IJCSN - International Journal of Computer Science and Network, Volume 6, Issue 3, June 2017
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Encryption and Decryption Using Genetic Algorithm Operations and Pseudorandom Number

[1] **P Srikanth; [2]Abhinav Mehta; [3] Neha Yadav; [4] Sahil Singh; [5] Shubham Singhal**

[1]Assistant Professor, School of Computer Science & Engineering,
University of Petroleum & Energy Studies
Dehradun, Uttarakhand-248007, India

[2, 3, 4, 5] Student, Final year B. tech CSE-IT, School of Computer Science & Engineering,
University of Petroleum & Energy Studies
Dehradun, Uttarakhand-248007, India

Abstract- Data security is crucial for almost all businesses and home computer users. Client information, payment information, personal files, bank account details etc. are very important and hard to replace. It is potentially dangerous and can grow into a threat if it falls in the wrong hands; to protect the data encryption is one of the most widely used techniques. This paper deals with the integrity and confidentiality of data, which is transmitted through different mediums. Genetic algorithms (GAs) have many functions, in this paper we use the genetic algorithm operation such as crossover and mutation functions, genetic algorithm concepts with pseudorandom function are being used to encrypt and decrypt data. The encryption process is applied over a binary file therefore the algorithm can be applied over any type of data.

Keywords - *Security, Integrity, Confidentiality, Crossover, Mutation, Pseudorandom Sequence*

1. Introduction

In today's world providing security to the data is one of the most concerned issue; there has been a huge loss of data through illegal access therefore, providing security is priority these days. To protect the important information from hackers or against illegal access and modifications, cryptographic schemes are needed. Cryptographic schemes are of two types: symmetric and asymmetric cryptography. The symmetric cryptographyis the one which uses the same key for encryption and decryption[1,2,3].In asymmetrical cryptography two keys are used, one for encryption(known as public key) and the other for decryption(known as the private key).

The genetic algorithm is a search algorithm which is based on the mechanics of natural selection and natural genetics. The set of operators usually consists of mutation, crossover and selection[3,4].

Genetic algorithms contain operations which are bio-inspired operators such as mutation, crossover and selection. They are used to optimize and search problems by generating high-quality solutions. In this paper crossover and mutation operation are used[5].

1.1. Crossover:

The process in which two chromosomes or two attributes are taken and a resultant chromosome(new) is formed by taking some part of first chromosome and the rest by second chromosome.

There are three types of crossover operation in genetic algorithm.

A.Single point crossover:the selected chromosome is broken into half and the new chromosome is formed by interchanging or swapping the half of the selected two chromosomes.
B. Two-point crossover: the selected chromosome is divided into three parts by taking two pointsand then one parts of each chromosomes are swapped to form new chromosome.
C. Multi point crossover: the selected chromosome is divided into 'n' number of parts and then the swapping is done in order to form new or resultant chromosomes[6].

1.2. Mutation

Mutation is a genetic operation which is similar to biological mutation and is used to create genetic diversity of its one generation from its successive generation.

Mutation allows the algorithm to prevent the population of chromosomes from becoming similar to each other.

1.3. Pseudorandom Number:

There are various methods through which random numbers can be generated, but the most commonly used method is multiplicative congruential generator also called as power residue generator. The function used to generate pseudo random number is

$X_{i+1}=X_i.a$ (modulo m)

Where X_i is the i^{th}pseudo random number and X_{i+1} is the succeeding pseudo random number of X_i. Here a and m are positive integer numbers, a will be constantly multiplied by X_i and the result i.e. $X_i.a$ will be divided by m until the remainder becomes less than m. The first number, also called as seed(X_0) is the number using which we start calculating pseudo random numbers.

To produce the maximum number of random number i.e., to maximize the period after which the numbers will start repeating, the value of a, $X_{i\ and}$ m has to be taken such that:

1. The value of random number will always be less that m, therefore the value of m should be largest number possible i.e., 2,147,383,648.
2. The value of a and X_0 should be relatively prime to m and since m is in power of 2 therefore the any odd number can be taken. But it is found that the best value for a is 2^{16} +3= 65,539[7].

2. Literature Review

In today's world data loss through the illegal access is one of the most concerned issues. Providing security is on the priority list therefore a performance measure produces between traditional cryptography algorithm and genetic algorithm in order to validate genetic algorithm methods in the field of cryptography has been done[5].

New cryptographic algorithm should be developed by using genetic algorithm methods and should be tested on various file's as well as should be validated in order to provide security better than old or traditional cryptography algorithm as done[3].

3. Proposed Method

The proposed method is important as in today's world providing security to data is on everyone's priority list therefore cryptography schemes are needed for preventing unauthorized access to data. This method contains the use of the operations of genetic algorithm in order to encrypt the data.

Studies tell us that Genetic algorithm for cryptography is better than typical algorithms for cryptography. Genetic algorithms contain process/operations which are bio-inspired operators such as mutation, crossover and selection. They are used to optimize and search problems by generating high-quality solutions. The method discussed below generate different key by pseudorandom function for each block of data according to which the crossover is applied and in order to provide more security mutation is also applied.

Since the proposed method is being applied to the binary data therefore it can be used to encrypt different type of file.

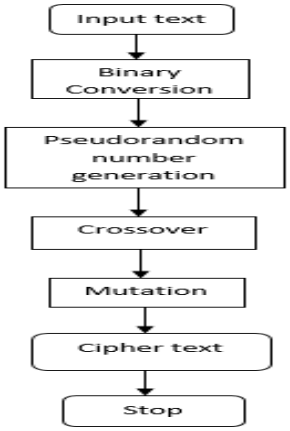


Fig.1 Encryption

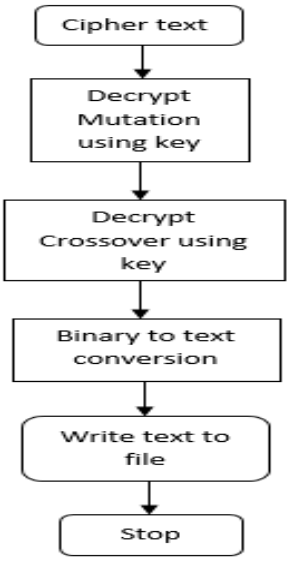


Fig.2 Decryption

The methods used are pseudorandom number generation, crossover method, binary conversion, Mutation and ASCII conversion.

3.1. Crossover

The three types of the crossover used are single point, two-point and multipoint crossover.
The crossover is chosen by modulating the pseudorandom number by 3.

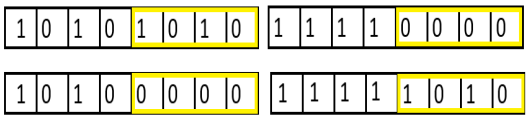


Fig. 3Single point crossover

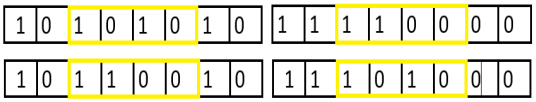


Fig. 4Two-point crossover

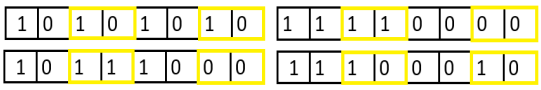


Fig.5 Multipoint crossover

3.2. Pseudorandom Number:

Pseudo random numbers are deterministically generated numbers which appears to be random. Various arithmetic approaches are used to generating pseudo-random numbers have been suggested, considered, and used on computers in the past thirty years or so. These approaches are usually recurrence relation and new numbers are generated from the earlier one by applying some simple scrambling operation. A fast, and the most commonly used method (or generator) is the so-called multiplicative congruential generator (sometimes also called as the power-residue generator).It consists of computing X[i+1]=X[i].a(modulo m),where X[i] is the pseudo-random number, X[i+1] is the next pseudo-random number, a is constant multiplier and, modulo m means that the number(X[i].a) is divided by m repeatedly till the remainder is less than m. The remainder is then set equal to the next number X[i+1]. The process is started with an initial value X [0] called seed.

3.3. Mutation:

In the mutation process flipping of the bits is done i.e. if the encountered bit is 1 then it is gets converted/flipped to 0.

3.4. Key:

The number which is being generated by the pseudorandom number method is stored as a key and further operations are applied to it.

4. Implementation

4.1. Encryption method:

1. Transform the file into ASCII form then into corresponding binary form.
2. Divide the binary form into the sets/blocks of 8bits. 8 is also stored as a secret key.
   N= number of blocks
   N= Length of binary string/8
   New binary blocks of 8 bits are denoted as S1, S2, S3….Sn.
3. Generate pseudorandom number for every two selected blocks. Which will act as a key and mod it by 3 to choose crossover and store the key?

0 for single point crossover
1 for two-point crossover
2 for multipoint crossover

4.Apply the crossover method on selected chromosomes or blocks. Blocks after crossover are denoted as C1,C2,C3….Cn.
5.Now apply the mutation on selected block or chromosomes, mutated blocks are denoted as M1, M2, M3…….Mn.
6. Repeat from step3 till the end of the blocks.
7. Now convert binary form into ASCII then corresponding file type.
8.Store the result in the file.

4.2. Decryption Process:

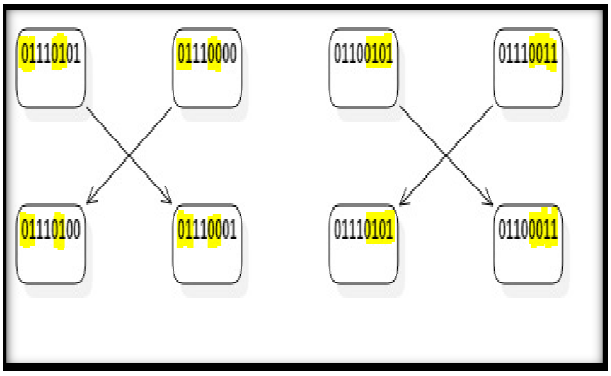
1.Transform the file into ASCII form and then to binary form.
2.Divide the binary form into the sets or block of 8 bits.
3.Apply mutation process on the blocks i.e. M1, M2, M3….Mn.
4.Now mod the key of the selected blocks by 3 to apply crossover method.
5.Apply the crossover method on the selected blocks C1, C2, C3….Cn.
6.Repeat onwards step 3 till the end of the blocks.

7.Convert or transform the binary form into ASCII form and then to the file form.
8.Store the result in the file.

5. Experimental Result

5.1. Encryption Process:

Step 1: File_content = upes
Step 2: File_content is converted into binary form i.e.
01110101011100000110010101110011.
Step 3: Divide the binary form into blocks containing 8 bits i.e.
s1=10001110 s2=10001011
s3=10011010 s4=10001100
Step 4: Generate pseudorandom number using the pseudorandom function for two blocks. Apply modulo operation (mod of 3) on the generated pseudorandom number.
Step 5: After applying the mod function according to the output the crossover function is chosen.
If output = 0 then Single point crossover is applied, if output = 1 then two-point crossover is applied and If output = 2 then uniform crossovers is applied.
23%3=2(Uniform crossover), 63%3=0(Single point crossover).
Step 6: Apply the crossover method on respective blocks.

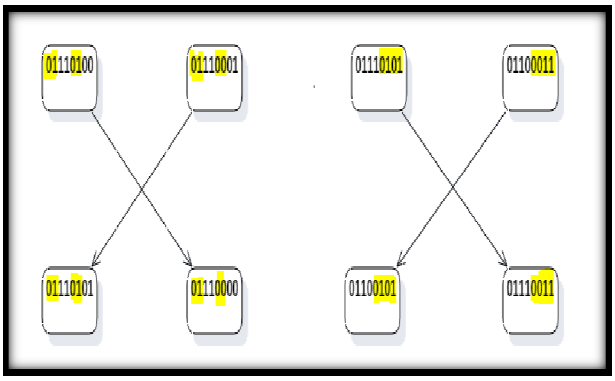


Step 7: Apply mutation function on the generated blocks.
01110100011100010111010101100011 ->10001011100011101000101010011100
Step 8: Convert the final block generated into text and that will be encrypted text.
Encrypted text:????

5.2. Decryption Process:

Step 1: Convert the text into binary form (blocks).
????->10001011100011101000101010011100.
Step 2: Apply mutation function on all blocks.
10001011100111010001010100111100 ->01110100011100010111010101100011.
Step 3: Read the random numbers from the key and perform modulo function (mod 3) on the random number.

63%3=0(Single point crossover), 23%3=2 (Uniform crossover).
Step 4: According to the output of mod function perform crossover function on two blocks.
S1=01110100 s2=01110001
S3=01110101 s4=01100011



Step 5: After performing crossover function convert the blocks into original form.

ORIGINAL FORM = upes

6. Application

We have tested the above proposed algorithm on various text files which includes data such as plain text, numeric values and special characters. Since the proposed algorithm work on the binary format of the data therefore this algorithm can be applied on various types of data such as video, audio, text etc.

S. No.	File Name	Original Text	Encrypted Text	Decrypted Text	Reference Figure
1	A.txt	this is symbol language = *&%$@ !12ADfa (+?	?????ÖÏ?? ??????Ó?? ????Ú?ßÕ ÙÚ¿ÛÞÎ- Þ?»Ö?ÐÄ	this is symbol language= *&%$@! 12ADfa(+ ?	Figure 6
2	B.txt	5000393 67 5000411 36 5000403	ÏÊÏÏÎÄÈÍÎ ØÏÊÏÏÏÊÎÌÍ ÛÏÊÏÏÏÈÌÏÏ ÚÊÎÏÏÄÎÇ ÈïÝ	50003936 7 50004113 6 50004030	Figure 7

		05 5000398 72		5 50003987 2	
3	C.txt	WE are STUDE NTS OF BTECH CSE IFM in UPES	¨º?Þ???ì«ª »³©Ï¼±¸ ¿Ýª»¿´¿Ü¨ ¾?þ±º?ÞÑ ?ª¯¾¨	WE are STUDEN TS OF BTECH CSE IFM in UPES	Figure 8

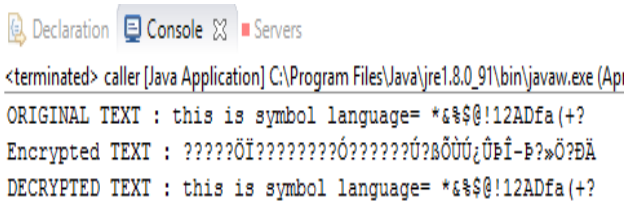


Figure6shows the encrypted and decrypted text that contains alphanumeric and special characters.

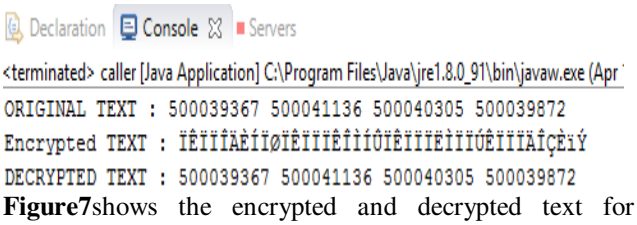


Figure7shows the encrypted and decrypted text for numeric values.

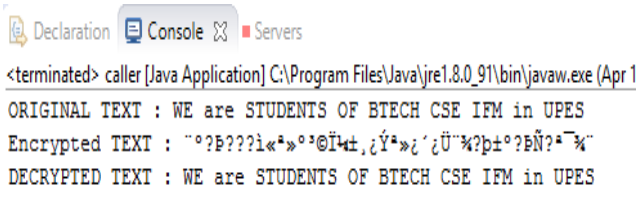


Figure8shows the encrypted and decrypted text that contains alphabets.

7. Conclusion and Future Work:

In this paper, a cryptography algorithm for encryption and decryption of data which uses the operations of genetic algorithm. Encryption of binary data is successful and we have satisfied our goals. Thus, we conclude that applying operations of Genetic Algorithm to provide security to the data in a file is a feasible.

The algorithm is tested and results are reported, we have used multiplicative congruential generator method for the generation of pseudorandom numbers. In the future work, same algorithm we can apply for media files like images and video and testing it over.

References

[1] Stallings, W.,Cryptography and network security principles and practice (5th ed.), Boston: Pearson, (2014).

[2] Deo, N., System simulation with digital computer, Prentice Hall of India Publications, (2011).

[3] SuvajitDutta andTanumay Das, "a Cryptography Algorithm Using the Operations of Genetic Algorithm & Pseudo Random Sequence Generating Functions",International Journal of Advances in Computer Science and Technology, Volume 3, (2014), ISSN 2320 – 2602.

[4] David E Goldberg, "Genetic algorithms in search, optimization and machine learning". (1989).

[5] Delman, B., "Genetic Algorithms in Cryptography",M.S. in Computer Engineering, Rochester Institute ofTechnology, Rochester, New York, July(2014).

[6] Goyat, S.,"GENETIC KEY GENERATION FOR PUBLIC KEY CRYPTOGRAPHY", International Journal of Soft Computing and Engineering (IJSCE), Volume 2(3), (2012).

[7] Bhasin, H., Bhatia, S., "Applications of Genetic Algorithm in Machine learning", IJSCIT, Volume 2(5), (2011).