The Applicability of Genetic Algorithm in Cryptanalysis: A Survey

Abstract

The Cryptanalysis has been the most fascinating area for science fraternity. The application of Genetic Algorithm (GAs) to the field of cryptanalysis is rather unique as no robust model for cryptanalysis using Genetic Algorithm exists. Genetic Algorithm (GAs) are the class of heuristic algorithm which are known for optimization and search problem. The paper presents the systematic review of Genetic Algorithm applied to the Cryptanalysis.

References

17. Goldberg,D,E et al.2000. Bayesuan Optimization Algorithm, population sizing and time to convergence, University of Illinois,USA.
The Applicability of Genetic Algorithm in Cryptanalysis: A Survey

cipher. In proceeding of the Fourth International Conference on Pattern Recognition and Information Processing.


29. Yaseen,I.F.T., Sahasrabuddhe,H.V.1998. A Genetic Algorithm for the cryptanalysis of Chor-rivest knapsack public key cryptosystem(PKC). In proceeding of the third International Conference on Computational Intelligence and Multimedia Applications


Index Terms

Computer Science Security

Keywords

Cryptanalysis, Genetic Algorithm (GAs), Cryptography.