ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 5, July 2014

International Conference On Innovations & Advances In Science, Engineering And Technology [IC - IASET 2014]

Organized by

Toc H Institute of Science & Technology, Arakunnam, Kerala, India during 16th - 18th July -2014

DNA Based Cryptography Using Permutation and Random Key Generation Method

Bonny B Raj[1], Panchami V[2]

Assistant Professor, Dept of Computer Science, Toc H Institute of Science and Technology, Ernakulam, India[1]

Assistant Professor, Dept of Computer Science, Toc H Institute of Science and Technology, Ernakulam, India[2]

ABSTRACT: DNA cryptography is a new instinctive cryptographic field emerged with the research of DNA computing, in which DNA is used as information shipper and the modern biological technology is used as accomplishment tool. Studies and implementation has proved that this method is very efficient in encrypting, storing and transmitting data and it is very powerful against many attacks. The contemporary main difficulty of DNA cryptography is the lack of effective protected theory and simple achievable method. The most important aim of the research of DNA cryptography is explore peculiarity of DNA molecule and reaction, establish corresponding theory, discovering possible development directions, searching for simple methods of understand DNA cryptography, and Laing the basis for future development. DNA cryptography uses DNA as the computational tool along with several molecular techniques to manipulate it. Because of very high storage capacity of DNA, this field is becoming very talented[4]. Presently it is in the development phase and it requires a lot of work and research to reach a established stage. By reviewing all the prospective and acerbic edge technology of current research, this paper shows the guidelines that need to be deal with development in the field of DNA cryptography.

KEYWORDS: DNA Cryptography, DNA Computing.

I. INTRODUCTION

A security system may have a lot of weak spots: the place where the ciphers are stored, the random number generator, the strength of the used algorithms and so on. The job of the security designer is to make sure none of these weaknesses gets exploited. Based on the confidentiality property in the domain of security the symmetrical and asymmetrical cryptographic algorithms are used. Cryptography consists in processing plain information applying a cipher and producing an encoded output, meaningless to a third-party whether knows about the key or not. In cryptography both encryption and decryption phase are determined by one or more keys. Depending on the type of keys used, cryptographic systems may be classified in:

a)Symmetric systems **:** use the same key to encrypt and decrypt data symmetric key encryption algorithms (also called ciphers) process plain text with the secret key to create encrypted data called *cipher text* are extremely fast and well suited for encrypting large quantities of data. They are vulnerable when transmitting the key examples: DES, RC2, 3DES PBE (password based encryption) algorithms are derived from symmetric algorithms; such algorithms use a salt (random bytes) and a number of iterations to generate a key.

b)Asymmetric systems **:**Overcome symmetric encryption's most significant disability the transmission of the symmetric key rely on key pairs (contains a public and a private key) the public key can be freely shared because it cannot be easily abused, even by an attacker messages encrypted with the public key can be decrypted only with the private key so, anyone

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 5, July 2014

International Conference On Innovations & Advances In Science, Engineering And Technology [IC - IASET 2014]

Organized by

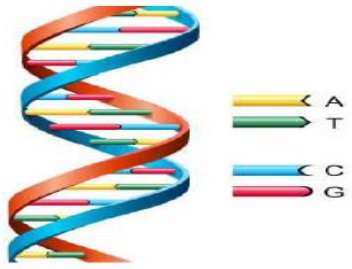
Toc H Institute of Science & Technology, Arakunnam, Kerala, India during 16th - 18th July -2014

can send encrypted messages, but they can be decrypted by only 1 person are not as fast, but are much more difficult to break common use: encrypt and transfer a symmetric key (used by HTTPS and SSL) .

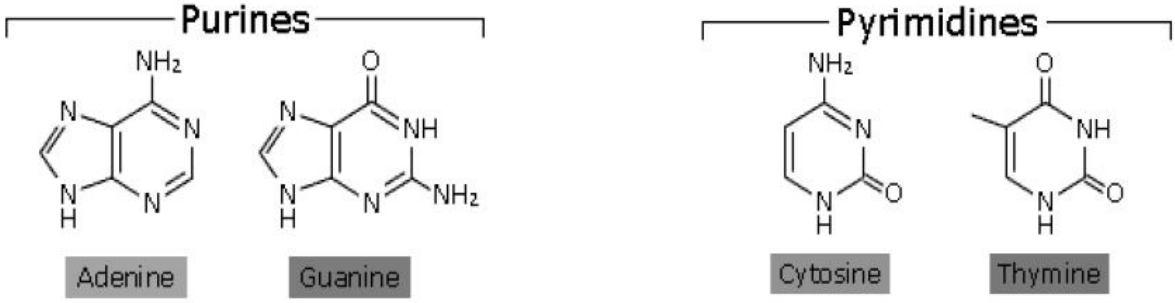
II. DNA

Deoxyribo nucleic acid (DNA) is a nucleic acid that contains the genetic instructions used for the growth and functioning of all living organisms. It is a collection of the most complex organic molecules. The substance is found in every cell of the organism and is essential for the identity of any living being [2]. The main responsibility of DNA molecules is to storage of information for long term. DNA is often compared with a set of blueprints, like any other code. Since it contains the instructions required to construct other components of cells such as proteins and RNA molecules. The DNA segments that hold this genetic information are known as genes, but other DNA sequences have structural purposes and they are involved in modifying the use of this genetic information. Just like a string of binary data is encoded with ones and zeros, DNA strands is encoded with four bases and are represented by letters A (Adenine), T (Thymine), C (Cytosine) and G (Guanine). The information in DNA is stored as a code made up with these four chemical bases as shown in figure 1 below. The bases (nucleotides) are spaced every 0.34 nanometres along the DNA molecule, can give a remarkable data density of nearly 18Mbits per inch. These nucleotides will come together in such a way that A always pairs with T and C always pairs with G[1].

Figure 1 Structure of DNA Molecule



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[2].



DNA is the basic storage medium for all living cells [2]. The main function of DNA is to absorb and transmit the data of life for billions years. Theoretically, we can calculate 10 trillion times simultaneously in a small space at one time.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 5, July 2014

International Conference On Innovations & Advances In Science, Engineering And Technology [IC - IASET 2014]

Organized by

Toc H Institute of Science & Technology, Arakunnam, Kerala, India during 16th - 18th July -2014

III. DNA CRYPTOGRAPHY

DNA cryptography is a new promising direction in cryptography research that emerged with the evolution of DNA computing field. DNA can be used not only to store and transmit the information, but also to perform computation. The extensive parallelism and extraordinary information density inbuilt in this molecule are exploited for cryptographic purposes. Several DNA based algorithms are proposed for encryption, authentication and so on. In this paper, the research conducted by a number of authors related to the discipline of DNA Cryptography is taken into consideration. It has been shown that how DNA cryptography uses DNA as the computational tool with a number of molecular techniques to manipulate it along with various algorithms for encryption [2].

IV. PROPOSED ALGORITHM

Proposed algorithm is a new encryption algorithm based on random generation of DNA pattern. So far we have come across many ideas which involve data encryption using traditional mathematical operations and/or data manipulating DNA techniques. When an encryption algorithm has been implemented and the data is transmitted via the transmission media, there are possibilities that the data, even if in the cipher form gets attacked or modified by any intruder. To avoid that we check our data for any kind of manipulation at the receiver's end.

A. Steps for the encryption

1) The plaintext is to be converted into its ASCII code first.
2) ASCII code is then again converted into binary form to get the data in 0's and 1's.
3) These binary values are encoded in DNA sequences using table (Table 1) of binary to nucleotide conversion where each of the four bases is represented by combinations of 0's and 1's.
4) Again, a DNA sequence is selected as a key and grouped in the blocks in which each block is of 4 characters each.
5) Then a table is created based on the positions of each character in the key sequence.
6) Based on that table and the randomly selected DNA sequence data gets converted into encrypted form (Figure 1).
7) The encrypted sequence with the key is send to the receivers end.

Table 1: Nucleotide to Binary Conversion

Nucleotide	Binary Form
A	00
C	01
G	10
T	11

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

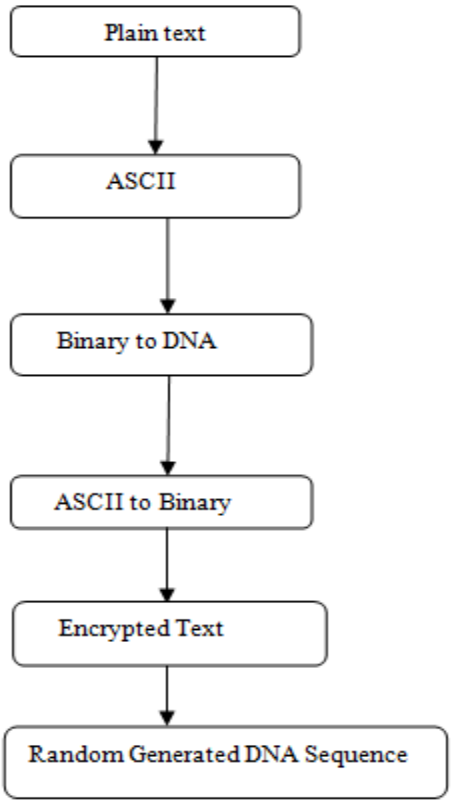
International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 5, July 2014

International Conference On Innovations & Advances In Science, Engineering And Technology [IC - IASET 2014]

Organized by

Toc H Institute of Science & Technology, Arakunnam, Kerala, India during 16th - 18th July -2014



B. Steps for Decryption

The cipher sequence along with the key are received here and the decryption algorithm is applied to find the actual DNA sequence hidden in the cipher DNA sequence.

1) The DNA sequence is then gets decoded into binary using the above same conversion table.

2) Binary is converted into ASCII and finally ASCII to the actual text.

V. CONCLUSION

DNA cryptography is basically hiding of data in terms of DNA sequences. This is done by using various DNA technologies with the biological tools. Here in this paper with the summarization of DNA, basics of where DNA is found are discussed. Various biological operations that can be carried on DNA are explained. Further DNA cryptography and the biological work on DNA cryptography is taken into consideration. It is shown that how traditional cryptography differs from the emerging DNA cryptography. Few of the advantages along with the limitations of DNA Cryptography are mentioned. Later on, the existing DNA cryptographic techniques are discussed and a comparison between different cryptographic schemes using DNA technology is explained. The future work will consist of analysing and comparing the performance of all the DNA cryptographic techniques based on secure data transmission processes.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 5, July 2014

International Conference On Innovations & Advances In Science, Engineering And Technology [IC - IASET 2014]

Organized by

Toc H Institute of Science & Technology, Arakunnam, Kerala, India during 16th - 18th July -2014

REFERENCES

[1] . Guozhen Xiao, Mingxin Lu, Lei Qin, Xuejia Lai: New field of cryptography: DNA cryptography. Journal of Chinese Science Bulletin June 2006, Volume 51, Issue 12, pp 1413-1420.
[2]. Sanjeev Dhawan, Alisha Saini Secure Data Transmission Techniques Based on DNA Cryptography. International Journal of Emerging Technologies in Computational and Applied Sciences, 2(1), Aug-Nov. 2012, pp. 95-100.
[3]. Kritika Gupta, Shailendra Singh DNA Based Cryptographic Techniques: A Review. International Journal of Advanced Research in Computer Science and Software Engineering 3(3), March - 2013, pp. 607-610.
[4]. Beenish Anam, Kazi Sakib, Md. Alamgir Hossain, Keshav Dahal Review on the Advancements of DNA Cryptography Journal SKIMA 2010, August 25-27, 2010, Paro, Bhutan.