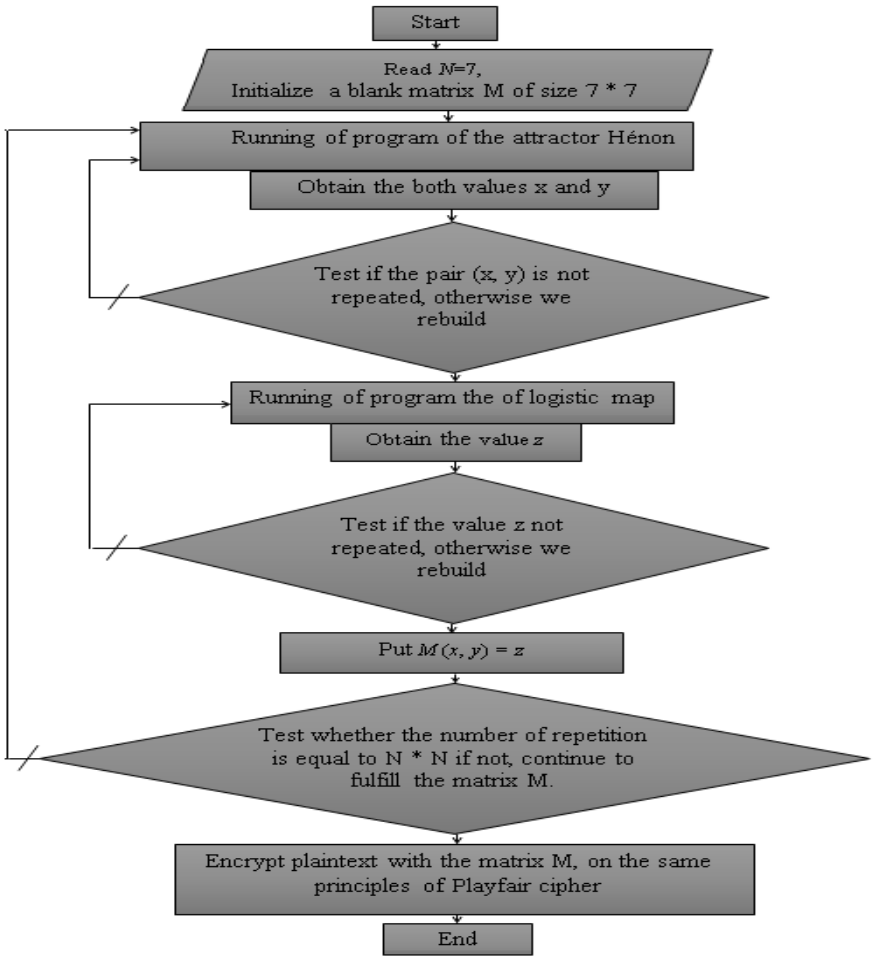
10^7 is a starting index value, mod and fix functions are MATLAB functions defined as follows: mod: Remainder after division (modulo operation) and fix: Round towards zero.

We propose the following chart:

1. With the initial conditions, for example, $(x_0 = 0.1\ et\ y_0 = 0.1)$, and $a = 1.4$ and $b = 0.3$: calculating the positions i and j according to the principle of the attractor Henon:
   - $Line\ i = mod(fix(x_n * 10^7), 7)$
   - $Column\ j = mod(fix(y_n * 10^7), 7)$
2. Calculate the z value of the logistical map according to the logistic equation, with $z_0 = 0.01, r = 3.9$: $z_n = mod(fix(z_n * 10^7), 49)$



3. Fill the new encryption matrix Playfair: $k(i,j) = z_n$ (z_n value built by logistics map), and the couple is kept (i,j) that fills the value of the matrix k only one time. This value is deducted against our base matrix Playfair (Table 1).
4. Repeat steps 1, 2, 3 and 4 until it completes the filling of the matrix k.
5. Encrypts the plaintext by k matrix with that on the same basic principles of the Playfair cipher.



The two characters (#, @) can be used to eliminate duplicate letters (the choice of this character is arbitrary). If there remains only one letter towards the end of the plaintext is added point where many places.

5. Results and Interpretations

The size of the encryption key space is the total number of different values that can be used in the encryption process. In the proposed algorithm, the secret key field is set as follows:

$$ST = \{x_0, y_0, z_0, N1, N2\}$$

Where x_0, y_0, z_0 are double precision numbers. $N1, N2$ are integer constants (starting index value attractors Henon map and logistics respectively).

If the calculating precision of: x0, y0, zo, is 10-16, and $N1|N2 \in [1,1000]$. Therefore, the key space is larger than $10^{16} \times 10^{16} \times 10^{16} \times 1000 \times 100, (avec 10^3 \approx 2^{10})$ in this case, we will have a key field of the order of 2^{180}, and it is huge. Therefore, the encryption algorithm has a very large key space to withstand all kinds of brute force attacks.

We give some Playfair encryption matrices for different encryption keys. It hangs like fixed values: $a = 1.4, b = 0.3, r = 3.9$.

1) The new variable values that form the encryption key are:
   - ✓ $x_0 = 0.95, y_0 = 0.56, z_0 = 0.02, N1 = N2 = 19$

Table 2. Encryption Matrix N°1

	0	1	2	3	4	5	6
0	A	?	I	-	H	T	C
1	0	=	N	.	K	V	)
2	#	U	@	2	M	4	+
3	(	L	3	8	J	y	D
4	/	P	X	E	G	F	,
5	S	%	9	5	W	*	R
6	6	O	7	1	Z	B	Q

2) The new variable values that form the encryption key are:
   - ✓ $x^0 = 0.9500000001, y_0 = 0.56, z_0 = 0.02, N1 = N2 = 19$

Table 3. Encryption Matrix N°2

	0	1	2	3	4	5	6
0	W	(	T	6	N	1	C
1	#	F	X	7	D	J	/
2	P	R	+	.	@	G	H
3	?	2	M	8	Y	)	O
4	0	-	L	S	=	I	%
5	U	S	V	3	B	Z	E
6	K	4	9	*	,	Q	A

3) The new variable values that form the encryption key are:
   - ✓ $x_0 = 0.95, y_0 = 0.5600000001, z_0 = 0.02, N1 = N2 = 19$

Table 4. Encryption Matrix N°3

	0	1	2	3	4	5	6
0	E	5	O	T	B	8	N
1	9	Q	L	0	U	#	W
2	P	D	C	-	M	F	X
3	.	,	6	S	?	K	%
4	Y	2	=	4	@	1	G
5	7	)	3	H	R	*	V
6	A	+	/	I	Z	(	J

4) The new variable values that form the encryption key are:

✓ $x_0 = 0.95, y_0 = 0.56, z_0 = 0.0200000001, N1 = N2 = 19$

Table 5. Encryption Matrix N°4

	0	1	2	3	4	5	6
0	R	A	.	4	3	9	6
1	F	B	M	V	?	0	J
2	E	K	Y	Z	D	N	+
3	)	H	G	C	5	X	#
4	7	*	(	,	@	1	I
5	T	%	2	U	W	S	8
6	Q	O	L	-	=	/	P

5) The new variable values that form the encryption key are:

✓ $x_0 = 0.95, y_0 = 0.56, z_0 = 0.02, N1 = 18, N2 = 19$

Table 6. Encryption Matrix N°5

	0	1	2	3	4	5	6
0	A	?	I	-	H	T	C
1	0	=	N	.	K	V	)
2	#	U	@	2	M	4	+
3	(	L	3	8	J	y	D
4	/	P	X	E	G	F	,
5	S	%	9	5	W	*	R
6	6	O	7	1	Z	B	Q

6) The new variable values that form the encryption key are:

✓ $x_0 = 0.95, y_0 = 0.56, z_0 = 0.02, N1 = 19, N2 = 18$

Table 7. Encryption Matrix N°6

	0	1	2	3	4	5	6
0	3	?	I	L	A	T	C
1	@	K	V	.	N	M	)
2	-	=	5	Z	F	4	D
3	(	Q	#	8	J	*	2
4	/	P	+	E	G	Y	,
5	S	%	9	H	W	0	R
6	6	X	7	O	U	B	1

It is noted through the encryption matrix N°2, N°3 and N°4 with respect to the encryption matrix N°1, they are completely different despite the minimal difference of the fields of the key. This proves that what we have proposed gives very satisfactory results.

The same can do it by appearing encryption matrices N°5 and N°6 to the encryption matrix N°1.

6. Conclusions

In this work, we presented a new system of Playfair cipher. We kept the same principle encryption, but we changed the dimension of the array of characters to a 5x5 size for 7x7 characters, and we've removed the keyword or phrase to remember, and we replace it with a key 180 bits.

The new encrypted so represented has given very good result and, There are a very large key space to withstand all kinds of brute force attacks.

References

[1] B Schneier. Applied Cryptography-Protocols. Algorithms and Source Code in C. John Wiley & Sounds, Inc. New York : Second Edition. 1996.

[2] Alam et al. Universal Playfair Cipher Using MXN Matrix. *International Journal of Advanced Computer Science*. 2011 ; 1(3) : 113-117.

[3] A Aftab Alam, B Shah Khalid and C Muhammad Salam. A Modified Version of Playfair Cipher Using 7×4 Matrix. *International Journal ofComputer Theory and Engineering*. 2013 ; 5(4).

[4] Gaurav Shrivastava, Manoj Chouhan, Manoj Dhawan. A Modified Version Of Extended Plafair Cipher (8x8). *International Journal Of Engineering And Computer Science*. ISSN: 2319-7242. 2013; 2(4) : 956 -961.

[5] 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)*. 2014 ; 3(1).

[6] Jitendra Choudhary, Ravindra Kumar Gupta, Shailendra Singh. A GENERALIZED VERSION OF PLAY FAIR CIPHER, COMPUSOFT. *An international journal of advanced computer technology*. ISSN:2320-0790. 2013 ; II(VI).

[7] Ashish Negi, Jayveer Singh Farswan, V.M Thakkar, Siddharth Ghansala. Cryptography Playfair Cipher using Linear Feedback Shift Register. *IOSR Journal of Engineering*. 2012; 2(5): 1212-1216.

[8] Vinod Kumar, Santosh kr Upadhyay, Satyam Kishore Mishra, Devesh Singh. Modified Version of Playfair Cipher Using Linear Feedback Shift Register and Transpose Matrix Concept.*International Journal of Innovative Technology and Exploring Engineering (IJITEE)*. ISSN: 2278-3075. 2013; 3(1).

[9] Packirisamy Murali and Gandhidoss Senthilkumar. Modified Version of Playfair Cipher using Linear Feedback Shift Register. *IJCSNS International Journal of Computer Science and Network Security*. 2008; 8(12).

[10] OOuday Nidhal Ameen Hanosh1, Baraa Wasfi Salim. 11 × 11 Playfair Cipher based on a Cascade of LFSRs. *IOSR Journal of Computer Engineering (IOSR-JCE)*, e-ISSN: 2278-0661, www.iosrjournals.org. 2013; 12(1) : 29-35.

[11] D Dalal Abdulmohsin Hammood. Breaking A Playfair Cipher Using Memetic Algorithm. *Journal of Engineering and Development.* ISSN 1813- 7822. 2013; 17(5).

[12] VVUK. Sastry, N Ravi Shankar and S Durga Bhavani. A Generalized Playfair Cipher involving Intertwining, Interweaving and Iteration. *International Journal of Network and Mobile Technologies*, 2010; 1(2).

[13] J Jitendra Choudhary, Ravindra Kumar Gupta, Shailendra Singh. A Survey of Existing Playfair Ciphers. *International Journal of Engineering and Advanced Technology (IJEAT)*. ISSN: 2249 – 8958. 2013; 2(4).

[14] Safwat Hamad. A Novel Implementation of an Extended 8x8 Playfair Cipher Using Interweaving on DNA-encoded Data. *International Journal of Electrical and Computer Engineering (IJECE),* http://iaesjournal.com/online/index.php/IJECE. 2014; 4(1) : 93-100.

[15] KKT Alligood, TD Sauer, JA Yorke. CHAOS: An Introduction to Dynamical Systems. Berlin : Springer-Verlag. 1996.

[16] JJ GLEICK. chaos theory. Albin Michel. 1989.

[17] S Steven H Strogatz. Nonlinear Systems and Chaos. Perseus publishing. 1994.