A Survey on DNA Based cryptography

Radha Shinde[*1], Lalit Gehlod[2]

Department of Computer Science, IET, DAVV
Indore, M.P.

Abstract—**cryptography is an art for hiding data in unreadable formats. Therefore a number of techniques are developed to hide the data more and more strongly. This technique needs a recovery technique also by which the original data can be recoverable. In this paper a new domain of cryptography is explored and studied by which the data is hided in the DNA based encoding. Therefore the paper includes a study about the DNA cryptography, recently developed methods and a new technique is also proposed by which the current domain of cryptography is enhanced in space overhead issues.**

Keywords*—*DNA cryptography, encryption, data manipulation, data recovery, data security.

I. INTRODUCTION

The cryptography is an art of data hiding that is performed for preserving information by transforming it. The transformation of information is known as encryption. The encryption results a transformed data called cipher text. After encryption of data the data at the receiving end is again recovered in their actual format known as the decryption of the message. Sometimes the attackers and hackers are also tries to recover the original message from the generated ciphers that process is known as cryptanalysis, also called code-breaking.

As the use of Internet is growing rapidly the use of electronic communication become more frequent. Therefore the data security is become important for data communication and preservation. In order to protect the data Cryptography is used. The cryptography is one of the popular technologies because it's effective and free for implementation.Cryptography can be divided into symmetric-key systems and public-key systems.There are other various different kinds of cryptographic schemes are available. These algorithms have their own characteristics of data manipulation and transformation [1] [2].

Symmetric Encryption:Symmetric encryption is the oldest and best-known technique. A secret key is applied to the text to change the content. This might be as simple as shifting each letter by a number of places. Both sender and recipient know the secret key, they can encrypt and decrypt all messages using this key.

Asymmetric Encryption: The keys exchange is huge problem in cryptography over the communication medium. Anyone who knows about key can decrypt the message. Asymmetric encryption is the answer of this process.There are two related keys one public key available to anyone who want to send message and a private key is kept secret to decrypt the message is used. This means need not to worry about passing public keys over the Internet. The problem with asymmetric encryptionis that it is slower than symmetric encryption.

Hybrid Cryptography: Symmetric and asymmetric ciphers each have their own advantages and disadvantages. Symmetric ciphers are significantly faster than asymmetric ciphers, but require sharing a secret key. So a hybrid cryptosystem is required to combine advantages of both techniques speed and security [2].

In the category of hybrid encryption techniques a new domain is found recently using the genetically inspired cryptographic algorithms. That is known as the DNA cryptography. The DNA cryptography is one of the most popular techniques of the cryptography for fast and effective data transformation. In this study in further the DNA and their cryptographic techniques are discussed.

II. BACKGROUND

This section provides the basic details of the DNA sequences and the DNA cryptography which is used with the encryption and decryption process development.

DNA (deoxyribonucleic acid) is a hereditary material in humans and also in all the creators. Every cell in body has the same DNA. Most DNA is located in the cell nucleus, but a small amount of DNA can also be found in the mitochondria.The information in DNA is stored as a code that is developed using the four components adenine (A), guanine (G), cytosine (C), and thymine (T). The order, or sequence, of these bases determines the information available for building and maintaining an organism, similar to the way in which letters of the alphabet appear in a certain order to form words and sentences. The example of DNA sequence organization is demonstrated using the figure 1. DNA bases pair up with each other, A with T and C with G, to form units called base pairs. Each base is also attached to sugar molecule and phosphate

molecule. Together, a base, sugar, and phosphate are called a nucleotide. Nucleotides are arranged in two long strands that form a spiral called a double helix. The structure of the double helix is somewhat like a ladder, with the base pairs forming the ladder's rungs and the sugar and phosphate molecules forming the vertical sidepieces of the ladder. [3]

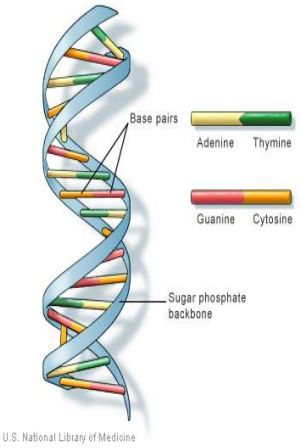

Figure 1.2 DNA structure

An important property of DNA is that it can replicate, or make copies of itself. Each strand of DNA in the double helix can serve as a pattern for duplicating the sequence of bases. This is critical when cells divide because each new cell needs to have an exact copy of the DNA present in the old cell.

DNA cryptography is one of the advanced technologies that work on concepts of DNA computing. The technique for securing data using biological structure of DNA called DNA Computing. That is invented by Leonard Max Adleman in the year 1994. According to the inventor DNA can be used to store and transmit data. The concept of DNA computing in the fields of cryptography and steganography can performed now in these days. There are some Advantages of DNA computing [4]:

Speed – Conventional computers can perform approximately 100 MIPS (millions of instruction per second). Combining DNA strands as demonstrated by Adleman, made computations equivalent to 10^9 or better, arguably over 100 times faster than the fastest computer.

Minimal Storage Requirements – DNA stores memory at a density of about 1 bit per cubic nanometer where conventional storage media requires 10^12 cubic nanometers to store 1 bit.

Minimal Power Requirements – There is no power required for DNA computing while the computation is taking place. The chemical bonds that are the building blocks of DNA happen without any outside power source. There is no comparison to the power requirements of conventional computers.

III. LITERATURE SURVEY

This section provides the study of the recently developed approaches of DNA based cryptography. The study of these techniques provides the guidelines for performance improvements of the traditional technique.

Security is one of the most significant and fundamental issue for data transmission in WSNs. DNA cryptography playsa vital role in areas of communications and data transmission. In DNA cryptography, biological DNA concept can beused not only to store data and information carrier, but also to perform computations. ***Monika et al [5]***proposed a DNA based security. That uses DNA cryptography with secure socket layer (SSL) for providing asecure channel with more secure exchange of information in wireless sensor networks.

MANET is collection of nodes with wireless communication that communicates with each other without any centralized control. Due to mobility and limited radio range, every node has to perform as routers for forwarding information. In MANET communication is done via open medium, so Transmitted information and network is vulnerable to different types of attacks. Thus, for providing security against unauthorized access to data a secure routing protocol is required.DNA Cryptography is used to safeguard the data against the unauthorized access. ***SonamModi [6]***considers protocol AODV to implement the required security in routing protocol.DNA cryptography is used in routing algorithm of MANET as security.DNA cryptography is an approach to ensure secure environment for data transmission across network.

DNA Cryptography is a rapidly emerging field of DNA Computing to provide cryptographic technique for the modern and the futuristic computers. Several DNA based cryptographic algorithms are proposed for encryption, decryption and authentication, etc. The first and foremost step of DNA based encryption is DNA encoding of plaintext. The main limitation of DNA encoding is the absence of effective, randomized, dynamic, secure DNA Encoding technique for DNA encoding of plaintext. To overcome this limitation, ***NoorulHussainUbaidurRahman et al [7]*** describe a novel DNA encoding algorithm. This encoding algorithm is based on a string matrix data structure, for generating the unique DNA sequences used to encode plain text as DNA sequences. The experimental results and comparison results have proved that the given DNA encoding algorithm is more effective than the existing DNA encoding algorithms.

Lot of techniques and systems has been developed based on modular arithmetic cryptography for encryption and decryption. However, these techniques are broken using DNA cryptography techniques and methods. DNA Cryptography is a new instinctive cryptographic field that has emerged from the research of DNA computing. Some algorithms that are available in DNA Cryptography have limitations in that they still use modular arithmetic cryptography at some of their steps or they are biological laboratory experiment based which

is not suitable in the digital computing environment. To overcome this lacuna, ***NoorulHussainUbaidurRahman et al [8]*** describe a novel, secure, unique and dynamic DNA based encryption and decryption algorithm and also provide an analysis of its performance.

Multiple secret sharing algorithms using the YCH scheme, combined with DNA encoding is proposed by ***L. JaniAnbarasi et al [9]***. Firstly, DNA encoding for multiple images is carried out; then the addition of these encoded components by DNA is performed. Secondly, the (t, n) scheme used the Lagrange interpolation polynomial to share these DNA scrambled matrices is performed. Thirdly, these shares are embedded using a modular operation. Finally, 't' or more shares are pooled which reconstructs the scrambled matrices, and by decoding the DNA scrambled matrices multiple secrets are reconstructed without loss. The simulation results and the security analysis prove that this algorithm is perfect, and produces results with better PSNR value. The correlation co- efficient shows that this also has the ability of resisting various attacks.

IV. PROPOSED WORK

This section provides the proposed solution for DNA based encryption technique. Therefore the encryption and decryption process of the proposed technique is described in detail.

Encryption Process

The proposed DNA cryptographic technique developed through the traditional computing technique and new approaches for enhancing the current process of the data encryption. Therefore the following processes are involved during the data encryption.

1. first input string is converted into ASCII values
2. the ASCII values are in next step converted into the binary strings
3. These binary values are further convert into hexadecimal values
4. On the other hand the original text is processed using the MD5 algorithm. MD5 algorithm generate 128 bit key
5. In next step the generated 128 bit string is converted into the hexadecimal string of length of 32 characters
6. Than using the generated 32 characters a dynamic mapping table is constructed. This table contains 16 values.
7. The generated mapping table is used to encode all the binary string of original text
8. The encoded string is further divided into two blocks of text
9. Now the user input is required here the number of iterations and rate of elitism. After that using the following formula the number of cross over is estimated.

$$nc = |(\alpha - Ne)/2|$$

Where α number of partition in our key

N = 16 fix that is hexadecimal number code

E = is rate of elitism that may take between 0-1 like 0.45, 0.78, 0.59 etc. This is private key for this method.

10. In this step according the value of cross pointsboth the text blocks are converted into new strings
11. Replace value of chunks by value of mapping table.
12. XOR performed over both the two new binary sequences
13. Combine the outcome of the XOR and one string is taken from both of the blocks
14. In this step combines all the data α, N and Ewith thestring of 13^{th} step. And used for transmission in unsecured network transmission.

Decryption

The decryption of the encrypted text needs additional parameters therefore the following process is taken place.

1. In this step encrypted file is passed as input
2. the value of α, key and data is extracted from received file
3. Now using the key mapping table is recovered
4. In this phase the recovered data is again converted into two equal length strings
5. Now perform XOR operation on these two strings and the second string is generated using this process
6. In this step the binary strings and again converted into the hexadecimal numbers according to mapping table
7. In this phase the α, and E values are used with the same crossover points to recover the original strings
8. Combine output for generating original text
9. Finally the hexadecimal valuesare convert into binary strings
10. this binary string is further converted into original text to recover the original text

This section provides the understanding about the proposed DNA based encryption and decryption technique. In further the conclusion of the entire study is provided.

V. CONCLUSIONS

In this paper the cryptographic techniques and their applications are discussed. In addition of that how traditional cryptography is replaced by new generation cryptographic algorithms are also studied. Finally a secure encryption

technique which is fast and efficient is discussed as the DNA computing methodology. There are some additional improvements are preformed recently therefore recently developed DNA based algorithms and their different areas of application is learned. Finally a new concept using the DNA sequences and genetic algorithm is proposed. The proposed DNA cryptographic algorithm is near future implemented using the JAVA development environment and their performance is compared with the existing approach.

REFERENCES

[1] C. Chandrasekar, V. Prabhakaran, "A Simple Symmetric Key Cryptographic Algorithm",Vol. 2 Issue 2 ISSN: 2278-7844,2013 IJAIR. ALLRIGHTS RESERVED

[2] SankalpPrakash, MridulaPurohit, "Applied Hybrid Cryptography in Key-pair Generation of RSA implementation", IJICCT–JUL 2013;Vol 1,Issue 1;ISSN 2347-7202

[3] SumanChakraborty, Prof. Samir K. Bandyopadhyay, An approach of image staganography by combine application of DNA sequence and arithmetic encoding, International Journal of Management & Information Technology, Vol. 5, No. 3

[4] Pierluigi Paganini, "The Future of Data Security: DNA Cryptography and Cryptosystems", February 20, 2015

[5] Monika, ShuchitaUpadhyaya, "Secure communication using DNA cryptography with secure socket layer (SSL) protocol in wireless sensor networks", 4thInternational Conference on Eco-friendly Computing and Communication Systems

[6] SonamModi, "Routing Algorithm using DNA Cryptography in MANET", © 2015 IJEDR | Volume 3, Issue 2 | ISSN: 2321-9939

[7] NoorulHussainUbaidurRahman, ChithralekhaBalamurugan, RajapandianMariappan, "A Novel String Matrix Data Structure for DNA Encoding Algorithm", International Conference on Information and Communication Technologies (ICICT 2014)

[8] NoorulHussainUbaidurRahman, ChithralekhaBalamurugan, RajapandianMariappan, "A Novel DNA Computing based Encryption and Decryption Algorithm", International Conference on Information and Communication Technologies (ICICT 2014)

[9] L. JaniAnbarasi, G.S.Anandha Mala, ModigariNarendra, "DNA based Multi-Secret Image Sharing", International Conference on Information and Communication Technologies (ICICT 2014)

