International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 4 1767 – 1769

The Particle Swarm Optimization Based Linear Cryptanalysis of Advanced Encryption Standard Algorithm

Dolly U. Jeswani, Swati G. Kale
Department of Information Technology, Yeshwantrao Chavan College of engineering, Nagpur, India
Jeswanidolly703@gmail.com,s12_kale@yahoo.com

Abstract:- The tremendous development in internet technology, wireless communication and the type of internet capable devices has increased the amount of network usage .Millions of users are associated with the network and thus there is need for network security. The sensitive data that is deposited and transmitted on the internet need protection from attackers and eavesdroppers who perform illegal actions. Cryptography algorithms are the key factor of the security mechanisms used for data storage and uninterrupted network transmissions. The data security purely depends on the Cryptography algorithm hence the keys must be managed in a good way. Security mechanisms are developed when a threat to security is identified. To identify the security risk associated with AES algorithm, a computational intelligence based approach for known cryptanalysis of Advanced Encryption Standard algorithm is introduced. Particle swarm optimization based cryptanalysis is used much now a days because of its fast convergence rate. A PSO oriented cryptanalysis technique for breaking the key used in advance encryption standard algorithm is introduced. This approach is for known cipher text-only attack for an AES encryption system, where the key is deduced in a minimum search space in contrast to the Brute Force Attack. The key used in AES can be detected effectively with Particle Swarm Optimization

Keywords - *Ant Colony Optimization (ACO), Artificial Neural Networks (ANN), Evolutionary Computation (EC), Cryptanalysis, Cryptography, Particle Swarm Optimization (PSO), Swarm Intelligence (SI),Genetic Algorithm (GA).*

*****

I. INTRODUCTION

Cryptography is the technique to encrypt the original message to the unreadable form know as cipher text so that actual recipients can decrypt and read the message [4]. Cryptanalysis is a technique to break cryptographic algorithms and attack the cipher text, without accessing the secret key. Cryptanalysis is a challenging task in cryptology. There are various types of attacks that a crypt analyser use to break a cipher, it depends

upon the amount of information available to the attacker. i.e. known plain text , known cipher text attack etc. The goal is to derive the key, so that the cipher text can be easily decrypted. Advanced Encryption standards is asymmetric block cipher which takes 128 bit plain text as input and generates 128 bit cipher text as output [2] The most known attack is the Brute-Force attack for Cryptanalysis ,which tries every possible combination of numbers, letters and symbols until the desired combination is discovered [11]. To perform Cryptanalysis on AES similar Brute Force attack needs to be done but even with the high speed computers which are available in today's era, it is not feasible to do this Brute Force attack due to the high cost incurred . This problem is solved effectively by Computational Intelligence, without searching the complete key space [1]. The optimization problems can also be solved by evolutionary techniques like Genetic Algorithm [8]. Evolution operations like crossover and mutation are not present in PSO. Swarm Intelligence is an innovative technique which is used for solving the complicated problems like the optimization problems [1].PSO is a population based optimization tool simulating the social behaviour of swarms of bee ,ants or schools of fish . The strength of Particle Swarm Optimization lies in its fast convergence rate , in comparison with many global optimizations like genetic algorithm and simulated annealing .The Strength of PSO lies in its increased convergence rate. It is widely used technique for Cryptography. Particle Swarm Optimization is a method which have some population, inspired by social behaviour of birds and animals such as bee colonies [3]. Population consists of individual particles which wander collectively in a multidimensional search space for finding the best solution known as the global optimum. The particles change their position and velocity as per the local and the global search [5]. The fitness function in PSO is problem-dependent and dynamic. PSO gives a region of the function space with best possible solution. The best position for each particle is retained it went through in its memory. At last, the best position found by all the particles is updated by each particle of the swarm. Optimal key search is the main goal of PSO based cryptanalysis. Finding the key employed in AES Algorithm using the Particle Swarm Optimization is the ultimate goal.

II. RELATED WORK

Cryptanalysis Techniques

A. Brute Force Attack

This is the most common technique which attempts to detect a key by trying every possible combination of numbers, letters and symbols until the desired combination is found [11] . A secret key can always be detected with the brute-force attack, but the difficulty is that it could take years to find it. Based on the key's length and complexity, there could be trillions of possible combinations The Brute Force attack needs 2^n combinations for a key length n i.e. for a 56 bit key it requires 2^{56} no. of combinations which is really difficult and a time consuming task [2]. The key used in AES can be detected with Brute Force Attack but as AES is very complex and due to large no of rounds in AES, it is very tedious task to apply the Brute Force technique.

B. Genetic Algorithm

It is an evolutionary algorithm which is used for the Cryptanalysis of block ciphers [6]. A Genetic algorithm works with several operations such as crossover and mutation. Considering the cipher text attack only few keys are produced based on their cost function value which depends on the frequency of the letters. Cryptanalysis of Four round DES based on genetic algorithm is already implemented [13] .To find the optimum keys, an efficient fitness measure is used which is based on higher fitness values. The valuable bits in these optimum keys that generate some sort of deviation from the various observed bits will turn up and these valuable bits can be considered to find other bits . The genetic algorithm takes large amount of time even several days for the cryptanalysis of block a ciphers. In the case of AES it would be a tough task for Cryptanalysis with Genetic Algorithm though it surely finds the secret key.

C. Support Vector Machine

Support vector machine is used to identify the encryption method i.e. cryptographic key. The identification of key bits from cipher text only attack is known as a document categorization task[7] . For generating a document vector from a cipher text, the common dictionary based and the class specific methods are considered. Due to the large dimension of document vector, support vector machines (SVM) based classifiers are used for detection of the cryptographic key.

D. *Ant Colony Optimization*

Ant Colony Optimization is used for the cryptanalysis of four-rounded Data Encryption Standard (DES) [12]. To recover the key of DES a known plaintext attack is used. A directed graph acts as the environment for the ants, which is the search space, and is used for finding the secret key. To measure the quality of a solution a heuristic function is used. On the basis of routes completed by ants various optimum keys are computed. The computed optimum keys are used to deduce each bit of the 56 bit cryptographic key used by DES. Similar Algorithm can be used for the AES Cryptanalysis purpose but the complexity would naturally increase because AES is more complex than DES.

E. Neural Networks

Artificial neural networks are the parallel interconnections of neurons which are the simple processing which work as a collective system. Neural Networks are used for the Cryptanalysis of a fiestel type block cipher. This type of attack is quite obvious, it involves construction of a set of know plain text - cipher text pairs , where a neural network is trained using the part of that set. The training is performed between the partially decrypted cipher text and the input to the last round by assuming the last round key .To test the output of the network and a record of the error between actual output of the neural network and the real output he rest of the set is used and the real output is recorded. Every sub key value is tried and then the key with the minimum error is assumed as correct key .The set of the minimum error values is used to do the local search. The attack was implemented and tested on a hypothetical cipher that is immune to known other attacks [10]

III. PROPOSED WORK

In the proposed work, the concept of Computational Intelligence i.e. Swarm Intelligence is applied here to find the optimum solution in the terms of a minimum search space of certain amount of population.. The swarm particles are associated with velocity and their position and by using the cost function and various other computations the best solution is computed in a specific time period. In terms of AES, the bits of Cryptographic key or the encryption key are deduced by using this Particle Swarm Optimization which is a Swarm Intelligence tool . The Particle Swarm Optimization is a powerful tool which guarantees the efficient and the optimized solution. The proposed work finds the bits of secret key used in the Advanced Encryption Standard Algorithm to some extent. The no of bits identified depends on the key length. Hence larger the key length, more complex it is to deduce the bits, The key length used here will be either 16 ,32 or 64 bits. The percentage of result obtained would be based on the key length.

IV. FLOW OF PROPOSED WORK

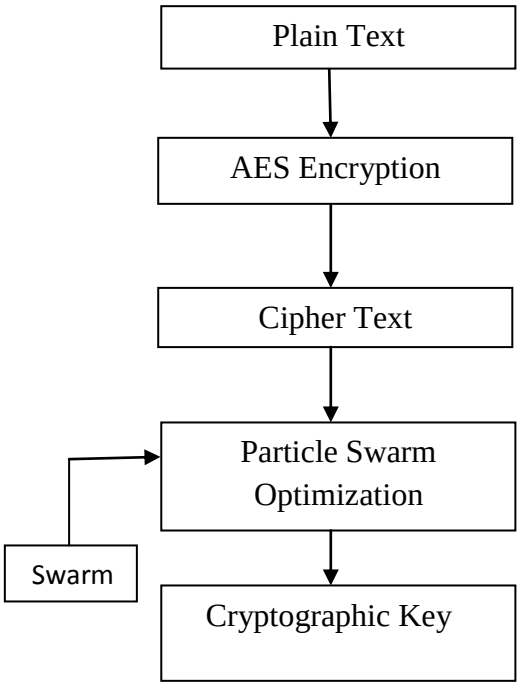

Figure 1: Flowchart of proposed model

V. EXPERIMENTAL SETUP AND RESULTS

The Proposed Work is implemented in MATLAB. MATLAB provides the PSO toolbox which is used for the Optimization purpose. The Particle Swarm Optimization

technique is applied on the Advanced Encryption Standard (AES). The key lengths used in the system are 16, 32 ,64 and 128 bits. The Results obtained for each of these key size is distinct. For the key Length 16 bit , 15 bits are identified from 16 bits i.e. 93.75 %. For the Key Length of 32 bits,24 bits are identified i.e. 75%, For the key Length of 64 bits, 40 bits are identified i.e 62.5 % and for the Key Length 128 bits , 76 bits are identified i.e 59.37%.

VI. CONCLUSION AND FUTURE SCOPE

Swarm Intelligence based Cryptanalysis provides with a best and the optimized solution. A new approach has been used for Linear Cryptanalysis of Advanced Encryption Standards (AES) Algorithm using Particle Swarm Optimization. The fitness function used in this method ensures the efficient solution. This technique identifies the bits of the Cryptographic key successfully using cipher text only attack ensuring the minimum search space i.e less overhead and the time efficient solution. The PSO is applied to the AES having the key length 128 bits. 76 bits are identified and the percentage of result obtained is 59.37 and the elapsed time is 17.3 sec. The use of Particle Swarm Optimization has led to the good reduction factor in Linear Cryptanalysis.

Improving the Particle Swarm Optimization by modifying the Parameters and its values to yield better result for the Linear Cryptanalysis of Advanced Encryption Standard Algorithm The PSO algorithm may be applied to the AES for the key length of 192 bits and 256 bits in future.

VI . REFERENCES

[1] Vimalathithan R. and M.L.Valarmathi "*Cryptanalysis of Simplified-AES using Particle Swarm Optimisation*"KPR Institute of Engineering and Technology, Coimbatore–641 404, India Government College of Technology, Coimbatore–641 013, India

[2] Behrouz A. Forouzan. "*Cryptography and Network security*".Tata Mc-Graw Hill, Special Indian Edition (2007)

[3] Engelbrecht, A.P. (2007*)" Computational Intelligence: An Introduction*". 2nd ed. Chichester : Wiley

[4] Stallings, W. "*Cryptography and Network Security Principles and Practices*". Pearson Education, (2004).

[5] Eberhart, R.C. and Kennedy, J. (2001) "*Swarm Intelligence*". London: Morgan Kauf-mann Publishers.

[6] R, Vimalathithan., and Valarmathi, M. L., "*Cryptanalysis of SDES using Genetic Algorithm*". International Journal of Recent Trends in Engineering, vol. 2, no. 4, pp.76-79, Nov. 2009

[7] Dileep A. D, and C. Chandra Sekhar "*Identification of Block Ciphers using Support Vector Machines*" International Joint Conference on Neural Networks Sheraton Vancouver Wall Centre Hotel,Vancouver, BC, Canada July 16-21, 2006

[8] Song, J., Zhang, H., Meng, Q., and Wang, Z., "*Cryptanalysis of Four-Round DES Based on Genetic Algorithm*". International Conference on Wireless Communications Networking and Mobile Computing, Issue 21-25, pp. 2326-2329. (2007).

[9] Anjali Dadhich ,Abhishek, Gupta, Surendra Yadav:"*Swarm Intelligence based Linear Cryptanalysis of Four-round Data Encryption Standard Algorithm"* International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)(2014)

[10] Ayman M. B. Albassal and Abdel-Moneim A. Wahdan" *Neural Network Based Cryptanalysis of a Feistel Type Block Cipher*" 0-7803-8575-6/04/$20.00 02004 IEEE

[11] *G. Sowmya, A. Naveen Kumar*, Jaya Prakash " *Brute Force Attack – Blocking Techniques*". International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume2 Issue 8 August, 2013 Page No. 2541-2543

[12] Salabat Khan, Waseem Shahzad, Farrukh Aslam Khan." *Cryptanalysis of Four-Rounded DES using Ant Colony Optimization*" 978-1-4244-5943-8/10/$26.00 ©2010 IEEE

[13] Jun Song, Huanguo Zhang, Qingshu Meng, Zhangyi Wang." *Cryptanalysis of Four-Round DES Based on Genetic Algorithm*" 1-4244-1312-5/07/$25.00 © 2007 IEEE