ELSEVIER

23 March 1998

PHYSICS LETTERS A

Physics Letters A 240 (1998) 50–54

Cryptography with chaos

M.S. Baptista

Institute for Physical Science and Technology, University of Maryland, College Park, MD 20742, USA

Received 30 September 1997; accepted for publication 26 January 1998
Communicated by A.R. Bishop

Abstract

It is possible to encrypt a message (a text composed by some alphabet) using the ergodic property of the simple low-dimensional and chaotic logistic equation. The basic idea is to encrypt each character of the message as the integer number of iterations performed in the logistic equation, in order to transfer the trajectory from an initial condition towards an ϵ-interval inside the logistic chaotic attractor. © 1998 Elsevier Science B.V.

PACS: 05.45.+b
Keywords: Chaos; Cryptography; Message; Security

Deterministic oscillations, called chaos [1], used to be treated as stochastic and unpredictable phenomena. Nowadays, this stochastic-like behavior that chaotic oscillations presents, characterized by a large broadband frequency spectrum, has been used to hide information, in order to safely transmit secret messages.

A first application for transmitting signals using chaos was proposed by Pecora and Carroll [2]. They showed that two similar chaotic circuits can have their trajectories synchronized. Then, the message to be sent is masked in one of the chaotic signals. During transmission, this message is extracted using a synchronous circuit, usually by the receiver.

Another idea for transmitting messages, using chaos, came up from the realization that chaos can be controlled by using small perturbations. In Ref. [3], the transmitter sends a controlled chaotic signal that encodes a binary message. Depending on which two half-planes in a Poincaré section the trajectory crosses, the receiver considers that a 0 or 1 binary digit is being transmitted. In Ref. [4], the transmitter sends a small parameter perturbation the receiver must apply to a chaotic system, in order to target the trajectory to some region in the phase space. The message is recovered by assuming that this region is associated with some alphabet unit. Also, using targeting techniques [5], the transmitter sends a feed back orbit correction the receiver must apply to the trajectory of a chaotic system, in order to make this trajectory reach some ϵ-neighborhood of a point in a pre-established interval of time. Information is then recovered by the receiver, assuming that some alphabet unit is associated with both the time of arrival and the reached ϵ-neighborhood.

In this work, the message to be transmitted is a text composed by some alphabet. As proposed in Refs. [3–5], we also associate portions (ϵ-intervals) of the attractor with alphabet units. However, the encrypted message to be transmitted, the ciphertext, is obtained from a text, the plaintext, neither using synchronous chaotic systems nor control and target techniques, but rather taking advantage of a typical

PII S0375-9601(98)00086-3

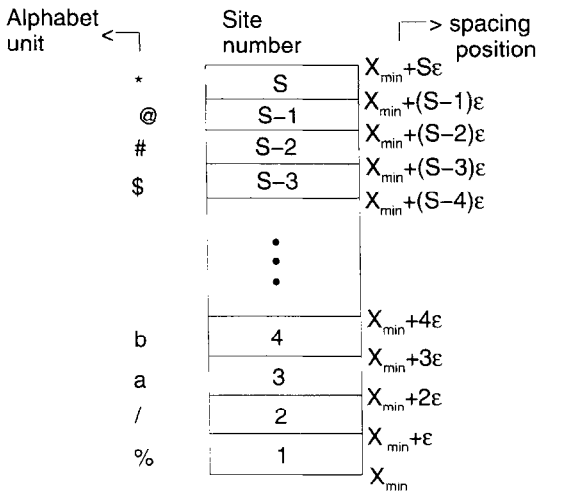

Fig. 1. Schematic representation of how an attractor is divided in S sites, each one with size $\epsilon = (X_{\max} - X_{\min})/S$, where $X_{\max}$ and $X_{\min}$ are some portion (or the whole) of the attractor. For each site an alphabet unit is associated.

property of any chaotic system: ergodicity.

Using the simple one-dimensional logistic map

$$X_{n+1} = bX_n(1 - X_n), \tag{1}$$

where $X_n \in [0, 1]$, for a control parameter b set to make (1) have a chaotic behavior, we can quickly and safely encrypt information for further transmission.

We propose that the encryption of some character is the number of iterations applied in Eq. (1) to make its trajectory, departing from an initial condition X_0, reach an ϵ-interval associated with that character.

In Fig. 1, we show a schematic representation of the way we associate the S-units alphabet with the S ϵ-intervals. Each interval, or site, is the range $[X_{\min} + (S-1)\epsilon, X_{\min} + S\epsilon)$, where, in this work, $S = 256$, $\epsilon = (X_{\max} - X_{\min})/S$, and $[X_{\min}, X_{\max}]$ is a portion of the attractor (it can be the whole attractor).

The number of iterations (the ciphertext) is used together with the secret keys: the S associations between the S ϵ-intervals and the S units of some alphabet, the first initial condition X_0, and the control parameter b (thus, we work with $S+2$ secret keys), allowing the receiver to decrypt the ciphertext (recovering the original character) by iterating Eq. (1) as much times as indicated by the ciphertext. The position of the final point, with respect to the S ϵ-intervals, points out the original character to the receiver.

In the previous paragraph, we referred to X_0 as the first initial condition, because whenever we encrypt a unit of a plaintext (for example, the world "hi" is a plaintext with two units), a new initial condition is considered. If $C1$ is the ciphertext of the first unit in a plaintext, to encrypt the second unit in this plaintext we use as the initial condition $X_0' = F^{C1}(X_0)$, where F^{C1} is the $C1$th iteration of Eq. (1). If $C2$ is the ciphertext of the second unit in that plaintext, the initial condition used to encrypt the third unit in that same plaintext is $X_0'' = F^{C2}(X_0')$. This rule is then straightforwardly applied to the remaining units in the plaintext.

The initial condition is switched to allow different plaintext units to have the same ciphertext unit. Owing to this trick our cryptography method is not of the class of one-by-one transformations, very common in the usual cryptography methods [6].

Note that X_0'' can also be given by $F^{C1+C2}(X_0)$. However, we prefer not to use this last notation, because we want to emphasize that, independently of the initial condition, the ciphertext unit Cn is a number that does not exceed the value 65 532. Besides this condition, the ciphertext units also depend on two parameters, a transient time N_0 and a coefficient η to be defined later.

Concerning the size of the trajectories used in this work, we have to review some points about ergodicity. Owing to ergodicity, an infinite number of trajectories (departing from any X_0) with different sizes reach the same ϵ-interval. As a result, a single unit in a plaintext could be encrypted in an infinite number of ways. However, to work with a such a large number of possibilities is impractical and, in fact, is not necessary.

The reason for which we can consider a low-size trajectory whose size represents an encrypted plaintext unit, relies on the existence of a natural invariant density for chaotic attractors. This invariant density, that is the space distribution of the infinite-size trajectory, can well be described by a finite-size trajectory. In addition to that, due to ergodicity, almost any initial conditions, when iterated, generate an attractor with the same natural invariant density. As chaotic systems are ergodic, almost any initial condition when iterated by such a system will reach any ϵ-interval many times, provided that this interval belongs to the attractor. And the frequency each portion of the attractor is visited depends on this density.

To compute the natural invariant density, but not

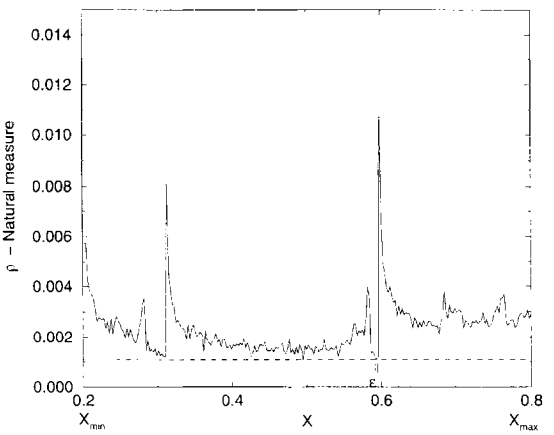

Fig. 2. Natural invariant density of Eq. (1) in the interval $[0.2, 0.8]$, obtained from a trajectory with size $N = 65\,536$. The control parameter $b = 3.78$, and the first initial condition is $X_0 = 0.432\,031\,250\,000\,00$.

in an analytic way, one must consider an N-iteration sized trajectory, starting from some X_0, and to check its distribution in many ϵ-intervals we divide the attractor. We choose to work with trajectories that do not exceed the 65 532-iteration size, such that the number Cn, a unit of the ciphertext, is quickly computed and sent to the receiver by using only one-byte integer transmission.

The natural invariant density of Eq. (1) for $b = 3.78$, obtained for a trajectory with components, $X_n = X_0, X_1, \ldots, X_N$, for $N = 65\,536$, shown in the interval $[X_{\min}, X_{\max}] \rightarrow [0.2, 0.8]$, split in 256 sites, can be seen in Fig. 2. Also, in this figure, the interval $\epsilon = 0.002\,343\,750$, denoted by two parallel lines, has the minimum density distribution over the whole attractor, $\rho \approx 0.0011$, which means that for the considered trajectory, 76 points lie within this interval. In addition, due to the fact that different initial conditions lead to the same invariant density, a 65536-iteration sized trajectory departing from any initial condition (inside the attractor) goes toward any ϵ-interval at least approximately 76 times, if $b = 3.78$.

Even though a different key, b, would result in a different natural density distribution, we can always find, in the case of a chaotic regime, a large number of ϵ-intervals with a non-vanishing density, for a 65 532-iteration sized trajectory. In general, for any chaotic system, one always finds ϵ-intervals with a non-vanishing density if $\epsilon = \alpha N^{-1/D_0}$, where D_0 is the box-counting dimension, and α depends on the system dynamics [7].

We limit the trajectory to have a size lower than 65 532. But we also do not consider the first iterations, the transient time N_0. Those many trajectories (departing from X_0) that go toward the interval indicated in Fig. 2, have different sizes. Suppose that this interval is the one associated with the letter "a". By definition, we represent the size of these different trajectories by n_i^{a} ($i = 1, 2, 3, \ldots$), with $n_{i+1}^{\mathrm{a}} > n_i^{\mathrm{a}}$ and $n_1^{\mathrm{a}} > N_0$, where N_0 is the transient time chosen to be $N_0 = 250$, and n_i^{a} are the possible encrypted characters (obtained from some X_0) of the letter "a", we can send to the receiver.

After disregarding the transient time, we may not have a trajectory that visits any ϵ-interval at least 76 times, for $b = 3.78$. However, since N_0 is very low, our choices are still large. The reason for this transient time is because, if one knows all the S keys, corresponding to the S associations between the S units of some alphabet and the S ϵ-intervals, but one does not have a complete knowledge of either the first initial condition X_0 or b (complete knowledge means we assume one knows these keys with the numerical precision used, that is 16-digits precision), one will not be able to break our cryptography method, since Eq. (1), applied using keys that have a value of 10^{-16}, far different from the real ones (b and X_0), led to different trajectories after 250 iterations, due to the sensitivity to initial conditions chaotic systems have. This need of a 16-digits certainty, in the two keys b and X_0, necessitates a trial-and-error method to break our cryptography (if these are the only unknown keys) in a large number of $10^{16} \times 10^{16}$ attempts.

So far, we constrain the ciphertext unit, Cn, to be a number higher than N_0 and lower than 65 532. But we have many options for Cn (as many, depending on the density distribution). Among those, the transmitter has to choose one to send to the receiver. The way the transmitter decides which Cn will be transmitted depends on the coefficient η, a number that only the transmitter knows. If $\eta = 0$, the message to be sent, Cn, is the number n_1, the minimum number of iterations needed to make the trajectory (departing from some X_0) reach the aimed site associated with the character, provided that $n_1 > N_0$. If $\eta \neq 0$, whenever (for $n_1 > N_0$) the trajectory falls within the aimed site, the transmitter gets a number κ from a random generator (a normal distribution within the interval $[0, 1]$)

and checks whether or not $\kappa \geqslant \eta$. If yes, n_i is considered the number of iterations it takes the trajectory to reach that site; otherwise, the transmitter keeps iterating Eq. (1) until this last inequality is satisfied.

We now encrypt a message using in Eq. (1) the key $b = 3.8$. We divide the attractor (limited by $[X_{\min} = 0.2,\ X_{\max} = 0.8]$) in a number $S = 256$ of ϵ-intervals (sites), for $\epsilon = 0.002\,343\,75$. The association between the sites and the ASCII alphabet (the chosen alphabet to transmit information) is made by using the FORTRAN function char(S), so, the letter "a" corresponds to the site number 97.

For $b = 3.8$, we verify that a 65 532-iteration sized trajectory goes toward any one of these 256 sites at least 60 times, and so no ϵ-interval has a null density. The transient, $N_0 = 250$, is also suitable for $b = 3.8$. In fact, the larger b is, the lower might be N_0, provided that Eq. (1) is chaotic.

For the first application of our method, we consider the coefficient $\eta = 0$, and $N_0 = 250$. Suppose the message to be encrypted is the word "hi", the first initial condition is $X_0 = 0.232\,323\,000\,000\,00$, and the parameter is $b = 3.8$. The letter "h" is associated to the site number 104 that represents the interval

$$[0.441\,406\,250\,000\,00, 0.443\,750\,000\,000\,00),$$

and the letter "i", associated with the site 105 that represents the interval

$$[0.443\,750\,000\,000\,00, 0.446\,093\,750\,000\,00).$$

To encrypt the word "hi", one possible ciphertext (C1 C2) is: 1713 364. The first ciphertext unit (1713) is obtained by iterating Eq. (1) till its trajectory falls within the site 104, provided that the number of iterations $n_1^h > N_0$. For obtaining the second ciphertext unit, we reset the initial condition to $X_0' = X_{1713}$, and iterate Eq. (1) until its trajectory falls within the site 105, provided that the number of iterations $n_1^i > N_0$.

These numbers are sent to the receiver who can recover the hidden message by checking that iterating Eq. (1) 1713 times, with $X_0 = 0.232\,323\,000\,000\,00$, the obtained point $X_{1713} = 0.441\,609\,054\,471\,36$, whose location is within the site 104, represents the letter "h". Then, the receiver resets its initial condition by setting $X_0' = 0.441\,609\,054\,471\,36$, and iterates this new initial condition 364 more iterations obtaining $X_{364} = 0.444\,865\,723\,626\,42$ which is within the site 105, associated with the letter "i".

We clearly see that the next ciphertext unit depends on the previous ciphertext unit, as chaotic systems depend on the initial condition. This dependence can be understood when we reset the initial condition by setting, as in the former example, $X_0' = X_{1713}$. We see that iterating Eq. (1), using this new initial condition, the point X_{364} reaches the site 105. However, for any other slightly different initial condition, we cannot guarantee that after 364 iterations the trajectory will eventually fall within the site 105. A consequence of this fact is that the frequency distribution of the units of a ciphertext depends only on the chaotic system used to encrypt the plaintext, and not on the type of the language of the plaintext.

For $\eta = 0$, further encryption of the word "hi", for an unchanged set of keys, b, and X_0, would always result in the same encryption. This is one of the shortcomings we can overcome by introducing the coefficient η. On the other hand, if we assume $\eta = 0.7$, without changing the keys, b, and the first initial condition X_0, the ciphertext of the word "hi" could be either 2471 1352 or 6581 15763. In fact, this simple two-letters word could be encrypted in at least 60^2 different numbers of ways, without changing the set of keys.

If we consider changing the first initial condition each time we transmit this same two letter word, for example, by making $X_0 = X'$, then the number of possible cipher texts would increase to almost $10^{16} \times 60^2$.

Another advantage of the coefficient η is the property of flattening the frequency distribution of a long ciphertext (or many short cipher texts joined). This flattening effect is very important, since the distribution of a generic ciphertext created using our method, though neither dependent on the type of language (English, Portuguese, German, ..., or randomly created texts) nor on the initial condition, does depend on the secret key b. Thus, in order not to let any eavesdropper find out an approximate value of b by doing a frequency distribution analysis [6], we have to work with the coefficient η.

To show the efficiency of the coefficient η, we apply our cryptography method (using $b = 3.8$ and $X_0 = 0.654\,765\,465\,000\,00$) to a text in English composed of 28 000 characters. After creating the ciphertext, for $\eta = 0$ and $N_0 = 250$, we analyze its frequency

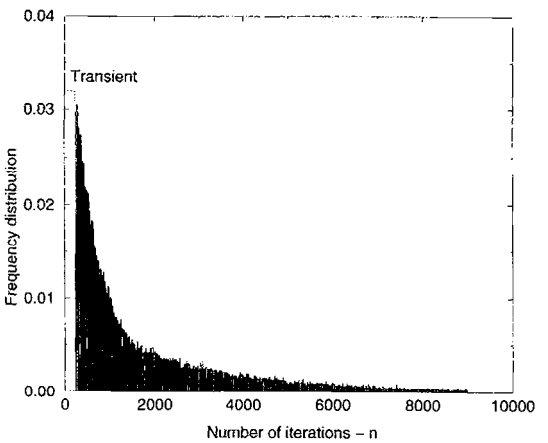

Fig. 3. Frequency distribution of a ciphertext obtained using our cryptography method (with $b = 3.8$ and the first initial condition, $X_0 = 0.654\,765\,465\,000\,00.$) in a 28 000 letter English text. Black bars correspond to a coefficient $\eta = 0$ and gray bars to $\eta = 0.7$.

distribution shown, in Fig. 3, by the dark black bars. We see that there is an exponential-type decay behavior, and this shape has a slope that is dependent on the key b. When we reapply our method to the same text, using $\eta = 0.7$, we see that the frequency distribution, shown by the gray bars, has been flattened.

In fact, the larger η, the flatter the frequency distribution of the cypher text. However, the larger is η, the higher might be the number of iterations needed to make the trajectory go toward the sites. We do not want this number to exceed 65 532. To achieve this requirement, we have worked with coefficients $\eta \leqslant 0.99$.

We show that the ciphertext unit is sent to the receiver by using only one-byte integer transmission, which is an advantage of our method over previous methods that used chaos for transmitting information [3–5]. Another favorable feature of working with integers is that its transmission is noise robust, and also, that we are not sending the message together with the chaotic signal, which would allow an eavesdropper to reconstruct the system dynamics [7] that generate the chaotic signal, and so identify the message. High-dimensional systems, whose dynamics reconstruction might be difficult, are no longer required. Thus, the simple low-dimension Eq. (1) can be used for cryptography.

An improvement in the security, often used in cryptography [6], would be to consider a periodically switching of the keys. Whenever a change in the keys must be done, no hard computation is required for a prompt encryption, but only a check if the ϵ-intervals have a non-null density distribution for the 65 532-iteration sized trajectory. In other methods [3–5], all targeting computations must be performed again, before starting sending any messages. On the other hand, instead of changing the keys, we rather can change only the coefficient η, a job performed by the transmitter only.

The method is based on numerical experiments. Thus, it might be machine dependent. However, to discard this inconvenience, we have also worked with an induced cut-off digit precision smaller than the double numerical precision. For example, the point $X_n = 0.368\,212\,981\,267\,567\,8$, before iterated, would have its value cut off at the fourteenth digit precision $X_n = 0.368\,212\,981\,267\,560\,0$. Using this cut-off, we successfully applied the method considering that the receiver has a different machine than the transmitter.

If a more complex alphabet is required, say a 65 523-unit alphabet, still considering 1-byte numbers of associated sites (256), each plaintext unit (in this 65 523-unit alphabet) could be associated with two of the 256 sites, since any two-byte integer smaller or equal than 65 523 can be decomposed by two one-byte integers. Therefore, for a 2^{8m}-unit alphabet we must send the receiver m one-byte integers.

I would like to thank Professor J. Yorke, Dr. E. E. Macau and Dr. E. Rosa for useful discussions, and Dr. R. Viana for a critical reading of the manuscript. This work was partially supported by the Brazilian financial agency CAPES, the Institute for Physical Plasma research, and U.S. Department of Energy (Mathematical, Information, and Computational Sciences Division, High Performance Computing and Communications Program).

References

[1] T.Y. Li, J.A. Yorke, Amer. Math. Monthly 82 (1975) 985.
[2] L.M. Pecora, T.L. Carroll, Phys. Rev. Lett. 64 (1990) 821.
[3] S. Hayes, C. Grebogi, E. Ott, A. Mark, Phys. Rev. Lett. 73 (1994) 1781.
[4] J. Schweizer, M.P. Kennedy, Phys. Rev. E 52 (1995) 4865.
[5] D. Gligoroski, D. Dimovski, L. Kocarev, V. Urumov, L.O. Chua, Int. J. Bifurcation Chaos 6 (1996) 2119.
[6] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Appl. Cryptography (CRC Press, New York, 1996).
[7] E. Ott, Chaos in Dynamical Systems (Cambridge University Press, New York, 1993).