International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

A Survey on DNA Based Cryptography

Manisha[1], Pooja Ahlawat[2]

[1]M.Tech Student, R. N. College of Engineering & Management, Maharshi Dayanand University, Rohtak, Haryana, India

[2]Associate Professor, Department of Computer Science and Engineering, R. N. College of Engineering & Management, Maharshi Dayanand University, Rohtak, Haryana, India

Abstract: ***Two level security needs the hiding of data into a cover medium that cover medium is also inserted into another cover media. Both cover media may be same or different depending upon features and applications. The paper study the DNA, operation on the DNA. Then the paper focus on DNA based security i.e. cryptography and Steganography by using DNA. This paper discusses DNA cryptography and the difference between the traditional and the DNA cryptography. This paper also brief the various work done in the field of the DNA cryptography.***

Keywords: DNA, cryptography, DNA cryptography, DES, PCR

1. Introduction

Cryptography is the science and art of secret writing [1][2]. It studies some mathematical techniques and provides mechanisms necessary to provide aspects related to information security like confidentiality, data integrity, entity authentication, and data origin authentication [2].

Symmetric algorithms are cryptosystems that either a secret key will be shared for both encryption and decryption [1][5]. The algorithms of symmetric cryptosystems are very strong against possible attacks, but mainly weakness of symmetric cryptosystems is brute-forcing the secret key. This characteristic creates the biggest critical act in any cryptosystem that uses symmetric algorithms which is distribution of the shared secret between the two parties like DES algorithms. Asymmetric algorithms use different values for encryption and decryption and do not need to share secret between two parties. Each party only has to keep a secret of its own. The earliest foundation of asymmetric algorithms known as public key cryptosystems comes from key exchange problem of symmetric algorithms. In 1976, Whitfield Diffie and Martin Hellman proposed a method were the sender and receiver do not have to share a secret. That was the first work on hybrid cryptosystem [1][2].

DNA cryptography, a new branch of cryptography utilizes DNA as an informational and computational carrier with the aid of molecular techniques. It is relatively a new field which emerged after the disclosure of computational ability of DNA [5]. DNA cryptography gains attention due to the vast storage capacity of DNA, which is the basic computational tool of this field. One gram of DNA is known to store about 108 tera-bytes. This surpasses the storage capacity of any electrical, optical or magnetic storage medium [5], [6]. Traditional cryptographic systems have long legacy and are built on a strong mathematical and theoretical basis. Traditional security systems like RSA, DES or NTRU are also found in real time operations. So, an important perception needs to be developed that the DNA cryptography is not to negate the tradition, but to create a bridge between existing and new technology. The power of DNA computing will strengthen the existing security system by opening up a new possibility of a hybrid cryptographic system. This needs the clear difference between the traditional and DNA based cryptography that is specified in the table 1.

Table 1: Comparison of traditional and DNA cryptography [4]

Characteristics	Traditional Cryptography	DNA cryptography
Security	Less	More
Time	Minutes to hours	Hours to days
Storage capacity	In MB	In TB
Dependency	On Implementation environment	On environmental conditions

2. Technology Used In DNA Computation

Today, various techniques are used to carry out DNA computation. Researchers use these techniques for performing the operations on informative DNA molecules. Some of these technologies are as follows:

Gel electrophoresis: It is a phenomenon used to separate the DNA fragments according to their length. A gel of polyacrylamide or agarose is prepared. The negatively charged DNA molecules are placed in the wells which are situated at one side of this gel. On the application of an electric current to the gel, the negatively charged DNA molecules will start moving towards the positive pole, where the shorter molecules travel faster than the larger ones. Hence, a separation between them can be detected easily [14].

Polymerase Chain Reaction (PCR): As it is difficult to manipulate the small amount of DNA, an amplification process is carried out. PCR has very high amplification efficiency, hence, this technology is used to amplify and quantify the DNA. In DNA amplification using PCR, required DNA segments are cloned into vectors. For PCR amplification two things are required, a primer and a DNA template. DNA template is a single-stranded DNA sequence which contains the segment which is to be amplified and primer is a complement sequence of that segment. A primer is annealed with the DNA template. After that, DNA polymerase enzyme initiates DNA synthesis process by

successively adding the nucleotides to 3' end of the primer, until the desired DNA strand is obtained. Primer always extends in the direction 5' to 3' only. The desired DNA strand starts with the primer and is always complementary to the DNA template. The whole PCR process can be divided into two steps:

- Designing the two primers and loading them separately, one at the beginning and another at the end of target DNA.
- Matching the primers with their complement sequences in template DNA [15].

DNA Chip technology: With the help of DNA chip, a vast amount of genome-sequencing data can be manipulated [16]. It is used to find the expression of several genes in parallel. DNA chips stores data in the form of DNA sequences. In DNA chips, a huge number of spots are embedded on solid surface, generally a glass slide. Each and every spot of a chip consists of different type and number of probes. Probes are small single-stranded DNA sequences have the ability to bind with their complementary DNA sequences. Binded DNA sequences are labelled fluorescently which are observed under laser dye. Depending upon the ratio of binding between probe and DNA of each spot, data is calculated by electronic means [17].

3. Related Work

Boris Shimanovsky et al. [4] (2003) proposed the original idea of hiding data in DNA and RNA. The first is a simple technique that hides data in non-coding DNA such as non-transcribed and non-translated regions as well as non-genetic DNA such as DNA computing solutions. The second technique can be used to place data in active coding segments without changing the resulting amino acid sequence. Monica Borda et al. [5] (2010) presented the principles of bio molecular computation (BMC) and several algorithms for DNA (deoxyribonucleic acid) steganography and cryptography: One- Time-Pad (OTP), DNA XOR OTP and DNA chromosomes indexing. Hayam Mousa et al. [6] introduced a reversible information hiding scheme for DNA sequence based on reversible contrast mapping. The scheme uses two words of the sequence with the reversible contrast mapping to achieve reversibility. Jin-Shiuh Taur et al. [7] proposed an improved algorithm named the Table Lookup Substitution Method (TLSM) to enhance the performance of an existing data hiding method called the substitution method. Moreover, a general form of the TLSM is discussed, which includes the original method as a special case.

Mohammad Reza Najaf Torkaman et al. [8] proposed to decrease the usage of asymmetric cryptography and introduced a novel cryptographic-steganography protocol. The main advantage of proposed cryptography protocol was using innovative DNA steganography techniques to conceal secret session key which is transferred among sender and receiver throughout unsecured channel. Ban Ahmed Mitras et al. [9] discussed a reference DNA sequence has been shared between sender and receiver. Not only this DNA reference sequence can be retrieved from EBI or NCBI databases but it can also be simply selected from any database. Therefore, by considering any sort of database, there are 163 million targets to select it. Virtually, guessing the correct DNA sequence by attacker is unachievable. Grasha Jacob et al. [10] (2013) analyzed the different approaches on DNA based Cryptography. They said that DNA binary strands support feasibility and applicability of DNA-based Cryptography. The security and the performance of the DNA based cryptographic algorithms are satisfactory for multi-level security applications of today's network. Debnath Bhattacharyya et al. [11] (2013) proposed an algorithm to hide secret message in DNA String to increase the security during transmission of data. In this paper, we propose a new Binary Coded DNA rules towards Data Hiding in DNA. K. These works are also explained in the following table i.e. table 2:

Table 2: Related Work

Author	*Year*	*Contribution*
Boris Shimanovsky et al. [4]	2003	Proposed the original idea of hiding data in DNA and RNA.
Monica Borda et al. [5]	2010	Presented the principles (BMC) and DNA steganography and cryptography.
Hayam Mousa et al. [6]	2011	Introduced a reversible information hiding scheme
Jin-Shiuh Taur et al. [7]	2012	Proposed an improved algorithm named the Table Lookup Substitution Method (TLSM)
Mohammad Reza Najaf Torkaman et al. [8]	2012	Decrease the usage of asymmetric cryptography
Ban Ahmed Mitras et al. [9]	2012	Increased security
Grasha Jacob et al. [10]	2013	analyzed the different approaches on DNA based Cryptography. DNA binary strands support feasibility and applicability of DNA-based Cryptography
Debnath Bhattacharyya et al. [11]	2013	Proposed an algorithm to hide secret message in DNA String to increase the security during transmission of data.

4. Drawback of Existing Work

The unintended user gets to know that data is hided in the particular DNA then the extraction of data is possible in the DNA based Steganography. It is due to the fact the data is in plain form in the DNA. While the cryptography makes the data in encrypted form but the data is visible to the unintended user. To make the process more robust and secure the data must hided must be cascaded by cryptography and the Steganography.

5. Conclusion

This paper discusses the structure of the DNA along with the DNA cryptography. This paper also briefs the work done in the area of the DNA cryptography. The difference between the traditional and DNA cryptography clears the importance of the DNA cryptography. The drawback of the previous work defines the open area of research in the field of DNA cryptography. In future an algorithm can be designed for DNA based cascaded Steganography and cryptography.

References

[1] Torkaman M.R.N., Nikfard P., Kazazi N.S., Abbasy M.R., and Tabatabaiee S.F.: Improving Hybrid Cryptosystems with DNA Steganography. E. Ariwa and E. El-Qawasmeh (Eds.): DEIS 2011, CCIS 194, pp. 42–52, 2011
[2] Alia, M.A., Yahya, A.: Public–Key Steganography Based on Matching Method. European Journal of Scientific Research, 223–231 (2010)
[3] Kumar, S., Wollinger, T.: Fundamentals of Symmetric Cryptography. Embedded Security in Cars, 125–143 (2006)
[4] Shimanovsky, B., Feng, J., & Potkonjak, M. (2003, January). Hiding data in DNA. In Information Hiding (pp. 373-386). Springer Berlin Heidelberg.
[5] Borda, M., & Tornea, O. (2010, June). DNA Secret Writing Techniques. In IEEE conferences.
[6] Mousa, H., Moustafa, K., Abdel-Wahed, W., & Hadhoud, M. M. (2011). Data hiding based on contrast mapping using DNA medium. Int. Arab J. Inf. Technol., Volume- 8 Issue (2), pp 147-154.
[7] Taur, J. S., Lin, H. Y., Lee, H. L., & Tao, C. W. (2012). Data Hiding In DNA Sequences Based On Table LookUp Substitution. International Journal of Innovative Computing, Information and Control, Volume 8 Issue (10).
[8] Torkaman, M. R. N., Kazazi, N. S., & Rouddini, A. (2012). Innovative approach to improve hybrid cryptography by using DNA steganography. International Journal of New Computer Architectures and their Applications (IJNCAA), Volume-2 Issue (1), pp. 224-235.
[9] Mitras, B. A., & Aboo, A. K. (2012). Proposed Steganography Approach Using Dna Properties. International Journal of Information Technology and Business Management, Volume-14 Issue 1.
[10] Jacob, G., & Murugan, A. (2013). DNA based Cryptography: An Overview and Analysis. International Journal of Emerging Sciences, Volume 3 Issue (1), pp.36-27.
[11] Bhattacharyya, D., & Bandyopadhyay, S. K. (2013) Hiding Secret Data in DNA Sequence. International Journal of Scientific &Engineering Research Volume 4.
[12] Mitras, B. A., & Aboo, A. K. (2012). Proposed Steganography Approach Using Dna Properties. International Journal of Information Technology and Business Management, Volume-14 Issue 1.
[13] Yamuna, M., Dangi, M. K., & Singh, K. (2013). Encryption of a Binary String Using DNA Sequence. International Journal of Computer Science, Volume 2, Issue (02).
[14] H. Lodish, A. Berk, P. Matsudaira, C. A. Kaiser, M. Krieger, M. P. Scott, S. L. Zipursky, and J. Darnell "Molecular Cell Biology", 5th ed. New York: W. H. Freeman and Co. 2003.
[15] G. Cui, L. Qin, Y. Wang, and X.Zhang, "An encryption scheme using DNA technology," in IEEE 3rd International conference on Bio-Inspired Computing: Theories and Applications (BICTA08), Adelaid, SA, Australia, pp. 37–42, 2008
[16] P. Gwynne and G. Heebner, "Technologies in DNA chips and microarrays: I," Science, vol. 4 May, p. 949, 2001.
[17] 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.

Author Profile

Manisha received the B.Tech (Computer Science) Matu Ram Engineering and Management College in 2013 and M.Tech degree in Computer Science and Engineering from R. N. College of Engineering & Management in 2015, respectively.