Application of Bioinpired Optimization Artificial Intelligence Technology for Solution Task of Cryptoanalysis of Encyption Systems

Yu. O. Chernyshev, A. S. Sergeyev, A. N. Ryazanov

Don state technical university

The report is devoted to a problem of use of new technologies of artificial intelligence - the bioinspired optimizing methods and algorithms imitating processes of evolution of wildlife for the solution of a task of cryptanalysis of classical and modern systems of enciphering. Application of genetic algorithms for cryptanalysis of classical codes of shifts, replacements along with experimental results is considered [1]. Also the possibility of cryptanalysis of the XOR codes for a some of special cases is investigated (a rejection of statistical characteristics from a random stream, reuse of parts of scale, modification of data in the channel, aprioristic information about the form and structure of the document). In addition, the possibility of the solution of a task of cryptanalysis with use of new models of the bioinspired methods algorithms of ant colonies and a bee swarm is described [2]. Distinctive features of these methods are considered, and also use of the bioinspired technologies for cryptanalysis of classical codes of shifts and replacement, asymmetric cryptosystems based on decision-theoretic task of cryptography (factorization of numbers and finding factors of a number), and modern block encryption standards along with some experimental results (the DES, AES, Russia standard, on the basis of determination of quantity of optimum symbols of the deciphered text at the cryptanalysis of type 2) is investigated [3]. In addition, the actual problem of development of the combined bioinspired technologies combining the main features of classical "natural" algorithms is considered. The combined bioinspired methods including the main operations of genetic algorithms, and also algorithms of ant and bee colonies are presented, demonstration examples of their implementation are provided.

References

1. Chernyshev Yu. O., etc. Cryptographic methods and genetic algorithms of the solution of tasks of cryptanalysis: Krasnodar, 2013.– 138 p.
2. Chernyshev Yu. O., etc. The bioinspired algorithms of the solution of tasks of cryptanalysis of classical and asymmetric cryptosystems: Krasnodar, 2015. – 132 p.
3. Chernyshev Yu. O., Sergeyev A. S., Dubrov E. O., Ryazanov A. N. Application of the bioinspired methods of optimization for realization of cryptanalysis of block methods of enciphering: Rostov-on-Don: DSTU publishing house, 2016. – 177 p.