ISSN 0027-1349, Moscow University Physics Bulletin, 2008, Vol. 63, No. 2, pp. 95–100. © Allerton Press, Inc., 2008.
Original Russian Text © A.Yu. Loskutov, A.A. Churaev, 2008, published in Vestnik Moskovskogo Universiteta. Fizika, 2008, No. 2, pp. 15–19.

# Application of Chaotic Mapping for the Encryption of Information

**A. Yu. Loskutov and A. A. Churaev**

*Department of the Physics of Polymers and Crystals, Faculty of Physics, Moscow State University, Leninskie gory, Moscow, 119992 Russia*

*e-mail: Loskutov@chaos.phys.msu.ru*

Received May 30, 2007

**Abstract**—A new method previously proposed [1] for the encryption of information by means of chaotic mappings is studied in detail. Cryptanalysis by exhaustive key search and correlation analysis of the ciphers are performed. The predictability of the cipher values is estimated. A web application permitting users to exchange text messages encrypted by the new method is described.

**DOI:** 10.3103/S0027134908020045

## INTRODUCTION

A process with the features of dynamic chaos can be utilized for carrying information, converting information, and for both these functions at once. The conversion of information with the use of chaotic signals is referred to as chaotic encryption–decryption. It is known that chaotic encryption can ensure a certain confidentiality level of data transmission, i.e., solve the traditional cryptographic problem. Up to now, a number of chaotic encryption algorithms and schemes have been proposed and tested (see, e.g., [1–12] and references therein) providing for different confidentiality levels. Some of them employ the instable cycles of chaotic systems, others are based on synchronization phenomena. Such systems ensure a high level of information protection, high speed of encryption, and a reliable noise resistance.

This study continues the investigation of the cryptographic method briefly described in [1]. The results obtained there suggest that chaotic mapping is applicable for the information encryption and transfer of the hidden data. The proposed method holds promise for conceptually new encrypting devices. It is based on the known fact [12–14] that, for sufficiently general families of 1D and N-dimensional maps, there exist periodic perturbations that lead to stabilization of cycles of a certain period and, therefore, set the system into a regular mode. Information can be encrypted on the basis of the one-to-one correspondence of the symbol characters to the periods of stable cycles of a perturbed map. Perturbations are used as signals to transmit information, and the map function serves as the decryption key.

## 1. ENCRYPTION ALGORITHM

Most PC operating systems store information on symbol characters in the form of the so-called ASCII codes, which are three-digit integers belonging to the interval [0; 255]. At the first stage of ciphering, it is necessary to obtain the ASCII codes of all symbols contained in the text to be ciphered, i.e., a sequence of ASCII codes. Let the resulting sequence be a numerical array composed of the ASCII code components. For example, character “a” with the ASCII code 97 is represented by three elements $n_1 = 0$, $n_2 = 9$, and $n_3 = 7$ in the array. After this, each element of the sequence $n_i$ should be interpreted (in nonlinear dynamics terms) as a period of a cycle performed by a certain dynamic system, which is quantitatively characterized by a dynamic variable. In order to avoid degenerated cycles (with a period of 0) and stable points (with a period of 1), each $n_i$ should be increased by two. Cycles with a period of 1 should be avoided because they do not change the value of the dynamic variable $x = \{x_1, \ldots, x_m\}$. The values of the control parameter $\hat{a} = \{a_1, \ldots, a_n\}$ that stabilize such cycles can be repeated, thus, decreasing the cryptographic resistance (resistance to code cracking) of the system. In addition, figure one is encountered more often than the other figures in a set of the ASCII components.

The next step is to obtain a numerical sequence with a length equal to the sum of all $n_i$ (increased by two). It is desired that such a sequence features the properties of a random one. The constructed sequence of random numbers is interpreted as a sequence of values of the dynamic variable $x$. Generation of such a sequence does not involve an external random generator but is based on several facts known from chaotic dynamics.

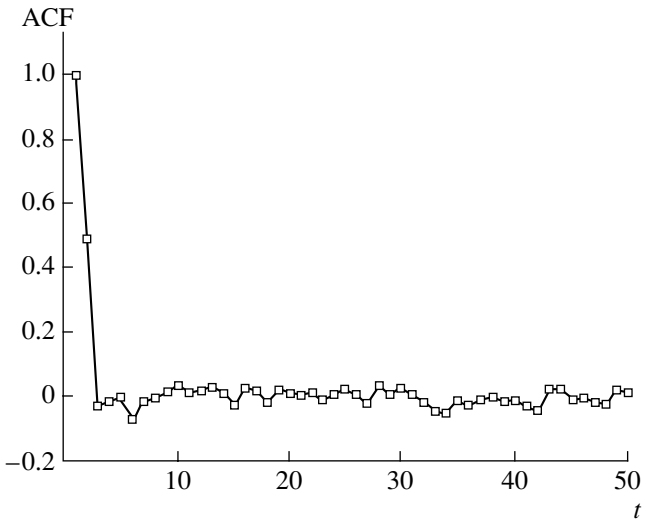


**Fig. 1.** Autocorrelation function; 9000 "o" (Latin) symbols were coded.

The algorithm is constructed with the use of discrete dynamic systems generated by mapping functions. A specific feature of such systems is that they can change their state only after a definite time period. For this reason, the behavior of a discrete dynamic system is specified by a set of values of the dynamic variable, each of which describes the state of the system at a certain time step. The relations between the systems with continuous time and the mapping functions are well known [15–17].

Now the task is to make $x$ vary in a cyclic manner. The number of cycles should be equal to the number of terms in the sequence of $n_i$ (tripled number of characters in the text to be encrypted), and the cycle periods should be equal to $n_i$. This can be readily realized using the theory described in [1].

Let us put the period of each stabilized cycle into correspondence with a definite symbol character and find the perturbation that stabilizes the cycle. Transmission of this perturbation to a detector will signify the transmission of the corresponding character. The deciphering process consists in applying the received periodic perturbation, which was used in the ciphering, to the mapping function that is stored in the detector. As a result, the dynamic variable of this mapping performs a number of cycles. The periods of the stabilized cycles determine the symbol character that has been received via the communication channel. In this manner, the received message is getting deciphered, with the encryption key being evidently given by the type of the mapping family.

## 2. CORRELATION ANALYSIS

Correlation analysis of the received ciphers is an instrument that permits one to determine the degree of predictability of the code sequence (which is directly related to the security of the encryption method, i.e., the amount of computation required for code breaking).

The security of the encryption method largely depends on the characteristics of the method applied to generate pseudorandom numbers, this dependence stems from the changes introduced into the pseudorandom numerical sequence at the initial stage of ciphering. It is of interest to analyze the sequences of dynamic variable values containing the information on the number and parameters of the cycles to be performed. The distribution of values in such a sequence is certainly not uniform. We estimated its correlation with a uniform sequence and the autocorrelation as well [15]. Then, we studied the cipher itself by performing its autocorrelation analysis.

Thus, the correlation analysis included the following stages: (1) to find a relation between the distribution function of the obtained sequence of dynamic variable values and the uniform distribution law; (2) to perform the autocorrelation analysis of the sequence of dynamic variable values; and (3) to carry out the autocorrelation analysis of the sequence of values of the control parameter (cipher).

We analyzed a sequence containing 9000 dynamic variable values, which was obtained for an encrypted message containing 1000 of the character "o." Transmission of the "o" character is the most vulnerable operation in the encryption method described, since the ASCII code of this character is 111. This signifies that, when ciphering a message, information about the "o" character will be contained in three sequential cycles with the period $n_i$ (= 1) + 2 = 3 and the repetition of these cycles is especially undesirable. The corresponding random numbers are integers from the interval (0; 10). Satisfactory results obtained in this case will guarantee an even higher protection degree for other symbol characters enciphered by this method.

As a result of performing the first stage, we determined the correlation coefficient $r$ = 0.0077 and obtained the regression equation in the form $y = 4.9322905 + 0.00499911509x$. The mean value over the sampling was 4.96478169. Hence, absence of correlation can be confirmed.

The autocorrelation function obtained at the second stage of the analysis was close to the delta function: even at $\tau = 2$, the function falls into the range (–0.02; 0.02) and does not go beyond its boundaries. This fact

permits us to conclude that there is almost no autocorrelation in the studied sequence.

It is worth noting that, for the chosen parameters of the pseudorandom number generator, the probability of an exact repetition of cycle in a sequence encrypting the "o" character is equal to 1/64. However, it is rather difficult to predict the points of the next cycle from the previous values, as follows from the results of the calculations.

At the third stage of the correlation analysis, numerical experiments were conducted for mappings with quadratic and exponential functions. In both cases, the autocorrelation function rapidly drops nearly to zero just at the beginning (Fig. 1), with the only difference being that, for the quadratic mappings, it strongly oscillates in the vicinity of zero. Such oscillations influence the predictability of the numerical values constituting the cipher. Therefore, exponential mappings appear to be preferable for encryption purposes.

## 3. CRYPTORESISTANCE ANALYSIS

The main quantitative characteristics of the cryptographic resistance of a cipher are the cost of cryptographic analysis and reliability of cryptanalytic techniques in application to this cipher. The cost of cryptographic analysis is usually characterized by the amount of computation resources (time or number of conventional calculation operations) expended for realization of the algorithm, as averaged over the tried cipher keys and decoded texts. The reliability of a cryptanalytic technique is related to the probability of decryption and characterizes the code-breaking method. As far as any code-breaking technique implies some uncertainty, for example, an incomplete knowledge of keys, decryption can be achieved with only a certain probability. Our aim now is to estimate the cost of cryptographic analysis and the reliability of a chosen cryptanalytic technique in application to the method under investigation.

Let us choose a widely used cryptanalytic method of the so-called exhaustive search, which implies a subsequent, random, and equiprobable testing of $r$ keys taken one by one from a set of keys $K$. The search continues until $k$ keys have been tried, where $k = j$ and $1 \le j < N$ is the number of the first key that transforms the encrypted text into a meaningful text or $k = N$ if this event does not occur for any $j \le N$.

In order to estimate the meaningful content of the text after applying a subsequent key, it is convenient to use the denotation $H_0$ for an open text (initial, decrypted) and $H_1$ for a random text (meaningless). In the probability model of the problem, the desired estimate depends on the following errors: (1) $\alpha = P(H_1/H_0)$ is the probability of rejecting a meaningful text and (2) $\beta = P(H_0/H_1)$ is the probability of mistaking a meaningless text for a meaningful one.

Parameters of the cost of the cryptanalytic attack

| Byte/coefficient | $\lvert K\rvert$ | $E^{\alpha,\beta}$ | $t_{(\lvert E\rvert)}$ |
|---|---|---|---|
| 1 | $2^{27}$ | $2^{26}$ | 67 s |
| 2 | $2^{51}$ | $2^{50}$ | 30 years |
| 3 | $2^{75}$ | $2^{74}$ | $6 \times 10^8$ years |
| 4 | $2^{99}$ | $2^{98}$ | $10^{16}$ years |
| 5 | $2^{123}$ | $2^{122}$ | $1.5 \times 10^{23}$ years |

Formally, the algorithm for calculating the cost of cryptographic analysis can be presented in the form

$$E^{\alpha,\beta}(|K|) = \frac{1}{|K|}\sum_{k=1}^{r} k(1-\beta)^{k-1} \times \left[\beta(r-k) + \frac{\alpha\beta}{1-\beta}(k-1) + (1-\alpha)\right] + \frac{r}{|K|} r\alpha(1-\beta)^{r-1} + \frac{|K|-r}{|K|}\left(\sum_{k=1}^{r} k(1-\beta)^{k-1}\beta + r(1-\beta)^{r}\right),$$

where $E^{\alpha,\beta}$ is the cryptanalytic cost, i.e., actually the expected average of the random value $e$ characterizing the termination of search and $r$ is the number of the tried keys. The calculation results obtained within the assumption of a faultless decision-making mechanism ($\alpha = 0$, $\beta = 0$) are listed in the table. The left column lists one of the parameters of the ciphering method: the byte-to-coefficient ratio (the number of bytes allocated for each value of the control parameter). The last column presents the cryptanalytic cost (in the units of time) calculated with allowance for the computation power of the present-day mainframes (approximately 1 instruction per 1 μs).

The reliability of the algorithm is calculated using the formula

$$P(r, \alpha, \beta) = \frac{1-\alpha}{|K|}\sum_{t=1}^{r}(1-\beta)^{t-1}.$$

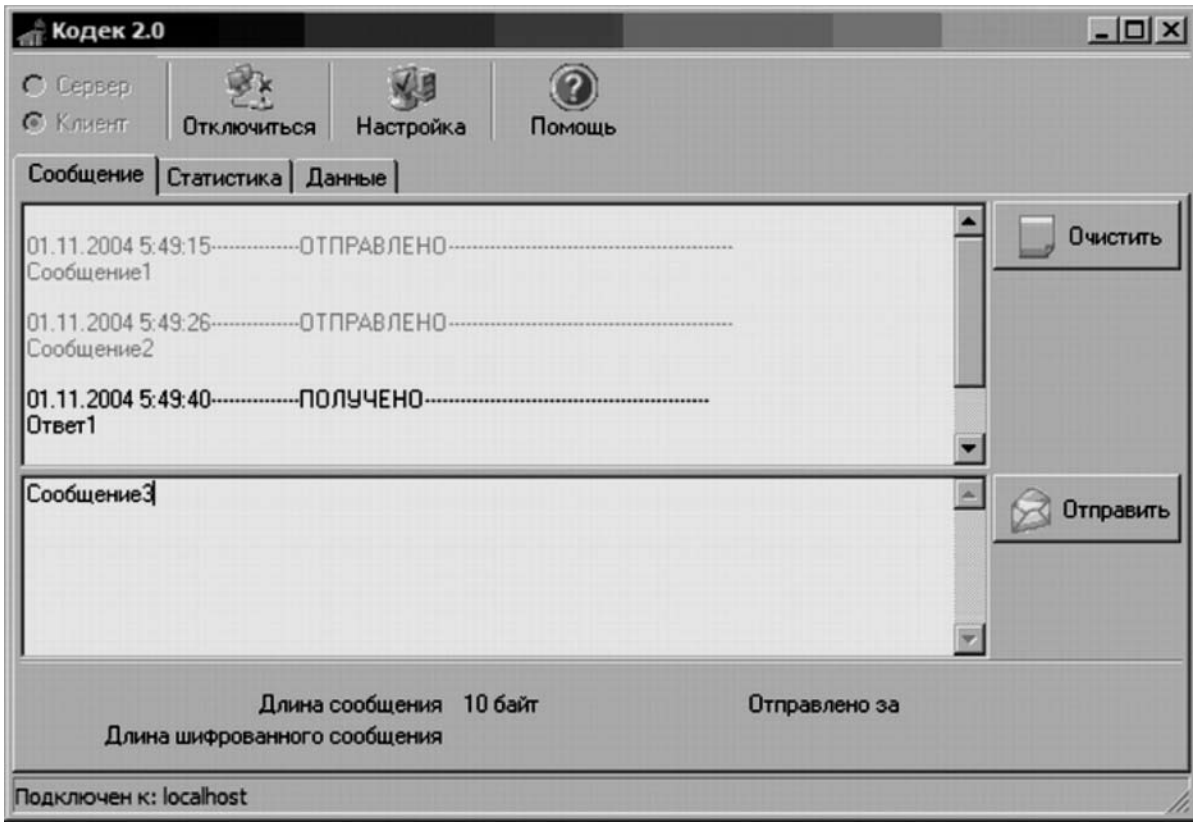


**Fig. 2.** Program messaging dialog box of the program.

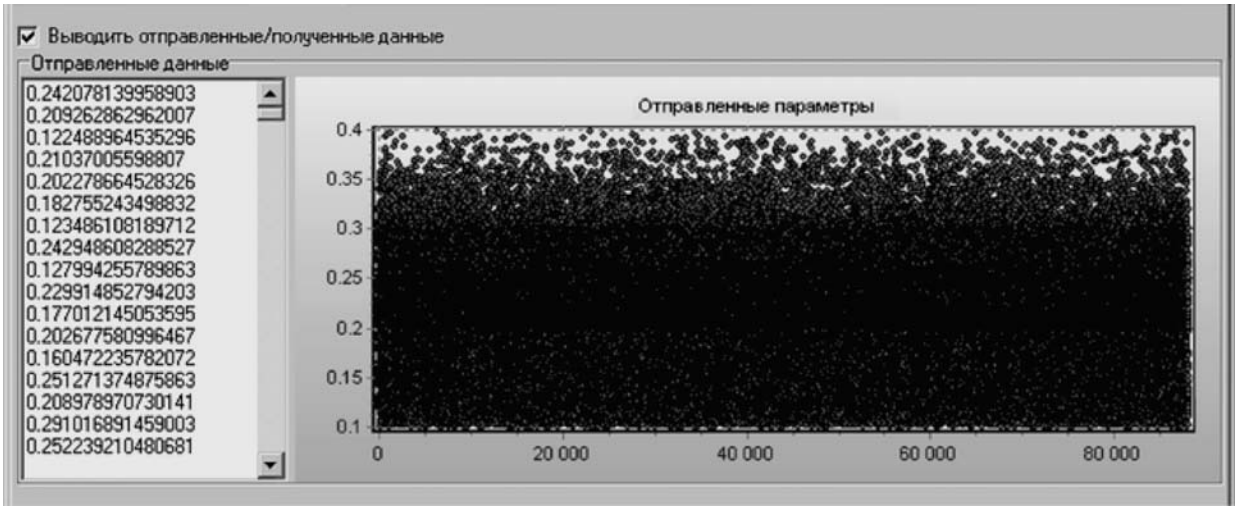


**Fig. 3.** Program "Data" dialog box.

It is evident that, under the assumption of faultless operation of the decision-making logics ($\alpha = 0$, $\beta = 0$), the reliability of the exhaustive search method is equal to 1.

## CONCLUSIONS

The results of this study support the expedience of the further development of the encryption method based on chaotic mappings. As the next step, we turn to

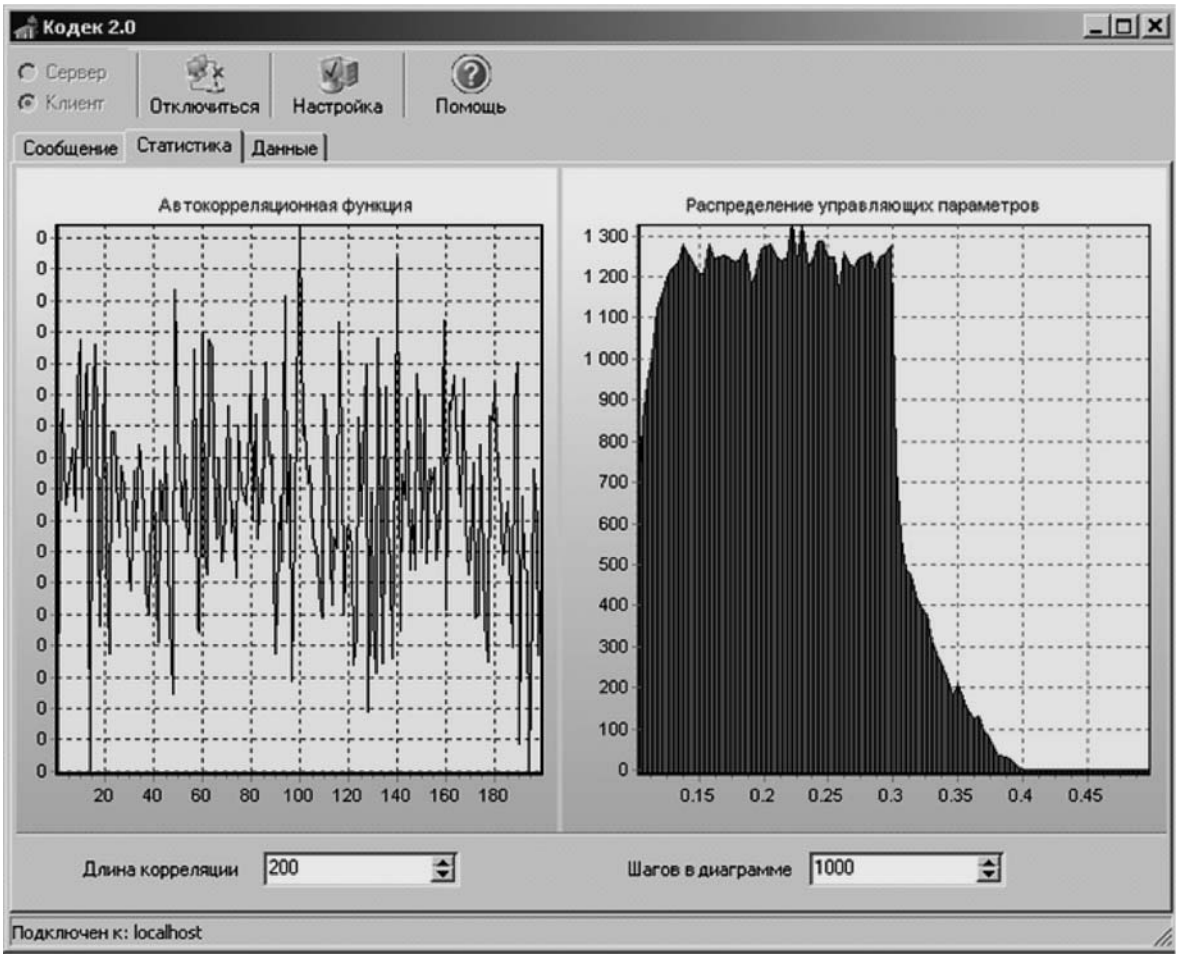


**Fig. 4.** Program "Statistics" dialog box.

practical implementation of the method. At present, a web application has been designed, which permits users to exchange encrypted text messages. The general idea of this program can be understood from Figs. 2–4.

The advantages of the proposed method can be summarized as follows: (1) each symbol character of the alphabet can be enciphered by a subset or even an entire region of a positive measure, (2) no preliminary synchronization of the transmission–detection system is required, (3) the method features a high cryptographic resistance and high correlation performance, and (4) the method is relatively simple and, hence, can be readily implemented.

## REFERENCES

1. A. Yu. Loskutov, S. D. Rybalko, and A. A. Churaev, Pis'ma Zh. Tekh. Fiz. **30** (20), 1 (2004) [Tech. Phys. Lett. **30**, 843 (2004)].
2. A. S. Dmitriev, Radiotekh. Élektron. (Moscow), No. 5, 101 (1991).
3. A. Dmitriev, A. Panas, and S. Starkov, in *Proceedings of the International Conference on Nonlinear Dynamics, Nizhni Novgorod, 1996*, p. 36.
4. A. S. Dmitriev, Yu. V. Andreev, and A. G. Bulushev, Zarubezhn. Radioélektron., No. 11, 27 (2000).
5. A. S. Dmitriev, L. V. Kuz'min. A. I. Panas, and S. O. Starkov, Radiotekh. Élektron. (Moscow) **43**, 1115 (1998) [J. Commun. Technol. Electron. 43, 1038 (1998)].
6. A. S. Dmitriev, G. Kassian, and A. Khilinsky, Int. J. Bifurcation Chaos **10**, 749 (2000).
7. A. S. Dmitriev, B. E. Kyarginskii, A. I. Panas, and S. O. Starkov, Radiotekh. Élektron. (Moscow) **46**, 224 (2001) [J. Commun. Technol. Electron. **46**, 207 (2001)].
8. A. Dmitriev, B. Kyarginskiy, A. Panas, and S. Starkov, in *Proceedings of the 9th Workshop on Nonlinear Dynamics of Electronic Systems, NDES-2001, Delft, Netherlands, 2001*, p. 157.
9. Yu. V. Andreyev, A. S. Dmitriev, and S. O. Starkov, IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **44**, 21 (1997).
10. Yu. V. Andreyev, A. S. Dmitriev, and D. A. Kuminov, Usp. Sovr. Radioélektron. (Zarubezhn. Radioélektron.), No. 10, 50 (1997).

11. Yu. V. Gulyaev, R. V. Belyaev, and G. M. Vorontsov, Radiotekh. Élektron. (Moscow) **48**, 1157 (2003) [J. Commun. Technol. Electron. 48, 1063 (2003)].
12. A. Loskutov and A. I. Shishmarev, Chaos **4**, 351 (1994).
13. A. Yu. Loskutov and A. I. Shishmarev, Usp. Mat. Nauk **48**, 169 (1993).
14. A. Loskutov, Comput. Math. Mod. **12**, 314 (2001).
15. A. Yu. Loskutov abd A. S. Mikhailov, *Principles of the Theory of Complex Systems* (PKhD, Moscow, 2007) [in Russian].
16. A. Loskutov, in *Nonlinear Dynamics: New Theoretical and Applied Results*, Ed. by J. Awrejcewicz (Academie, Berlin, 1995), p. 126.
17. A. Loskutov, V. M. Tereshko, and K. A. Vasiliev, Int. J. Bifurcation Chaos **6**, 725 (1996).
18. *Theory and Practice of Providing the Information Security*, Ed. by P. D. Zegzhda (Yakhtsmen, Moscow, 1996) [in Russian].
19. *Introduction to Cryptography*, Ed. by V. V. Yashchenko (MTsNMO–CheRo, Moscow, 2000) [in Russian].