Chapter 24
A Bio-Inspired Algorithm for Symmetric Encryption

Kadda Benyahia
Laboratory Technology of Communication, University of Tahar Moulay, Saida, Algeria

Meftah Mustapha
Department of Electronic, University of Science and Technology of Oran, Algeria

Latreche Abdelkrim
University of Saida, Algeria

ABSTRACT

The exploits of the structure of the DNA to realize the cryptographic systems is a new direction. The security of data transfer is an important factor for data transmission. Cryptography is one of the methods that ensures this constraint by techniques for sending data confidentially. Harnessing the benefits of DNA to secure information content makes cryptography more efficient. In this article, the authors propose a symmetric cryptography system based on DNA called Stegano-DNA- which operates under two main modules: scrambling and encryption. In its scrambling phase, Stegano-DNA eliminates the logical order of the letters in the clear text by the use of boxes of substitutions, and in its encryption phase, looks for the short sequence DNA in the chromosome sequence and memorizes only the number of positions needed to optimize the encryption time than when memorizing all positions.

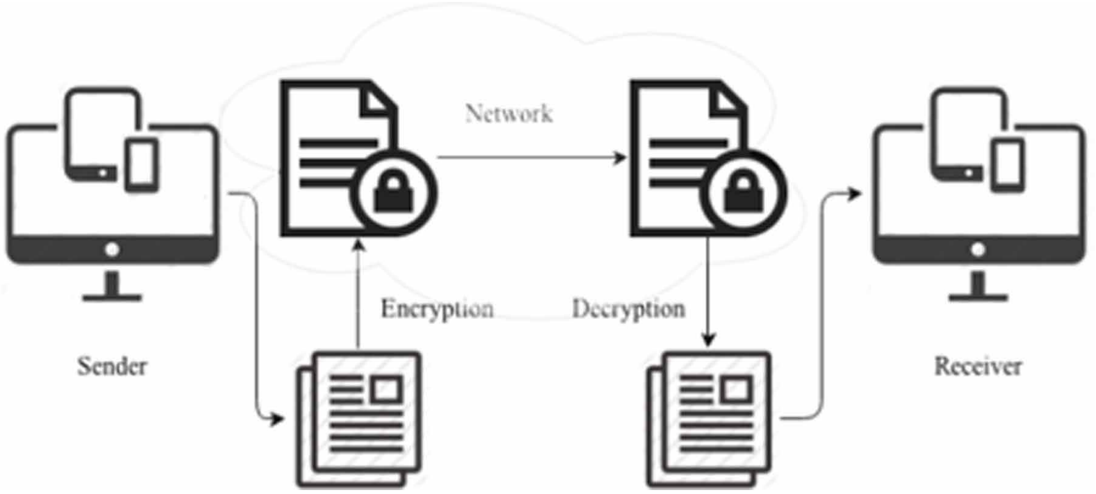
1.INTRODUCTION

Cryptology, etymologically the science of secrecy, encompasses cryptography, the art of hidden writing, and cryptanalysis whose goal is to attack cryptographic methods (Phan & Pointcheval,2005), it has become a separate science that precisely integrates mathematics, computer science and other sciences. Figure 1 represents the cryptographic process that encompasses two main phases encryption and decryption.

Recently, a new line of research in cryptography has emerged. It exploits the structure of the DNA to realize the cryptographic systems It is the cryptography with the DNA.

DOI: 10.4018/978-1-7998-7705-9.ch024

Figure 1. Process of cryptography (Bhatia & Sumbaly, 2014)



The DNA

DNA, or deoxyribonucleic acid, is the hereditary material in humans and almost all other organisms. The information in DNA like in Figure 2 is stored in a code made of four chemical bases: adenine (A), guanine (G), cytosine (C), and thymine (T).

DNA cryptography (DNA cryptography) is a new research focus in bio-inspired cryptography. Due to its large storage capacity and massive parallelism in computing, DNA can be very useful in cryptography.

2.STATE OF THE ART

Advanced algorithms and methods of security and confidentiality are proposed in different axes, Cloud Bioinformatics (Chang, 2014), smart IoT-based healthcare (Yang et al., 2019), cloud-of-things environments (Sohal et al., 2018) and quantum attack (Yang et al., 2017), whose goal is to ensure the objectives of security: integrity, confidentiality, availability, non-repudiation, and authentication.

Cryptography by DNA is one of these advanced methods. There are different techniques of cryptography DNA that has been developed. In 1994, Adleman (Adleman, 1994) laid the foundation of DNA informatics by providing solutions to combinatorial problems using molecular computation using some Standard Enzym (Rozenberg & Salomaa, 2006). This work was extended by Lipton (1995) by solving another NP-complete problem called "satisfaction" by using DNA molecules in a test tube to encode the graph for 2-bit numbers.

Lipton (1996) exploited the work of Adelman and Lipton to break one of the symmetric key algorithms used for cryptographic purposes known as DES (Data Encryption Standard). They performed biological operations on the DNA strands, they broke DES in just 4 months.

Based on the work of Adelman, in 1997 Ouyanag et al. (1997) showed the effectiveness of DNA by generating solutions of NP-complete problems. DNA cryptographic approach based on the "one-time-pad" molecular theory and performed the encryption / decryption of the 2D image is developed by Chen (2003).