Received: April 2
Revised: May 5
Accepted: May 16

A Comparative Analysis of DES, AES and Blowfish Based DNA Cryptography

Narayan Dhamala[1]
[1]Department of Computer Science and Application
Mechi Multiple Campus, Bhadrapur, Jhapa
Tribhuvan University, Nepal
Krishna Prasad Acharya[2]
[2]Department of Computer Science and Application
Mechi Multiple Campus, Bhadrapur, Jhapa
Tribhuvan University, Nepal

Abstract

Protecting sensitive information while transmitting data across communication channel is very important. The field of study which deals with transmitting information in an unreadable form isknown as cryptography. A modern cryptography technique, DNA Cryptography, is used to encode messages in the form of DNA genes. The DNA consists of four genes: Adenine (denotedby A), Cytosine (denoted by C), Thymine (denoted by T) and Guanine (denoted by G). The DNA encryption process converts the given messages in the form DNA sequences and the DNA decryption process converts the resulting DNA sequences in the original form. In this paper, the output of three different Symmetric Cryptographic algorithms: DES, AES and Blowfish are compared in terms of average encryption time, average decryption time for different datasets and the effect of length of plaintext on encryption time and decryption is analyzed so as to measure the performance of those algorithms. While comparing the above algorithm it is found that: The AES based DNA Cryptography algorithm takes more encryption and decryption time while the DES based DNA algorithm takes less encryption time and the Blowfish based DNA algorithm takes less decryption time. The result also shows that the decryption time is much faster as compared to that of encryption time.

Keywords: Cryptography, Decryption, Encryption, Key, XOR**.**

Introduction

In today's competitive world, data is the most important valuable resources. The organizations may have important data that needs to be passed through insecure channel like: internet. So, a method, called cryptography, is needed to facilitate stronger security. The encryption process converts the given plaintext (original message) in the form of ciphertext (decoded message) and the decryption process converts the ciphertext into plaintext. There are two types of modern cryptographic algorithms: Symmetric key cryptography and Asymmetric key cryptography. The symmetric key cryptography uses the single secret key for both encryption and decryption where as the asymmetric key cryptography uses two keys: one for encryption and other for decryption. The cryptographic algorithms like: DES, Triple DES, AES, Blowfish, RC4 and RC5 are symmetric key cryptography whereas algorithms like: RSA, Digital Signatures are asymmetric key cryptography. Some symmetric cryptographic algorithms are breakable cryptosystem while till now some cryptographic algorithms are unbreakable but a consideration is needed for the future which helps to protect data more securely. For that the concept of DNA Cryptography is used. The DNA Cryptography is a field of cryptography which encodes messages in the form of DNA Genes (A- Adenine, C- Cytosine, T-Thymine and G-

Guanine) instead of binary bits. For coding each gene, a pair of binary digits are used which are presented in the below table.

Table 1

Mapping table for a Gene

Gene	Binary Digit
A	00
T	01
C	10
G	11

DES (Data Encryption Standard)

DES is a symmetric block cipher algorithm that takes a plain text block of length 64-bit and key length of apparently 64-bits but the 8^{th} key bit is used for parity checking so effective key length is 56-bits and produces a cipher text block of length 64-bits.

AES (Advanced Encryption Standard)

AES is a symmetric block cipher algorithm which is used to encrypt the data blocks of 128bits by using symmetric keys of length 128, 192 or 256 bits.

Blowfish

Blowfish is a symmetric block cipher algorithm which is used as an alternative to DES encryption algorithm. It uses a 64-bit block size and variable length key size varying from 32 to 448 bits. The blowfish uses 4 substitution boxes having 18 numbers of sub keys and 16 rounds in total.

DNA Cryptography

DNA cryptography is an emerging field of cryptography which deals with encrypting data in the form of DNA sequences and decrypting resulting DNA form cipher text in original form.

Encryption Process

a) Convert each input text to ASCII value and then each ASCII value to 8-bit binary value.
b) Generate a random sequence of binary number (called as Key in DNA Cryptography) that is equal to the length of the input text in binary form.
c) Perform the XOR operation between binary value obtained from step a) and b).
d) Start scanning the pair of binary sequence, obtained from XOR operation result, from left to right to find the Occurrences of 0's and 1's.
   - If first two digit of binary bit is 00 then replace it with alphabet 'A'.
   - If first two digit of binary bit is 01 then replace it with alphabet 'T'.
   - If first two digit of binary bit is 10 then replace it with alphabet 'C'.
   - If first two digit of binary bit is 11 then replace it with alphabet 'G'.
e) Repeat step d) for all the occurrences of 1 s and 0 s and put them all together to obtain the resulting cipher text in DNA Sequence form

The Decryption algorithm is the reverse process of DNA encryption algorithm.

Problem Statement

The classical cryptographic algorithms like: Shift cipher, vigenere cipher, vernam cipher, hill cipher, ceaser cipher are easily breakable cryptosystem. Some modern cryptographic algorithms like: DES, Blowfish are vulnerable to cryptographic attacks but still they are in use because of their standardness and fastness. The AES algorithm till now is unbreakable but it has simpler

algebraic structure and can be encrypted each block in the same manner. So in AES, if the logic for one block encryption is known then the whole block can be easily known hence a future security is needed that makes it difficult to attack the block. The Blowfish algorithm is vulnerable to cryptographic attack due to its small key size. A large number of algorithms exist for encrypting and decrypting the data but the selection of best algorithm is a wide spread problem. Hence in this research, the comparative study of DES, AES and Blowfish Based DNA cryptography is done based on the parameters: average encryption time and average decryption time and the effect of length of plaintext on encryption time and decryption time is analyzed.

Research Questions

Some important research questions in this study are as follows:

1. How traditional cryptographic algorithm security strength can be enhanced by applying the concept of DNA Encoding scheme on them?
2. Out of three algorithms (DES based DNA Cryptography, AES based DNA Cryptography and Blowfish based DNA Cryptography) which algorithm takes less encryption time in an average?
3. Out of three algorithms (DES based DNA Cryptography, AES based DNA Cryptography and Blowfish based DNA Cryptography) which algorithm takes less decryption time in an average?
4. What is the effect of length of plaintext on encryption and decryption time?
5. Either Encryption or Decryption algorithm takes less time?

Objective

The main objectives of this research are as follows:

- To encode messages in the form of DNA sequences and decode DNA sequences in the form of original message by using DES, AES and Blowfish based DNA cryptographic algorithms.
- To perform the comparative analysis of those algorithms based on average encryption time, average decryption time and the effect of length of plaintext on encryption time and decryption time.

Literature Review

The purpose of the study described by Hammad, B. T., and et.al. (2020) [4] is to perform a comparative review on symmetric and asymmetric DNA based cryptography. The DNA cryptography uses four bases A, C, T and G in which a pair of binary code is used to denote each bases of DNA. The two binary digit 00 is represented by A, 01 is represented by T, 10 is represented by C and 11 is represented by G. The symmetric algorithm OTP and Asymmetric algorithm RSA along with it's DNA combination DNA-OTP and DNA-RSA is used to analyze the size of plain text and size of cipher text for each test cases and encryption and decryption time comparison among those algorithms. The result shows that the DNA- RSA algorithm encrypts the text file into huge size while the other algorithms take a normal size. The size of decryption text in DNA-OTP is about four times more than plaintext because the plaintexts are converted into DNA bases form. The DNA sequence takes more execution time for both encryption and decryption due to nature of conversion in DNA coding.

In a study conducted by Al-Mahdi and et.al. (2019) [2] design and analyze DNA encryption and decryption technique based on asymmetric cryptography system. Here the asymmetric (RSA) cryptography DNA encoding technique is used for encoding and decoding the plaintexts. The basic idea used by author is to create a dynamic DNA table based on the plaintext, using multilevel security, generating 14 round keys and performing the encryption and decryption

process. The performance of this proposed method is tested in terms of avalanche effect and found that avalanche effect is found to be good.

In the paper of Ahmed and et.al. (2017) [1] developed a new hybrid cipher algorithm using DNA and RC4. To add more complexity and make system more secure, the author combines a stream cipher algorithm RC4 and DNA indexing algorithm. The pair of binary digits is replaced by A, C, T, G bases in this indexing scheme. The performance of the algorithms is analyzed in terms of secrecy of cipher, randomness test and encryption time. The result shows that RC4-DNA algorithm provides more secrecy and more randomness compared to RC4 but native RC4 algorithm executes faster than Proposed RC4-DNA algorithm.

In a study published by Kolate and et.al. (2021) [2] performed an information security using DNA cryptography along with AES algorithm. Here the input message is first converted into an ASCII value form. The ASCII numbers are then grouped into blocks by applying encoding scheme for a pair of binary digits to encode in DNA sequence form. Apply the DNA processed AES algorithm and finally transform the resulting DNA sequence form in to binary form. By varying the message input size the performance of the algorithm: AES and AES with DNA is analyzed on the basis of encryption time and found that the AES with DNA takes more time for each input test cases than AES solely.

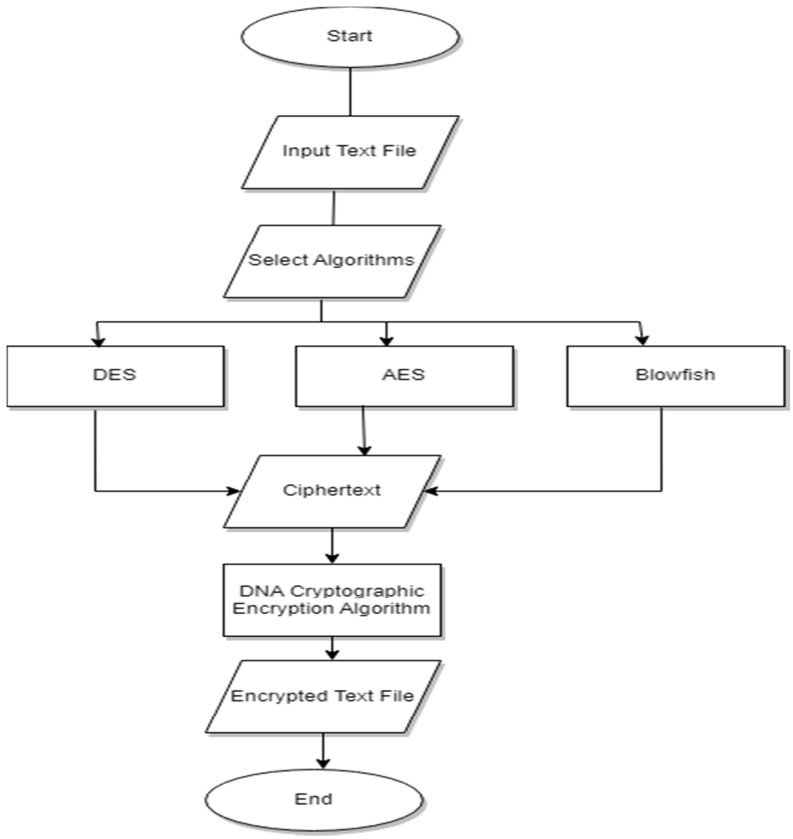
The authors Elkamchouchi and et.al. (2018) [3] performed security enhancement of blowfish algorithm using DNA genetic technology. In order to increase confusion and diffusion, the input data is changed using rotation and XOR'ed to produce new plaintext for blowfish algorithm. Then the resulting data is encrypted with blowfish several stages of the DNA genetic technique were added. The security is analyzed for blowfish and DNA Genetic technique and the avalanche effect is also calculated. The result shows that the proposed DNA genetic technique has more avalanche effect than that of blowfish.

In a study published by Sohal and et.al[6] performed a comparative analysis of symmetric key cryptographic algorithms (DNA, DES, AES, Blowfish) with a new proposed novel symmetric key encryption cryptographic technique (BDNA) which is inspired by DNA Cryptography. The comparative analysis is done in terms of cipher text size, encryption time and throughput. The result shows that the newly proposed technique outperforms the traditional method.

Methodology

The overall methodology of DES, AES and Blowfish based text file encryption can be represented by the following flowchart.

Figure 1
Overall Methodology of Text File Encryption



Data Collection

The input data for the experiment are the primary as well as secondary data. The different text datasets that may vary in length are used. The text file may contain different types of text like: alphabets only, digits only, special symbols only and the combination of all above. The secondary dataset for this research purpose are collected from different online tools, and paragraph from newspaper.

The different test dataset used in this research are as follows:

Dataset 1

This is the small primary dataset which contains only special symbols. The random special symbols are typed in office word and used as a testing dataset. The length of the plaintext in this data set is 150.

Dataset 2

This is the secondary dataset which contains only alphabets symbols and this dataset is taken from Himalayan Times Newspaper (https://thehimalayantimes.com/opinion/editorial-decide-cases-in-time). The special symbols are removed from there and only the alphabets having size 600 is taken.

Dataset 3

This is the secondary dataset which contains only digits. The digits having the size 600 is generated by using online random digit generator tool (https://onlinetools.com/random/generate-random-digits).

Dataset 4

This is the primary dataset which contains the combinations of all above. The length of the plaintext in this data set is 1200. The random alphabets, digits and special symbols are typed in the office word and are used as a dataset.

Research Method

The quantitative research method is most suitable in this research since to compare and to analyze the mentioned algorithm, the performance parameters like: the average encryption time, t -he average decryption time and the effect of length of plaintext on encryption time and decryption time the data is required.

Algorithms

The different algorithms used for encryption and decryption of text file in this research are as follows

DES Based DNA Cryptographic Algorithm (DSDNA)

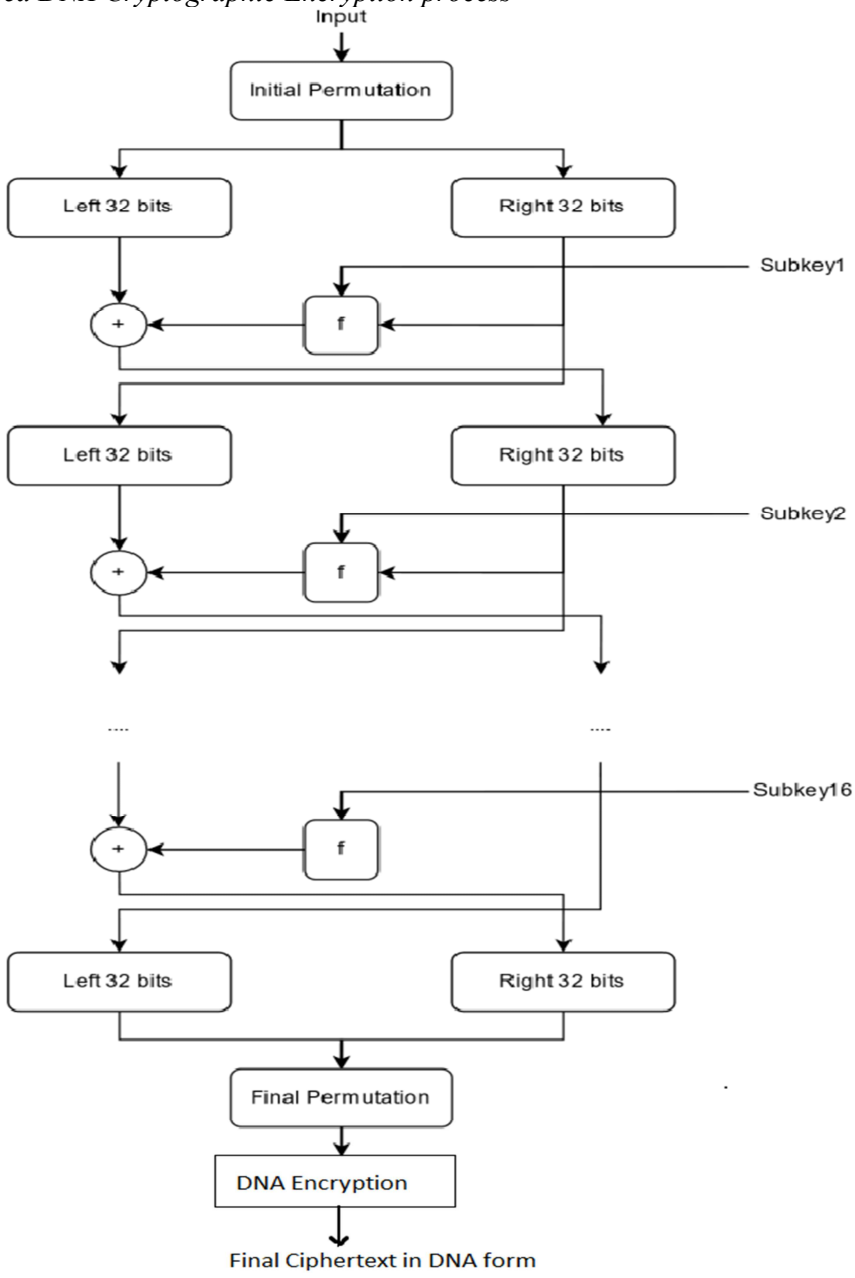
The encryption algorithm for DSDNA is as follows

1. The given text file is input which is divided into a block of 64-bits and A block of 64-bits is permutated by an initial permutation called IP.
2. Resulting 64-bits are divided into two equal halves, each containing 32-bits, left and right halves.
3. Right half goes through a function F (Feistel Function)
4. Left half is XOR-ed with output from the F function obtained in above step.
5. Left and Right half are swapped (except last round).
6. IF last round, apply an inverse permutation (IP^{-1}) on both halves that is the last step which produces a cipher text.
7. Apply DNA Cryptographic algorithm to the resulting Cipher text to produce the final cipher text in the form of DNA Sequences.

The Decryption algorithm of DSDNA is the reverse process of DSDNA encryption algorithm.

Figure 2

DES Based DNA Cryptographic Encryption process



AES Based DNA Cryptographic Algorithm (ASDNA)

The encryption algorithm for ASDNA is as follows:

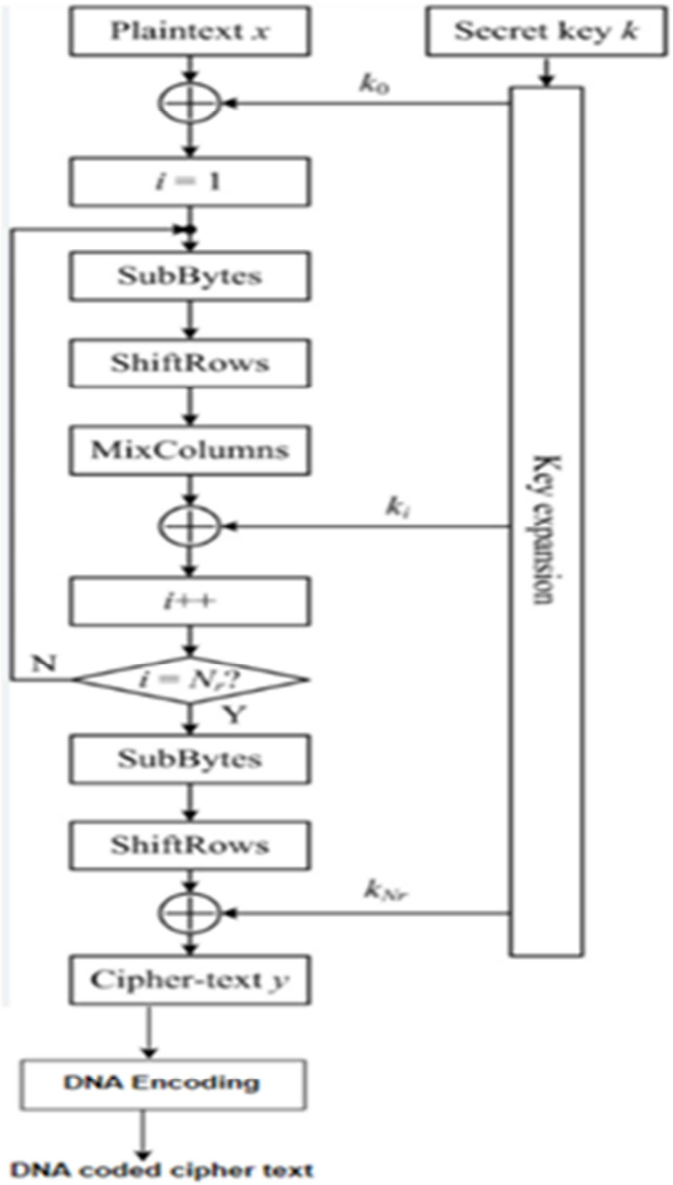
1. Input a text file which is divided into a block of 128-bits
2. Derive the set of round keys from the cipher key.
3. Initialize the state array with the block data (plain text).

4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (cipher text).
7. Apply DNA Cryptographic algorithm to the resulting Cipher text to produce the final cipher text in the form of DNA Sequences.

The Decryption algorithm of ASDNA is the reverse process of ASDNA encryption algorithm.

Figure 3

AES Based DNA Cryptographic Encryption Process



Blowfish Based DNA Cryptographic Algorithm (BSDNA)

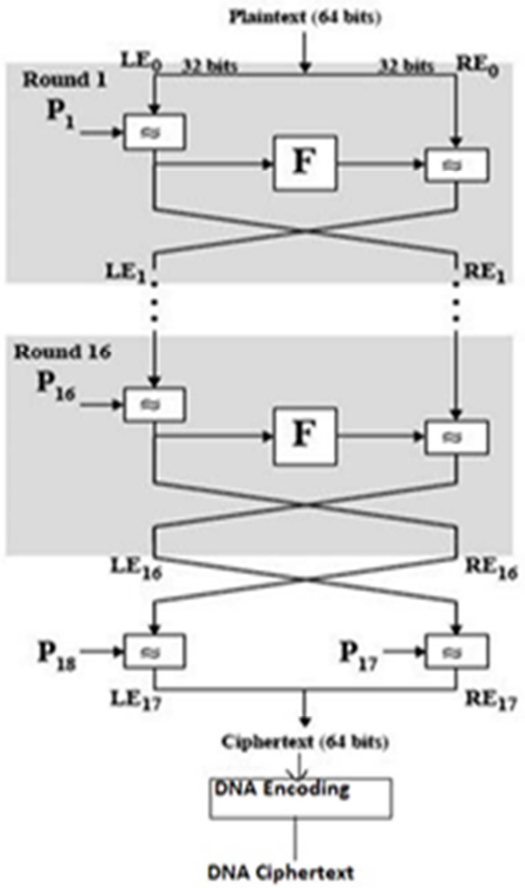
The encryption algorithm of BSDNA is as follows:

1. The first step is to initiate the substitution box (Sbox) and permutation box (Pbox).
2. Next, split 64-bit plaintext into two equal blocks, L and R.
3. Enter an encryption loop that runs 16 times. The following steps take place in each loop:
   a. XOR L with P_i, where i depends on the loop's current iteration.
   b. Then XOR R with F, which is a function of L that makes use of the Sbox split into 4 blocks.
   c. Finally, L and R are swapped before the loop enters its next iteration.
4. After the loop finishes, L and R are swapped once more.
5. Next, make use of last two unused Pbox entries by XORing R with Pbox entries and L with P box entries.
6. Finally, combine L and R to retrieve the cipher text of Blowfish.
7. Apply DNA Cryptographic algorithm to the resulting Cipher text to produce the final cipher text in the form of DNA Sequences.

The Decryption algorithm of BSDNA is the reverse process of BSDNA encryption algorithm.

Figure 4

Blowfish Based DNA Cryptographic Algorithm



Result, Analysis and Comparison

The results obtained by implementing the above mentioned algorithm on analysis parameters: average encryption time, average decryption time and the effect of length of plaintext on encryption time and decryption time are presented in the bar graph.

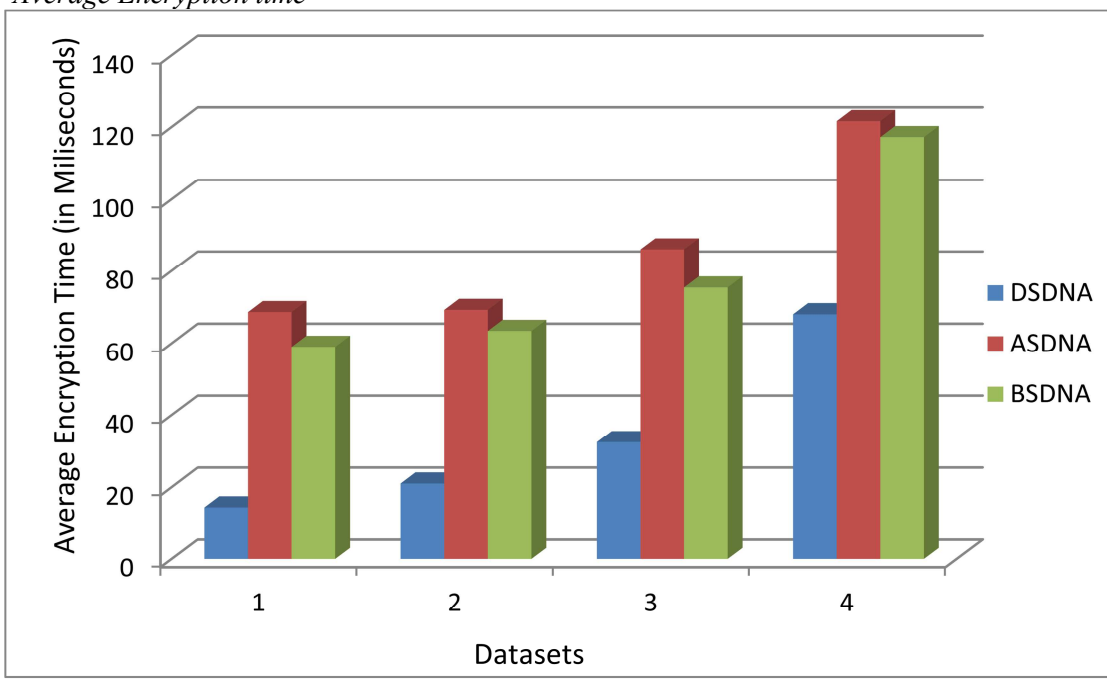
Average Encryption Time

The encryption time is the time taken by the algorithm to convert the given plaintext (original message) into the form of cipher text (in DNA Sequences form). Each cryptographic algorithm is executed five times on the same data set and in each run the encryption time is calculated. From that the mean encryption time is calculated by summing out all the encryption time. Finally, the average encryption time is calculated by dividing the mean encryption time by five.

The results obtained by different cryptographic algorithm on different datasets are presented below:

Figure 2

Average Encryption time



The bar graph shows that the average encryption time of DSDNA is less as compared to rest of the algorithm in all the datasets. The ASDNA algorithm takes more encryption time than that of BSDNA and DSDNA algorithm.

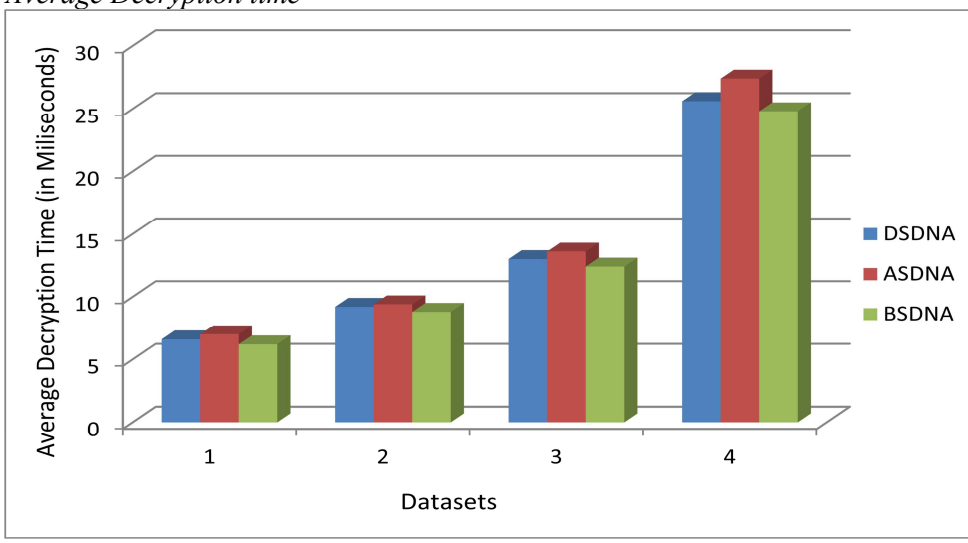
Average Decryption Time

The decryption time is the time taken by the algorithm to convert the given cipher text (DNA Sequences) into the form of plain text (Original messages). Each cryptographic algorithm is executed five times on the same data set and in each run the decryption time is calculated. From that the mean decryption time is calculated by summing out all the encryption time. Finally, the average decryption time is calculated by dividing the mean decryption time by five.

The results obtained by different cryptographic algorithm on different datasets are presented in the figure.

Figure 3

Average Decryption time



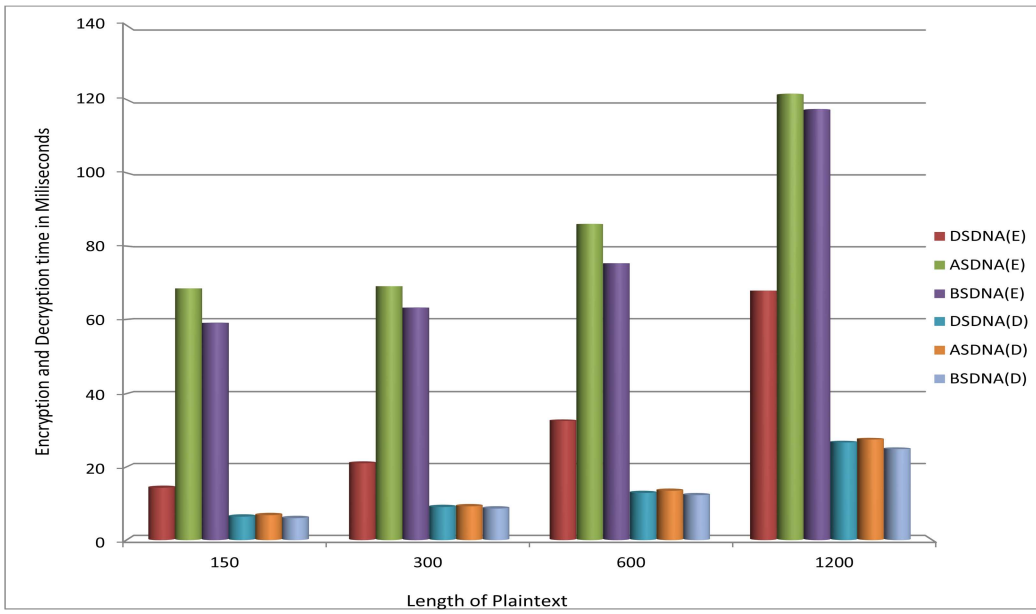
In an average, the decryption time of ASDNA algorithm is more as compared to DSDNA and BSDNA. The BSDNA algorithm has faster decryption time than the entire algorithm. The DSDNA algorithm takes more decryption time than BSDNA but less as compared to that of ASDNA.

Effect of Length of Plaintext on Encryption Time and Decryption Time

How the changes in the size of plaintext affect the time taken by the algorithm to encrypt and decrypt is shown in figure.

Figure 4

Effect of length of Plaintext on Encryption Time and Decryption Time



The figure shows that: by increasing the length of plaintext the encryption and decryption time increases. It is also seen that the decryption time is very low as compared to that of encryption time in each dataset.

Conclusion and Policy Implication

In this research, the traditional cryptographic technique can be made more secure by applying the concept of DNA Cryptography on them. DNA Cryptography encodes the messages in the form of DNA Sequences: Adenine (denoted by A), Cytosine (denoted by C), Thymine (denoted by T) and Guanine (denoted by G). The DES, AES and Blowfish based DNA Cryptographic algorithms are implemented in this research and the comparison is done based on the parameters: average encryption time, average decryption time and the effect of length of plaintext on encryption time and decryption time. The result shows that: the AES based DNA cryptographic algorithm takes more encryption time and decryption time than DES and Blowfish based DNA Cryptographic algorithm. The Blowfish based DNA Cryptographic algorithm takes more average encryption time than that of DES based DNA Cryptographic algorithm but less than that of AES based DNA Cryptographic algorithm in all the datasets. The Blowfish based DNA Cryptographic algorithm is faster in comparison to other two. The AES based DNA Cryptographic algorithm takes more decryption time. While the size of plaintext increases, the encryption and decryption time also increases. In each dataset, the algorithm takes more encryption time as compared to that of decryption time.

The research shows that the biological DNA concept can be used for encrypting and decrypting messages by combining with the existing Cryptographic algorithm in order to improve the security strength. Moreover, the concept can be used to protect medical data in medical field and can be used to secure and protect sensitive information such as passwords, financial data, and personal information.

References

[1] Ahmed, R. K., & Mohammed, I. (2017). Developing a New Hybrid Cipher Algorithm using DNA and RC4. International Journal of Advanced Computer Science and Applications, 8(10).

[2] Al-Mahdi, H., Alruily, M., Shahin, O. R., & Alkhaldi, K. (2019). Design and Analysis of DNA Encryption and Decryption Technique based on Asymmetric Cryptography System. International Journal of Advanced Computer Science and Applications, 10(2). https://doi.org/10.14569/IJACSA.2019.0100264.

[3] Elkamchouchi, H., Ahmed, F., & ElMaksoud, A. A. (2018). Blowfish Security Enhancement using DNA–Genetic Technique. Journal of Advanced Research Design, 43(1), 10-16.

[4] Hammad, B. T., Sagheer, A. M., & Ahmed, I. T. (2020). A comparative review on symmetric and asymmetric DNA based cryptography. Bulletin of Electrical Engineering and Informatics, 9(6), 2484-2491. https://doi.org/10.11591/eei.v9i6.2470.

[5] Kolate, V., & Joshi. (2021). An Information Security Using DNA Cryptography along with AES Algorithm. Turkish Journal of Computer and Mathematics Education, 12(1), 183-192.

[6] Sohal M. & Sandeep S.(2022). BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing, Journal of King Saud University-Computer and Information Sciences 34.1, 1417-1425.