A Survey on different DNA Cryptographic Methods

Asha Cherian[1], Surya R. Raj[2], Abey Abraham[3]

[1]Rajagiri Educational Charitable Trust – Indira Gandhi National Open University, Rajagiri School of Engineering & Technology, Rajagiri Valley, Kochi, Kerala 682039, India
ashacherian14@gmail.com

[2] Rajagiri Educational Charitable Trust – Indira Gandhi National Open University, Rajagiri School of Engineering & Technology, Rajagiri Valley, Kochi, Kerala 682039, India
surya.rraj1@gmail.com

[3]Department of Information Technology,Rajagiri School of Engineering & Technology, Rajagiri Valley, Kochi, Kerala 682039, India
abeya@rajagiritech.ac.in

Abstract: ***The relevance of information security in the modern days has increased manifold as online threats are affecting millions of users. The traditional methods of cryptography are now defenseless to attacks. The idea of DNA based Cryptography has been identified as a feasible and effective methodology to create nonintrusive algorithms. This paper provides an overview of different approaches used in DNA Cryptography.***

Keywords: DNA, Cryptography, Security, Encryption**.**

1. Introduction

The computation carried out using DNA sequences is called DNA Computing. Extensive and prolonged problems can be solved using the vast parallelism and has a huge information storage capacity [1] of DNA. Since DNA has the capability to act as a Nano processor, there is a chance that it will replace the silicon based processors. It is capable of solving a large number of mathematical or computational problems within a fraction of a second. This is done by using a DNA molecule or a group of DNA molecules as a processor.

The strands of DNA can be used to encrypt information. In this type of encryption method, the data is developed through DNA. This idea was introduced by J.D. Watson [2]. A hybrid security [1] system can be developed by combining traditional cryptography methods with DNA cryptography. The main advantage of this scheme is that, by using extended ASCII, all kinds of digital data can be encrypted.

2. Biological Background

DNA (Deoxyribo Nucleic Acid) is a nucleic acid which supports the functioning and development of all the living organisms. The genes in organisms are made up of DNA. As the DNA holds the necessary genetic information which can help to build other cells like proteins and RNA (Ribo Nucleic Acid), this can be considered as a recipe to create them. There are 4 bases in DNA which are named as Adenine(A), Thymine(T), Guanine(G) and Cytosine(C).

Hybridization: This is the formation of double stranded DNA molecules using single stranded DNA molecules. In this process Adenine always pair with Thymine while

Guanine always pair with Cytosine [2] .

Polymerase Chain Reaction (PCR): This is scheme which amplifies a single or multiple copies of a piece of DNA across several orders of magnitude to produce millions of copies of a certain DNA sequence.

Primer: It is a strand of nucleic acid that functions as a beginning point for DNA synthesis.

Transcription and Splicing: In this process, a DNA segment that constitutes a gene is read from the beginning position of the DNA segment. The non-coding areas are removed and the remaining coding areas are rejoined. The sequence is transcribed into a single stranded sequence of messenger RNA which then moves from nucleus into cytoplasm.

Translation: The mRNA sequence is translated into an arrangement of amino acids as the protein is made.

3. Survey on DNA Cryptography

Leonard M. Adleman [3] found that the bio-computational capability of DNA can be used to solve highly complex mathematical problems. He was also able to conclude that chemistry can be used to solve un-solvable problems with the help of dedicated computers. The Hamiltonian Path Problem was solved by him in which the molecules are encoded in a sequence and bio-chemical operations are used for computations. To solve the computational problems, the data is encoded in DNA strands and molecular biological tools are used to perform operations.

This paper summarizes the different DNA cryptographic methods**.**

3.1 Encryption scheme using DNA technology

Primers are used as key to encode and decode data which will result in a DNA template. The technology used in this scheme is Polymerase Chain Reaction (PCR) which is a

DNA digital coding technique [4]. Data is first converted into its corresponding Hexadecimal code and then into its Binary code. These binary digits are then converted into DNA sequence which is used as the DNA template. The forward primer [5] is used to perform the PCR. Now that the DNA sequence has been changed, it will be entirely different from the original data. To decrypt the encoded data, reverse primer is used to convert the PCR DNA sequence to the original data. This is then transformed into its corresponding Binary which is then altered to the original information. This technique has both technical and mathematical difficulties which will prevent an adversary to identify the original information.

3.2 Encryption algorithm inspired from DNA

A plain text message is transformed into a 4 x 4 matrix on which an initial permutation is performed to generate a secret key. XOR operation is performed with this generated key which is subjected to DNA module transcription (DNA to RNA) and translation (RNA to Protein). Guangzhou Cui. [4] developed this concept by the use of Symmetric key block cipher algorithm and Biological methods.

3.3 A pseudo DNA Cryptography

Based on the work of A. Gehani [6], the pseudo cryptography was developed by Ning Kang [7]. In this method, the original information is converted into a DNA sequence. This sequence is in-turn converted into two forms of DNA namely Spliced form and Protein form. For doing this, introns are cut into specific patterns. This method is not using the actual DNA sequence. Instead it use the mechanisms of DNA functions, hence the name Pseudo DNA cryptography. The principal ideas of central dogma of molecular biology such as Transcription, Translation and Splicing are used to simulate this technique**.**

3.4 Asymmetric encryption and Signature method with DNA technology

In DNA –Public Key Cryptography (PKC) [8], two types of keys are used. First key is used for encryption and decryption while the second type is used for creating signatures. The encryption of original message is encrypted using a public key. Only the owner of the private key will be able to decrypt this message. For creating a signature, the sender signs the message with the private key. Only the corresponding public key owner will be able to decrypt the encrypted message. Thus, forging can be prevented because of this method. The keys in this method are biological molecules. The security is relied on the difficult biological problems. DNA PKC is immune from Quantum computer based attacks. Since it is impossible to replicate the cypher text, cloning can be prevented**.**

3.5 Symmetric Key Crypto-system with DNA technology

This is designed using the application of advanced DNA biotechnology and micro-array in Cryptographic technologies. DNA probes are used to form the encryption and decryption keys. The cypher text is embedded in specially designed micro arrays. DNA fabrication is used for Encryption while DNA hybridization is used for Decryption. In this technique, millions of DNA probes are identified and hybridized at the same time. The decryption is done in a parallel and massive way. [9]

3.6 DNA based bimolecular cryptography design.

This is a DNA based cryptographic technique which uses the huge parallel processing capabilities of bio molecular computation. A library of one time pads is assembled secretly in the arrangement of DNA strands. Modulo 2 arithmetic operations methodology is used for encryption purpose. With the use of one time pads, a very large number of short message sequences can be encrypted. The encryption and decryption of two dimensional images can also be done using this technology. [10]

4. Conclusion

Encoding or encrypting information using DNA sequences can be performed by DNA Cryptography. This can be implemented using DNA technologies with the help of different biochemical processes. Conventionally DNA Cryptography is realized using biological implements. These DNA cryptographic methods can also be combined with other schemes for applications in various fields.

References

[1] R. J. Lipton,” Using DNA to Solve NP-Complete problems," Science, vol. 268, pp. 542 545, 1995
[2] J. D. Watson, F. H. C. Crick, “A structure for de oxy ribose nucleic acid”, Nature, vol. 25, pp. 737-738, 1953
[3] Leonard M. Adleman “Molecular Computation of solution to combinatorial problems” Science, New Series, Vol. 266,No. 5187.pp. 1021-1024 Nov. 11, 1994
[4] Guangzhou Cui “An Encryption scheme using DNA Technology”,IEEE pg 37-42 ,2008
[5] Taylor Clelland, “Hiding messages in DNA Microdots”.Nature Magazine vol.399,June 1999
[6] A. Gehani, T. LaBean, and J. Reif, “DNA-Based Cryptography”, Lecture Notes in Computer Science, Springer. 2004.
[7] Ning Kang, A pseudo DNA cryptography Method,http://arxiv.org/abs/0903.2693 ,2009
[8] LAI XueJia, LU MingXin “Asymmetric encryption and signature method with DNA technology” Vol. 53 No. 3:506–514 March 2010
[9] LU MingXin, “Symmetric Key Cryptosystem With DNA Technology” Science China pg 324-333,June 2007
[10] J Chen “A DNA-based, Bimolecular Cryptography Design”ISCAS'03.Proceedings2003

Author Profile

Asha Cherian received the BTech degree in Computer Science Engineering from Mahatma Gandhi University, Kottayam, India and currently pursuing M.Tech Degree in Information System Security.

Surya R Raj received the BTech Degree in information Technology from Kerala University in 2010 and currently doing M. Tech Degree in Information System Security.

Abey Abraham got her MTech degree from Karunya University, Coimbatore, India and is presently working as Assistant Professor at Rajagiri School of Engineering & Technology, Kochi, India.