THE USE OF GENETIC ALGORITHMS IN CRYPTANALYSIS

Zurab Kochladze*, Lali Beselia**
*Iv. Javakhishvili Tbilisi State University, . Tbilisi, Georgia, zurab.kochladze@tsu.ge
**Sokhumi State University, Tbilisi, Georgia, lalibeselia@mail.ru

Genetic algorithms were first used for the solution of optimization problems. After some time they were also used in different fields of science. Genetic algorithms are based on one of the basic principles of biological evolution: struggle for population saving by maximal adjustment to the environment that is reached by improvement and development of the best features in new generations. One of the most significant advantages of the genetic algorithms compared to other search algorithms is the possibility of their parallelization. This significantly decreases the attack time. Use of genetic algorithms for cryptanalysis of cryptographic algorithms is a new trend, which has not been yet developed in practical cryptology. There are several hundreds of works, the authors of which make their efforts to show that this approach may have advantages compared to other ones. In that regard, we tried to crack the already cracked Merkle-Hellman cryptosystem by means of genetic algorithms[1,2]. Then we compared our results to the results obtained by the use of Shamir algorithm[3]. There are several works, where the Merkle-Hellman cryptosystem is cracked by genetic algorithms, though in all cases the attack is carried out on the basis of ciphertext [4,5]. Unlike these works and like the Shamir method, we search for the cipher key by attacking against the open key. We elaborated new heuristical methods, which made the use of genetic algorithms more precise and faster. The results of research and software given in this article may be used for cryptanalysis of other asymmetric cryptosystems as well.

References

1. Merkle R.C., Hellman M.E.: Hidding information and signatures in trapdoor Knapsak, IEEE Trans. Inform. Theory, IT-24 (1978), pp. 535-530
2. Martello S., Toth P.: Knapsack problems John Wiley and Sons 1990.
3. Salomaa A.: Public-key Cryptography Springer-Verlag 1990
4. Garg P., Shastri A.: An Improved Cryptanalytic Attack on Knapsack Cipher using Genetic Algorithm. International Journal of Information Technology 3:3 2007.
5. Muthuregunathan R., Vekataraman D., Rajasekaran P.: Cryptanalysis of Knapsack Ciher Using Parrallel Evolutionary Computing. International Journal of Recent Trends in Engineering, Vol. 1, No 1, May 2009.