

ENHANCED SECURITY USING GENETIC ALGORITHM IN CRYPTOGRAPHY

B. SRIPRIYA¹, N. SRINIVASAN²

¹M. Tech Scholar, Department of Computer Science & Engineering, Raghu Engineering college, Dakamarri(V), Visakhapatnam, AP, India.

²Senior Assistant Professor, Department of Computer Science & Engineering, Raghu Engineering college, Dakamarri(V), Visakhapatnam, AP, India.

Abstract - In present age of information technology the transmission of data with security is a big challenge. Both symmetric and asymmetric cryptography systems are not correct for high level security. Latest hash based function are far better than the traditional systems but the complex algorithms functions are very time consuming. In tradition way of system data is first encrypted with the help of key but there are still possibilities of hacking the key and changing the text. So, the key should be so strong and efficient, so a format should be proposed which have the advantage of theory of natural selection. Genetic Algorithm is used to solve many problems by simplifying genetic process and it is considered as optimization algorithm. With this Genetic algorithm we can improve the strength of the key, which can ultimately make the whole algorithm good and efficient. In this proposed method, data encryption is done in number of steps. Firstly, the key is generated by random number generator and by the application of genetic algorithm operations. Secondly, the data should be diffused by using genetic operations and logical operations should be performed between diffused data and the key. Finally, comparative study should be done between proposed method and cryptography algorithm. It has been observed that proposed algorithm is having much better results with strong and efficient key but comparative less efficient than others.

Key Words: Symmetric Key Cryptography, Genetic algorithm, Genetic Key, Encryption, Decryption.

1. INTRODUCTION

Cryptography is completely based on Encryption and Decryption. In the Encryption, the data which is to be sent from sender to receiver is converted into unreadable form which is called as encrypted form. And that data is send from sender to receiver, at the receiver side the data which is in encrypted form is converted into original form, which is called as decryption. Both the encryption process and decryption process requires a key. For the protection of important and valuable data, different models of cryptography algorithms are designed. Mainly there two types of cryptographic algorithms:

1. SYMMETRIC CRYPTOGRAPHY
2. ASYMMETRIC CRYPTOGRAPHY

In symmetric cryptography, same key is used in both encryption and decryption. This process is mostly used in encryption of data due to high performance. In asymmetric

cryptography the key will differ in encryption and in decryption.

2. METHOD – GENERATION OF GENETIC KEY

Genetic algorithm is a kind of algorithms which makes use of the mechanics of natural selection and genetics. It is a part of Evolutionary Algorithms which are used to solve optimization problems with the help of mechanisms like crossover, selection and mutation. The process of solving optimization problems using Genetic Algorithms.

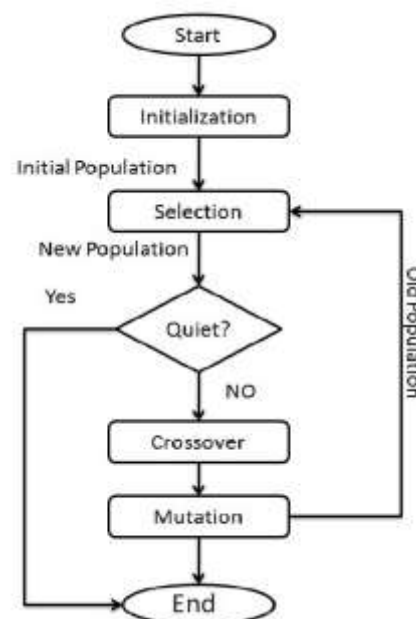


Fig. 1. Fitness Function of Genetic Algorithm

The main idea of Genetic Algorithm is to imitate the randomness of the nature of selection process and behavior. The natural system make population of individuals able to adapt the surrounding. We can say the survival and reproduction of the individuals is supported by exclusion of less fitted individuals.

The population is generated in such a way that the individual with the highest fitness value is most likely to be replicated and unfitted individual is discarded based on threshold set by an iterative application of set of stochastic genetic operators. Genetic Algorithm performs following operations to transform the population to new population based on fitness value.

3.1 Crossover

Crossover is a genetic operation which joins two chromosomes to form new chromosome. The newly generated child chromosome is composed of chromosomes from each parent.

Crossover is classified as single point, two point and uniform crossover. In Single Point only one crossover point is selected to generate new child. In Two Point crossover two crossover points are selected to generate new child. In Uniform crossover bits are selected uniformly from each.

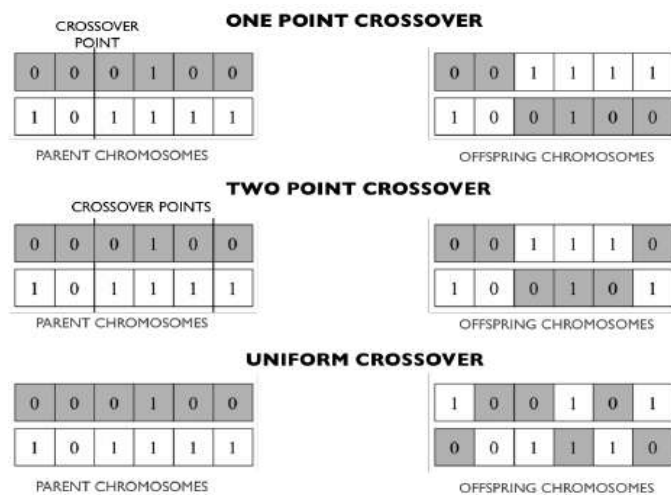


Fig. 2 Types of cross overs

3.2 Mutation

In mutation after crossover at least one bit in each chromosome is changed. This is performed to reflect the effect of around in natural genetic process. There are two major types of Mutation i.e Flipping of Bits and Boundary Mutation. In Flipping of Bits one or more bits are converted into 0 to 1 or 1 to 0. In Boundary Mutation randomly upper or lower block in swapped in chromosome.

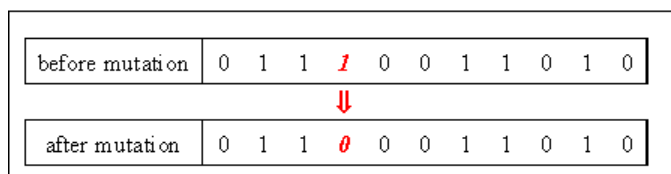


Fig. 3 Mutation

3.3 Selection

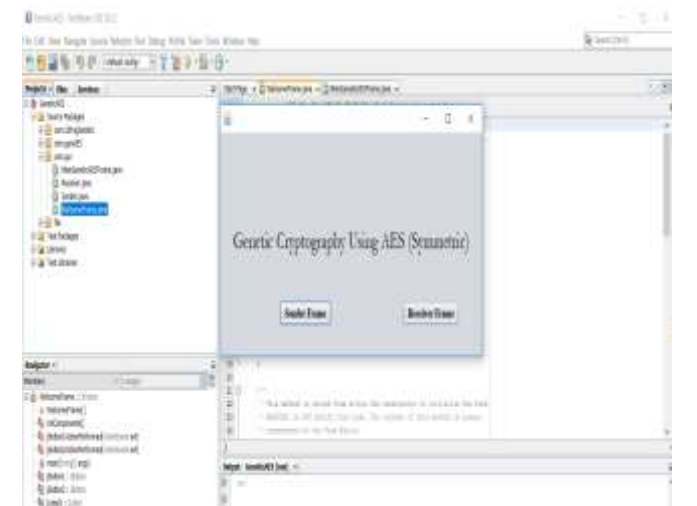
In selection, chromosomes are chosen from the population for generating new population. The selection is based on value of fitness. If the value is high then the selection chances will be more. Selection is classified as Roulette-wheel Selection, Tournament Selection; Truncation Selection.

3.4 Fitness Function

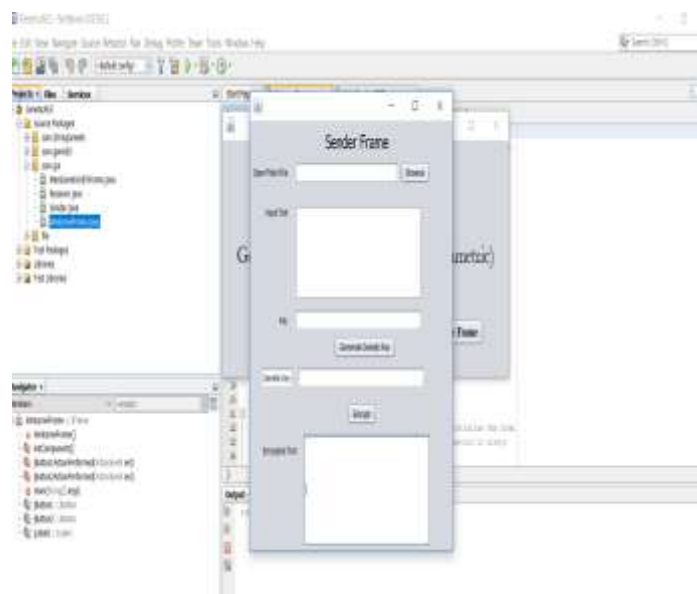
Fitness function is one of the most important function in Genetic algorithm because good fitness is useful for the exploration of search space efficiently and bad fitness functions are for local optimum solution. Fitness Function can be categorized as two types. One is Constant fitness function and another one is Mutable fitness function.

In cryptography, Key Selection is one of the selection problem and when we consider the key is selected, the key with highest fitness and randomness is selected. The applications of Genetic Algorithm are also in heuristic problems, which make the Genetic algorithm for key generation and data encryption.

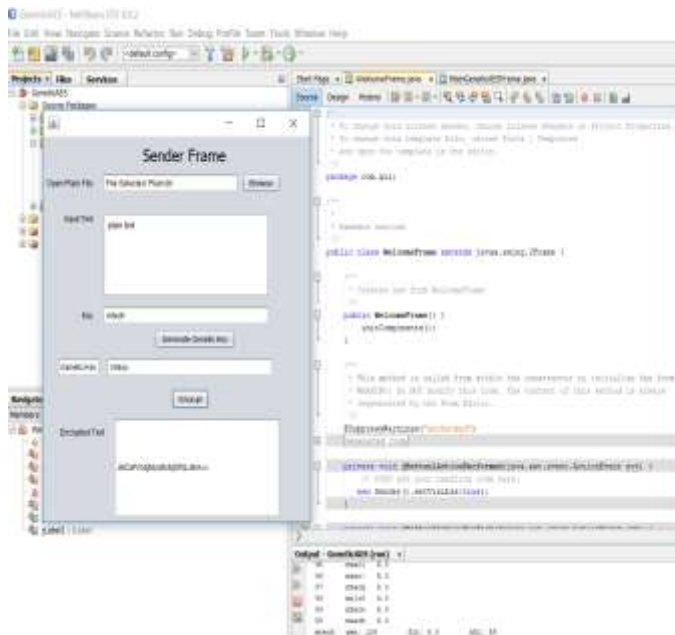
4. RESULTS



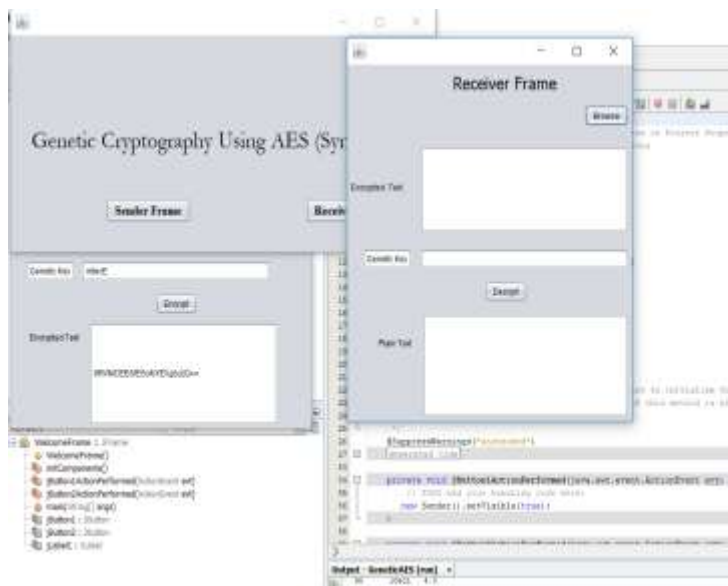
After running the file we will get the above screen as first screen and that is called as welcome screen, This screen contains two buttons. One is Sender Frame button, another one is Receiver Frame button.



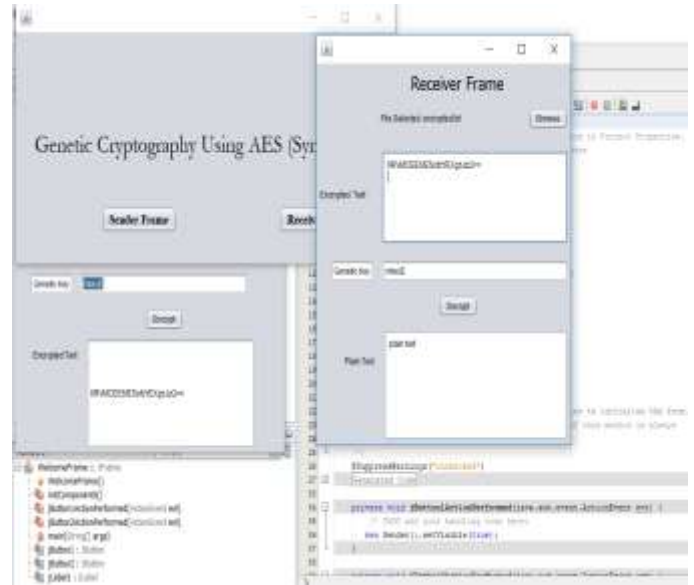
By clicking the Sender Frame button in the welcome Screen, this screen will appear. And the above screen is “ Sender Frame Screen”.



In the above result we are Uploading the file by using the button Browse, after that by enter the key, click the Generate Genetic key button and then Genetic key will be generated. By clicking the Encrypt button we can get the Encrypted data.



After encrypting the data. The sender will send the file, then the Receiver Frame button should be clicked in the welcome frame and the above Screen is “Receiver Frame”.



After encryption the encrypted data is stored in default file. Open Receiver frame and upload the encrypted file by using the browse button and then enter the genetic key. Click the Decrypt button and then we can get the Plain text.

5. CONCLUSION

In this paper, we used the Genetic Key for the encryption of data. The genetic key generated helps us in providing the privacy along with secrecy. The various techniques such as mutation, crossover, fitness functions are used for the generation of genetic key. After the genetic key generation data is diffused and XOR ed for encryption. In future, we wish to enhance this project to all types of files including images, video files and other miscellaneous files. And we would also increase the efficiency.

6. REFERENCES

- [1] R. Jhingran and A. Prof, “A Study on Cryptography using Genetic Algorithm VikasThadaShivali Dhaka,” Int. J. Comput. Appl., vol. 118, no. 20, pp. 975–8887, 2015.
- [2] A.-K. S. O. Hassan, A. F. Shalash, and N. F. Saady, “MODIFICATIONS ON RSA CRYPTOSYSTEM USING GENETIC OPTIMIZATION,” Int. J. Res. Rev. Appl. Sci., vol. 19, no. 2, p. 150, 2014.
- [3] S. K and P. D. S, “A Symmetric Key Encryption Technique Using Genetic Algorithm.”
- [4] A. Soni and S. Agrawal, “Using Genetic Algorithm for Symmetric key Generation in Image Encryption,” Int. J. Adv. Res. Comput. En. Technol., vol. 1, no. 10, pp. 2278–1323, 2012.
- [5] S. Jawaid and A. Jamal, “Article: Generating the Best Fit Key in Cryptography using Genetic Algorithm,” Int. J. Comput. Appl., vol. 98, no. 20, pp. 33–39, Jul. 2014.

- [6] G. M. Krishna and V. Lakshmi, "A Proposed Method for Cryptographic Technique by Using Genetic Function," Int. J. Emerg. Eng. Res. Technol., pp. 1–7, 2015.
- [7] S. Das, S. N. Mandal, and N. Ghoshal, "Diffusion and Encryption of Digital Image Using Genetic Algorithm," in Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014, 2015, pp. 729–736.
- [8] A. Almarimi, A. Kumar, I. Almerhag, and N. Elzoghbi, "A NEW APPROACH FOR DATA ENCRYPTION USING GENETIC Original Image Pseudorandom Binary Sequence Generator using GA and Decryption Decrypted Image," Computer (Long. Beach. Calif).pp. 2–6, 2014.

BIOGRAPHIES



B. Sripriya,
M. Tech Scholar,
CSE Department,
Raghu Engineering college,
Vishakapatnam.



N. Srinivasan,
Senior Assistant professor,
CSE Department,
Raghu Engineering college,
Vishakapatnam.