An Encryption Technique Using Genetic Operators

Amritha Thekkumbadan Veetil

Abstract: Encryption is a tool for protecting and securing data. Security provides safety and reliability. As the need for communication is increasing day by day, there comes necessity of encrypting data in-order to ensure a secure communication. This paper presents application of genetic operators in the field of cryptography. As mostly tampering of data occurs in the network, the messages should be protected when it is transmitted through any network. This paper introduces a new encryption technique where the genetic operators 'crossover' and 'mutation' are used to encrypt messages, so as to protect the data during transmission. The goal is to provide a better encryption technique which is difficult for cryptanalysis.

Keywords: Genetic Algorithm, Crossover, Mutation, Encryption, Decryption, Secret key, Cryptography.

1. INTRODUCTION

Process of encrypting data in-order to restrict the access of data to only authorized person is referred to as cryptography. Cryptography offers efficient solution to protect sensitive information including personal data security, internet security, military communication security, etc.

1.1 Types of Cryptography:

1.1.1 Symmetric key cryptography: In this type, the sender and the receiver use the same key for encryption and decryption and hence the key is shared between them [1][2].

Example: DES (Data Encryption Standard) and AES (Advanced Encryption Standard).

1.1.2 Asymmetric key cryptography: The technique is also known as public key cryptography. In this type, the sender and the receiver use different keys for encryption and decryption and hence the key is not shared between them [1][2]. Example: RSA (Ron Rivest, Adi Shamir and Leonard Adleman).

1.2 Genetic Algorithm

Genetic algorithm [3] is a heuristic search method based on the theory of natural selection. Generally, genetic algorithms have five steps which contain three basic operators: population generation, crossover, and mutation.

1.2.1 Population generation: Genetic Algorithms (GA), usually, starts with the process of population generation. The chromosomes are represented in either binary or hex.

1.2.2 Crossover: Process of obtaining parent solution (new generation) by applying the crossover operator on individuals of the existing generation. The new generation is always more fit than the parent generation.

1.2.3 Mutation: It is the important process of genetic algorithm as it brings genetic diversity in the species. A mutation operator is used to perform the process of mutation.

- *Amritha Thekkumbadan Veetil*
  M Tech, Computer science
  Invertis University, Bareilly
  Uttar Pradesh, India.

2. RELATED WORK

Many works have already been done in the field of cryptography using genetic algorithm. In 2012, Ankita garwal proposed an encryption method, where genetic algorithm based secret key image encryption using genetic operator is discussed [4]. After two years, in 2014, Sindhuja K and Pramela Devi S, have proposed method to encrypt data using right shift, matrix addition, modulo operation and genetic operations [5].

3. PROPOSED WORK

Proposed encryption and decryption methods are summarized as follows:

Encryption Steps

Step 1: Consider the message to be encrypted as 'THIS'.

Step 2: Calculate the numeric value of the first alphabet (the position in which it reside in the alphabetic sequence). The numeric value of 'T' is 20.

Step 3: Convert 20 to binary.
Binary of 20 is 10100

Step 4: Select a default (any randomly generated) chromosome as the second parent for crossover. I have taken the default chromosome as 11111,

Step 5: A crossover point is randomly selected and crossover is performed. Here the crossover point is selected as 2. The crossover is performed as follows:

Parent 1

Parent 2

COP = 2

New Child

Step 6: Two values are obtained from the above step. New child – 10111 Left out value – 11100 (this value is used during decryption). Decimal representation of the left out value is 28.

Step 7: A mutation point is randomly selected and mutation is performed to invert any particular bit of the chromosome. Here the mutation point is selected as 4.

Step 8: Now 'T' is represented as '10101'. Convert this binary value to decimal, which is '21'. Convert the number to alphabet. The alphabet corresponding to 21 is 'U'. Thus 'T' will be replaced by 'U'. Note: If any decimal value crosses 26, then we can repeat the alphabets and can represent the alphabets with a '*'. For example if the decimal value obtained is 28, then we can represent it in alphabets as B*. During encryption, for every word the default chromosome, crossover point and the mutation point varies. The cipher text corresponding to 'THIS' is {U28,M24,M25,U27}. For decryption the cipher text along with 3124 is send to the receiver, where 31 is the decimal representation of the second parent (11111), 3 is the crossover point and 4 is the mutation point.

Decryption Steps:
The receiver receives the cipher text {U28,M24,M25,U27 along with 3124.

Step 1: Take the first letter U28. Convert both U (decimal value 21) and 28 to binary.
U - 10101
28 – 11100

Step 2: From 3124, it's known that '4' is the mutation point, so invert the fourth bit in U.

U

Bit inverted

Step 3: Decrypt the crossover operation. From 3124, it's known that crossover point is '2'.

28(value associated with U)

Pair the similar shaded bits.
10100
11111

Step 4: Convert both the binary values to decimal.
10100 - 20
11111 – 31

The alphabetic value corresponding to 20 is 'T'. This is the first letter of the plain text. From '3124' it's already known that '31' is the default parent. The value obtained from reverse crossover matches with the value of default parent in '3124', thus providing verification.

4. CONCLUSION

The method proposed in this paper is simple and easy to implement in cryptographic system. Crossover and mutation operators of genetic algorithm are used for encryption which provides high security to the transmitted data. Frequent binary and decimal conversions increases strength of the method. As a future work this method can be implemented to encrypt images.

REFERECES

[1] Behrouz A. Forouzan , "Cryptography & Network security", Tata McGraw – Hill, 2007.

[2] William Stallings,"Cryptography and Network Security", 3rd Edition.

[3] S., N. Sivanandan, S. N. Deepa, "Introduction to Genetic Algorithm",Springer Verlag Berlin Heidelberg, 2008.

[4] 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.

[5] 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).