Military Technical College
Kobry Elkobbah,
Cairo, Egypt

8th International Conference
on Aerospace Sciences &
Aviation Technology

Private Key Cryptosystem using One-dimensional Chaotic Map

Alaa Fahmy*

ABSTRACT

A cryptosystem is a family of uniquely reversible transformations from a set of plaintexts into a set of cryptograms. A private key cryptosystem uses a key exchanged by some secure means between two users, the possession of which enables both of them to encrypt and decrypt messages sent between each other. In this paper, we introduce a new application of chaos in cryptography. The main idea is to use one-dimensional (1-D) chaotic map to construct a private key block cryptosystem.

1. INTRODUCTION

The irregular and unpredictable time evolution of many non-linear systems has been dubbed chaos. One of the basic tenets of science is that deterministic systems are predictable. That is, given the initial condition and equations describing a system, the behaviour of the system is always predictable. The discovery of chaotic phenomena has eliminated this viewpoint.

1.1 One-dimensional Chaotic Maps

Consider a real interval I and a function f, which transforms a point x of I into some point x` in the same interval I. This is called a map of the interval

$$f: I \rightarrow I. \tag{1}$$

The one-dimensional (1-D) chaotic maps can be described by:

$$x_{n+1} = f(\mu, x_n), \quad n = 0,1,2,\ldots\ldots, \tag{2}$$

where x_n is called the state, a real numbers on the unit interval (0,1) and μ is a non-linear parameter. The function f has one maximum on the interval I and it maps the state x_n to the next state x_{n+1}. Starting with initial condition $x_0 \in I$, repeated applications of f yield a sequence of points $\{x_n\}$, $0 \le n < \infty$, called the iterate (orbit) of x_0.

---

* Ph.D., Dpt. of Electrical Engineering, Military Technical College, Cairo, Egypt.

Equation (2) can be rewritten as:

$$x_n = f_\mu^n(x_0), \qquad n = 1,2,3,\ldots\ldots, \tag{3}$$

where f^n denotes the nth iterate of f. For a function f, a fixed point x^*, is said to be stable if the magnitude of the slope of f is less than 1 [1], i.e.,

$$|f'(\mu, x^*)| < 1. \tag{4}$$

2. LOGISTIC MAP

One of the simplest, well-known, models of a non-linear dynamical system is the logistic map [2]. It is one-dimensional and non-linear map. It is fully deterministic in the sense that there is no random force and the future is completely determined by the initial condition. The logistic map can be described by the following difference equation:

$$L_\mu(x_n) = x_{n+1} = \mu x_n(1-x_n), \qquad 0 < x_n < 1, \quad 0 < \mu \le 4. \tag{5}$$

The function, L_μ, is two-to-one map and it is said to be a map of the interval (0,1) into itself when the parameter μ in the range $0<\mu\le4$. The parameter μ determines the strength of the non-linearity. Solving the quadratic map, eq. (5), we get its inverse eq. (6), which is one-to-two map:

$$L_\mu^{-1}(x_n) = x_{n-1} = 1/2 \pm 1/2\sqrt{(1-\frac{4x_n}{\mu})}. \tag{6}$$

Figure 1 shows the bifurcation diagram of the logistic map. For $\mu < 3$, all the initial conditions converge to a fixed point. This fixed point becomes unstable and the iterate is attracted to a new fixed point x^*, where

$$x^* = 1 - \frac{1}{\mu}. \tag{7}$$

Increasing $\mu \approx 3.2$, the fixed point x^* becomes unstable and an attracting 2-cycle is born. As μ continues to increase, the long time motion converges to period 4, 8, 16, 32,... cycles. Finally accumulating to a cycle of infinite period for $\mu_\infty \approx 3.57$ and that is the route to chaos. When $\mu \ge 3.9$, the values of x span the entire intervals in an apparently random fashion.

2.1 Main Features of One-dimensional Chaotic Maps

In general, one-dimensional chaotic maps have the following features:
* The sensitive dependence on initial conditions;

* The control parameter μ, which dramatically affects the behaviour of the map;
* The stretching and folding process [3], which is necessary to keep chaotic trajectories within a finite volume of phase space;
* The manifestation of the unpredictability of chaotic dynamical systems, that is, the time evolution is computationally irreducible.

3. PRIVATE-KEY BLOCK CRYPTOSYSTEM

A good cryptosystem is one in which all the security is inherent in knowledge of the key and non is inherent in knowledge of the algorithm [4]. We utilize the main features mentioned above to construct a secure private-key block cryptosystem. In this way, the logistic map, as an example of one-dimensional chaotic maps, is used to construct a private-key block cryptosystem. The general procedures to construct a private-key block cryptosystem, using one-dimensional chaotic maps, are given below.

3.1 Secret Key

Both the sender and receiver use the control parameter μ as a secret key (16-digits or ≈ 54 bits). The secret key μ is selected in the chaotic region ($3.56 \le \mu \le 4.0$) under user control.

3.2 Encryption

Let L_μ, and L_μ^{-1} (double valued function) denote a one-dimensional chaotic map and its inverse respectively. The encryption process consists of the following steps:
(i) Use the ASCII code to convert the alphabetic plaintext M, into a binary form Z.
(ii) Divide the encoded plaintext Z into N blocks of fixed size b ≈ 64 bits (or P= 20-digits)

$$Z = \{z_1, z_2, ..., z_N\}, \tag{8}$$

where the bits of each block are written as

$$z_i = m_1, m_2, ..., m_b, \qquad i = 1,2,....,N. \tag{9}$$

(iii) Pad Z, if necessary, so that its length becomes a multiple of the block size b.
(iv) Use the transformation

$$F: z_i \rightarrow r_i, \tag{10}$$

to transform the binary block z_i into decimal number $r_i \in (0,1)$, with p digits accuracy (P=20-digits), where

$$r_i = \sum_{j=1}^{b} m_j * 2^{-j}, \quad i = 1,2,.....,N. \tag{11}$$

(v) Set r_i as an initial condition x_0.
(vi) Calculate the ciphertext block $s_i \in (0,1)$ by iterating L_μ^{-1} n-times (n = 66)

$$s_i = L_\mu^{-n}(x_0 = r_i). \tag{12}$$

As suggested in [5], the ciphertext block s_i requires some more digits for correct decryption. One can select at random, for example by tossing a coin at each iteration step, one of the two values of L_μ^{-1}.
(vii) Convert the decimal number s_i into a binary one c_i and send it to the receiver.
(viii) Repeat the steps (iv-vii) for each plaintext block to get the binary ciphertext blocks

$$C = \{c_1, c_2, \ldots\ldots, c_N\}. \tag{13}$$

3.3 Decryption

The decryption process begins with receiving the binary ciphertext block c_i and the following steps are performed to recover the original plaintext M:
(i) Convert the ciphertext block c_i into decimal number s_i.
(ii) Set s_i as an initial condition x_0.
(iii) Calculate the recovered plaintext block r_i by iterating L_μ, n-times (n = 66)

$$r_i = L_\mu^n(x_0 = s_i). \tag{14}$$

(iv) Use the transformation

$$F^{-1}: r_i \rightarrow z_i, \tag{15}$$

to transform the decimal number r_i into a binary block z_i.
(v) Use the ASCII code to convert the binary plaintext block z_i into an alphabetic form.
(vi) Repeat the steps (i-v) for each ciphertext block to recover the original plaintext M (in alphabetic form).

4. RESULTS AND DISCUSSIONS

Figure 2 and Fig.3 show the encryption and decryption of a plaintext "FIGURES" (r_i=0.3850537935019245) using the logistic map, where L_μ^{-1} and L_μ, are given by eq. (6) and eq. (5) respectively. Since L_μ^{-1} is double valued function, one plaintext has 2^n ciphertexts and only one is sent to the receiver.

Meanwhile, Fig.4 shows the distribution of ciphertexts, produced by iterating L_μ^{-1}. The resulting ciphertexts are just as random as any stochastic process with a continuous distribution (it follows Chebyshev distribution). Figure 5 shows the error propagation property, where a single bit change in the ciphertext block causes a radical change in the recovered plaintext as the number of iterations is increased. Figure 6 can represent the iterations of eq. (6).

When x_n varies over the interval, the lower value of x_{n-1} varies over the lower half of the interval (left branch of the map) and the higher value of x_{n-1} varies over the upper half of the interval (right branch of the map). After n iterations the interval is divided into

2^n segments each being a map of the interval for one particular combination of choice. Therefore, when the inverse of one-dimensional chaotic map is iterated with an accuracy of P-digits, the width of each segment is 10^{-P} after $n = P/\log_{10}2$ iterations [6].

At that point all information about x_n is lost because the variation of x_n over the interval causes a decrease in the precision of x_n by a factor 2 per iteration. Consequently, any P-digit number of the interval is a code for the unique combination of choices, which would lead to the number in $p/\log_{10}2$ iterations of eq. (6). In principle, ciphertexts generated by eq. (6) with a decision making can be reconstructed in reverse order (as long as the key is known) when the last ciphertext is used as the origin for the iterations of eq. (5).

Since the last ciphertext generated by the inverse of one-dimensional chaotic map does not contain information dating farther back than $P/\log_{10}2$ steps, the reconstruction of the ciphertexts (and consequently the original plaintext) from the last one cannot be carried beyond that point. For correct decryption, the ciphertext size S should be greater than ξ [5] where,

$$\xi = n \log_{10} 2 + \log_{10} 3 + P. \tag{16}$$

Therefore, for a plaintext with P = 20-digits and the times of composite of inverse map n=66, the ciphertext size should be greater than 40.3. Figure 7 illustrates the rate of correct decryption versus the ciphertext size, obtained by a computer simulation. The ciphertext requires more than 50-digits, for correct decryption and it is independent of the secret key.

The constructed private-key block cryptosystem, using one-dimensional chaotic maps, is based on simple repeated iterations. It is required n-times multiplication. Since the memory of computer has finite size, it is necessary to set a computation size. In this way, for a 20-digit plaintext, the number of iterations are set to n = 66. Since the inverse of one-dimensional chaotic maps is one-to-two maps, the number of possible combinations of ciphertexts are 2^n ($2^{66} \approx 7.378 \times 10^{19}$). Since the secret key consists of 54 bits, there are also 2^{54} possible keys.

5. CONCULSION

Chaos is referred to the irregular and unpredictable time evolution of many non-linear systems. This paper introduces a new application of chaos in cryptography. The main idea is to use one-dimensional (1-D) chaotic map to construct a private key block cryptosystem. The forward map L_μ is used for decryption, while the inverse one (L_μ^{-1}) is used for encryption. Since L_μ^{-1} is double valued function, one plaintext has 2^n ciphertexts and only one is sent to the receiver.

The resulting ciphertexts are just as random as any stochastic process with a continuous distribution. A single bit change in the ciphertext block causes a radical change in the recovered plaintext as the number of iterations is increased. The ciphertext generated by the inverse of one-dimensional chaotic map, does not contain information dating farther back than $P/\log_{10}2$ steps (P is the number of accuracy digits).

For a plaintext with P = 20-digits and the times of composite of inverse map n = 66, the ciphertext size should be greater than 40.3 and it is independent of the secret key.

REFERENCES

[1] Mitchell Feigenbaum, "Universal Behaviour in Non-linear Systems," Los Alamos Science 1, pp. 4-27, 1980.

[2] Hao Bai-Lin, Chaos II, Singapore, London: World Scientific, 1990.

[3] G.L. Baker and J.P. Gollub, Chaotic Dynamics, An Introduction, Cambridge: C.U.P, 1990.

[4] Bruce Schneier, Applied Cryptography, Protocols, Algorithms, and Source code in C, John Wiley & Sons, Inc., 1996.

[5] Whitfield Diffie and Martin E.Hellman, "Privacy and Authentication: An Introduction to Cryptography," Proceedings of the IEEE, Vol.67, No.3, March 1979.

[6] C.E. Shannon, "Communication Theory of Secrecy Systems," Bell System Technical Journal, 28, pp. 656-715, 1949.

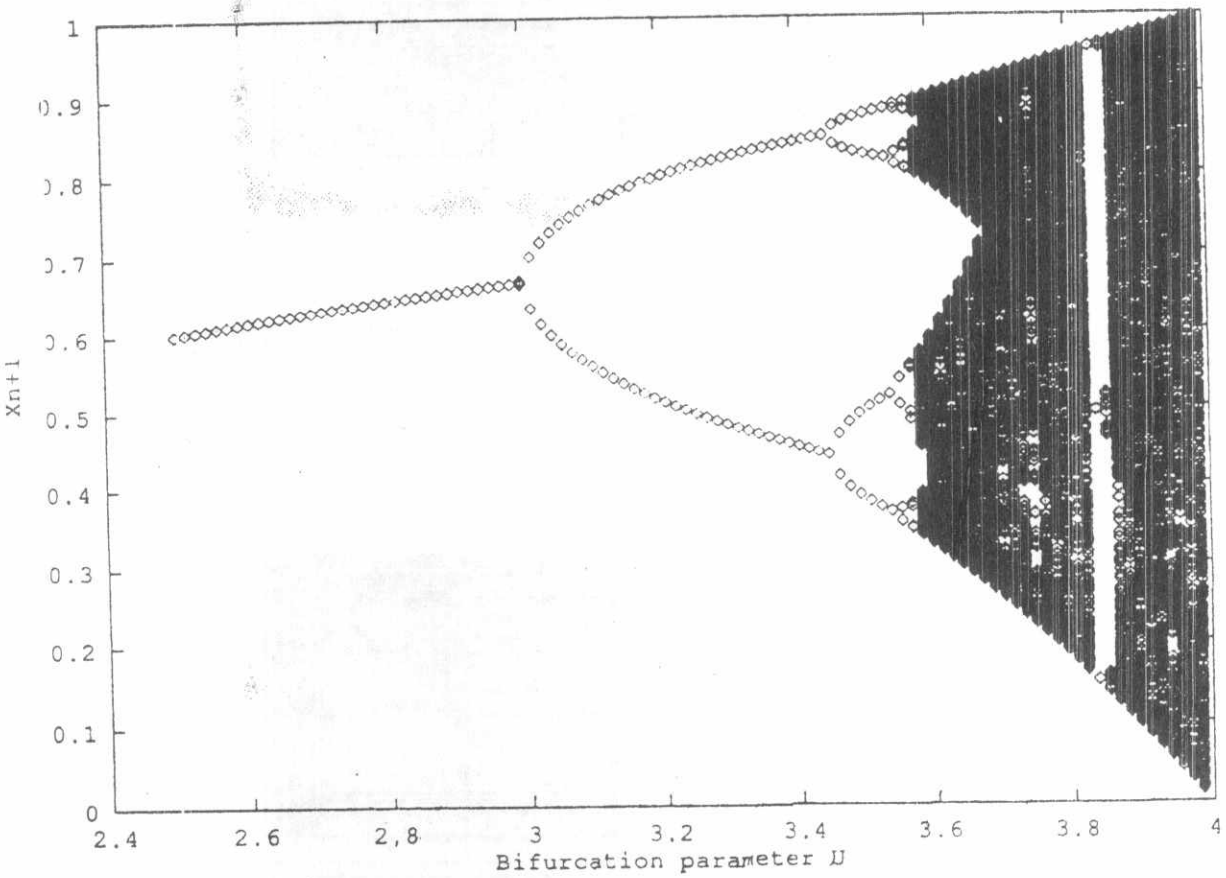

Fig.1 The bifurcation diagram of the logistic map

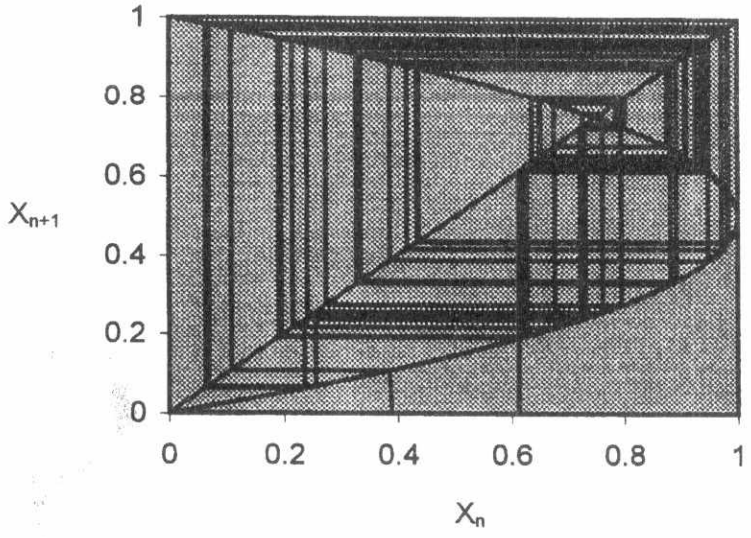

Fig.2 Encryption using the inverse of logistic map

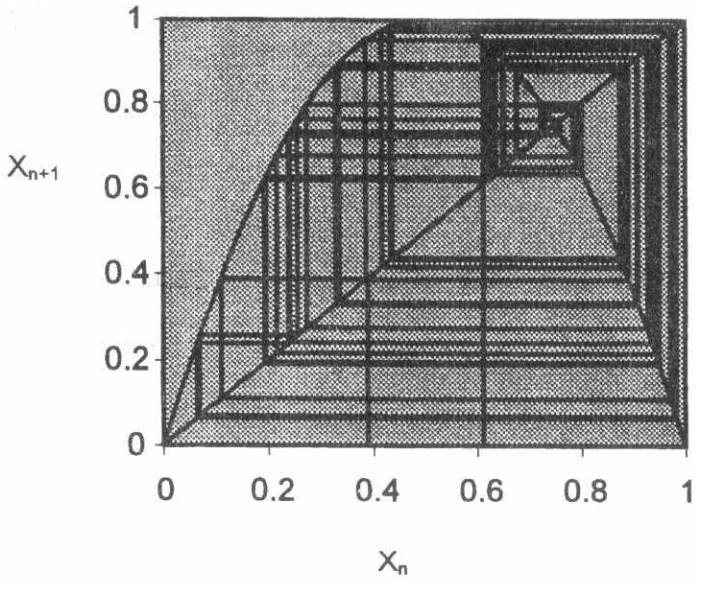

Fig.3 Decryption using logistic map

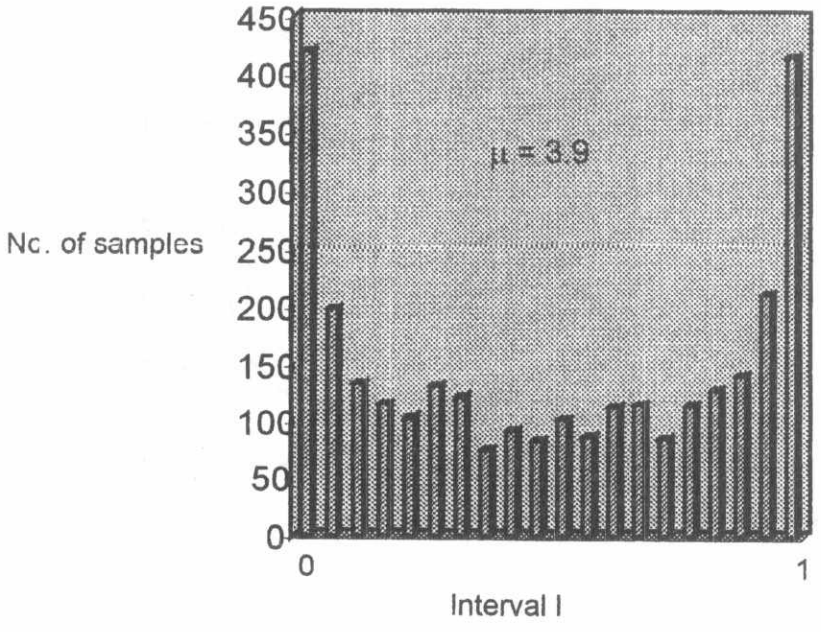

Fig.4 Histogram of the ciphertext produced by the inverse of logistic map

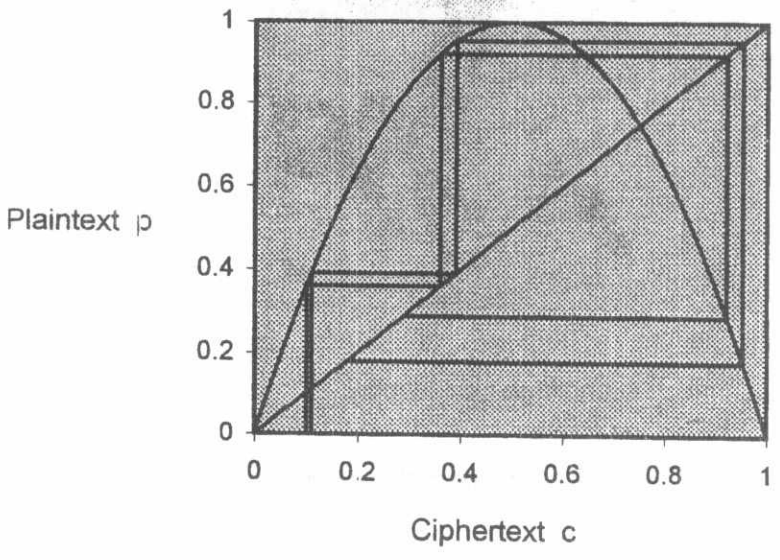

Fig.5 Error propagation property

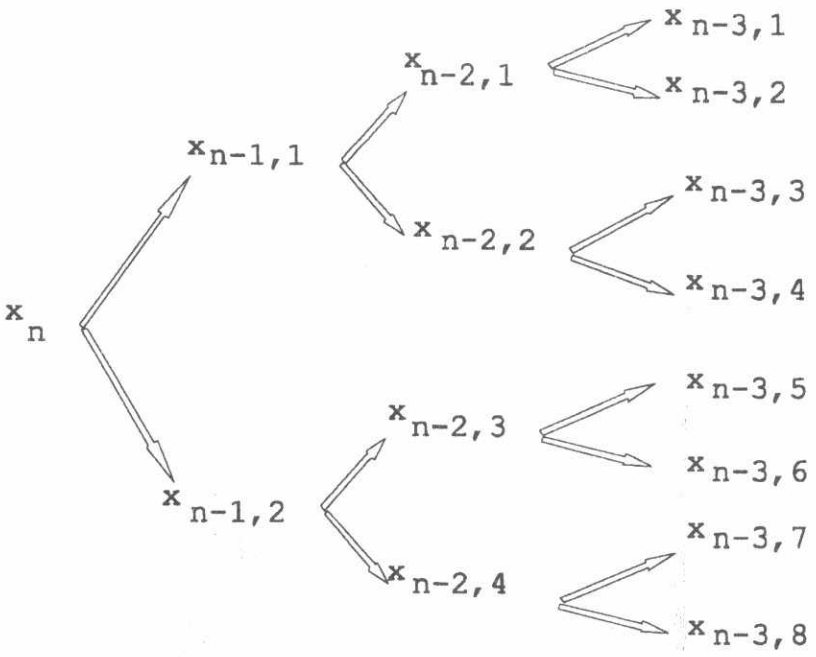

Fig.6 The iterate of 1-D inverse map

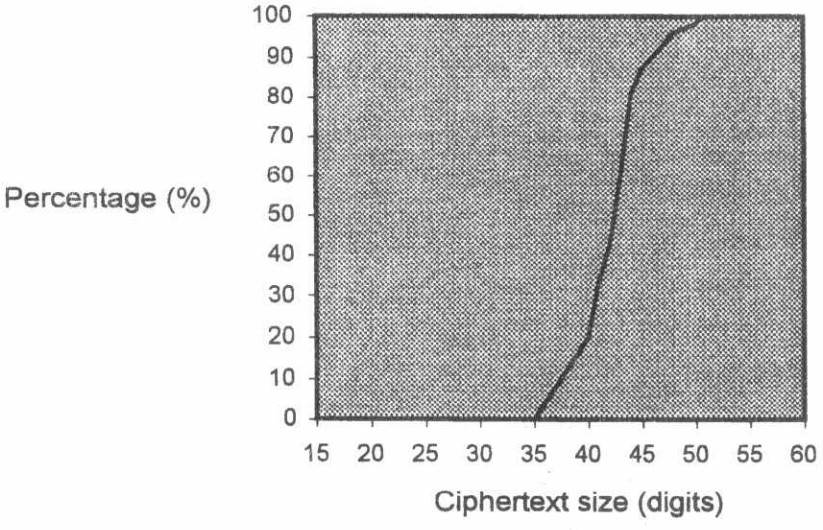

Fig.7 The rate of correct decryption