Abstract

Cryptanalysis of knapsack cipher is a fascinating problem which has eluded the computing fraternity for decades. However, in most of the cases either the time complexity of the proposed algorithm is colossal or an insufficient number of samples have been taken for verification. The present work proposes a Genetic Algorithm based technique for cryptanalysis of knapsack cipher. The experiments conducted prove the validity of the technique. The results prove that the technique is better than the existing techniques. An extensive review has been carried out in order to find the gaps in the existing techniques. The work paves the way of the application of computational intelligence techniques to the discipline of cryptanalysis.

References


Index Terms

Computer Science  Security

Keywords

Knapsack Cipher, Cryptanalysis, Genetic Algorithms, Fitness function.