Viktor Kyrychenko
Candidate of physical and mathematical sciences, associate professor of the computer sciences department
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
v.kyrychenko@nubip.edu.ua
Yana Kryvoruchko
Candidate of physical and mathematical sciences, associate professor of the computer sciences department
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
yanakryvoruchko@nubip.edu.ua

APPLICATION OF DISCRETE DYNAMIC SYSTEMS FOR SECURITY COMMUNICATION CHANNELS

Abstract. Dynamic systems with chaotic behavior are currently intensively used and applied in various fields, in particular for cryptographic protection of information. Generators of pseudo-random sequences can be built on the basis of such systems, which are later used for gamification of open text. On the other hand, the dynamic system can be used directly to transform information. A cipher is created on its basis. A necessary condition for unambiguous decryption is the existence of a reverse system. This work is based on the method of encryption using forward and reverse systems. Lorentz, Chua, and Ressler systems were used as dynamic chaotic systems. Software implementation of algorithms based on such systems leads to the necessity of transition from differential equations to their finite-difference analogs. However, in this case, if you do not impose restrictions on the length of the numbers used, the problem of a sharp increase in the volume of the encrypted text arises. This is especially true when converting large volumes of data. Therefore, the obtained finite-difference equations were interpreted as equations in finite rings or fields, which in this case are understood as equations defining such a discrete dynamical system as a finite state machine. On the basis of such a transition, an information transformation algorithm is implemented, in which the encrypted sequence is interpreted as a sequence of control actions of a dynamic system, and the sequence of output reactions of the latter is understood as encrypted information. The reverse system is used to decrypt information.

Keywords: encryption and data protection; direct and inverse dynamic systems; Lorentz, Chua, and Ressler systems.

1. INTRODUCTION

The problem statements. The problem of confidentiality of data transmission over communication channels and the broader problem of protecting this data is becoming more and more relevant in the market of communication technologies. A typical requirement for data encryption schemes is the possibility of mass application and low cost per unit of "information" products. When solving such problems, tools based on deterministic chaos generated by nonlinear dynamic systems can be successfully applied [1]. With the help of such systems, it is possible to build generators for pseudo-random sequences, which will be used in the future to suppress open data. On the other hand, any dynamic system with an input-output structure can be used directly to transform information. An encoder is created on the basis of such systems. The input to the system is a digitized message, and the output is an encrypted signal that is sent to information channels. A necessary condition for unambiguous decryption is the existence of an inverse system.

Analysis of recent studies and publications. Recently, a new direction in cryptology has been developing, which is connected with the use of dynamic systems with chaotic behavior [2,3]. One of the main approaches in this area, based on the use of reversible control systems for the construction of cryptographic algorithms [4].

The article's goal – to investigate the application of algorithms for the generation of pseudo-chaotic sequences for the transmission of messages through information channels based on dynamic systems.

2. THE RESULTS AND DISCUSSION

Any information processed by various discrete computers can ultimately be represented by a binary sequence. This presentation, in fact, is used in the transformation of data using various dynamic chaotic systems.

The encryption algorithm used in this work is based on the use of a discrete model of a dynamic chaotic Lorentz system [4]. A Lorentz finite state automaton is described by a system of equations:

$$y(t) = x_2(t) + h(A_2 x_1(t) - x_2(t) - x_1(t)x_3(t) + Au(t))$$
$$\begin{cases} x_1(t+1) = x_1(t) + hA_1(x_2(t) - x_1(t)) \\ x_2(t+1) = x_2(t) + h(A_2 x_1(t) - x_2(t) - x_1(t)x_3(t) + Au(t)) \\ x_3(t+1) = x_3(t) + h(x_1(t)x_2(t) - A_3 x_3(t)) \end{cases} \quad (1)$$

Here. the additive component is the current input symbol of the output information $u(t)$, $y(t)$ – corresponding symbol of encrypted information. Sets of input and output symbols, components $x_i(t), i = 1,2,3$ are understood as elements of a finite field $GF(q)$ or rings $Z(q)$, and the operations of addition and multiplication are the corresponding operations in this field, or ring [5].

Decoding is carried out by an inverse Lorentz automaton, which exists for any $A \in GF(q)$ or $A \in Z(q)$, A $\neq 0$. The coefficients of the system and the initial state of the automaton are the key of the encryption system. System (1) will be rewritten as follows:

$$\begin{cases} \dot{S}_1 = a_{11}S_1 + a_{12}S_2 \\ \dot{S}_2 = a_{21}S_1 + a_{22}S_2 + a_{23}S_1S_3 + a_{24}u \\ \dot{S}_3 = a_{31}S_3 + a_{32}S_1S_2 \end{cases}$$
$$y = \dot{S}_2$$

Coefficients of the Lorentz automaton $(a_{11}, a_{12}, a_{21}, a_{22}, a_{23}, a_{24}, a_{31}, a_{32})$, as well as input states S_1, S_2, S_3 is the key of the encryption system. If necessary, the value can also be a key parameter *k*, which specifies the size of the data block that is processed in one iteration (a quantum of information) in *k* byte.

The main stages of the encryption algorithm are as follows:

1. Initialization of the automaton - its coefficients and input state according to the encryption key and quantum size are set;
2. Processing of the next quantum of information using system (1). which is in the current state, and issues an encrypted quantum, after which it moves to a new state. This step is repeated until the end of the data stream being processed.

When calculating the state values of the automaton, all operations take place in the field $GF(2^p)$ or rings $Z(2^p)$.

The result of the encryption algorithm will be some sequence, which should have the properties of pseudo-random. Two groups of tests were used for its research: graphical and evaluative, which are part of the NIST statistical test package [5].

Test 1. To visualize the input as well as the output binary sequence, it is imagined in the form of some matrix. The image of such a matrix is built according to the following rule: a black pixel displays an element of the matrix equal to zero, and correspondingly, a white pixel represents an element equal to one. For this test, 10 different input sequences of length 320,000 bits were used. Each sequence was encrypted with different, arbitrarily chosen parameters. As a result of the tests, the following conclusions were obtained. When encrypting in a ring $Z(2^8)$ using the Lorentz system, in no case is a homogeneous picture observed; In the case of

pronounced areas in the source file, their contours remain in the source file, which indicates the heterogeneity of the source data. As the power of the ring increases, the "blurring" improves.

Test 2. Use of the NIST statistical test package to assess the quality of PVP generators. In this test, a sequence of units with a power of 100,000 is encrypted 125 times. Each parameter is traversed step by step $2^n / 5$ and all their possible combinations are taken. Thus, 125 sequences are obtained. The NIST battery of tests is applied to them.

NIST tests show that Lorentz encryption in the Z_8 ring performs poorly. As the power of the ring increases, the result improves and the time of the tests decreases. When adding a predicate to the system, there is a slight improvement in the result.

3. CONCLUSIONS

Any controlled dynamic system having an input-output structure can be used directly to transform information. The idea of using reversible control systems with complex behavior of trajectories is at the basis of the task of synthesizing new effective algorithms for information protection, primarily from unauthorized access.

The conducted studies and their assessment allow us to say that new results were obtained that expand the theoretical base of modern cryptology and are promising for the creation of effective cryptographic algorithms. At the same time, a number of questions remain open related to the influence of dynamic parameters on the resistance of crypto-algorithms to attacks, resistance to information distortions, the appearance of invariant manifolds.

REFERENCES

1. *Kyrychenko V.V., Lesina Ye.V.* Application of dynamic systems for encoding data in telecommunication channels // Electronics & Control Systems. – 3 (53), 2017. – P. 11-16.
2. *Adee, R.; Mouratidis, H.* A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography. Sensors 2022, 22, 1109. https://doi.org/10.3390/s22031109
3. *Kyrychenko V.V., Lesina Ye.V.* Effect of dynamic degradation in algorithms for data security // Electronics & Control Systems. – 1 (59), 2019. – P. 27-32.
4. *Sobhy M.I., Shehata A.* Secure computer communication using haotic algorithms. – Int.J. of Bifurcation and Chaos. Vol. 10, N12, 2000, – P. 2831-2839.
5. A statistical test suite for random and pseudorandom number generators for cryptographic applications / Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, San Vo. – National Institute of Standards and Technology Special Publication 800-22 revision 1a, April 2010. – 131 p. [Електронний ресурс]. – Режим доступу: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

МАТЕРІАЛИ

XI Міжнародної науково-практичної конференції

ГЛОБАЛЬНІ ТА РЕГІОНАЛЬНІ ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ В СУСПІЛЬСТВІ І ПРИРОДОКОРИСТУВАННІ '2023

15-16 листопада 2023 року

Київ, НУБіП України

Київ 2023

УДК 004

Рекомендовано до друку вченою радою факультету інформаційних технологій Національного університету біоресурсів і природокористування України (протокол № 4 від 20.11.2023)

Укладач: к.е.н., доцент Харченко В.В.

Збірник матеріалів XI Міжнародної науково-практичної конференції "Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2023", 15-16 листопада 2023 року, НУБіП України, К. НУБіП України, 2023. 117 с.

Відповідальність за зміст публікацій несуть автори.