MEDWIN PUBLISHERS
Committed to create value for Researchers

Bioinformatics & Proteomics Open Access Journal

DNA Cryptography an Area of DNA Computing

Senapati KK*

Department of Computer Science and Engineering, Birla Institute of Technology, MESRA, India

Editorial

Volume 1 Issue 1

Received Date: September 12, 2017

Published Date: September 26, 2017

***Corresponding author:** Kishore Kumar Senapati, Assistant Professor, Department of Computer Science and Engineering Birla Institute of Technology, MESRA, Ranchi, Jharkhand, India Tel: 09431768348; Email: kksenapati@bitmesra.ac.in

Editorial

The coming era of research will totally have to be depended on the advancement of bioinformatics. Bioinformatics will be a driving force for the industry and young researcher in coming time. I wish all the research will be go through the path of Bioinformatics. There are many dimensions of DNA computing. Out of that in one recent research dimension, scientist discovers a key to longer life in DNA. The major challenge in DNA computing is derivation of a formula for GENE structure [1]. If we know the formula for GENE structure then we can easily code it and decode also. This can be think in present perspective of human transfer from one place to another place. For any kind of transfer, you need data and a medium of transmission. So, if we know the arrangement of Genetic structure of Homo sapiens we can break them at one end and transfer through the transmission medium and reassemble at the other end. This may be flimsy in present environment but this will be possible in the coming time and the entire theory will be based on GENE structure coding. The editor also tried to use DNA for computer security purpose. Today innovative and improvised methods of information security are constantly being required to protect the data, as everyday there is some new breach that is found on the existing information systems. Some of the good cryptographic algorithms such as DES, and MD5 are broken. In the pursuit of finding new and improved mechanisms of information security DNA computing came into existence which gave birth to another relatively new field of cryptography that is DNA Cryptography [2].

The cryptography technique is to make some piece of important information unintelligible by encoding the message. The main purpose and advantage behind using the DNA molecular structure and its complex processes such as hybridization, polymerase chain reaction or others is its vast parallelism, exceptional and high energy efficiency and extraordinary storage capacity [3]. DNA cryptography is a relatively new and promising field in cryptography which emerged with the progress of DNA computing. The concept of massive parallelism and large information density inherent in DNA molecule are exploited for cryptographic purposes. Currently, the main difficulties of DNA cryptography are the requirement of high technology enabled biomolecular laboratory and computational complexity [3,4]. The research of DNA cryptography is still at its initial stage, and there are many problems yet to be solved. Though many researchers are working on this field it is far from maturity both in theory and realization. Again, on the other hand, currently DNA technology is based upon the modern biological technologies which are extensively laboratory dependent [1]. There is not any specific general theory about applying DNA molecules into cryptography.

DNA cryptography is a new born cryptography technique in which DNA is used as information carrier and the modern biological technology is used as implementation tool [5]. The vast parallelism and extra ordinary information density that are inherent in DNA molecules are explored for all sorts of cryptographic techniques. The study of DNA can be applied in DNA cryptographic systems that are based on DNA and onetime - pads, and if it is used correctly, it is virtually impossible to crack the system. The size of one-time pad depends on the cryptographic system. There are various procedures for DNA one – time - pad encryption schemes. From the cryptographic point of view, DNA is very powerful. The binding capabilities of nucleotide bases (A-T, G-C) offer the opportunity of creating self-assembly structures that are excellent means of executing computations [2]. Another advantage is that DNA has a huge storing capacity. Today one can see the

use of OTP (One Time Password) in applications being frequently used like in banking sectors, mobile applications, e-commerce platforms where transactional nature of data is involved and many other financial institutions [6]. A DNA computing algorithm based on a test message which was taken and then, it is converted to its numeric equivalent using ASCII codes which is then transformed to its binary form. This output is then converted into a single stranded DNA sequence which is then complemented using Watson Crick Complementary Rule [5]. These bases are then assigned random numbers according to a table that will be kept secret just like the key (OTP) itself. The random numbers assigned will then be transformed into its corresponding binary form and this binary sequence is gone through a process of XOR operation with the binary equivalent of the DNA OTP that will be taken randomly [7]. Since this is symmetric type of cryptography therefore the original message again will be recovered using the reverse process.DNA molecules are extensively explored for cryptographic purposes such as encryption, authentication, digital signature, and so on. Though DNA cryptography goes forward from the research of DNA computing; it is not after all a direct result of it. The DNA computing model given by Adleman [8] cannot be taken as DNA cryptography directly. In DNA computing, technology of DNA is used to solve difficult computational problems, while in DNA cryptography, different difficult biological problems are studied and it lays the secure foundation of DNA cryptosystems. The encryption process and the decryption process can be considered as computation. But not every DNA computation is involved in cryptography. DNA's great information density has great potential utility value. Their method of storage might be very effective for solving the storage problem of one-time pad. The disadvantage is that it is tedious to prepare a huge DNA OTP in which data can be easily separated and read out [6]. For both the sender and receiver, they must perform complex biological experiments, which is possible only in a well-equipped laboratory and that too is expensive to achieve [7].

However, in many regions there are legal and privacy issues and the use of DNA strands pertaining to individuals or living organisms [9]. The underlying actual chemistry involved in the process of DNA is still untapped. There is lot more in the DNA molecule apart from only PCR amplification or DNA Hybridization.DNA cryptography can be implemented by using modern biological techniques as tools and biological hard problems as main security basis to fully exert the special advantages. Encryption and decryption are procedures of data transformation which, if incorporated by mathematical methods, are easier in implementation rather than physical and chemical ones in the present day of electronic computers and the Internet. DNA cryptography can be further developed, if the advantages inherent in DNA will be fully explored, such as developing Nano scope storage based on the DNA's tiny volume, realizing fast encryption and decryption based on the vast parallelism, and using difficult biological problems then these can form the secure foundation of DNA cryptography to realize novel crypto-system which can resist the attack from quantum computers [10,11].

In the future research in DNA cryptography, the research target could lie first in security and feasibility, and secondly in storage density [2]. In fact, it is still difficult to operate the small-scale DNA directly. Scientists can somehow operate DNA with the aid of kinds of restriction enzymes but only after DNA strands are amplified due to amplification technology such as PCR [12]. Currently, the major task for DNA cryptographers is establishment of the theory foundations and to gather the practical experience. The vast parallelism, high energy efficiency and extraordinary information density inherent in DNA motivates the prospective research of DNA computing and cryptography. The current goal is to find and make the most use of the utmost potential, but the related research is at its initial stage. Sound theories must be founded for both DNA computing and cryptography. DNA Cryptography is difficult to realize and expensive in application. Experiments which require modern and advanced equipment's for biological experiments and at the same time must be readily available for everyone. I hope this analysis about DNA Computing highlights a new dimension of research in Bioinformatics. I also wish for the beginning and Journey ahead for the publishers and researchers and readers.

References

1. Anam B, Sakib K, Hossain MA, Daha KP (2010) "Review on the advancements of DNA Cryptography"

2. Kumar D, Singh D (2011) Secret data writing using DNA sequences. Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference pp: 402-405.

3. Pramanik S, Setua SK (2012) "DNA cryptography," Electrical & Computer Engineering (ICECE), 2012 7th International Conference pp: 551-554.

4. Wang X, Zhang Q (2009) "DNA computing-based cryptography," Bio-Inspired Computing, 2009. BIC-TA '09. Fourth International Conference pp: 1-3.

5. Borda M, Tornea O (2010) "DNA secret writing techniques," Communications (COMM), 2010 8th International Conference pp: 451-456.

Copyright© Senapati KK.

6. Jain S, Bhatnagar V (2014) A novel DNA sequence dictionary method for securing data in DNA using spiral approach and framework of DNA cryptography. Advances in Engineering and Technology Research (ICAETR), 2014 International Conference on, Unnao pp: 1-5.

7. Jain S, Bhatnagar V (2014) Analogy of various DNA based security algorithms using cryptography and steganography. Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on pp: 285-291.

8. Jain S, Bhatnagar V (2014) Bit based symmetric encryption method using DNA Sequence. Confluence the Next Generation Information Technology Summit (Confluence), 2014 5th International Conference on pp: 495-498.

9. Adleman ML (1994) Molecular Computation of Solutions to Combinatorial Problems. Science 266(5187): 1021-1024.

10. Roy B, Rakshit G, Singha P, Majumder A, Datta D (2011) An Improved Symmetric Key Cryptography with DNA Based Strong Cipher. Devices and Communications (ICD eCom), 2011 International Conference on pp: 1-5.

11. Ashish Gehani, LaBean Thomas, John Reif (2004) DNA-based cryptograph. Aspects of Molecular Computing, Springer Berlin Heidelberg pp: 167-188.

12. Chen Jie (2003) A DNA-based bio molecular cryptography design", Proceedings of IEEE International Symposium 3: 822.

Copyright© Senapati KK.