DES Security Enhancement using Genetic Algorithm

Ayman E. Mohammed[1], Faisal M. Abdalla[2]

[1]Computer Science and Information Technology (CSIT), Sudan University of Science and Technology (SUST),
[2]College of computer science, Karary University
aymenrad@hotmail.com

Received: 12/12/2014
Accepted: 23/02/2015

ABSTRACT - In this paper is proposed method for creating Data Encryption Standard (DES) sub-keys. The proposal simplifies the creation and expansion process of the encryption key of the Data Encryption Standard (DES) algorithm, which is considered one of the most important elements in the process of encryption. The sub-keys generation methods is implemented by using a genetic algorithm. The sub-keys generated using this method, based on genetic algorithm; they give a totally different group of pseudorandom sub-keys each time program is executed.Furthermore, comparison analyses between the proposed method sub-keys generation process and the standard technique used in Data Encryption Standard (DES) it give optimum results.The proposed method is also evaluated and subjected to many randomness tests in order to measure it's strength after encryption using National Institute of Standards and Technology-Test Suite is a statistical (NIST-STS) for randomness tests. The result shows that the proposed method gives good result and can be used it in many ciphers for sub-keys generation.

Keyword: *Cryptography, Key scheduling algorithm, Sub-key Generation, Block Ciphering Algorithm.*

المستخلص *– في هذه الورقة أُقترح أسلوب لإنشاء المفاتيح الفرعية لخوارزمية التشفير القياسي. الاقتراح ببسط عملية انشاء وتوسيع مفاتيح التشفير لخوارزمية التشفير القياسي التي تعتبر واحدة من اهم العناصر في عملية التشفير. تم تنفيذ أسلوب توليد المفاتيح الفرعية باستخدام الخوارزمية الجينية. المفاتيح الفرعية المولدة باستخدام هذا الأسلوب تعتمد على الخوارزمية الجينية التي تعطي مجموعة مختلفة تماما من المفاتيح الفرعية شبة العشوائية في كل مرة يتم فيها تنفيذ البرنامج. وعلاوة على ذلك تم تحليل مقارنة اسلوب توليد المفاتيح المقترح مع التقنية القياسية المستخدمة في خوارزمية التشفير القياسي التي أعطت نتائج أفضل. الأسلوب المقترح أيضا تم تقييمه بتعريضه لمجموعة من لاختبارات من اجل اختبار قوته بعد عملية التشفير باستخدام برنامج اختبار الإحصائية للمعهد الوطني للمقاييس والتكنولوجيا. النتائج تظهر ان الأسلوب المقترح يعطي نتائج جيدة ويمكن استخدامه هذا الاسلوب في العديد من خوارزميات التشفير لتوليد المفاتيح الفرعية.*

INTRODUCTION

Data Encryption Standard (DES) is block cipher, which process block of plaintext as a whole, and used to produce a cipher-text in the same length, DES is Symmetric encryption type. Use single key for encryption and decryption and use 16 sub-keys in 16 round.In Data Encryption Standard (DES) a primary master key used to create a number of sub-keys according to specified key scheduling algorithm; the design of a good key schedule is a crucial aspect of cipher design; it has a few specific keys termed "weak keys" and "semi-weak keys". These keys cause the encryption mode of Data Encryption Standard (DES) to act identically to the decryption. [1]. the National Institute of Standards and Technology-Test Suite is a statistical (NIST-STS) tool was used for evaluate algorithm [2].

STATEMENTOFTHEPROBLEM

According to the method used in Data Encryption Standard (DES) to generate a sub-key for each round of the algorithm, certain initial keys can be produced. [3].the initial key value is split into two halves, and

each half is shifted independently. If all the bits in each half are either 0 or 1, then the key used for any cycle of the algorithm is the same for all the cycles of the algorithm. This can occur if the key is entirely 1s, entirely 0s, or if one half of the key is entirely 1s and the other half is entirely 0s.Also, two of the weak keys have other properties that make them lesssecure; additionally, some pairs of keys encrypt plaintext to the identical cipher-text. In other words, one key in the pair can decrypt messages encrypted with the other key in the pair. This is due to the way in which Data Encryption Standard (DES) generates sub-keys; instead of generating 16 different sub-keys, these keys generate only two different sub-keys. Each of these sub-keys is used eight times in the algorithm. These keys called semi weak keys [4].

Related Works

Many studies have been conducted to improve Block Ciphers algorithms. Krishna C Kommanapalli in [5] a study presents way of Subkey generation for block symmetric encryption, which operates on numbers rather than bits.

Soukaena H. Hashem, Mohammad A. AL Hamami, Alaa H. AL-Hamami in [6] introduce two fusion methods proposed togenerate the block cipher keys. Artificial Neural Network (ANN) and genetic Algorithm (GA).

Jamal N. BaniSalameh in [7] in his study he describe technique to generate pseudorandom sub-keys to use in cryptographic algorithm.

SlimanArrag, Abdullatif Hamdoun, AbderrahimTragha and Salah eddineKhamlich in [8] presents algorithms thatsimplify the creation and expansion process of the encryption key of the AES algorithm.

THE PROPOSED METHOD

Genetic algorithms Philosophy is based on; generating a large number of possible solutions to a particular problem then, evaluate each of these solutions. The best solutions have greater opportunities to generate other solutions. In the proposed method (shown in Figure 1) a genetic algorithm is used to generate, sub-keys depending on the primary key in order to enhancing the Data Encryption Standard (DES) algorithm depending on key.

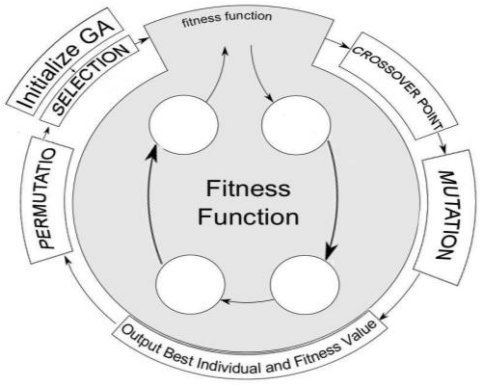


Figure 1: proposed algorithm process

I. Permutation:

Mathematically, a permutation is a rule that tells us how to rearrange a set of elements. Permutation operation is performed before each operation of generating new sub-key as we solve the issue programmatically. The researcher must encode each chromosome to make it easier in dealing with a computer according to the issue raised. Generally, there are many methods to encoding but we used Binary Encoding so that each chromosome is a set of sequence (1s or 0s). The bits are inserted into the matrix of two dimensions (8*8); Columns are moved from the bottom-up and placed in rows in the following order:

The first col. is moved to the first row position, the third col. is moved to the second row position, the fifth col. is moved to the third row position, and the seventh col. is moved to the fourth row position, then the second col is moved to the fifth row position, the fourth col is moved to the sixth row position, the sixth col. is moved to the seventh row position, finally the eighth col. is moved to the eighth row position, the 8 Blocks resulting from this phase represent a new population that will be used in Sub-key Generation, that are discussed in next paragraph.

```
for i = 0 to 7 Step 2
  for j = 7 to 0 Step −1
      NewPoula[ ] = OldPoula[j, i]
Next
                if i = 6 then
```

$$i = -1$$

Algorithm Permutation

II. Selection Operation:

The selection phase is the first phase of the genetic algorithm as a new generation is chosen from older generation (two blocks per time); to place all individuals in a group and choose most suitable which is FITNESS.

III. Fitness Operation:

The fitness operation used as measuring unit in optimization techniques. The fitness operation used to determine the 16 sub-keys as best sub-keys. The following algorithm is explain this operation.

$$x_i = a_j + a_{j+1} + a_{j+2} + a_{j+3}$$
$$if\ a_0 = a_1 = a_2 = a_3\ then$$
$$if\ a_j = 0\ then$$
$$a_j = 1$$
$$else: a_j = 0$$

Algorithm Fitness

IV. Crossover Operation:

havemanyThe Crossover phase is the most important phase in the genetic algorithm, which mimic the biological mating process between neighborhoods. The prevailing beliefs that the mating between individuals hold good attributes will often result in individuals hold good qualities at least. During this phase, eight children are generated to fill the new generation. For each Child, the two adjacent parents could be selected as x_i and x_{i+1}.Then both Parents are crossed together.

- ***Single Point Crossover***

Two rows are selected each row of the matrix is considered in parents so that Crossover grades to produce children's. As shown in Figure 2.

Parent 1	1 0 1 1 0	0 1 0
Parent 2	1 0 1 0 1	1 1 1

⇩

Child 1	1 0 1 1 0	1 1 1
Child 2	1 0 1 0 1	0 1 0

Figure 2: Single Point Crossover

V. Mutation Operation:

Is the last stage of a series of iterative processes, which have a good contribution in reaching the best solution quickly. Changing in the bits of the block can help to step closer to the best solution, (as shown in Figure 3).

Parent	1 **0** 1 1 0 **1** 0 1
Child	1 **1** 1 1 0 **0** 0 1

Figure 3 Mutation Operation

RESULTS AND DISCUSSION

The researcher evaluated his proposed technique through some tests using simulation on (.net). The main goal of the first test is to make sure that the generator is able to generate pseudorandom different sub-keys. In this experiment, the researcher assumed that the master key has a size of 64-bit, the size of each sub-key is 8-bit and the encryption algorithm requires 16 sub-keys for each round. First, the result for this experiment is shown in Figure 4. As we see in this Figure, the sub-key generator is able to give random different sub-keys.
key value =11111111.

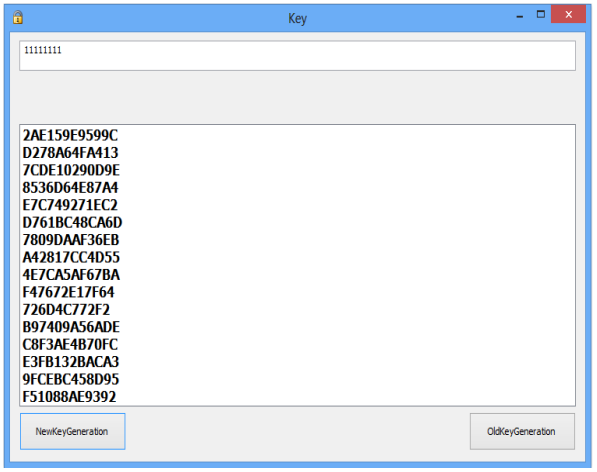
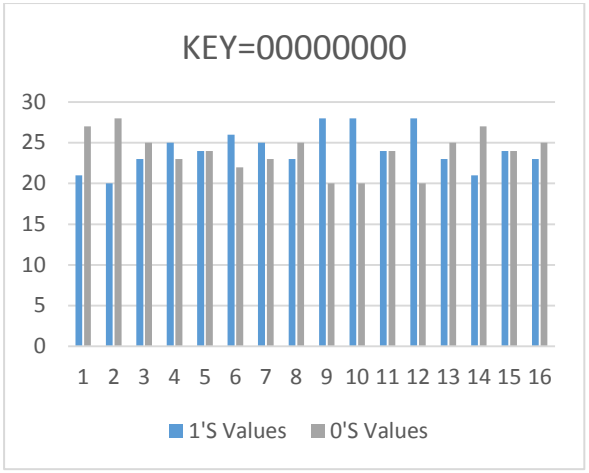


Figure 4: Proposed method 16 sub-key

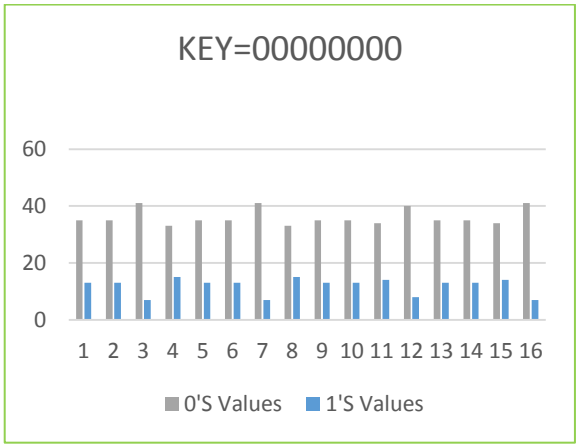
Randomness of the proposed technique compared to the old one used in DES:

In the following set of experiment, the researchers apply the proposed key schedule on DES and evaluate its randomness under different metrics. Here, the researcher present the results of simulations of the proposed technique compared with the standard technique used in DES sub-keys. To evaluate the randomness. In order to have a clearer view of the results, the purpose of this comparison is to determine whether the number of ones and zeroes in a key are an approximately the same as

would be expected for truly random keys. As shown in (fig .5 (a)), the proposed method is more randomness.



(a)



(b)

Figure 5: results for (a) proposed method Randomness (b) standard DES method Randomness

As shown in Figure (5) above columns that reflect the zeroes (gray color) and one's (blue color). Figure (5(a)) convergent that means a good degree of randomness, while Figure (5 (b)) far from certain.

CONCLUSIONS

The proposed method is used to generate sub-keys to use in encryption process, then evaluated and subjected to many randomness tests in order to measures its strength. The following points conclude from the analysis of the experimental results:

- The proposed method is able to give different 16 sub-keys
- The NIST Test Suite is a statistical five tests to are given good results.
- The proposed Method can be use with other encryption algorithms.

REFERENCES

[1] Donald W. Davies,"Some Regular Properties of the 'Data Encryption Standard' Algorithm",springscience+bushiness media new York, Vol. 89, No. 96,1983.

[2] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, San VO, "A Statistical Test Suite For Random And Pseudorandom Number Generators For Cryptographic Applications", NIST Special Publication 800-22, with revisions dated May 15, 2001.

[3] M E Hellman, R Merkle, R Schroeppel, L Washington, W Diffie, S Pohlig, P Schweitzer,"Results of an Initial Attempt to Cryptanalyze the NBS Data Encryption", Technical Report SEL, Vol. 42, No. 76, 1976.

[4] Bruce Schneir,AppliedCryptography.Peachpit Press,1996.

[5] Krishna C Kommanapalli, "Sophisticated Subkey Generation For Symmetric Encryption",GESJ: Computer Science and Telecommunications, Vol. 70, No. 75, 2010.

[6] Soukaena H. Hashem, Mohammad A. AL-Hamami and Alaa H. AL-Hamami, "Developing a Block-Cipher-Key Generator Using Philosophy of Data Fusion Technique", Journal of Emerging Trends in Computing and Information Sciences, vol. 2 No.5, MAY 2011.

[7] Jamal N. BaniSalameh," A New Technique for Sub-Key Generation in Block Ciphers", World Applied Sciences Journal, vol. 1630, No. 1639, November 2012.

[8] SlimanArrag, Abdellatif Hamdoun, AbderrahimTragha and Salah eddine Khamlich" Replace AES Key Expansion AlgorithmBy Modified Genetic Algorithm", Applied Mathematical Sciences, Vol. 7, no. 144, 7161 - 7171, July 2013.