A Comparison of Six DNA-based Cryptographic Methods

Ratheesh Kumar R
Lecturer in Computer Technology
Government Polytechnic College, Nedumangad
Trivandrum, Kerala, India
Email - ratheesh1976kumar@gmail.com

Abstract - DNA computing is a recent concept that creates a new dimension in cryptography and steganography. It makes use of the structural properties of DNA for representing the data. DNA cryptography can be viewed as an alternative to traditional methods of cryptography. This paper collects the features of six DNA-based cryptographic methods and compares their similarities and differences.

Keywords – security, DNA, cryptography, steganography

I. Introduction

Some data are very valuable, so they are to be secured. There are numerous cryptographic methods for securing data, namely traditional encryption methods such as 3DES, AES, RSA, XOR, etc., alternative encryption methods such as DNA computing, Chaotic theory, custom-scrambling, etc., and the combinations and mixtures of them. All of these have many advantages and limitations. Some are appropriate for text encryption, some others are suitable for image encryption, and some others are apt for video encryption.

This is an attempt to state the idea of DNA computing and to compare six encryption techniques based on DNA computing.

II. DNA Computing, Six Methods, and Comparison

2.1 DNA Computing –

The idea of using DNA computing in the field of cryptography has been identified as a new promising technology for unbreakable algorithms, as traditional cryptographic methods built on mathematical and theoretical models are prone to security attacks. DNA cryptographic techniques help the users of both ends by protecting their sensitive information from anonymous access. To make data more secure from pre-broadcast attacks, data is encrypted using DNA sequences. DNA-based cryptography technique is a new model in the cryptography field used to protect data. Recently, numerous researches have been conducted on DNA-based data protection and concealment projects. Most use the biological features of DNA sequences. DNA computing includes both cryptography and steganography. The combination can provide maximum protection and strong security for data.[7][8][9]

DNA computing is a new technique for securing data using the concept of the biological structure of DNA. The concept of using DNA computing in the fields of cryptography and steganography has been identified as a possible technology that gives new hope for unbreakable algorithms. DNA is made by linked nucleotides. The related nucleotides are Adenine (A), Cytosine (C), Guanine (G), and Thymine (T). DNA cryptography can be defined as hiding data based on the DNA sequence. With DNA cryptography, each letter of data is converted into a different combination of the four bases of DNA. DNA cryptography can be of particular benefit to secure data storage, authentication, digital signatures, and steganography. DNA can also be used to make ID cards and tickets. Multiple studies have been conducted on various biomolecular methods for encrypting and decrypting data stored as DNA.

DNA cryptography has not been well studied, and widespread work on cryptography has laid the foundation for the application of DNA methods in cryptography and steganography over the past several years. To some extent, several schemes offering DNA cryptography have been proposed and are being explored. Currently, the work on DNA cryptography is focused on using DNA sequences to encode binary data in some form or another. While the field is complex and current jobs are still in development, there is much hope that DNA computing will serve as a good technology for information security. Steganography helps to hide the existence of data. By using steganography, confidential details can be included in a cover file and forwarded to the intended person without causing doubt. A successful steganographic system contains information invisibly in a cover file while ensuring that accurate information can be extracted on the other hand. The growth in the information technology industry and its continued adoption in all aspects of life requires a reliable and secure identification. DNA steganography is the research direction of DNA cryptography. If primer sequences are kept from a competitor, DNA steganography is safer than the usual cryptography. However, this is not easy. If the primer sequences are all the same, the security will be weak. If the primer sequences are different each time, security will be strong. DNA steganography adds more complexity to hiding and retrieving on the one hand, and on the other, it supports a higher level of protection and security.[7][8][9]

2.2. Six DNA based Cryptographic Methods –

Here is a statement of six encryption methods that are used for securing text data.
Prajapati Ashishkumar B and Prajapati Barkha [1]: Various researchers around the world have applied many approaches to strengthen the security of data stored in cloud computing to address the issue of security in cloud storage. One such data security technology is the Bi-Directional DNA Encryption Algorithm (BDEA). However, the existing technology ignores the non-English user of cloud computing and focuses solely on the ASCII character set. Therefore, this specific activity focuses on increasing BDEA for use with Unicode characters. It provides two levels of security.

Sonam Baghel and Vinay Jain [2]: Their system enables the client to scramble the plain text message, and the resulting math content is DNA setting, which can provide a better classification for cryptic messages, can be used to produce advanced marks and DNA tests for testing. The client will provide the plain text message as information and create the numeric content and advanced mark as a framework DNA succession. DNA cryptography can provide two-fold security by incorporating atomic strategies and existing calculations. It provides two levels of security.

Leyi Shi, Yuwen Cui, Xiaotong Liu, Hui Sun, Zhiyu Xue, and Shufen Zhang [3]: A new plan to apply DNA microdot to random port hopping to provide security for the communication system; It is a combination of DNA nucleotide and IP address authentication. This technology makes the communication situation difficult to conduct an analysis for hostile attackers. Through several experiments, they claim that this communication model is a reliable and useful solution for defending DoS/DDoS and listening to attacks. This model provides two levels of security.

Sajisha K S and Dr. Sheena Mathew [4]: claim that their model achieves the multi-layer security of the system along with DNA-based AES encryption. The steganography methods adopted here do not develop the reference DNA sequence, and the embedded data can be extracted without the need for the actual DNA reference sequence. Their system offers three-layer security.

Sreeja Cherillath Sukumaran and Misbahuddin Mohammed [5]: Their method for securing data for cloud storage uses DNA-based encryption techniques. DNA-based encoding, encryption techniques, DNA steganography, and indexing methods are proposed to secure data in the cloud. The proposed DNA cryptographic technique differs from the original DNA sequences or the DNA cryptography used by oligos because the calculations make use of digital DNA. It has three levels of security.

Ratheesh Kumar R and Jabin Mathew [6]: Here, this DNA encryption algorithm provides five levels of security, DNA cryptography, DNA steganography, Morse encoding, AES/3DES, and OTP. There are two different systems, one with AES and the other with 3DES. The system will perform the comparison of Encryption and Decryption, and AES and 3DES by finding the execution time as evaluation criteria, and graphs are plotted for the substantiation of the definition for small input files, AES is slower than 3DES. Two systems have been developed - (1) DNA crypt, DNA steg, AES, Morse, and OTP, and (2) DNA crypt, DNA steg, 3DES, Morse, and OTP. The method is implemented in 5 levels: In level 1, DNA-based cryptography was initially applied to encrypt the secret message. In level 2; the encrypted message, in the form of a DNA sequence, is hidden by a substitution method into some reference DNA. The hiding process is done by replacing the bases of the reference DNA with those of the encrypted DNA depending on a defined rule. In level 3, the encoded text gets Morse-encoded to form new text. In level 4, AES/3DES encryption was applied to produce encrypted text. In level 5, an OTP was generated for the use of decryption. The algorithm was tested on different DNA sequences. In addition, a parameter called time was tabulated. In conclusion, the proposed scheme not only encrypts secret text into DNA sequences but also hides the encrypted data into another DNA sequence providing a high level of security. Morse Encoding, AES/3DES, and OTP provide the system more security.

2.3. Comparison of these Cryptographic Methods –

The following table gives us the details of the above methods.

Ref	System – Authors and Title	I/P	Encryption Type	Enc Algorithm	Stegano graphy	Key	Security level	Additional
[1]	Prajapati Ashishkumar B and Prajapati Barkha, **'Implementation of DNA Cryptography in Cloud Computing and Using Socket Programming'**	**Text**	**Symmetric**	**DNA (2 layers)**	**No**	**No key**	**2**	
[2]	Sonam Baghel and Vinay Jain, **'Data Encryption Algorithm based on DNA Encoding and Steganography'**	**Text**	**Symmetric**	**DNA**	**Yes**	**No key**	**2**	
[3]	Leyi Shi, Yuwen Cui, Xiaotong Liu, Hui Sun, Zhiyu Xue, and Shufen Zhang, **'A Covert Communication Scheme based on DNA Microdots for Port Hopping'**	**Text**	**Symmetric**	**DNA**	**No**	**No key**	**2**	**Port Hopping**
[4]	Sajisha K S and Dr. Sheena Mathew, **'An Encryption based on DNA cryptography and Steganography'**	**Text**	**Symmetric**	**DNA + AES**	**Yes**	**Secret key**	**3**	
[5]	Sreeja Cherillath Sukumaran and Misbahuddin Mohammed, **'DNA Cryptography for Secure Data Storage in Cloud'**	**Text**	**Symmetric**	**AES + DNA**	**Yes**	**Secret key**	**3**	
[6]	Ratheesh Kumar R and Jabin Mathew, **'A System with 5-Level Security for Cloud Data and a Comparison of AES and 3DES'**	**Text**	**Symmetric**	**AES/3DES + DNA + Morse coding**	**Yes**	**Secret key + OTP**	**5**	**AES vs 3DES** **Encryption vs Decryption**

III.CONCLUSION

All the above DNA-based cryptographic methods are great and they have their advantages and features. This paper is not a statement of superiority. All the above methods are beneficial in one or another aspect and period.

REFERENCES

[1] Prajapati Ashishkumar B, and Prajapati Barkha, “Implementation of DNA Cryptography in Cloud Computing and Using Socket Programming”, International Conference on Computer Communication and Informatics (ICCCI -2016), Jan. 07 09, 2016, INDIA

[2] Sonam Baghel, and Vinay Jain, “Data Encryption Algorithm Based on DNA Encoding and Steganography”, International Research Journal of Engineering and Technology (IRJET), Nov 2016

[3] Leyi Shi, Yuwen Cui, Xiaotong Liu, Hui Sun, Zhiyu Xue, and Shufen Zhang, “A Covert Communication Scheme based on DNA Microdots for Port Hopping”, International Journal of Performability Engineering, Sept 2017.

[4] Sajisha K S, and Dr. Sheena Mathew, “An Encryption based on DNA cryptography and Steganography”, International Conference on Electronics, Communication and Aerospace Technology, Nov 2017.

[5] Sreeja Cherillath Sukumaran, and Misbahuddin Mohammed, “DNA Cryptography for Secure Data Storage in Cloud”, International Journal of Network Security (IJNS), May 2018.

[6] Ratheesh Kumar R and Jabin Mathew, “A System with 5-Level Security for Cloud Data and a Comparison of AES and 3DES”, International Journal of Advanced Research in Engineering and Technology (IJARET), Volume 11, Issue 6, pp. 1046-1055, 2020.

[7] Pierluigi Paganini, The Future of Data Security: DNA Cryptography and Cryptosystems, https://securityaffairs.co/wordpress/33879/security/dna-cryptography.html, created on February 20, 2015 and accessed on May 9, 2019.

[8] Mohammed Nazeh Abdul Wahid, Abdulrahman Ali, Babak Esparham and Mohamed Marwan, A Comparison of Cryptograhic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention, https://symbiosisonlinepublishing.com/computer-science-technology/computerscience-information-technology32.php, created on August 10, 2018 and accessed on May 2, 2019.

[9] Abdel-Karim Al Tamimi, Performance Analysis of Data Encryption Algorithms, https://www.cse.wustl.edu/jain/cse567-06/ftp/encryption perf/index.html, accessed on May 2, 2019.