Chapter 42
A Novel Ammonic Conversion Algorithm for Securing Data in DNA Using Parabolic Encryption

Shipra Jain
Ambedkar Institute of Advanced Communication Technologies & Research, India

Vishal Bhatnagar
Ambedkar Institute of Advanced Communication Technologies & Research, India

ABSTRACT

In today's era, the traditional cryptographic methods are not sufficient to provide security to the data. Everyone wants to secure their data whether the data is bank transaction, email transaction, personal data or the data related to work. To provide security to the data, DNA cryptography emerges as a new field. DNA cryptography is a new branch of cryptography. It provides security to the data by converting the data in the form of DNA sequence. A lot of research has been done in the area of this cryptography. It consists of various stages like converting data in the form of DNA, reverse conversion, various methods of encryption etc. Various methods of encryption are present until now in the DNA cryptography. But the problem with them is that they all have more emphasis on biological encryption methods. There is a need of methods which make use of simple biological methods and complex binary or other number system encryption. In this paper, the authors are proposing a new algorithm for providing security to the data at two levels. The authors propose a parabolic transposition in a circular arrangement of data. In the proposed algorithm, data is arranged in a circular way. The number of rows and columns acts as a key for binary encryption. For encrypting the DNA sequence, the authors convert the DNA sequence into amino acid. This amino acid sequence will act as a cipher text and send to the receiver through the open environment. The proposed algorithm is a type of block cipher. It is a transposition cipher. It changes the position of data for binary encryption.

DOI: 10.4018/978-1-5225-5634-3.ch042

1. INTRODUCTION

With the increasing amount of data and computational power, traditional cryptography does not satisfy the need of security. The security of data is a matter of great concern in today's generation. The speed of computers is too fast. They can process gigabytes of data in a moment. The number of attacks is increasing exponentially with the help of such fast computers. Traditional cryptography does not provide security to the highest level to secure the data. A new science is needed to protect the data from the new and dangerous attacks. DNA cryptography emerges as a new and promising field in the area of information security. It provides security of the data by converting it in the form of DNA sequence. It is a combination of two domains. It combines the process of computer domain and biological domain. DNA cryptography has the advantage of large storage capacity of DNA. A 1gm of DNA can store 10^6 TB of data. This large storage capacity provides a wide scope in this field. It encrypts the data in the form of DNA nucleotides. A large number of methods have been proposed in this field till now. But most of methods are depends upon the biological functions of DNA. The implementation of these methods requires the establishment of laboratories. The cost of these laboratories is very large. It becomes very expensive to establish the laboratories and encrypt the information. So here, the motive of authors is to propose a new method which is a combination of both. The proposed method uses the biological process which can be implemented by computer tools. In this paper, the authors present a new algorithm for encrypting any type of data. The data may be a video file, an audio file, an image file or a text file. The authors propose a new way for encrypting the binary data. Then convert the binary data into DNA sequence. After this, the DNA sequence is converted into the amino acid. This amino acid is send to the receiver through the open channel. The authors propose a new method of transposition here. The author chooses the parabolic transposition in a circular way. In simple, authors improve the encryption process by making the parabolic transposition in circular arrangement. Till now, all encryption methods encrypt the data in a matrix arrangement or in simple row arrangement. No method encrypts the data in circular arrangement. By doing the transposition in circular arrangement and arranging data in the variable number of rows and columns increases the level of security. It makes use of key. Here, key will give the number of rows and columns in such a way that the resulting arrangement will have 64 blocks. The key will be different for everyone and it will increases the level of security.

The following paper is divided into 5 sections. First section will explain the DNA and DNA cryptography, its branches. Second section consists of literature review. This section explains the work done in this field till now. Third section contains the proposed algorithm. Fourth section demonstrates the example to show the working of proposed algorithm. The last section concludes the paper.

2. DNA CRYPTOGRAPHY

For understanding the DNA cryptography, the researcher must know about the DNA. DNA stands for Deoxyribo nucleic acid. It is the basic genetic element of every living organism whether it is a small organism or a human being. It is a blueprint of living organism. It is unique for everyone. It consists of four nucleotides i.e. adenine (A), thymine (T), cytosine (C) and guanine (G). DNA forms the double helical complementary structure. This structure was identified by James Watson and Francis Crick (Watson et.al., 1953).

Related Content

Managing Tacit Knowledge to Improve Software Processes

Alberto Heredia, Javier García-Guzmán, Fuensanta Medina-Domínguezand Arturo Mora-Soto (2018). *Computer Systems and Software Engineering: Concepts, Methodologies, Tools, and Applications (pp. 1567-1585).*

www.irma-international.org/chapter/managing-tacit-knowledge-to-improve-software-processes/192936

Mobile Cloud Computing Security Frameworks: A Review

Anita Dashti (2018). *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications (pp. 501-520).*

www.irma-international.org/chapter/mobile-cloud-computing-security-frameworks/203521

Quantitative Reasoning About Dependability in Event-B : Probabilistic Model Checking Approach

Anton Tarasyuk, Elena Troubitsynaand Linas Laibinis (2012). *Dependability and Computer Engineering: Concepts for Software-Intensive Systems (pp. 459-472).*

www.irma-international.org/chapter/quantitative-reasoning-dependability-event/55339

A Proposed Pragmatic Software Development Process Model

Sanjay Misra, M. Omorodion, Amit Mishraand Luis Fernandez (2018). *Computer Systems and Software Engineering: Concepts, Methodologies, Tools, and Applications (pp. 607-622).*

www.irma-international.org/chapter/a-proposed-pragmatic-software-development-process-model/192895

Series of Aggregation Operators for Picture Fuzzy Environments and Their Applications: Aggregation Operators for Picture Fuzzy Sets

Saleem Abdullahand Shahzaib Ashraf (2020). *Handbook of Research on Emerging Applications of Fuzzy Algebraic Structures (pp. 328-351).*

www.irma-international.org/chapter/series-of-aggregation-operators-for-picture-fuzzy-environments-and-their-applications/247661