International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Review Paper Volume-5, Issue-6 ,2018 Regular Edition E-ISSN: 2349-7084

A Review on Cryptography Techniques using DNA Computing

Pritesh Bhimani[1*]

[1*]*Computer Engineering, Diwaliba Polytechnic*

e-mail:Pritesh.bhimani1992@gmail.com

Available online at: http://www.ijcert.org

Received: 22/June/2018, Revised: 24/June/2018, Accepted: 26/June/2018, Published: 28/June/2018

Abstract:- Cryptography and steganography are one of the most critical and needed areas of computer and data security. A mixer of both can make more secure the data. Cryptography is the way to secure the transfer data from sender to receiver. Steganography is a way to ensure the data by the hiding it. One new term is added with the Cryptography for making data more secure is DNA. DNA cryptography is a new hopeful way in cryptography research. DNA can be used to store and transmit the information with the more secure method and most used to perform the computation. Combination of DNA and Cryptography make sure for the security in this world. Nowadays DNA cryptography is in the development phase, and it requires lots of work, efforts and research to reach a fully developed stage. This paper describes different DNA based cryptography techniques that increase the security of cryptography techniques.

Keywords: DNA structure, Polymer Chain Reaction (PCR), Central Dogma of Molecular biology, DNA digital coding, DNA Cryptography, RSA, OTP, IDEA.

---

1. Introduction

Cryptography must be needed for transmitting information securely. The techniques that are used for cryptography must be that much powerful and secure so that no one can break it. DNA cryptography is one of the major concern areas for reliable and powerful cryptography system. DNA cryptography can be used in encrypting or encoding the data using DNA computing techniques. Because of DNA properties like parallel molecular computing, storing, transmitting the data and computing capabilities, DNA is also used for other cryptographic purposes like - authentication, signature, etc. Due to this DNA cryptography research field is one of the secure and robust areas for some applications. We are not using real biological DNA strands for computing, but just the principle ideas of the central dogma of molecular biology. It contains some operations like transcription, splicing, and translation process of the fundamental doctrine. To get the proper idea, we have to know about DNA structure and molecular biology operations.

Rest of the paper is organized as follows, Section I contains the introduction DNA Cryptography, Section II contains the related work of DNA Computing, Section III contain some methods of DNA based computing Cryptography algorithms, Section IV include the comparison between techniques, section V explains the concludes research work.

2. Related Work

Bio-molecular Technology Background

A. DNA Structure

 https://doi.org/10.22362/ijcert/2018/v5/i6/v5i604

DNA, the principal support of genetic information (genetic blueprint) of any organism in the biosphere, is composed of two long strands of nucleotides, each containing one of four bases (A – adenine, G – guanine, C – cytosine, T – thymine). A DNA molecule has a double-stranded structure obtained by two single-stranded DNA chains, bonded together by hydrogen bonds: A = T double bond and C ≡ G triple bond [1]. As per the Watson- crick's DNA base pairing, Adenine(A) always forms a base pair with Thymine(T) and Guanine(G) still forms a base pair with Cytosine(C) [3].

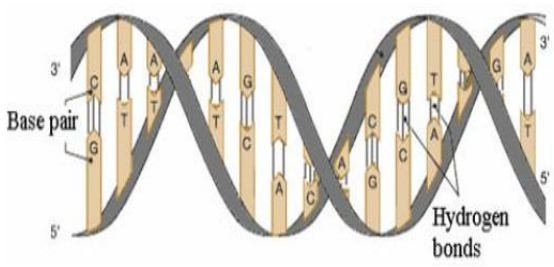

Figure 1: DNA Structure [1]

B. Central Dogma of Molecular Biology

The genetic information transfer from DNA into RNA is called transcription and from RNA to protein is called translation. This whole process is called central dogma of molecular biology. So, the central dogma of molecular biology deals with the residual transfer of sequential information.

Figure 2: Central Dogma of Molecular Biology [1]

C. Polymerase Chain Reaction

Polymerase chain reaction is a quick amplification process of DNA. Due to complex work to manipulate small amounts of DNA, PCR used to amplify a large number of chosen DNA in short period. To achieve PCR amplification needs to know the DNA chain selected and primer (DNA sequence which contains some nucleotides), then the primer will be amplified for the selected DNA. Thus one can effectively increase a lot of DNA strands within a concise period. PCR amplification is very sensitive, and it is affected due to change in temperature [1].

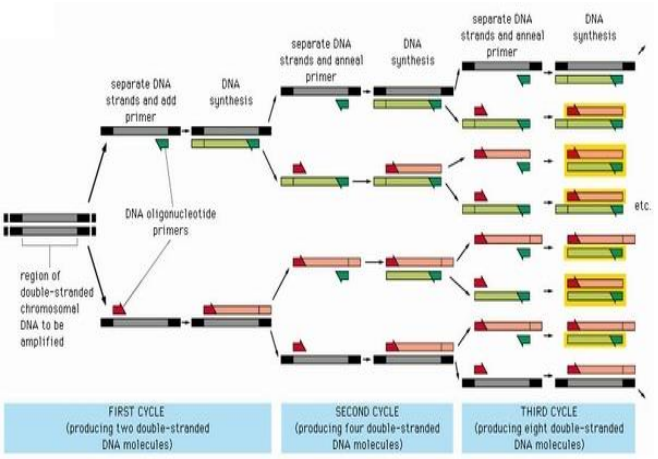

Figure 3: Polymerase Chain Reaction [6]

D. DNA Digital Coding

The primary coding method is binary digital coding, which is encoded by two number 0 or 1 and a combination of 0 and 1. So to encrypt the A, C, T, G we can use the four digits: 0(00), 1(01), 2(10), 3(11). There are 4!=24 possible coding patterns by this encoding format, but as per Watson-Crick complementarily rule 0(00) is a complement to 3(11), and 1(01) is a complement to 2(10). So from these 24 patterns, only eight kinds of models which are topologically and identically fit the complementary rule of the nucleotide bases. It is suggested that the coding pattern in accordance with the sequence of molecular weight, 0123/CTAG, is the best coding pattern for the nucleotide bases. This digital encoding technique is used in traditional cryptography methods like RSA, DES and AES [5].

Table 1: DNA Digital coding [5]

0123 CTAG	0123 CATG	0123 GTAC	0123 GATC
0123 TCGA	0123 TGCA	0123 ACGT	0123 AGCT

3. Cryptographic Techniques based on DNA

DNA cryptography is the new promising direction for the better security performance of cryptography methods. DNA cryptography and information science were born after research in the field of DNA computing by Adleman [1]. BMC methods were proposed by Adleman to solve difficult combinatorial search problems, using the tremendous available parallelism to the combinatorial search among a

large number of possible solutions represented by DNA strands. After that many difficult problems can be solved by the DNA computing.

A. DNA Computing Based Cryptography

This technique shows [5] the combination of DNA computation and RSA algorithm for better security purpose. RSA algorithm provides the best security in Public Key Cryptography (PKC).

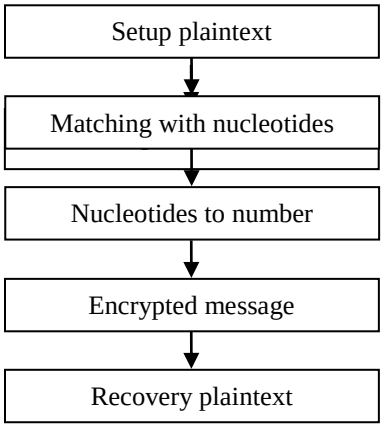

Fig.4: Algorithm (Wang and Zhang, 2009)

Steps to computing algorithm as per DNA computing based cryptography.
Step 1: Set positive integer n and e. both must be the prime number.

Step 2: Covert plaintext into base nucleotides using below a table.

Table 2: Encode Plaintext [5]

A-CCA	**B-GTT**	**C-TTG**	**D-GGT**	**E-TTT**
F-TCG	**G-CGC**	H-ATG	**I-AGT**	**J-CGA**
K-GAA	**L-CGT**	**M-CCT**	**N-TCT**	**O-CGG**
P-ACA	**Q-CAA**	**R-ACT**	**S-GCA**	**T-CTT**
U-GTC	**V-TCC**	**W-GCC**	**X-ATC**	**Y-AAA**
Z-TCA				

Step 3: Turn nucleotides into numbers using below a table.

Table 3: Nucleotides to Number [5]

A – 01	C - 03	G - 07	T - 20

Step 4: Calculate e^{th} power of n. Compute decipher exponential d.

Step 5: Separate the number into three parts. Make sure every part of the name is less than n.

Step 6: Through calculation of three parts numbers, we get ciphertext. In the calculation process, it needs to compute Euler's theorem with.

$$CT = PT^{K} \bmod N \quad (1)$$

Step 7: For decryption, calculate the plaintext from the ciphertext as this:

$$PT = CT^{D} \bmod N \quad (2)$$

Now reverse transformation from table 2 and table 3 is calculated and the result of this process is plain text.

B. DNA Secret Writing Techniques

OTP (one time pad): in this method, the ssDNA (single strand DNA) sequence is used for OTP key generation.

DNA XOR OTP: here the DNA tiles are used, each tile contains one bit either 0 or 1. This has upper and lower end with DNA strand, used for binding other tiles with complementary DNA strand.

DNA chromosome indexing: The index of the point where the DNA sequence for the character is matched with FASTA file sequence considered as a pointer and stored in the ciphertext. So, instead of sending a text to the receiver the index of DNA FASTA file has been posted [1]

C. Encryption Scheme Using DNA Technology

In this paper [2] DNA technology is proposed with the traditional cryptography technique.

Key generation: The sender and receiver respectively generate and exchange a pair of PCR primers over a secure communication channel. The encryption and decryption keys are a pair of PCR primers. In this scheme, the two primer pairs were not independent designed by sender or receiver, but respectively outlined complete cooperation by sender and receiver. So, this could increase the security of this encryption scheme, because even if anyhow one caught one of a primer pair, the amplification was not efficient when one of a primer pair is incorrect, only when both of the primer sequences were correct, the amplification could be successful.

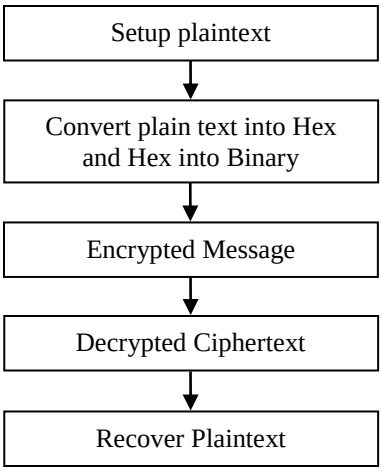

Figure 5: Step of Algorithm

Data pretreatment: Plaintext will be converted into the hexadecimal format, and then this hex code converts into a binary representation.

Encryption: Sender will encrypt the binary plaintext into the binary ciphertext by using receiver's public key. Then, the receiver converts the binary ciphertext into the DNA sequence by using the DNA digital coding technology. Secret-message DNA sequence containing an encoded message with forward and reverse PCR primers. Thus, the secret-message DNA is prepared. After mixing the secret-message DNA sequence with a certain number of dummies, the sender sends the DNA
the mixture to the receiver using an open communication channel, such as DNA ink or DNA book.

Decryption: Receiver gets the DNA mixture, it can quickly pick out the secret-message DNA sequence by using the correct primer pairs. Receiver translates the secret-message DNA sequence into the binary ciphertext by using the DNA digital coding technology. Then, the receiver can decrypt the binary ciphertext into the binary plaintext by using own secret key.

Data post-treatment: After the binary plaintext has been recovered, the receiver can retrieve the plaintext from the binary plaintext by using data post-treatment.

D. Integrating DNA Computing in International Data Encryption Algorithm (IDEA)

Here basic IDEA algorithm is proposed with the variation in structure to make it more secure and efficient. Using the DNA computing introduce IDEA algorithm [6].

Steps of Algorithms:-

At Sender Side:
Step 1: Enter text to be encrypted
Step 2: Apply DNA encryption algorithm to the book entered
Step 3: Encrypt DNA encrypted text with IDEA encryption Algorithm with a 128-bit key
Step 4: Convert the 64-bit ciphertext obtained into DNA sequence using a lookup table
Step 5: Send DNA sequence obtained as a cypher

At the receiver side:

Step 6: DNA sequence obtained is used to get usual cypher for IDEA decryption algorithm
Step 7: IDEA decrypts the message using initial cypher accomplished through DNA sequence
Step 8: DNA decryption algorithm further decodes message recovered from IDEA
Step 9: Original plaintext is recovered

After completing this steps receiver get plaintext text back secure way.

4. Results and Discussion

As we have seen that there is many techniques based on DNA computing, first we seen public key cryptography using RSA algorithm in that within the DNA digital coding encryption will be done. Moreover, in DNA secret writing technique, they used the DNA Computing theories for encryption. Furthermore Encryption scheme using DNA technology where PCR amplification, digital coding concept used for better encryption, decryption and key generation purpose. But this all techniques are difficult to realise and expansive to apply.

Table 4: Comparison between Techniques

DNA Cryptography Schemes	**Technology Used**
DNA Computing Based Cryptography	Plaintext convert using encoded table than encrypted by RSA algorithm

DNA Secret Writing Techniques	DNA computing theories used in OTP, DNA XOR OTP, DNA chromosome indexing
An Encryption scheme using DNA Technology	PCR primers are used in a key generation which is used to encrypt and decrypt the message.
Integrating DNA Computing in International Data Encryption Algorithm (IDEA)	Plaintext convert using encoded table than encrypted by IDEA algorithm

5. Conclusion

Using the properties of DNA like parallel molecular computing, storing, transmitting the data and computing capabilities we can get the better performance and security in cryptographic techniques. Mix-up of DNA computing theories and cryptography concepts gives the new promising direction. Still, this concept is its initial stage.

6. Acknowledgement

I take this opportunity to express my sincere thanks and broad sense of gratitude to Ms Drashti Vadaviya for imparting me valuable guidance. She helped me by solving many doubts and providing many references. She helped me by giving helpful suggestions and encouragement. She is also in having a better insight into this field.I am also thankful to Mr Fenil Khatiwala who encourages me to do such a research and implementation part.

References

[1] M Borda, T. Olga, *"DNA Secret Writing Techniques", Communications (COMM), 2010* 8th International Conference. Pp. 451-456, IEEE 2010.

[2] C. Guangzhao, Q. Limin, W. Yanfeng, Z. Xuncai, "*An Encryption Scheme Using DNA Technology* ", *Bio-Inspired Computing: Theories and Applications, 2008.* BICTA 2008. 3rd International Conference. Pp. 37-42, IEEE-2008.

[3] Crick Francis, *"Molecular Structure of Nucleic acid: A Structure of Deoxyribose Nucleic Acid", April 25, 1953.* Nature 171(April 25,1953): 737-738

[4] Dhawan Sanjeev, Saini Alisha, "*Secure Data Transmission Techniques Based on DNA Cryptography", International Journal of Emerging Technologies in Computational and Applied Sciences, 2012.*

[5] Wang Xing, Zhang Qiang, *"DNA computing-based cryptography", Bio-Inspired Computing, 2009*. BIC-TA '09. Fourth International Conference. PP. 1-3, IEEE 2009

[6] P. Rakheja, "*Integrating DNA Computing in International Data Encryption Algorithm (IDEA)*", International Journal of Computer Applications, 2011, Volume 26 – no.-3, July 2011.

Authors Profile

Pritesh D. Bhima received his B.Eng. Degree in Computer Engineering from Gujarat Technical University, Gujarat, India, in 2013 and the M.Tech degree in Computer Engineering from UKA tarsadia University, Bardoli, India in 2016. He is now an assistant Professor with Department of Computer Engineering, Uka Tarsadia University, Bardoli, Gujarat, India from 2016 to date. His research interests include Wireless Sensor Network and Information Security.

