Proceedings of
National Conference on Innovative Trends in Computer Science Engineering (ITCSE-2015)
held at BRCMCET , Bahal on 4th April 2015

A Review Paper Of DNA Based Cryptographic

[1]Ritu Mor , [2]Praveen Kanth
[1]M.Tech Scholar , [2]Assistant professor
[1,2]Department of Computer Science and Engineering, BRCM ,Bahal,Haryana,India

Abstract :**DNA Cryptography is used for secure communication on a network. In DNA Cryptography change the plain text into cipher text by using Bio. molecular and One Time Pad Technologies for Encryption.DNA sequences get more powerful when combine with Nucleotide base A-T AND C-G(A- Adenine, T- Thymine ,C- Cytosine ,G-Guanine).To extract massage the DNA cipher text converted into plane text involves biological process of PCR(Polymerase Chain Reaction). Each DNA Cryptography method first convert the plane text into ASCII code and then further process start.DNA Computing has large storage capacity, massive parallelism and error prone that makes DNA Computing attractive for Cryptography application.**

Keywords :A- Adenine, T- Thymine ,C- Cytosine ,G- Guanine , ASCII Code

I.INTRODUCTION

Today, information has become very important resource and so is its security. For secure communication from sender to receiver, it is not only to encrypt message but also necessary to hide encrypted message. Many traditional mathematical algorithms have been developed for encrypting the information or data for security purposes like RSA and DES but they have limitations. DNA cryptography is also used for hiding the data, Hidden message is known by only sender and receiver. DNA encryption, on the other hand, is much more effective as it has got much more storage and computing capabilities. DNA encryption comes from DNA computing, initiated with the idea of "computing using DNA not on DNA".DNA Cryptography based on biological problems .DNA Cryptography have the power of potency and function which traditional computers cannot match. DNA computing may not be fast but it is massively parallel.

With the right kind of setup, it has the potential to solve huge mathematical problems .The biological researchers proved that DNA is similar to computer that used to transmit signals from the binary codes. DNA solved the directed HPP (Hamiltonian Path problem) with seven vertices in graph which the molecules are encoded in a sequence and the computation is performed by biochemical operations. Lipton solved another NP-complete, the satisfaction problem which can also be called as searching algorithm. Several DNA-based cryptographic techniques have been proposed. Some of these use Polymerase Chain Reaction (PCR).while others use DNA chip technology. A DNA tile assembly model has also been used for one-time pad cryptosystems

II. DNA CRYPTOGRAPHY METHODOLOGIES

DNA cryptography methodology uses different- different type of encode data. Different DNA cryptography methodology is used for secure message transmission like bio molecular, Polymerase chain reaction (PCR), chip technology, one-time-pad etc. PCR technique is a DNA Digital coding technique, in which message are converted hexadecimal code into binary code and further converted into DNA sequence, which is used in DNA template. Bio molecular technique uses parallel processing capabilities of bio molecular computation. One-time-pad technique is used to encrypt and decrypt images. We have proposed the algorithm and this is based upon a reference sequence known only to the sender and the receiver.

Types of DNA Methodologies

A)Bio Molecular Structure

- Bio molecular structure present in all living thing.
- All living organisms have unique DNA molecule to store information of different living organisms.
- Bio-molecular structure is used to encrypt and decrypt message for data transmission.
- In Bio molecular structure is most used Cryptography techniques than other techniques like Polymerase chain reaction, DNA hybridization, DNA fabrication, DNA fragment techniques.

B) **OTP (One Time Pad)**

- One-time-pad was first introduced by Vernam. It is random key generation, which is used in encryption and decryption process.
- Shanon explained key size, which was greater than or equal to plaintext. Key should be unique and not to be reused. Random code book can be used only once.
- Key shared advance by both sender and receiver.

C) **. DNA chip technology**

- To identify independent biological sample by DNA chip technology.
- Use of microscopic array of DNA technologies on solid surface to examine biochemical sample.
- DNA chip microarray utilizes the high density of molecular array to effective use.
- Two layer of security one for limitation of biotechnology other for computing security.

D) **DNA Fragmentations**

- DNA fragmentation was first represented in 1970 by Williamson. He observed fragment during initial cell death.
- DNA fragmentation is breaking of DNA strands into small and small pieces. It can be extended to future generation for better result.

E)**Polymerase chain reaction(PCR)**

- Polymerase chain reaction (PCR) is a rapid amplification technology of DNA. DNA cryptography is implemented by modern Biological techniques and biological hard problems. DNA amplification techniques include clouding.
- Polymerase chain reaction (PCR) is as molecular biology process that used to exponentially in DNA.

- The generated DNA used as template, which describe the exponential amplification.
- Finding of the target DNA under the action of the polymerase and its amplification.

III. BIOLOGICAL STUDY

DNA is Deoxyribo nucleic acid, and it is the family of molecules which is referred as nucleic acid with two strands of sugar phosphate backbone.

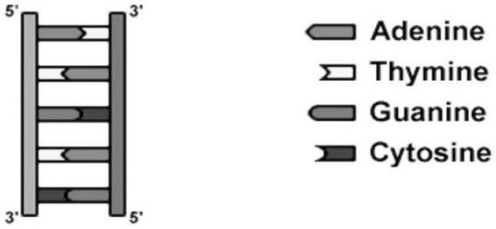
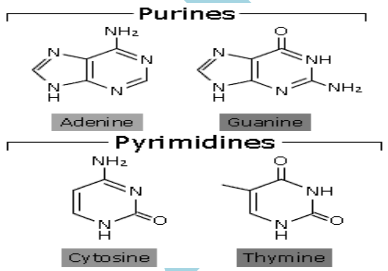


Figure 1. Combinations of Bases Forming Purines & Pyrimidines

DNA contains the genetic instruction needed to construct other cells like RNA and proteins. The complex structure of the living body consists of human parts which are the result of applying simple operations to the initial information encoded in a DNA sequence called genes. Likewise the complicated mathematical operation is made up of simple addition and subtraction .The major advantage of DNA which contains a four bases, Adenine (A), Thiamine (T), Guanine (G) and Cytosine(C).The combination of the bases results in purines (combination of Adenine and Guanine) and pyrimidines (combination of Cytosine and Thymine) as shown in figure 2 below. The two strands of a DNA molecule are anti parallel where each strand runs in an opposite direction [23].This complementarily makes DNA a unique data structure for computation and can be exploited in many ways.



The easiest way to encode is to represent these four units as four figures:

1. A(0) –00;
2. T(1) –01;
3. C(2)–10;
4. G(3)–11.

Obviously, by these encoding rules, there are 4! = 24 possible encoding methods. For DNA encoding, it is necessary to reflect the biological characteristics and pairing principles of the four nucleotides. Based on this principle, we know that:

A(0) – 00 and G(3) – 11 make pairs,

T(1) – 01 and C(2) – 10 make pairs.

In these 24 programs, there are only 8 programs

0123/CTAG,
0123/CATG,
0123/GTAC,
0123/GATC,
0123/TCGA,

Applied Cryptography and Network Security

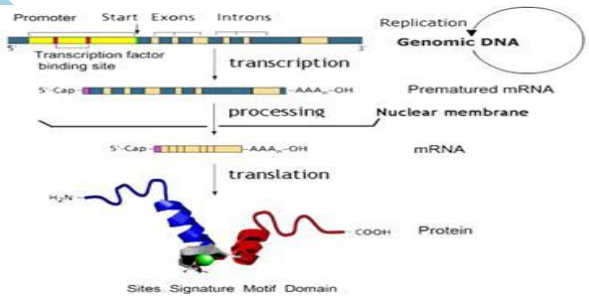
362

0123/TGCA,
0123/ACGT,

0123/AGCT match the DNA pair of a complementary principle. The coding scheme should be consistent with the weight of a molecular chain, so we get that 0123/CTAG is the best encoding scheme.

V EMERGING SCIENCE OF DNA CRYPTOGRAPHY

If DNA computing can be used to break codes, then the machinery of life can be exploited to encrypt data too .Molecular biologists have long thought of DNA as an information storage device. The body processes this information with an impressive array of computing machinery which, since the 1990s, we've exploited to carry out a few of our own calculations. DNA computing may not be fast but it is massively parallel. With the right kind of setup, it has



the potential to solve huge mathematical problems. It's hardly surprising then, that DNA computing represents a serious threat to various powerful encryption schemes such as the Data Encryption Standard (DES). But if DNA can be used to break codes then it can also be exploited to encrypt data. Various groups have suggested using the sequence of nucleotides in DNA (A for 00, C for 01, G for 10, T for 11) for just this purpose. One idea is to not even bother encrypting the information but simply burying it in the DNA so it is well hidden, a technique called DNA steganography. But that all sounds to simple for Nang King, an independent researcher who today puts forward an entirely new approach based on the way in which information from DNA is processed inside cells. The processing works in two stages called transcription and translation. In transcription, a DNA segment that constitutes a gene is converted into messenger RNA (mRNA) which floats out of the nucleus and into the body of the cell. this happens only after the non coding parts of the gene have been removed and the remaining sequences spliced back together. In translation, molecular computers called ribosome's read the information that mRNA carries and uses it to assemble amino acids into protein chains. This

is a one way process. Information can be transferred from DNA to a protein but it cannot be converted back. There reasons are various. How would this process know where to reinsert the non coding regions of DNA that were originally cut out or what these non coding sequences would have consisted of in the first place?

Nang's idea is that Alice encodes her message in the original DNA sequence and allows this to be transcribed and translated. The resulting protein is then like a public key which can be sent to Bob through a public channel. Meanwhile, Alice sends Bob the secret key which consists of the information he needs to reassemble the DNA such as the location of the non coding regions that need to be reinserted. Nang says that this form of cryptography is surprisingly secure to a number of powerful attacks. But he also points out various weaknesses such as that the encryption becomes increasingly difficult if more complex keys are used.But it piques the interest for sure. And as an additional weapon in the cryptographer's armoury, it's surely an idea worthy of further study.

LIMITATIONS

- Need of secure channel for secret key exchange.
- Too many keys.
- Origin and authenticity of message cannot be guaranteed.
- In asymmetric encryption major disadvantages are:

  Public key should be authenticated.

  Slow.

  More computer resources are required.

  Loss of private key may be irreparable.

The fundamental idea behind this encryption technique is the exploitation of DNA cryptographic strength, such as its storing capabilities and parallelism in order to enforce other

VI **CONCLUSION**

DNA Cryptography based on biochemical method to encryption or hiding the data in terms of DNA sequence. DNA algorithm based upon a reference sequence these sequence known only by sander ad receiver .This reference sequence can be select from any web site associated with DNA sequences. It is impossible to guess this sequence because there are million web sites of DNA sequences .The performance of DNA cryptography can be tested in order to prove the efficiency of an algorithm.

VII FUTURE SCOPE

DNA Cryptography is the future of information security. Its complexity and randomness provide a great uncertainty which makes encoding of data in DNA format better than other Mechanism . We can not decode the data without précis knowledge of the key. DNA Cryptography improved the security and complexity.

REFERENCES

[1] Leonard M. Adleman "Molecular Computation of solutionto combinatorial problems" Science, New Series, Vol. 266, No. 5187. pp. 1021-1024 Nov. 11, 1994

[2] Alberts, B., Bray, D., Lewis, J., Raff, M., Roberts, K. and Watson, J. D., Molecular Biology of the Cell, New York & London: Garland Publishing, 1994.

[3] R. J. Lipton," Using DNA to Solve NP-Completeproblems," Science, vol. 268, pp. 542 545, 1995

[4] J. D. Watson, F. H. C. Crick, "A structure for de oxy ribose nucleic acid", Nature, vol. 25, pp. 737-738, 1953

[5] Taylor Clelland, "Hiding messages in DNA Microdots".Nature Magazine vol.399,June 1999

[6] D. Boneh, "Breaking DES using Molecular computer", American Mathematical Society, pp 37-65, 1995

[7] Donald Nixon, "DNA and DNA Computing in Security Practices – Is the Future in Our Genes", GSEC Assignment Version 1.3, SANS Institute 2000 – 2002.

[8] William Stallings, *"Cryptography and Network Security"*, Third Edition, Prentice Hall International -2003.

[9] Guangzhou Cui "An Encryption scheme using DNATechnology",IEEE pg 37-42 ,2008

[10] A. Gehani, T. LaBean, and J. Reif, "DNA-Based Cryptography", Lecture Notes in Computer Science, Springer. 2004.

[11] Zhihua Chen. "Efficient DNA Sticker Algorithm for DES"pg 15-22.IEEE 2008.

[12] Ning Kang, A pseudo DNA cryptography Method, http://arxiv.org/abs/0903.2693 ,2009

[13] L.M Adleman "On Applying Molecular Computation to the Data Encryption Standard." Journal of Computational Biology, 6 (1). pp. 53-63. 1999 Computing,"IEEE International Workshop on Anticounterfeiting Security, , pp. 288–291, 2007

[14] G. Z. Cui, "New Direction of Data Storage: DNA Molecular Storage Technology," Computer Engineering and Applications, vol. 42, pp. 29–32, 2006.