RESEARCH ARTICLE OPEN ACCESS

Enhancing Asymmetric Encryption using DNA Based Cryptography

Mamta Rani[1], Sandeep Jain[2], Asha[3]
Department of Computer Science and Engineering[1 &2],
Kurukshetra, and Karnal
Department of Computer Science and Application[3],
Maharshi Dayanand University, Rohtak-124001
Haryana- India

ABSTRACT
Cryptography is the most important component part of the infrastructure of communication security and computer security [8]. The most important advantage offered by most proposed models of DNA computation is the ability to handle millions of operations in parallel. The parallel processing capabilities of DNA computers can be designed to offer the potential to find tractable solutions to intractable problems which are impossible to solve by the traditional systems, as well as potentially speeding up large polynomial time problems(NP-Complete) requiring relatively few operations. This research was focused on DNA Based encryption Methods; we have used XOR encryption for providing DNA based encryption systems. We were able to create DNA Encryption method based on XOR algorithm, Most of the work can be easily import into splice and then replace mitochondria DNA using the developed method. The XOR Cipher algorithm is very fast in Encryption can encrypt a message in polynomial time, the work also show how to work on DNA of mitochondria when a given length of Encrypted DNA strand are available.

Keywords:- DNA Computing, Encryption, Decryption DNA Strands, DNA Cryptography, Biological Terms.

I. INTRODUCTION

DNA is a small molecule that encodes genetic information which is very essential for execution and growth of all organisms. DNA stands for Deoxyribo Nucleic Acid. DNA is a polymer made up of monomers called deoxyribo nucleotides [2]. Every nucleotide consists of three main parts: deoxyribose, sugar and phosphate group and a nitrogenous base. The nitrogenous bases are Adenine, Guanine, Cytosine and Thymine (“A”,”G”,”C”,”T”). DNA is formed by a double helix which is formed by base pairs attached to a sugar-phosphate backbone. DNA (Deoxyribose Nucleic Acid) computing, also known as molecular computing which is a new approach that provides parallel computation, developed by Adleman. DNA computing was designed for solving a class of difficult computational problems in which the computing time can grow exponentially with problem size (the 'NP-Complete’ or non-deterministic polynomial time complete problem). DNA computer is basically a collection of specially selected DNA strand which all together will result in the solution to some problem, depending on the nature of problem.

DNA Based Cryptography

Cryptography is a technique that deals with all the aspects of privacy, confidentiality, key exchange, authentication and non-reputation for the safe and secured communication over an unsafe channel. As stated before, DNA enables a good base to protect data and the method is called as DNA cryptography. In this method, by using one of the bases of nucleotides sequences (“A”,”T”,”C”,”G”), the plain text is encoded into the form of DNA strands. Pure DNA acquired from the biological theory can be rearranged using different unusual bases which would enable consecutive processing. DNA cryptography or the information science was born after research in the field of DNA computing field by Adleman. Many scholars from all over the world have done a large number of studies on DNA cryptography.

II. DNA ENCRYPTION

If the encrypted wants to encrypt the plaintext [8], he/she first requests to transform the plaintext by using the code rules. Next, he/she obtains the DNA sequence with its base sequence represented a special meaning and he/

she then uses the biotechnology and - according to DNA sequences - artificially synthesizes the DNA chain as the target DNA.

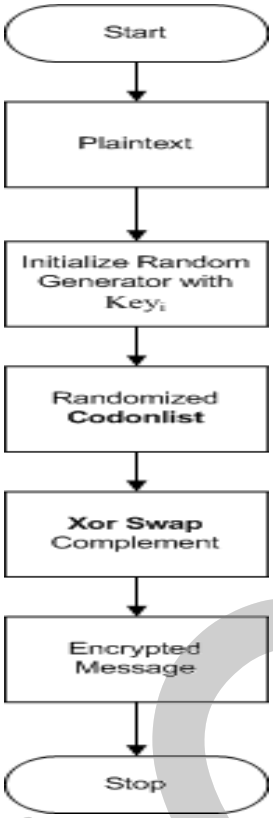

Figure 1.1: Encryption Process

After this, he/she can design the appropriate primers as the key. When the sender has the key, he/she loads them onto the target DNA for its strand and end according to the sequence synthesis primers of the primer. On this basis, we use DNA technology to see that whether it can splice into a long DNA chain. Finally, he/she adds an interfere DNA chain, namely the common DNA chain. The sequence of these chains does not contain any meaningful information. After completing the key design it begins to encrypt the plaintext and make a cipher text. It is shown above in figure1.1.

1. Explicating that which is converted into binary code;
2. Using the DNA encoding rule pre-treatment the binary code for chaos;
3. Bringing Key B into the chaotic system to produce the chaotic pseudo-random number sequence;
4. Operating the sequence and the plaintext sequence corresponding to the binary by XOR so as obtain the processed binary sequence.

III. RESULTS

i. When we first run the DNA Encrypt algorithm it asks users for the key and secret message, the screen is shown below in figure 1.2.

Figure 1.2: DNACrypt Algo. Asks for key and plaintext

ii. As user enters key and plaintext, corresponding DNA strands will generate as shown in figure 1.3.

Figure 1.3: DNA strands Of an Encrypted Message.

iii. Now DNA strands can be count and analysed with the help of bar chart as shown in figure 1.4a and 1.4 b.

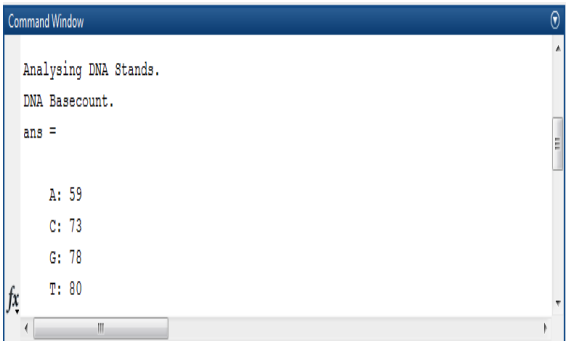

Figure 1.4(a): Analyse DNA strands Count.

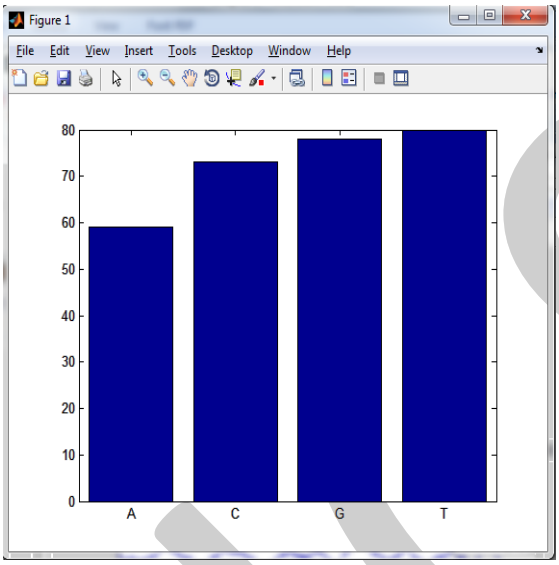

Figure 1.4(b): Bar Chart Shows DNA Strands.

Nucleotides are organic molecules that serve as the monomers, or subunits, of nucleic acids like DNA and RNA. The building blocks of nucleic acids, nucleotides are made of a various bases. Nucleotide density displays the density of nucleotides A, C, G, and T in sequence. NT density (SEQ) returns a structure of the density of nucleotides A, C, G, and T.We use NT density function to show denstity of DNA strands as shown in figure 1.5. Compared NT density of Encrypted message with mitochondria DNA, mitochondria DNA has heavy NT density. Hence the Encrypted message can be spliced over mitochondria DNA.

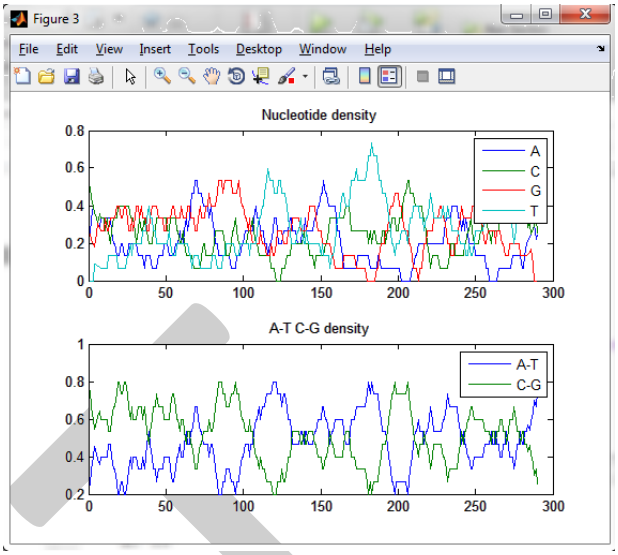

Figure 1.5 NT Density Of An Encrypted Message.

IV. CONCLUSIONS

DNA computing is a type of computational technology that uses DNA in place of the fixed silicon-based chips as in conventional computer. The main focus of DNA computing lies in the fact that DNA molecules can store huge information than any existing conventional computer chip. DNA computing use different methods for analysis purpose. The Research in this area concerns with applications of DNA computing. The most important advantage offered by most proposed models of DNA computation is the ability to handle millions of operations in parallel. The parallel processing capabilities of DNA computers can be designed to offer the potential to find tractable solutions to intractable problems which are impossible to solve by the traditional systems, as well as potentially speeding up large polynomial time problems(NP-Complete) requiring relatively few operations.

This research was focused on DNA Based encryption Methods; we have use XOR encryption for providing DNA based encryption systems. We were able to create DNA Encryption method based on XOR algorithm, Most of the work can be easily imported into splicing and then replacing mitochondria DNA using the developed technique. The XOR Cipher algorithm is very fast in Encryption. It can encrypt a message in **O (logn)** time; the work also shows how to work on DNA of mitochondria when a given length of Encrypted DNA strands are available.

V. FUTURE WORK

Mostly, today in the age of smart cards and wearable PCs find that statement laughable. We has made huge advance in efficiency since the days of room-sized computers, yet the underlying computational framework has remain the same. Today supercomputers still use the sequential logic, used by the mechanical dinosaur of the isolated past. Some researchers are now looking beyond these boundaries and investigate completely new media and computational models. With the growth of technical advancement, the threats deal by a user grows exponentially.

Hence security has become a critical issue in data storage and transmission. As traditional cryptographic system are now vulnerable to attack, the concept of using DNA Cryptography has been identified by a possible technology that brings and forward a new expect for unbreakable algorithms. This paper analyze the different approach on DNA based Cryptography.

As a medium with high information density, DNA was proposed for computational purpose by Adelman in 1994. Since the several approaches have been investigated, but little attention has been made in encryption strategies. In this research work it has been shown how to molecular encryption can be performed on the basis of DNA binary strand using XOR encryption approach for encryption. This work strengthens the fact that biotechnological method can be used for cryptography. We work on XOR based different cryptographic approach for DNA binary strand. This work show how to DNA binary strand can be used for encryption and decryption. Many problems still exist in the proposed work which leaves the window for future; we can work on following aspects in the future:

1. Apply AES, or Asymmetric Methods for Encryption process.

2. Support for Unicode Input the input messages and Key phrase.

3. DNA space complexity reduction using various methods.

REFERENCES

[1]. Grasha Jacob, "An Encryption Scheme with DNA Technology and JPEG Zigzag Coding for Secure Transmission of Images", arXiv preprint arXiv:1305.1270 May 2013.

[2]. Grasha Jacob, et. al, 2013, in "DNA based Cryptography: An Overview and Analysis", International Journal of Emerging Sciences, ISSN: 2222-4254, Page No.(36-42), March 2013.

[3]. Amish S Desai, "Xml security using DNA Technology" , International Journal of Engginering Research & Technology**, Pages(25-26), Jan 2013.**

[4]. Asha Cherian, "A Survey on different DNA Cryptographic Methods" , International Journal of Science and Research (IJSR), ISSN: 2319-7064, Vol-02 ,Issue-04, April 2013.

[5]. Komal Kumbharkar, "An improved Symmetric key cryptography with DNA based strong cipher" , international journal of advanced and innovative research, ISSN: 2278-7844,Vol-02, Issue-03,2013.

[6]. Kritika Gupta, " DNA Based Cryptographic Techniques: A Review", International Journal of Advanced Research in Computer Science and Software Engineering 3,**2013**.

[7]. Er.Ranu Soni, "Innovative field of cryptography: DNA cryptography", International Conference on Information Technology Convergence and Services,**2012**.

[8]. Yunpeng Zhang," Research on DNA Cryptography", InTech Press, Rijeka, Croatia,Page No.(**357-376**), **2012.**

[9]. Bibhash Roy, "An improved Symmetric key cryptography with DNA Based strong cipher", IEEE Explorer, ISBN: **978142449189-6**, Page No(**1-5**),Jan **24-25, 2011**.

[10].Radu Terec, "DNA Security using Symmetric and Asymmetric Cryptography", International Journal of New Computer Architectures and their Applications (IJNCAA), Page No. (**34-51**), **2011**.

[11].A. Leier, "Cryptography with DNA binary strands," Biosystems 57, Page No. (**13–22**), Jan **14**, **2000**.

[12].Louis Allamandola, "The Science Nucleobases and Their Production during the Photolysis of Astrophysically-relevant Ices", **2009**, [online

available] http://www.astrochem.org/sci/Nucleobases.php

[13]. Class 4 learning,"Travelling Salesman Problem", February 19, **2011**, [Online Available] http://class4bds.wordpress.com/2011/02/19/travelling-salesman-problem.

[14]. Simpson, R. E. "The Exclusive OR (XOR) Gate." §12.5.6 in Introductory Electronics for Scientists and Engineers, 2nd ed. Boston, MA: Allyn and Bacon, Pages No. (**550-554**), **1987**.

[15]. Adleman, L, "Molecular computation of solutions to combinatorial problem". Science 266 (5187): 1021–4. doi:10.1126/science.7973651. PMID 7973651,**1994.**