American Journal of Networks and Communications
2015; 4(3): 32-36
Published online April 24, 2015 (http://www.sciencepublishinggroup.com/j/ajnc)
doi: 10.11648/j.ajnc.20150403.12
ISSN: 2326-893X (Print); ISSN: 2326-8964 (Online)

Cryptanalysis of Simplified Data Encryption Standard Using Genetic Algorithm

Purvi Garg, Shivangi Varshney, Manish Bhardwaj

Department of Computer Science and Engineering, SRM University, Modinagar, Utter Pradesh, India

Email address:
purvigarg71@gmail.com (P. Garg), shivangi.varshney100@gmail.com(S. Varshney), aapkaapna13@gmail.com(M. Bhardwaj)

To cite this article:
Purvi Garg, Shivangi Varshney, Manish Bhardwaj. Cryptanalysis of Simplified Data Encryption Standard Using Genetic Algorithm. *American Journal of Networks and Communications*. Vol. 4, No. 3, 2015, pp. 32-36. doi: 10.11648/j.ajnc.20150403.12

Abstract: Cryptanalysis of cipher text using evolutionary algorithm has gained much interest in the last decade. In this paper, cryptanalysis of SDES has been performed using Genetic Algorithm with Ring Crossover operator. Cryptography has been prone to many attacks but the scope of this paper is limited only to the cipher text attack. Different combinations of keys are generated using the Genetic Algorithm and hence it is concluded that Genetic Algorithm is a better approach than the Brute Force for analyzing SDES.

Keywords: Cryptanalysis, Cipher Text Attack, SDES, Genetic Algorithm, Brute Force, Key Search Space

1. Introduction

Cryptography, a word with Greek origins, means "secret writing." It is basically the science and art of transforming messages to make them secure and immune to attacks. But we cannot completely immune ciphers from different attacks and this attacking or breaking of ciphers is termed as cryptanalysis, in which the intruder converts the cipher text into plaintext with or without knowing the key.

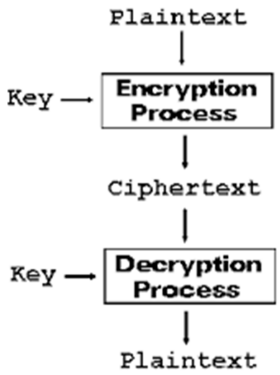

Fig. 1. *The process of cryptography [23].*

Cryptographic systems have a finite key space so that the intruder can easily search for a key, but still the system remains secure because of the size of the key search space.

And hence, optimization techniques have got significant importance in finding the solution (key), by optimizing key search space. In this paper, we are working on the cryptanalysis of Simplified Data Encryption Standard (S-DES), using Genetic Algorithm and Brute Force.

2. Related Works

Cryptanalysis has got much attention in the last few years. In the year 1993, R.Spillman used Genetic Algorithm to attack the Knapsack cipher [4] and substitution ciphers [5]. The first experimental cryptanalysis of DES using a linear cryptanalysis technique was shown by Matusi in [7]. An important analysis on how different optimization techniques can be used in the field of cryptanalysis is shown in by Clark [6]. In 2006 Nalini [3] used GA, Tabu search and Simulated Annealing techniques to break S-DES. Later in 2008, Garg [1, 2] presented the use of memetic algorithm and genetic algorithm to break a simplified data encryption standard algorithm. Vimalathithan [9] also used GA to attack Simplified-DES. In 2012, Sharma and others [21] showed the breaking of the S-DES using Genetic Algorithms.

3. The S-Des Algorithm

Simplified Data Encryption Standard (S-DES) is developed by Edward Schaefer of Santa Clara University. The S-DES [8, 10] is an encryption algorithm which is basically designed for educational purpose. It is not sufficiently secure. This algorithm takes 8 bit block of plaintext and a 10 bit key as input and gives 8 bit block of

cipher text asoutput. This is the encryption process. To get the plaintext back, we again provide the 8 bit block of cipher text and the same 10 bitkey that was given at the time of encryption, as an input to the decryption algorithm and the 8 bit block of plaintext is obtained as the output.

In the process of encryption, five basic functions are used: an initial permutation (IP), a complex function labeled f_k which involves both permutation and substitution operations and depends on a key input, a simple permutation function that switches (SW) the two halves of the data, the function $f_k$again and a permutation function that is the inverse of the initial permutation (IP–1).

Key Generation for f_k

For key generation, a 10-bit key is considered fromwhich two 8-bit sub keys are generated. In this case, the key is first subjected to a permutation P10= [3 5 2 7 4 10 1 98 6], then a shift operation is performed. The numbers in the array represent the value of that bit in the original 10-bit key. The output of the shift operation then passes through a permutation function that produces an 8-bit output P8 = [6 3 74 8 5 10 9] for the first sub key (K1). The output of the shift operation also feeds into another shift operation and another instance of P8 to produce the second sub key

K2. In all bit strings, the leftmost position corresponds to the first bit.

A) Initial and Final Permutations

The input to the algorithm is an 8-bit block of plaintext, which we first permute using the IP function IP= [2 6 3 1 4 8 5 7].This retains all 8-bits of the plaintext but mixes them up. At the end of the algorithm, the inverse permutation is applied; the inverse permutation is done by applying, IP-1 = [4 1 3 5 7 2 8 6] where we have IP-1(IP(X)) =X.

B) The Function f_k

The function f_k, which is the complex component of S-DES, consists of a combination of permutation and substitution functions. The functions are given as follows. Let L, R be the left 4-bits and right 4-bits of the input, then, f_k (L, R) = (L XOR f(R, key), R) Where XOR is the exclusive-OR operation and key is a sub -key. Computation of f(R, key) is done as follows.

1. Apply expansion/permutation E/P= [4 1 2 3 2 3 4 1] to input 4-bits.
2. Add the 8-bit key (XOR).
3. Pass the left 4-bits through S-Box S0 and the right 4-bits through S-Box S1.
4. Apply permutation P4 = [2 4 3 1].

The S-boxes operate as follows:

$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array}$$

$$S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

Fig. 2. *Working of S –box [19].*

The first and fourth input bits are treated as 2-bit numbers that specify a row of the S-box and the second and third input bits specify a column of the S-box. The entry in that row and column in base 2 is the 2-bit output.

C) The Switch Function

The function f_k only alters the leftmost 4 bits of the input. The switch function (SW) interchanges the left and right 4 bits so that the second instance of f_k operates on a different 4 bits. In this second instance, the E/P, S0, S1, and P4 functions are the same. The key input is K2.

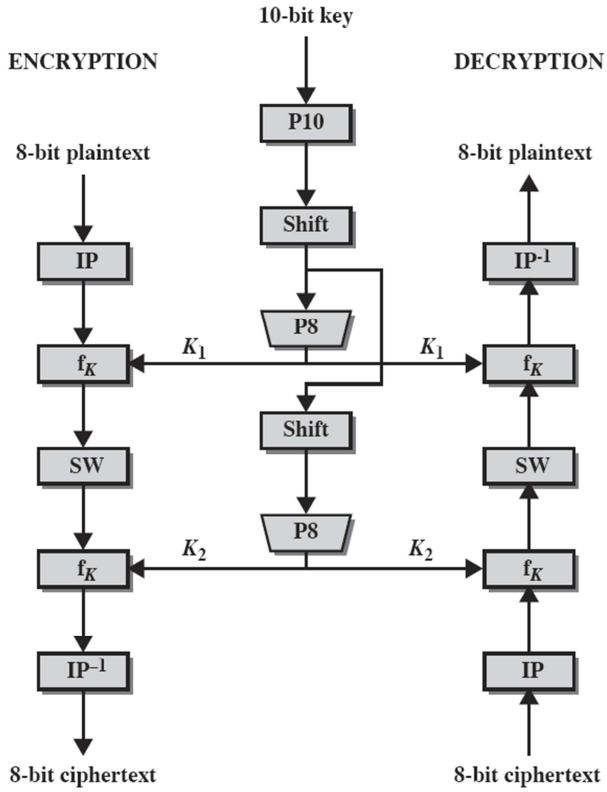

Fig. 3. *The Simplified Data Encryption Algorithm [19].*

4. The Genetic Algorithm

The genetic algorithm is an optimization and search algorithm based on natural selection. GA is a subclass of EA and works on two basic things: Genetic Representation of the solution domain and Fitness function to evaluate solution domain. To some extent, heuristics used in the genetic algorithm is an important reason of its success. The GA involves three basic operations: Selection, Crossover and Mutation.

A) Selection

In this step, we basically decide which chromosomes will take part in evolution process. We use the fitness function to decide the fitness of the chromosome, more the fitness of chromosome, more number of times, it will be selected in the process of evolution.

B) Crossover

In this step, we create a new generation of population by combining the parents and producing off spring. There are

different types of crossover operators which can be used to produce new population. In this paper we are using the ring crossover operator. In ring crossover, we combine two parents and form a ring, and then randomly select a crossover point, and with reference to this point, one of the children is created in clock wise direction and the other one is created in anticlockwise direction. In ring crossover operator, swapping and reversing processes are also included.

C) Mutation

Mutation is used to prevent falling all solution in the population into a local optimum of solved problem. In mutation, bits are randomly interchanged or altered to differentiate new population of solution from the existing one.

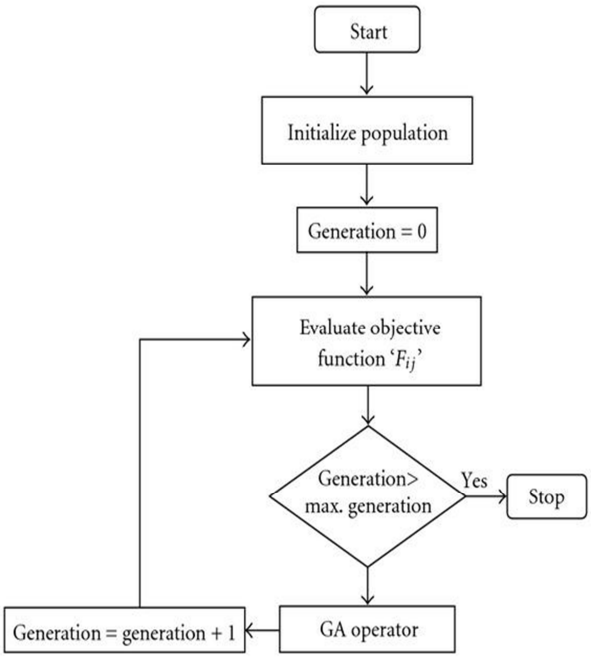

Fig. 4. *Flowchart showing the steps of Genetic Algorithm [22].*

5. Brute Force

Brute Force is a traditional search algorithm. In Brute Force algorithm, all possible keys are checked until the correct one is found. In the worst case, it may be possible that the correct key is the last key of the entire search space. With a key of 56 bits, there are 2^{56} possible keys i.e., $7.2X10^{16}$ keys approximately. Assuming, on an average half the key space has to be searched, a single machine performing one S-DES encryption per microsecond would take more than a thousand years to break the cipher.

6. Objective

The goal of this paper is to perform a comparison between Brute Force Search Algorithm and Genetic Algorithm and to show the use of Genetic Algorithm in the field of cryptanalysis. The primary goals of this work are to produce aperformance comparison between traditional Brute forcesearch algorithm and genetic algorithm with improvedparameters based method, and to determine the use oftypical GA-based methods in the field of cryptanalysis.

The procedure to carry out the cryptanalysisusing GA in order to break the key is as follows:

1. Input: cipher text, and the language statistics.
2. Randomly generate an initial pool of solutions (keys).
3. Calculate the fitness value of each of the solutions inthe pool using equation (1).
4. Create a new population by repeating followingsteps until the new population is complete
   a. Select parent (keys) from a current population according to their fitness value (the better fitness, the bigger chance to be selected). Here Tournament selection is used.
   b. With a crossover probability cross over the parents to form new offspring (children). In our genetic algorithm we are using Ring Crossover Operator
   c. For each of the children, perform a mutation operation with some mutation probability to generate new children.
   d. Place new children in the new population
5. Use new generated population for a further run of the algorithm.
6. If the end condition is satisfied, stop, and return the best solution in current population

A. Cost Function [19]

Equation (1) is a general fitness function usedto determine the suitability of an assumed key (k). Here, Adenotes the language alphabet (i.e., for English, [A. Z, _], where _ represents the space symbol), K and Ddenote known language statistics and decryptedmessage statistics, respectively, and the u, b, and tdenote the unigram, diagram and trigram statisticsrespectively; α, β and γ are the weights assigning different weights to each of the three statistics where $\alpha + \beta + \gamma = 1$. In view of the computational complexity of trigram, only unigram and diagram statistics are used.

$$C^K = \alpha \sum (i \varepsilon \bar{A}) |K(i)^u - D(i)^u| + \beta \sum (i, j \varepsilon \bar{A}) | K(i, j)^b - D(i, j)^b | + \Upsilon \sum (i, j, k \varepsilon \bar{A}) | K(i, j, k)^t - D(i, j, k)^t | \quad (1)$$

7. Result & Discussion

There are a variety of cost functions used by other researchers in the past. The most common cost function uses gram statistics. Some use a large amount of grams while others only use a few. Equation 1 is a general formula used to determine the suitability of a proposed key. A number of experiments have been carried out by giving different inputs and applying genetic algorithm and Brute force attacks for breaking Simplified Data Encryption Standard. The results are shown in table1.The table below shows that the key bits matched using GA and Brute Force search algorithm for the given cipher text .the choice of the Genetic Operators play a vital role in GA and are described below:

GA Parameters

The following are the GA parameters used during the experimentation:

Population Size: 100
Selection: Tournament Selection operator
Crossover Ring Crossover
Crossover: .85
Mutation: .02
No. of Generation: 50

Table I. *Comparison of GA and Brute Force Algorithm [19].*

S. No	Amount Of Cipher Text	No. of bits matched using GA	No. of bits matched using Brute Force Search	Time Taken by GA (M)	Time Taken by Brute Force Search (M)
1.	200	5	5	4.7	24.3
2.	400	4	3	2.1	24.7
3.	600	7	6	1.9	23.6
4.	800	8	7	3.1	24.1
5.	1000	9	7	2.6	25.1
6.	1200	9	8	2.1	25.5

From the above table, it is found that both GAworks better than Brute force algorithm in terms of timetaken as well as obtaining number of key bits.

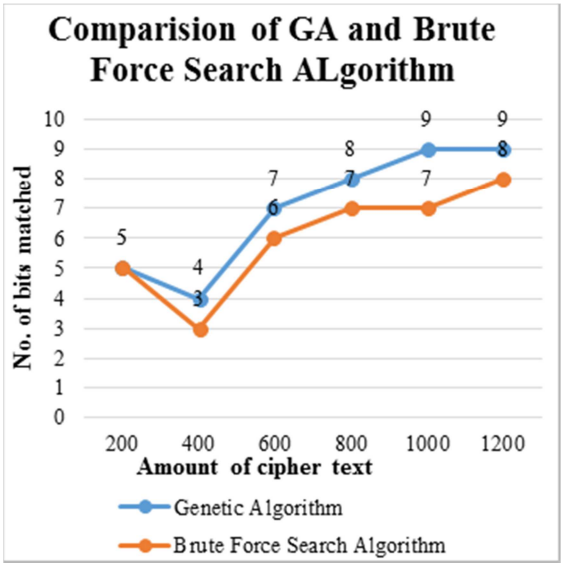

Fig. 5. *Comparison of Genetic algorithm and BruteForce Search algorithm [19].*

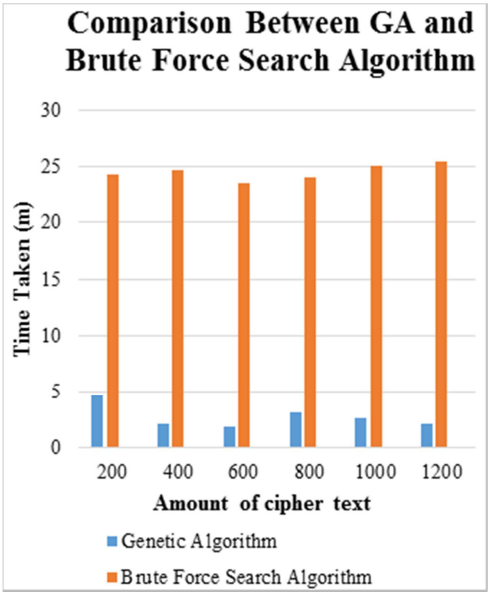

Fig. 6. *The running time comparison of GeneticAlgorithm and Brute Force Search Algorithm [19].*

8. Conclusion

To conclude, in this paper we have discussed the working process of S-DES. We have mentioned the causes for the success of Genetic Algorithm and its 3 basic operations: selection, crossover and mutation. We have pointed out the loopholes of the Brute force attack. Hence proving the success of Genetic Algorithm over brute force in the cryptanalysis of the cipher text.

References

[1] G Poonam, Memetic Algorithm Attack on Simplified Data Encryption Standard algorithm, proceeding of International Conference on Data Management, February 2008, pg 1097-1108.

[2] Garg Poonam, Genetic algorithm Attack on Simplified Data Encryption Standard Algorithm, International journal Research in Computing Science, ISSN1870-4069, 2006.

[3] Nalini, Cryptanalysis of S-DES via Optimization heuristics, International Journal of Computer Sciences and network security, vol 6, No 1B, Jan 2006.

[4] Spillman, R.: Cryptanalysis of Knapsack Ciphers Using Genetic Algorithms.Cryptologia XVII(4), 367– 377 (1993)

[5] Spillman, R., Janssen, M., Nelson, B., Kepner, M.: Use of A Genetic Algorithm in the Cryptanalysis of simple substitution Ciphers. Cryptologia XVII(1), 187–201 (1993)

[6] Clark A and Dawson Ed, "Optimisation Heuristics for the Automated Cryptanalysis of Classical Ciphers", Journal of Combinatorial Mathematics and Combinatorial Computing, Vol.28,pp. 63-86, 1998.

[7] M. Matsui, Linear cryptanalysis method for DES cipher, Lect. Notes Comput. Sci. 765 (1994) 386– 397.

[8] William Stallings, Cryptography and Network Security Principles and Practices, Third Edition, Pearson Education Inc., 2003.

[9] Vimalathithan.R, M.L.Valarmathi, "Cryptanalysis of SDES Using Genetic Algorithm", International Journal of Recent Trends in Engineering, Vol2, No.4, November 2009, pp.76-79.

[10] Schaefer E, "A Simplified Data Encryption Standard Algorithm", Cryptologia, Vol .20, No.1, pp. 77-84, 1996.

[11] Yılmaz Kaya, Murat Uyar, Ramazan Tekdn," A Novel Crossover Operator for Genetic Algorithms: Ring Crossover".

[12] Davis,L. "Handbook of Genetic Algorithm",Van Nostrand Reinhold, New York,1991.

[13] D. E. Goldberg,"Genetic algorithms in search. Optimization and Machine Learning.Reading. M.A. addison -Wesley.1989.

[14] A, Michalewiez and N. Attia." Evolutionary optimization of constrained problems." InProc.3rd annu. Conf. on Evolutionary Programming. 1994.pp 98-108

[15] Z. Michalewicz. "Genetic algorithms+ Data structures = Evolution programs 3rd Ed. New York. Springer,1996.

[16] N.Koblitz, "A Course on number theory and cryptography", Springer-Verlag New York,Inc., 1994.

[17] Alfred J. Menezes. Menezes, Alfred J. Handbook of Applied Cryptography, CRC, 1997.

[18] R. Toemeh, S. Arumugam, Breaking Transposition Cipher with Genetic Algorithhm Electronics and Electrical Engineering,ISSN 1392 – 1215 2007. No. 7(79).

[19] Lavkush Sharma , Bhupendra Kumar Pathak & Ramgopal Sharma Breaking of Simplified Data Encryption Standard Using Genetic Algorithm

[20] Kalyanmoy Deb, Multi-objective Optimization using Evolutionary Algorithms, John Wiley and Sons, 2001.

[21] C.W. Wu and N. F. Rulkov, Studying chaos via 1-Dmaps—atutorial, IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications, vol. 40, no. 10, pp. 707–721, 1993.

[22] http://www.hindawi.com/journals/mse/2009/540895/fig1/

[23] http://www.decodesystems.com/mt/98oct/crypt.html.