Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.199

IJCSMC, Vol. 8, Issue. 4, April 2019, pg.108 – 114

Message Transmission Using DNA Crypto-System

Saifali Mavanai[1]; Ajay Pal[2]; Ravi Pandey[3]; Asst Prof. Deepika Nadar[4]

[1]B.E. Computer Engineering student, St.John College Engineering Mumbai, Maharashtra, India
saifalimavani95@gmail.com

[2]B.E. Computer Engineering student, St.John College Engineering Mumbai, Maharashtra, India
ajaypal9173@gmail.com

[3]B.E. Computer Engineering student, St.John College Engineering Mumbai, Maharashtra, India
pandeyravi735@gmail.com

[4]Assistant Professor, St.John College Engineering Mumbai, Maharashtra, India
kdeepika343@gmail.com

Abstract: In today's modern world of technological advancement modifications to the system are made according to the system requirements. This may lead to much security loop holes which are easily recognizable by the attackers. DNA Cryptography is the novel technique which is based on the Helical structure of DNA molecule. ssDNA is preferred for DNA cryptography which has four nucleotide bonds complementary to each other. The main objective of this project is to design a system that is reliable, efficient, and robust for secure message transmission. A group of words are arranged in the random sequence of four DNA bases that makes up the human DNA (Deoxyribonucleic Acid).

Keywords: Encryption, Decryption, Single Stranded DNA, Hybrid DNA technique

I. INTRODUCTION

With growing speed of internet and network advancement the security threats are increasing tremendously. 50% growth in cybercrime is observed in past few decades which involve trespassing the Security barriers, hacking various social accounts, Stealing confidential information. There are various types of attacking technology or tools with the help of that always try to break into system in order to steal crucial information in order to damage the integrity of data and to use it for blackmailing or to destroy the redeemed organization. So it is very important to prevent the modern security systems from these threats and attacks. From the past few years many security mechanisms are proposed and Cryptography and Steganography are most commonly used techniques. Cryptography is a technique where a set of alphabets or sequences is encrypted in a special format which can be only decrypted by the intended person. DES, AES are some cryptographic algorithms which are used for long lime.

In cryptography the encryption/decryption of data/plaintext is done with the help of key. A new technique for securing data using the biological structure of DNA is called DNA Computing (A.K.A molecular computing or biological computing). [1]It was proposed by Leonard Max Adleman in the year 1994 for solving and suggesting solution for the complex problems such as the directed Hamilton path problem and the NP-complete problem similar to The Traveling Salesman problem. He is also known as the 'A' in the RSA. DNA can be used to store and transmit data. [2] The recent technology based on DNA cryptography was One-Time- Pad(OTP). It uses the concept of complementary DNA strand and generates a random sequence along with a shared private key is sent to the receiver. [3]There is also a methods based on index based symmetric DNA encryption algorithm which uses a symmetric key. The concept of using DNA computing in the fields of cryptography and steganography has been identified as a possible technology that may bring forward a new hope for unbreakable algorithms.

Strands of DNA are long polymers of millions of linked nucleotides. These nucleotides consist of one of four nitrogen bases, a five carbon sugar and a phosphate group. The nucleotides that make up fused rings of these polymers are named after the nitrogen base that it consists of: Adenine (A), Cytosine (C), Guanine (G) and Thymine (T). Mathematically, this means we can utilize this 4 **letter alphabet Σ = {A, G, C,** and T} to encode information, which is more than enough considering that an electronic computer needs only two digits, 1 and 0, for the same purpose. The inspiration behind the using human DNA structure for cryptography is because of its space compatibility. The main objective of DNA cryptography is based on encryption of message in DNA digital form and the decrypting it on receiver**'**s side. DNA cryptography ensures the Confidentiality, Integrity and Availability of data which is the basic requirement of security. Encrypting the data/plaintext using Transposition, Folding and ssDNA complementary operations is the basic approach of algorithm. Researchers and scientist are continuously searching for an adaptive technology for improving encryption methods. After failure of many cryptographic algorithms in latest network attacks it is imminent for a reliable system and algorithm mentioned in the paper is a good replacement.

Real World problems with existing algorithms based on DNA cryptography

1. More space required to store message
2. Not compatibility on all the systems
3. Time required is more for processing
4. Precise result is not obtained
5. Security loopholes can be formed

II. BIOLOGICAL BACKGROUND

DNA(Deoxyribonucleic acid) is one of the major components in human body which stores all the genetic data of an individual. It is a thread like structure which has the information about development, growth, reproduction of the individual. DNA is very compact structure which can able to store tremendous amount of data in a single molecule. DNA is a long polymer of deoxyribonucleotides. Chemically, DNA is compared to three components of a pentose sugar, phosphoric acid and four types of nitrogenous bases.

Pentose sugar in DNA is deoxyribose sugar. The four nitrogenous bases belongs to two sequence groups purines which are two-ringed nitrogen compound and includes adenine(A) and guaninie(G) and pyrimidines which are formed of one ring only and include Thymine(T) and Cytosin(C). James Watson and Francis Creek proposed DNA consist of two strands, which are helically coiled. The two strands are said to be complementary. The strands are said to be Anti-Parallel i.e. one in5**'** 3**'** direction and the other in 3**'** 5**'** direction.

Between T and A there are 2 hydrogen bonds and between G and C there are three hydrogen bonds. The stacking of bases creates two types of grooves called major and minor grooves. Each turn accommodate 10 bases. The gradient of the helix is 3.4 nm. The DNA model, irrespective of its source, always has the A—T base pairs equal in number to the G—C base purines.

The purines and pyrimidines are always in equal proportion, i.e A+T=G+C. The amount of adenine is always equal to the amount of thymine and the amount of guanine is always equal to the mount of cytosine i.e A=T and G=C. However, the amount is not necessarily equal to G+C. However, the amount is not necessarily equal to G+C.

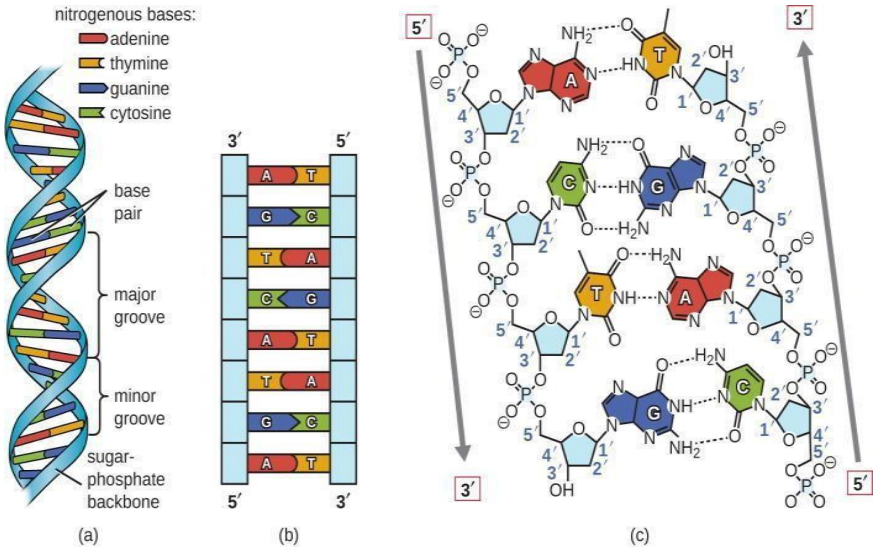

Fig 1: Architecture Of DNA Strand

III. PROPOSED METHODOLOHY

The proposed methodology is a combination of various operations which involves transposition, shifting, and single stranded complementary approach. Transposition approach is performed to change the location of data matrix element. Folding operation shuffles one of the elements with another like a paper fold.

A. Encryption

Encryption process converts ASCII values into binary into 8- bit binary format and them substitute the values for a combination of various binary bits. Now transposition matrix is performed in an irregular fashion like an s curve and we obtain cipher text in 16- bit format. Folding operation is performed on the transposed matrix in three ways - row folding, column folding and diagonal folding.

Algorithm

1) Convert the Plain Text into it's respective ASCII value and then into 8 bit binary format.
2) Substituting binary value into ATGC format.
   a) 00-A
   b) 01-T
   c) 10-G
   d) 11-C
3) Now perform the Transposition operation in Zig-Zag manner on obtained cipher text in 16 bit, 4x4 format.
4) After the Transposition operation perform the folding operations on row, column and diagonally.
5) Now compliment the obtained cipher text by its corresponding DNA compliment.
   a) T-A
   b) C-G

B. Decryption

Decryption process is reverse of encryption process which follows the entire procedure in the reverse order.

Algorithm

1) Perform the DNA compliment operation on the obtained string.
   a) A-T
   b) G-C
2) Now perform 16 bit, 4x4 tabular reverse Folding operation.
3) After that perform the Reverse Transposition operation on obtained table
4) Re-substitute the value of ATGC format.

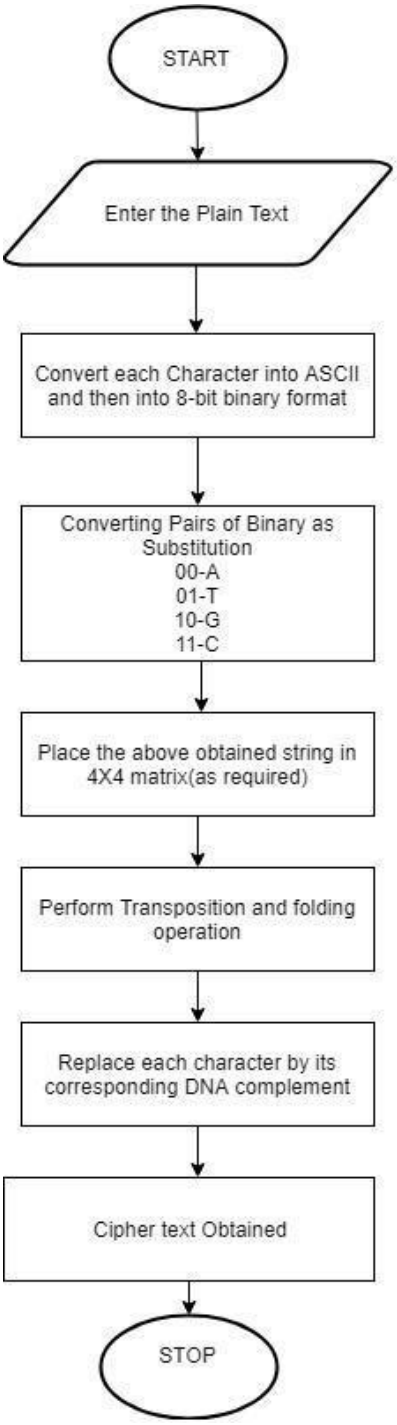

Fig 2: Flow Chart for Encryption

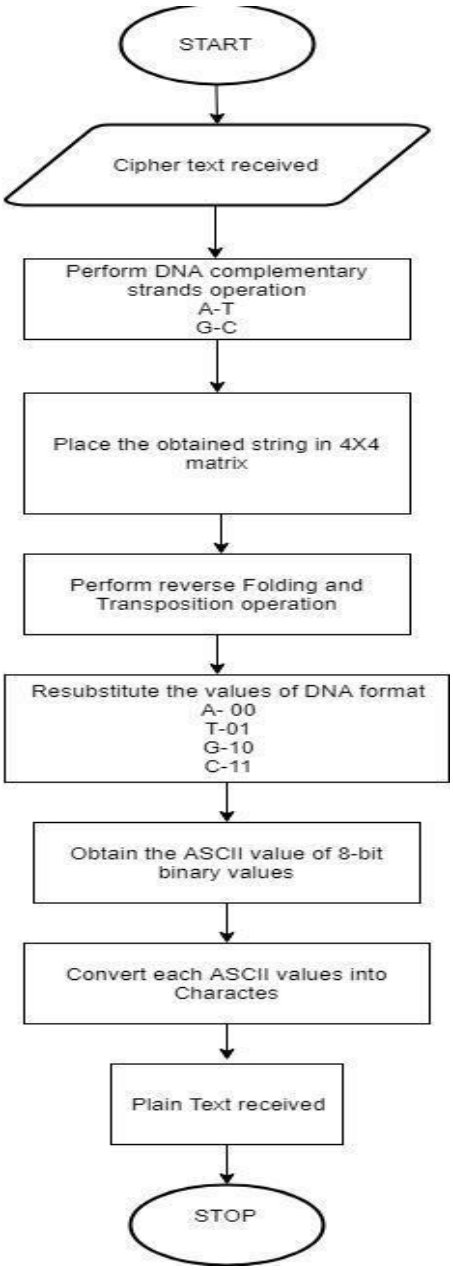

Fig 3: Flow Chart for Decryption

IV. EXAMPLE AND ILLUSTRATION

Step 1- For example if user enter the text

```
Enter text:vcet
```

Step 2- Their respective ASCII value.

```
118  99  101  116
```

Step 3- Their binary value

```
01110110011000110110010101110100
```

Step 4- After substitution

```
TCTGTGACTGTTTCTA
```

Step 5- Form 16 bit table

```
16 bit matrix is:
T       C       T       G
T       G       A       C
T       G       T       T
T       C       T       A
```

Step 6-Perform Transposition

```
Transposition matrix is:
T       C       T       T
G       T       G       A
G       T       C       T
C       T       T       A
```

Step 7- Perform folding

```
Folded matrix is:
T       T       C       G
C       T       T       T
T       C       G       G
T       A       T       A
```


Step 8- Perform DNA Compliment

```
A       A       G       C
G       A       A       A
A       G       C       C
A       T       A       T
```

Step 9- Obtained Encrypted string is

```
AAGCGAAAAGCCATAT
```

Step 10- Decryption process convert the string into 16 bit format (4x4 table).

```
matrix in 16-bit:
A       A       G       C
G       A       A       A
A       G       C       C
A       T       A       T
```

Step 11- Reverse DNA compliment

```
T       T       C       G
C       T       T       T
T       C       G       G
T       A       T       A
```

Step 12- Reverse Folding operation

```
Folded matrix is:
T       C       T       T
G       T       G       A
G       T       C       T
C       T       T       A
```

Step 13- Reverse transpose matrix

```
Transposition matrix is:
T       C       T       G
T       G       A       C
T       G       T       T
T       C       T       A
```

Step 14- Convert it into binary format

```
01110110011000110110010101110100
Recovered ascii valueis
118 99 101 116
```

Step 15- Recovered string is

```
vcet
```


V. RESULTS

Length Of Encrypted String	TFS DNA Encryption Algorithm	Feistel DNA Encryption algorithm
1	16 bytes	20 bytes
2	16 bytes	25 bytes
4	16 bytes	50 bytes
8	32 bytes	105 bytes
16	64 bytes	252 bytes

Table 1: Comparing TFS and Feistel

VI. CONCLUSION

In this paper we have suggested DNA cryptography various methods and also discussed about the comparison factors between the latest and the proposed methodology. The methodology proposes a strong approach for encrypting and decrypting of messages which is strong against brute force attacks. The concept of transposition and shifting with complementary DNA strands make it more resistant against cyber-attacks (Power Analysis Attacks, Man in Middle Attack, Side Channel Attack, Timing Attacks, Dictionary Attack). Search for a new approach to the existing module which fascinates them about various concepts and this can be new technique. After going through various test methods and trying the algorithm for various scenarios we have created a table of comparative study based on the amount of messages that it takes as input to send to the receiver. The storage requirement is mentioned in the table with the help of varying message size. This gives analysis of a better suggestion for algorithms including the hybrid DNA algorithm.
The algorithm can also be integrated with the DNA nano chips that were invented in recent time. Researchers are always in
Advantages-
1. Secure, Reliable and Robust system with minimal errors
2. Fast and time efficient in very aspects

Disadvantages-
Too many messages can cause increase in time for receiver to obtain the message

Future Scope
The DNA cryptography can be used as in the recent systems such as following
1. Can be used for website transmission of data
2. Can be used for handling very secure data
3. Can be used to secure mobile systems

REFERENCES

[1] L. M. Ad leman, "Molecular computation of solution to combinatorial problems Science, (1994) 11, (266): 1021-1024.
[2] Ashish kumar kaundal, **"**Feistel Inspired structure for DNA cryptography**"** in June (2014).
[3] Yunpeng Zhang, Bochen Fu, and Xianwei Zhang, "DNA cryptography based on DNA Fragment assembly," In Information Science and Digital Content Technology (ICIDT), IEEE International Conference on, vol. 1, pp. 179-182, (2012).
[4] Lightweight Symmetric Encryption Algorithm for Secure Database Hanan A. Al-Souly, Abeer S. Al- Sheddi, Heba A. Kurdi Computer Science Department, Computer and Information Sciences College Imam Muhammad Ibn Saud Islamic University Riyadh.
[5] Mohammad Reza Abbasy, Azizah Abdul Manaf, and M.A. Shahidan, "Data Hiding Method Based on DNA Basic Characteristics", International Conference on Digital Enterprise and Information Systems, July 20-22, (2011), London, UK, pp. 53–62.
[6] H. J. Shiu, K. L. Ng, J. F. Fang, R. C. T. Lee and C. H. Huang, "Data hiding methods based upon DNA sequences", Information of Science, vol.180, no.11, pp.2196-2208, 2010.
[7] Jin-Shiuh Taur1, Heng-Yi Lin1, Hsin-Lun Lee1 and Chin-Wang Tao, "Data Hiding in DNA Sequences Based On Table Lookup Substitution", International Journal of Innovative Computing, Information and Control, Volume 8, Number 10(A), October 2012.
[8] Debnath Bhattacharyya, Samir Kumar Bandyopadhyay, "Hiding Secret Data in DNA Sequence", International Journal of Scientific &Engineering Research Volume 4, Issue 2, February- 2013 ISSN 2229-5518.
[9] Ing-an He, Chun Li and Jun Wang; "Finding Protein Coding Genes in the Yeast Genome Based on the Characteristic Sequences", Internet Electronic Journal of Molecular Design", Sep. 2005, Vol. 4, No. 9, Pp. 613-62.

