International Journal of Bio-Science and Bio-Technology
Vol.6, No.5 (2014), pp.215-222
http://dx.doi.org/10.14257/ijbsbt.2014.6.5.22

Message Transmission Based on DNA Cryptography: Review

Tausif Anwar[1], Dr. Sanchita Paul[2] and Shailendra Kumar Singh[3]
[1]Dept. of Computer Science & Engg.
Birla Institute of Technology, Mesra Ranchi, 835215, India
[2]Dept. of Computer Science & Engg.
Birla Institute of Technology, Mesra Ranchi, 835215, India
[3]Dept. of Computer Science & Engg.
Birla Institute of Technology, Mesra Ranchi, 835215, India.
[1]tausifanwar30@gmail.com, [2]sanchita07@gmail.com, [3]sks.it2012@gmail.com

Abstract

DNA cryptography is used to encrypt message for secure communication on a network. It is a information carrier for transferring message from sender to receiver. For secure communication, it is not only to encrypt message but also necessary to hide encrypted message. DNA cryptography is also used for hiding the data, Hidden message is known by only sender and receiver. DNA computing is used to solve problems in cryptography, cryptanalysis and steganography. DNA sequences based data encryption seems to be a promising strategy for fulfilling the current information security needs.

This paper focus on the comparative study of some existing works on DNA Cryptography. Message transmission is a process to transmit encrypted data through secure communication channel using DNA cryptography. Text message is encoded in DNA sequence. Message transmission process reduces the time complexity of transferring encrypted message. Bio molecular and one-time- pad technologies is used for secure message encryption.

***Keywords:** - DNA Cryptography, DNA Sequences, Data hiding, Secure Transmission*

1. Introduction

DNA cryptography is a branch of biological science, which has large data storage capacity. It stores information of living organisms. Living organisms has unique DNA information. It is defined as information storage, massive parallel processing and highly secured data transmission. DNA cryptography is based on one-time-pads scheme. Cryptography has to combine with molecular biology for more secure data transmission and data hiding. A plaintext message is encoded in DNA sequences. DNA sequences get powerful, when combined with nucleotide base A-T and C-G. DNA cryptography technology is needed in information security to protect and hide data. In traditional cryptography (like as DES, RSA), encrypted messages are detectable by attacker. DNA has capacity to store huge information rather than existing algorithm. DNA is introduced as a new technology for unbroken data. Genetic information is encoded as a sequence of nucleotides Guanine-G, Adenine-A, Thymine-T and Cytosine-C. Adenine, Thymine and Guanine, Cytosine are base pairs, which are attached to a sugar and a phosphate to maintain helical structure. DNA strands combined with hydrogen bond. A and T DNA sequences are combined with double hydrogen bond while C & G are combined with triple bond. Each nucleotide consists of the following three components, A Nitrogenous Base, A five carbon Sugar, A Phosphate Group.

ISSN: 2233-7849 IJBSBT

There are two types of DNA structure- single strand DNA and double strand DNA, which are complementary to each other. The encryption methods encrypt plaintext to cipher-text through one-time-pad scheme. The decryption methods decrypt received individual cipher-text packets to plaintext. The advantages of DNA molecular structure is its vast parallelism, exceptional energy efficiency and extra ordinary storage space. The disadvantages of DNA cryptography is it require huge computing time, high computational complexity and high tech bimolecular laboratory. Existing cryptography uses modern biological technologies. These technologies include PCR amplification and hybridization. These biological technologies are costly, complex and require a lot of time. DNA has much more storage capacity which is equal to (1gm=10^8 tera bytes). It means small amount of DNA can stores world's information.

DNA chain has a large scale of parallelism. Its computing speed is 1 billion times per second. DNA cryptography is a subfield of information science and emerged after the research of DNA computing in 1994. It provides a parallel processing capability with molecular level, to solve complex computational problem. DNA cryptography and information science is an effective application in design, analysis and application of DNA cryptosystem. Research on DNA cryptography is in the initial stage and required a lot of research in this field. DNA technology used to solve Hamilton path problems, combinatorial problems and extends to solve NP-complete problem by Lipton. DNA digital coding is based on binary digital coding, which is encoded by combination of 0 and 1. This paper focuses on different DNA methods of encryption process, which are powerful and secure than other traditional cryptography. DNA and RNA are media for data storage due to very large amounts of data that can be stored in compact volume. They far exceed the storage capacities of conventional electronic, magnetic and optical media.

2. DNA Cryptography Methodologies

DNA cryptography methodology uses different process to encode data. Different DNA cryptography methodology is used for secure message transmission like Polymerase chain reaction (PCR), bio molecular, one-time-pad. PCR technique is a DNA Digital coding technique, in which message are converted hexadecimal code into binary code and further converted into DNA sequence, which is used in DNA template. Bio molecular technique uses parallel processing capabilities of bio molecular computation. One-time-pad technique is used to encrypt and decrypt images.

Table 1. Types of DNA Methodologies

Types of DNA Methodologies	Description
1. Bio Molecular Structure	• Bio molecular structure present in all living thing. • All living organisms have unique DNA molecule to store information of different living organisms. • Bio-molecular structure is used to encrypt and decrypt message for data transmission. • Bio molecular structure is most prominent Cryptography techniques than Polymerase chain reaction, DNA hybridization, DNA fabrication, DNA fragment techniques.

2. OTP (One Time Pad)	• One-time-pad was first introduced by Vernam. It is random key generation, which is used in encryption and decryption process. Later on this theory is extended by Shanon. • Shanon explained key size, which was greater than or equal to plaintext. Key should be unique and not to be reused.
3. DNA chip technology	• DNA chip technology was developed to identify independent biological sample. • Use of microscopic array of DNA technologies on solid surface to examine biochemical sample. • DNA microarray utilizes the high density of molecular array.
4. DNA Fragmentations	• DNA fragmentation was first represented by Williamson in 1970. He observed fragment during initial cell death. • DNA fragmentation is breaking of DNA strands into small pieces. It can be extended to future generation.
5. Polymerase chain reaction (PCR)	• Polymerase chain reaction (PCR) is a fast DNA amplification technology. DNA cryptography is implemented by modern Biological techniques and biological hard problems. • Polymerase chain reaction is as molecular biology process used to exponentially in DNA. • The generated DNA used as template, which describe the exponential amplification.

3. Exiting Works on DNA Cryptographic

In 2003, Jie Chen [2] presented the DNA cryptographic approach based upon carbon nanotube message transformation and DNA based cryptosystem. Carbon nanotube-based is used to transfer data between DNA and conventional binary storage.

In 2004, Sabari Pramanik1 *et al.*, [3] presented the parallel cryptography technique by using DNA molecular structure, one time pad, DNA digital coding technique and DNA hybridization technique. One-time-pad technique is used for encryption key, which increases computational complexity.

Tushar Mandge *et al.*, [4] proposed DNA encryption technique based on matrix manipulation and secure key generation scheme. They explained about the DNA computing, vast parallelism and exceptional energy efficiency, which provide better security than traditional technique.

In 2005, Kazuo Tanaka [5] proposed the DNA cryptographic approach based on Public Key. Public key is used to encrypt message in DNA sequences and encrypted message sequence forwarded to the immobilization process and then for PCR amplification. Polymerase Chain Reaction (PCR) amplifications are used two primers to encode a message.

In 2006, Sherif T. Amin [6] proposed the DNA cryptographic approach based on symmetric key, where key sequences are obtained from the genetic database and remain same at both ends (sender and receiver). Message/plaintext is first converted into binary format and then to DNA format using substitution.

In 2008, Guangzhao Cui *et al.*, [7] 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.

In 2008, Lai Xin-she *et al.*, [8] proposed A novel generation key scheme based on DNA using key expansion matrix. They used random key generation scheme to increase computational speed. In this algorithm author used block cipher, data signature, identity authentication, DNA sequences, which randomized database.

In 2010, Lai Xuejia *et al.*, [9] proposed Asymmetric encryption and signature method with DNA technology. This paper proposed DNA public key cryptosystem, an asymmetric encryption and signature cryptosystem. DNA (PKC) uses encryption and signature. Key and cipher-text is biological molecule in DNA (PKC). In DNA (PKC) key and cipher-text are transmitted physically and it's difficult to replicate. DNA public key cryptosystem is based on DNA microarray chip. It is fabricated with probes for encryption and decryption. Existing probes are used as a key. If the probes have intensity greater than some fixed value then it is denoted as probe 1 and if the probes have intensity lesser than some fixed value, it is denoted as probe 0. For encryption process two key are used PKs and PKr. First plaintext converted into its ASCII code and then it converted into binary code, binary code is arranged in the form of matrix.

In 2011, Deepak Kumar *et al.*, [10] proposed a new secret data writing techniques based on DNA sequences. They have explained about one-time-pad (OTP) technique for secure data transformation and DNA coding technique. They used cryptography and steganography technique for encryption and hiding data.

In 2011, Bibhash Roy *et al.*, [11] proposed an improved symmetric key cryptography with DNA based strong cipher. Author focused on DNA computational logic, used for encrypting, storing and transmitting the data. This paper proposed about the unique cipher-text procedure and key generation procedure. Author discussed only about DNA cryptography and DNA computing.

In 2012, Yunpeng Zhang *et al.*, [12] proposed a DNA cryptography based on DNA fragment assembly. Author mentioned features of DNA molecular, key bio technologies, DNA digital coding and related software. Using the DNA digital coding and DNA fragmentation author designed symmetric system algorithm, it converted plaintext into binary ASCII code and then into DNA sequences.

In 2013, Wang Zhong *et al.*, [13] proposed an Index based DNA encryption algorithm. They used Block cipher and Index of string for encrypting message into DNA sequences, which is send to the receiver by a secure communication medium. First message converted into ASCII code then converted into binary code, which is further converted into DNA sequence. DNA sequence search in the key sequence and writes in index number.

In 2014 K. Menaka *et al.*, [14] proposed Message Encryption Using DNA Sequences. They described about data hiding based on DNA sequence. DNA sequences based data encryption algorithm fulfilling the current information security needs. In this paper, an algorithm using DNA sequences for data hiding is proposed and discussed for secure data transmission and reception.

The following Table-2 shows that the comparative study of existing works on DNA Cryptography based on the following parameters.

1) **Cryptography mechanisms**
2) **Software (s/w) -** used for the implementation of designed algorithm.
3) **Methodology**
4) **Advantages**
5) **Disadvantages**

Table 2. Existing Works Based on DNA Cryptography

Author/ Year	Paper Title with ref.	Cryptographic mechanisms	S/W used	Methodology Used	Advantages	Disadvantages
Jie Chen 2003	A DNA-based, Bimolecular Cryptography Design.[2]	Symmetric key	java	1. DNA molecular structure. 2. One-time-pad.	1. Storing large amount of data in compact volume. 2. Massive parallel processing capabilities of bio molecular computation.	1. Decrypt message as given in the code book. 2. Difficult to send message which is not in code book.
Sabari Pramanik et al., 2004	DNA-Based Cryptography [3]	Symmetric key	Vb.net	1. DNA hybridization. 2. DNA molecular structure.	1. Parallel technique to decrypt message. 2. Extra ordinary storage Capacity. 3. Reduce the time complexity.	1. Require high tech bio molecular laboratory. 2. Huge computing time.
Sherif T Amin et al. 2006	A DNA based implementation of YAEA encryption algorithm [6]	Symmetric key	Vb.net	1. DNA nucleotides , searching algorithms	1.Real message is not transfer over network 2. Scalable for large digital information products.	1. Size of plain text increases the encryption time and decryption time.
Tushar Mandge et al., 2008	A DNA Encryption Technique Based on Matrix Manipulation and Secure key Generation Scheme[4]	Symmetric key	Vb.net	1. Matrix manipulation. 2. Key generation.	1. Secure generation algorithm to generate a new key for encryption process. 2. Always get new cipher data from same plaintext. 3. It provides good security layer which does not give any hint about plaintext.	1. It includes only basic operation. 2. Security only depends upon key.
Guangzhao Cui et al., 2008	An Encryption Scheme Using DNA Technology [7]	Asymmetric key	java	1. DNA synthesis. 2. DNA digital coding. 3. PCR amplification.	1. Prevent attack from a possible word as PCR primers. 2. The complexity of Biological scheme and cryptography computing provide a double security safeguards for the scheme. 3. Cost of encryption scheme is low.	1. Security can depend only on decryption key. 2. The encryption scheme is still far away being a perfect scheme.

LI Xin-she et al., 2008	A Novel generation key scheme based on DNA[8]	Symmetric key	Vb.net	1. key expansion matrix	1. DNA sequence reduces the computation complexity. 2. Computation speed is increased.	1. Security depends upon the key.
Deepak Kumar et al., 2011	Secret Data Writing Using DNA Sequences [10]	Symmetric key	Vb.net	1. One-time-pad.	1. Any change in the cipher text is easily detectable. 2. Remove the deficiencies in the scheme of DNA steganography and Cryptography.	1. Security depends upon key.
Zhang Yunpeng et al., 2011	Index-Based Symmetric DNA Encryption Algorithm [13]	Symmetric key	java	1.Xor operation 2.Position Indexing	1. Exact position of DNA sequence is not identified. 2.Huge key space, high sensitivity to plaintext on encryption. 3. Proper random key sequence to improve security.	1. Higher security, could encrypt a longer DNA Sequence takes more time. 2. Security completely depends upon key.
Yunpeng Zhang et al., 2012	DNA Cryptography Based on Fragment Assembly [12]	Symmetric key	Matlab	1. DNA Fragmentation	1. Length of cipher-text is secure and short.	1. Length of DNA Fragment is short, attacker can easily detect.

4. Discussion & Future Scope

In 2012, Sabari Pramanik1 et al. [3] a new technique worked on DNA hybridization, DNA digital coding and uses one-time-pad as an encryption key. It reduces time complexity. This method uses parallel technique to decrypt message and also minimize time for decryption. This method can be implemented in multi core environment and increasing computational complexity is future work.

In 2014, Ashish kumar kaundal [16] discussed about feistel inspired structure DNA cryptography for encryption process. The results indicate that the feistel inspired structure for DNA cryptography using one time pad for key generation achieves a better encryption although the cost of increased encryption and decryption time.

In 2006 Sherift Amin *et al.*, [6] explained about plaintext messages and images are transformed into sequences of DNA nucleotides. Proposed algorithm could easily be improved using a larger DNA strand.

In 2011 Wang Zhong, Zhy Yu [13] *et al.*, In this paper a new index-based symmetric DNA encryption algorithm has been proposed. The algorithm has achieved the computing-security level in the encryption security estimating system. A DNA computing and biological characteristic uses to eliminate the disadvantages of block cipher mode.

Table 3. Future Direction over Existing Works

Author/Year with Ref	Title	Exiting Method	Future Scope
SherifT Amin et al., 2006[6]	A DNA-based Implementation of YAEA Encryption Algorithm	1. Encryption and Decryption Digital information from biological DNA strand.	1. Proposed algorithm could easily be improved using a larger DNA strand.
Lai et al., 2010 [9]	Architectural Framework for Encryption & Generation of Digital Signature Using DNA Cryptography	1. Encryption, Decryption and Generation of digital signature.	1. Improving Encryption/Decryption time complexity.
Deepak Kumar et al., 2011 [10]	Secret Data Writing Using DNA Sequences	1. Data hiding algorithm using DNA sequences and traditional steganography.	1. DNA computing has brighter development possibilities in field of steganography and authentication.
Wang Zhong et al., 2011 [13]	Index-Based Symmetric DNA Encryption Algorithm	1. Symmetric key cryptosystem based on DNA symmetric key cryptosystem and applying index.	1. To provide a theoretical proof of DNA cryptosystem's validity to make it be provable security level, and perfect the algorithm's Security model. 2. Use of DNA computing and biological characteristics to eliminate the disadvantages of block cipher mode.
Pramanik Sabari et al. 2012 [3]	DNA Cryptography	1. DNA digital coding technique. 2. DNA hybridization technique. 3. Use one-time-pad as the encryption key.	1. To be implemented in multi core environment. 2. Increase computational complexity.
Ashish kumar kaundal 2014 [16]	Feistel Inspired structure for DNA cryptography	1. Discussing about implementation of feistel inspired structure and compared with traditional algorithm.	1. DNA cryptography is looking implementation of integrity factor and extend to steganography to provide more protection and increases complexity. 2. Improving space complexity of this algorithm.

References

[1] L. M. Ad leman, "Molecular computation of solution to combinatorial problems Science, **(1994)** 11, (266): 1021-1024**.**

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

[3] Pramanik Sabari, and Sanjit Kumar Setua, "DNA cryptography," In Electrical & Computer Engineering (ICECE), 7th IEEE International Conference on, pp. 551-554, **(2012).**

[4] Tushar Mandge, Vijay Choudhary. "A DNA encryption technique based on matrix manipulation and secure key generation scheme". Information Communication and Embedded Systems (ICICES), International Conference on 21-22 Feb. (**2013)**.

[5] Kazuo Tanaka, Akimitsu Okamoto, and Isao Saito, "Public-key system using DNA as a one-way function for distribution". Bios stems 81, 1, pp. 25-29, **(2005).**

[6] Sherif T. Amin, Magdy Saeb and El-Gindi Salah, “A DNA-based implementation of YAEA encryption algorithm,” In Computational Intelligence, pp. 120-125, **(2006)**.

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

[8] Lai Xin-she, Zhang Lei, “A novel generation key scheme based on DNA”. Computational Intelligence and security, IEEE, International conference on 13-17 Dec. **(2008).**

[9] Lai, XueJia, "Asymmetric encryption and signature method with DNA technology," Science China Information Sciences 53.3, page 506-514, **(2010).**

[10] Deepak Kumar, and Shailendra Singh, "Secret data writing using DNA sequences," In Emerging Trends in Networks and Computer Communications (ETNCC), IEEE International Conference on, pp. 402-40, **(2011).**

[11] Bibhash Roy, Pratim singha, “An improved symmetric key cryptography with DNA based strong cipher”. Devices and Communications (ICDeCom), IEEE, 2011 International Conference on 24-25 Feb. **(2011).**

[12] A. K. Verma, Mayank Dave, R.C. Joshi, “Securing Ad hoc Networks Using DNA Cryptography”, IEEE International Conference on Computers and Devices for Communication (CODEC06), pp. 781-786, Dec. 18-20, **(2006).**

[13] Yunpeng Zhang, Bochen Fu, and Xianwei Zhang, "DNA cryptography based on DNA Fragment assembly," In Information Science and Digital Content Technology (ICIDT), IEEE International Conference on, vol. 1, pp. 179-182, **(2012).**

[14] Wang Zhong, Zhy Yu, “Index-based symmetric DNA encryption algorithm”. Image and Signal Processing (CISP), 2011 4th International congress on image and signal processing, 15-17 oct. **(2011).**

[15] Olga Tornea, and Monica E. Borda, "Security and complexity of a DNA-based cipher," IEEE Roedunet International Conference (RoEduNet), 11th, pp. 1-5, **(2013).**

[16] Borda, Monica, and Olga Tornea, "DNA secret writing Techniques," In Communications (COMM), 8th IEEE International Conference on, pp. 451-456, **(2010).**

[17] Ashish kumar kaundal, “Feistel Inspired structure for DNA cryptography” in June **(2014).**

Authors

Tausif Anwar, obtained his B.Tech degree in Computer Science and Engineering from Bhadrak Institute of Engineering & Technology, Odisha in 2010. Currently he is pursuing Master of Engineering in Software Engineering from Birla Institute Of Technology, Mesra, Ranchi (India).

Dr.Sanchita Paul, is an Assistant Professor in Department of Computer Science & Engineering, Birla Institute of Technology, Mesra, Ranchi (India). She obtained B.E, M.E and Ph.D Degree in Computer Science and Engineering. Her area of Interests is Artificial Intelligence, Cloud Computing, Bioinformatics, NLP, Automata Theory, Design and Analysis of Algorithms.

Shailendra Kumar Singh obtained his B.Tech degree in Information Technology from UPTU (Lucknow) in 2012. Currently he is pursuing Master of Engineering in Software Engineering from Birla Institute Of Technology, Mesra, Ranchi (India).