Poly encrypted text based on dynamic selection and chaotic behavior

Amaria Wael
University of Science
and Technology of Tunis, Tunisia
Amaria.wael@hotmail.fr

Seddik Hassene
University of Science
and Technology of Tunis, Tunisia
seddik_hassene@yahoo.fr

Bouslehi Hamdi
University of Science
and Technology of Tunis, Tunisia
Hamdouchb@gmail.com

Received: April 15, 2019. Revised: May 27, 2021. Accepted: October 27, 2021. Published: November 17, 2021.

***Abstract*— Indeed, the current cryptography suffers from the rise of the computing power of computers and the advent of quantum computers could be the death knell of these algorithms. Therefore, with this paper, we present a new encryption approach based on chaotic outputs to insure more protection. This approach combines two encryption techniques in addition to random permutation. The first one consists to put in disorder binary data and the second technique is based on conditional logical function. The choice between those two techniques is perfectly random and generated from chaotic outputs. Each process has her own keys which make the encryption more complicated.**

***Keywords*— poly encryption; symmetric Encryption; random permutation; multiple key; chaotic functions; dichotomous permutation**

I. Introduction

Cryptography [1] can be defined as the conversion of data into a scrambled code that can be deciphered and sent across a public or private network. As more and more information is stored on computers or communicated via computers, the need to insure that this information is invulnerable to snooping and/or tampering becomes more relevant.

The desire to transmit messages securely is not new. For centuries, people have had a need to keep their communications private. Today, digital communications systems, particularly those related to the internet, are used to carry vast amounts of sensitive data. Sending credit card information to a web site in an e-commerce transaction or exchanging confidential trade secrets by e-mail are typical examples. The field of cryptography deals with the techniques for conveying information securely. The goal is to allow the intended recipients of a message to receive the message properly while preventing eavesdroppers from understanding the message. The message in its original form is called plaintext. The transmitter in a secure system will encrypt the plaintext in order to hide its meaning. This reversible mathematical process produces an encrypted output called cipher text. The algorithm used to encrypt the message is a cipher. Cryptanalysis is the science of breaking ciphers, and cryptanalysts try to defeat the security of cryptographic systems. A cipher text can be transmitted openly across a communications channel. Because of its encrypted nature, eavesdroppers who may have access to the cipher text will ideally be unable to uncover the message’s meaning. Only the intended recipient can decrypt the message to recover the plaintext for interpretation.

II. Logistic function

The logistic map [2] is a basic mapping polynomial, which has chaotic behavior, and it can be obtained by a very simple nonlinear dynamical equation [3].

Recurrence logistics is an example where the recurrence is not linear. This recurrence was popularized by the biologist Robert May in 1976. Its recurrence relation is.

$$\tau(x_n) = x_{n+1} = \lambda\, x_n (1 - x_n) \qquad (1)$$

The control parameter “λ” is fixed and chosen so that equation (1) has a chaotic behavior [4]. However, if we study the map with a different value of “λ”, it shows that it is a trigger for the chaos. Mathematically, the “Logistic map” is written with

”x” is a number between 0 and 1, and represents the initial condition

“λ” is a positive number [5].

III. Algorithm encryption based on the iteration of the improved “Logistic Map”

After the iteration of the function of "Logistic map" N times, we obtain N value Xn between 0 and 1 and x0: the initial value and $0 < x_0 < 1$ and λ : control parameter.

In our encryption algorithm we take $x_0 = 0.1777 \in [0, 1]$ and $\lambda = 3.759889 \in [3.57, 4]$, we obtain a chaotic signal and the value which generated chaotic sweep the entire range of value between 0 and 1. After 70 iterations, the signal from equation 1 is summarized in (figure 1).

Indeed, the chaotic function “Logistic Map” has several properties, such as frequency and sensitivity to initial conditions (this is a characteristic of all chaotic systems: if we take a different value which is very close to then the values changes completely from the iteration. If we take a different value which is very close to the values of "λ "the iteration changes dramatically: this can be seen through a simulation tool Matlab, in particular by the value of these functions which are completely random. Although they are limited from a few bands, the iterative values never give the impression to converge even after an infinite number of iterations. The change of control parameters (λ) and the initial condition (x_0) by very close values in order to obtain the decryption algorithm which always gives cryptograms so radically different that it is interesting to use the function in logistic encryption).

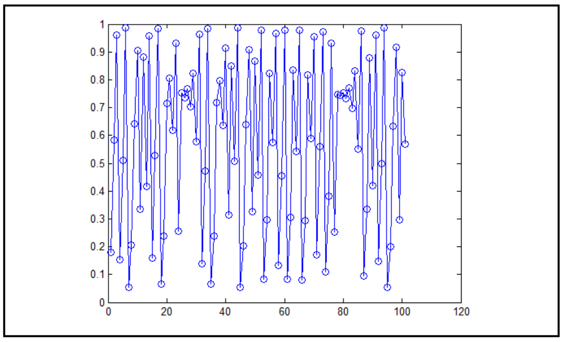

Fig. 1. The logistic map outputs after 100 iterations

IV. PROPOSED APROCH

This approach is based on poly encryption technique. We combine more than one encryption algorithm to scramble the plaintext and remove the meaning of sentences. These algorithms are performed on parallel to optimize the response time and make the task more complicated.

$$MSG = \{MSG_1, MSG_2, \ldots\ldots\ldots\ \ldots\ldots\ldots,\ MSG_n\} \qquad (2)$$

$$\mathrm{M} = \mathrm{ASCII}\,(\mathrm{MSG}) \qquad (3)$$

$$M = \{M_1, M_2, \ldots\ldots\ldots\ \ldots\ldots\ldots,\ M_n\} \qquad (4)$$

Such as:
"MSG" is the text to encrypt
"M" is a vector of "n" integers
"n" is the length of the plaintext.
And ASCII a function: X → Y which x is a set of letters and Y a vector of integers.

A. Permutation

The first step to execute on the plain text is the permutation. The disorder is crucial in cryptography. It is used to remove the meaning of the sentence. Even if a cryptanalyst has managed to decode the message, it will be a set of letters that have no meaning. This procedure is simple and effective and it is a key dependent.

$$M = \{M_1, M_2, \ldots\ldots\ldots\ \ldots\ldots\ldots,\ M_n\} \qquad (5)$$

$$P(M) = \{\ M_{(n/2)+1}, M_1, M_{(n/2)+2}, M_2, .., M_n, M_{(n/2)}\ \}(6)$$

$$P(M) = \{P_1, P_2, \ldots\ldots\ldots\ \ldots\ldots\ldots,\ P_n\} \qquad (7)$$

Such as "P" is a function: Y → Y which x is a set of letters and Y a vector of integers.

The process of permutation is partitioned into several rounds. The number of rounds is generated by logistic function which 'key11' and 'key12' are used as control parameters. The modification applied in each round is explained by this diagram:

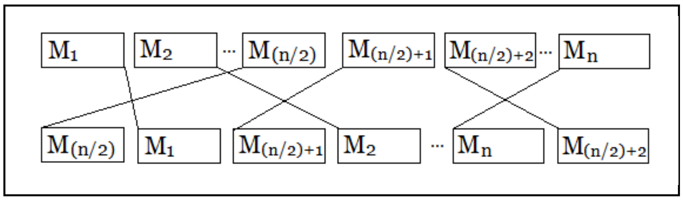

Fig. 2. Permutation diagram

B. Selection

After permutation performed on the original text, we apply the encryption process. We use more than one only encryption process to make it more difficult to broke. These algorithms are applied in parallel to make it more and more complicated and to optimize the response time. We don't have to execute all process.

The selection between different encryption systems is based on logistic function which offers us binary output values. Binary 'zero' output means we have to use the first algorithm, if not we use the second one. These outputs are generated by the logistic function which its control parameters are considered such as keys called 'key21' and 'key22'.

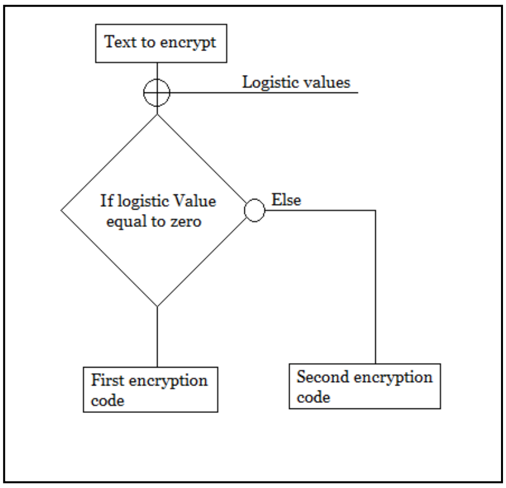

Fig. 3. Selection diagram

C. First encryption process

The first encryption code consists to apply a 'not' logic function. This latter is reversible and conservative but it is simple to broke, the raison why we modified function to make it more complicated. The logic function won't be applied to all binary values of each entry but only for some of them. The selection will be made through a random logistic value generated with control parameters already defined by users. These parameters are considered as keys, called 'key31' and 'key32'. After application of the logic function, we add to the result the same logistic value used to make the selection.

$$P = \{P_0, P_1, ..., P_7\} \qquad (8)$$

$$C = \{C_0, C_1, ..., C_7\} \qquad (9)$$

$$\text{if } C(i) = 1 \ E(i) = not(Pi) \text{ Else } E(i) = (Pi) \qquad (10)$$

$$E(P) = \{E_0, E_1, ..., E_7\} \qquad (11)$$

$$E = E + C \qquad (12)$$

Such as i ∊ [0, 7] and E a function Y→Y which Y is a vector of integers.

The process is illustrated by the following diagram:

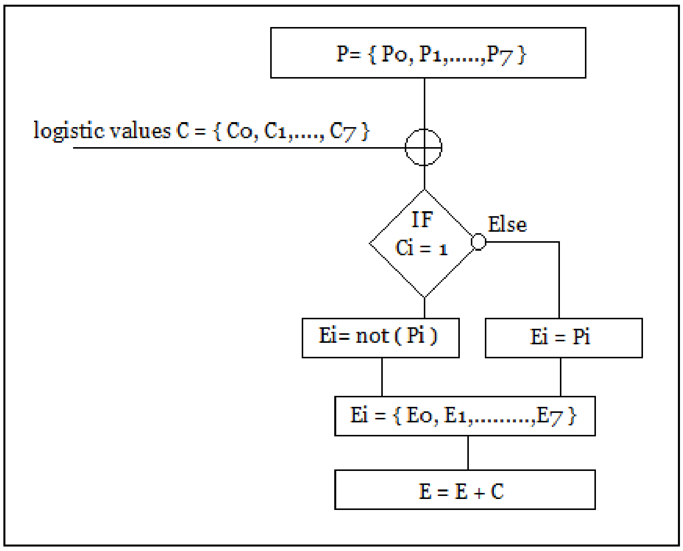
P= { Po, P1,.....,P7 }
logistic values C = { Co, C1,...., C7 }
IF
Ci = 1
Else
Ei= not (Pi)
Ei = Pi
Ei = { Eo, E1,.........,E7 }
E = E + C

Fig. 4. First encryption diagram

D. Second encryption process

The second encryption algorithm could be called a dichotomous shift. The value is converted to the binary base, and subdivided on 2 blocks. Each one of them under-goes a left or right shift. The numbers of rotations are called "c1" and "c2" and they are defined by a logistic function and it cannot be the same for the 2 group. The control parameters for the logistic function are considered as keys called 'key41" and 'key42'.

$$P = \{P_0, P_2, ..., P_n\} \qquad (13)$$

$$P_i = \{a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \ \} \qquad (14)$$

$$R(P_i) = \{a_{0+4-c1}, a_{1+4-c1}, ..., a_{3+4-c1}, a_{(4+c2)}, a_{(5+c2)}, ..., a_{(7+c2)}\} \qquad (15)$$

$$R(P) = \{R(P_1), R(P_2), ..., R(P_n)\} \qquad (16)$$

Such (c1, c2) ∊ [0, 4] and R a function Y→Y which Y is a vector of integers.

In (15), if the index reaches the value 8 is reduced by 4.

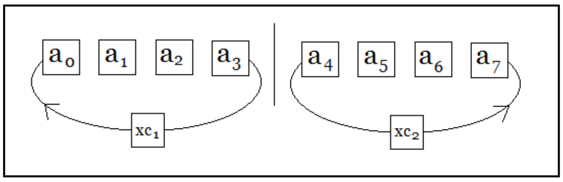

Fig. 5. Second encryption diagram

E. The whole algorithm

The whole approach can be illustrated by the following diagram.

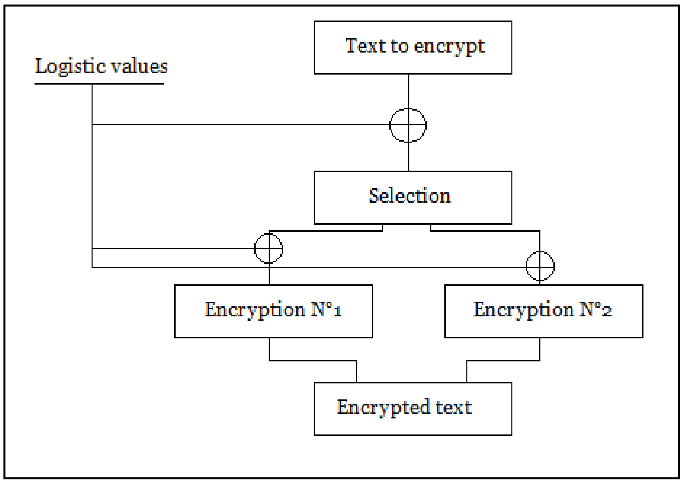

Fig. 6. *The whole approach diagram*

V. Decryption

A. Selection

By the same way, the selection between different decryption systems is based on logistic function which offers us binary output values. Binary 'zero' output means we have to use the first decryption algorithm, if not we use the second one. These outputs are generated by the logistic function which. 'key21' and 'key22' which are sent by user are considered as control parameters.

B. First decryption process

The encrypted value is converted to the binary base, and subdivided on 2 blocks. Each one of them undergoes a left shift if it rotated to the right during the encryption process or right shift if it is rotated to the left during the encryption process. The number of rotation is defined by a logistic function. The control parameters for this function are sent as keys called 'key41" and 'key42'.

$$R = \{R_0, R_2, \ldots\ldots\ldots\ \ldots\ldots\ldots,\ R_n\} \tag{17}$$

$$R_i = \{a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7\ \} \tag{18}$$

$$DR(R_i) = \{a_{0+c1}, a_{1+c1}, \ldots, a_{3+c1}, a_{(4-c2)}, a_{(5-c2)}, \ldots,\ a_{(7-c2)}\} \tag{19}$$

$$DR(R) = \{P_1, P_2, \ldots\ldots\ldots\ \ldots\ldots\ldots,\ P_n\} \tag{20}$$

Such as i ∊ [0, 7] and DR a function Y→Y which Y is a vector of integers. In the first 4 terms in (19), if the index reaches the value 4 it is reduced by 4 and in the last 4 terms if the index decreases to 3 it is increased by 4.

VI. Decryption

Evaluation tools are used to evaluate the encryption performance so we must quantify its performance and characteristics.

A. MSE (mean square error)

We use MSE to quantify the error between the original signal and the encrypted one. It could be defined by the following function:

$$MSE = \frac{\sum_{i=1}^{n} (M_i - M_i{*})}{n} \tag{21}$$

Such as n is the length of the sequence.
M and M* and represent respectively the original signal and the encrypted one.
In our case, MSE=0

B. Correlation

A correlation is a number between 0 and 1 which measures the degree of association between two signals. A positive value for the correlation implies a positive association. A negative value for the correlation implies a negative association. In our case we studied the correlation between the original signal and the signal decoded.
The correlation between the original text and decrypted text is equal to 1 which means that our algorithm is reversible 100%.

C. Histograms

This approach was tested on a text of 410 letters including spaces, commas, points and other special characters. The two following histograms show the effect of the application of this algorithm. Although we note that this approach is effective.

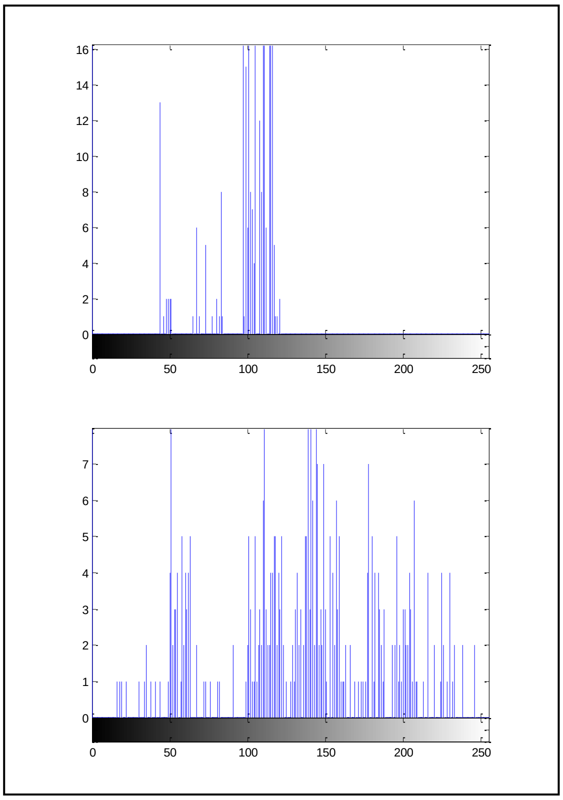

Fig. 7. Respectively Plaint text and cipher text histograms

D. Diagonal correlation

Another useful tool for testing the effectiveness of the algorithm is the diagonal correlation. It shows the relationship of each letter with the letter to neighbors. Diagonal correlation was tested on the same plain text and we got the following result.

E. Interpretation

As seen above, the decrypted text and the original text are the same. So this approach can be mathematically defined as:

$\forall x \in N$ Such as $A(x) = y$ so $\exists\ A^{-1}(y) = x$ with $A \circ A^{-1}(x) = I$ and $A^{-1}(y) - x = \varepsilon$ with $\varepsilon \to 10^{-4}$.

This approach is one hundred per cent reversible and conservative.

F. Conclusion

In this paper we presented a new poly encryption approach that contain all the criterion of an encryption algorithm that is robust: the randomness of the function used which is provided by the chaotic function and the function of the permutation, so that complexity of the key in our case it is ensured by the choice of key, although the choice of encryption methods they have to be conservative and reversible, which is the case in our work.

This approach we guarantee the reversibility and the keeping and impeccable results. It is effective as it is simple.

REFERENCES

[1] University of nevada reno department of science & engineering. Cryptography - IEEE Potentials 0278-6648/01/$10.00 © 2001 IEEE

[2] A. Masoud and A. H. Tewfik, "Geometric Invariance in Image Watermarking," IEEE Trans. Image Processing, vol. 13, no. 2, pp. 145-153, Feb. 2004.

[3] Luo, J.; Shi, H., "Research of Chaos Encryption Algorithm Based on Logistic Mapping", IIH-MSP '06, International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2006, pp. 381-383, Dec 2006.

[4] Rich Schlesinger," A Cryptography Cource for Non-Mathematicians», the 1st annual conference on information security curriculum development, K Kennesaw , Georgia, October 08-08,2004.

[5] 1Sudhir Keshari, 2Dr. S. G. Modani 'Image Encryption Algorithm based on Chaotic Map Lattice and Arnold cat map for Secure Transmission' 1,2Department of Electronics and Communication Engineering, Malaviya National Institute of Technology, Jaipur, India. March 2011