International Journal of PharmTech Research
CODEN (USA): IJPRIF, ISSN: 0974-4304
Vol.9, No.3, pp 422-428, 2016

Genetic-Crypt: A Novel Encryption Approach for Secure Communication using Genetic Operations

Kalaichelvi V*, Manimozhi K, Meenakshi P, Poornima M, Sumathi A

SASTRA University, Kumbakonam, India

Abstract: Security is the primary concern in the field of Information technology. Cryptography plays an important role in the field of secure communication. This Paper proposes a novel technique for encryption and decryption. It is based on the Genetic operations like selection, crossover and mutation. For selection operation, it uses a new PRNG method called M-CSPRNG (Modified-Cryptographically Secure Pseudo Random Number Generator). This M-CSPRNG method increases the complexity for the attacker. Based on the random number only, the successive operation such as crossover and mutation is performed on the plain text. So, it will be very difficult for the attacker to generate the random number. Moreover, radix 64 conversion is used at the end. So, it will create confusion to the hacker that how the encryption and decryption algorithm is carried out.
Keywords: Genetic algorithm, PRNG, Mutation, Crossover operation and Radix 64..

1.0 Introduction

Cryptography plays an important role in the field of secure communication. There are two types of cryptosystem: Symmetric key cryptosystem and Public Key cryptosystem. Using Symmetric key Cryptosystem, we can achieve confidentiality service. Many algorithms are published such as DES, 3-DES, Blowfish, AES IDEA, etc,. Using Public Key Cryptosystem, we can achieve both confidentiality and authentication services. In Public key Cryptosystem, there are many popular algorithms such as RSA, ECC, ElGamal, etc,. All Symmetric Key algorithms are based on Substitution and Permutation operations and Public key algorithms uses lot mathematical concepts. But, this paper stands different that this paper proposes the Genetic Operations for encryption and decryption. Evolutionary algorithm (EA) is a subset of Evolutionary Computation (EC). Genetic Algorithm is the main paradigm of Evolutionary Computation. It is necessary to explain some of the terms. **Chromosome** is a set of genes. **Gene** is a part of chromosome. For example, a **pixel** in an image is a Chromosome. Genes are **R, G, B** and **Intensity** components. There are three important operators in Genetic Algorithm: **Selection, Crossover and Mutation.**

The organization of the paper is as follows. Section 2 discuss about the various encryption approaches based on genetic operations. Basic concepts of Genetic Operations and Radix 64 conversions are outlined in section 3. Section 4 discuss about the procedure for proposed Pseudo Random Number Generator. In section 5, Proposed encryption / decryption methods are presented with examples. Finally, section 6 describes the concluding remarks.

2.0 Literature Survey

Sindhuja K et.al., constructs two matrices such as text matrix and key matrix from the given inputs. An Additive matrix is generated from those two matrices. Then, linear substitution technique is applied on additive

matrix to generate intermediate cipher text. Finally, the Genetic operation such as mutation and crossover operation is applied to produce cipher text. Generally, Decryption is the reverse process of encryption. But, in addition to the cipher text more information such as user input (Key), Block size, Prime numbers which is used in substitution and mutation and crossover points. If these information are plainly transferred to the other end, It may be vulnerable to the cryptanalysis. Moreover, it will degrade the efficiency [4]. Wafa' Slaibi Alsharafat et.al., uses mutation and crossover genetic operator for converting plain text into cipher text. It may be one of the substitution or transposition techniques. There is no complexity in any part so that it is more vulnerable to the cryptanalysis [5]. Amritha Thekkumbadan Veetil et.al., uses only Mutation and crossover operator. It is a simple technique and it is more vulnerable to the cryptanalysis. Moreover, the sender has to transfer lot of information to receiver side [6].

3.0 Genetic Algorithm

Evolutionary algorithm (EA) is a subset of Evolutionary Computation (EC). Genetic Algorithm is the main paradigm of Evolutionary Computation. It is necessary to explain some of the terms. **Chromosome** is a set of genes. **Gene** is a part of chromosome. For example, a **pixel** in an image is a Chromosome. Genes are **R, G, B** and **Intensity** components. There are three important operators in Genetic Algorithm: **Selection, Crossover and Mutation.**

Selection:

Selection means extract a subset of genes from an existing population according to any definition of quality (i.e., based on fitness function value). In this paper, random number is generated and based on that number the value is chosen to apply both crossover and Mutation operation.

Crossover:

Crossover selects genes from parent chromosomes and creates a new offspring. It combines two chromosomes to produce a new chromosome. There are different types: One-point, Two-point, Uniform, Arithmetic and Heuristic crossover.

One-point crossover:

One-point crossover operator randomly selects one crossover point and then copies everything before this point from the first parent and then copies everything after this point from the second parent

Example:

With the two parents selected above, we randomly generate a number 2 as the crossover point:

Parent1: **7 3 7 6 1 3**
Parent2: **1 7 4 5 2 2**

Then we get two children:

Child 1 : **7 3** | **4 5 2 2**
Child 2 : **1 7** | 7 6 1 3

Two-point Crossover

The procedure of two-point crossover is similar to that of one-point crossover except that we must select two positions and only the bits between the two positions are swapped. This crossover method can preserve the first and the last parts of a chromosome and just swap the middle part.

Example:

With the two parents selected above, we randomly generate two numbers 2 and 4 as the crossover positions:

Parent1: **7 3 7 6 1 3**

Parent2: **1 7 4 5 2 2**

Then we get two children:

Child 1 : **7 3**| **4 5**| **1 3**
Child 2 : **1 7**| **7 6**| **2 2**

Uniform Crossover

Each gene of the first parent has a 0.5 probability of swapping with the corresponding gene of the second parent.

Example:

For each position, we randomly generate a number between 0 and 1, for example, 0.2, 0.7, 0.9, 0.4, 0.6, 0.1. If the number generated for a given position is less than 0.5, then child1 gets the gene from parent1, and child2 gets the gene from parent2. Otherwise, vice versa.

Parent1: **7 *3 *7 6 *1 3**
Parent2: **1 *7 *4 5 *2 2**

Then we get two children:

Child 1 : **7 7* 4* 6 2* 3**
Child 2 : **1 3* 7* 5 1* 2**

Mutation Operation:

Mutation is a genetic operator used to maintain genetic diversity from one generation of a population of chromosomes to the next. The mutation operator can overcome this by simply randomly selecting any bit position in a string and changing it.

3.1 Radix 64 Conversion

Radix 64 conversion is a binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation. Radix 64 conversion table uses 65 characters. It consists of 26 Uppercase letters, 26 lower case letters, 10 digits and 2 special characters i.e., + and / and a padding character ('='). So, totally it contains 65 characters. Radix 64 encoding procedure used in encryption side and Radix 64 decoding procedure used in decryption side. It takes 3 characters and then it is converted into binary based on the ASCII value of the characters. So, we will get totally 24 bits. This 24 bits split into 4 groups of 6 bits and find the corresponding decimal value. Finally, pick the corresponding radix 64 value from the Radix 64 conversion table. Radix 64 decoding is the reverse process of Radix 64 encoding procedure.

4.0 Modified Cryptographically Secure Pseudo Random Number Generator (M- CSPRNG)

A popular approach to generating secure pseudorandom numbers is known as the Blum, Blum, Shub (BBS) generator. This paper proposes considerably modified version of CSPRBG.

First, choose two large prime numbers, and that both have a remainder of 3 when divided by 4.That is, $p \equiv q \equiv 3 \bmod 4$. Generate the list of relatively prime numbers ($\varphi(n)$) which are relatively prime to n. From this list, generate another list using Euclid's algorithm. Each element should satisfy the following condition $GCD(\varphi(n),N) = 1$.

1. Select two prime numbers p and q, i.e., $p \equiv q \equiv 3 \bmod 4$.
2. Calculate $n=p \times q$
3. Calculate $\varphi(n) = (p-1) \times (q-1)$,Generate the numbers which are relatively prime to n.
4. Generate another list using Euclid's algorithm, i.e., $GCD(\varphi(n),N) = 1$ and $1< N < \varphi(n)$.
5. From the above list, take only the last two elements, namely X_0 and Y_0 and the algorithm proceeds as follows:

X_0 = last element -1 and Y_0 = last element
For I =1 to ∞
{$Y_i = X_{i-1} * Y_{i-1} \bmod n$
$C_i = Y_i \bmod 12$
$M_i = Y_i \bmod 4$
$X_i = Y_{i-1}$ }

Where C_i = Crossover point and M_i = Mutation Point. X_0 , Y_0 is considered as seed values.

5.0 Proposed Methodology

This paper proposes a novel technique for encryption and decryption. This paper introduces a new Pseudo Random Number generator method called, M –CSPRNG. It is the modified version of Cryptographically Secure Pseudo Random Number Generator (otherwise known as Blum Blum Shub Generator). Each time, it will generate unique random number. Based on the generated random number, Crossover and Mutation Genetic operation is performed on the plain text. Finally, the radix 64 encoding is performed to produce the final Cipher text. Decryption is the reverse process of an encryption. But, the sender should share the p and q (which is used in M-CSPRNG Process) values with the receiver. Then only, the receiver can generate random number to perform Mutation and Crossover operation. Because of this novel random number generator technique, it increases the strength to this algorithm. The proposed encryption and decryption procedure is explained (Fig.1-2) in the following section.

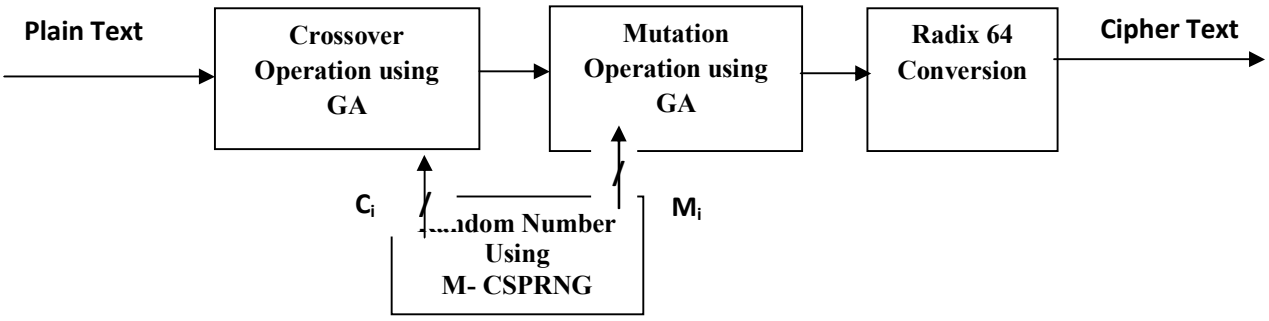


Fig.1 Proposed Encryption

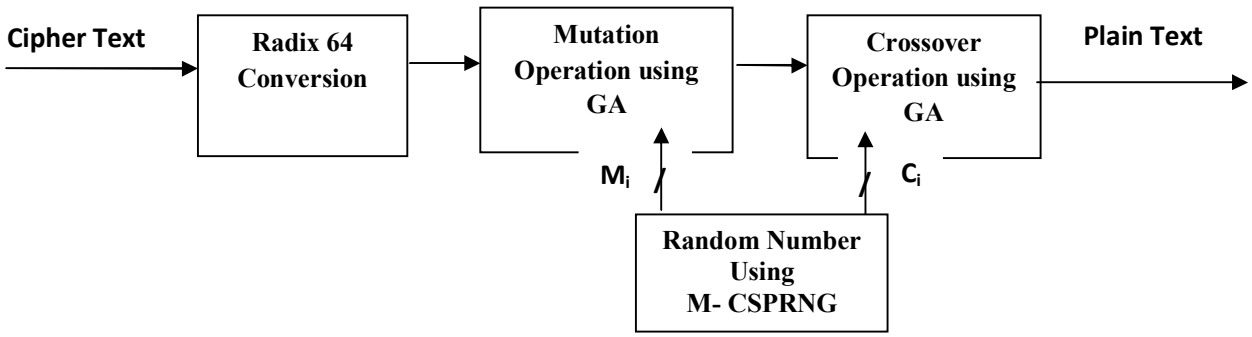


Fig. 2 Proposed Decryption

5.1 Encryption:

1. Convert the ASCII into binary
2. Generate the random number using proposed method.
3. Apply Crossover operation based on the random number sequence.
4. Apply mutation operation based on the random number.
5. Finally, apply Radix 64 encoding to get Cipher text.

5.2 Decryption:

Decryption is the reverse process of encryption. The cipher text is divided into groups of four characters and the following procedure is followed.

1. Apply Radix 64 decoding.
2. Generate Random number using Blum Blum Shub Generator.
3. Apply Mutation operation based on the random number.
4. Apply Crossover operation based on the random number sequence.
5. Finally, convert the binary into Decimal to get the original one.

5.3 Illustration:

Text : CRYPTO

Encryption:

67 82 89 80 84 79

Chromosome 1 Chromosome 2

01000011 01010010 01011001 01010000 01010100 01001111

Each Chromosome length is 24 bits. Each chromosome consists of four genes which is 6 bits of length.

010000 110101 001001 011001

Gene 0 **Gene 1** **Gene 2** **Gene 3**

Two prime numbers are p=3 and q=11, n=33 and φ(n)=20, where φ(n)={1,2,4,5,7,8,10,13,14,16,17,19,20,23,25,26,28,29,31,32}. Choose numbers, which satisfies the condition GCD(φ(n),N) = 1 and 1< N < φ(n). So the list contains {7,13,**17,19**}

X0=17 and Y0=19, after applying algorithm, the value of C1=2 and M1=2

Each chromosome consists of 4 genes that should be written in the following way.

01| 0000 110101

00|1001011001

After applying crossover operation, the resultant value will be

011001011001 000000110101.

It can be written as a collection of four genes. i.e., 011001 011001 000000 110101

After applying mutation operation, the resultant value will be

011001 011001 111111 110101

25 25 63 53

Z Z / 1

Similarly, the same procedure is applied for the remaining text. So, The Final Cipher text would be ZZ/1rPRF

Decryption:

Cipher text : ZZ/1 rpRF

Take the corresponding decimal value from the Radix 64 table. So, The values for the cipher text ZZ/1 will be 25 25 63 53. Then, the decimal value is converted into binary.

011001 011001 111111 110101

After applying mutation operation, the value will be

011001 011001 000000 110101

Then, the crossover operation is performed by writing the value in the following format.

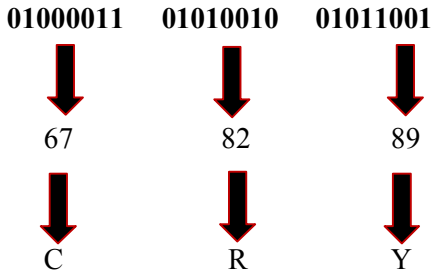
01|1001011001

00|0000110101

After applying crossover operation, the resultant value will be

010000110101001001011001

Finally, Split the value into groups of 8-bits and then covert it into corresponding ASCII character from its decimal value.



Similarly, the same procedure is applied for the remaining cipher text. So, The Final plain text would be CRYPTO.

6.0 Conclusion:

This Paper proposes a novel technique for encryption and decryption. It uses the genetic operations like selection, crossover and mutation. For selection operation, it uses a new PRNG method called M-CSPRNG (Modified-Cryptographically Secure Pseudo Random Number Generator). This M-CSPRNG method increases the complexity for the attacker. Based on the random number only, the successive operation such as crossover and mutation is performed on the plain text. So, it will be very difficult for the attacker to generate the random number. Moreover, radix 64 conversion is used at the end. So, it will create confusion to the hacker that how the encryption and decryption algorithm is carried out.

References

1. William Stallings, “Cryptography and Network Security”, 5th Edition.
2. S., N. Sivanandan, S. N. Deepa, “Introduction to Genetic Algorithm”, Springer Verlag Berlin Heidelberg, 2008.
3. Ankita Agarwal, “Secret Key Encryption Algorithm Using Genetic Algorithm”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012.

4. Sindhuja K , Pramela Devi S, “A Symmetric Key Encryption Technique Using Genetic Algorithm”, International Journal of Computer Science and Information Technologies, Vol. 5 (1), 2014.
5. Wafa' Slaibi Alsharafat, “Evolutionary Genetic Algorithm for Encryption”, 2014 IEEE International Conference on Computational Intelligence and Computing Research, 2014.
6. Amritha Thekkumbadan Veetil , “An Encryption Technique Using Genetic Operators”, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 4, ISSUE 07, JULY 2015 ISSN 2277-8616
7. Bruce Schneier, "Applied Cryptography" , John Wiley & Sons, Inc 1996
8. Richard Smith "Internet Cryptography",Pearson Edn Pvt.Ltd
9. Atul Kahate “Cryptography and Network Security”, Tata Mc.Graw Hill

*****