This article was downloaded by: *[Roda, Fernando]*
On: *19 November 2010*
Access details: *Access Details: [subscription number 929825795]*
Publisher *Taylor & Francis*
Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK

Information Security Journal: A Global Perspective
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t768221795

Chaotic Cipher Using the Duffing Equation

Fernando Roda[a]; Luis Lara[bc]
[a] Industrial Department, CONICET-FCEIA, Universidad Nacional de Rosario, Rosario, Argentina [b] Physics Department, FCEIA, Universidad Nacional de Rosario, Rosario, Argentina [c] FRR, UTN - Information Systems Department, Rosario, Argentina

Online publication date: 19 November 2010

To cite this Article Roda, Fernando and Lara, Luis(2010) 'Chaotic Cipher Using the Duffing Equation', Information Security Journal: A Global Perspective, 19: 6, 320 — 327

To link to this Article: DOI: 10.1080/19393555.2010.514889

URL: http://dx.doi.org/10.1080/19393555.2010.514889

PLEASE SCROLL DOWN FOR ARTICLE

Full terms and conditions of use: http://www.informaworld.com/terms-and-conditions-of-access.pdf

This article may be used for research, teaching and private study purposes. Any substantial or systematic reproduction, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The accuracy of any instructions, formulae and drug doses should be independently verified with primary sources. The publisher shall not be liable for any loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.

Information Security Journal: A Global Perspective, 19:320–327, 2010
Copyright © Taylor & Francis Group, LLC
ISSN: 1939-3555 print / 1939-3547 online
DOI: 10.1080/19393555.2010.514889

Taylor & Francis
Taylor & Francis Group

Chaotic Cipher Using the Duffing Equation

Fernando Roda[1] **and**
Luis Lara[2,3]
[1]CONICET-FCEIA, Universidad Nacional de Rosario, Industrial Department, Rosario, Argentina
[2]FCEIA, Universidad Nacional de Rosario, Physics Department, Rosario, Argentina
[3]FRR, UTN - Information Systems Department, Rosario, Argentina

ABSTRACT We propose a plain files cipher by means of a stream cryptosystem scheme with chaotic addition and a symmetric key. The sequence of numbers used for encryption is generated by a continuous chaotic dynamical system; in particular, we choose the forced Duffing equation since this kind of systems is sensitive to the initial conditions. In a chaotic system, the answer can became periodic during the process of numeric integration. We introduce an heuristic method to break this periodicity.

KEYWORDS chaotic system, cryptography, Duffing equation

Downloaded By: [Roda, Fernando] At: 15:44 19 November 2010

INTRODUCTION

Information transmission through free access media, such as the Internet, demands confidentiality, which mean that nonauthorized people should not be able to manipulate data or just read it. Cryptography makes use of mathematical and numerical methods to hide data such as messages or files so that only the intended information addressees can get them by applying decryption techniques that only they know. For centuries, cryptographic systems have been used with different purposes. In the last decades, cryptography has been applied in computer science with great success, allowing the encryption of a wide variety of files for safe transmission and storage (Schneier, 1996). Cryptography, considered as a discipline from information security, has essentially four objectives:

1. Confidentiality or secret.
2. Informative integrity.
3. Emitter authenticity.
4. Nonrejection either by the sender or the receiver.

As far as ciphers' classification is concerned, and according to the chosen encryption scheme, it can be classified in stream or block cipher. A block cipher operates with fixed-length groups of bits, termed *blocks*, with an unvarying transformation. This kind of cipher uses a block of plaintext and a key as inputs, and returns a block of ciphertext of the same size as output. On the other hand, a stream cipher operates on individual digits, one at a time, and the transformation varies during the encryption. It creates an arbitrarily long stream of key material, which is combined bit-by-bit or character-by-character with the

Address correspondence to
Fernando Roda, CONICET - FCEIA,
UNR (Universidad Nacional de Rosario),
Industrial Department, Av. Pellegrini 250,
2000 Rosario, Argentina.
E-mail: ferrodamarani@yahoo.com.ar

Downloaded By: [Roda, Fernando] At: 15:44 19 November 2010

plaintext. The distinction between the two types is not always clear: A block cipher, when used in certain modes of operation, acts effectively as a stream cipher.

Independently from the selected encryption scheme, ciphertext should have a pure random distribution in order to successfully hide data without any evidence of the original frequency patterns, so that if the file to encrypt is a text, the outgoing message will lose the language source. Consequently, a goal in cipher schemes is to achieve a histogram as random as possible, and this is why in the last decades the interest in the dynamic systems with chaotic answer has constantly grown. They are useful in different fields such as physics, mathematical, and engineering and are characterized by presenting an unpredictable evolution, whose behavior is sensitive to their parameters and initial conditions.

These latter proprieties are responsible for the recent years growing tendency to use both continuous and discrete chaotic systems to design cryptosystems capable of generating robust ciphering against statistical attacks (Stinson, 1995; Menezes, Oorschot, & Vanstone, 1997; Pecora & Carroll, 1990; Boccaletti, Grebogi, Lai, Mancini, & Maza, 2000; Grebogi, Lai, & Hayes, 1997). A Logistic map is perhaps the simplest example of a discrete chaos. It models the population growth and can be expressed as:

$$X_{\mathrm{n}+1} = \lambda X_{\mathrm{n}}(1 - X_{\mathrm{n}}), \tag{1}$$

where X_0 and λ are, respectively, the initial condition and the system parameter. It has been shown that Equation (1) has a period doubling route to chaos in the system parameters range from 1 to 4. A well-known cryptosystem making use of the logistic map was developed by Batista (1998). The basic idea was 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 interval previously associated to the character.

In this paper, unlike other publications which based on discrete dynamics, we propose a stream ciphering scheme with a symmetrical key derived from the chaotic properties that enclose some continuous dynamic systems.

DUFFING EQUATION

In the literature (Amigo, Kocarev, & Szczepanski, 2007; Pareek, Patidar, & Suda, 2003; de Oliveira & Sobottka, 2008; Vaidya & Angadi, 2003; Wong, Ho, & Yung, 2003), different equations have been used in chaotic cryptosystems, many of which are based on discrete one-dimensional chaotic systems. However, our method uses a two-dimensional dynamic system described by Duffing's equation. The equation is:

$$\begin{gathered} my' + cy + kx + \beta x^3 = f_0 \cos wt, \\ x' = y \qquad (2) \\ where' = \frac{d}{dt} \end{gathered}$$

This is a nonlinear second order equation that was first studied by G. Duffing in 1918 and is used in different disciplines. On a mechanic system, equation terms can be interpreted as follow: cy is a viscous dissipation force, $-(kx + \beta x^3)$ represent a restoring force that came from de potential $V(x) = k/2\, x^2 + \beta/4\, x^4$ and the term f_0 *cos wt* is due to a external force. In our application, we take $k = -1$ and $m = b = c = w = 1$.

This dynamical system exhibits chaotic behavior for certain values of f_0 because of the nonlinearity of its equations and being a not homogeneous term (Chicone, 1999; Hale & Kocak, 1996; Strogatz, 1994).

It is almost impossible to find exact solutions when the equations are nonlinear. There are several methods for the numerical resolution, as this is a subject in constant development (Garcia, Martin, & Gonzalez, 2002; Press et al., 1986; Parker & Chua, 1989; Hairer, Norsett & Wanner, 2000; Hindmarsh & Petzold, 1995). We used the Runga-Kutta method of order 8 to integrate the Duffing equation because of its numerical stability. An aspect to emphasize is that it is not advisable to take very long integration intervals since numerical methods accumulate errors generated in each stage of integration, and this produces spurious solutions. In Figure 1 we can observe the dynamics of the system for some values of parameter f_0; for $f_0 = 0.6$ (solid line) the variable x has a periodic behavior, whereas for a slightly higher value of $f_0 = 0.8$ (dashed line) the dynamics is chaotic.

Another important feature of chaotic systems is the sensitivity of the solution with respect to small

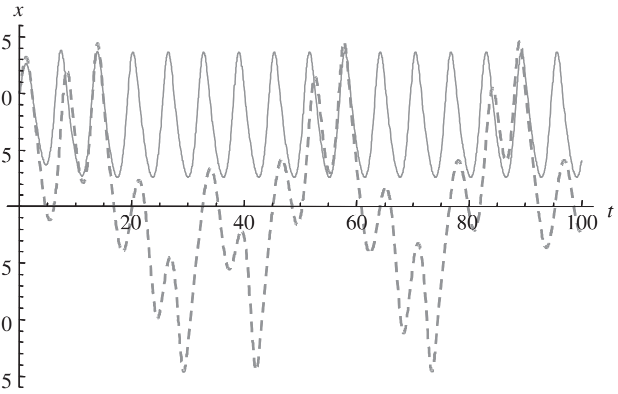

FIGURE 1 X Progression Versus Time.

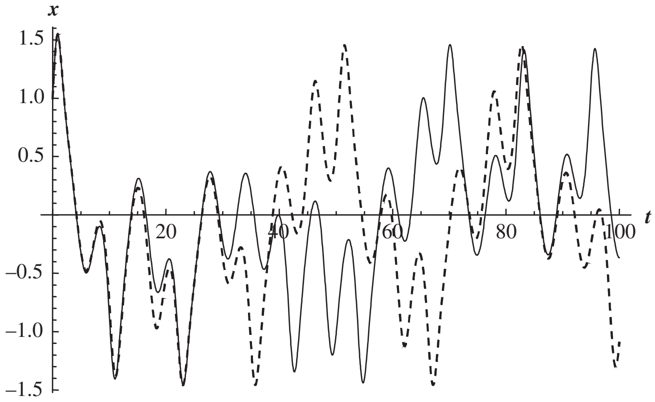

FIGURE 2 Sensitivity under an initial conditions change.

fluctuations in the initial conditions. In Figure 2 we compared two different solutions of the Duffing equation. The solid line represent a solution in which the initial conditions are x(0) = 1, y(0) = 1; for the other solution (represented by the dashed line), the initial conditions have been slightly modified to x(0) = 1 and y(0) = 1.03. Although a numerical experiment is not a demonstration, Figure 2 qualitatively showed that they are sensitive to changes in the initial values and that there is an initial stage in which both solutions are similar but finally become separated.

The numerical solution of the differential equation may be periodic due to numerical truncation produced by computer finite representation. It is a nondesirable feature in a good stream algorithm. In the same way, if the local error produced by the truncation of the method is not properly controlled, it will miss the desired chaotic behavior. To illustrate, let us consider that in the Taylor second-order scheme, when increasing the integration step *h* above a certain critical value, solution stops being chaotic to become into a periodic one as shown in Figure 3.

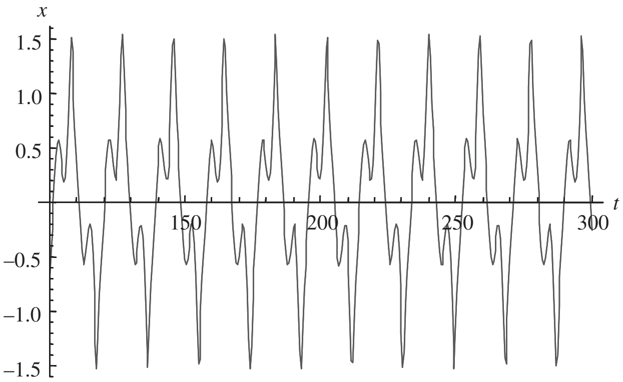

FIGURE 3 Truncation effect in finite representation.

Therefore, when designing the resolution method, it is also important to select carefully the integration step.

PROPOSED METHOD

Though there are interesting papers on cryptography based on discrete dynamic systems (Amigo, Kocarev & Szczepanski, 2007; Pareek, Patidar, & Suda, 2003; de Oliveira & Sobottka, 2008; Vaidya & Angadi, 2003; Wong, Ho, & Yung, 2003), we present here an alternative encryption scheme using a continuous one. The proposed algorithm uses a sequence of chaotic values of *x* and *y* generated by Duffing equation in order to cipher the bytes of the original file one by one. Although it operates with 1-byte blocks, the technique used in encryption is essentially a stream cipher. As we have noted, while dynamics is continuous, the numerical solution of this equation is discrete, and we should select equidistant values in time with separation D to form a discrete table. In order to obtain a suitable succession for stream cipher, their elements must have a low autocorrelation.

Then, let:

- X_i : be *i*-th value of the discrete succession of *x*.
- X_{i-p}: be the element of the discrete succession of *x* that is *p* positions before X_i.

In Figure 4, we analyzed the correlation between X_i and X_{i-p} as function of the displacement p for different values of D. It has been considered the following values of *D*: 1 (line of point and ray), 0.25 (solid line) and 0.1 (dotted line). As expected, the graph shows that the smaller interval *D*, the greater correlation between successive terms. Thus we choose to construct successions

Downloaded By: [Roda, Fernando] At: 15:44 19 November 2010

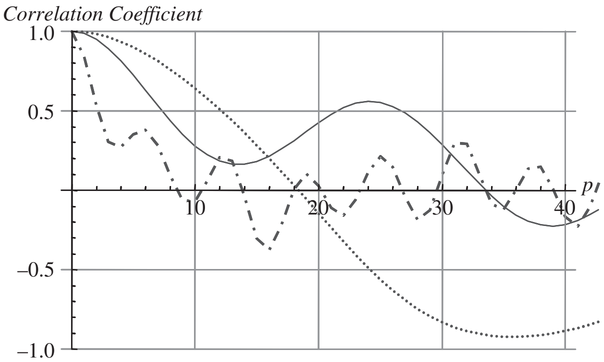

FIGURE 4 Correlation coefficient versus displacement p.

of x and y taking a distance of $D = 1$. We introduce them as X_i and Y_i, respectively.

In order to explain the proposed method we introduce the following steps:

1. Set the system parameters, as we will define later. They include the initial conditions x_0 and y_0 obtained from the secret key.
2. Using these initial conditions, numerically integrate the Duffing Equation (2) with Runga-Kutta method of order 8 to obtain two lists of values

$$\begin{aligned} X_i &= \{x_0, x_1, x_2, \ldots\} \\ Y_i &= \{y_0, y_1, y_2, \ldots\} \end{aligned} \tag{3}$$

where $x_0 = x(0)$, $x_1 = x(h)$, $x_2 = x(2h)$, etc., and h is the integration step.
3. Our goal is to make use of these values to construct a suitable keystream. So that this procedure would be effective to prevent to non-authorized people to accede to the information without having the complete key, we must achieve that by a small change in the key (such as a digit modification) the system should produce a keystream totally different from the original. Consider again Figure 2, where there is an initial interval in which the solution is not sensitive to those fluctuations. Therefore. in the numerical integration, we will discard the first values of *x(t)* and *y(t)* while preserving that obtained for $t \geq 100$.
4. As we analyzed at the beginning of the section, to provide a low autocorrelation take only values of *x* and *y* with a distance of $D = 1$ time units. Then we redefine (3) as

$$\begin{aligned} X_i &= \{x'_0, x'_1, x'_2, \ldots\} \\ Y_i &= \{y'_0, y'_1, y'_2, \ldots\} \end{aligned} \tag{4}$$

Therefore $x'_0 = \mathrm{x}(100)$, $x'_1 = \mathrm{x}(100 + \mathrm{D})$, $x'_2 = \mathrm{x}(100 + 2\mathrm{D})$, and so forth.
Taking $\mathrm{D} = 1$. $x'_0 = \mathrm{x}(100)$, $x'_1 = \mathrm{x}(101)$, $x'_2 = \mathrm{x}(102)$.
5. We are now able to build the keystream $s_{\mathrm{i}.}$ It is constructed with q elements of X_i followed by q elements of Y_i standardized to integers in the domain [0,255]. Here, *q* is a system parameter and it must be set carefully at the beginning of the process. Then

$$s_{\mathrm{i}} = \left\{x'_0, x'_1, \ldots, x'_q, y'_0, y'_1, \ldots, y'_q, \ldots\right\} \tag{5}$$

6. Next we are going to cipher the first 2q character of the plaintext. Let:
   - m_i: be the i^th^ character (in ASCII code) of a flat file to cipher (source file).
   - s_i: be the i^th^ value of the keystream arranged according to the criteria explained above.
   - c_i: be the i^th^ character (in ASCII code) of the ciphered file or ciphertext.

   Then the ciphering of character m_i is obtained by means of the addition:

$$c_i = (s_i + m_i) Mod\, 256 \tag{6}$$

7. To continue the encryption of the next character, we propose to reintegrate (2) with new initial conditions. These are obtained as follows:

$$\begin{aligned} x_0^* &= X_{end} \\ y_0^* &= (Max[y] - Min[y] \times \tfrac{F}{255} + Min[y]) \end{aligned} \tag{7}$$

where $F = m_i \oplus m_{i-1} \oplus m_{i-2} \oplus \ldots \oplus m_{i-q}$; x_0^*: is the new initial condition for x; y_0^*: is the new initial condition for y; X_{end}: is the last observed value of x for the current solution (it was x_{q} in the first iteration); $\oplus$ is the binary XOR operator; and $Max[y]$ and $Min[y]$: are the maximum and minimum values of the sequence Y_i from the current solution.
Note that by construction $0 \leq F \leq 255$, and that it depends on the string. $Max[y]$ and $Min[y]$ is obtained from the sequence of q previous values of y.
8. Thus we obtain new lists X_i, Y_i and the process is repeated from step 3) to 8) until the encryption of the entire plaintext is completed.

Downloaded By: [Roda, Fernando] At: 15:44 19 November 2010

Downloaded By: [Roda, Fernando] At: 15:44 19 November 2010

There are two remarkable features in this algorithm:

1. Since the Duffing system is two-dimensional and for every n x_i-values there are n y_i-values in correspondence, we can encrypt $2n$ characters, being this feature an additional advantage compared with one-dimensional systems because it reduces the length of integration.
2. We have adopted the approach that, every q elements X_i and Y_i, the Duffing equation is re-integrated with new initial conditions. It has two significant outcomes: the first one is that the cipher is sensitive to changes in the plaintext as we will analyze in the next section. The second one is the elimination of cycles in the x and y sequences, present when a chaotic map becomes discrete on a digital computer.

One of the weakest cryptosystems facets is the key, so a way to enhance its security is to increase the number of bits in the key. When cryptosystems are based on dynamical systems, the key is usually associated with the initial conditions.

Since in a computer implementation, the initial conditions are real numbers, its dimensions are 32, 64, or 128 bits, depending on the used arithmetic. We have employed a two-dimensional system, which requires a word for each initial value. This increases the key dimension over one-dimensional systems.

Relative to the key scheme, our system is classified as symmetric, making use of a private key. In such systems, both sender and receiver use the same secret key at each end of communication. The receiver applies the secret key to a decryption algorithm whose operation is inverse to that used in encryption. In the proposed scheme, the feasibility of this operation is guaranteed, since during decryption, the process retrieves the m_i-characters as resulting from the subtraction $(c_i - s_i) Mod$ 256. Thus it obtains q necessary elements to change the initial conditions and go on with the process.

We proposed a simple key scheme, composed of two sequences of up to seven numeric digits each one. These are converted to a single precision floating-point representation (as in IEEE 754 of 32 bits each), in which the sequence is taken as the positive decimal part and the exponent value is set to 1. It produces two numbers to be used as initial conditions x_0, y_0. For example, the sequences 01234567, 76543210 will result in the initial conditions $x_0 = 0.1234567$, $y_0 = 7.654321$. Although the Duffing′s chaotic behavior depends essentially on the values of its coefficient, we took the initial conditions near the stable fixed point of the homogeneous equation on x(0) = 1,y(0) = 0 in order to always get chaotic orbits.

In summary, we have developed a symmetric-key algorithm based on the integration of the Duffing equation in a chaotic regime. From this one, q values of x and q values of y are determined in order to cipher $2q$ bytes of the source file. Then initial conditions are changed using the information of the source text and the procedure is repeated again to cipher other $2q$ bytes, until the source file is completely encrypted.

RESULTS

We have considered three important properties to be fulfilled in the cryptosystems development:

1. Sensitivity with respect to the original message: a change in a character must generate a totally different ciphertext.
2. Sensitivity with respect to the key: a change in one digit of the key results in a totally different ciphertext.
3. The ciphertext obtained must have the appearance of a text generated as random pattern with no evidence of the frequency of the original message.

In order to evaluate these properties, in the examples given below we have used a 218828 KB text file with a Spanish message and we have set the following parameters: $q = 10$, $f_0 = 0.8$, $y_0 = 1$, $x_0 = 0.5$ (or as specified in each case).

To analyze the first goal, in Figure 5 we included two sequences of encrypted characters. The dashed line represents the interpolation of encrypted characters (in code ASCII) of the original message (the last one represented by the solid line) and the dotted line corresponds to the encryption of an analogue message in which the nineteenth character was changed from ‘a’ to ‘h’. The graph clearly shows that both curves are separated, giving evidence of the generation of different ciphertexts.

Regarding sensitivity with respect to the key-change, in Figure 6 we have shown encrypted ASCII characters with two slightly different keys. Dotted line represents the resultant ciphertext using a key generating

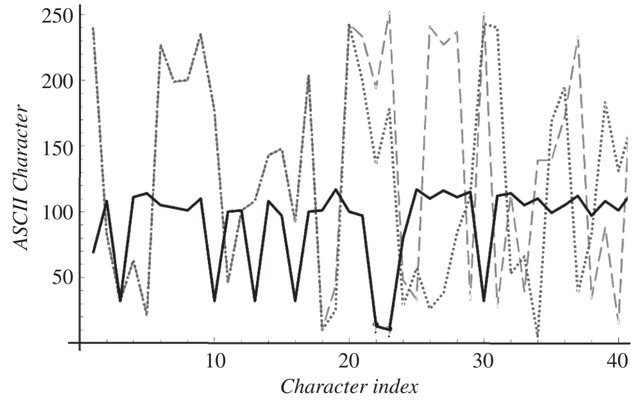

FIGURE 5 Sensitivity with respect to the alteration of the text.

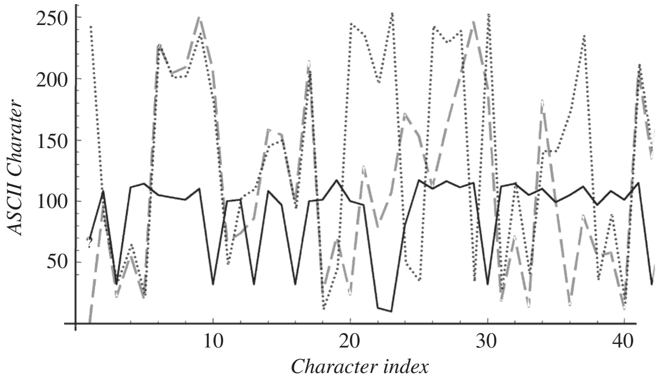

FIGURE 6 Sensitivity with respect to a key change.

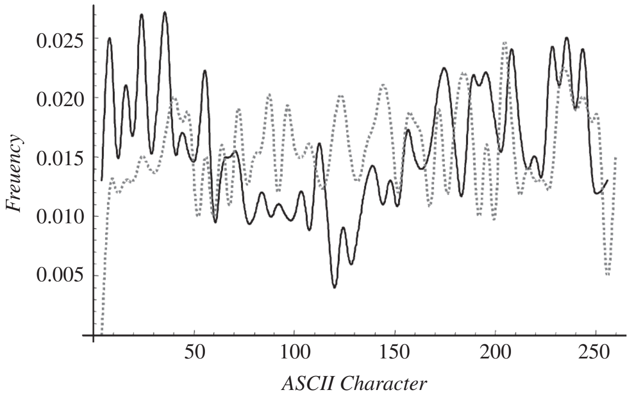

FIGURE 7 Ciphertext distribution versus a random one.

the initial conditions $x_0 = 1, y_0 = 0.5$. Dashed line shows the ciphertext for the initial conditions $x_0 = 1$, $y_0 = 0.501$. In the graph we can check up on the differences between both ciphertexts showing the cryptosystem's sensitivity with respect to the key.

Finally, we qualitatively analyzed the ciphertext distribution in search of randomness. We used pseudorandom numbers from a programming language in order to obtain a random plain file. In Figure 7 we show its frequency distribution (dotted line) and the corresponding one for the ciphertexts obtained using the developed algorithm with a Spanish text (solid line). In this graph it can be observed that both curves have an almost uniform distribution in the whole range, from 0 to 255. Furthermore, the plaintext frequencies cannot be distinguished in the ciphertext distribution.

Now we introduce a run time survey of the proposed scheme to evaluate efficiency. For this analysis, our method has been programmed with Mathematica 6.0 and has been executed for three different files size and different values of the parameter q on an Intel Pentium IV-3 GHz PC with 512 MBytes RAM memory. The parameters used were the same mentioned in the examples above and the initial conditions obtained from the key were $x_0 = 1.$ and $y_0 = .05$. The samples were built with the encryption times of four runs for each case, of which we evaluated its mean values. In addition, in order to achieve a first approach to a comparative analysis with other major chaotic schemes, we expose some results obtained by Wong (2002). They relate to the following algorithm:

1. Batista original method (1998)
2. The Batista modified method that generates only one random number for each input block (Alvarez et al., 1999)
3. The Wong fast method with input block size equal to 8 bits (2002)

These algorithms were implemented using C++ programming language running on a personal computer with Pentium III-800 MHz processor and 256 MB RAM.

Table 1 summarized the results, and in Figure 8 we sketched a linear interpolation of the run times to illustrate its upward trends.

TABLE 1 Encryption Time (in seconds) of Three Referenced Chaotic Cryptosystems and the Proposed Algorithm for Different Values of q

Method	File 1 98304 bytes	File 3 210944 bytes	File 3 487000 bytes
Batista	12,50	24,20	56,20
Modified method	6,80	13,60	31,70
Wong 8-bits	5,40	11,00	24,70
Proposed method $q = 10$	39,37	84,50	194,56
Proposed method $q = 100$	8,91	19,17	44,42
Proposed method $q = 1000$	5,89	12,76	29,55

Downloaded By: [Roda, Fernando] At: 15:44 19 November 2010

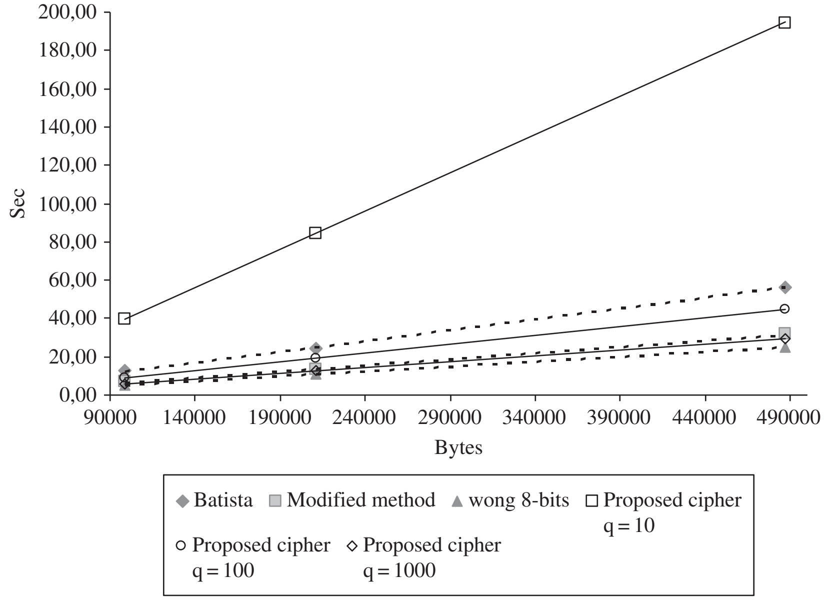

FIGURE 8 Performance comparison of chaotic cryptographic algorithms.

Downloaded By: [Roda, Fernando] At: 15:44 19 November 2010

It is important to remark that our algorithm was executed under an interpreter and is slower than a compilation. Therefore, this is only an initial approximation of the processing time, and it is difficult to do a comparative efficiency analysis with other algorithms. Nevertheless, we should not forget one very important feature: In the proposed cipher, the size of the ciphertext file is the same as that of its corresponding plaintext file, because the cryptosystem maps one to one correspondence between plaintext and ciphertext file. It is important because in an efficient communication if the ciphertext file is big, a large amount of time will be required to transmit it over a public network or Internet, and this may became a hinder to practical use. However, in the cryptographic scheme developed by Baptista (1998) and then improved by Alvarez et al. (1999) and Wong (2002), the ciphertext files are twice the sizes of their respective plaintext files as we showed en Table 2. Hence, although the implementation of these algorithms is fast, they generate large files that take much longer in its transmission and greater storage cost.

TABLE 2 Size of the Ciphertext Files (in Bytes)

Method	File 1 98304 bytes	File 2 210944 bytes	File 3 487000 bytes
Batista	196608	421888	974000
Modified method			
Wong 8-bits			
Proposed method	98304	210944	487000

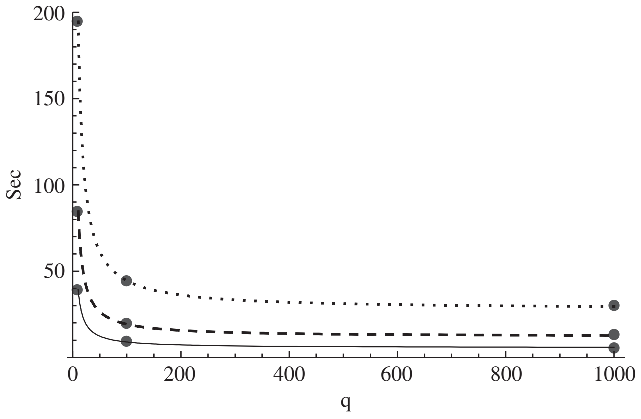

FIGURE 9 Processing time fall for different values of q.

As mentioned in the method description, the parameter *q* must be carefully set because it determines the processing time and the sensitivity with respect to a character change. In fact, the higher the value of *q*, the faster execution, but lower sensitivity. Figure 9 show the same encryption time gave in Table 1 for the proposed scheme, but now we present its evolution with the q variations. The lines are rational least-squares fits of the encryption times for each file. Dotted line corresponds to the processing of file 1, dashed line corresponds to the processing of file 2 and the solid one to the processing of file 3. This exemplify how important is to choose a suitable value for q.

The encryption time decreases sharply as we enlarge q from 10 to 100, but when we increase to 1000, the variation is not so significant. This illustrates that the number of reintegration cycles decrease for big values of q, and it is no longer a critical factor on the processing time.

We have not considered different key sizes in this analysis because, on the underlying numerical method, a bigger key size does not require additional computing effort. The values of the initial conditions are lost after the first iteration of the method, and the complexity of the next iterations do not depend on them.

CONCLUSION

In this survey we have not emphasized the system efficiency but instead proposed an alternative chaotic cryptosystem to obtain a robust cipher against statistical attacks. We have developed a symmetric-key cryptosystem based on a continuous dynamic system. We have make use of the Duffing equation as it is characterized by: 1) the numerical stability of the solution obtained by Runge-Kutta's method, 2) having six parameters and only for specific values it has a chaotic behavior, and 3) requiring two initial conditions different from one-dimensional discrete chaotic methods. By using two sets of values and a mechanism that changes the initial conditions at constant intervals, we avoided the periodicity caused by computer finite representation. This cryptosystem qualitatively satisfies the following three important properties: a) sensitivity with respect to the original message, b) sensitivity with respect to the key, and c) lost of evidence from the original text. Finally, we introduce a brief analyze of the system efficiency and showed how the parameters settings affects system performance. In particular, we studied the system behavior for different values of the parameter q, and we noticed that the higher the value of *q*, the faster execution but lower sensitivity. Nevertheless, a large increase in this parameter does not imply that the processing time fall down in proportion.

Downloaded By: [Roda, Fernando] At: 15:44 19 November 2010

ACKNOWLEDGMENTS

This paper was made with the support of ING195 subsidy, UNR.

REFERENCES

Alvarez, E., Fernandez, A., Garcia, P., Jimenez, J., and Marcano, A. (1999). New approach to chaotic encryption. Phys. Lett. A, 293, 373–375.

Amigo, J. M., Kocarev, L., and Szczepanski, J. (2007). Theory and practice of chaotic cryptography. Phys. Lett. A, 366, 211–216.

Baptista, M. S. (1998). Cryptography with chaos. Phys. Lett. A, 240, 50–54.

Boccaletti, S., Grebogi, C., Lai, Y. C., Mancini, H., and Maza, D. (2000). Phys. Rep., 329(3), 103.

Chicone, C. (1999). Ordinary differential equations with applications. New York: Springer-Verlag.

de Oliveira, L. and Sobottka, M. (2008). Cryptography with chaotic mixing. Chaos, Solitons and Fractals, 35, 466–471.

Edwards, C. H., Jr. and Penney, D. E. (1993). Elementary differential equations with boundary value problems (3rd.edition). New York: Prentice Hall.

García, A., Martin, P., and González, A. (2002). New methods oscillatory problems based on classical codes. Appl. Numer. Math., 42, 141–157.

Grebogi, C., Lai, Y. C., and Hayes, S. (1997). Int. J. Bifur. Chaos, 7, 2175.

Hairer, E., Norsett, S. P., and Wanner, G. (2000). Solving ordinary differential equations I (2nd edition). New York: Springer-Verlag.

Hindmarsh, A. C. and Petzold, L. R. (1995). Practical numerical algorithms Part I. Comput. Phys., 9(1), 34–41.

Hindmarsh, A. C. and Petzold, L. R. (1995). Practical numerical algorithms Part II. Comput. Phys., 9(2), 148–155.

Menezes, A. J., Oorschot, P. C. V., and Vanstone, S. (1997). Handbook of applied cryptography. Boca Raton, FL: CRC Press.

Pareek, N. K., Patidar, V., and Suda, K. K. (2003). Discrete chaotic cryptography using external key. Phys. Lett. A, 309, 75–82.

Parker, T. S. and Chua, L. O. (1989). For numerical practical algorithms chaotic systems. New York: Springer-Verlag.

Pecora, L. M. and Carroll, T. L. (1990). Phys. Rev. Lett., 64(8), 821.

Press, W., Flannery, B., et al. (1986). Numerical recipes. New York: Cambridge University Press.

Pull ahead, J. and Kocak, H. (1996). Dynamics and bifurcations. New York: Springer-Verlag.

Schmitz, R. (2001). Journal of the Franklin Institute, 338(4), 429–441.

Schneier, B. (1996). Applied cryptography: Protocols, algorithms and source code in C. New York: Wiley.

Stinson, D. R. (1995). Cryptography: Theory and practice. Boca Raton, FL: CRC Press.

Strogatz, S. (1994). Nonlinear dynamics and chaos. New York: Addison-Wesley.

Vaidya, P. G. and Angadi, S. (2003). Decoding chaotic cryptography without access to the superkey. Chaos, Solitons and Fractals, 17, 379–386.

Verhulst, F. (1990). Nonlinear differential equations and dynamical systems. New York: Springer-Verlag.

Wong, K.-W. (2002). A fast chaotic cryptographic scheme with dynamic look-up table. Phys. Lett A, 298, 238–242.

Wong, K.-W., Ho, S.-W., and Yung, C.-K. (2003). A chaotic cryptography scheme for generating short ciphertext. Phys. Lett. A, 310, 67–73.

BIOGRAPHY

Fernando Roda is a researcher of the National Council of Scientific and Technological Research in Argentina (CONICET) and a University professor at UCEL. He is an Information System Engineer and a System Analyst awarded for highest GPA of the promotion. He is also a member of the System Dynamics Research Team at UNR. Some years ago, F. Roda was granted a Scholarship by the Information System Department at The National Technological University for his work on cryptography.

Luis Lara, PhD, is a researcher of the National Council of Scientific and Technological Research in Argentina (*CONICET*) and professor in the Physics Department at the Universidad Nacional de Rosario, Argentina.