Various Approaches towards Cryptanalysis

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 127
Number 14

Year of Publication: 2015

Authors:
Shaligram Prajapat, Ramjeevan Singh Thakur

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
Various Approaches towards Cryptanalysis

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

2. Shivendra Mishra, Dr. Aniruddha Bhattacharya , “Pattern analysis of cipher text : a
combined approach”, proceeding of Recent Trends in Information Technology (ICRTIT), 2013
3. Sushila Omer Sharif, saad P. Mansoor , “Performance evaluation of classifiers of
encryption algorithm”, ACEEE International Journal on Network Security , Vol. 02, No. 04, Oct
2011
4. S. Swapna, A. D. Dileep, C. Chandra Sekhar, and Sri Kant, “Block cipher identification
using support vector classification and regression”, Journal of Discrete Mathematical Sciences
5. Malte Nuhn, Kevin Knight , “Cipher type detection”,
http://www-i6.informatik.rwth-aachen.de/~nuhn/2014-classification-poster.pdf,
pp.1769–1773,2014
6. Sambasiva Rao Baragad, P. Satyanarayana Redd “Studies on the advancements of
Nerual Networks and Neural Network based cryptanalytic works”, International Journal of
Emerging Trends & Technology in Computer Science (IJETTCS),Volume 2, Issue 5, September
– October 2013 ISSN 2278-6856
7. E.C. Laskari, G.C. Meletio, Y.C. Stamatiou, M.N. Vrahatis ,“Cryptography and
Cryptanalysis through Computational Intelligence”, proceeding of Computational Intelligence in
Information Assurance and Security, Studies in Computational Intelligence Volume 57, 2007, pp
1-49
machine using a genetic algorithm”, In proceedings of 7th International Conference on genetic
algorithms,ICGA97,1997
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
3 Issue: 2, pp.273-289,2008
13. P. Khadivi, M. Momtazpour , “Application of Data Mining in Cryptanalysis”,
pp.358-363,2009
15. Arne Winterhof , “Polynomial Interpolation of the Discrete Logarithm”, Vol. 25 Iss: 1,
pp.63-72,2001
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
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