International Journal of Organizational and Collective Intelligence
Volume 10 • Issue 1 • January-March 2020

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.

KEYWORDS

Bio-Inspired, Cryptography, Decryption, DNA, Encryption, Security

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.

The DNA

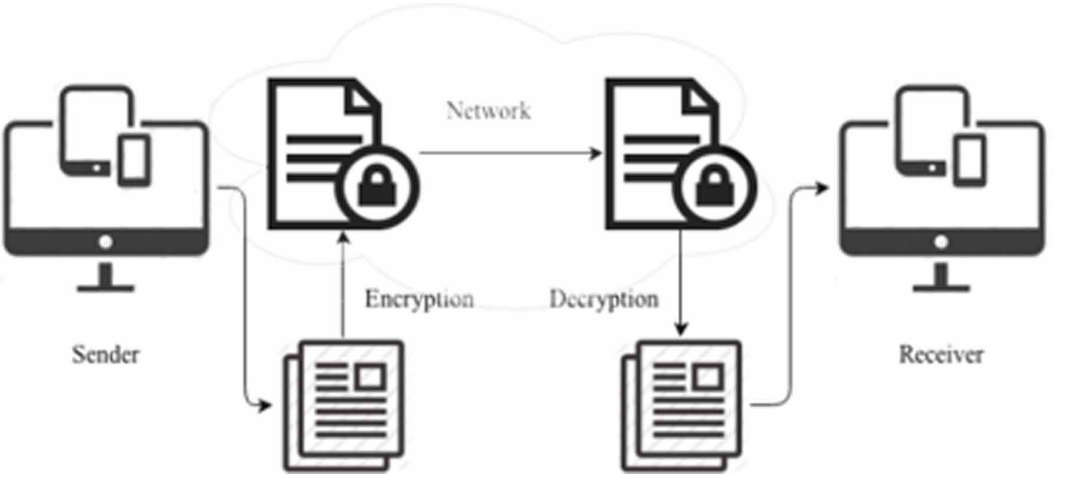
DNA, or deoxyribonucleic acid, is the hereditary material in humans and almost all other organisms. The information in DNA like in Figure 2 is stored in a code made of four chemical bases: adenine (A), guanine (G), cytosine (C), and thymine (T).

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.

DOI: 10.4018/IJOCI.2020010101

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

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



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).

Gibert et al. (2004) laid the foundation for the DNA cryptography basics using the molecular approach and the one-time-pad concept. They proposed an encryption and decryption method that relies on a DNA chip and one -time pad. It is therefore very difficult for the adversary to obtain the encrypted message, this approach is followed by a public key based cryptographic system (one way) by Tanaka et al. (2005).

Amin et al. (2006) proposed a symmetric key based cryptographic DNA approach, where key sequences are obtained from the genetic database.

In 2008, Verma et al. (2008) proposed a new paradigm for secure routing in ad hoc mobile networks (Manet) that uses the pseudo-DNA cryptography approach to secure networks. ad hoc. By transforming the message into a DNA format then it goes through an mRNA transcription phase that will be translated into proteins (translation) which is the result of encryption. This encrypted Text is sent through a secure channel to the recipient and a symmetric key with one-time pad is used at the endpoints (encryption and decryption).

11 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/a-bio-inspired-algorithm-for-symmetric-encryption/243675

Related Content

Applications in Multiobjective, Constrained and Minimax Problems
E. Parsopoulos Konstantinosand N. Vrahatis Michael (2010). *Particle Swarm Optimization and Intelligence: Advances and Applications (pp. 245-268).*
www.irma-international.org/chapter/applications-multiobjective-constrained-minimax-problems/40638

Feature Ranking Computation Algorithm
Boris Igelnik (2012). *International Journal of Organizational and Collective Intelligence (pp. 1-21).*
www.irma-international.org/article/feature-ranking-computation-algorithm/100000

Design of Multi-Criteria PI Controller Using Particle Swarm Optimization for Multiple UAVs Close Formation
Xiangyin Zhang, Haibin Duan, Shan Shaoand Yunhui Wang (2012). *Innovations and Developments of Swarm Intelligence Applications (pp. 99-113).*
www.irma-international.org/chapter/design-multi-criteria-controller-using/65808

COVID-19: New Order for Employment Relations and Human Resource Management
Kabiru Ishola Genty, Foluso I. Jayeoba, Mike O. Aremo, Tinuke M. Fapohundaand Rafiu A. Bankole (2021). *Handbook of Research on Using Global Collective Intelligence and Creativity to Solve Wicked Problems (pp. 454-475).*
www.irma-international.org/chapter/covid-19/266795

Minimum Span Frequency Assignment Based on a Multiagent Evolutionary Algorithm
Jing Liu, Jinshu Li, Weicai Zhong, Li Zhangand Ruochen Liu (2011). *International Journal of Swarm Intelligence Research (pp. 29-42).*
www.irma-international.org/article/minimum-span-frequency-assignment-based/60161