International Journal of Technology and Science, ISSN (Online) 2350-1111, (Print) 2350-1103 Volume 3, Issue 4, 2016 pp. 42-44

Cryptanalysis for S-DES using Genetic Algorithm

Ms. P. A. Bagane[1], and Prof. Dr. S. Kotrappa[2]
[1]CSE Department, SITCOE, Yadrav – Ichalkaranji, India
Email: poojabagane@sitcoe.org.in
[2] CSE Department, KLE Dr. MSSCET, Belgaum, India
Email: kotrappa06@gmail.com

***Abstract*— Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptanalysis which is one of the parts of cryptography refers to the study of ciphers, cipher text, or cryptosystems with a view to finding weaknesses in them that will permit retrieval of the plaintext from the cipher text, without necessarily knowing the key or the algorithm. Genetic Algorithms (GA) is typically used to obtain solution for optimization and search problems. This paper presents implementation of GA as application in the field of cryptanalysis for breaking the S-DES.**

Index Terms **— Cipher, Cryptanalysis, Genetic Algorithms, and S-DES.**

I. Introduction

Cryptanalysis is the process of attempting to recover the plaintext and /or key from a cipher text. In the Brute Force attack the attacker tries every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained; it has the disadvantage of high computational complexity. In order to overcome this drawback, the optimization heuristics techniques like Genetic Algorithms (GA) are used. Genetic algorithms (GA) are adaptive heuristic search algorithms based on the evolutionary ideas of natural selection and genetics which are based on the principle of Darwinian idea of survival of the fittest and natural genetics [1]. S-DES is a simplified version of the Data Encryption Standard (DES). This algorithm is not cryptographically secure. It was originated by Edward Schaefer, the professor at Santa Clara University [2].The S-DES encryption algorithm takes an 8-bit block of plaintext (example: 10111101) and 10-bit key as input and produces an 8-bit block of cipher text as output, while the S-DES decryption algorithm takes an 8-bit block of cipher text and the same 10-bit key used to produce that cipher text as input and produces the original 8-bit block of plaintext [3]. The most focus of work is on the use of a GA to conduct a directed random search of a key space and to guess the Plain Text.

The rest of the paper is organized as follows: In section 2 about Cryptanalysis, S-DES, and Genetic Algorithms. Section 3 gives review of previous related work. Section 4 gives the implementation details. Section 5 gives a detailed description of the problem instances and results. Finally, we outline the conclusions of our study.

II. Cryptanalysis, S-DES, and Genetic Algorithms

This section gives the brief idea about Cryptanalysis, S-DES, and Genetic Algorithms.

A. *Cryptography and Cryptanalysis*

Cryptography is the art of secret writing. More generally, people think of cryptography as the art of mangling information into apparent unintelligibility in a manner allowing a secret method of unmangling. The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. It consists of two complementary fields of study: cryptography and cryptanalysis [3]. Traditional use of cryptography: A message in its original form is known as plaintext or clear text. The mangled information is known as cipher text. The process for producing cipher text from plaintext is known as encryption. The reverse of encryption is called decryption.

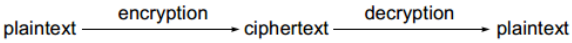

Figure 1. Basics of Cryptography

While cryptographers invent clever secret codes, cryptanalysts attempt to break these codes. Cryptanalysis refers to the study of ciphers, cipher text, or cryptosystems (that is, to secret code systems) with a view to finding weaknesses in them that will permit retrieval of the plaintext from the cipher text, without necessarily knowing the key or the algorithm [2]. Breaking is sometimes used interchangeably with *weakening*. This refers to finding a property (fault) in the design or implementation of the cipher that reduces the number of keys required in a brute force attack which is, simply trying every possible key until the correct one is found. Cryptanalysis Problem is one of the types of Optimization problem where we have to minimize the time and maximize the accuracy.

B. *S-DES*

Simplified DES is an algorithm that has many features of the DES, but is much simpler then DES [2]. Like DES, this algorithm is also a bock cipher. In Simplified DES, encryption/decryption is done on blocks of 12 bits. The plaintext/cipher text is divided into blocks of 12 bits and the algorithm is applied to each block.

C. Genetic Algorithms

International Journal of Technology and Science, ISSN (Online) 2350-1111, (Print) 2350-1103 Volume 3, Issue 4, 2016 pp. 42-44

Genetic Algorithms (GAs) are randomized yet structured search and optimization algorithms based on the evolutionary ideas of natural selection and genetics [1]. GAs simulates the survival of the fittest among individuals over consecutive generations for solving a problem. Each generation consists of a population of individuals. Each individual represents a point in a search space and a possible solution. The individuals in the population are then made to go through a process of evaluation through three operators. Selection operator equates the survival of the fittest. Crossover operator represents mating between individuals. Mutation introduces random modification.

The basic GA procedure has following operation:

1. Initialization.

GAs usually generates the initial population of candidate solutions randomly according to a uniform distribution over all admissible solutions. However, the initial population can sometimes be biased using prior problem-specific knowledge or other optimization procedures.

2. Selection.

Each GA iteration starts by selecting a set of promising solutions from the current population based on the quality of each solution. Selection operator equates the survival of the fittest.

3. Variation.

Once the set of promising solutions has been selected, new candidate solutions are created by applying recombination (crossover) and mutation to the promising solutions. Crossover operator represents mating between individuals. Mutation introduces random modification. For example, if original streams are 10010011 and 11001110, then crossover result streams are 10011110 and 11000011. If original stream is 10010011, then mutation result is 10000111.

4. Replacement.

After applying crossover and mutation to the set of promising solutions, the population of new candidate solutions replaces the original one or its part, and the next iteration is executed (starting with selection) unless termination criteria are met.

Genetic algorithms are proven to be one of the effective techniques to solve different Optimization problems.

III. Related Work

Different algorithms for Cryptanalysis are found in the literature such as Genetic Algorithm, Brute force Attack Algorithm, Particle Swarm Optimization Algorithm etc. Farah Al Adwan, Mohammad Al Shraideh etl [3] presents GA with an improved crossover operator was used for the cryptanalysis of Simplified data encryption standard problem (S-DES). Results have shown that GA performance is better than brute force search technique in breaking S-DES key.

The cipher text attack only is considered by Lavkush Sharma, Bhupendra Kumar Pathak & Ramgopal Sharma [4] and several keys are generated in the different run of the genetic algorithm on the basis of their cost function value which depends upon frequency of the letters. The results on the S-DES indicate that, this is a promising method and can be adopted to handle other complex block ciphers like DES, AES.

Poonam Gerg [5] explored the use of genetic algorithm to break a simplified data encryption standard algorithm (SDES). To test its performance, she compared the implemented genetic algorithm attack with brute force search algorithm attack. Through extensive experiments and analysis it can be concluded that genetic algorithms attack run ten times faster than brute force search algorithm attack with accuracy. A generalized version of cryptanalysis of SDES will give better insight into the attack of DES and other cipher.

IV. Implementation of Algorithm

This section describes our implementation that uses steady state genetic algorithms, the solution representation, and the operators employed. We have implemented the attack using "Java" language. The attack is implemented by generating independent keys to represent the target key. The first generation is generated randomly using a simple uniform function.

Solution representation: In this work we have used 1D representation of Text.

Steady state genetic algorithms: The implemented steady-state genetic algorithms works with 20% overlapping populations. In each generation, the original population size is maintained by replacing a portion of the population by the newly generated individuals. The genetic operators applied are, standard roulette wheel selection, one point crossover with probability 0.8 and swap mutation with probability 0.01. Table 1 describes the parameters of Genetic Algorithm.

Type of Genetic Algorithm	Steady State Genetic Algorithm
Solution Representation	1D Representation
Selection	Standard roulette wheel selection
Crossover	Single Point crossover
Crossover Probability	0.8
Mutation	Swap Mutation
Mutation Probability	0.2

Table 1. Parameters of Genetic Algorithm

V. Results & Discussion

This section gives details of results obtained by Genetic Algorithms for breaking S-DES. Genetic Algorithm is implemented using Java. Standard genetic algorithms components from GAlib [1] are used in genetic implementation. The attack had been implemented several times, initial genetic algorithm parameters were used in the experiment are listed in Table 1.

We are taking key size and Cipher Text as Input. After applying the Genetic Algorithm, we got the

International Journal of Technology and Science, ISSN (Online) 2350-1111, (Print) 2350-1103 Volume 3, Issue 4, 2016 pp. 42-44

optimal output. Figure 2 shows the picture of Output by Genetic Algorithm.

Figure 2. Output by GA on S-DES

CONCLUSIONS

This paper presents Genetic algorithms for breaking S-DES. The problem is formulated as optimization problem where objective is to minimize the total time of execution. 1D solution representation is used. Genetic provides good results with time objective. In all the experiments results obtained with genetic algorithms are slightly better than traditional attack. Results indicate that GAs are subject to premature convergence. As a part of our future work, we would like to improve the performance of algorithms and test for other advanced ciphers like AES, DES.

APPLICATIONS. REFERENCES

[1] Goldberg, D. E., "*Genetic Algorithms in Search, Optimization, and Machine Learning*", Addison-Wesley, 1989.

[2] Williams Stallings, "*Cryptography and Network security Principles and Practices"*, Pearson Education.

[3] Farah Al Adwan , Mohammad Al Shraideh etl, "*A Genetic Algorithm Approach for Breaking of Simplified Data Encryption Standard*", International Journal of Security and Its Applications, Vol.9, No.9 (2015), pp.295-304.

[4] Lavkush Sharma, Bhupendra Kumar Pathak & Ramgopal Sharma, "*Breaking of Simplified Data Encryption Standard Using Genetic Algorithm*", Global Journal of Computer Science and Technology, Volume 12 Issue 5, March 2012.

[5] Poonam Garg," *Genetic Algorithm Attack on Simplified Data Encryption Standard Algorithm*", Research in Computing Science 23, pp. 139-149, 2006.

[6] Farhat Ullah Khan, Surbhi Bhatia, "*A Novel Approach To Genetic Algorithm Based Cryptography"*, International Journal of Research in Computer Science, ISSN 2249-8265 Volume 2 Issue 3 pp. 7-10, 2012.

[7] Sonia Goyat, "*Cryptography Using Genetic Algorithms (GAs)*", IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 1, Issue 5, PP 06-08, May-June 2012.