Abstract

Cryptanalysis is very important step for auditing and checking strength of any cryptosystem. Some of these cryptosystem ensures confidentiality and security of large information exchange from source to destination using symmetric key cryptography. The cryptanalyst investigates the strength and identifies the weakness of the key as well as enciphering algorithm. With the increase in key size, the time and effort required predicting the correct key increases. So, the Trend of increasing key size from 1 Byte to 8 Bytes to strengthen the cryptosystem and hence algorithm continues with compromise on the cost of time and computation.

Automatic Variable Key (AVK) based symmetric key cryptosystem is an alternative to this style by fixing up key size and adding security level direction. Whenever any new cryptographic method is invented to replace existing vulnerable cryptographic method, it’s deep analysis from all perspectives (Hacker / Cryptanalyst as well as User) is desirable and proper study and evaluation of its performance is must. New cryptic techniques may exploit benefits of advances in computational methods like ANN, GA, SI etc. These techniques for cryptanalysis are
changing drastically to reduce cryptographic complexity. In this paper a detailed survey and direction of development work has been conducted. The work compares these new methods with state of art approaches and presents future scope and directions from the cryptic mining perspectives.

References


10. Weiqing Jin, , “Fuzzy Classification Based on Fuzzy Association Rule Mining”, http://repository.lib.ncsu.edu/ir/bitstream/1840.16/5924/1/etd.pdf, 2004


35. Andreas S. Weigend (NA) “Introduction to Theory of Neural Computation”, To appear in
Various Approaches towards Cryptanalysis


47. Shaligram Prajapat, R. S. Thakur, "Towards Optimum size of key for AVK based cryptosystem", Communicated and CJICT, Nigeria in June-Dec. 2015. ISSN (Online): 2354 - 3507; ISSN (Print): 2354 – 3566


51. Shaligram Prajapat, A. Thakur, K. Maheshwari, R. S. Thakur, " Cryptic Minining in the light of Artificial Intelligence", (Extended version), Published in International Journal of Advanced
Various Approaches towards Cryptanalysis

Computer Science and Applications (IJACSA), 6(8), 2015. (DOI):10.14569/IJACSA.2015.060808

52. Shaligram Prajapat, G. Parmar, R.S. Thakur, "Towards investigation of efficient Cryptosystem using SGcrypter". ICCP-2015 and (extended paper) is in press IJAER.

Index Terms

Computer Science Networks

Keywords

cryptanalysis, Hacker, AI, Genetic Algorithm, Swarm Intelligence, cipher, neural network, cryptography, Artificial Neural Networks