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

Enhancement of Security With The Help Of DNA Cryptography

[1]Ritu Mor , [2]Praveen Kanth
[1]Research Scholar , 2Assistant professor
BRCM ,Bahal,Haryana,India
[1]ritumor97@gmail.com

***Abstract*- We use Cryptography to enhances the security feature of data or information transmission. We have different type of techniques as traditional Cryptography like Substitution techniques, Transposition techniques, hashing Functions and algorithms like DES , RSA, AES, IDEA, ECCetc. Are used. DNA Cryptography new emerging technique for providing ultra scale computation , massive parallelism, information storage and energy efficient. The DNA materials are stable and long lasting.**

DNA Cryptography based on bio-molecular reaction and DNA used bio-molecular computation ability to deoxyribo nucleic acid.DNA consist of three main component like suger phosphate and base DNA encoded with four bases A(Adenine),G(Guanine),T(Thymine)and C(Cytosine) in this paper we reviewing various current cryptographic techniques.

Keywords Cryptography, DNA Techniques, DNA Capabilities ,DNA Cryptography.

1 INTRODUCTION

Now a days data and information security is critical aspects for providing security for this we use different type of cryptography .The goal is to transmit a information between sander and receiver securely. In Cryptography system plain text is a natural sequence of character for encryption we using algorithm and secrete key to convert plain text into cipher text and then decryption is reverse process to encrypted information back to original fome . For this we have different type of methodologies in DNA Cryptography like Bio-molecular structure , Polymerase chain reaction (PCR),DNA Fragmentation , DNA Chip Technology and One Time Pad (OPT)

II.BACKGROUND

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.. DNA solved the complex problem like 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. There are many desktop and web applications which uses cryptography.

III.CRYPTOGRAPHY

The field of study related to encoded information comes from Greek word .

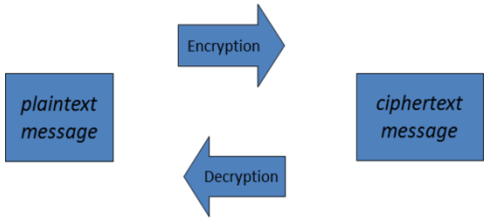


Figure 1 Cryptography

It is a mishmash of two words: (a) krypto means “hidden” and (b) grafo means to “write”. So the literal meaning of cryptography is “hidden writing”.The process of converting plaintext into ciphertext are called Encryption we can not read encrypted dataand the process of converting ciphertext into plaintextare called Decryption we can read decrypted data.

Encryption and decryption are both methods used to ensure the secure passing of messages and other sensitive documents and information.

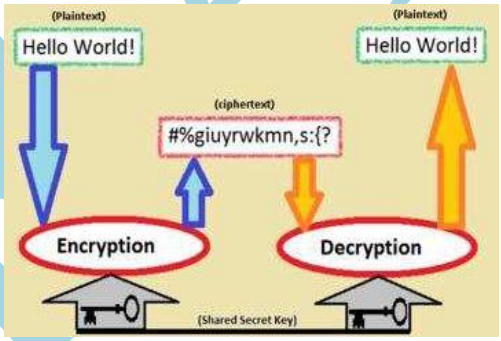


Figure 2 Structure of Cryptography with Encrypted or Decrypted data

We use different type of cryptography like Cryptographic engineering , Quantum cryptography, Multivariate cryptography , DNA cryptography, Steganography ,Visual cryptography etc.

IV.BRANCH OF CRYPTOGRAPHY

4.1 Cryptographic engineering

Cryptographic Engineering is the discipline of using cryptography to solve human problems. Cryptography is typically applied when trying to ensure data confidentiality, to authenticate people or devices, or to verify data integrity in risky environments

4.1.1 Cryptographic implementations

Hardware architectures for public-key and secret-key cryptographic algorithms

- Cryptographic processors and co-processors
- Hardware accelerators for security protocols (security processors, network processors, etc.)
- True and pseudorandom number generators
- Physically unclonable functions (PUFs)
- Efficient software implementations of cryptography for embedded processors attacks against implementations and countermeasures against these attacks
- Side channel attacks and countermeasures
- Fault attacks and countermeasures

- Hardware tamper resistance
- Hardware trojans

4.1.2 Tools and methodologies

- Computer aided cryptographic engineering
- Verification methods and tools for secure design
- Metrics for the security of embedded systems
- Secure programming techniques

4.1.3Applications

- Cryptography in wireless applications (mobile phone, WLANs, analysis of standards, etc.)
- Cryptography for pervasive computing (RFID, sensor networks, smart devices, etc.)
- FPGA design security
- Hardware IP protection and anti-counterfeiting
- Reconfigurable hardware for cryptography
- Smart card processors, systems and applications
- Security in commercial consumer applications (pay-TV, automotive, domotics, etc.)
- Secure storage devices (memories, disks, etc.)
- Technologies and hardware for content protection
- Trusted computing platforms

4.2 Quantum cryptography

Quantum cryptography describes the use of quantum mechanical effects (in particular quantum communication and quantum computation) to perform cryptographic tasks or to break cryptographic systems.

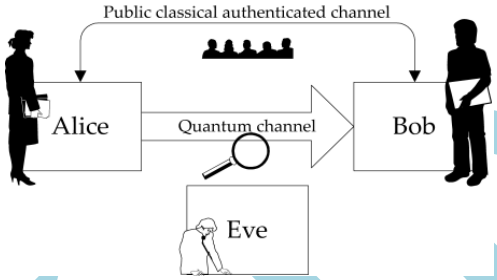


Figure 3 Quantum key distribution comprises a quantum channel and a public classical authenticated channel

Well-known examples of quantum cryptography are the use of quantum communication to exchange a key securely (quantum key distribution) and the hypothetical use of quantum computers that would allow the breaking of various popular public-key encryption and signature schemes. The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication (see below for examples). For example, quantum mechanics guarantees that measuring quantum data disturbs that data; this can be used to detect eavesdropping in quantum key distribution.

As a universal convention in quantum cryptography, Alice sends quantum states to Bob through a quantum channel. Eve is suspected of eavesdropping on the line.

4.3 Visual cryptography

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images or layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

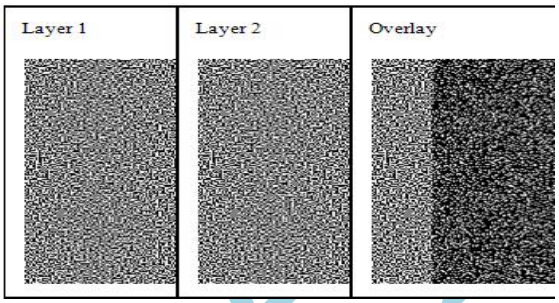


Figure 4 Visual cryptography

4.4 DNA cryptography

DNA is a polymer. The monomer units of DNA are nucleotides, and the polymer is known as a "polynucleotide". The four nucleotides are given one letter abbreviations as shorthand for the four bases. A DNA cryptographic technique in which each letter of the alphabet is converted into a different combination of the four bases A(Adenine), G(Guanine), T(Thymine) and C(Cytosine) that make up the human deoxyribonucleic acid (DNA).

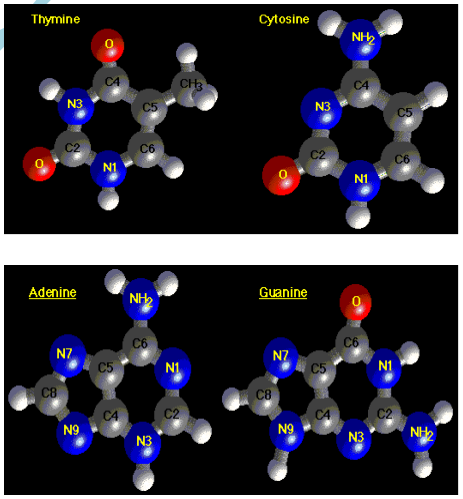


Figure 5 Structure of DNA Molecule

A piece of DNA spelling out the message to be encrypted is then synthesized, and the strand is slipped into a normal fragment of human DNA of similar length. The end result is dried out on paper and cut into small dots. As only one DNA strand in about 30 billion will contain the message, the detection of even the existence of the encrypted message is most unlikely.

The information in DNA is stored as a code made up of these four chemical bases as shown in figure 1 below. The bases

(nucleotides) are spaced every 0.34 nanometers along the DNA molecule, giving it a remarkable data density of nearly 18Mbits per inch. These nucleotides will only come together in such a way that A always pairs with T and C always pairs with G. 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 antiparallel where each strand runs in an opposite direction .This complementarily makes DNA a unique data structure for computation and can be exploited in many ways.

DNA cryptography depends upon the hard biological processes related to the field of DNA technology such as One Time Pad, Polymerase Chain Reaction (PCR) for a sequence without knowing the correct two primer pairs and another is extracting information from the DNA chip without having the knowledge about the sequences because sequences are present in different spots of DNA chip .

4.4.1 DNA Encryption And Decryption Encryption

Step1:The binary data, text or image, is used under the form of ASCII code (in decimal format).

Step2:These numbers are then grouped in blocks and encrypted in using a traditional method (eg. DES)

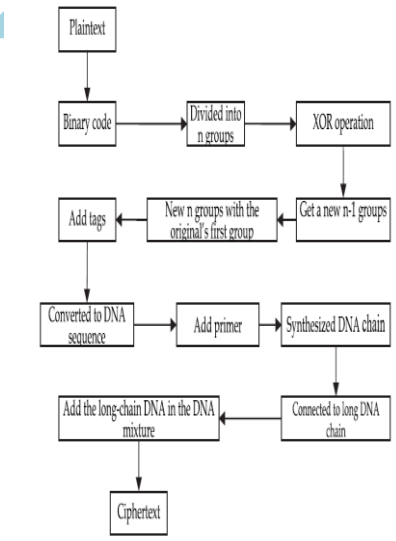
Step3:This encoded message is then changed to binary format.

Step4: Then these digits are grouped into two and substituted as A for 00, T for 01, G for 10, and C for 11.

Step5: We then fit the primers on either side of this message. Primers will act as stoppers and detectors for the message.

Step6: This message is then flanked by many sequences of DNA or by confining it to a microdot in the micro-array.

Step7: If considered as a pseudo method: this sequence is transferred to the receiver through the Internet.



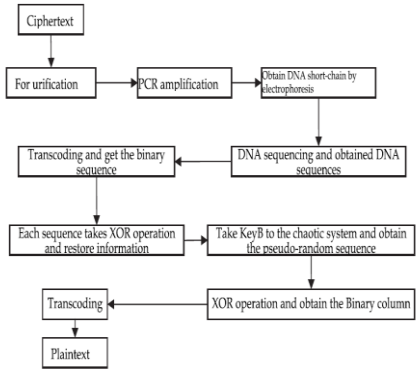
. Encryption Process

Figure 6 DNA Encryption mechanism

4.4.2 Decryption

Step-1: The Decrypter would take the DNA and run it through what's known as next-generation high-throughput sequencing (NGS).

Step-2: It analyzes and compares multiple copies of the same sequence and then uses majority-voting to check out the correct base.



4. Decryption Process

Figure 6 DNA Decryption mechanism

Step-3: Compression algorithms could be reversed to restore the raw data into its original form.

Step-4: Snap the fragments back together in correct order so that the DNA strands could be decoded back into useful data to get the correct result. Input and output of the DNA data can be moved to conventional binary storage media by DNA chip array. At this point the binary data may be encoded in DNA strands with the help of an alphabet of short oligonucleotides sequences.

V.DNA CRYPTOGRAPHIC TECHNIQUES

DNA CRYPTOGRAPHIC TECHNIQUE	WORKING
DNA Digital Coding Polymers' Chain Reaction PCR	This technique use POLYMERIZE chain reaction for the amplification for the DNA Strands
DNA Based Bimolecular Cryptographic Design	This cryptographic method uses one time pad (OTP) and dynamic code book
Symmetric Key Crypto System Using DNA	This technique uses a single DNA strand key for encryption and decryption process. Fabrication and hybridization is done for encryption and decryption process respectively.
Asymmetric Key Crypto System Using DNA	This technique uses a Dual DNA strand key, one for encryption and another for decryption process.
Pseudo DNA Cryptography Method	This technique based on the functioning of DNA. It uses mRNA form to generate Cipher text according to genetic code table
DNA Chip Based Technologies	It uses the genomic sequence of molecular array. It contain series of blots , which are able to bind nucleotide by which data is electronically calculated on the basis of binding probe in each blot
Chaotic coding	This coding uses pseudo-randomness and deterministic which are two features of chaotic systems. Also it is dependent on the initial condition

VII. ADVANTAGE OF DNA CRYPTOGRAPHY

- DNA Encryption make data more secure then other Cryptography.
- DNA Cryptography provide parallelism and fast computation.
- It take less power consumption.
- IT have large storage capacity a one gram of DNA contain 1021 DNA base.
- Use reference sequence to encrypted data virtually not possible to guess this sequence.
- It is error prone

VIII.CONCLUSION & FUTURE SCOPE

DNA Cryptography provide secure communication then other technique .It provide massive parallelism and fast computation . In DNA Blood analysis may prove to be a secure and cost effective biometric method of selecting private keys for use in DNA encryption techniques.Encryption instance to describe all of the encryption algorithm. Moreover, we have analysed each encryption effect. Finally, we analysed the security and operability of the entire system, and used biology software to demonstrate the bio-security of the analogue of the amplification primers, using computer to analyse the statistics and demonstrate the effect of the chaotic system. DNA Cryptography chaotic encryption for dealing with plain text .it eliminates the statistic rule in plain text. security has been improved. Even if the attacker deciphered the DNA code, he will still face a lot of chaoscode that it would be necessary to decrypt. In future we enhance the working of (PCR) technology.

REFERENCE

[1] Leier A et al. Cryptography with DNA binary strands [J]. Biosystems, 2000, 57(1): 13-22.
[2] Beenish Anam et al. "Review on the Advancements of DNA Cryptography", eprint arXiv:1010.0186, 10/2010
[3] Cui G et al. DNA computing and its application to information security field [C] IEEE Fifth International Conference on Natural Computation, Tianjian, China, Aug.2009.
[4] Xiong Fuqin, Cryptography Technology and Application [J]. Science, 2010.
[5] Luque G et al. Metaheuristics for the DNA Fragment Assembly Problem. International
[6] Journal of Computational Intelligence Research, 2005, 1(2), 98–108.
[7] Hayashi et al. Anonymity on paillier's trap-door permutation[C]. Springer Verlag, 2007 , 200-214.
[8] Huo J-J et al. Encoding Technique of DNA Cryptography [J]. Information Security and Communications Privacy, 2009, 7: 90-92.
[9] Chen J. A DNA-based, biomolecular cryptography design [J]. ISCAS, 2003, 3:822-825.
[10] Adleman L, Molecular computation of solutions to combinatorial problems [J]. Science,1994, 266: 1021-1024.
[11] Limin Qin. The Study of DNA - Based Encryption Method [D]. Zheng Zhou: Zheng ZhouUniversity of Light Industry, 2008.)
[12] Borda M. & Tornea O. DNA secret writing techniques [C]. In COMM(2010), Chengdu: IEEE, June 10-12, 2010: 451-456.
[13] C Popovici. Aspects of DNA Cryptography [J]. Annals of the University of Craio hnology
[14] L. M. Ad leman, "Molecular computation of solution to combinatorial problems Science, (1994) 11, (266): 1021-1024.
[15] Chen Jie, "A DNA-based bio molecular cryptography design," Proceedings of IEEE international Symposium, Vol. 3, pp. III-822, (2003).
[16] Pramanik Sabari, and Sanjit Kumar Setua, "DNA cryptography," In Electrical & Computer Engineering (ICECE), 7th IEEE International Conference on, pp. 551-554, (2012).