Paper Title: Evolutionary Algorithms in Cryptography: A survey

Author: Dipankar Dasgupta

Abstract:

One of the key components of cyber security is cryptography. It provides the confidentiality in storage data and allows secure communication over the Internet. Traditionally, Cryptanalysis is the art and science of solving cryptograms (writings in cipher or code) or cryptographic systems (devices for enciphering and deciphering) through analysis without prior knowledge of the encryption method. Using known techniques and imagination, a Cryptanalyst systematically identifies basic elements in a cipher code which may lead to its solution." [NSA website]. There are different types of encryption/decryption methods available today, but the use of evolutionary algorithms in this area is primarily in cryptanalysis and is in very early stage. In particular, Genetic Algorithms (GAs) have been applied in finding keys for Three Rotor Machine ciphers [Bagnall et al. 1996,1997], simple substitution ciphers [Spillman et al. 1993], Chor-Rivest knapsack PKC [Yaseen et al. 199] and in a few other applications [Clark et al 1999, Russell et al 2003, Sipper 1996]. The method used by Spillman (1993) involved using language characteristics, specifically digram analysis (frequency of common two letter combinations). Subsequent works were done with Polyalphabetic Substituion Cipher and Transposition Ciphers [Clark et al 1999, Russell et al 2003]. The paper will review the works on genetic cryptanalysis and mention their strength and weakness and explore avenues for further research.

References:

- Spillman, Janssen, Nelson, and Kepner. Use of a Genetic Algorithm in the Cryptanalysts of Simple Substitution Ciphers from Cryptologia. In CRYPTOLOGIA, Volume XVII Number 1, January 1993
- A.J. Bagnall. The Aplications of Genetic Algorithms in Cryptanalysis, Master's Thesis, University of East Anglia, 1996.
- M. Sipper and M. Tomassini. Co-evolving Parallel Random Number Generators. Proceedings of the Fourth International Conference on Parallel Problem Solving from Nature (PPSN IV), H.-M. Voigt, W. Ebeling, I. Rechemberg and H.-P. Schwefel (Eds.), Lecture Notes in Computer Science 1141, Springer-Verlag, 950-959, 1996.
- J. Bagnall, G.P. McKeown and V.J. Rayward-Smith. The Cryptanalysis of a Three Rotor Machine Using a Genetic Algorithm, 1997
- Imad F.T. Yaseen, H.V. Sahasrabuddhe. A Genetic Algorithm for the Cryptanalysis of Chor-Rivest Knapsack Public Key Cryptosystem (PKC). In Third International Conference on Computational Intelligence and Multimedia Applications, New Delhi, India, September 23 - 26, 1999
- Andrew Clark and Edward Dawson. A Parallel Genetic Algorithm for the Analysis of the Polyalphabetic Substituion Cipher. 1999.
- Matthew Russell, John A Clark and Susan Stepney. Making the most of Two Heuristics: Breaking Transposition Ciphers with Ants. In IEEE CEC Special Session on Evolutionary Computation in Computer Security and Cryptography. Canberra, 8-12 December 2003.