Symmetric Cryptography using Genetic Algorithm

Bondada Sripriya[1], N.Srinivasan[2]
[1] *M.tech Scholar, Dept. of CSE, Raghu Engineering College, Visakhapatnam, Andhra Pradesh, India.*
[2] *Senior Asst.Prof, Dept. of CSE, Raghu Engineering College, Visakhapatnam, Andhra Pradesh, India.*

Abstract - In today's age of information technology secure transmission of information is a big challenge. Symmetric and asymmetric cryptosystems are not appropriate for high level of security. Modern hash function based systems are better than traditional systems but the complex algorithms of generating invertible functions are very time consuming. In traditional systems data is being encrypted with the key but still there are possibilities of eavesdrop the key and altered text. Therefore, key must be strong and unpredictable, so a method has been proposed which take the advantage of theory of natural selection. Genetic Algorithms are used to solve many problems by modeling simplified genetic processes and are considered as a class of optimization algorithms. By using Genetic Algorithm the strength of the key is improved that ultimately make the whole algorithm good enough. In the proposed method, data is encrypted by a number of steps. First, a key is generated through random number generator and by applying genetic operations. Next, data is diffused by genetic operators and then logical operators are performed between the diffused data and the key to encrypt the data. Finally, a comparative study has been carried out between our proposed method and two other cryptographic algorithms. It has been observed that the proposed algorithm has better results in terms of the key strength but is less computational efficient than other two.

I. INTRODUCTION

Recently, secure data transmission over network has become a vital and critical issue due to increased demand of digital media transmission and unauthorized access of important data [1]. Cryptography uses mathematical techniques for information security, data integrity, confidentiality, nonrepudiation and authentication. Cryptography is based on concepts of Encryption and Decryption [2]. When data is sent from sender to receiver, the data is converted to some unreadable form called encryption of data and at receiver side data is again converted to its original form called decryption of data. Both encryption and decryption process require the key. For protection of valuable information from unlawful imitation, eavesdropper's attack and modification, different types of cryptographic algorithms are designed. There are two major types of such algorithms: symmetric cryptography [3] and asymmetric cryptography [4]. In asymmetric key cryptography two different keys are used, one for encryption called public key and one for decryption called private key.

Only one same key is used in symmetric scheme. The applications of both schemes differ due to efficiency of scheme; symmetric scheme is mostly used for encryption of data due to its high performance while asymmetric is often used for digital signature and distribution of key. Moreover, no any symmetrical ciphering technique such as AES, DES, Advanced AES, and IDEA has taken any benefit from most recent advances in information processing technology. Various kinds of modern data encryption techniques [2], [5] are found in the literature. Genetic Algorithms (GAs) [6] are among such techniques.

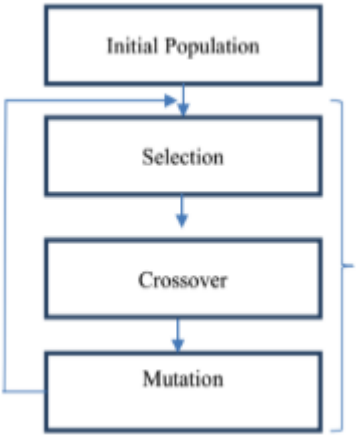

Fig1: Flowchart of genetic algorithm

GA is kind of adaptive search algorithms which make use of the mechanics of natural selection and genetics. GA is part of Evolutionary Algorithms; which are used to solve optimization problems with the help of biological mechanism like selection, crossover and mutation [7]. Fig. 1 shows the process of solving optimization problems using Genetic Algorithms.

The key idea of GA is to imitate the randomness of the nature where natural selection process and behaviour of 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 [8]. Genetic Algorithm performs following operations to transform the population to new population based on fitness value.

Crossover

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

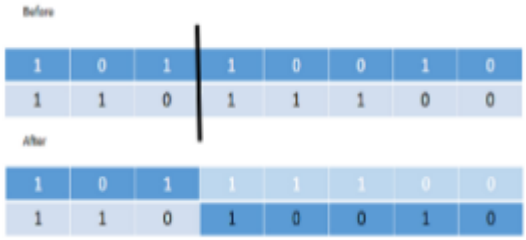

Fig2: Single point crossover

Crossover is classified as single point, two point and uniform crossover. In Single Point only one crossover point is selected to generate new child (Fig. 2). In Two Point crossover two crossover points are selected to generate new child. In Uniform crossover bits are selected uniformly from each (Fig. 3) [8].

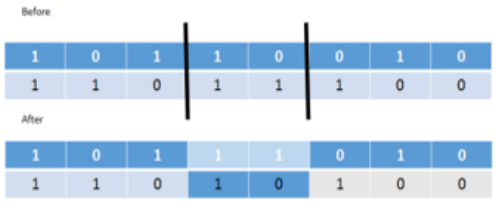

Fig. 3. Two point crossover.

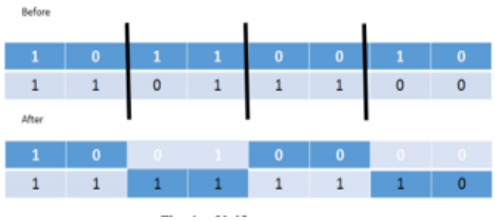

Fig.3. Uniform Crossover

Mutation

In mutation after crossover at least one bit in each chromosome is changed (Fig. 4) [9]. This is performed to reflect the effect of surrounding 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 [9].

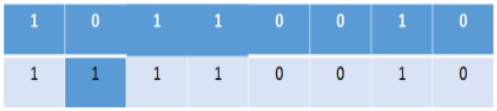

Fig.4. Mutation

Selection

In selection, chromosomes are chosen from the population for generation of new population. The selection is based on fitness value, higher the value more is the chances to be selected. Selection is classified as Roulette-wheel Selection, Tournament Selection; Truncation Selection [8].

Fitness Function

This is very important function of Genetic Algorithm because good fitness functions are useful for exploring the search space efficiently and bad fitness functions are confined to local optimum solution. Fitness Function can be categorized as Constant fitness function and Mutable fitness function [9].

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

II. LITERATURE SURVEY

With the help of GA most of the research has been done by different researchers in the area of data encryption and key-generation. Some of the work is defined in this section. Jhingran et al. [7] conducted survey on applications of genetic algorithm in the field of cryptography.

Hassan et al. [10] have used the concept of encryption and encryption with the help of GA and RSA. First the key was generated with the help of GA and then generated key was used in RSA to encrypt the data. In this way the strong key was generated that was non-repeating too and this was not easy to break. This algorithm is better in terms of key strength than DES, AES, and RSA, etc. Sindhuja et al. [11] has given asymmetric key cryptosystem by applying GA. Key matrix andtext matrix were added to create an additive matrix and then substitution cipher was applied on additive matrix to create the intermediate cipher. Crossover and Mutation were then applied on intermediate cipher to encrypt the data. This method is simple and easy to implement.

AartiSoni et al. [12] proposed a new algorithm in which pseudorandom number generator was used to generate the key. The random number generator used the current time of computer for random numbers. Then genetic operations were performed on random numbers. Finally selected key was used in AES symmetric algorithm to encrypt the image. The benefits of this algorithm were increased efficiency, less computational time and irregularity of key. The same method of key generation was also followed by Sania Jawed et al. [13] but in this, fitness value was calculated by applying Frequency and Gap test along with hams distance between the two binary keys. This algorithm was implemented in Java technology where 100 chromosomes, 0.5 mutation rate, 2.5 crossover rate were selected for the algorithm.

The performance analysis of scheme revealed that the algorithm possesses the good statistical results, key sensitivity and can handle the plaintext attack, brute force attack, entropy attack and differential attack. Kirshna et al. [15] proposed cryptographic algorithm by using genetic function. In this algorithm substitution matrix and double point crossover was used to encrypt the data. This algorithm was implemented in Xilinx 13.2 version and verified using Spartan 3e kit. Almarimi et al. [16] dealt with security of electronic data over network. The proposed algorithm integrated the GA and pseudorandom sequence for encryption and decryption of data. Random sequence was obtained by using nonlinear shift register. Time and speed of algorithm was calculated for observing results.

Fitness of key was calculated by Pearson coefficient of autocorrelation. Two keys public and private were generated by using random number generator, crossover and then mutation. Finally Gap and Frequency tests were applied to select the best sample of key. The process was repeated until there was no best key. C++programming was used to implement the algorithm and frequency was tested by chi-square test. The genetic operations were repeated until fitness value of any chromosome is less than threshold. Once completed the final selection of key was done through GA. Selected key was unique and non-repeating.

In this paper two enhanced AES cryptosystems were proposed by using GA in SP boxes. AES was modified to accommodate the nonlinear Neural Network SP network. This scheme ensured the increased security against timing attacks and reduction of computational time. Subhajit et al [17] encrypted an image by using genetic algorithm. Then statistical test were performed to visualize the feasibility of solution. The work done by researchers has impressive results but each research work has used some existing cryptographic algorithm in combination with genetic operators. Our motivation is to create novel cryptographic algorithm with the help of Genetic operations, which is easy to implement and secure in terms of key strength and attack time.

III. SYSTEM ANALYSIS

Existing system

Symmetric and asymmetric cryptosystems are not appropriate for high level of security. Modern hash function based systems are better than traditional systems but the complex algorithms of generating invertible functions are very time consuming. In traditional systems data is being encrypted with the key but still there are possibilities of eavesdrop the key and altered text. Therefore, key must be strong and unpredictable, so a method has been proposed which take the advantage of theory of natural selection.

Proposed system

The proposed algorithm (Genetic Cipher) is produced using AES symmetric key cryptosystems in terms of encryption, decryption time and key strength. The key strength is categorized by key search space size means how many alternative keys can be tried to break the cipher, Attack

Scenario means how much time is required by eavesdropper to attack on data.

The genetic operators are used in both key generation and data diffusion. Initial population is generated through random number generator. For simplicity one point crossover and bit filliping techniques are used for Crossover and Mutation respectively. Fitness value of key is calculated through Shannon Entropy because entropy is one of important feature of randomness.

Components of the UML

The UML consists of a number of graphical elements that combine to form diagrams. Because it's a language, the UML has rules for combining these elements. The purpose of the diagrams to present multiple views of the system, and this set of multiple views is called a Model. A UML Model of a system is something like a scale model of a building. UML model describes what a system is supposed to do. It doesn't tell how to implement the system. The following are the main nine component Diagrams of U M L:

Class Diagram

A Class is a category or group of things that has similar attributes and common behavior. A Rectangle is the icon that represents the class it is divided into three areas. The upper most area contains the name, the middle area contains the attributes and the lowest areas show the operations. Class diagrams provides the representation that developers work from. Class diagrams help on the analysis side, too.

Object Diagram

An object is an instance of a class- A specific thing that has specific values of the attributes and behavior. A Rectangle is the icon that represents the object diagram but the name is underlined. The name of the specific instance is on the left side of the colon, and the name of the class is on the right side of the colon.

Use-Case Diagram

A Use-Case is a description of a systems behaviour from a user's stand point. For system developer this is a valuable tool: it's a tried-and-true technique for gathering system requirements from a user's point of view. That is important if the goal is to build a system that real people can use. A little stick figure is used to identify an actor the ellipse represents use-case.

State Diagram

At any given time, an object is in particular state. One way to characterize change in a system is to say that its objects change the state in response to events and to time. The UML

State Diagram captures this kinds of changes it presents the states an object can be in along with the transitions between the states, and shows the starting point and end point of a sequence of state changes.

A Rounded Rectangle represents a state, along with the solid line and arrow head that represents a transition. The arrow head points to the state being transition into. The solid circle symbolizes starting point and the bull's eye that symbolizes the end point.

Sequence Diagrams

In a functioning system objects interacts with one another and these interactions occur over time. The UML Sequence Diagrams shows the time based dynamics of the interaction. The sequence diagrams consists of objects represented in the usual way-as named rectangles (If the name underlined), messages represented as solid line arrows and time represented as a vertical progression.

Activity Diagrams

The state diagram shows the states of an object and represents activities as arrows connecting the states. The Activity Diagram highlights the activities. Each activity is represented by a rounded rectangle-narrower and more oval-shaped than the state icon. An arrow represents the transition from the one activity to the next. The activity diagram has a starting point represented by filled-in circle, and an end point represented by bull's eye.

Collaboration Diagram

An object diagram shows the objects and their relationships with one another. A collaboration Diagram is an extension of the object diagram. In addition to the associations among objects, the collaboration diagram shows the messages the objects and each other.

IV. RESULTS

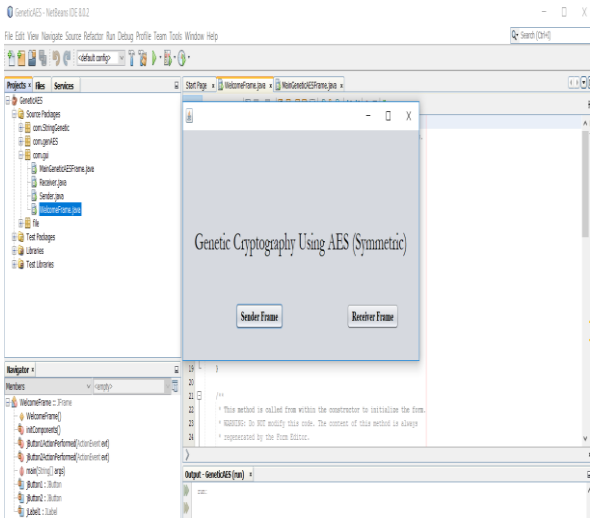

Fig.5. Output of Generic Cryptography using AES

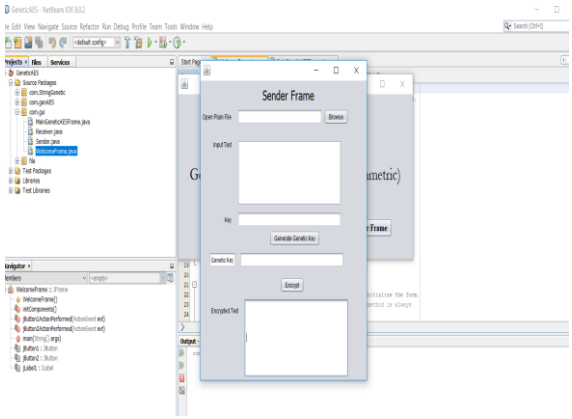

Fig.6. sender frame

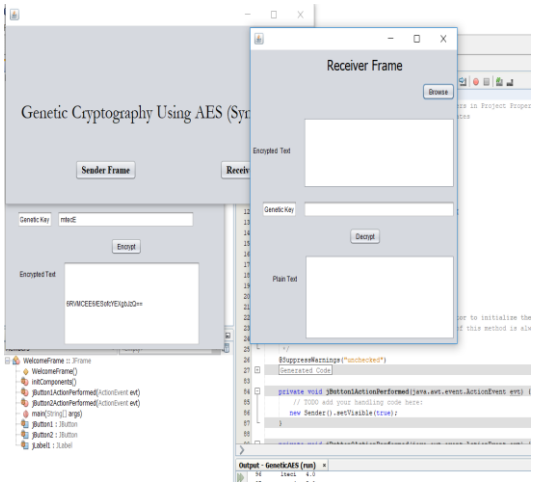

Fig.7. Receiver side frame

V. CONCLUSION

In this paper we have adopted a new way to encrypt the data i-e using GA. First a key of is generated by applying genetic operations on randomly 1 https://www.grc.com/haystack.htm generated characters and prime numbers. Shannon Entropy is used to calculate the fitness value of each chromosome. After key generation, data is diffused again by applying crossover and mutation on data. At last key and diffused data are XORed for encryption. The result shows that although the proposed algorithm take little longer encryption time than DES and AES but the key strength is better than the other two compared algorithms.

In future we will prepare to improve this algorithm for multimedia encryption like images, video and audio. Efficiency in terms of time will be considered first. From the evaluation point of view, we will compare this genetic cipher with other cryptographic algorithms. Also, we can use more statistical techniques for evaluation of key randomness.

VI. REFERENCES

[1] 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.

[2] D. R. Stinson, Cryptography: Theory and Practice, vol. 30. 2005.

[3] J. Daemen and V. Rijmen, The Design of Rijndael: AES – The Advanced Encryption Standard. 2002.

[4] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Commun. ACM, vol. 21, no. 2, pp. 120–126, 1978.

[5] W. M. H. Company, Modern Cryptography: Theory and Practice, vol. 170, no. 2. 2003.

[6] D. E. Goldberg, Genetic Algorithms in Search, Optimization, and Machine Learning. 1989.

[7] R. Jhingran and A. Prof, "A Study on Cryptography using Genetic Algorithm Vikas Thada Shivali Dhaka," Int. J. Comput. Appl., vol. 118, no. 20, pp. 975–8887, 2015.

[8] S. Mishra and S. Bali, "Public key cryptography using genetic algorithm."

[9] A. Kumar and K. Chatterjee, "An efficient stream cipher using Genetic Algorithm," 2016 Int. Conf. Wirel. Commun. Signal Process. Netw., pp. 2322–2326, 2016.

[10] A.-K. S. O. Hassan, A. F. Shalash, and N. F. Saudy, "MODIFICATIONS ON RSA CRYPTOSYSTEM USING GENETIC OPTIMIZATION," Int. J. Res. Rev. Appl. Sci., vol. 19, no. 2, p. 150, 2014.

[11] S. K and P. D. S, "A Symmetric Key Encryption Technique Using Genetic Algorithm."

[12] 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.

[13] 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.

[14] N. K. Pareek and V. Patidar, "Medical image protection using genetic algorithm operations," Soft Comput., vol. 20, no. 2, pp. 763–772, 2014.

[15] G. M. K. and V. Lakshmi, "A Proposed Method for Cryptographic Technique by Using Genetic Function," Int. J. Emerg. Eng. Res. Technol., pp. 1–7, 2015.

[16] K. Kalaiselvi and A. Kumar, "Enhanced AES cryptosystem by using genetic algorithm and neural network in S-box," in 2016 IEEE International Conference on Current Trends in Advanced Computing, ICCTAC 2016, 2016.

[17] 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.