International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

DNA CRYPTOGRAPHY

Karthiga S[1], Murugavalli E[2]

[1]*PG Scholar, Department of ECE, Thiagarajar college of Engineering, Madurai, India*
[2] *Assistant Professor, Department of ECE, Thiagarajar college of Engineering, Madurai, India*

Abstract - *As traditional encryption algorithm have severe security problems. The field of information security give importance to the new way of protecting the data. The DNA based cryptography has identified as new way of secure data in the form DNA molecules which uses DNA strands to hide the information. The main objective of DNA cryptography is to provide confidentiality when the persons sends data over a network. This paper discuss about DNA Cryptography, difference between traditional cryptography and DNA Cryptography, various works done in the field of DNA Cryptography*

Key Words: Adenine, Thymine, Guanine, Cytosine, Polymerase Chain Reaction, Primer

1. Introduction

In the digital world, data plays a vital importance in the field of business, military etc… if the data is highly sensitive and confidential it is necessary to protect the data. Different techniques has been used to keep the unauthorized uses away such as cryptography, data hiding etc… Cryptography is essential in both network and computer security. It is the art of secret writing to protect the information between two communication parties which converts plain text into cipher text so that unauthorized person cannot access the data. Traditional cryptography applies complex and mathematical procedure to secure and store the information. Due to this complex nature DNA cryptosystem emerges. DNA Cryptosystem is the new innovative approach used to encrypt the data in terms of DNA sequence.

2. DNA & DNA Cryptography:

DNA (Deoxyribonucleic Acid) is a nucleic acid is the backbone of all the living organisms. The DNA holds the necessary genetic information which can help to build other cells like proteins and RNA (Ribonucleic Acid), DNA is double helix structure in which two strands are coiled to each other and it is made of nucleotides There are 4 bases in nucleotide which are named as Adenine (A), Thymine (T), Guanine (G) and Cytosine (C) Shown in Fig-1. In DNA Cryptography base pairs forms an information carrier. DNA Cryptosystem encrypts the data in the form of A, T, C, G which is the combination of 0's and 1's such as 00-A, 01-T, 10-C 11-G.Hybridization in which double stranded DNA molecules uses single stranded DNA molecules. In this process Adenine always pair with Thymine while Guanine always pair with Cytosine. Polymerase Chain Reaction (PCR) is the process of amplifying a single or multiple copies to produce millions of copies of DNA sequence. Primer is a strand of nucleic acid that functions as a beginning point for DNA synthesis. Transcription and Splicing is the process of removing the non-coding areas and rejoining the remaining coding areas and the information of DNA is moved into mRNA. Translation in which the information of mRNA sequence is translated into amino acid which is protein made.

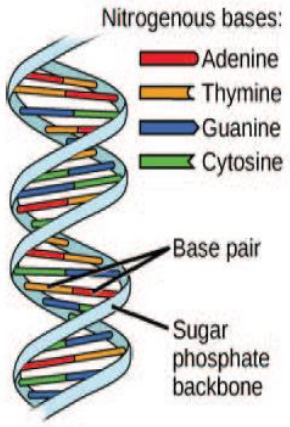

Fig -1: DNA Cryptography

3. Traditional Cryptography:

Cryptography is the technique for protecting a data. It is capable of keeping a data in secret form while saving the information in unsafe network like internet, this is done to secure the data from the adversaries and to make it understandable to the intended receiver Shown in Fig-2.

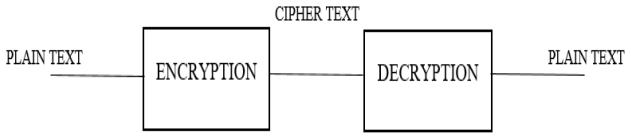

Fig -2: Traditional Cryptography

Plaintext: It is source message or information which is used as an input to the encryption process.

Encryption: An approach or method which is performed by data hiding algorithms to convert plaintext into cipher text.

Cipher text: An encrypted message which sends to the receiver using private or public channel.

Decryption: An inverse encryption process applies on cipher text at receiver end for obtaining original message.

Table -1: Comparison of Traditional Cryptography and DNA Cryptography

	SECURITY	TIME COMPLEXTIY	STORAGE MEDIUM	STORAGE CAPACITY
TRADITIONAL CRYPTOGRAPHY	ONE FOLD	FEW SECONDS	SILICON CHIPS	16 MB
DNA CRYPTOGRAPHY	TWO FOLD	FEW HOURS	DNA STRANDS	10^8TB

Table -2: Advantages and Disadvantage of different Algorithm

ALGORTHIM	ADVANTAGE	DISADVANTAGE
RSA	• Reverse process is difficult	• Quiet slow • Key generation is complex • Large number of factorization is difficult
DIFFIE HELLMAN	• Short length key	• Man in the middle attack
ELLIPTICAL CURVE CRYPTOGRAPHY	• Better security • Compute key through elliptical curve equation	• Difficult to implement
DSA	• Very fast • Secures the data from man-in-the-middle attack • Provide non-reputation and authentication	• It has short life span

4. Types of Cryptography:

There are three prominent branches or sub fields of cryptography named as:

1) Modern Cryptography
2) Quantum Cryptography
3) DNA Cryptography.

These three fields depend upon different difficult problems concerning to different disciplines for which there is no known solution until now. The modern cryptography is based upon the difficult mathematical problems such as prime factorization, elliptic curve problem, for which there is no known solution found so far. Quantum cryptography which is also relatively a new field, is based upon the Heisenberg uncertainty principle of Physics, and DNA cryptography depends upon the difficult biological processes concerning to the field of DNA technology.

Table -3: Difference between Classical and Modern Cryptography

Classical Cryptography	Modern Cryptography
• It manipulates traditional characters, i.e., letters and digits directly.	• It operates on binary bit sequences.
• It is mainly based on 'security through obscurity'. The techniques employed for coding were kept secret and only the parties involved in communication knew about them.	• It relies on publicly known mathematical algorithms for coding the information. Secrecy is obtained through a secrete key which is used as the seed for the algorithms. The computational difficulty of algorithms, absence of secret key, etc., make it impossible for an attacker to obtain the original information even if he knows the algorithm used for coding.
• It requires the entire cryptosystem for communicating confidentially.	• Modern cryptography requires parties interested in secure communication to possess the secret key only.

5. Survey on DNA Cryptography:

Adelman [1] laid the foundation of DNA computing by giving solutions to the combinatorial problems using molecular computation, one of which is "Hamiltonian path" problem. He solved the instance of graph containing seven vertices by encoding it into the molecular form by using an algorithm and then computational operations were performed with the help of some standard enzymes. This was solved by brute force method.

Lipton [2] extended the work of Adleman by solving another NP-complete problem called "satisfaction" by using DNA molecules in a test tube to encode the graph for 2 bit numbers.

Dan Boneh et al. applied the approaches of DNA computing used by Adleman and Lipton, in order to break one of the symmetric key algorithm used for cryptographic purposes known as DES (Data Encryption Standard). They performed biological operations on the DNA strands in a test tube, such as extraction, polymerization via DNA polymerase, amplification via PCR and perform operations on the DNA strands which have the encoding of binary strings. Then DES attack is planned by generating the DES-1 solution, due to which key can be easily guessed from the ciphertext and further evaluate the DES circuit, lookup table and XOR gates. By using their molecular approach they broke DES in merely 4 months[3]

Table -4: Survey on DNA Cryptography

S.NO	Algorithm Title	Problem Solved	Methodology
1	Molecular Computation of Solutions to Combinatorial Problems	Hamiltonian Path	DNA Molecular Theory.
2	DNA Solution of Hard Computational Problems	SAT	DNA Molecular Theory.
3	Breaking DES Using a Molecular Computer	DES	Molecular Computer based on DNA molecules.
4	DNA Solution of the Maximal Clique Problem	Clique Problem	DNA Molecular Theory.
5	A DNA-based, Bimolecular Cryptography Design	Symmetric key	Molecular, One-time pad.
6	Symmetric-key cryptosystem with DNA Technology	Chip Cipher Text	DNA sequence
7	Data hiding methods based upon DNA sequences	Different attacks	DNA sequence
8	data hiding method based on deoxyribonucleic acid coding	PDF file as Cipher Text	DNA sequence
9	Encryption Scheme Using DNA	Asymmetric key	DNA synthesis, DNA digital coding, PCR amplification
10	Secret Data Writing Using DNA Sequences	Symmetric key	One-time pad.
11	DNA Cryptography	Symmetric key	Hybridization, One-time pad.
12	DNA Cryptography Based on Fragment Assembly	Symmetric key	DNA Fragment assembly.
13	An encryption algorithm inspired from DNA	Different attacks	CDMB technique
14	Security and Complexity of DNA Based Cipher	Symmetric key	One-time pad, DNA Indexing.

Qi Ouyang et al. applied the approaches of DNA molecular theory in order to generate the solution for maximal clique problem, which is another NP-complete problem. Thus shows the efficiency of DNA: to solve Hard-problems and vast parallelism inherent in it which makes the operations fast.[4]

Chen et al. Proposed that hard problem can be solved by DNA computing using various DNA operations. They solved DES by using the DNA computing. [5]Chen et al.'s proposed algorithm included three functions: initial function for initialization of the key space with every possibility, Encryption process, and third is to detect right corresponding key. Algorithm referred as molecular sticker algorithm which includes enzymes, short memory strands, and tubes

MingXin et al. Introduced a symmetric-key DNA cryptosystem using the inclusion of DNA biotechnology, microarray into the cryptography technologies. In MingXin et al.'s algorithm, encryption and decryption key formed by use of DNA probes and ciphertext embedded into microarray (DNA chip). Security of algorithm based on the advancement of DNA chip.[6]

Shiu et al. Introduced three cryptographic approaches such as Insertion method, Complementary pair method, and Substitution method using the properties of DNA sequences. They showed that substitution method is better than other two approaches.

Liu et al. proposed a new data hiding approach using DNA sequence and encrypted each character of ciphertext in a word file. In Liu et al.'s algorithm, plaintext got convert into DNA sequence using DNA coding. Chebyshev maps generate two pseudorandom DNA sequence XXOR and YPrimer, and generate one time key using selected DNA sequence key. XXOR added with message DNA sequence and then YPrimer got attach with generated output. After some shift operations had applied to the previous output, they got ciphertext. This ciphertext encrypted in the word file and after conversion of word to PDF. The generated PDF sent to the receiver as final ciphertext.

Guangzhao Cui et al. proposed the public key encryption technique that uses DNA synthesis, DNA digital coding and PCR amplification to provide the security safeguard during the communication. This encryption scheme has high confidential strength.

Deepak Kumar and Shailendra Singh proposed a new secret data writing techniques based on DNA sequences. They have explained this algorithm by using a simple example of "HELLO" as a plaintext and generate a ssDNA One-time pad key of 350 bits which is 70 times longer than the plaintext and perform encryption and decryption on the plaintext using symmetric key cryptography. So to find the exact key, adversary has to search among 4310 different ssDNA strings which is almost impossible [8].

Sabari Pramanik and Sanjit Kumar Setua proposed a new parallel DNA cryptography technique using DNA molecular structure and hybridization technique which certainly minimize the time requirement. They have explained how message is exchanging safely between sender and receiver with an example.

Yunpeng Zhang et al. proposed a DNA cryptography based on DNA fragment assembly.[10] In their algorithm they have clearly mentioned how sender converts the plaintext into binary sequence and then into long chain of DNA, which is further fragmented into small DNA chains. Key of short chain

implantation takes place in the fragments and forward to the receiver as a ciphertext and then receiver deciphers it and starts fragment reassembly to obtain the plaintext.

Sadeg et al. worked on Central Dogma of Molecular Biology (CDMB) and designed an algorithm that works better than AES algorithm under various attacks. This proposed algorithm involves three phases. In the first phase, plaintext get convert into bits using the XOR operation with sub key that was generated by sub key generator. In second and third phase long sequence of bits converted into ciphertext by Transposition, CDMB, Permutation, and XOR operations.

Olga Tornea and Monica E. Borda [11] proposed a DNA based cipher which is based on DNA indexing. They take the random DNA sequence from the genetic database and use as a One-time pad key, which is send to the receiver by a secure communication channel. The encryption mechanisms takes place by converting the plaintext into its ASCII code and then converts it into the binary format which is converted into the DNA sequence (A, C, G, and T). Now DNA sequence formed is search in the key sequence and writes down the index numbers. The array of integer numbers obtained are our ciphertext which is decrypted by the receiver only using the key and index pointer.

6. Time Analysis:

Cryptographic techniques such as RSA, DES AES, Elliptical Curve Cryptography etc., are not secure enough and it also take much time for the process to take place. Due to this time complexity DNA Cryptography is emerged and time analysis of different cryptographic technique is shown in Chart-1. Elliptical Curve Cryptography technique consumes more time for both encryption and decryption when comparing with other cryptographic techniques DNA consumes less time for encryption and decryption.

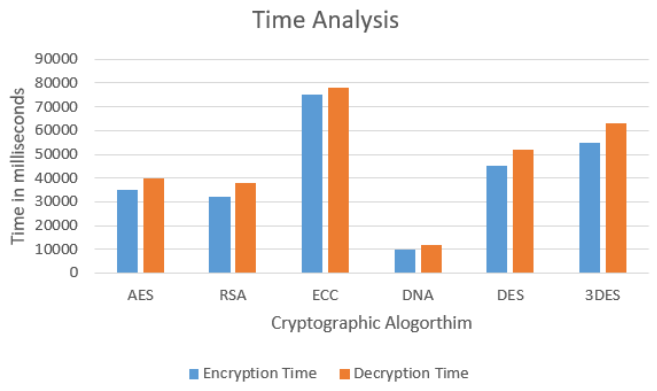

Chart -1: Time Analysis

7. Conclusion:

The world of information security is always on the pay attention to protect the data that we transmit over non secured communication. The attractiveness of these DNA research trends is found the possibility of protecting the data and it also solve many difficult problems. With the summarization of the progress of DNA cryptographic research, the advantages, future trends and several problems have also been identified. All the three kinds of cryptography have their own advantages and disadvantages and can be treated as the complement of each other in future security applications. However, the difficulties that are identified in other cryptography is overcome by DNA cryptography which can readily be implemented in the field of security.

REFERENCES

[1] Adleman. M. L (1994), Molecular Computation of Solutions to Combinatorial Problems, Science, vol. 266, pp. 1021- 1024.

[2] J. Lipton. R (1995), Using DNA to solve NP Complete problems, Science, Vol. 268, pp. 542-545.

[3] Boneh. D (1996), Breaking DES using Molecular computer, American Mathematical Society, pp 37-65.

[4] Ouyang Qi, D. Peter Kaplan, Liu Shumao and Albert Libchaber (1997), DNA solution of the maximal clique problem, Science 278, 5337, 446-449.

[5] Chen Jie (2003), A DNA-based bio molecular cryptography design, Proceedings of IEEE International Symposium, Vol. 3, pp. III-822.

[6] Lai XueJia, MingXin Lu, Lei Qin, Han JunSong, and Fang XiWen (2010),Asymmetric encryption and signature method with DNA technology, Science China Information Sciences 53, no. 3, pp. 506-514.

[7] Cui Guangzhao, Limin Qin, Yanfeng Wang, and Xuncai Zhang (2008), An encryption scheme using DNA technology, In Bio-Inspired Computing: Theories and Applications, BICTA, 3rd IEEE International Conference on, pp.37-42

[8] Deepak Kumar, and Shailendra Singh (2011), Secret data writing using DNA sequences, In Emerging Trends in Networks and Computer Communications ETNCC), IEEE International Conference on, pp. 402-405.

[9] Yunpeng Zhang, Bochen Fu, and Xianwei Zhang (2012), DNA cryptography based on DNA Fragment assembly, Information Science and Digital Content Technology (ICIDT), 8th IEEE International Conference, Vol. 1, pp. 179-182.

[10] Olga Tornea, and Borda E. Monica (2013), Security and complexity of a DNA-based cipher, In Roedunet International Conference (Roedunet), 11thEEE International Conference, pp. 1-5.

[11] G. Cui, L. Cuiling, L. Haobin, and L. Xiaoguang, "DNA computing and its application to information security field", IEEE Fifth International Conference on Natural Computation, Tianjian, China, Aug. 2009, pp. 148 - 152.

[12] G. Cui, L. Qin, Y. Wang, and X. Zhang, "An encryption scheme using DNA technology", IEEE 3rd International conference on Bio-Inspired Computing: Theories and Applications (BICTA08), Adelaid, SA, Australia, 2008, pp. 37–420.

[13] X. Guozhen, L. Mingxin, Q. Lei, and L. Xuejia, "New field of cryptography: DNA cryptography" Chinese Sience Bulletin, Springer Verlag, Germany, vol. 51, 2006, pp. 1413–1420.

[14] Noorul Hussain Ubaidur Rahman, Chithralekha, Balamurugan, Rajapandian, and Mariappan, "A Novel DNA Computing based Encryption and Decryption Algorithm", IEEE, 2015.

[15] G. Shanmuga Sundaram, S. Pavithra, A. Arthi, B. Madhu Bala and S. Mahalakshmi, "Cellular Automata based DNA Cryptography Algorithm", ISCO, IEEE, 2015.

[16] Asish Aich, Alo Sen, Satya Ranjan Dash, and Satchidananda Dehuri, "A Symmetric Key Cryptosystem using DNA Sequence with OTP Key", Springer, 2015.

[17] Ravi Gupta and Rahul Kumar Singh, "An Improved Substitution method for Data Encryption using DNA Sequence and CDMB", Springer, 2015.

[18] Samiha Marwan, Ahmed Shawish, Khaled Nagaty, "DNA-based cryptographic method for data hiding in DNA media", Elsevier,2016.

[19] Tushar Mandge, and Vijay Choudhary, "A DNA Encryption Technique Based on Matrix Manipulation and Secure key Generation Scheme", IEEE, 2013.