Wolf Pack Algorithm for Cryptanalysis of Symmetric Cryptosystems

T. Mekhaznia[1] and A. Zidani[2]

1. LAMIS Laboratory, University of Tebessa, Algeria
t.mekhaznia@univ-tebessa.dz

2. University of Batna, Algeria
zidani@free.fr

Keywords : Meta-heuristics, WPS Algorithm, Cryptanalysis.

1 Introduction

In recent years and, with the increasing usage of communication networks, the security of information became obvious. The usually way to protect information against misuse or manipulation is to use encryption mechanisms. Cryptanalysis refers to the analysis of ciphers and encrypted information for the purpose to detect their weakness which permits retrieval of its meaning without necessary knowing the secret data that its normally required such encryption key or the algorithm. This fact allows evaluating the efficiency of used cryptosystems in order to perform more robust algorithms. Symmetric encryption methods are actually, popular cryptosystems due to their portability and simplicity of implementation. They operate on large blocks of data by using a fixed transformation. The most common symmetric cryptosystem is DES[1] which characterized by its high speed of encryption and resistance against various attacks[2].

Cryptanalysis has been tackled using several methods, such brute force attack, linear and differential cryptanalysis and heuristic-based methods. In this paper, we present a variant of Wolf Pack Algorithm (WPA) as a meta-heuristic attack of some variant of symmetric cryptosystems. The fitness function is evaluated based on the most common bigrams and trigrams. Results show the effectiveness of the proposed algorithm by reporting results of some preliminary experiments, including comparison results obtained with Particle Swarm Optimization (PSO) [3], Genetic Algorithms (GA) [4] and BAT Algorithm.

2 Cryptanalysis of symmetric cryptosystems using WPA

Wolf Pack Algorithm (WPA) [5] is a new well-known swarm intelligent algorithm used to approximate solutions to various real-word optimization problems. WPA is a population-based meta-heuristic inspired by the social foraging behavior of the jungle predators. It consists basically in making animals (wolves) hunt, find the trace of pry and capture it under the command of a lead wolf. The pry capture is accomplished in three intelligent steps: a) *scouting* wolves walk around and looking for preys, b) when a scout-wolf finds a trace of pry smell it will howl, *ferocious* wolves move fast towards the pry, c) after capturing the pry, it distributed in an order from the strong to weak and causes the dead of weak wolves for lack of food which consists in maintaining an active and strong pack at any time.

In a search space represented by a connected graph of n nodes, each wolf *i* represent a random initial solution of the problem that corresponds to a decryption key *k*, a vector of *n* bits. At each move from node x_i^t to node x_i^{t+1}, the wolf *i* performs a decryption key $k_{x^t,x^{t+1}}$ obtained by swapping the bits x^t and x^{t+1}. The performance of each node corresponds to the cost of text obtained using the decryption key $k_{x^t,x^{t+1}}$ according to a cost function. After a fixed number of iterations (correspond to a scouting phase), the wolf with the best solution becomes a lead wolf, the weak wolf with bad solution will be deleted and replaced by a new generated one. The process will be stopped after a fixed number of iterations or if no improvement in lead wolf solution.

3 Preliminary results

Some experiments have been conducted to test the performance of the proposed algorithm on a set of binary texts of 2400 to 3000 bits. Encryption methods used are Simplified Data Encryption Standard (SDES) [6], 4-rounds Data Encryption Standard (4DES) [7] and Data Encryption Standard. Table 1 shows the results obtained in terms of key length, encryption rounds and much bits.

Table 1. Cryptanalysis results of WPA algorithm

Symmetric cryptosystem	Key-size (bits)	Encryption rounds	Avg. much bits	Avg. Processing Time (s)
SDES	10	16	10	28,12
4DES	56	4	38	71,04
DES	56	16	26	154,27

Table 2 shows results obtained with PSO, BAT and GA.

Symmetric cryptosystem	Avg. much bits		
	PSO	BAT	GA
SDES	10	10	10
4DES	41	35	39
DES	33	25	26

The above results show that the proposed algorithm can be successfully used to solve such problem. We think also, that is possible to improve results by a well choice of environment parameters.

References

[1] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[2] R. Singh, D. B. Ojha (2010). An Ordeal Random Data Encryption Scheme (ORDES), International Journal of Engineering Science and Technology, 2(11), 6349- 6360.

[3] R.C. Eberhart, and J. Kennedy (1995), A New Optimizer Using Particle Swarm Theory. Proceeding of the Sixth International Symposium on Micro Machine and Human Science, Nagoya, Japan, 39-43.

[4] J. Holland (1978). Adaptation in natural and artificial systems. Ann Arbor, MI: university of Michigan Press.

[5] W. Hu-Sheng and Z.Feng-Ming (2014). Wolf Pack Algorithm for Unconstrained Global Optimization. Mathematical Problems in Engineering, V 2014.

[6] E. Schaefer. (1996). A Simplified Data Encryption Standard Algorithm, Cryptologia, 20(1), 77-84.

[7] E.C. Laskari & al. (2005). Evolutionary computation based cryptanalysis: A first study. Nonlinear Analysis: Theory, Methods and Applications 63 e823–e830.