International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 9, 2017 ISSN: 2348-6600
Reference ID: IJCS-196 PAGE NO: 1199-1202
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

AN INNOVATIVE APPROACH TO GENETIC ALGORITHM BASED CRYPTOGRAPHY

Dr. G.RAJKUMAR[1] Dr. K.PARIMALA[2] A.RUBA[3]
[1 2 3] Assistant Professor – Department of Computer Applications,
N.M.S.S.Vellaichamy Nadar College, Nagamalai, Madurai.

ABSTRACT- In today's computer world security, integrity, confidentiality of the organization's data is the most significant problem. Cryptography is an important technique for securing information. Many problems can be solved using genetic algorithms through modeling a simplified version of genetic processes. The Genetic Algorithms (GAs) are exploration algorithms based on the theory of natural selection with an inventive finesse of nature. The central idea of research on GAs has been robustness. The technique has been implemented and analyzed. Cryptography proposed efficient solution to save from harm sensitive information in a large number of applications including personal data security, internet security, diplomatic and military communications security, etc. through the processes of encryption/decryption.

Keywords: Genetic Algorithm, Mutation, Encryption, Decryption, Cryptography.

INTRODUCTION

In today's age of information technology secure transmission of information is a big challenge. Traditional symmetric and asymmetric methods are not suitable when the needed level of security is high. There are two types of cryptographic schemes: symmetric cryptography and asymmetric cryptography. The symmetric scheme applies the same key for encryption and decryption. Two keys are used in asymmetrical cryptography, one for encryption, known as the public key, and the other for decryption, known as the private key. GA is one such evolutionary algorithm. GA has emerged as a practical, robust optimization technique and search method. A GA is a search algorithm that is inspired by the way nature evolves species using natural selection of the fittest individuals. Genetic Algorithms (GAs) being optimization algorithms unite 'survival of the fittest' and a beginner's version of Genetic course. The application of Genetic Algorithm and cryptography has been discussed in several works. In most of the cases GA approach has been apply to decrypt simple ciphers. The basic entity of GA is chromosome. Every chromosome symbolizes a solution to the problem and is composed of a string of cells of finite length. The binary digit {0, 1} is often used to represent these cells but integers can be used depending on the application. The set of operators usually consists of mutation, crossover and selection.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 9, 2017 ISSN: 2348-6600
Reference ID: IJCS-196 PAGE NO: 1199-1202
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

CRYPTOGRAPHY

In most of the cases GA approach has been applied to decrypt simple ciphers. Many works have already been done in the field of cryptography using genetic algorithm.

Types of Cryptography:

Symmetric key cryptography:

In this type, the sender and the receiver use the same key for encryption and decryption and hence the key is mutual between them. Example: DES (Data Encryption Standard) and AES (Advanced Encryption Standard).

Asymmetric key cryptography:

The technique is also known as public key cryptography. In this type, the sender and the receiver use different keys for encryption and decryption and hence the key is not shared between them.

GENETIC ALGORITHM

Genetic algorithm is a randomized search and optimization technique guided by the principle of natural selection systems. Three basic operators used in Genetic algorithms contain: selection, crossover and mutation. Key generation in cryptography has been dealt with in many papers but the use of GA in the process has not yet been explored. It is the most important part of encoding the data. A chromosome is a string of binary digits and each digit that makes up a chromosome is called a gene. Here PRNG is used to ensure confidentiality in networks, which is combined and implemented with the help of genetic functions such as crossover and mutation that provides additional data security.

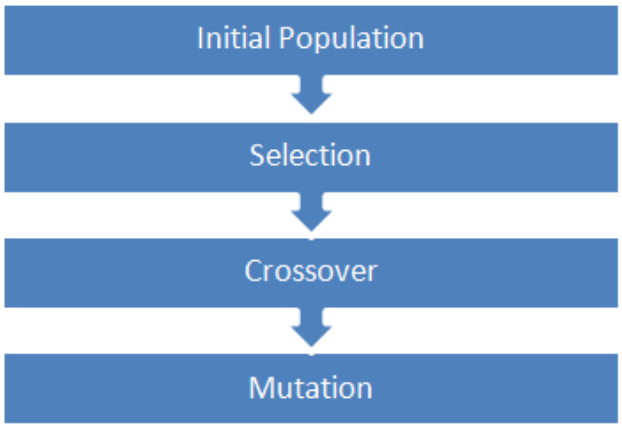

Figure 1: Flow chart – Genetic Algorithm

BASIC TERMINOLOGY

Population – It is a separation of all the possible (encoded) solutions to the given problem. The population for a GA is analogous to the population for human beings except that instead of human beings.

Chromosomes – A chromosome is one such solution to the given problem.

Gene – A gene is one element position of a chromosome.

Allele – It is the value a gene takes for a particular chromosome.

Genotype – Genotype is the population in the computation space. In the computation space, the solutions are represented in a way which can be easily understood and manipulated using a computing system.

Phenotype – Phenotype is the population in the actual real world solution space in which solutions are represented in a way they are represented in real world situations.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 9, 2017 ISSN: 2348-6600
Reference ID: IJCS-196 PAGE NO: 1199-1202
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

Fitness Function – A fitness function simply defined is a function which takes the solution as input and produces the suitability of the solution as the output. In some cases, the fitness function and the objective function may be the same, while in others it might be different based on the problem.

Genetic Operators – These alter the genetic composition of the offspring. These include crossover, mutation, selection, etc.

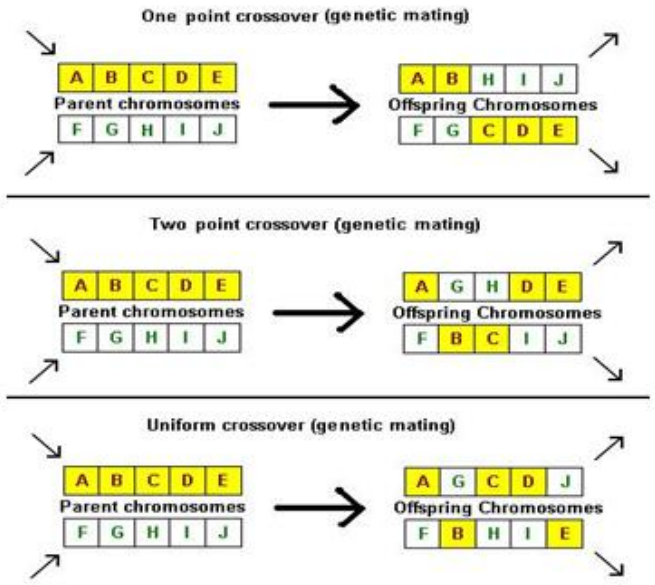

Figure 2: Types of Crossover

GENETIC ALGORITHM AS RANDOM NUMBER GENERATOR

Genetic algorithm in cryptography can be used for producing the key. Key generation in cryptography is the most significant part of encoding data. If the key is randomly preferred and non-repeating used then this cipher is called one time pad. The one time pad is theoretically unbreakable. One of the most used one time pad is in Vernam cipher. Vernam cipher is a stream cipher where plaintext is transformed into cipher text. One of the feasible methods of generating the key is described in the work. It consists of generating binary population, Selection, Crossover, Mutation and Fitness function.

Encryption Process:

Figure 3: Encryption Process

- The encryption makes use of genetic algorithm and pseudo random number generation.
- The encryption process comprises a plain text and writes the ASCII equivalent of the plain text.
- Choose the block size, the last block if it is not equal to n.
- Convert ASCII to binary equivalent.
- Generate the PRNG.
- Generate pseudorandom sequence of numbers
- Apply crossover and mutation on the binary stream.
- Convert the bytes to hexadecimal equivalent which is the final cipher.
- The cipher text and the key will be sent to the receiver for decryption.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 9, 2017 ISSN: 2348-6600
Reference ID: IJCS-196 PAGE NO: 1199-1202
Sri Vasavi College, Erode Self-Finance Wing 3rd February 2017
National Conference on Computer and Communication NCCC'17
http://www.srivasavi.ac.in/ nccc2017@gmail.com

Figure 4: Decryption Process

Decryption process: The steps for decryption are just reversal of the encryption process.

CONCLUSION

The algorithm proposed in this paper is simple and easy to execute in cryptographic system. The genetic algorithm can be very helpful for solution of various groups of problems. One of them is application in the cryptography. It is usually used in cryptanalysis, but it can be used for the random number generators or for training and designing artificial neural networks. The random number generator is a very significant part of any cryptographic system. The method proposed in this paper is simple and easy to execute in cryptographic system. Crossover and mutation operators of genetic algorithm are used for encryption which provides high security to the transmitted data. The Genetic Algorithm can keep the strength of the key to be long and still on working to make the complete algorithm better enough.

REFERENCES

[1] Amritha Thekkumbadan Veetil, "An Encryption Technique using Genetic Operators". International Journal of Scientific and Technology Research, Volume 4, Issue 07, July 2015.

[2] Ankita Agarwal, "Secret Key Encryption Algorithm using Genetic Algorithm". International Journal of Advanced Research in Computer Science and Software Engineering, Vol: 2, Issue 4, April 2012.

[3] Farhat Ullah Khan, Surbhi Bhatia, "A Novel Approach to Genetic Algorithm based Cryptography". International Journal of Research in Computer Science, 2 (3): pp. 7-10, April 2012. doi:10.7815/ijorcs.23.2012.022.

[4] Martin Javurek and Marcel Harakal, "Cryptography and Genetic Algorithms", Science and Military 1/2016.

[5] Pushba B R, "Data Encryption Technique using Genetic Algorithm and Random number generator". International Journal of Innovative Research in Engineering and Science, Volume 4, Issue 4, April 2015.

[6] Rajat Jhingran, Vikas Thada, Shivali Dhaka, "A Study on Cryptography using Genetic Algorithm". International Journal of Computer Applications, Volume 118 – No. 20, May 2015.

[7] Sindhuja K and Pramela Devi S, "A Symmetric Key encryption technique using Genetic Algorithm". (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1), 2014, 414-416.