© 2015 IJSRSET | Volume 1 | Issue 3 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Literature Survey on the Usage of Genetic Algorithms In Recent cryptography Researches

Alhussain Amanie Hasn
Information Technology Department, Peoples' Friendship University of Russia, Moscow, Russia

ABSTRACT

This paper will take a brief look at the usage of genetic algorithms in cryptography. Since there is no standard classification, this paper classified the usage into three categories according to its application and usage, they are: The usage of genetic algorithm in key generation, in creating new encryption process, in improving the standard encryption algorithm. And in each approach, its advantages and disadvantages were discussed.

Keywords: genetic algorithm, key generations, encryption, decryption, cryptography, pseudorandom number generators.

I. INTRODUCTION

The need of usage genetic algorithm in cryptography or its benefit over the traditional methods is that: traditional symmetric and asymmetric methods are not suitable when the needed level of security is high. Hash function based systems are although better than traditional methods but are still inadequate in many cases due to their algorithmic complexity as they need the invertible functions to generate hashes which are time consuming and complex. Digital signature is the new concept in field of cryptography but is much complex in implementation and increase server overhead, while a genetic algorithm for cryptography has been proposed to find an optimized solution for a problem. The concept of genetic algorithm has been incorporated within cryptography algorithm to get an optimized solution and within minimum possible time.

There are no standard classifications of using genetic algorithm in cryptography, because it is new approach in this field. It could be applied in many ways either to generate keys or to improve the standard encryption algorithm to increase its level of security or to generate new symmetric /asymmetric algorithm. So the classification in this paper is supposed according to the researches and studies that are done in this approach.

The usage of genetic algorithm in cryptography could be classified into three categories according to the goals that services and applied (this classification is not standard ,it is supposed by authors): the first one using it to generate keys (private/public)[8,5], the second one using it to create new encryption process[3,6], the third one improvement the standard encryption algorithm[1,4,7,2].

II. LITERATURE REVIEW

In this section, some of recent studies and techniques of the usage of genetic algorithm in cryptography will be covered. This research divides the methods into three classifications:

The first classification: The usage of genetic algorithm in key generation

Swati Mishra, Siddharth Bali, Public Key Cryptography Using Genetic Algorithm

Swati Mishra, Siddharth Bali [8] have presented a system which was application of genetic algorithm in the field of key generation. The genetic algorithm in this system correlates nature to a great extent and produce population of keys such that keys with higher fitness value are replicated often.

The advantages of the system are:

1. Applying the fitness function on the generated keys, Pearson's Coefficient of auto-correction was used to calculate the fitness of keys.
2. The key samples satisfy the tests including gap test, and frequency test.
3. The private key generated cannot be derived from public key.
4. The final keys are purely random and non-repeating which increased the keys strength and security.

The disadvantages of the system are:

1. How to generate the initial population is not clear and Ambiguous, and on which bases used.
2. The length of the keys is constant: 192 bit.
3. The time for applying the three fitness values (Shannon Entropy, chi square and coefficient of auto-correlation) to meet the threshold take too much time.
4. The tests applied on the bit level for the population of 192 key lengths, which consume a lot of the time.
5. There are no descriptions or examples on how each pair of the key would be implemented in the asymmetric encryption algorithm

Poornima G.Naik ,Girish R. Naik, Asymmetric key Encryption using Genetic Algorithm

The method proposed by Poornima G.Naik ,Girish R. Naik [5], describes an attempt to exploit the randomness involved in crossover and mutation processes for generating an asymmetric key pair for encryption and decryption of message.

The advantages of system are:

1. The algorithm is further strengthened by making it difficult to break by permuting the asymmetric key by a predefined permutation factor agreed upon by both the sender and the intended receiver.
2. The randomness in the generation of nine components of key give the strength to the generated key, and hence the strength to the algorithm.

The disadvantages of the system are:

1. The key length is constants and too small, here the length of key =36 bit.
2. The algorithm process one block of 32 byte at a time, which consumes time.
3. For each 32 byte the process of generating (private/public)keys would be repeated;
4. Where to store the generated pairs of keys which are created during the encryption process is not mentioned.

<u>The second classification: The usage of genetic algorithm to create new encryption process</u>

Faiyaz Ahamad, Saba Khalid, and Mohd.Shahid Hussain, Encrypting Data Using The Features of Memetic Algorithm and Cryptography

The system supposed by Faiyaz Ahamad, Saba Khalid, and Mohd.Shahid Hussain [3], highlights an approach for encrypting data using the concept of genetic algorithms in cryptography along with the randomness properties of Linear Congrential method.

The advantage of system is:

1. In key generation procedure, nine parameters are used which provide strength to the algorithm rendering it difficult for cryptanalysis by intruder.

The disadvantages of the system are:

1. Only one pseudorandom number generator, which is Linear Congrential method, is used; but PRNG is periodic and Shorter than expected periods for some seed states;
2. There are no improvements of the randomness which is generated by pseudorandom number generator.

Sindhuja K, Pramela Devi S, A Symmetric Key Encryption Technique Using Genetic Algorithm

Sindhuja K. and Pramela Devi S. have described a system [6], which is proposes a genetic algorithm based

symmetric key cryptosystem for encryption and decryption. The steps of algorithms could summarize as follow:

1. The plaintext and the user input (key) is converted into text matrix and key matrix respectively.
2. An additive matrix is generated by adding the text matrix and key matrix.
3. A linear substitution function is applied on the additive matrix to produce the intermediate cipher.
4. Then the GA functions (crossover and mutation) are applied on the intermediate cipher to produce the final cipher text.

The advantage of the system is improvement of the traditional substitution algorithm by using genetic algorithm functions (crossover and mutation).

The disadvantages of the system are:

1. The procedure of choosing the cross points is not mentioned;
2. the key here consists of many parts (user input (key), block size, substitution key and cross over points),but how to recognize each one and separate among them not clear;

The third classification: The usage of genetic algorithm to improve the standard encryption algorithm

Aarti Soni, Suyash Agrawal, Using Genetic Algorithm for Symmetric key Generation in Image Encryption

The system mentioned by Aarti Soni, Suyash Agrawal [1], proposes a method based on genetic algorithm which is used to generate a key by the help of pseudo random number generator to be used to improve the key of symmetric key algorithm AES. The random number will be generated on the basis of the current time of the system.

The advantage of the system is improvement of the key used in AES

The disadvantages of the system are:

1. Which pseudorandom number generator is used not cleared.
2. The first step of generating the key depends on the date and time of the system using millisecond function to generate random population, but when this method is applied on the second side, it would not produce the same binary sequence because it is depend on the date and time, so this key should be exchanged in secret channel, it could not be reproduced.
3. The basics of choosing the cross points and mutation points are not mentioned.

Farhat Ullah Khan, Surbhi Bhatia, A Novel Approach To Genetic Algorithm Based Cryptography

The system supposed by Farhat Ullah Khan, Surbhi Bhatia [4], proposes the intention to create a key as strong if not stronger than the vernam cipher.

The advantage of the system is:

The system recognized the ability of genetic algorithm to produce a good quality random sample of keys, which are better than existing pseudorandom number generator.

The system has the following disadvantages:

1. The chosen pseudorandom number generator is not mentioned;
2. The method of the objective function is ambiguous.
3. The key length is constants and too small, here the length of key =36 bit.

Sonia Goyat, Cryptography Using Genetic Algorithms (GAs)

The method mentioned by Sonia Goyat [7], highlights a method to create one time pad key by the help of genetic algorithm to be used in vernam cipher.
The advantage of the system is:
The algorithm generates random keys of Vernam Cipher, which are stronger and better than existing pseudorandom number generator.

The system has the following disadvantages:

1. The chosen pseudorandom number generator is not mentioned;
2. The method of generating cross points and mutation points is ambiguous.

Dilbag Singh, Pooja Rani, Rajesh Kumar, To Design a Genetic Algorithm for Cryptography to Enhance the Security

The system created by Dilbag Singh, Pooja Rani, Rajesh Kumar [2], highlights an algorithm which used the concept of genetic algorithm with pseudorandom number generator and AES. The idea in the proposed algorithm is that the password would generate a key which would be used to generate a pseudorandom binary sequence by the help of random number generator. The role of PRNG is to define crossover point and to be used in the encryption process.

The advantage of the system is improvement of the standard AES by using genetic algorithm and the randomness property of pseudorandom number generator.

The disadvantages of the system are:

1. Which PRNG that is used in the encryption algorithm not mentioned.
2. The algorithm process block size =16byte at a time, that is consume a lot of time.

In the encryption process there is a use of and (&) operator in a place it should not be used, because it is not reversal operator so the plain text could not be retrieved from the cipher text because of that usage of and operator.

III. CONCLUSION

Some of recent studies that introduce the usage of genetic algorithm in cryptography are listed and described in brief in this research. This paper classified the usage into three categories according to its application and usage, they are:

1. The usage of genetic algorithm in key generation
2. The usage of genetic algorithm to create new encryption process
3. The usage of genetic algorithm to improve the standard encryption algorithm

In each method in the classification, its advantages and disadvantages were discussed.

IV. REFERENCES

[1] Aarti Soni, Suyash Agrawal, Using Genetic Algorithm for Symmetric key Generation in Image Encryption, *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), ISSN: 2278 – 1323, Volume 1, Issue 10, December 2012,137-140.*

[2] Dilbag Singh, Pooja Rani, Rajesh Kumar, To Design a Genetic Algorithm for Cryptography to Enhance the Security, international journal of innovations in engineering and technology(IJIET) ,ISSN:2319-1058, Volume 2, Issue 2 ,2013,pp. 380-385.

[3] Faiyaz Ahamad, Saba Khalid, and Mohd.Shahid Hussain, Encrypting Data Using The Features of Memetic Algorithm and Cryptography, International Journal of Engineering Research and Applications (IJERA),ISSN: 2248-9622,Vol. 2, Issue 3, May-Jun 2012, pp.3049-3051.

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

[5] Poornima G.Naik ,Girish R. Naik, Asymmetric key Encryption using Genetic Algorithm ,international journal of latest trends in engineering and technology (IJLTET),ISSN:2278-621X, volume-3, Issue-3, January 2014, pp.118-128.

[6] Sindhuja K , Pramela Devi S, A Symmetric Key Encryption Technique Using Genetic Algorithm, International Journal of Computer Science and Information Technologies (IJCSIT), ISSN: 0975-9646,Vol. 5 , Issue 1, 2014, pp.414-416.

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

[8] Swati Mishra, Siddharth Bali, Public Key Cryptography Using Genetic Algorithm, International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, volume-2, Issue-2, May 2013, pp.150-154.