Radioelectronics and Communications Systems
Vol. 49, No. 4, pp. 19–25, 2006

Izvestiya VUZ. Radioelektronika
Vol. 49, No. 4, pp. 27–37, 2006
UDC 681.3.06:519.248.681

ANALYSIS OF EFFECTIVENESS OF MEASURES FOR CONCEALMENT OF INFORMATION IN COMMUNICATION SYSTEMS AND NETWORKS BY CHAOTIC DYNAMICS METHODS

P. Yu. Kostenko, A. V. Antonov, and T. P. Kostenko

Kharkov University of Air Forces, Ukraine

The paper is devoted to analysis of information reticence in communication systems and networks when the reticence is achieved by the methods of chaotic dynamics. As distinct from traditional methods of information protection, which rely on "computational complexity" of cryptoanalysis, the advantage of the new method consists in ambiguity of inversion of the chaotic mapping. Characteristics of resistance of the method to some kinds of "krypto-invasions" are considered and defined.

Along with wide application of communication systems and networks, there is a growing need in confidential exchange of information, i.e., information reticence, protection of information from non-sanctioned access and other violence, etc. These tasks can be resolved by various means of cryptographic protection of information. The whole stock of means for cryptographic protection of information, added by the necessary key, normative, maintenance, and other documentation (including that responsible for safety), which ensure the required level of confidentiality of information to be processed and/or transferred in communication systems and networks, constitute the cryptographic system (cryptosystem for brevity). In a narrower mathematical sense, by a cryptosystem $S = \{X, Y, K_e, K_d, f_e, f_d\}$ is meant some unambiguous transform of information $f_e: X \times K_e \to Y$ and $f_d: Y \times K_d \to X$, defined on the set of initial states X (the open text), final states Y (the ciphered text), and keys K_e and K_d. The state $x \in X$ represents the message to be processed. In the computer-aided cryptography the sets of initial and final states, as well as keys, are established by the binary alphabet {0, 1}, and the transforms f are defined by the program (algorithm) realized by Turing's machine.

The pressing problems, still in force in the contemporary cryptography, consist in elaborating the traditional and seeking for new approaches to protection of information, and in creation of new promising cryptosystems ensuring a maximum of information protection.

One of new ways to improvement of cryptosystems is considering them from the positions of the nonlinear chaotic dynamics [1, 2]. Following this line, we can assess unambiguously both the existing cryptosystems and those under development. Moreover, this approach permits to assert that the use of methods of chaotic dynamics for information protection in communication systems and networks may be rather effective from the viewpoint of their defiance to deciphering. Development of cryptosystems based on the chaotic dynamics principles has been elucidated in a number of works of foreign authors, for example, in [3–5].

Consider the cryptographic systems with the open (public) key [6]. Their resistance to deciphering is based on "computational complexity" of cryptoanalysis of the number-theoretic algorithms. However, the "computational complexity" depends on the state-of-the-art of the mathematical methods used for treatment of the number-theoretic problems (such as simple factorization of numbers, taking discrete logarithms, etc.), which makes these systems

REFERENCES

1. N. I. Ptitsyn, Application of the Deterministic Chaos Theory in Cryptography [in Russian], MGTU, Moscow, 2002.

2. L. Kocarev, Chaos-Based Cryptography: A Brief Overview, IEEE Circuits and Systems Magazine, Vol. 1, pp. 6–21, 2001.

3. L. Kocarev and Z. Tasev, Public-Key Encryption Based on Chebyshev Maps, Proceedings of the IEEE Symposium on Circuits and Systems (ISCAS-2003), Vol. 3, pp. 28–31, 2003.

4. N. Matsuda and K. Aihara, Cryptosystem with Discretized Chaotic Maps, IEEE Transactions on Circuits and Systems 1: Fundamental Theory and Applications, Vol. 49, No. 1, pp. 28–39, 2002.

5. Z. Kotulski et al., Applications of Discrete Chaotic Dynamical Systems in Cryptography — DCC Method, International Journal of Bifurcation and Chaos, Vol. 9, pp. 1121–1135, 1999.

6. W. Diffie and M. E. Hellman, New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. 22, pp. 644–654, 1976.

7. J. Cowie et al., A World Wide Number Field Sieve Factoring Record: On to 512 Bits, Proceedings of ASIACRYPT'96, November 1996.

8. A. Odiyzko, The Future of Integer Factorization, CryptoBytes, summer 1995.

9. M. Wiener, Cryptoanalysis of Short RSA Secret Exponents, IEEE Transactions on Information Theory, Vol. IT-36, 1990.

10. R. Rivest, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public Key Cryptosystem, Communications of the ASM, 1978.

11. The Federal Information Processing Standard — FIPS PUB 186, NIST USA, 1996.

12. T. El-Gamal, A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Transactions on Information Theory, Vol. 31, pp. 469–472, 1985.

13. C. Schnorr, Efficient Signatures for Smart Card, Journal of Cryptology, No. 3, 1991.

14. Z. Kotulski et al., On Constructive Approach to Chaotic Pseudorandom Number Generator, RCMCIS, 2002.

15. F. Moon, Chaotic Oscillations — A Primary Course for Researchers and Engineers [Russian translation], Mir, Moscow, 1990.

16. T. Kohda and T. Yoshimura, Statistical Attack on Chaos-Based El-Gamal Public Key System, Proceedings of the IEEE Symposium on Circuits and Systems (ISCAS-2004), pp. 1–13, 2004.

17. V. Stolings, Cryptography and Network Protection: Principles and Practice, 2nd edition [Russian translation], The "Williams" Publishing House, Moscow, 2001.

1 November 2005