



Study of DNA Cryptography: A Review

Pramod Singh

Assistant Professor

Bastar University, Jagdalpur (C.G.), INDIA.

Abstract: With the growth of technological advancements the database threats are also grow exponentially. Hence data security has become a critical issue in distributed database environment. Now traditional cryptographic systems are vulnerable to attacks, so that a new concept of cryptography using DNA Crypto has been identified as a possible technology that brings forward a new hope for unbreakable security approaches. In this study we have analyzes the different approaches of DNA Cryptography to understand the basic concept of DNA cryptography.

I. Introduction

The rapid growth of computer and internet technology changes the life of every one and all information including sensitive information such as financial transactions, medical and personal records is transmitted through internet. In this open environment security of the sensitive information is became an important issue. Cryptographic techniques play an important role to ensuring the security of such sensitive information. Cryptography helps the users to securely store or transmit sensitive information across insecure networks so that it can be understood only by the intended recipient [1]. Cryptographic systems transform information into encrypted output which will be meaningless to an unintended user who has no knowledge of the key.

The crypto system can be broadly classified as Symmetric Key Cryptography (SKC) and Asymmetric Key Cryptography (AKC). Symmetric encryption consume same key for both encryption and decryption whereas asymmetric encryption consumes separate keys for encryption and decryption [1, 2].

The security of the encrypted information is strongly dependent on the strength of the cryptographic algorithm and the keys used for encryption and decryption. There are number of encryption algorithms are used in database security but they are also vulnerable to attackers [2]. To overcome this problem a new emerging crypto system is called as DNA cryptography. The main objective of this method is to encrypt the plaintext and hide it in the DNA digital form. DNA cryptography supports high confidentiality of data then the modern methods. The concept of DNA computing is a combination of biological and information technology plays an important role in the field of computer security. It becomes more powerful and unbreakable cryptographic algorithm now days[.]

II. DNA Computing

DNA is a biological term stands for Deoxyribonucleic acid, discovered by Watson in 1953[1]. DNA stores genetic information of the entire living objects like human being to small viruses. It is a combination of two polynucleotide chains. DNA has the capacity to store the information to form another cell. Formulation of DNA is based on two strands of nucleotides which creates double helix structure[2]. These two strands are bind together with four nitrogen bases, A(Adenine),T(Thymine),C(Cytosine) and G(Guanine),(A, T, C, G), all the c information about organism are stored with the combination of these pairs[1,2,3]. The combination of Adenine and Guanine are called purines, whereas Thymine and Cytosine are called pyrimidines[1,2]. DNA is a double helix structure as shown in the Figure 1.

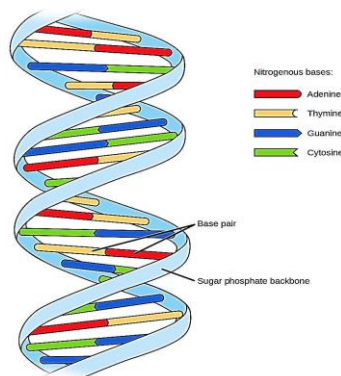


Figure1.DNA Structure [5]

The basic encoding methods of DNA encryption are digital coding (DC) and Polymerase chain reaction Amplification (PCR)[4,5].

Digital coding is a binary coding scheme which is based on 0 and 1 while DNA coding is based on four nucleotide based on A, C, T and G, as shown in table1.

DNA Nucleotide	Binary coding
A	00
T	01
C	10
G	11

Table1. DNA Coding Pattern

Polymers chain reaction is a technique of DNA amplification. In this scheme DNA sequence is encoded by using two primers which are a small DNA fragments. The message which we want to secure with this scheme is placed between two primer pairs[1,5].

III. Basic DNA Encryption Techniques

There are number of DNA encryption methods are available today to secure information in open environment, some important are given in figure2.

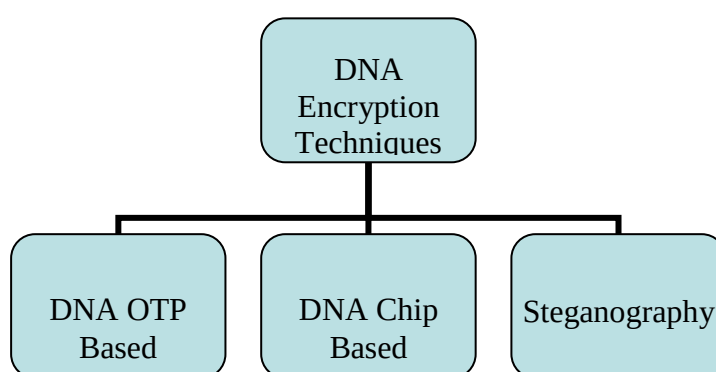


Figure2. Basic types of DNA Encryption Techniques

3.1 One Time Pad

One time pad technique is implemented by using the set of randomly choosing none repeating characters as an input cipher text. These set of characters are used as a pad. This technique supports high degree security of data because the input cipher do not repeated again it can be used only once[1,5]. The length of text should be equal to the length of pad. There are number of schemes are available in literature to implement one time pad technique.

3.2 DNA Chip

DNA chip is nothing but it is a microarray which contains biological information of generic sequences. It can be defined as an ordered sequence of micro spots, where spot contains a single species of nucleic acid[1,3,5]. These spots embedded on solid surface such as a glass substrate and bind together to form complimentary structure. This techniques is useful to encrypt any type of data like text, images etc. the DNA is a biological element and its properties can be changed if the change made into the environment[4,8]. So the encryption results may be changed and unstable if environmental changes may occur.

3.4 DNA Steganography

Steganography is a very old method to hide message in to another message or images. Today this technique is used with DNA to hide huge volume of data into the form of audio, video or images[6,7]. there are number of methods are available today to hide information some of them are, invisible ink, tiny pins pictures and many more. In DNA Steganography message is tagged with random secret key called DNA Strands [5]. Which are further hidden inside other random distracter, DNA strands[7].

IV. Conclusion

Data security is an important issues today global business environment. To protect data in motion number of encryption algorithms has been developed. To overcome the problem with traditional cryptography a new concept has been arise called as DNA Encryption. It is a new technology which has capability to huge data storage and parallelism. There are big chances in this field because not much work has been done in this field till now.

References

1. Kritika Gupta and Shailendra Singh, "DNA Based Cryptographic Techniques: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 3, 2013, ISSN: 2277-128X.
2. Tushar Mandge and Vijay Choudhary, "A Review on Emerging Cryptography Technique: DNA Cryptography", International Journal of Computer Applications, 2012, ISSN: 0975-8887.
3. Sarbjeet Kaur and Sheenam Malhotra, "A Review on Image Encryption Using DNA Based Cryptography Techniques", International Journal of Advanced Research in Computer Science and Management Studies, Vol. 4, No. 3, 2016, ISSN: 2321-7782.
4. Sanjeev Dhawan and Alisha Saini, "Secure Data Transmission Techniques Based on DNA Cryptography", International Journal of Emerging Technologies in Computational and Applied Sciences, Vol. 2, No. 1, ISSN: 2279-0047.
5. Mazhar Karimi and Waleej Haider, "Cryptography using DNA Nucleotides", International Journal of Computer Applications, Vol. 168, No. 7, 2017, ISSN: 0975 – 8887.
6. Manshi rathi, Shreyas Bhaskar, Tejas Kale, Niraj Shah and Naveen Vaswani, "Data Security Using DNA Cryptography", International Journal of Computer Science and Mobile Computing, Vol. 5, No. 10, 2016, ISSN: 2320-088X.
7. Sanjana Kalyani and Nidhi Gulati, "Pseudo DNA Cryptography Technique Using OTP Key for Secure Data Transfer", International Journal of Engineering Science and Computing, Vol. 6, No. 5, 2016, ISSN: 2321-3361.
8. Mabuba Begum, Jannatul Ferdus and Md. Golam Moazzan, "A Hybrid Cryptosystem using DNA, OTP and RSA", International Journal of Computer Science and Applications, Vol. 172, No. 8, 2016, ISSN: 0975-8887.