Chapter 19
A Comparative Study on DNA-Based Cryptosystem

Thangavel M
Thiagarajar College of Engineering, India

Varalakshmi P
Madras Institute of Technology, India

Sindhuja R
Thiagarajar College of Engineering, India

ABSTRACT

Information security plays a vital role in almost every application that we handle in our day-to-day life since the communication needs to be protected in terms of the messages that we send and receive. Thus, cryptography the science of encoding the secret information provides security from being known by the unintended receivers. It ensured confidentiality, integrity, and authentication of messages. To simplify the methodology of traditional cryptography with the usage of genetic concepts lead to the field of DNA cryptography. This chapter gives an insight on various methods so far proposed related to DNA cryptography that involves the characteristics of DNA incorporating the traditional cryptographic techniques and a detailed comparison of these techniques thereby proposing the requirements for an efficient DNA-based cryptographic system. These techniques also include the area of steganography that conceals the message within a cover or a career media to eschew the attacks from the intruders.

INTRODUCTION

In this era, every piece of information that is communicated needs a security measure. It is quite challenging to provide security to the big data that dynamically evolves at a faster pace. To overcome these challenges, the traditional cryptographic techniques provided security by encoding the messages transferred from the sender to the receiver and the receiver used to decode the encoded message to view the original message. Those techniques were commonly classified as public key encryption or asymmetric encryption and private key encryption or symmetric encryption. These approaches increased the time

DOI: 10.4018/978-1-5225-1785-6.ch019

and space complexity. In certain cases the intruders were able to compromise the system to view the original message. It resulted with the concept that, increase in complexity increased the security.

To provide an alternative approach towards less complexity in order to gain high level of security became the goal of DNA cryptography. The major part of DNA cryptography was based on the prominent nature of the DNA molecules. Leonard Adleman used the DNA molecules to solve the NP-Complete problem in 1994, which lead to the remarkable innovations in DNA computing, the backbone of DNA cryptography that inherits the properties of DNA to design the cryptographic techniques.

DNA is a deoxyribonucleic acid made up of two strands comprising the four nucleotide bases namely Adenine (A), Thymine (T), Cytosine (C), and Guanine (G) (Doublehelix 2016). DNA acts as a carrier of the genetic information in the living organisms. So, these DNA molecules were incorporated to carry the encrypted information in it for secure data transfer.

By the concept of Watson and Crick, these nucleotides form the complementary pairs such as Adenine pairs with Thymine (A-T) and Cytosine pairs with Guanine (C-G). This concept is almost included in every technique that includes both biological and arithmetic operations. The biological operation involves like Polymerase Chain Reaction (PCR), hybridization, and transcription (Flashcards, 2016) whereas the arithmetic operation involves XOR, insertion, substitution, complement and generation of random functions. The various works in DNA cryptography dealt with laboratory processes such as DNA synthesis, generation of probes, using of fluorophores, PCR amplification and DNA chips.

These processes provide utmost security but at the same time it relies on biological equipments and so the DNA cryptographic approach has to be computable with minimum biological resources that must be easily available for anyone to encrypt and decrypt their information. At the same time it should serve security needs by maintaining computational complexity and time complexity. Thus, the reliability and security of the information is to be enhanced efficiently with reduced complexity in the system.

The DNA cryptography has a wider scope to provide data confidentiality in real time applications that handle large amount of data for its operations. The several algorithms that have been proposed in different ways to achieve better security and data confidentiality have also been proved by various experimental results. These experimental results are of both theoretical and practical implementations that support the novel ideas of the proposed work. All these dimensions of the different works are analyzed and are studied in this following chapter.

BACKGROUND

Until today, there are so many DNA cryptosystems proposed either as an algorithmic approach or implemented as a part of an application to provide data confidentiality to the application data. Among algorithmic approach there are very few authors who incorporate both the biological and arithmetic operations to satisfy the optimality of the system (Hussain, 2015). Other than that, DNA cryptosystems are used for providing layered security in applications that also includes other cryptographic algorithms like traditional cryptosystems (Raju, 2015).