Volume 3, Issue 7, July 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Modern Review on DNA Cryptographic Techniques

Rupali Soni[*]
PG Scholar
Department of Computer Science & Engineering
Central India Institute of Technology, Indore, India

Gopal Prajapati
Assistant Professor
Department of Computer Science & Engineering
Central India Institute of Technology, Indore, India

Abstract—In today's era as the rate of information storage and transformation is growing day by day; so as information security is becoming more important. To provide security to information there are various types of techniques as traditional cryptographic methods like Substitution techniques, Transposition techniques, hashing Functions and algorithms like DES , RSA, AES, IDEA, ECC etc. are used. DNA cryptography is also new emerging technique for providing security to data and information. The DNA cryptography uses Bio-molecular computational abilities of Deoxyribo Nucleic Acid. There are large amount of DNA researches have been performed to secure data and information form attack. By reviewing various current cryptographic techniques, this paper en-lights the comparison between them.

Keywords— DNA structure, DNA cryptography, DNA techniques, comparison, utilization.

I. INTRODUCTION

Data security and cryptography are critical aspects of conventional computing and may also be important to DNA database applications. Here we provide basic terminology, which is used in most of the cryptographic techniques. The goal is to transmit a message between a sender and receiver, such that an eavesdropper cannot understand the message [28]. In cryptographic system, Plaintext refers to a sequence of characters drawn from a finite set of alphabets, such as natural language, Encryption is the process of scrambling the plaintext using a known algorithm and a secret key and the output is a sequence of characters known as the cipher text. Decryption is the reverse process, which transforms the encrypted message back to the original message using a key [23]. The goal of encryption is to prevent decryption by an adversary who does not know the secret key. An unbreakable cryptosystem is one for which successful cryptanalysis is not possible. Such a system is the one-time-pad cipher. It gets its name from the fact that the sender and receiver each possess identical notepads filled with random data. Each piece of data is used once to encrypt a message by the sender and to decrypt it by the receiver, after which it is destroyed. Rest of the paper contains section II, which gives the knowledge of background of DNA cryptography. Section III introduces various related algorithms or techniques related to DNA cryptosystem. Section IV describes the comparison criteria between various techniques. Section VI describes the conclusion based on the observation of result obtained in the last section.

II. BACKGROUND

Modern cryptography consists of the interaction between the application of mathematics, computer science and engineering. There are many desktop and web applications which uses cryptography. Here the discussion is starting with the basic of cryptography to the current techniques.

A. *Cryptography*

Cryptography is way of achieving the security by converting or modifying the plaintext message into the cipher text message i.e. no one can understand the actual meaning of original message. In the modern information era as the evolution of e-money and online transactions are on the large scales, which require more secured and new cryptography techniques. Because The cryptanalysis which means to analysis and try to break the system proposed by the cryptography techniques runs parallel with the evolution of the cryptography techniques.[1]

B. *Cryptographic Branches*

There are some branches of the cryptography which are

a. Cryptographic engineering[31]
b. Multivariate cryptography[30]
c. Quantum cryptography[25]
d. Steganography[19]
e. Visual cryptography[29]
f. DNA cryptography[1]

Cryptographic engineering is mainly used for providing the confidentiality authenticity to the devices from unauthorized access and also provides the data integrity from the attacks [31].

Crypto Engineering = Efficient Implementation + Secure Implementation

Multivariate cryptography is also known as asymmetric cryptography. It is based on multivariate polynomial functions over finite fields [30]. Quantum cryptography is mainly used in key distribution mechanism. It is based on the Heisenberg uncertainty principal of physics [25].The Steganography is the process of hiding the message such that only intending recipient know about the existence of message [19]. The visual cryptography is the technique in which the visual information is encrypted in such a way that the decryption becomes mechanical operation with the help of human and which does not require any decryption algorithm [29]. The next section describes the DNA Cryptography in detail.

III. DNA CRYPTOGRAPHY

A. DNA

In human body to transform the genetic inform from one part to another part nucleic acids are present. There are two type of nucleic acid DNA and RNA which code for all type of instructions needed for the cell to perform different function. The DNA Stands for Deoxyribo Nucleic Acid. DNA is the molecule that contains the genetic code of organism. DNA is material that governs Genetic similarity of looks, nature in human and animals [6]. The DNA is having the complex structure shaped like a twisted ladder with four types of acids like A(Adenine),G(Guanine),T(Thymine)and C(Cytosine),which are used to store and transformation of information [32]. A strand contains a sequence of bases in specific patterns. This double helical structure is formed by the hydrogen bond between the T with C and G with A[1] as shown in figure1.

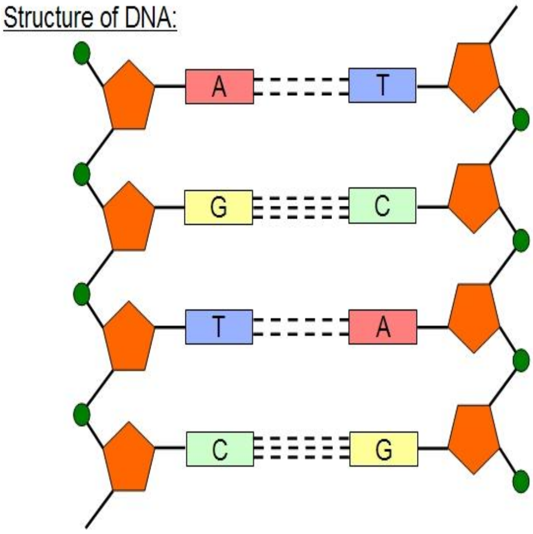

Figure 1 Structure of DNA

B. DNA Computing

DNA computing is also molecular computing, is a new approach to the massively parallel computing. This computing paradigm computes the problems using DNA sequence. It is used to resolve the varieties of problem in fractions of second. It is a form of computing which uses DNA Biochemistry and molecular biology instead of the traditional silicon based computer technologies [4]. This computing is having brighter potential in all the field such as Steganography, authentication, image encryption, data encryption, visual encryption, one-time pad etc.[9]

DNA strands store a large amount of data and complex information into the molecule or group of molecules, where 1gm of DNA can store 10^8 terabyte of data. It is also used to search possible solutions of the problem simultaneously which is represented by DNA strands [1].It is also used for secure communication over the medium without any attack threat, it provides key strength data confidentiality, key strength, non-repudiation, data integrity [1].DNA computing is the fast developing interdisciplinary area. Its' research and development is concerned with the theory, practical experiments and applications.

C. DNA Cryptography

DNA cryptography provides higher security to data, in this technique plain text message is converted in to DNA strength by using DNA sequence. This Cryptographic scheme was introduced in 1994 by Dr. Leonard M. Adelman of the University of Southern California to solve the complex mathematical problem. He found that the biological Deoxyribo Nucleic Acid have the high computation capabilities. He proves this technique by solving the NP-Complete Hamiltonian Path Problem of seven vertices [1].

It provides two fold securities by using complex computation. It uses bio-molecular method for encryption and decryption process, as the bio molecule has complex structure which is difficult to analyses easily. As above mentioned DNA is made up of four nucleic acid AGTC so, for encryption process the four acids are converted in to binary number such as 00,01, 10 and 11 respectively and may be manipulated in different ways or may be encoded in to the different sequence of binary numbers [10][16]. DNA cryptography is temperature dependent cryptographic method [11].

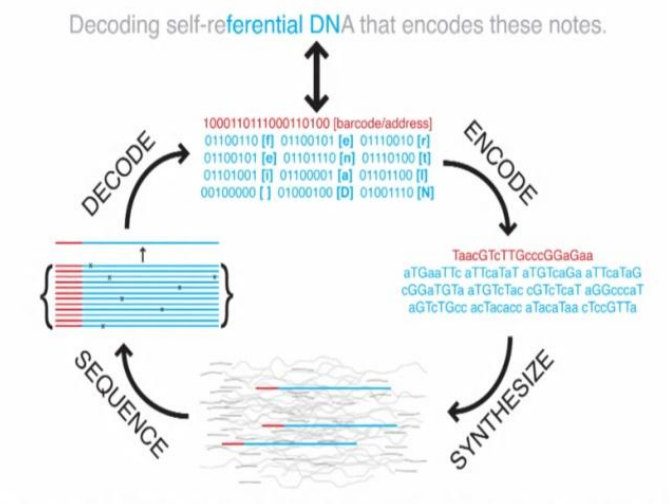
Decoding self-referential DNA that encodes these notes.
1000110111000110100 [barcode/address]
01100110 [f] 01100101 [e] 01110010 [r]
01100101 [e] 01101110 [n] 01110100 [t]
01101001 [i] 01100001 [a] 01101100 [l]
00100000 [ ] 01000100 [D] 01001110 [N]
ENCODE
TaacGTcTTGcccGGaGaa
aTGaaTTc aTTcaTaT aTGTcaGa aTTcaTaG
cGGaTGTa aTGTcTac cGTcTcaT aGGcccaT
aGTcTGcc acTacacc aTacaTaa cTccGTTa
SYNTHESIZE
SEQUENCE
DECODE

Figure 2: DNA Encryption and Decryption mechanism.

IV. DNA TECHNIQUES

There are various DNA Cryptography Techniques which has been developed; here some of the DNA techniques which are widely used and recently developed are shown:

A. DNA Digital Coding Polymers' Chain Reaction PCR

PCR stands for "Polymerize chain reaction". It is highly efficient amplification and quantification process of DNA [2]. DNA amplification is very difficult, to amplify the DNA strands, so PCR method is used. This method was invented by analysis of biological catalyst known as polymerase. These polymerases are present in a chaining fashion, which represent that the amplification process occurs in various cycles in chain one by one as a cascading manner. By applying PCR small DNA sequence can be dissolved in to samples containing very minute quantity of DNA. PCR amplification can be used for DNA cloning and clustering i.e. It having the nature of duplicating the DNA [7]. In short we can identify the PCR process in to two phases:

i. In first phase the two DNA chromosomes, are, merged into target DNA.

ii. In second phase the polymerase amplification process is applied for forming the target DNA.

PCR amplification is very sensitive method; it is affected by change in temperature.

B. DNA Based Bimolecular Cryptographic Design

Bimolecular cryptographic system scrambles the data into DNA code by using olignucleotide sequences [17]. It uses the one time pad (OTP) technique of cryptography which is based on the principle of unbreakable [13]. The actual experiment of cryptographic scheme follows OTP which are having limitation in transmission over convention electronic media because of the size of the OTP. DNA strands are very neat in design as storage media and small amount of DNA is enough for large amount of OTP[9].We use One time pad encryption, which uses a code book to scramble the part of small segment of plaintext message to cipher text message. The code book used here is a random code book i.e. One secret code is used only once for encryption and decryption, not repeatedly. The OTP of the plaintext message is distributed to both sender and receiver in advance [19].

DNA based bimolecular cryptographic encryption having following schemes:

1) Substitution

In substitution method the pair wise mapping is performed between the libraries of various pads, which are randomly generated. Here the encryption process is random and reversible, where plaintext is converted to cipher strands and plaintext strands are removed. Later on the DNA substitution uses long DNA pads which contain various parts, and each part have a cipher word followed by a plaintext word. Here the cipher word is attached with plaintext word to form word-pairs. It also acts as hybridization site for binding of primer. Word-pair here generated for DNA strands are used as a lookup table in scrambling of plaintext to cipher text.

2) XOR mapping

This XOR mapping uses molecular computation and index, random key strings. IT maps DNA strands in random reversible way in which plaintext is scrambled to cipher strands and plaintext strands are removed.

C. Symmetric Key Crypto System Using DNA

The symmetric system uses same key for the encryption and decryption process[23]. These are extremely fast and widely used for process on huge amount of data. It is having some threat of attack while transmitting over the communication media for example man in the middle. These are accessible by the external. In this method the plain text is converted DNA Sequence in which DNA Strands are used as the unique key for encryption and decryption [12].

D. Asymmetric Key Crypto System Using DNA

The Asymmetric system uses two different key for the encryption and decryption process [23]. we can also be called it as DNA-Public key cryptography. These are extremely fast and widely used for process on huge amount of data because it is much secure as compare to the symmetric key encryption process. It cannot be easily accessible by external users. In this method the plain text is converted DNA Sequence in which DNA Strands are used as the unique key for encryption and decryption [14].

E. DNA Steganography

Steganography is the technique of hiding secret message apart from the sender and receiver. DNA Steganography can be said to the supplement of the classical DNA cryptography. The DNA Steganography has a constraint that this method is open to attack [17].In this process the original message is covered by the DNA samples to a microdot size.

In the DNA Steganography encryption process, the original message is converted to DNA strands and those strands are combined with the other DNA strands to generate a dummy DNA strand of equal length and size. However the encryption is not of a primary importance in Steganography, therefore a simple substitution cipher can be encode to character in DNA triplets. In decryption process the secret key the dummy DNA strands are amplified by applying PCR process. The cipher message will be converted into original message only by the intended recipient who knows the PCR primer or key or PCR strands sequence.

F. Pseudo DNA Cryptography Method

Pseudo DNA cryptography is varying from DNA cryptography. This method depends on the function of the DNA not on the DNA strands. In this method the scrambling and unscrambling process is based on the flow of genetic information within biological system [15] .Sender translate mRNA form of the data into protein according to genetic code table. The key are send to receiver in a secure channel.

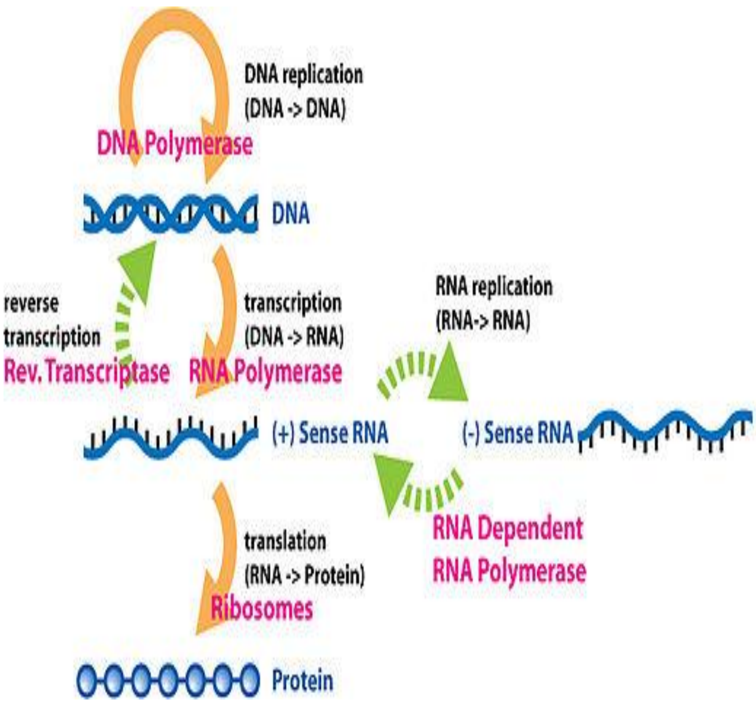

Figure 3: DIAGRAM OF Flow of genetic information

G. DNA Chip Based Technologies

DNA Chip technology uses micro arrays of molecules which are restrict over the solid surface for biochemical analysis. DNA Chips are useful in manipulating the large amount of data from genome sequencing and to find parallel expression of various genes [5]. DNA Chip contains the array of moles of DNA Sequence called as probe. The encryption and decryption process in DNA Chips are not stable as the property of nucleotides changes with the climatic or surrounding conditions [18].

H. Chaotic coding

Chaos encoding is the behavioural study of the dynamic systems which are very much dependent on the initial condition. Chaos means the state of disorder. We should follow the following properties.

1. It must be dependent on initial condition.
2. It must be topologically mixed.
3. It must have dense periodic orbits.

Cycling chaos is used for encoding of image pixels positions and rearranging the pixels grey value by using DNA sequencing masking. When a random process is occurring in a non-liner dynamic system, it is said to be chaos. Chaotic systems are mainly used for the dynamic systems. This method is vilely used in image encryption. DNA primers store the encoded image pixels into the form of matrix [36].

Image encryption is done by

$$A_{k+1\,=}\ \mu.a_k.\ (1-a_k)$$

Where a_0 is initial condition it varies between 0 and 1. µ is the control parameter having value between 0.3 <µ <4[27].

V. Comparison Of Various Techniques

Here is the table showing the comparison working of different techniques of DNA Cryptography.

Table 1: Comparison between various Techniques

S. No.	DNA Cryptographic Technique	Working
1	DNA Digital Coding Polymers' Chain Reaction PCR	This technique use POLYMERIZE chain reaction for the amplification for the DNA Strands [26].
2	DNA Based Bimolecular Cryptographic Design	This cryptographic method uses one time pad (OTP) and dynamic code book[17]
3	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. [12]
4	Asymmetric Key Crypto System Using DNA	This technique uses a Dual DNA strand key, one for encryption and another for decryption process.[14]
5	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[15].
6	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[21][28].
7	Chaotic coding	This coding uses pseudo-randomness and deterministic which are two features of chaotic systems. Also it is dependent on the initial condition [20][27].

VI. Conclusion

The DNA Cryptography is the art of securing data using the DNA Sequences. This process uses various techniques as all techniques mentioned above in the paper. Each technique has different algorithms for Encryption and Decryption of the information. This paper represents detail study and comparison between the various techniques and algorithms used for DNA cryptography.

References

[1] L. Adelman, "Molecular computation of solutions to combinatorial problems, "Science in JSTOR, vol. 266, pp. 1021–1025, 1994.

[2] G. Cui, Y. Liu, and X. Zhang, "New direction of data storage: DNAmolecular storage technology,"Computer Engineering and Application,vol. 42, no. 26, pp. 29–32, 2006.

[3] J. Chen, "A DNA-based, biomolecular cryptography design," in IEEE International Symposium on Circuits and Systems (ISCAS), 2003, pp. 822–825.

[4] G. Cui, L. Qin, Y. Wang, and X. Zhang, "An encryption schemeusing DNA technology," in IEEE 3rd International conference on Bio-Inspired Computing: Theories and Applications (BICTA08), Adelaid, SA,

[5] L. MingXin, L. XueJia, X. GuoZhen, and Q. Lei, "Symmetric-key cryptosystemwith DNA technology," Science in China Series F: InformationSciences, Springer Verlag, Germany, vol. 50, no. 3, pp. 324–223, 2007.

[6] L. H. N. C. for Biomedical Communications, Handbook on GeneticCells and DNA. USA: National Library of Medicine, National Institute of Health, Department of Health and Human Services., 2010.

[7] T. Kazuo, O. Akimitsu, and S. Isao, “Public-key system using DNA asa one-way function for key distribution,” BioSystems, Elsevier Science,vol. 81, no. 1, pp. 25–29, 2005

[8] J. Fuscoe, W. Branham, C. Melvin, V. Desai, C. Moland, T. Han, L. Shi,W. Tong, A. Scully, and R. Delongchamp, “Technical issues involvedin obtaining reliable data from microarray experiments,” RegulatoryResearch Perspective, National Center for Toxicological Research, USA, vol. 6, no. 1, pp. 1–22, 2006.

[9] A. Gehani, T. LaBean, and J. Reif, DNA based cryptography. Germany:Aspects of Moleculer Computing, Springer-Verlag., 2004.

[10] M. Amosa, G. Paun and G. Rozenbergd. “Topics in the theory of DNA computing,” Theoretical cience, vol. 287, pp. 3–38, 2002.

[11] G. Z. Xiao, “New field of cryptography: DNA cryptography,” Chinese Science Bulletin, vol. 51, pp. 1139–1144, 2006.

[12] LU MingXin, “Symmetric KeyCryptosystem With Dna Technology” Science China pp 324-223,June 2007.

[13] J Chen “A DNA-based, Bimolecular Cryptography Design”ISCAS'03.Proceedings2003

[14] LAI XueJia, LU MingXin “Asymmetric encryption and signature method with DNA technology” Vol. 53 No. 3: 506–514 March 2010.

[15] Ning Kang, A pseudo DNA cryptography Method, http://arxiv.org/abs/0903.2693 ,2009.

[16] Monica Borda, “DNA secret writing Techniques” IEEE conferences 2010.

[17] Ashish Gehani, Thomas H. LaBean and John H. Reif “DNA-based Cryptography” 5th Annual DIMACS Meeting on DNA Based Computers(DNA 5), MIT, Cambridge, MA, June 1999.

[18] V. M. M. Shyam, N. Kiran, “A novel encryption scheme based on dna computing,” in 14th IEEE International Conference, Tia, India, Dec.-2007.

[19] A. Gehani, T. LaBean, and J. Reif, DNA based cryptography. Germany:Aspects of Moleculer Computing, Springer-Verlag., 2004.

[20] Kuldeep Singh ,Komalpreet Kaur “Image Encryption using Chaotic Maps and DNA Addition” Operation and Noise Effects on it, International Journal of Computer Applications (0975 – 8887)Volume 23– No.6, June 2011

[21] M Gabig, G Wegrzyn, “An introduction to DNA chips: principles, technology, applications and analysis.”, Department of Biotechnology, Royal Institute of Technology, Stockholm, Sweden. Acta biochimica Polonica (impact factor: 1.49). 02/2001; 48(3):615-22. Source: PubMed

[22] V.I.Ricsa, “DNA based steganography”, cryptologia, tylor & francics, vol 25 no. 1 pp 37-49,2001.

[23] Atul Kahate Cryptography and Network Security - Third Edition (McGraw-Hill)

[24] William Stallings, “Cryptography and Network Security”, Third Edition, Prentice Hall International -2003.

[25] Elliott. C. “Quantum Cryptography” in Security and privacy, IEEE volume 2 issue 4

[26] Y. Zhang, D. Zhou, L. HE, Y.H. Karanafil, B. FU, “A new DNA Cryptogram Scheme based on PCR technology” in JATIT volume 45, 15-Nov-2012

[27] Aradhna Soni, Anuja Kumar Acharaya,”A Novel Image Encryption Approach using an Index based Chaos and Encoding and its Performance analysis”, in IJCA volume 47, June-2012.

[28] Justin Zhan, Luis Cabrera, Gasim Osman, Ronak Shah, “Using Private Matching for Securely Querying Genomic Sequences” in IEEE International Conference on Privacy, Security, Risk, and Trust, and IEEE International Conference on Social Computing, 2011

[29] Jena D, “A novel visual Cryptographic Scheme”, in IEEE conference, ICACC, 2009, Singapore

[30] Danilo Gligoroski and Simona Samardjiska,” The Multivariate Probabilistic Encryption Scheme MQQ-ENC”, http://eprint.iacr.org/2012/328.pdf

[31] Christof Paar, “Crypto Engineering: Some History and Some Case Studies”, nvited Talk. CHES 2009. EPFL Lausanne, September 6-9, 2009

[32] J. D. Watson, F. H. C. Crick, “A structure for de oxy ribose nucleic acid”, Nature, vol. 25, pp. 737-738, 1953