Chapter 37
DNA Cryptography

Pradipta Roy
West Bengal University of Technology, India

Debarati Dey
West Bengal University of Technology, India

Debashis De
West Bengal University of Technology, India

Swati Sinha
University of Calcutta, India

ABSTRACT

In today's world, sensitive information like secret message, financial transaction, medical report, personal information is transferred over public communication channel. Since the advancement of communication begins, data security becomes a massive problem. The increasing rate of eavesdropping over communication channel leads the introduction of cryptography algorithm for data transmission. Different traditional cryptographic technique is adopted worldwide for protected data transmission. The recent advancement on this field is DNA based cryptography. This chapter describes the application of DNA as computational tool after the exposure of its capability was discovered by Leonard M. Adleman in 1994. Its random nature also helps the cryptography algorithm to become unbreakable. Conventional cryptography methods are sometimes susceptible to attack by the intruder. Therefore the idea of using codon based DNA as a computational tool is used in this cryptography method as an alternative method that fetches new hope in communication technology.

INTRODUCTION

Learning new technologies for secure data transmission has very essential implication to us. Technology regularly looks for novel ways of maintaining and resting declare to information. Over number of years, DNA computing has confirmed its efficiency as a programming method for the training set that controls and develops life. Its efficiency and tendency for fixing complicated, extremely related computational problems are also been confirmed. The capability to cover up, watermark, and explanatory information in this method is visibly significant.

DOI: 10.4018/978-1-5225-5634-3.ch037

Nowadays, genetics and molecular biology are intensely investigated areas with significant quantities of intangible property. Educational and professional organizations may experience more relaxed performing many years expensive research to identify and recombine that gene accountable for some important compound, if there was a handful of path to include an impressive work to determine their participation and declare the performance. The characteristics of DNA are of this kind that, once the actual perform of identifying and determining is done, duplicating is simple.

Furthermore, it is established the DNA has important computational energy to execute billions of similar functions. This area is still in developing phases but DNA processing is already being paid a lot of attention, not only for uniqueness of the complete factor, except in theory, it does factors in days or hours that the present electronic computer systems cannot do in a life-time. There is already a lot of interest to watermarking electronic circuits and alternatives created by electronic computer systems. It appears helpful to regard as the same types of factors with respect to DNA.

DNA computing is basically a programming method. Just similar to a RAM or hard drive, DNA lengths contain details which can be considered and duplicated. On the other hand, DNA contains a series of four nucleic acids, such as, Adenine (A), Thymine (T), Cytosine (C) and Guanine (G) rather than a binary reflection of ones and zeroes, which are allocated for individual knowing. These four nucleotides are used to scribe binary details. Ongoing the example, concealing a key concept in a binary series can be achieved by including the concept and improving the dimension the series as a whole, and by changing some section wisely so that the information is not changed perceptibly or functionally. To include this type of concept, no one will randomly add or intersperse details. It needs a finish knowing of the unique concept and the equipment that procedures it. In the same way, one would not thoughtlessly modify a series of nucleotides basically to accomplish a hiding mechanism.

As we know that, over the years, DNA has established its competence as a programming tool since Leonard M. Adleman's experiment on DNA computing reveals (Adleman, 1994). After Adleman's experiment in 1994, a new path has been opened in research. Moreover, the advancement of molecular biology and genetics in research pathways helps to adopt DNA as a computing tool (Adleman, 1994). Adleman got this concept from the book "Molecular Biology of the Gene" written solely by Dr. James D. Watson, who was the sole author for the first three editions of the book. The second edition was published in 1970 (Watson, 1970). Dr. Watson and Francis Crick invented DNA's double helical configuration in 1953, which is known as Watson-Crick Model (Watson & Crick, 1953). Based on this model Adleman got the idea and he later solved Hamiltonian Directed Path Problem (HDPP) with seven nodes. Still now Adleman's experiment is the landmark in the area DNA computing. After rigorous investigation and testing DNA is established as an important computing tool in today's world. A new section of technological innovation has been introduced with the growth of DNA processing. Educational and professional organizations may feel more relaxed of expensive research to identify and recombine the accountability of gene for various important compounds, if there was a number of a technique to include a considerable work for determining their participation. Therefore, the cryptographic method has also changed from its traditional approach to DNA based approach. It is already proved that with its modest energy and area the DNA consumes huge computational power that capable to execute billions of similar functions. Though it is still in developing phase, but DNA processing is already receiving huge importance, for its uniqueness of the entire factor, and in theory, it does factors in days or hours that the present electronic computer systems cannot do in a life-time. Nowadays, cryptography plays