# Two Level Text Data Encryption using DNA Cryptography

**E. Vidhya**
*Department of Computer Science*
*Periyar University*
*Salem, India*
*vidhya11tamilarasi@gmail.com*

**R. Rathipriya**
*Department of Computer Science*
*Periyar University*
*Salem, India.*
*rathi_priyar@periyaruniversity.ac.in*

***Abstract*- DNA Cryptography is one of new method in the cryptography research area. DNA can be used to encrypt the data in the form of storage and transmit and it also performs the computation. In DNA cryptography, the main role is to create a DNA sequence. The DNA sequence is created based on the information carrier and the biological technology. The main target of this paper is to increase the complexity of the DNA sequence. The main objective of this paper is to given the data in high security level. The proposed work of this paper is to provide two levels of security. The first level is to transform the plain text to an ASCII text with the shift key and then convert the text to a binary numbers. Apply the insertion method to binary numbers; convert the binary numbers to DNA sequence which is represented as cipher text. The receiver will apply the Insertion decryption method to cipher text the plaintext will appear. The Shannon entropy is used to measure the data compression and the time complexity is used to measure the execution time of the proposed work.**

**Keywords: DNA cryptography, Insertion method, Shannon entropy.**

## 1. INTRODUCTION

### 1.1 Data Encryption

Data encryption is a process to encrypt the data from one form to another form. This data is called an encrypted data. The encrypted data is mainly called as a cipher text. The original data is called as an plaintext. The data encryption contains two types. They are asymmetric encryption, also known as public-key encryption, and symmetric encryption.

In Data encryption the basic operation is a string operation. The substitution method is one of the basic methods in string operation. For example the plaintext string is traverse and each character is replaced by some other character according to a fixed rule.

The Caesar cipher scheme is one of the basic process in data encryption process to create the cipher text. The caser cipher process is to replacing each letter one by one the letter that appears k positions later in the alphabet for some integer k.

For example, using the character set A B C D E F G H I J K L M N O P Q R S T U V W X Y Z.

Encrypt the string “MARCH” with integer k has value 3:

Character set: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z.

Plaintext: MARCH

Cipher text: PDUFK

## 2.1 DNA Cryptography

DNA cryptography is one of the new fields to encrypt the data. DNA (Animesh Hazra) has been used new technologies like DNA Computation, PCR(Polymerase Chain Reaction), Microarray, etc.,. DNA computation (Fu) is high level computation and storing huge amount of data. A single DNA gram contains 1021 DNA base which is equal to 108 terabytes of data. (Nirantar, 2017), (Verma, 2014). In Figure.1 shows the DNA structure which contains an four bases that are Adenine(A), Thymine(T), Cytosine(C) and Guanine(G) and Phosphate backbone (Lee).Let us assume that the data has been encrypt in the form of A, G, C ,T with the combination of 0's and 1's shown in the table 1.

Table 1. DNA Binary Conversion

| DNA BASE | BINARY VALUE |
|---|---|
| A | 00 |
| G | 01 |
| C | 10 |
| T | 11 |

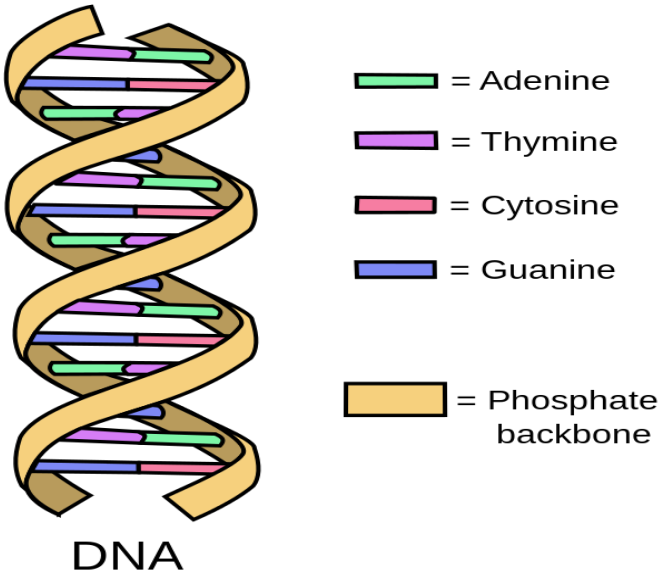


Figure 1. Structure of DNA

This paper is organised as follows: Section II describes the Literature Review needed for this research work. Section III discusses the methods required for the study. Section IV Proposed work is described. Section V presents the results with discussion in that the Shannon entropy for data compression and execution time complexity. Finally, section VI conclude the proposed work with possible future enhancement

# 2. RELATED WORKS

This section is to provide the general overview of related works in the field of DNA cryptography. In particular, for those works are survey and received in detailed of Insertion method technique are listed below.

| Author Name | DNA Cryptography | Description | Remarks |
|---|---|---|---|
| Prashanth Mogali and Neha Kaura | Novel algorithm for data encryption. | DNA cryptography research is fully depth on DNA computing. In this paper cost and complexity is higher for securing the data. | Reducing complexity and cost for encryption and providing high level security. |
| Ritu Mor and Praveen *Kanth* | Steganography | DNA cryptosystem provide lot of implementation | DNA is used for information storage. |
| H. Z. Hsu and R. C. T. Lee | Insertion method, Complementary method, Substitution method. | DNA sequences is used to encrypt data with a three methods. | Real time data has applied to this approach and example with an Mathematical properties. |
| Yunpeng Zhang* and Liu He Bochen Fu | PCR-based amplification technology and chaotic encryption system | Chaotic pseudo-random sequence is generate for handle the plaintext and then for eliminating the statistical rules which contains two ways. One is to makes the encryption algorithm protected the statistical attack. And the other one is to increases the key space.. | To Increase the decryption complexity use the new type of encryption system that is DNA code is based on a different security with some other code. |
| Sriram Vajapeyam | Shannon's Entropy | Uses of Shannon entropy and how to measure the entropy value for text and image data. | Shannon’s Entropy is used to calculate the lower-bound on the number of actual bits required to store or transmit information |
| Tausif Anwar, Abhishek Kumar, Sanchita Paul. | One time pad and DNA technologies | DNA Cryptography, new cryptography technique is proposed using Symmetric Key Exchange, one-time pad scheme and DNA hybridization to minimize time complexity. This method is very efficient in encrypting, hiding, transmitting and preventing powerful attacks. | The lot of traditional Cryptography techniques combined with DNA cryptography it gives a better hybridization. The use of higher complexity for encryption and decryption and to minimize the time complexity. |
| R. Pradeep Kumar Reddy, C. Nagaraju and N. Subramanyam | Steganography | The main role is to given high security to data; the proposed method is used three levels for encryption to encrypt the data. | In The text message contain only ASCII characters. Making it to work with any kind of text data only in the way of Unicode character set and the limitation is that if message contains binary data, it needs some kind of Mapping in lookup table for level-3. |

| Author Name | DNA Cryptography | Description | Remarks |
|---|---|---|---|
| Ashish Kumar Kaundal and A.K Verma | DNA cryptography | Analyze has been done about the DNA cryptographic and present the merits and demerits of each | Addition of one-time pad in DNA symmetric key cryptography makes it more strong and secure and protect from brute force attacks. |
| Animesh Hazra, Soumya Ghosh, and Sampad Jash. | Data Security, DNA Cryptography, E-Commerce | DNA cryptography methods and the techniques of real time implementation. Limitations of DNA cryptography and its advantages are explained. | DNA cryptography is implementation will need bio-molecular labs and costly instruments which are major constraints for the smooth progress in this field. |
| Wang | Information & Entropy. | How the entropy is worked and given with an simple example. | Calculate the entropy with an large data. |
| Nikita Parab, Ashwin Nirantar. | DNA Cryptography | survey of DNA cryptography, the advantages and challenges of these algorithms. | DNA cryptography indicate that biological molecules can be used for cryptographic purpose and has unique property. |
| H.J. Shiu, K.L. Ng, J.F. Fang, R.C.T. Lee, C.H. Huang. | Complementary pair, Data recovery | The data hiding methods crated based on the properties of DNA sequences. The three methods are: the Insertion Method, the Complementary Pair Method and the Substitution Method. | For all image media schemes and text message, the three methods are easy to implement and hard to detect |
| Mansi Rathi1, Shreyas Bhaskare, Tejas Kale, Niral Shah, Naveen Vaswani | DNA Cryptography, DNA Sequencing | This technique encrypt the data in a very complex and it prove it is very efficient algorithm with high accuracy | Implementing the DNA sequencing to the cipher text it will enable the cipher text to get strong encrypted and it can be also used for banking applications to encrypt the vital data of the customer such as the account number or pin or password. |

From the above study, it is observed that three level encryption techniques is used very frequently. But in this work, the two level encryption techniques is proposed to achieve better accuracy with in shorter execution time.

## 3. METHODS

### 3.1. Method 1: DNA Cryptography Encryption and Decryption

DNA Cryptography technology is creating a DNA sequence. The DNA sequence is called as a cipher text.

**Algorithm 1-1: Encryption algorithm for DNA Cryptography:**

**Input:** Plaintext as S.
**Output:** DNA Sequence as S'.
Step 1: Given the plaintext S and convert the S into their respective ASCII numbers (in decimal format) are grouped into blocks
Step 2: The ASCII numbers are converted into Binary numbers(0's and 1's).
Step 3: The Sequence of Binary numbers are broken in pairs. The pairs could be 00,01,10,11. These pairs are assigning to nucleotide such are given in table 1
Step 4: Based on Step 3 the DNA sequence as S' are created.
Step 5: Return S' and Send the S' to receiver.

In algorithm 1-1 the plaintext S can be converted into the respective ASCII numbers in decimal format are grouped into blocks and convert the ASCII numbers into the binary numbers 0's and 1's. The binary sequence are broken into an pairs with an 00,01,10,11 and the pairs can be represented in an table 1. The DNA sequence has been created as S' and it is represented as a cipher text.

**Algorithm 1-2: Decryption algorithm for DNA Cryptography:**

**Input :** DNA Sequence as S'.
**Output:** Plaintext as S.
Step 1: The DNA Sequence S' is received from sender.
Step 2: S' is converted into Binary numbers.
Step 3: The Binary numbers are converted to an ASCII numbers.
Step 4: ASCII numbers are transferred as on plaintext S.
Step 5: Return S.

In algorithm 1-2: the DNA sequence S' is received from sender and the DNA sequence S' is converted into binary numbers as 0's and 1's. The binary numbers are converted to an ASCII numbers. The numbers are transferred as a plaintext S. the receiver can decrypt the original text.

### 3.2. Method 2: Insertion Method for Encryption and Decryption:

**Algorithm 2-1: Encryption algorithm for Insertion Method:**

**Input:** DNA Sequence SS, a secret binary message M and a binary coding scheme to code A ,C, G and T.
**Output:** Fake DNA Sequence SS1.
Step 1: Convert DNA Sequence SS to binary sequence by using the binary coding scheme.
Step 2: Divide SS into segments of random number generate as k bits represented S1 and generate r To divide the secret message M into Segments. Each k and r is larger than 1 or equal to 1. Denote S1 as s1,s2,s3,…,sn and M by m1,m2,m3,…,mn.
Step 3: Insert each mi of M before si of S1 to produce new binary sequence . Delete s p+1, sp+2,..,sn. Denote the resulting binary sequence by s2.
Step 4: Convert the binary sequence s2 to a fake DNA sequence SS1 by using same binary coding scheme used in Step 1.
Step 5: Return SS1.

In algorithm 2.1 the DNA sequence are encrypted with an secret message. The secret message can be added to the suffix of the DNA sequence and create the fake DNA sequence. The fake DNA sequence is send to an receiver by sender.

**Algorithm 2-2: Decryption algorithm for Insertion Method**

**Input:** DNA Sequence SS, a secret binary message M and a binary coding scheme to code A ,C, G and T.
**Output:** Fake DNA Sequence SS1.
Step 1: Convert DNA Sequence SS to binary sequence by using the binary coding scheme.
Step 2: Divide SS into segments of random number generate as k bits represented S1 and generate r
To divide the secret message M into Segments. Each k and r is larger than 1 or equal to 1.
Denote S1 as s1, s2, s3,…,sn and M by m1,m2,m3,…,mn.
Step 3: Insert each mi of M before si of S1 to produce new binary sequence. Delete s p+1, sp+2,..,sn.
Denote the resulting binary sequence by s2.
Step 4: Convert the binary sequence s2 to a fake DNA sequence SS1 by using same binary coding scheme used in Step 1.
Step 5: Return SS1.

In algorithm 2.2, The Fake DNA sequence is received by the receiver. The receiver can remove the suffix secret message in the fake DNA sequence and the receiver can fetch the original DNA sequence. In this algorithm, the attackers cannot easily fetch the original message.

## 4. PROPOSED ENCRYPTION SCHEME.

The proposed work is to eliminate the limitations of existing method of low security. The two level of security is explained below.

Level 1: Shift key value.

Level 2 : Insertion Method.

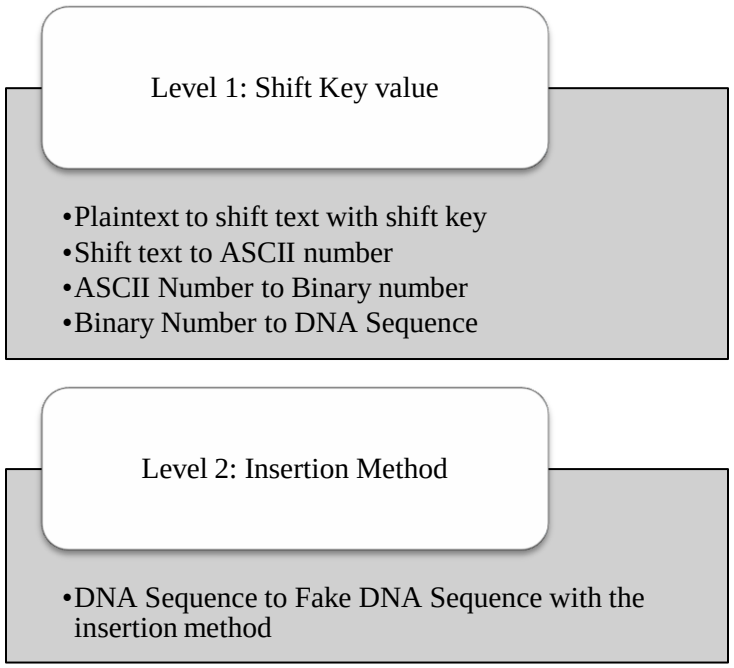


Figure 2. Steps showing where to apply keys

### 4.1 Proposed Work Flow for Encryption and Decryption Process

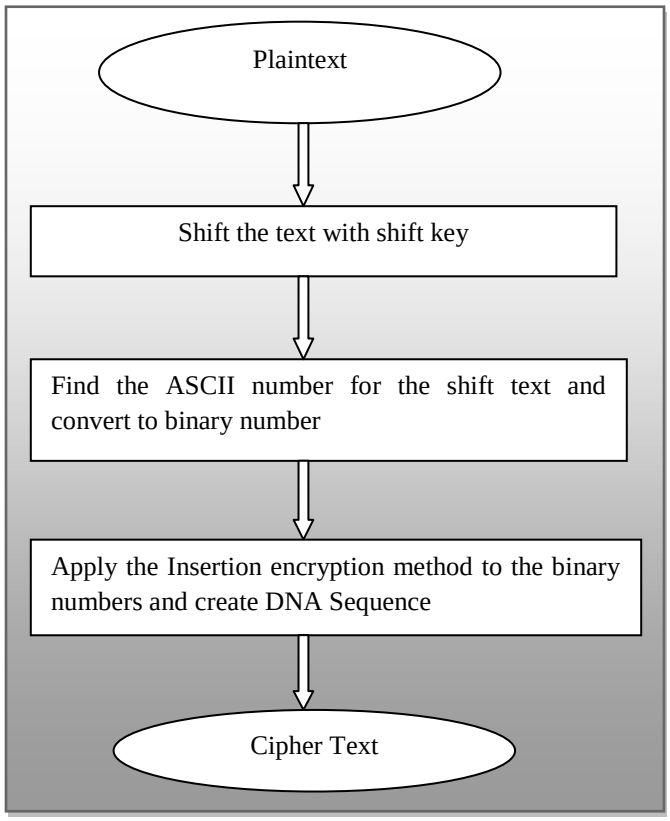


Figure 3. Flow chart for Encryption.

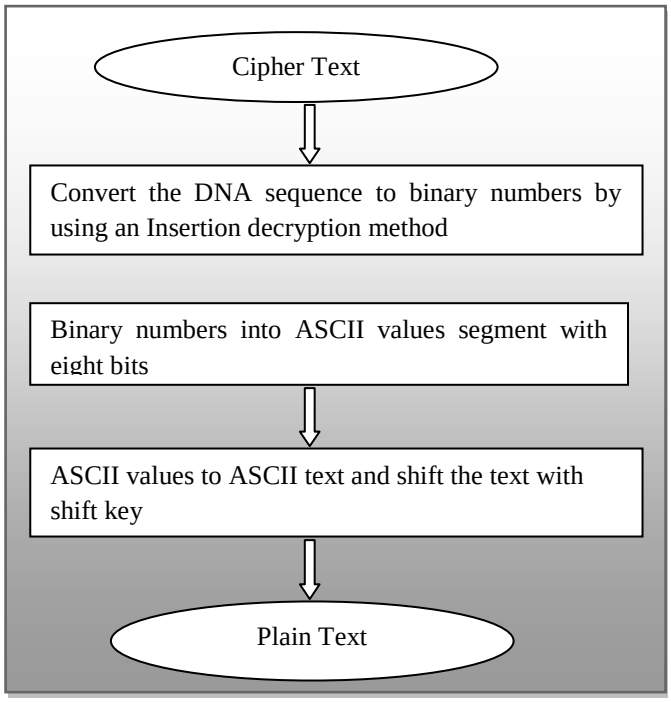


Figure.4. Flow chart for Decryption

Encryption process the plaintext is taken. The shift key is apply to the plaintext in that the shift text is occurred for that the shift text the ASCII number is found. Convert the ASCII number to the binary number. The Insertion method is apply to the binary numbers and the binary numbers are converted to an DNA sequence based on the table 1. In figure 3 the cipher text are created and send to an receiver.

The Receiver can receive the DNA sequence. Convert the DNA sequence to binary based on the table 1. And remove the suffix secret message. Based on figure 4 the binary numbers are converted to an ASCII numbers with the weight of eight bits. The ASCII numbers are transfer to an ASCII values for that ASCII values apply the shift key the plaintext is occurred by an receiver. In figure 4. The decryption process is done by receiver.

## 4.2 Proposed Algorithm

**Algorithm 1: Encryption algorithm for DNA cryptography with Insertion method**

**Input:** Plaintext S.
**Output:** Cipher text S'.
*/* First Level*/*
Step 1: Input the plaintext and shift the plaintext by using key (k1) of any length.
Step 2: Convert the shift text to the ASCII values.
Step 3: ASCII values can be convert to a binary numbers.
*/* Second Level*/*
Step 4: Apply the Insertion Encryption method to binary numbers and create DNA Sequence with the DNA conversion table.
Step 5: Return Cipher text.

In the proposed algorithm 1. The plaintext has converted to a shift text with shift key and the shift value is converting an ASCII numbers to a binary numbers. Apply the Insertion method to binary numbers and create a DNA sequence based on table 1 and the sender get the cipher text. The cipher text is send to a receiver.

**Algorithm 2: Decryption algorithm for DNA cryptography with Insertion method**

**Input:** Cipher text S'.
**Output:** Plaintext S.
Step 1: Replace the received text with DNA sequence by applying Insertion Decryption Method.
Step 2: Convert the DNA sequence into binary numbers by using the DNA binary conversion table.
Step 3: Convert the binary values into correspondent ASCII values with an segment of 8.
Step 4: Shift the ASCII values with the key length of (k1).
Step 5: Return Plaintext.

Algorithm 2, The reverse process of algorithm 1. The receiver can receive the DNA sequence from the sender. The receiver remove the secret message and the convert the binary values to ASCII number. ASCII numbers to ASCII values that values are shift by shift key and the original text is appeared by the receiver.

## 4.3 Example for Proposed Algorithm

**Encryption process:**

*// first level encryption*

*Plaintext :* CRYPTOGRAPHY.
*Shift key :* 5
*Shift text :* HWDUYTLWFUMD

Table 2. Conversion table of ASCII character to DNA sequence.

| Shift text | ASCII Values | Binary values | Binary values Segment | DNA Sequence |
|---|---|---|---|---|
| H | 72 | 01001000 | '01', '00', '10', '00' | ['G', 'A', 'C', 'A'] |
| W | 87 | 01010111 | '01', '01', '01', '11' | ['G', 'G', 'G', 'T'] |
| D | 68 | 01000100 | '01', '00', '01', '00' | ['G', 'A', 'G', 'A'] |
| U | 85 | 01010101 | '01', '01', '01', '01' | ['G', 'G', 'G', 'G'] |
| Y | 89 | 01011001 | '01', '01', '10', '01' | ['G', 'G', 'C', 'G'] |
| T | 84 | 01010100 | '01', '01', '01', '00' | ['G', 'G', 'G', 'A'] |
| L | 76 | 01001100 | '01', '00', '11', '00' | ['G', 'A', 'T', 'A'] |
| W | 87 | 01010111 | '01', '01', '01', '11' | ['G', 'G', 'G', 'T'] |
| F | 70 | 01000110 | '01', '00', '01', '10' | ['G', 'A', 'G', 'C'] |
| U | 85 | 01010101 | '01', '01', '01', '01' | ['G', 'G', 'G', 'G'] |
| M | 77 | 01001101 | '01', '00', '11', '01' | ['G', 'A', 'T', 'G'] |
| D | 68 | 01000100 | '01', '00', '01', '00' | ['G', 'A', 'G', 'A'] |

*Concatenate the binary values segment*

['01', '00', '10', '00', '01', '01', '01', '11', '01', '00', '01', '00', '01', '01', '01', '01', '01', '01', '10', '01', '01', '01', '01', '00', '01', '00', '11', '00', '01', '01', '01', '11', '01', '00', '01', '10', '01', '01', '01', '01', '01', '00', '11', '01', '01', '00', '01', '00']

*//Second level encryption*

*Secret message:*['1010000101010101'] → ['1', '0', '1', '0', '0', '0', '0', '1', '0', '1', '0', '1', '0', '1', '0', '1']

*Bits for segmentation:* 3

['010', '010', '000', '101', '011', '101', '000', '100', '010', '101', '010', '101', '100', '101', '010', '100', '010', '011', '000', '101', '011', '101', '000', '110', '010', '101', '010', '100', '110', '101', '000', '100']

*Add the secret message to binary values segment*

[0101, 0100, 0001, 1010, 0110, 1010, 0000, 1001, 0100, 1011, 0100, 1011, 1000, 1011, 0100, 1001, 0101, 0110, 0001, 1010, 0110, 1010, 0000, 1101, 0100, 1011, 0100, 1001, 1100, 1011, 0000, 1001]

*Segmentation above binary values to two*

['01', '01', '01', '00', '00', '01', '10', '10', '01', '10', '10', '10', '00', '00', '10', '01', '01', '00', '10', '11', '01', '00', '10', '11', '10', '00', '10', '11', '01', '00', '10', '01', '01', '01', '01', '10', '00', '01', '10', '10', '01', '10', '10', '10', '00', '00', '11', '01', '01', '00', '10', '11', '01', '00', '10', '01', '11', '00', '10', '11', '00', '00', '10', '01']

*Cipher text*
GGGAAGCCGCCCAACGGACTGACTCACTGACGGGGCAGCCGCCCAATGGACTGACGTACTAACG]

**Decryption process:**

*Receive the cipher text*

**[**GGGAAGCCGCCCAACGGACTGACTCACTGACGGGGCAGCCGCCCAATGGACTGACGTACTAACG]

Cipher text to binary values based on DNA conversion table (table 1)

['01', '01', '01', '00', '00', '01', '10', '10', '01', '10', '10', '10', '00', '00', '10', '01', '01', '00', '10', '11', '01', '00', '10', '11', '10', '00', '10', '11', '01', '00', '10', '01', '01', '01', '01', '10', '00', '01', '10', '10', '01', '10', '10', '10', '00', '00', '11', '01', '01', '00', '10', '11', '01', '00', '10', '01', '11', '00', '10', '11', '00', '00', '10', '01']

*Concatenate the above values*

0101010000011010011010100000100101001011010010111000101101001001010101100001101001101010000011010100101101001001111001011000010010

*Bits for segmentation:* 3

['010**1**', '010**0**', '000**1**', '101**0**', '011**0**', '101**0**', '000**0**', '100**1**', '010**0**', '101**1**', '010**0**', '101**1**', '100**0**', '101**1**', '010**0**', '100**1**', '010**1**', '011**0**', '000**1**', '101**0**', '011**0**', '101**0**', '000**0**', '110**1**', '010**0**', '101**1**', '010**0**', '100**1**', '110**0**', '101**1**', '000**0**', '100**1**']

*Remove the secret message*

['010', '010', '000', '101', '011', '101', '000', '100', '010', '101', '010', '101', '100', '101', '010', '100', '010', '011', '000', '101', '011', '101', '000', '110', '010', '101', '010', '100', '110', '101', '000', '100']

*Concatenate*

['0100100001010111010001000101010101011001010101000100110001010111010001100101010101001101010000100']

*Segment by two bits*

['01', '00', '10', '00', '01', '01', '01', '11', '01', '00', '01', '00', '01', '01', '01', '01', '01', '01', '10', '01', '01', '01', '01', '00', '01', '00', '11', '00', '01', '01', '01', '11', '01', '00', '01', '10', '01', '01', '01', '01', '01', '00', '11', '01', '01', '00', '01', '00']

*Convert to DNA sequence based on DNA Conversion Table (table 1)*

['G', 'A', 'C', 'A', 'G', 'G', 'G', 'T', 'G', 'A', 'G', 'A', 'G', 'G', 'G', 'G', 'G', 'G', 'C', 'G', 'G', 'G', 'G', 'A', 'G', 'A', 'T', 'A', 'G', 'G', 'G', 'T', 'G', 'A', 'G', 'C', 'G', 'G', 'G', 'G', 'G', 'A', 'T', 'G', 'G', 'A', 'G', 'A']

*Convert DNA Sequence to Binary values*

['01', '00', '10', '00', '01', '01', '01', '11', '01', '00', '01', '00', '01', '01', '01', '01', '01', '01', '10', '01', '01', '01', '01', '00', '01', '00', '11', '00', '01', '01', '01', '11', '01', '00', '01', '10', '01', '01', '01', '01', '01', '00', '11', '01', '01', '00', '01', '00']

*Segment the binary values eight bit*

[['01', '00', '10', '00'], ['01', '01', '01', '11'], ['01', '00', '01', '00'], ['01', '01', '01', '01'], ['01', '01', '10', '01'], ['01', '01', '01', '00'], ['01', '00', '11', '00'], ['01', '01', '01', '11'], ['01', '00', '01', '10'], ['01', '01', '01', '01'], ['01', '00', '11', '01'], ['01', '00', '01', '00']]

*Join every eight bits*

[['01001000'], ['01010111'], ['01000100'], ['01010101'], ['01011001'], ['01010100'], ['01001100'], ['01010111'], ['01000110'], ['01010101'], ['01001101'], ['01000100']]

Table 3. conversion binary values to shift text

| Binary values | ASCII Values | Shift text |
|---|---|---|
| 01001000 | 72 | H |
| 01010111 | 87 | W |
| 01000100 | 68 | D |
| 01010101 | 85 | U |
| 01011001 | 89 | Y |
| 01010100 | 84 | T |
| 01001100 | 76 | L |
| 01010111 | 87 | W |
| 01000110 | 70 | F |
| 01010101 | 85 | U |
| 01001101 | 77 | M |
| 01000100 | 68 | D |

*Shift text:* HWDUYTLWFUMD

*Shift key:* 5

*Plaintext:* CRYPTOGRAPHY

# 5. RESULTS AND DISCUSSION

## 5.1 Shannon Entropy

Shannon entropy is defined as the amount of information in a variable, that variable has been providing the basic theory around the notation of information. It can be simply defined in terms of probabilistic model. (Entropy (information theory)), (Wang).It means that the modules which have many possible rearrangements then the system has high entropy, and the system have very few rearrangement, then the system has low entropy.

The Shannon entropy equation (1) is used to estimate the average minimum number of bits needed to encode a string of symbols, based on the frequency of the symbols.

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log_b P(x_i) \quad (1)$$

Where P is Probability of given symbol, b is the base of logarithm

Table.2. Shannon Entropy with Frequencies of alphabet symbols

| Number of Characters | Shannon Entropy Value | Frequencies of Alphabet Symbols | | | |
|---|---|---|---|---|---|
| | | A | C | T | G |
| 3 | 1.88 | 0.187 | 0.375 | 0.125 | 0.312 |
| 101 | 1.90 | 0.283 | 0.291 | 0.133 | 0.291 |
| 482 | 1.921 | 0.316 | 0.268 | 0.120 | 0.294 |
| 1809 | 1.935 | 0.314 | 0.253 | 0.133 | 0.298 |
| 599 | 1.937 | 0.316 | 0.253 | 0.135 | 0.294 |
| 601 | 1.929 | 0.312 | 0.266 | 0.126 | 0.294 |

In table 2. Shannon entropy value are calculated based on number of character presented in first column for the number of character the alphabet symblos A, C, T, G frequencies values are calculated

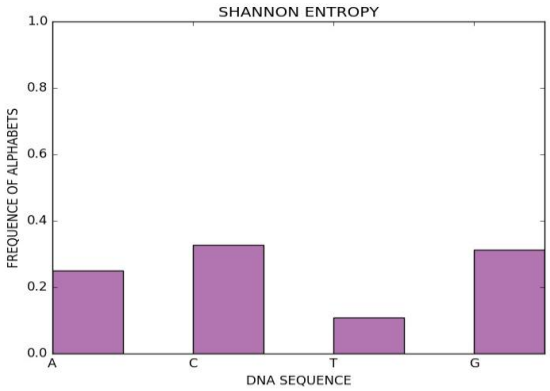


Figure.5. Shannon entropy with Frequencies of alphabet symbols (diagram for 1809 characters)

## 5.2 Execution Time

The experiments are conducted by number of characters. In proposed system the execution time are calculated based on the number of characters which are presented in table 3. The characters are increased the execution time also increased.

Table .3. Execution Time complexity

| Text in Characters | Execution Time in Milliseconds(m/s) |
|---|---|
| 3 | 2.37 |
| 101 | 3.86 |
| 482 | 4.93 |
| 931 | 6.52 |
| 601 | 6.04 |
| 1448 | 7.46 |
| 1446 | 7.09 |
| 1809 | 9.34 |

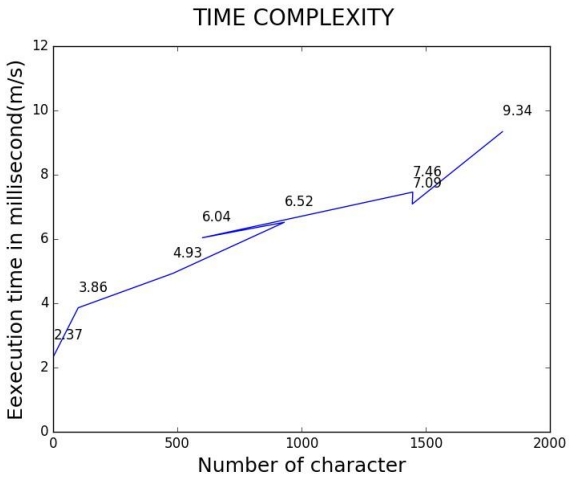


Figure .6. Execution Time complexity

## 6. CONCLUSION

The data security plays a vital role in the many places. Large numbers of data are occurred every day but the data security level is low. The main contribution of this paper is to improve the data security level to high by using DNA cryptography with insertion method. The proposed work is to encrypt the data with a DNA sequence and with an Insertion method. It is difficult for an attacker to achieve the original data. If the DNA sequence is known by any of the attacker, it is impossible to get correctly decrypted the data without knowing about the Insertion method secret message. This proposed work is to secure the text data with a high level security by the measure of data compression values. In future the proposed work is applied to a different types of data like an image, video, audio and soon.

## REFERENCES

Animesh Hazra, S. G. A Review on DNA Based Cryptographic Techniques. International Journal of Network Security , 20 (6).

Bandyopadhyay, D. B. Embedding Data in DNA Sequence for Security. International Journal of Reliable Information and Assurance , 1 (1).

Data Security Using DNA Cryptography. (2016). International Journal of Computer Science and Mobile Computing, 5 (10), 123 – 129.

Fu, Y. Z. Research on DNA Cryptography. College of Software and Microelectronics Northwestern Polytechnical University .

H.J. Shiu, K. N. Data hiding methods based upon DNA sequences. Information Sciences, Elsevier .

Kanth, R. M. (2015). A Research Paper of DNA Cryptography Security Enhancement. International Journal of Computer Application , 5 (6).

Kaura, P. M. (2016). Encryption Algorithm Based On DNA Strand. International Science Press , 9 (33), 49-59.

Lee, H. Z. DNA Based Encryption Methods.

Nirantar, N. P. (2017). Survey of different DNA Cryptography based algorithms. International Research Journal of Engineering and Technology , 4 (12).

R. Pradeep Kumar Reddy, C. N. (2014). Text Encryption Through Level Based Privacy Using DNA Steganography. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) , 3 (3).

Tausif Anwar, A. K. . DNA Cryptography Based on Symmetric Key Exchange. International Journal of Engineering and Technology .

Vajapeyam, S. (2014, March). Understanding Shannon's Entropy metric for Information.

Verma, A. K. (2014). DNA Based Cryptography: A Review. International Journal of Information & Computation Technology., 4 (7).

Wang. Information & Entropy.