ANALYSIS OF DNA CRYPTOGRAPHY'S IMPROVEMENTS FOR THE MODELING OF SECURED CORPUS

Animesh Kairi[1*], Tapas Bhadra[2], Arindam Roy[3], Tufan Saha[4], Madhab Chandra Samanta[5], Sameek Bhattacharya[6]

Abstract

The development of cryptography and cryptographic analysis are regarded as active research trends, as security is one of the major concerns of civilized society. The present paper focuses on DNA cryptography. It is known for the discovery of Deoxyribonucleic Acid's computing capability (DNA). The work has been carried out with the help of several molecular manipulation techniques. In the present work, DNA is used as the computational tool in DNA cryptography. This topic is becoming quite promising since DNA has a very large capacity for storing information. It is an emerging area which is going to explore lots of effort for further implementation. This article outlines the paths that need to be further explored in the area of DNA cryptography by examining all the possibilities and cutting-edge technology of recent trends.

Keywords: DNA Cryptography, DNA Computing, Encryption, Decryption

[1*]Institute of Engineering & Management, Kolkata, India, Email: ani.kairi@gmail.com
[2]Aliah University, Kolkata, India, Email: tapas.bhadra@aliah.ac.in
[3] Institute of Engineering & Management, Kolkata, India, Email: arindammtech@gmail.com
[4] Institute of Engineering & Management, Kolkata, India, Email: tufan.saha@iem.edu.in
[5] Institute of Engineering & Management, Kolkata, India, Email: madhab.samanta@iem.edu.in
[6] Institute of Engineering & Management, Kolkata, India, Email: bhattacharyasameek@gmail.com

***Corresponding Author:** Animesh Kairi
* Institute of Engineering & Management, Kolkata, India, Email: ani.kairi@gmail.com

DOI: 10.48047/ecb/2023.12.si10.00467

I. INTRODUCTION

Using molecular methods, DNA is used as a transport of information and computation in DNA cryptography, a novel area of cryptography. It is still a very new field which developed following the revelation of the processing capacity of Deoxyribonucleic acid (DNA) [1]. Due to the DNA's ability for storing, which serves as the primary computational unit in this field, DNA cryptography is attracting greater interest. In one gram of DNA, there are approximately 108 trillion bits. This has a greater storage capacity than any other storage like magnetic storage, optical storage, or electrical storage medium [2,3]. For instance, Barish et al. showed a tile system that uses DNA to transform input into output [4]. The study of DNA cryptosystems is still in its infancy. So, there are many other dimensions to the study that may be done in this new sector. Both of these aspects still need to grow, therefore work has to be done from theory to actuality. A recent study found that several essential DNA research methods, including DNA synthesis, DNA digital coding, and the Polymerase Chain Reaction (PCR), have just recently been developed [12]. Conventional cryptography methods have a rich history and are based on solid mathematical and theoretical principles. Real-time activities may also be found using conventional security systems like RSA, DES, or NTRU. This study presents a straightforward comparison of conventional and DNA cryptography techniques. It explores the methods now employed in this subject and provides an understanding of the advantages that DNA cryptography may bring about. It also emphasizes the necessity of combining conventional and DNA cryptographic approaches so that emerging cryptographic systems can profit from both disciplines. It also examines the necessity for more study in this area to reach the realization stage and identifies certain gaps in the field. This essay's remaining sections are organized as follows: The background on the field of the use of cryptography genetic material, and the cryptography of DNA is provided in Section [II], along with an outline of the fundamental knowledge needed to comprehend DNA cryptography. This section also explains a typical cryptographic scenario that will be used in subsequent sections. The techniques used in DNA cryptography are discussed in Section [III]. Section [IV] will cover what has already been accomplished and what is still outstanding. Section [V] then comes to a conclusion.

II. BEGINNINGS AND CONNECTED WORK

Modern cryptography makes use of interdisciplinary linkages among the fields of computing, biology, engineering, and mathematics. Cryptography has a variety of uses, including e-commerce, computer authentication, and online banking. First, the most basic form of cryptography is presented, and then improvements are demonstrated. Cryptography forms the foundation of the security of all information. Cryptography is a very important and often utilized discipline. Although it is an extremely old profession, its importance has expanded in current times as a result of the growing usage of the internet. Web applications are now being developed for all manual processes, most notably the banking, defence, and commerce systems. Sensitive information transmitted over the internet may be targeted by several security concerns, including tampering, man-in-the-middle attacks, droplet attacks, and others [13]. We rely on the power of encryption to protect our systems and applications. Cryptanalysis works in tandem with cryptography. Analysis and attempts to circumvent the security measures provided by the cryptography sector are the objectives of cryptanalysis [14]. In other words, the degree to which a cryptosystem is susceptible to cryptanalysis determines its level of strength [15].

The study of cryptanalysis and cryptography has received a lot of attention. As a result, several technologies (such as RSA, ECC, and others) have been developed to attain a high level of security.

In cryptography, a typical scenario is that Alice (sender) wishes to convey certain information surreptitiously to Bob (intended receiver). Plain text communication is written in everyday language that everyone understands. Encryption is the process of transforming plaintext into a form that cannot be understood without specific information. The precise information is referred to as the encryption key, and this unintelligible format is known as cypher text.

Decryption is the conversion of cypher text back into plain text using special knowledge, whereas the decryption key is the special knowledge used for decryption. Only the recipient knows this particular information, and only the receiver may decrypt a cypher text using this special knowledge, known as the decryption key. Traditional cryptography uses techniques for which there is now no viable fix to encrypt data and decode it [6]. The three most significant branches or subfields of cryptography are Contemporary cryptography, Quantum cryptography and DNA cryptography. These three sectors are dependent on several challenging issues from other disciplines for which

there is now no recognized answer. Modern cryptography is built on challenging mathematical puzzles like the elliptic curve issue and prime factorization, for which there is now no known solution. DNA cryptography relies on challenging biological procedures related to DNA technology, such as:

i)Polymerase Chain Reaction (PCR) for a sequence without knowing the right two primer pairs [6], [12], based on the physics' Heisenberg uncertainty principle, which is a relatively recent subject.

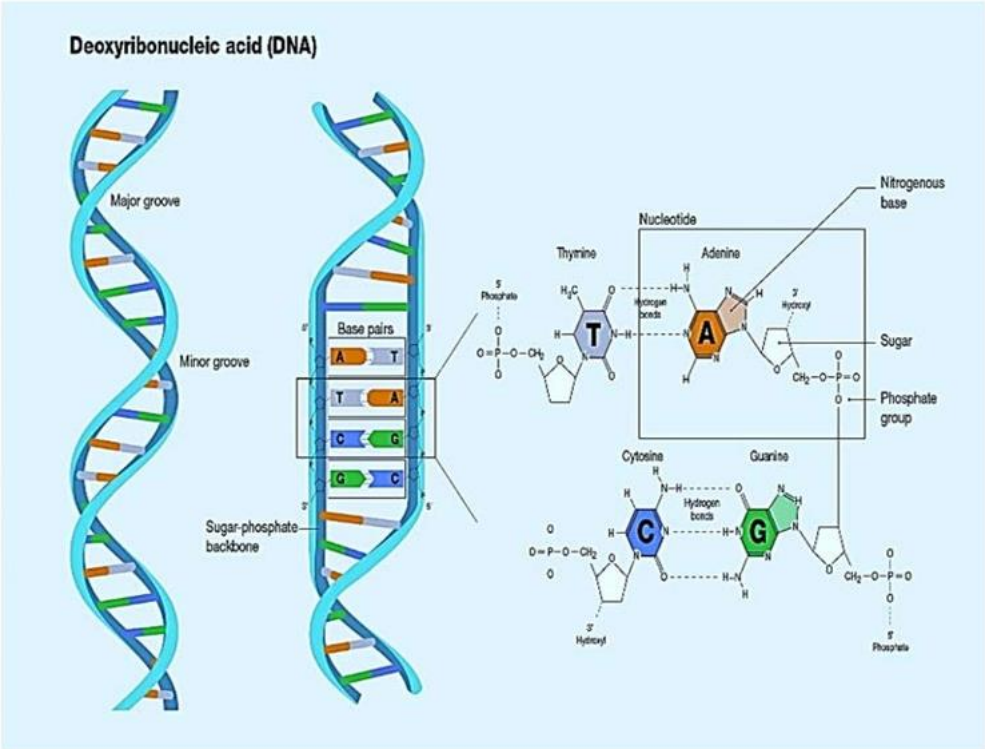

Fig. 1 Structure of DNA

ii) The approach involves reading data from a DNA chip without being aware of the sequences that are present in various locations [16].In Section 3, a thorough description of these techniques is provided.

The structure of DNA is shown in Figure 1. Deoxyribonucleic acid (DNA) is the genetic makeup of nearly all living things, from tiny viruses to intricate humans [17]. All biological forms use it as a data transport. The sort of nitrogenous base that each of the four nucleotides has determines which of them they are. Adenine, Cytosine, Thiamine, and Guanine are the four distinct bases respectively [18,19]. Figure 1 depicts the double helix structure of DNA, which consists of two strands running counterclockwise.

The lengthy polymer of nucleotides that makes up DNA is tiny. Each nucleotide is made up of three parts:

i) A nitrogenous base
ii) A sugar with five carbons.
iii) A phosphate group

Before 1994, it was thought that DNA contained solely biological information, but Adleman's solution of the NP-complete Hamiltonian route problem with seven vertices [1] disproved this notion and demonstrated DNA's computing capabilities. DNA uses only the characters A, C, T, and G to store the enormous and complex information of an organism's genome. These bases build the framework of DNA strands by forming bonds of hydrogen with each other to hold the two segments of DNA together. A makes a hydrogen connection with T whereas C and G establish bonds with each other [20]. Figure 1 shows it clearly.

The discipline of cryptography meets all requirements for safe communication across an insecure medium, including authentication, nonrepudiation, key exchange, privacy, and confidentiality. As previously noted, DNA offers a great way to safeguard data; this method is known as DNA cryptography. Such methods employ an alphabet of oligonucleotide sequences to encode plaintext message data as DNA strands. Natural DNA obtained from biological resources may be captured with unusual bases to facilitate further

processing [1], [17]. The input and output of DNA data from DNA chip arrays may be transferred to a conventional binary storage medium. where oligonucleotide sequences can be utilized to encode digital data in DNA strands in a tiny alphabetical fashion.

While DNA cryptography works with the DNA strands that are altered by biological methods, traditional cryptography often uses computers through a network and silicon chips as its store media. By integrating both biological and computational challenges, DNA cryptographic approaches offer two-fold security when comparing the security offered by the two techniques. Traditional cryptography solely depends on computational problems, therefore security may be said to be one-fold.

III. DNA CRYPTOGRAPHY USES COMPLEX BIOLOGICAL PROBLEMS

Biological techniques are used for both encryption and decryption in DNA cryptography. The most well-known cryptographic methods among these are DNA chip technology [16] and PCR, or polymerase chain reaction [6,12]. However, there is also research on DNA steganography. The following describes each of these methods.

i) Polymerase Chain Reaction (PCR)

The PCR technique amplifies and measures DNA. PCR architecture aims to boost the quantity of DNA because it is very difficult to cope with a small number of DNA strands. The term "polymerase chain reaction" implies the use of enzyme (biological catalyst) polymerase in the technique, and the word "chain" denotes the repetition of the amplification process across several cycles. Short DNA sequences can be analyzed with PCR, even in samples with minuscule amounts of DNA. Small DNA strands can be chosen by PCR and amplified. Amplification of DNA typically includes cloning target segments into vectors for expression. Due to PCR's tremendous efficiency, little amounts of chosen DNA may be used to create an infinite number of copies. Additionally, PCR makes use of the same chemicals that nature employs to replicate DNA. To make the appropriate starting point, which is a pattern that contains a few nucleotides that are complementary to the specific DNA sequence that has to be amplified, one must be conscious of the exact sequence of DNA that requires amplifying to do PCR [6]. The PCR procedure could be split into two steps, which are:

i) Short single-stranded DNA sequences called "primers" that mark the beginning and conclusion of the DNA stretch are used.
ii) The polymerase enzyme, which travels along the DNA segment, reads its instructions and puts the copy together.

In this instance, the encryption key is composite and is made up of a pair of PCR primers and a public key. Comparably, the private key and complementary primer pairs make up the decryption key.

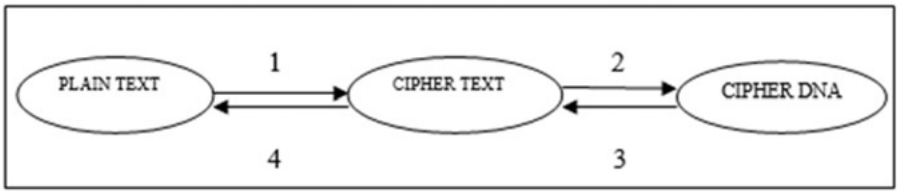

Fig. 2 Summary of the PCR-based cryptographic method

Through the use of a secure channel, Alice and Bob exchange two primers (forward and reverse) to begin the encryption process [6].

The produced cypher DNA is then combined with a variety of other unidentified DNA while being flanked by the covert primers. Bob receives this DNA combination from Alice [6]. By running PCR using the cypher DNA's secret primer and reversing the whole encryption process, Bob may obtain the cypher DNA for decryption [6]. The target cypher DNA cannot be recovered without knowing the two primers [12]. Figure 2 illustrates stages 3 and 4 of decryption. Number 3 in the same diagram indicates that the cypher DNA may be decoded using secret primers and then turned into cypher text using a coding method. The encrypted text is finally deciphered by the RSA private key, as indicated by the number 4 in the picture. For encryption, pre-processing is possible so that the entire technique, such as RSA, can be performed first. This procedure is designated as Step 1 in Figure 2. Then, the text encrypted may be converted into a DNA sequence using the coding scheme illustrated in number 2 in Figure 2. This results in a completely new cypher text being produced [6]. In literature, the terms "cypher DNA" and "plain text DNA" refer to cypher text and plain

text, respectively, both of which take the form of DNA sequences.

ii) DNA-based Steganography

Stenography is a technique for hiding information. While cryptography strives to make data inaccessible to a third party, steganography aims to hide the information from a third party. A very general explanation of the stenographic procedure is given in the formula at equation 1: a + b + c = x (1)

Where a= cover medium, b= hidden data, c= key stego and x= stego medium.

The file that contains the concealed data is referred to in this context as the cover medium. Another key called key stego may also be used to encrypt the resulting file. Finally, the file that will be transferred is the stego medium. Typical file-covering media include audio and picture files. However, DNA is becoming more and more popular as a steganography covering medium because of its enormous storage capacity.

The basic concept behind DNA steganography is as follows. One or more input DNA strands are chosen and marked as the plaintext message for encryption. The input DNA is supplemented with one or more secret key strands that were created randomly. The resulting "tagged plaintext" DNA strands are concealed by blending them with several other "distracter" DNA strands that may likewise be created through random assembly. A variety of possibly known recombinant DNA separation techniques may be used to decrypt DNA strands if the "secret key" strands are known. For example, the complements of the "secret key" strands might be put in solid support on magnetic beads or a prepared surface, allowing the plaintext message strands to be sorted out by hybridization.

One such approach is presented in [26]. DNA and common biological procedures are used in the steganographic method that Viviana I. Risca suggested. The suggested approach encrypts the data in the DNA strand sequence is surrounded by two hidden primers. aimed towards areas. It employs monoalphabetic encryption.40 random but distinct 3-base DNA codons must be assigned, punctuation and alphanumeric characters. Then came the key plaintext texts into the basic sequence of an oligonucleotide that has been artificially created. The resulting DNA strand is then encased in an enormous number of junk DNA strands of identical size. To take out one must be aware of the primers needed to bind the message. Orderly areas on the DNA strand that contains the message magnify the needed molecule with precision.

Asish Gehani et al. [15] suggest an enhancement because this crude approach is straightforward and readily compromised. The objective is to distinguish between a plaintext source's probability distribution and a distracted DNA strand [15]. As previously stated, DNA-based steganography converts plaintext into plain text DNA rather than encrypting it. Simply said, it makes the plaintext DNA difficult to detect and amplify for anyone who doesn't know the primer by blending it into a significant amount of other DNA. This approach can reduce the cost of encryption, but it is vulnerable to statistical analysis. As a result, PCR-based encryption is considered to be more secure [6], [22].

iii) Technology using DNA Chip

A brief overview of DNA chip innovation is given to help explain the concept behind this cryptography strategy. In fewer than ten years, genetic chips and microarrays have changed how researchers do their studies. Researchers may manipulate the enormous volumes of data from genome sequencing thanks to DNA chips [27]. Technology based on DNA chips is crucial for manipulating biological data.

It is frequently employed to determine the parallel expression of several genes [11]. Data in the form of DNA sequences may be handled and stored on these chips, which are similar to silicon chips.

To create DNA chips, several locations are inserted on a stable surface, most typically a glass slide. There are various types and numbers of probes at each location. Short nucleotide sequences known as probes can attach to complementary nucleotides. The nucleotides that connect to these probes when any sequence of DNA binds to them are luminously tagged.

According to the ratio of the probe's binding to the DNA in each place, data is electronically computed while the object is seen under a laser dye [28], [29]. Smaller biochips with improved information processing capabilities are now being developed by manufacturers, and these chips will be more useful for research in many areas, including cryptography. The method includes the stages listed below, taking into account a common cryptographic scenario:

- The encryption key is an assortment of specified probes, whereas the decryption key is a combination of identical probes with

complementary sequences. The key that unlocks the encryption is then securely sent to Bob.

- Plaintext is used to build binary data. The resulting binary format is then inserted into the genetic material chip (cypher DNA) as a cypher text. Without the decryption key, it is impossible to read plaintext information from the DNA chip.
- Bob combines the cypher DNA using the decryption key. He can extract plain text using computer software [16]. The XOR One-time-Pad cryptosystem [15] is one example. Using DNA chip technology, a one-time pad is created by grouping many copies of a single sequence into a tiny pixel on an array of immobilized DNA strands. The strands can be addressed visually. There are several ways to synthesize unique DNA sequences at each optically accessible point of the array. Combinatorial synthesis is one of the well-known examples of such a technology, which is carried out concurrently at several places. In 4n chemical processes, the 4L sequences are synthesized to create oligonucleotides of length L. A significant prefix number of length L0 is appended to a plaintext message as encryption. An additional element to the unencrypted message tag is created by introducing a unique prefix index tag with identical size L0 to the one-time-pad gene sequence. Using annealing and ligation, each suitable pair of unencrypted texts and a one-time-pad pattern is concatenated. The message is then encrypted using the bitwise XOR technique. Equation 2 depicts the XOR process with C standing in for the cypher data or sections, M for the plaintext message, and S for a set of bits that are spread randomly.

$$C_i = M_i \oplus S_i \quad \text{for } i=1\ldots n \qquad (2)$$

The plaintext strands are discarded and the pieces of the plaintext are transformed into cypher strands. As illustrated in Equation 4-5, the bit-wise XOR operation's commutative feature is exploited for decryption.

$$Ci \oplus Si = (Mi \oplus Si) \oplus Si \qquad (3)$$
$$= M_i \oplus (S_i \oplus S_i) \qquad (4)$$
$$= M_i \qquad (5)$$

The DNA symmetric-key encryption system (DNASC), developed by MingXin et al. using DNA chip technology, is a method of symmetric key encryption. Lai et al. recently proposed an asymmetrical data encryption system using DNA semiconductor technology and have also created fingerprints using this type of DNA chip innovation [30]. This system would allow Alice and Bob to authenticate one another. There are encryption techniques that use DNA chip technology that are not just limited to encrypting text; they can also be used to encode and decode pictures. Gehani et al. created one such cryptosystem in which they created to encrypt and decrypt 2D images, they developed a substitution one-time-pad technique. It's crucial to emphasize that they additionally used PCR for amplifying certain DNA strands [15]. In their study, Shyam et al. employed similar techniques to construct plaintext and encrypted text pairs on images using DNA chipping [31]. They also proposed a cryptosystem. Despite offering a wide range of concurrent information processing abilities, DNA chips' current applicability is constrained by their interoperability with other storage media.

IV. FUTURE SCOPE

There are a lot of benefits that seem to be related to DNA cryptography. DNA has an enormous amount of storage, which makes it a particularly alluring subject for study. Additionally, it is thought that the cryptographic methods created by including this field will provide a very high level of security [6].

According to the research on DNA cryptography that has been done so far, it is possible to create several DNA-based techniques to crack existing cryptosystems.

The foundation of modern cryptosystems is frequently RSA public key encryption. The vulnerability of prime factorization is a prerequisite for RSA public key encryption because there are no known efficient methods for finding the prime factors of extremely large numbers. Equation 6 demonstrates

$$n = p * q \qquad (6)$$

Finding p and q, wherein p and q are prime numbers, is impossible when n is an extremely large number. Any method that can determine how to calculate a given "n" will cause the entire RSA scheme to fail.

There are techniques for breaking the RSA system that have been created for DNA cryptography. Using self-assemblage of DNA tiles, these techniques utterly ruined the RSA system [32], [9]. If these techniques are successful in cracking RSA, then RSA will be useless. ECC is a type of cryptography that is used for both key exchange and digital signatures. The difficulty of solving the discrete logarithm issue for elliptic curves determines the security of these cryptosystems [33]. DNA-based strategies have been created to break elliptic curve-based cryptosystems. These methods have produced an equivalent multiplier,

divider, and adder for accumulating elements on elliptic curves by using basic biological operations [34].

One-time pads are cyphers—encryption methods—that only require a single key. The OTP cypher is theoretically 100 per cent secure. DNA can be used to make a key area for OTP encryption because of its vast storage capacity. Several areas need to be improved. For any form of cryptographic system, for example, time and computing difficulty are two of the most important elements. DES, RSA, and other incredibly efficient classical cryptography algorithms take a lot less time than DNA encryption, which deals with modifying DNA sequences [8], [9]. A further risk of DNA cryptography is that it might not work if the encryption algorithm DNA is tainted by undesired DNAs. This can be controlled by using caution and maintaining the lab's cleanliness. Additional research is still required to overcome the reliability issues. To summarize the entire conversation, the following elements are crucial
i) It is feasible to determine that PCR-based cryptography methods use two keys for encryption and two decryption keys. The RSA open-source cryptosystem used the (n, e) combination of keys as one set of decryption and encryption keys. The primers in question had to be safely transferred among Alice and Bob because specific primer pairs are required to recover DNA. This means that the primer pairs, coupled with the public as well as the private keys, must be supplied in secret. In encryption with a public key, just one shared knowledge exists, and that is Bob's confidential key. This approach also requires the covert delivery of primer pairs [6].

Since primer pairs are made up of groups of nucleotides, the environment might affect these molecules. To consider this, conditions in the environment should be maintained throughout the transit process.

Another strategy is to send Bob the primer pair's A, C, T, and G sequence in electronic format, much as how keys are transferred when using traditional cryptographic techniques. Bob can then make his primer set in the lab using the sequence Alice has provided. The environment should remain the same during the course of this process. ii) Systems for DNA steganography can be used in addition to conventional DNA cryptography, however, they include flaws that could be discovered.

Different DNA steganography techniques can be broken with a few assumptions about the information-theoretic sensitivity of plaintext messages. The procedure is probably brute force because of the advancement of computing technologies. To make things better, plaintext communications can be reduced before being encrypted, although in this case, unencrypted messages must first be handled. Therefore, it is not known whether or not impenetrable DNA steganography systems can be developed using natural DNA plaintext input. The plaintext DNA has been imprinted with primers and cloaked in other waste DNA that is the same duration as the plaintext DNA using the DNA steganography approach. This is a simple method for ensuring confidentiality.

The same issue might arise if environmental conditions change how DNA attaches to the primer. Furthermore, the primer may attach to additional junk DNA, making it difficult to separate the original unencrypted DNA [6], [22].

iii) The arrays of Pico bugs make up DNA chips. DNA sequences are known as "probes." Given that an array can accommodate numerous probes, a DNA microchip can do multiple computations simultaneously. However, DNA chip data is challenging to transfer across standard storage mediums due to the lack of uniformity in manufacturing, operations, and analysis methodologies [35]. This problem is referred to as an interoperability difficulty in bioinformatics. Furthermore, it can be demonstrated that DNA cryptography uses DNA chip technology for both decryption and encryption processes.

Being a biological molecule, DNA's characteristics are influenced by its surroundings. For instance, altering environmental factors can alter DNA's capacity to attach to other nucleotides. As a result, the encryption and decryption processes are unstable. Because of this unpredictability, decryption as well as encryption may provide a variety of outcomes depending on the context.

Conventional encryption, which is still in use, cannot completely be replaced by DNA cryptography. For this field to be in a place where it can be used practically, a lot of research and work must be done. There is a need for knowledge sharing between experts in classical cryptography and DNA technology, and cryptosystems should be designed so that users can gain advantages from both domains.

V. CONCLUSION

DNA computing led to the development of DNA cryptography, a relatively recent topic of study in cryptography. In this specific discipline, DNA serves as the implementation method while biotechnology, like PCR, serves as the communication carrier. For encryption, authentication, and permission, DNA molecules are used because of their lavish storage capacity and parallel computability. Polymerase Chain Reaction (PCR), DNA steganography, and DNA chip technology are the current DNA cryptography methods covered in this study. The benefits, potential trends, and several issues have also been highlighted in the summary of DNA cryptographic research's advancement. All three types of cryptography have their benefits and drawbacks, and in upcoming security applications, they may be thought of as a complement to one another. However, the lack of theoretical support and practical approaches that can be quickly used in the security area is noted as a challenge in DNA cryptography.

The DNA molecule's computing ability might open the door for additional biological molecule-based computation methods. Once DNA cryptography has been developed and examined, efforts may be made to convert the cypher DNA into cypher proteins or RNA, which can offer another degree of security for us. It won't be feasible unless considerable research is done and DNA computing is used in real-world applications.

REFERENCES

1 Adleman, Leonard M. "Molecular computation of solutions to combinatorial problems." science 266.5187 (1994): 1021-1024.

2 Cui, G. Z., Y. Liu, and X. Zhang. "New direction of data storage: DNA molecular storage technology." Computer Engineering and Applications 42.26 (2006): 29-32.

3 Chen, Jie. "A DNA-based, biomolecular cryptography design." 2003 IEEE International Symposium on Circuits and Systems (ISCAS). Vol. 3. IEEE, 2003.

4 Barish, Robert D., Paul WK Rothemund, and Erik Winfree. "Two computational primitives for algorithmic self-assembly: Copying and counting." Nano letters 5.12 (2005): 2586-2592.

5 Rothemund, Paul W. K., Nick Papadakis, and Erik Winfree. "Algorithmic self-assembly of DNA Sierpinski triangles." PLoS Biology 2.12 (2004): e424.

6 Cui, Guangzhao, et al. "An encryption scheme using DNA technology." 2008 3rd International Conference on BioInspired Computing: Theories and Applications. IEEE, 2008.

7 Boneh, Dan, Christopher Dunworth, and Richard J. Lipton. "Breaking DES using a molecular computer." DNA-based computers 27 (1995): 37-66.

8 D. Beaver, “Factoring: The DNA solution,” in 4th International Conferences on the Theory and Applications of Cryptology. Wollongong, Australia: Springer-Verlag, Nov. 1994, pp. 419–423.

9 Y. Brun, “Arithmetic computation in the tile assembly model: Addition and multiplication,” Theoretical Computer Science, Science Direct, Elsevier, vol. 378, no. 1, pp. 17–31, 2007.

10 Pelletier, Olivier, and Andre Weimerskirch. "Algorithmic self-assembly of DNA tiles and its application to cryptanalysis." arXiv preprint cs/0110009 (2001).

11 X. C. Zhang, “Breaking the NTRU public key cryptosystem using self-assembly of DNA tilings,” Chinese Journal of Computers, vol. 12, pp. 2129–2137, 2008.

12 Tanaka, Kazuo, Akimitsu Okamoto, and Isao Saito. "Public-key system using DNA as a one-way function for key distribution." Biosystems 81.1 (2005): 25-29.

13 Galbreath, Nick. Cryptography for Internet and database applications: developing secret and public key techniques with Java. John Wiley & Sons, 2003.

14 A. Menezes, P. Oorschot, and S. Vanstone, Handbook of applied cryptography. CRC Press, 1996. [15] A. Gehani, T. LaBean, and J. Reif, DNA-based cryptography. Germany: Aspects of Molecular Computing, Springer-Verlag., 2004.

16. Lu, MingXin, et al. "Symmetric-key cryptosystem with DNA technology." Science in China Series F: Information Sciences 50 (2007): 324-333.

17. Suresh Babu, E., C. Nagaraju, and M. H. M. Krishna Prasad. "Light-Weighted DNA-Based Cryptographic Mechanism Against Chosen Cipher Text Attacks." Advanced Computing and Systems for Security: Volume 1 (2016): 123-144.

18. Zhang, Mingjun, et al. "Interactive DNA sequence and structure design for DNA nano applications." IEEE Transactions on Nanobioscience 3.4 (2004): 286-292.

19. Watson, James D., and Francis HC Crick. "Molecular structure of nucleic acids: a

structure for deoxyribose nucleic acid." Nature 171.4356 (1953): 737-738.
20. Xiao, Guozhen, et al. "New field of cryptography: DNA cryptography." Chinese Science Bulletin 51 (2006): 14131420.
21. Leier, André, et al. "Cryptography with DNA binary strands." Biosystems 57.1 (2000): 13-22.
22. Cui, Guangzhao, et al. "DNA computing and its application to the information security field." 2009 fifth international conference on natural computation. Vol. 6. IEEE, 2009.
23. Farnel. (2010) Silicon storage technology - sst25vf016b-50-4is2af-16m flash memory, spi eeprom, soic8. [Online]. Available: http://uk.farnell.com/silicon-storage-technology/sst25vf016b-50-4is2af/16m-flash-memory-spi-eepromsoic8/dp/1368695
24. A. A. Jabri, "A statistical decoding algorithm for general linear block codes," in 8th IMA International Conference on Cryptography and Coding, Cirencester, UK, Dec. 2001, pp. 1–8.
25. M. Yamamoto, S. Kashiwamura, A. Ohuchi, and M. Furukawa, "Largescale dna memory based on the nested PCR," Natural Computing, an international journal, vol. 7, no. 3, pp. 335–346, 2008.
26. V. I. Risca, "DNA-based steganography," Cryptologia, Tylor and Francis, vol. 25, no. 1, pp. 37–49, 2001.
27. P. Gwynne and G. Heebner, "Technologies in DNA chips and microarrays: I," Science, vol. 4 May, p. 949, 2001. [28] T. Tsukahara and H. Nagasawa, "Probe-on-carriers for oligonucleotide microarrays (DNA chips)," Science and Technology of Advanced Materials, Elsevier Science, vol. 5, pp. 359–362, 2004.
29. P. Brown and D. Botstein, "Exploring the new world of the genome with DNA microarrays," Nature Genetics, vol. 21, pp. 33–37, 1999.
30. L. XueJia, L. MingXin, Q. Lei, H. JunSong4, and F. XiWen1, "Asymmetric encryption and signature method with DNA technology," SCIENCE CHINA Information Sciences, vol. 53, pp. 506–514, 2010.
31. Shyam, M., N. Kiran, and V. Maheswaran. "A novel encryption scheme based on DNA computing." HIPC2007 (2007).
32. Y. Brun, "Nondeterministic polynomial time factoring in the tile assembly model," Theoretical Computer Science, Science Direct, Elsevier, vol. 395, no. 1, pp. 3–23, Apr. 2008.
33. Miller, Victor S. "Use of elliptic curves in cryptography." Conference on the theory and application of cryptographic techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985., pp. 417–426.
34. Li, Kenli, Shuting Zou, and Jin Xv. "Fast Parallel Molecular Algorithms for DNA-Based Computation: Solving the Elliptic Curve Discrete Logarithm Problem over $GF(2n)$." Journal of Biomedicine and Biotechnology 2008 (2008). [35] Fuscoe, J., et al. "Technical issues involved in obtaining reliable data from microarray experiments." Regulatory Research Perspectives (2004)., vol. 6, no. 1, pp. 1–22, 2006.