Breaking of Simplified Data Encryption Standard Using Genetic Algorithm

By Lavkush Sharma, Bhupendra Kumar Pathak & Ramgopal Sharma

Fet Rbs College, Agra

Abstract - Cryptanalysis of ciphertext by using evolutionary algorithm has gained so much interest in recent years. In this paper we have used a Genetic algorithm with improved crossover operator (Ring Crossover) for cryptanalysis of S-DES. There so many attacks in cryptography. The cipher text attack only is considered here 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.

Keywords: Cryptanalysis, Ciphertext attack, Simplified Data Encryption Standard, genetic algorithm, Key search space

GJCST Classification: E.3

Strictly as per the compliance and regulations of: Open Association of Research Society, USA
Breaking of Simplified Data Encryption Standard Using Genetic Algorithm

Lavkush Sharma\textsuperscript{a}, Bhupendra Kumar Pathak\textsuperscript{b} & Ramgopal Sharma\textsuperscript{c}

Abstract - Cryptanalysis of ciphertext by using evolutionary algorithm has gained so much interest in recent years. In this paper we have used a Genetic algorithm with improved crossover operator (Ring Crossover) for cryptanalysis of S-DES. There so many attacks in cryptography. The cipher text attack only is considered here 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.

Keywords : Cryptanalysis, Ciphertext attack, Simplified Data Encryption Standard, genetic algorithm, Key search space

I. INTRODUCTION

A cipher is a secret way of writing in which plaintext is converted into a scrambled (encrypted) version of the original message (ciphertext) by using a key. Those who know the key can easily decrypt the ciphertext back into the plaintext. Cryptanalysis is the study of breaking ciphers that is finding the key or converting the ciphertext into the plaintext without knowing the key. Many cryptographic systems have a finite key space and, hence, are vulnerable to an exhaustive key search attack. Yet, these systems remain secure from such an attack because the size of the key space is such that the time and resources for a search are not available. Optimization techniques have got a significant importance in determining efficient solutions of different complex problems. One such problem is to break S-DES. This paper considers cryptanalysis of S-DES. In the brute force attack, the attacker tries each and every possible key on the part of cipher text until desired plaintext is obtained. A brute force approach may take so much time to guess the real key which is used to generate a cipher text, so the difficulty of breaking the cipher is directly proportional to the number of keys. On the other hand optimization technique can be used for the same purpose. Genetic algorithm is an evolutionary algorithm that works well and takes less time to break cipher as compared to Brute force attack.

The remaining paper is organized as follows: Section II discusses the earlier works done in this field. Section III presents overview of S-DES and Section IV gives the overview of Genetic Algorithm. Experimental results are discussed in Section V. Conclusion are presented in section VI At last References are given.

II. RELATED WORK

In the last few years, so many papers have been published in the field of cryptanalysis. R.Spillman etc. showed that Knapsack cipher\cite{4} and substitution ciphers\cite{5} could be attacked using genetic algorithm. In the recent years Garg\cite{1,2} presented the use of memetic algorithm and genetic algorithm to break a simplified data encryption standard algorithm. Nalini\cite{3} used efficient heuristics to attack S-DES. In 2006 Nalini used GA, Tabu search and Simulated Annealing techniques to break S-DES. Matusi\cite{7} showed the first experimental cryptanalysis of DES using an linear cryptanalysis technique. Clark\cite{6} also presented important analysis on how different optimization techniques can be used in the field of cryptanalysis. Vimalathithan\cite{9} also used GA to attack Simplified-DES. In this paper, a Genetic Algorithm with improved parameters is used to break S-DES.A population of keys is generated and their fitness is calculated by using efficient fitness function. At the end, we will find the key in less time.

III. S-DES

In this section we will provide the overview of S-DES Algorithm. Simplified DES, developed by Professor Edward Schaefer of Santa Clara University is an educational rather than a secure encryption algorithm. The S-DES \cite{8, 10} encryption algorithm takes an 8-bit block of plaintext and a 10-bit key as input and produces an 8-bit block of ciphertext as output. The S-DES decryption algorithm takes an 8-bit block of ciphertext and the same 10-bit key used to produce that ciphertext as input and produces the original 8-bit block of plaintext. The encryption algorithm involves five functions: an initial permutation (IP); a complex function labeled fK, 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 fK again; and finally a

\textsuperscript{a} Author : Lavkush Sharma, FET RBS Agra, E-mail : lavkush07@yahoo.com
\textsuperscript{b} Author : B. K. Pathak, juit, solan, E-mail : bhupendra.pathak@juit.ac.in
\textsuperscript{c} Author : R.G. Sharma, FET RBS Agra, E-mail : cs.ramgopal@gmail.com
permutation function that is the inverse of the initial permutation \( \text{IP}^{-1} \).

The function \( f_K \) takes as input not only the data passing through the encryption algorithm, but also an 8-bit key. S-DES uses a 10-bit key from which two 8-bit subkeys are generated. In this, the key is first subjected to a permutation \( \text{P10} \). Then a shift operation is performed. The output of the shift operation then passes through a permutation function that produces an 8-bit output \( \text{P8} \) for the first subkey \( K_1 \). The output of the shift operation also feeds into another shift and another instance of \( \text{P8} \) to produce the second subkey \( K_2 \).

**Figure 1:** Simplified Data Encryption Algorithm

### 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 \( \text{IP} = [2 6 3 1 4 8 5 7] \). 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, \( \text{IP}^{-1} = [4 1 3 5 7 2 8 6] \) where we have \( \text{IP}^{-1}(\text{IP}(X)) = X \).

### 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,

\[
f_K(L, R) = (L \text{ XOR } f(R, \text{ key}), R)
\]

Where XOR is the exclusive-OR operation and key is a sub-key. Computation of \( f(R, \text{ key}) \) is done as follows.

1. Apply expansion/permutation \( \text{E/P} = [4 1 2 3 2 3 4 1] \) 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 \( \text{P4} = [2 4 3 1] \).

The S-boxes operate as follows:

- 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.

### IV. Genetic Algorithm

The genetic algorithm \([13, 20]\) is a search algorithm based on the natural selection and on "survival of the fittest", the main idea is that in order for a population of individuals to adapt to some environment, it should behave like a natural system. This means that survival and reproduction of an individual is promoted by the elimination of useless traits and by rewarding useful behavior. The genetic algorithm belongs to the family of evolutionary algorithms. An evolutionary algorithm maintains a population of solutions for the problem at hand. The population is then evolved by the iterative application of a set of stochastic operators. The simplest form of genetic algorithm involves three types of operators: selection, crossover and mutation. A selection operator is applied first.

**Selection**: This selection operator selects chromosomes in the population for reproduction. The better the
chromosome, the more times it is likely to be selected to reproduce.

**Crossover**: Crossover selects genes from the parent chromosomes and creates a new offspring. The simplest way to do this is to choose randomly some crossover point and everything before this point is copied from the first parent and then, everything after a crossover point copied from the second parent.

**Mutation**: After a crossover, mutation is performed. This is to prevent falling all solutions in population into a local optimum of solved problem. Mutation changes randomly the new offspring. In binary GA we can switch a few randomly chosen bits from 1 to 0 or from 0 to 1.

The primary goals of this work are to produce a performance comparison between traditional Brute force search algorithm and genetic algorithm with improved parameters based method, and to determine the use of typical GA-based methods in the field of cryptanalysis.

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

1. Input: ciphertext, and the language statistics.
2. Randomly generate an initial pool of solutions (keys).
3. Calculate the fitness value of each of the solutions in the pool using equation (1).
4. Create a new population by repeating following steps 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**

Equation (1) is a general fitness function used to determine the suitability of a assumed key \((k)\). Here, \(A\) denotes the language alphabet (i.e., for English, \([A...Z, _]\), where _ represents the space symbol), \(K\) and \(D\) denote known language statistics and decrypted message statistics, respectively, and the \(u, b,\) and \(t\) denote the unigram, digram and trigram statistics respectively; \(\alpha, \beta,\) and \(\gamma\) 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 digram statistics are used.

\[
C^k = \alpha \sum_{i} |K(iu) - D(iu)| \\
+ \beta \sum_{i,j} |K(ij) - D(ij)| \\
+ \gamma \sum_{i,j,k} |K(ijk) - D(ijk)|
\]  

(1)

V. RESULTS AND DISCUSSION

Our objective in this paper is to compare the results obtained from Brute Force search algorithm with the Genetic Algorithms with improved parameters. The experiments were conducted on Core 2 Duo system. 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 table 1. 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>
<thead>
<tr>
<th>S. No</th>
<th>Amount of Cipher Text</th>
<th>No. of bits matched using GA</th>
<th>No. of bits matched using Brute Force search</th>
<th>Time Taken by GA (M)</th>
<th>Time Taken by Brute Force search (M)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>200</td>
<td>5</td>
<td>5</td>
<td>4.7</td>
<td>24.3</td>
</tr>
<tr>
<td>2.</td>
<td>400</td>
<td>4</td>
<td>3</td>
<td>2.1</td>
<td>24.7</td>
</tr>
<tr>
<td>3.</td>
<td>600</td>
<td>7</td>
<td>6</td>
<td>1.9</td>
<td>23.6</td>
</tr>
<tr>
<td>4.</td>
<td>800</td>
<td>8</td>
<td>7</td>
<td>3.1</td>
<td>24.1</td>
</tr>
<tr>
<td>5.</td>
<td>1000</td>
<td>9</td>
<td>7</td>
<td>2.6</td>
<td>25.1</td>
</tr>
<tr>
<td>6.</td>
<td>1200</td>
<td>9</td>
<td>8</td>
<td>2.1</td>
<td>25.5</td>
</tr>
</tbody>
</table>

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

VI. CONCLUSION

In this paper, we have used a Genetic algorithm with Ring crossover and other operators for the cryptanalysis of Simplified Data Encryption Standard. We found that Genetic Algorithm is far better than Brute Force search algorithm for cryptanalysis of S-DES. Although S-DES is a simple encryption algorithm, GA with Ring Crossover method can be adopted to handle other complex block ciphers like DES and AES.

REFERENCES

This page is intentionally left blank