A Study on Genetic Algorithms for Cryptography

B. Reddaiah
Department of Computer Applications
Yogi Vemana University
Kadapa, A.P, India

ABSTRACT
In this electronic era institutions and enterprises thinks that there data is very crucial in all their activities. As this based on electronic transmission of data from one place to other, secure mode of transmission is needed. This is to counter security attacks that are evident in transmission. Different security services and mechanisms are needed to provide security and integrity to the resource owners. Security mechanisms that provide security are to be constantly updated to counter attacks. In the process of providing new services and mechanisms, special functions are to be included to strengthen the processing. In this paper different genetic algorithms are discussed that are gaining importance in the field of cryptography that in providing security to data.

Keywords
Security mechanisms, Security attack, selection, Crossover, Mutation, Fitness function.

1. INTRODUCTION
E-commerce is filed that is growing with rapid speed in the field of computers and electronics. Every individual today is using the service provided by e-commerce than a traditional one. Because of this companies are looking for security measures that provide security for their data as well as customer's data. As the electronic business field is growing every day with greater pace and a large number of secured applications are essential. From the olden days, a systematic approach to give provides confidentiality and integrity is Cryptography. This art have a extensive and attractive narration [5] and has developed into a crucial element of modem systems [4]. In the past, Julius Caesar also designed secured methods to transmit secret information to important people in military [7].

Security provided by cryptosystems is entirely based on mechanisms build with a variety of functions and operations. For example use of mathematical paring, functions is one of the strong ways of providing security [1]. By using cryptography enciphering and deciphering of text was started around 1900 BC, when Egyptians initially applied usual procedures to correspond [3]. The underlying principle is to hide the information from unauthorized people. To make this possible the original text is transformed into the meaningless text to keep the data safety [2]. In order to change original text into the meaningless text, strong mechanisms are needed. Information security is based on enciphering and deciphering methods and the type of secret key used to process the data [6]. Along with key, a strong function in both algorithms is required to derive the meaningless text that cannot be easily understood. In this paper, different types of genetic functions for cryptography with their advantages and disadvantages are discussed.

2. PRINCIPLES OF CRYPTOGRAPHY
Cryptography is essential to use in situations that demand privacy to protect data, trade secrets, for example, business transactions, e-commerce, and extramarital affairs. Every organization develops its own mechanisms to provide security for their valuable information. These organizations use secure mechanisms through which sender and receiver can communicate with each other. The science of cryptography is divided into symmetric cryptography and asymmetric cryptography. Symmetric cryptosystems have five ingredients such as plain text, encryption algorithm, key, and decryption algorithm. Whereas asymmetric cryptosystems have six ingredients in which key is different from symmetric. Here the key is in two forms as a public key and private key. The strength of the enciphering and deciphering methods is based key that is used in providing security.

In both symmetric and asymmetric cryptosystems encryption is the process of changing the original form of text to unreadable form and decryption process gets the original form of data from the meaningless text. These two algorithms stand as the backbone of the entire process in cryptography along with the key. The processing of text to get others form of text is defined in these algorithms. So it is up to the organizations to develop strong algorithms along with strong keys that process the text. The outcome of these systems is to achieve confusion and diffusion. The goal is to achieve more diffusion in the final text so that it makes unauthorized people feel difficult in getting the original information. The principle is that a small change in the text should produce a great change in the outcome that may lead to confusion, so that the intended receiver of the message can receive the message securely.

Security is made possible in cryptography by using mathematical functions and operations. Mathematics derivations play an important role in developing the security mechanisms to protect data from security attacks that are from unauthorized people. Every function in cryptosystems is based on these mathematical functions and operations. Operations like addition, subtraction, OR, XOR, etc., are used in building functions. By using these in different forms organizations build their functions to provide security. Modern cryptographic systems stands on mathematical theory and number theory besides this cryptographic systems are based on computational hardness, proposition that makes algorithms stronger and harder to break unauthorized person. To look at these it is possible to break them theoretically but it is infeasible to break them practically. Therefore these systems are computationally secure. Other than this cryptography supports various functions like genetic algorithms. In this paper different genetic functions are discussed which can be used as a part of encryption and decryption algorithms.

3. INTRODUCTION TO GENETIC ALGORITHMS

The foundation for Genetic algorithms is its unsystematic nature of search operation and optimized techniques that are directed through the standards of the natural selection system. The principles are based on such mechanisms in usual selections and natural genetics. It is like a natural system that adapts some kind of environment for a population of the individual. With the removal of worthless or unsafe behaviour and by satisfying with some helpful actions, the survival and reproduction of individuals are promoted. Basically, genetic algorithms start from a arbitrarily produced set of individuals. As the initial population is formed genetic algorithm directly enter into the loop. By using some stochastic operators to the earlier population, a new population might be produced at the iteration and it is named as generation. The process of genetic algorithms is shown in Figure 3.1

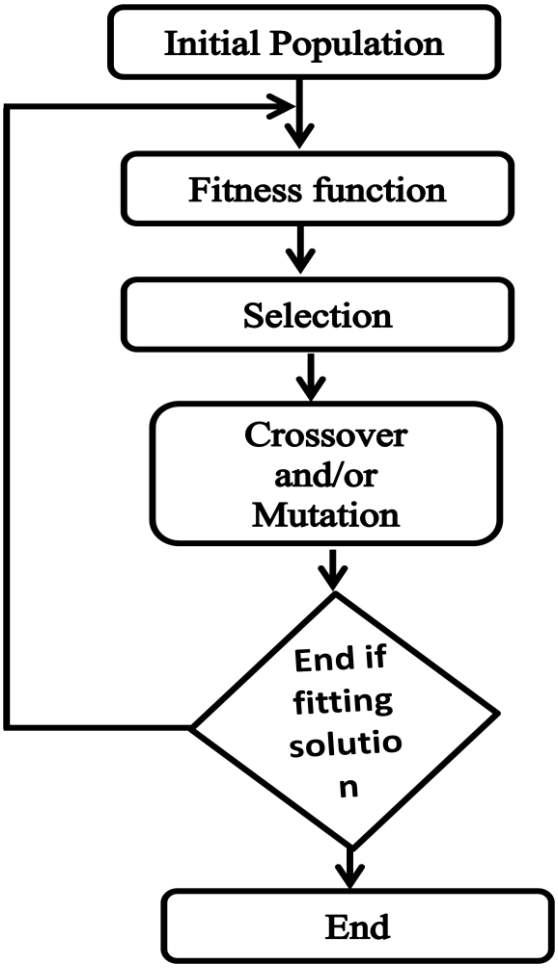

Fig. 3.1 Flow chart of Genetic Algorithms

4. GENETIC ALGORITHMS

The genetic algorithms are used to initialize a population and to achieve a suitable outcome that is of suitable size and form a suitably selected fitness function. It uses four operators to transform a population into the new population with a good fitness function. Different types of genetic algorithms generally used in cryptography for providing security, they are Selection, Crossover, Mutation and Fitness function.

4.1 Selection Function

Selection is one of the genetic functions, where a single chromosome is picked from a group for reproduced chromosome. It is based on fitness value. It is implemented by choosing the random choices, the chromosome with higher fitness value is considered first.

4.2 Crossover Function

Crossover is also one of the genetic operators, where it generates or reproduces a new child by taking two chromosomes i.e. taking some attributes from first and remaining from the second chromosome. Crossover is divided into three types, they are Single point crossover, two-point crossover, and uniform crossover.

4.2.1 Single point crossover function

The nature of single point crossover is that only one point is selected to reproduce a new child as shown in Figure 4.1 and 4.2.

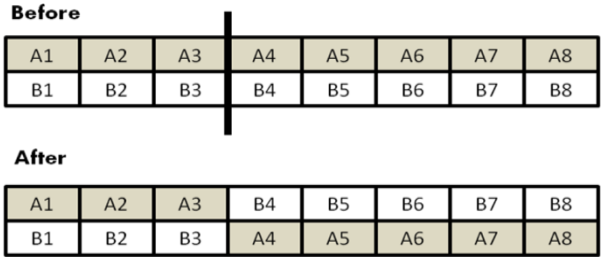

Fig. 4.1 Model of Single point crossover

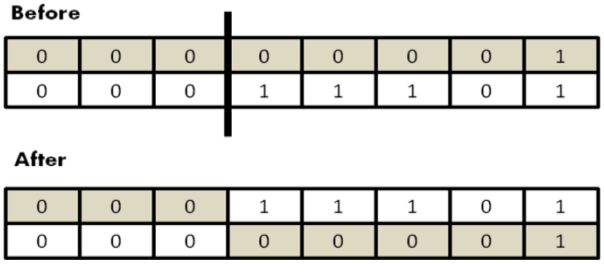

Fig. 4.2 Example for Single point crossover

4.2.2 Two-point crossover function

In these two point crossover functions in two points are taken to reproduce a new child as shown in Figure 4.3 and 4.4

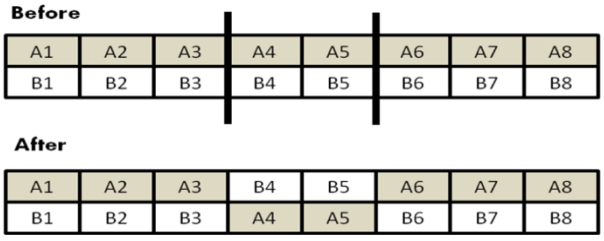

Fig. 4.3 Model of Two-point crossover

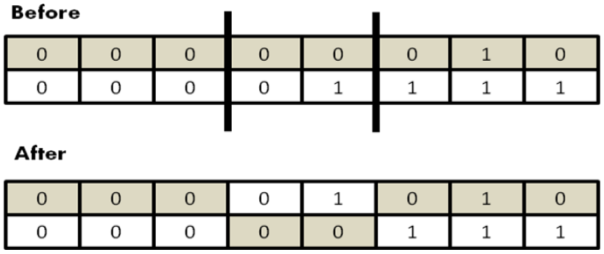

Fig. 4.4 Example of Two-point crossover

4.2.3 Uniform crossover function

In this uniform crossover, bits are taken uniformly for each to reproduce a new child as shown in Figure 4.5 and 4.6

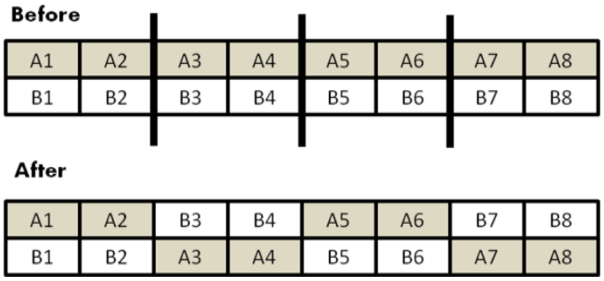

Fig. 4.5 Model of Uniform crossover

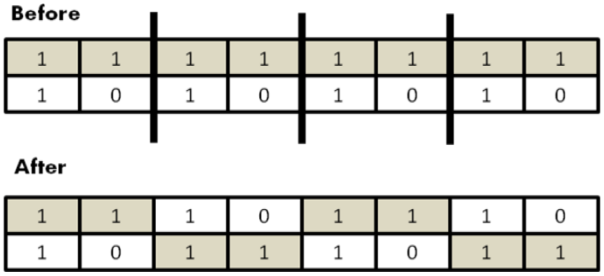

Fig. 4.6 Example of Uniform crossover

4.3 Mutation Function

At least one bit in each chromosome is changed by mutation function. By the exestuation of this function It reflect the consequence of neighboring in natural genetic process. Mutation function exists in two forms namely flipping of bits and boundary mutation.

4.3.1 Flipping of Bits

In function flipping of bits, one or more bits are toggled from 0 to 1 or 1 to 0 as shown in Figure 4.7 and 4.8

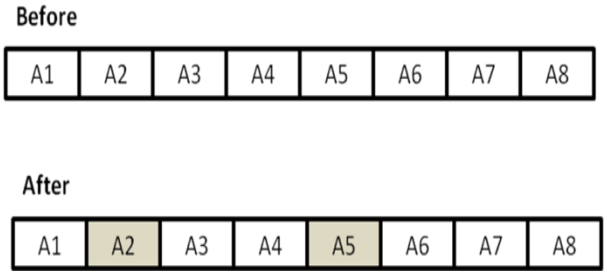

Fig. 4.7 Model of Flipping of bits

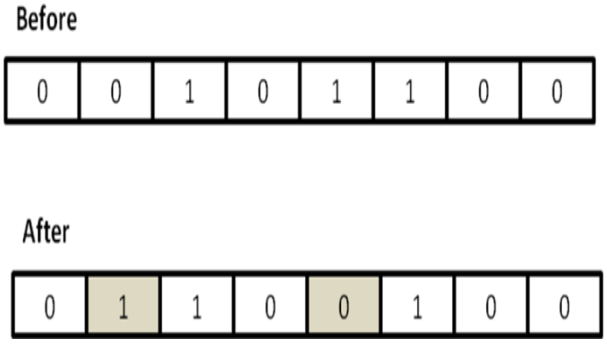

Fig. 4.8 Example for Flipping of bits

4.3.1 Boundary Mutation

In this mutation, arbitrarily higher or inferior block is exchanged in the chromosome as shown in Figure 4.9 and in 4.10.

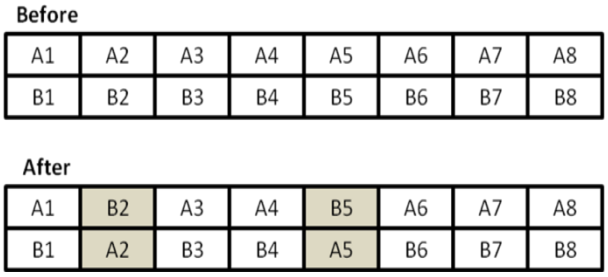

Fig. 4.9 Model of Boundary mutation

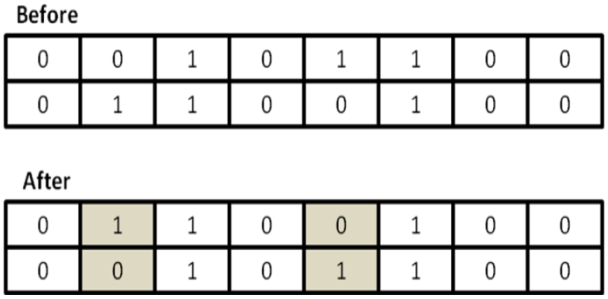

Fig. 4.10 Example of Boundary mutation

4.4 Fitness Function

The other function is fitness function from genetic algorithms that are based on mathematical equations which are mostly used. This is because a good fitness function is useful for exploring the search efficiently, as it is the based on mathematical values. The fitness value of each individual is evaluated on the basis of the symbol which is repeated for more number of times The formula in fitness function is

$$F=n+(€/m)$$

Where, F = Fitness function

n is the total number of symbols used in the key formation

m is the percentage of maximum symbols appeared

€ is the ideal percentage of each symbol

Hence these are the different types of operators that are frequently used in genetic algorithms to get reliable and accurate results

5. CONCLUSION

In developing cryptosystems different functions like pairing functions, various mathematical functions and different types of operators are used to provide security and to increase the security. The recent trend in cryptography is going beyond traditional operators to different functions. This trend is gaining its importance in providing security. This is because even though the size of the key is reduced genetic algorithms produce good security for data. In other cases, key management is becoming a difficult task. A detailed description is given on different genetic functions that are supported by cryptography.

6. REFERENCES

[1] B. Reddaiah. "A Study on Pairing Functions for Cryptography," IJCA (0975-8887), Vol. 149, No. 10, September 2016: pp.4-7.

[2] P. P Charles & P. L. Shari, "Security in Computing: 4th edition", Prentice-Hall, Inc.,2008.

[3] S. Hebert, "A Brief History of Cryptography", an article available at http://cybercrimes.net/aindex.html

[4] A. S. Tanenbaum, "Modern Operating Systems", Prentice Hall, 2003.

[5] D. KHAN, "The Codebreakers", Macmillan Publishing Company, New York, 1967.

[6] Behrouz A. Forouzan, Cryptography, and Network Security, Special Indian Edition, TATA McGraw Hill.

[7] S. William, Cryptography and Network Security: Principles and Practice, 2nd edition, Prentice-Hall, Inc., 1999 pp 23-50.