FEISTEL INSPIRED STRUCTURE FOR DNA CRYPTOGRAPHY

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering

in

Information Security

Submitted By

Ashish Kumar Kaundal

(Roll No. 801233002)

Under the supervision of:

Dr. Anil Kumar Verma

Associate Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

June 2014

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, ***"Feistel Inspired Structure For DNA Cryptography"***, in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Information Security* submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Anil Kumar Verma* and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

(Ashish Kumar Kaundal)

801233002

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. Anil Kumar Verma)

Associate Professor, CSED

Countersigned by

(Dr. Deepak Garg)
Head
Computer Science and Engineering Department
Thapar University
Patiala

(Dr. S. K. Mohapatra)
Dean (Academic Affairs)
Thapar University
Patiala

ACKNOWLEDGEMENT

"The successful completion of any task would be incomplete without accomplishing the people who made it possible and whose constant guidance and encouragement secured the success". First of all I wish to acknowledge the benevolence of omnipotent God who gave me strength and courage to overcome all obstacles and showed me the silver lining in the dark clouds.

With profound sense of gratitude and heartiest regard, I express my sincere feelings of indebtedness to my Guide **Dr. Anil Kumar Verma**, Associate Professor, Computer Science and Engineering Department, Thapar University for his positive and excellent guidance, constant encouragement, keen interest, invaluable co-operation, generous attitude and above all his blessings have been persistent source of inspiration for me. I am grateful to **Dr. Deepak Garg**, Head of Department and **Dr. Jhilika Bhattacharya**, P.G. Coordinator, Computer Science and Engineering Department, Thapar University for the motivation and inspiration that triggered me for this thesis.

Last but not the least I would like to express my heartfelt thanks to my parents and my friends who with their thought provoking views, veracity and whole hearted co-operation helped me in doing this thesis.

Ashish Kumar Kaundal

(801233002)

ABSTRACT

DNA cryptography is a novel field being taken up by the researcher community for research now a days in order to have secure communication on a network. This technique is inspired from biological science, in which DNA is used as an information carrier from one generation to another. DNA cryptography is preferred for a secure end to end communication due to the vast parallelism and extra ordinary information density that are inherent in any DNA molecule. In this paper previous algorithm based on DNA cryptography is enhanced in terms of its security parameter by incurring feistel inspired structure in it. This adds some sort of confusion and diffusion, which makes it complex enough that it restricts the adversary to perform any kind of brute force attack and hence preserve the confidentiality. The work presented makes use of the most popular Feistel structure for enhancing the encryption process. The results indicate that the feistel inspired structure for DNA cryptography using one time pad for key generation achieves a better encryption (confidentiality) although the cost of increased encryption and decryption time.

Keywords - DNA computing, DNA cryptography, One Time Pad (OTP).

TABLE OF CONTENTS

Chapter 3 Problem Statement

Chapter 4 Proposed Work

Chapter 5 Simulation and Results

Chapter 6 Conclusion and Future Scope

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

A	Adenine
AES	Adavnce Encryption Standard
C	Cytosine
C_{dna}	Ciphertext in DNA form
DNA	Deoxy Ribonucleic Acid
DES	Data Encryption Standard
D_K	Decryption Key
E_K	Encryption Key
G	Guanine
K_{dna}	Key sequence in DNA form
K_{size}	Key size
MD5	Message Digest
mRNA	Messenger Ribo Nucleic Acid
MANETS	Mobile Adhoc Networks
OTP	One Time Pad
PCR	Polymerase Chain Reaction
PGP	Pretty Good Policies
RC4	Rivest Cipher
RNA	Ribo Nucleic Acid
RSA	Rivest-Shamir-Adleman
ssDNA	Single Stranded Deoxy Ribonucleic Acid
T	Thymine
TB	Tera Byte
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

CHAPTER 1

INTRODUCTION

1.1 Motivation

With the growing pace of Internet and network technology day by day, the security threats are also increasing for the users, due to lot of information flow on the network. There are various adversaries who always try to break into the system in order to steal the crucial information or to destroy the integrity of data. So information security becomes necessity for modern computing systems. There are some sectors like government, banks, military who can't afford any leaks to their secret data. From our past to till date the secret writing techniques are used to protect the data from the adversaries and the techniques such as cryptography and steganography are most common and widely used methods. Cryptography performs the encryption of the data whereas steganography hides the data from the hacker. In cryptography the encryption and decryption of data /plaintext is done with the help of key.

The most secure and presently used technique is the modern methods of cryptography which involves much mathematical computations and two types of keys, the public and private keys. Nowadays, there is another newly emerging cryptographic technique in the field of cryptography called DNA cryptography. The main objective of this method is to encrypt the plaintext and hide it in the DNA digital form. DNA cryptography enables the confidentiality of data more high then the modern methods with the use of one time pad (OTP) keys and its size. Also it is believed that in DNA cryptography the key can be generated for the huge length of data compared to the modern methods in which key are generated only for smaller length of the data.

Few years ago making use of 56 bit encryption seemed to be safe forever but as the computing power and knowledge of man increased these encryption schemes also disappeared. So with the failure of modern cryptographic algorithm like DES and MD5, new methods of information security are needed to protect our data [22]. Scientists and mathematicians are continuously trying to improve the encryption methods while staying within the limits of technology available to us. Existing algorithm RSA which is based on public key cryptography have been not cracked yet by anyone but future we can't predict. The concept of DNA computing provide us a ray of hope in the field of

computer security which is assumed to be a more powerful and unbreakable cryptographic algorithm now a days. With the help of DNA computing, Adleman and Lipton solved the combinatorial problems like Hamiltonian path and satisfaction problem [1, 22]. Besides the combinatorial problems DNA computing has many exciting applications for example DNA and RNA can store large amount of data in a compact volume. They vastly exceed the capacity of the other storage mediums such as electronic, magnetic and optical medium. A gram of DNA can store 10^{21} DNA bases or about 10^{8} TB [11]. Hence, a few gram of DNA can store all the data around the world. In spite of its advantages it has also some disadvantages such as the requirement of maximum computation time, hi-tech bimolecular laboratory and high computational complexity.

1.2 Cryptography

Cryptography is the scientific study of techniques for protecting digital information, distributed computations and transactions [14]. It is capable of keeping the data in secret while saving the information or passing it over the unsafe networks like internet. This is done in order to secure the data from the black hat hackers/adversaries and make it understandable only to its intended receiver. Because of its security base cryptography is one of the most vastly used and the most important fields.

The general process of cryptography involving both encryption and decryption is shown in the Figure 1.2.

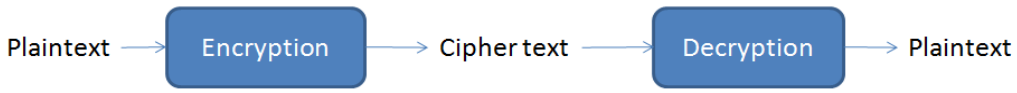


Figure 1.2 Flow Diagram of Cryptography

- **Plaintext**: The original data which is to be transmitted is considered as plaintext.
- **Encryption**: The method of obtaining the cipher text from plaintext is known as encryption.
- **Ciphertext**: The plain text in an encrypted form.
- **Decryption**: Decryption is the reverse process of encryption. The original message or the plaintext is obtained as a result of this process.

1.3 Goals of Security

Security consists of various goals but among these common and noticeable one lies in CIA (confidentiality, integrity and Availability) [5, 14].

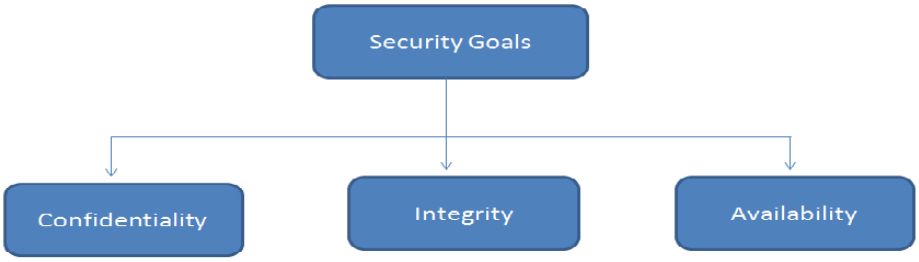


Figure 1.3 Main goals of Security

- **Confidentiality**: Hiding/preventing information from adversaries/unauthorized user.
- **Integrity**: Preventing Information/data from modification by the adversary.
- **Availability**: Resources should be available to the authorized users.

1.3.1 Threats to Confidentiality

- **Snooping**

  It refers to the unauthorized access or interception of information, with the help of some monitoring tools like as key logger or eavesdropping.
- **Traffic Analysis**

  In this traffic is analyzed with the help of tools like wire shark, in order to obtain the information about the encrypted text/file during transmission.

1.3.2 Threats to Integrity

- **Modification**

  In this attacker will modify the information which is send by the sender, so that the receiver will get wrong information/result.
- **Masquerading**

  In this spoofing attacks are performed by the attacker, so that the sender and receiver traffic will pass through the attacker.

1.3.3 Threats to Availability

- **Denial of service**

  Generating lot of traffic to the target or consuming the network bandwidth by attacker such that the intended receiver will not get the desired requested service at that time.

1.4 Encryption Techniques

1.4.1 Symmetric Encryption

Symmetric encryption is also known as shared key encryption. In symmetric encryption, a single key is used for encryption and decryption process [14].

$$E_K = D_K = K$$

$$E\ (K, P) = C$$

$$D\ (C, K) = P$$

Where

C – Ciphertext, P – Plaintext, E – Encryption, D – Decryption, K – Key

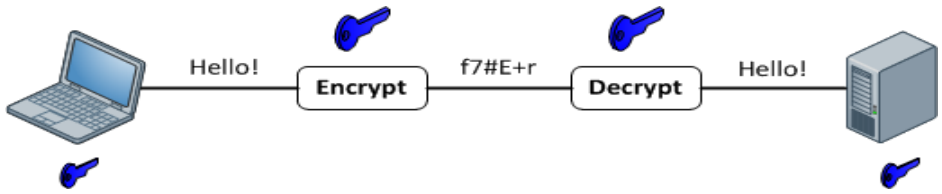


Figure 1.4.1 Symmetric Encryption [12]

Substitution and Transposition are some of the operations on which symmetric key cryptography is based. In substitution for each plaintext we assign some secret value and in transposition we change the order of plaintext or in other words we add permutation. Caesar and Vigenere ciphers are based on substitution whereas DES is based on both substitution and transposition [24]. Some of common symmetric key encryption algorithms are DES, AES, and RC4. AES is commonly used in IPSec and VPNs. RC4 is deployed on wireless networks as the base encryption used by WEP and WPA version 1. Symmetric key encryption algorithms are extremely fast and have low complexity than asymmetric key encryption [14]. Symmetric algorithm is further of two types: Stream ciphers and block ciphers. In stream cipher encryption is performed bit by bit whereas in block ciphers encryption is performed on the fixed size block at a time.

1.4.2 Asymmetric Encryption

Asymmetric encryption is also known as public-key cryptography. Asymmetric encryption is different from symmetric encryption primarily in keys that are used [14].

$$E_K \neq D_K$$

In this two keys are used: one key for encryption known as public key and another one for decryption known as private key. Both the keys are generated by using some mathematical functions. In this type of cryptographic approach anyone can encrypt the message using public key but decryption will be performed by the receiver only and hence solve the problem of key management. Asymmetric key cryptography was first introduced by Diffi and Hellman then it is further extended by RSA and ElGamal. Commonly used asymmetric encryption algorithm is RSA [12].

As compared to symmetric encryption, asymmetric encryption incurs a high computational burden, and tends to be slower. So it is not typically employed to protect payload data. The major strength is its ability to establish a secure channel over an unsecure medium (for e.g. Internet) [24]. All the process is done by the exchange of public keys, which is used for the encryption of data. Private Key which is never shared is used for decryption.

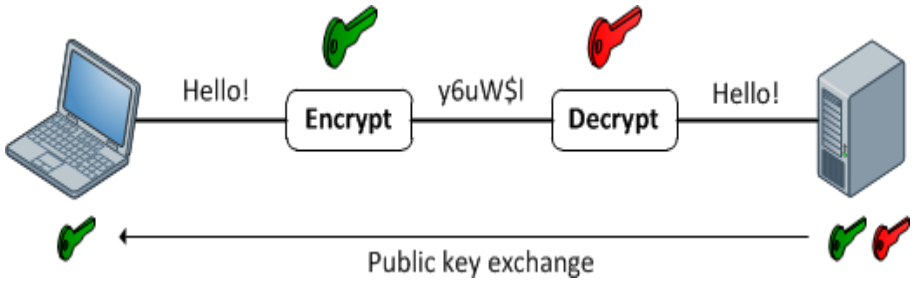


Figure 1.4.2 Asymmetric Encryption [12]

The differences in both the encryption methods can be summarized as:

Table 1.4 Differences between symmetric and asymmetric encryption

Sr. No.	Symmetric Encryption	Asymmetric Encryption
1.	Same key is used for both encryption and decryption.	Different keys are used for encryption and decryption.
2.	Fast	Slow
3.	No requirement of third party.	Third party required.
4.	Most popular algorithms are	Most popular are RSA, ECC,

	DES, 3DES and AES.	El Gamal.

1.5 DNA

Deoxyribonucleic Acid (DNA) is the hereditary material of almost all living organisms ranging from very small viruses to complex human beings. It is an information carrier of all life forms. DNA is a long polymer of small units called nucleotides. Each nucleotide consists of the following three components [22]:

- A Nitrogenous Base
- A five carbon Sugar
- A Phosphate Group

There are four different nucleotides depending upon the type of nitrogenous base they have got. There are four different bases A, C, T, G called Adenine, Cytosine, Thymine and Guanine respectively.

DNA is a double helical structure with two strands running anti parallel as shown in figure 1.5(a) below.

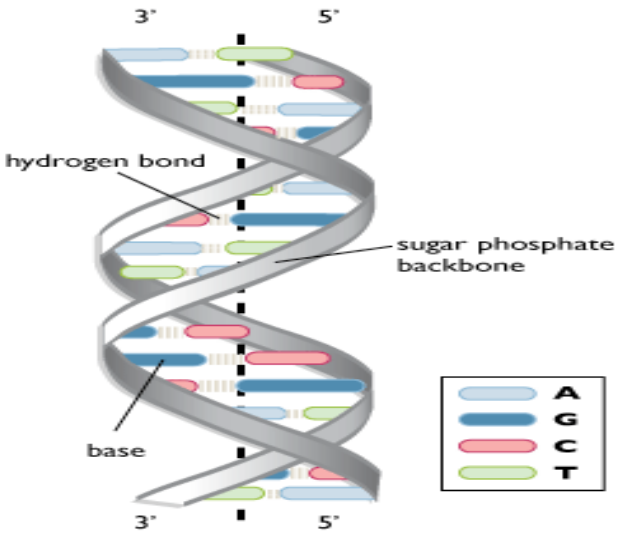


Figure 1.5 (a) Double Helical Structure of DNA [19]

DNA stores all the huge and complex information about an organism with the combination of only these four letters A, C, T and G. These bases form the structure of DNA strands by forming hydrogen bonds with each other to keep two strands intact. A forms hydrogen bond with T whereas C and G forms bond with one another and are complementary to each other which is also known as Watson Crick's complementary form [9].

Also, Adenine and Guanine are called purines and Thymine and Cytosine are called pyrimidines in biological terms.

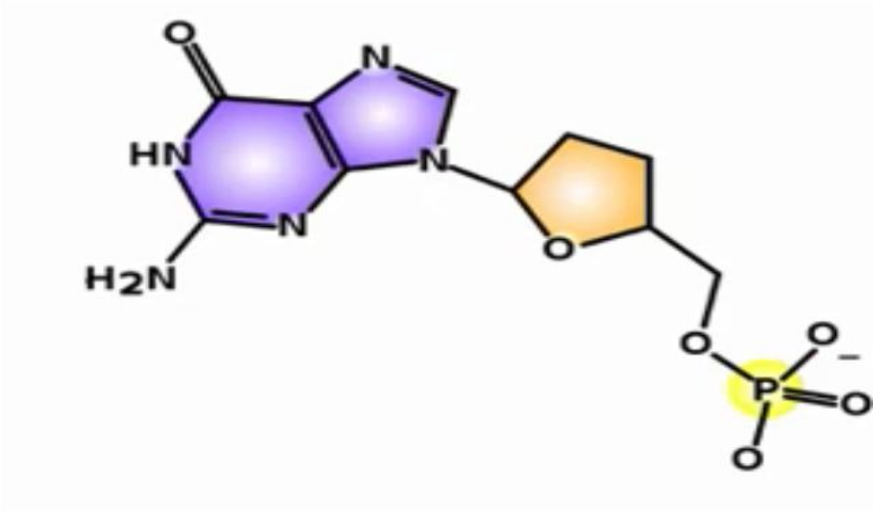


Figure 1.5 (b) Chemical Structure of DNA [19]

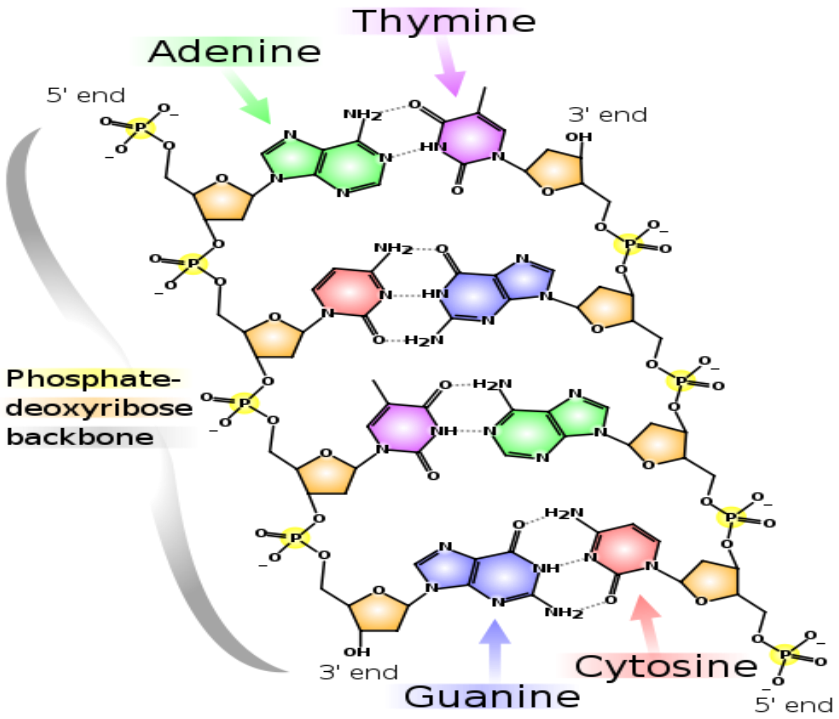


Figure 1.5 (c) DNA Helical Structure (Chemical) [19]

1.6 DNA Cryptography

DNA cryptography is an emerging field now a days, on which various researches are going- on in order to generate a strong cryptographic techniques. Concept of DNA cryptography can be realized with either DNA computing or conventional cryptographic approach. DNA cryptography based on DNA computing uses molecular theory which

consists some of the common techniques like DNA micro-array, DNA fragmentation, DNA hybridization, central dogma etc which can be realize with both symmetric and asymmetric key cryptography. The vast parallelism and extraordinary information density inherent in DNA molecules are explored for cryptographic purposes such as encryption, authentication, and signature. With the use of One Time Pad and DNA study collaborately lead to a secure system.

DNA cryptography based on conventional cryptographic approach consists of key generation, encryption and decryption process [18]. But the differences exist in it from conventional one is: key generation where we use key sequences in a DNA format like ATCGCCAG which act as a one time pad, ciphertext produced during encryption process by converting plaintext is also in the DNA form and decryption process converts the DNA cipher into its original plaintext. DNA cryptography is based on both symmetric and asymmetric key cryptography, but it is easier to realize with symmetric key rather than asymmetric key. Also its bio-computational complexity makes it more complex for the adversaries to breach it. The enormous denseness and the huge uniformity in the DNA molecules are discussed for related cryptographic purposes, in the next chapters.

1.7 OTP (One Time Pad)

Random key generation based on one time pad was first introduced by Vernam's and is known by its name Vernam's cipher. Later on it is extended by Shannon theory by showing that it has perfect secrecy [14].

According to Shannon theory:

- Size of key should be at least equals to its plaintext.

$$K_{size} \geq \text{Plaintext}$$

- It should be truly random.
- Not be reused
- Should be kept secret

To realize the concept of one time pad in symmetric key cryptography, Pseudo random generator is used in our proposed algorithm. So it is difficult for the adversary to guess the right key in order to obtain the original plaintext/message.

1.8 Cryptanalysis

1.8.1 Cryptanalysis

Deciphering a message without any knowledge of encrypting details is called cryptanalysis and a person who performs this is called cryptanalyst [14, 5]. The straightforward way of finding the secret key is brute-force attack which includes all the possible combinations of keys. According to Kerckhoff's principal and Shannon's maxim the encryption algorithm is known to all, but key should be secret. So it is necessary that key length is of sufficient size and design of algorithm is good in order to avoid the brute-force attack. Cryptanalyst uses various cryptanalysis techniques to find the flaws in the cryptosystem that helps him in obtaining the key in lesser time. Before triggering an attack, attacker should have sufficient information about the attack and its types. Some of the common types of attacks are following which is helpful for cryptanalysis by the cryptanalyst [14].

- **Ciphertext-only attack**

  In this type of attack cryptanalyst have encryption algorithm and ciphertext for cryptanalysis.
- **Known plaintext attack**

  In this type of attack cryptanalyst have information about encryption algorithm, set of ciphertext and corresponding portion of plaintext.
- **Chosen-plaintext (chosen-ciphertext) attack**

  In this type of attack cryptanalyst have the secret key associated with the cryptosystem and perform encryption and decryption according to his choice in order to obtain the desired plaintext-ciphertext pairs.
- **Adaptive chosen plaintext or ciphertext attack**

  This type of attack is the adaptive version of previous mentioned attack. Here cryptanalyst can adapt the plaintext according to the results of previous encryptions.

1.8.2 Brute-force Attack

In this attacker tries each and every possible combination of keys until an intelligible translation of ciphertext into desired plaintext is achieved. It is also called exhaustive key search and applied when the attacker has no information about the encryption algorithm that makes the cryptanalysis easier.

1.9 Thesis Outline

We have organized the thesis into 6 chapters which include Introduction; Literature Review; Problem Statement; Proposed work; Simulation and Results and finally Conclusion and Future Scope.

Chapter 2 presents the earlier related work on DNA computing and DNA cryptography with their approaches and technology used.

Chapter 3 present gaps in study, problem statement and methodology.

Chapter 4 discusses the proposed algorithm to countermeasure the problems discussed in the problem statement.

Chapter 5 highlights the simulation environment based on the proposed algorithm and a comparison is made between the proposed algorithm using feistel inspired structure and the other without using feistel structure, evaluating the performance of both the algorithms by making use of encryption time and decryption time and analyzing the results.

Chapter 6 finally summarizes the conclusions drawn in the thesis along with its future scope.

CHAPTER 2

LITERATURE REVIEW

2.1 State of the Art in DNA Cryptography

This chapter concentrates on the literature review of the DNA cryptography in chronological order. By studying the data through many sources we work for future for improving the performance of DNA cryptography in the security field.

2.1.1 DNA Computing

In 1994, Adleman [1] laid the foundation of DNA computing by giving solutions to the combinatorial problems using molecular computation, one of which is "Hamiltonian path" problem. He solved the instance of graph containing seven vertices by encoding it into the molecular form by using an algorithm and then computational operations were performed with the help of some standard enzymes [13]. This was solved by brute force method.

In 1995, Lipton [15] extended the work of Adleman by solving another NP-complete problem called "satisfaction" by using DNA molecules in a test tube to encode the graph for 2 bit numbers.

In 1996, Dan Boneh et al. [6] applied the approaches of DNA computing used by Adleman and Lipton, in order to break one of the symmetric key algorithm used for cryptographic purposes known as DES (Data Encryption Standard). They performed biological operations on the DNA strands in a test tube, such as extraction, polymerization via DNA polymerase, amplification via PCR and perform operations on the DNA strands which have the encoding of binary strings. Then DES attack is planned by generating the DES^{-1} solution, due to which key can be easily guessed from the ciphertext and further evaluate the DES circuit, lookup table and XOR gates. By using their molecular approach they broke DES in merely 4 months.

In 1997, Qi Ouyang et al. [21] applied the approaches of DNA molecular theory in order to generate the solution for maximal clique problem, which is another NP-complete problem. Thus shows the efficiency of DNA: to solve Hard-problems and vast parallelism inherent in it which makes the operations fast.

Table 2.1.1 DNA Computing (Related Work)

Year	Algorithm Title	Problem Solved	Technology Used
1994	Molecular Computation of Solutions to Combinatorial Problems [1]	Hamiltonian Path	DNA Molecular Theory.
1995	DNA Solution of Hard Computational Problems [15]	SAT	DNA Molecular Theory.
1996	Breaking DES Using a Molecular Computer [6]	DES (56 bit)	Molecular Computer based on DNA molecules.
1997	DNA Solution of the Maximal Clique Problem [21]	Clique Problem	DNA Molecular Theory.

2.1.2 DNA Cryptography

In 2003, Jie Chen [8] presented the DNA cryptographic approach based upon molecular theory, One-time pad and performed encryption/decryption of 2-dimensional image. In 2004, Ashish Gehani et al. [4] laid the foundation of DNA cryptography by using molecular approach and the concept of One-time pad- which has perfect secrecy, according to Vernam's and Shannon: inventor of One-time pad. They have proposed a method of encryption and decryption which is based on DNA chip and One-time pad. So it is very hard for the adversary to guess the encrypted message.

In 2005, Kazuo Tanaka et al. [16] proposed the DNA cryptographic approach based on Public Key (one way). In this approach they have clearly explained about the formation of public keys by using solid supports mixture for PK_A and ODN mixture for PK_B. After generating the keys, message is encoded in a DNA sequence with the help of one of the public key, which is further synthesized with the DNA synthesizer and then the encoded message sequence is ligated with the another public key. Now the outcome of the previous process is forwarded to the immobilization process and then for PCR amplification, where the amplification is done with the help of secret sequence, in order to decode the encoded DNA sequence.

In 2006, Sherif T. Amin et al. [23] proposed the DNA cryptographic approach based on symmetric key, where key sequences are obtained from the genetic database and remain same at both ends (sender and receiver). Message/plaintext is first converted into binary format and then to DNA format using substitution. Once the substitution has been

performed and message is in the form of DNA sequence, then we choose the quadruple from the sequence we have obtained and match it with the key sequence and where match occurs we note the position. Like this all the random position for each character in the plaintext are obtained and the file which contains these positions are our ciphertext which is send to the receiver and then decryption is perform in reverse order.

In 2008, Anil Verma et al. [2, 3] proposed a novel paradigm for secure routing in Mobile Adhoc Networks (MANETs) that uses Pseudo DNA cryptography approach in order to secure the Adhoc networks. Adhoc network is a wireless network which has no fixed infrastructure and where each node act as a host and router and there is no centralized authority which makes them vulnerable to the security attacks present in the networks. Pseudo DNA cryptography approach they have used is based on the central dogma of molecular biology. Concept of how messages are stored in DNA and then transfer to the mRNA (transcription), and then to the proteins (translation) which is our ciphertext. Ciphertext is send through the secure channel to the intended receiver and symmetric key with One-time pad is used at both the ends (encryption and decryption).

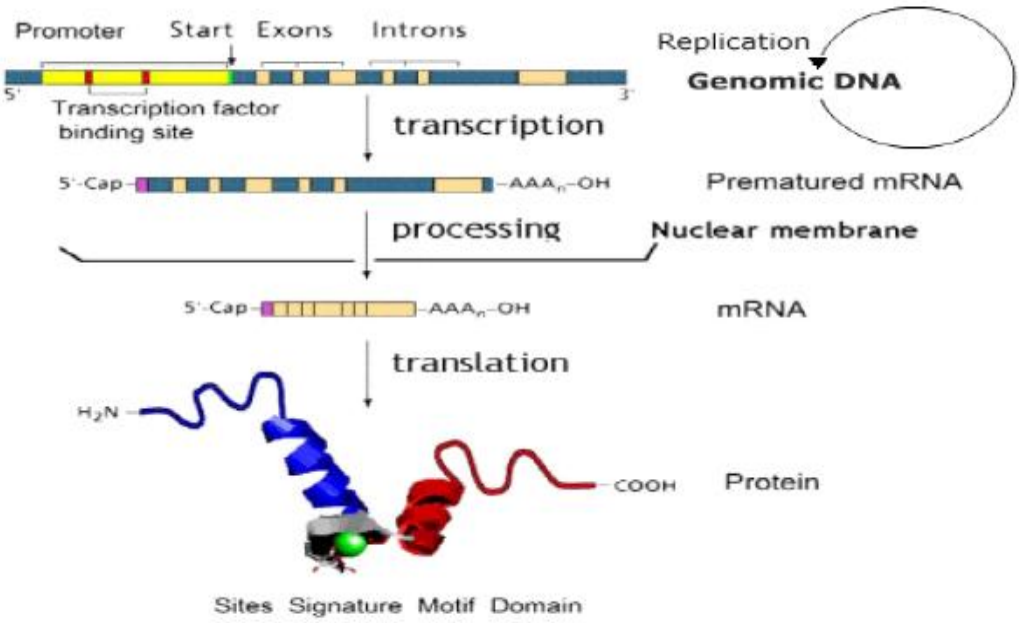


Figure 2.1.2 (a) central dogma of DNA [2]

In 2008, Guangzhao Cui et al. [10] proposed the public key encryption technique that uses DNA synthesis, DNA digital coding and PCR amplification to provide the security safeguard during the communication. This encryption scheme has high confidential strength.

In 2010, Lai Xuejia et al. [17] proposed a DNA public key cryptosystem which is based on DNA microarray/chip technology in which DNA chip is fabricated with probes. One set of probes are used for encryption process and another set for decryption process. In key generation process existing probes are selected as keys from the National Engineering Centre for Biochip at sanghai. Some signals are also selected which are used for measuring the intensity of probes after hybridization result. If the probes have intensity greater than some fixed value it is denoted as probe 1 and if the probes have intensity lesser than some fixed value, it is denoted as probe 0. Each encryption key consists of equal number of probe 0 and probe 1. For encryption process two keys are used PKs (sender) and PKr (receiver) to encrypt the plaintext. Firstly the plaintext is converted into its ASCII code then its equivalent binary code. These binary codes are arranged in the form of matrix. For 0 in the matrix probe 0 is selected from the encryption key and spotted on the DNA chip, for 1 in the matrix probe 1 is selected from the encryption key and spotted on the DNA chip. The chip fabricated according to the above concept is designated as a ciphertext. Receiver hybridizes the encrypted ciphertext with the decryption key Sk. Light spot in the chip indicate the high intensity of the hybridization and denoted as binary digit 1 and dark spot denotes the digit 0.

In 2011, Deepak Kumar and Shailendra Singh [11] proposed a new secret data writing techniques based on DNA sequences. They have explained this algorithm by using a simple example of "HELLO" as a plaintext and generate a ssDNA One-time pad key of 350 bits which is 70 times longer than the plaintext and perform encryption and decryption on the plaintext using symmetric key cryptography. So to find the exact key, adversary has to search among 4^{310} different ssDNA strings which is almost impossible.

In 2012, Sabari Pramanik and Sanjit Kumar Setua [22] proposed a new parallel DNA cryptography technique using DNA molecular structure and hybridization technique which certainly minimize the time requirement. They have explained how message is exchanging safely between sender and receiver with an example.

In 2012, Yunpeng Zhang et al. [25] proposed a DNA cryptography based on DNA fragment assembly. In their algorithm they have clearly mentioned how sender converts the plaintext into binary sequence and then into long chain of DNA, which is further fragmented into small DNA chains. Key of short chain implantation takes place in the fragments and forward to the receiver as a ciphertext and then receiver deciphers it and starts fragment reassembly to obtain the plaintext.

In 2013, Olga Tornea and Monica E. Borda [20, 7] proposed a DNA based cipher which is based on DNA indexing. They take the random DNA sequence from the genetic database and use as a One-time pad key, which is send to the receiver by a secure communication channel. The encryption mechanisms takes place by converting the plaintext into its ASCII code and then converts it into the binary format which is converted into the DNA sequence (A, C, G, and T). Now DNA sequence formed is search in the key sequence and writes down the index numbers. The array of integer numbers obtained are our ciphertext which is decrypted by the receiver only using the key and index pointer.

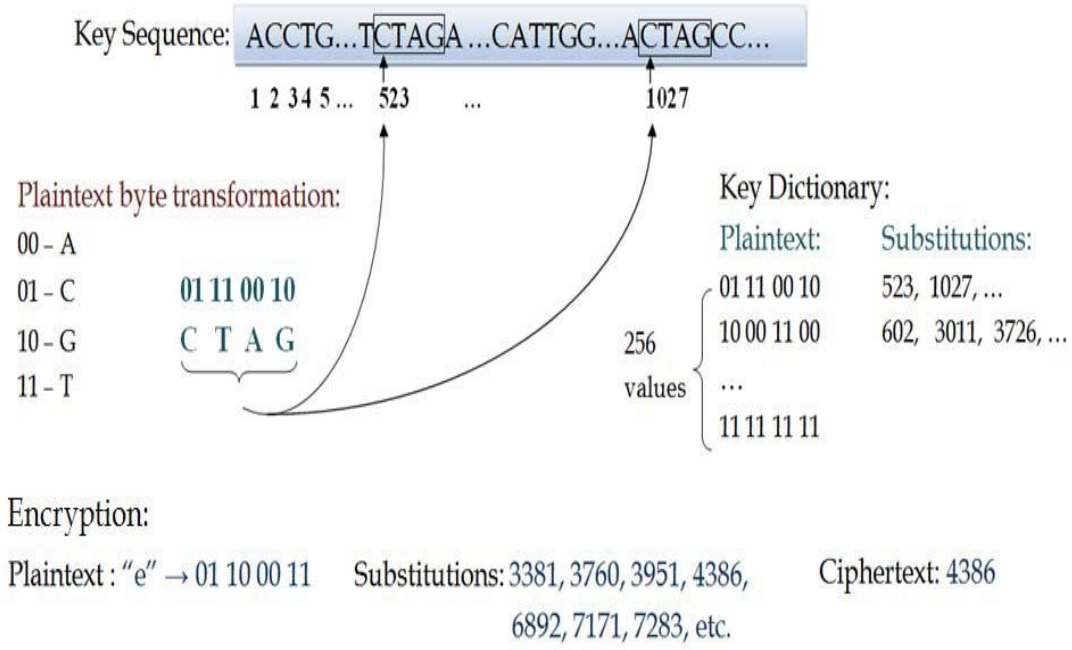


Figure 2.1.2 (b) DNA Indexing [20]

Table 2.1.2 DNA Cryptography (Related Work)

Year	Algorithm Title	Cryptographic Approach	Technology Used
2003	A DNA-based, Bimolecular Cryptography Design [8]	Symmetric key	Molecular, One-time pad.
2004	DNA-Based Cryptography [4]	Symmetric key	Molecular, DNA chip, One-time pad.
2005	Public-key system using DNA [16]	Asymmetric key	Molecular, DNA synthesis, PCR amplification.
2006	YAEA DNA Encryption	Symmetric key	Substitution, One-time

	[23]		pad.
2008	DNA Cryptography: secure routing in MANETs [2, 3]	Symmetric key	Central dogma of molecular biology, One-time pad.
2008	Encryption Scheme Using DNA [10]	Asymmetric key	DNA synthesis, DNA digital coding, PCR amplification.
2010	Asymmetric Encryption and Signature with DNA [17]	Asymmetric key	DNA chip technology, Hybridization.
2011	Secret Data Writing Using DNA Sequences [11]	Symmetric key	One-time pad.
2012	DNA Cryptography [22]	Symmetric key	Hybridization, One-time pad.
2012	DNA Cryptography Based on Fragment Assembly [25]	Symmetric key	DNA Fragment assembly.
2013	Security and Complexity of DNA Based Cipher [20, 7]	Symmetric key	One-time pad, DNA Indexing.

CHAPTER 3

PROBLEM STATEMENT

3.1 Gaps in Study

There are basically two DNA cryptographic approaches for securing data on networks – DNA cryptography based on molecular theory that realize the concept of cryptography by using DNA molecules and other one is DNA cryptography based on the conventional cryptography approach. DNA cryptography based on molecular theory uses some of the common techniques like DNA micro-array, DNA fragmentation, DNA hybridization, central dogma etc which can be realize with both symmetric and asymmetric key cryptography. The vast parallelism and extraordinary information density inherent in DNA molecules are explored for cryptographic purposes such as encryption, authentication, and signature. Major limitation of using DNA cryptography based on molecular theory is its implementation part for which high-tech molecular labs are required.

DNA cryptography based on conventional cryptographic approach consists of key generation, encryption and decryption process. But the differences exist in it from conventional one is: key generation where we use key sequences in a ssDNA format like ATCGCCAG which is purely based on One Time Pad, ciphertext produced during encryption process by converting plaintext is also in ssDNA form and decryption process converts the DNA cipher into its original plaintext. DNA cryptography is based on both symmetric and asymmetric key, but it is easier to realize with symmetric key rather than asymmetric key. Though the earlier cryptographic method are capable to prevent certain types of attacks such as brute force attack, integrity attack, but the later approach create some opportunities for brute force attacks due to their design issues and key generation approaches. The solutions discussed in the previous chapter are quite good at their part but there is a need to devise some improvement on their design issues which makes them more secure.

3.2 Problem Statement

The ultimate goal of DNA cryptography is to achieve the higher level of confidentiality while sending data over a network and protect original data from brute force attack. In existing security scheme/algorithms there is some uncertainty in fixed unit of

oligonucleotides due to which length of the key obtained is small. So for small length plaintext say single character when encrypted, may provide opportunities to the attacker for performing brute force attacks. Also the encryption scheme is simply based on the DNA substitution method and OTP key. The objective of this thesis is to remove the uncertainty in fixed unit of oligonucleotides and devise a novel algorithm based on the concept of confusion and diffusion which offers better design and security prospects than its counterpart.

3.3 Methodology

- Set fixed number of oligonucleotides so that it will be suitable for small size of plaintext as well as for big size.
- Devise an algorithm which is based on feistel inspired structure in order to make the ciphertext strong and secure.
- Simulator is designed for the algorithm in Vb.net platform capable of simulating all its aspects.
- Variable length plaintexts consisting of numeric, alphanumeric and alphabets are simulated in order to generate the results.
- Time complexities are calculated for both encryption and decryption process to evaluate the performance of the proposed method.

CHAPTER 4

PROPOSED WORK

4.1 Proposed Method

So to overcome the mentioned problem in the previous chapter we have proposed a hybrid symmetric key method and algorithm in this chapter which is based on DNA cryptography and feistel inspired structure that offers greater security than its previous counterpart. Two parties involved in this approach: one is sender (Alice) and other is receiver (Bob). Alice encrypts the plaintext using symmetric DNA key sequence

$$\text{Alice} \rightarrow E(K_{dna}, P) = C_{dna}$$

and the ciphertext obtained in DNA form is then send to the intended receiver Bob through some insecure channel like internet. Bob receive the ciphertext and decrypt it using the shared DNA key sequence and obtained the desired plaintext.

$$\text{Bob} \rightarrow D(C_{dna,}\, K_{dna}) = P$$

Now we describe the proposed DNA cryptographic technique in detail.

(a) Key Generation

According to Vernam and Shannon theory OTP (One Time Pad) is very secure [10]. In this paper we generate a random key sequence based on One Time Pad (OTP) that uses pseudo-random generator and provide the seed of 32 bytes DNA sequence as an input to it from the genetic database (Genbank) and kept the source secret. This pseudo-random generator will generate the high quality OTP sequence based on the seed and is very much secure than the other random functions that are used in C. It produces the unique result every time according to some statistical calculations.

In our proposed approach we have fixed 5-mer oligonucleotide which is a small DNA sequence of 5 nucleotide e.g. ATCGC. Now length of this unit is multiplied with the length of binary plaintext every time when the plaintext is generated. The final length produced after the multiplication is our key length. On the basis of this key length pseudo-random generator will generate the ssDNA key sequence. Less than fixed 5-mer oligonucleotides will produce a key length which can be computable if brute force is made. Since our approach is purely based on symmetric key cryptography, ssDNA key is

same at both the ends: sender (Alice) and receiver (Bob) and destroyed after its use. So it is impossible for the adversary to have an idea of the correct key sequence.

(b) Encryption

In encryption process the plaintext entered is first converted into its ASCII form then into its binary form which is denoted by EB'. Now EB' is passed to the feistel inspired structure where it is divided into two equals half's.

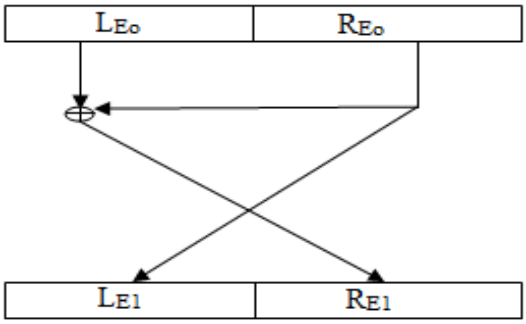


Figure 4.1 (b) Feistel inspired structure for reordering binary plaintext

First half is denoted by L_{Eo} and second half is denoted by R_{Eo} and then both the half's are XOR. Result of XOR moves towards the second half R_{E1} and left half L_{E1} contains the value of R_{Eo} as it is. Now both the half's L_{E1} and R_{E1} are concatenated which is denoted by EB''. By using the above structure we have changed the order of binary plaintext or in other words some sort of permutation (diffusion) to the binary plaintext. Now the concept of confusion [10] is applied on EB'' so that the relationship between plaintext and ciphertext is obscured. For this EB'' binary value is scanned from left to right and ssDNA key sequence from right to left. If 1 comes in EB'' then 5-mer oligonucleotide is picked from the key sequence and if 0 comes then space of 5-mer oligonucleotide is left from the key sequence. Whole process continues like this until the last digit of EB'' and finally the ssDNA sequence is formed. Now ssDNA sequence is converted into its Watson Crick's complementary form which is our ciphertext.

Now ciphertext is send to the receiver (Bob) in the form of packets using some insecure communication channel like internet.

(c) Decryption

After receiving the packets from the sender (Alice), receiver (Bob) will arrange the packets in sequential order and obtained the ciphertext from it. Now Bob will perform Watson Crick's complementary of ciphertext and use the hybridization technique by

scanning the ciphertext of 5-mer oligonucleotide from left to right and key from right to left. When match occurs 1 is marked at that position and for unmatched position 0 is marked. Whole process continues until the ciphertext length ends and the resultant binary sequence has been obtained which is denoted by DB'.

Now concept of diffusion [10] is applied by using two feistel inspired structure:

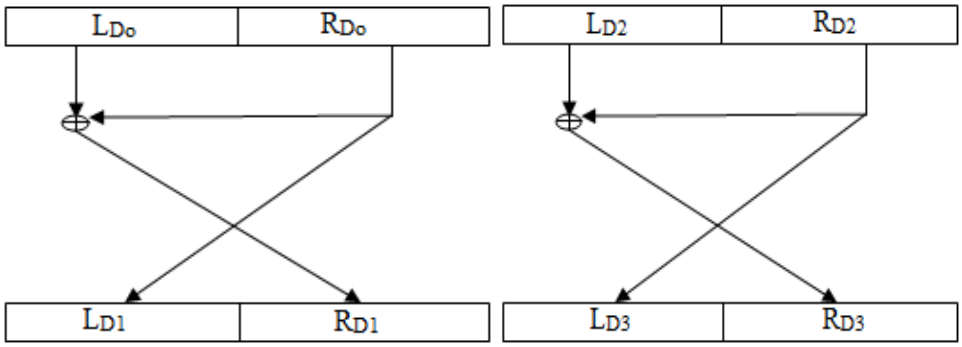


Figure 4.1 (c) Feistel inspired structures used for diffusion

Sequence of DB' is divided into equal half's. First half is denoted by L_{Do} and another is by R_{Do}, now both the half's are XOR with each other. The XOR value moves towards R_{D1} and L_{D1} contains the value of R_{Do}. Now both the half's are concatenated and sequence obtained is denoted by DB''. Again DB'' is divided into two equal half's, first half is denoted by L_{D2} and second half is denoted by R_{D2}. XOR both the half's and sequence obtained is stored in R_{D3} whereas L_{D3} contains the value of R_{D2} as it is. Now both the half's are concatenated and the final sequence obtained is denoted by DB'''. The value of DB''' is further converted into its ASCII form and then to the desired plaintext.

The whole process is complex enough that it will restrict the adversary to perform/think any type of brute force attack without knowing the correct ssDNA key sequence pair.

4.2 Algorithm

The proposed method will consist of following encryption algorithm to encrypt the message at sender (Alice) side:

Step 1: Select the plaintext P to be sent and convert into ASCII and then to binary plaintext, EB'.

Step 2: Reordering (Diffusion) of binary plaintext using feistel inspired structure, EB''.

Step 3: Confusion is performed on EB'' with the help of ssDNA key as follows:

(a) EB'' is scanned from left to right and key is from right to left.

(b) During scanning of EB'', if 1 occur then 5-mer oligonucleotide is picked from the right side of the key and if 0 occurs then 5-mer oligonucleotide is left from the key sequence.

(c) Whole process continues till up to the length of EB".

Step 4: ssDNA sequence form obtained as a result of step 3.

Step 6: Now ssDNA sequence is converted into its Watson Crick's complementary form which is our ciphertext.

Step 5: Sender (Alice) sends the ssDNA sequence in the form of packets to the receiver through some insecure channel.

Decryption algorithm to decrypt the message at receiver (Bob) side will consists of the following steps:

Step 1: Receiver (Bob) receives the packets, arranges them and obtained the ciphertext.

Step 2: Watson Crick's complementary form of Ciphertext is done to obtain ssDNA sequence.

Step 3: Hybridization is performed on the ssDNA sequence with the help of ssDNA key as follows:

(a) ssDNA sequence is scanned from left to right and key from right to left.

(b) 5-mer oligonucleotide is picked from the ciphertext as mentioned in (a) and hybridized with the key sequence.

(c) If match occurs, then mark 1 otherwise 0.

(d) Whole process continues till up to the length of ciphertext ends and obtain DB' as a result.

Step 3: Diffusion is performed on DB' using two feistel inspired structure in order to obtain DB'' and DB'''.

Step 4: DB''' is then converted into ASCII format and then to the desired plaintext.

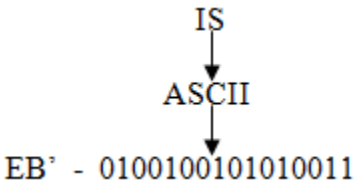
In the following section we will discuss the above algorithm with the help of an example which clearly demonstrates its security characteristics.

4.3 Illustration

Let us take the plaintext "IS", we want to encrypt and decrypt it using our approach which consists of following steps:

Step 1: Key Generation

In our proposed algorithm key depends upon the plaintext we enter and 5-mer oligonucleotide. So plaintext is first converted into its ASCII and then to its binary EB'.



Now the length of EB' is 16

Therefore, ssDNA key (K_{dna}) sequence length becomes: EB' * 5 => 16*5 => 80

Now OTP generates K_{dna}: 80 bytes

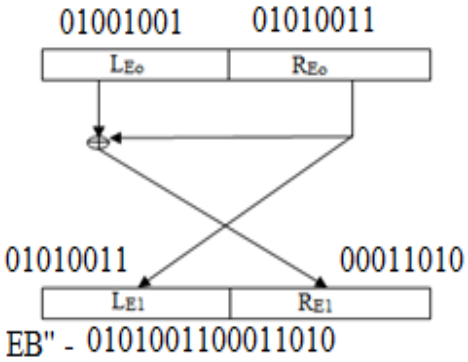
TAATCCCCGGTTTCACACACAGCGAAGGGGCGTAAGACAATATTAACGAAA
GACTGCCTATCCCACACGAGTCGTATAAA

K_{dna} is shared between both Alice (sender) and Bob (receiver) for this session only after that it is destroyed.

Step 2: Encryption

In encryption process the order of EB' is changed by using feistel inspired structure and confusion is performed on EB''.

EB' - 0100100101010011



Now substitution is performed on EB'' with the help of key sequence. EB'' is scanned from left to right and key sequence from right to left. In EB'' when 1 comes during scanning then 5-mer oligonucleotides are selected/picked from the key sequence from right to left and if 0 comes then 5-mer oligonucleotides are left without selecting from the key sequence. This process continues until the last digit of EB''. After substitution we obtained an ssDNA sequence as follows:

ssDNA sequence - GTCGTTCCCAACGAATATTAAGCGACACACCCCGG

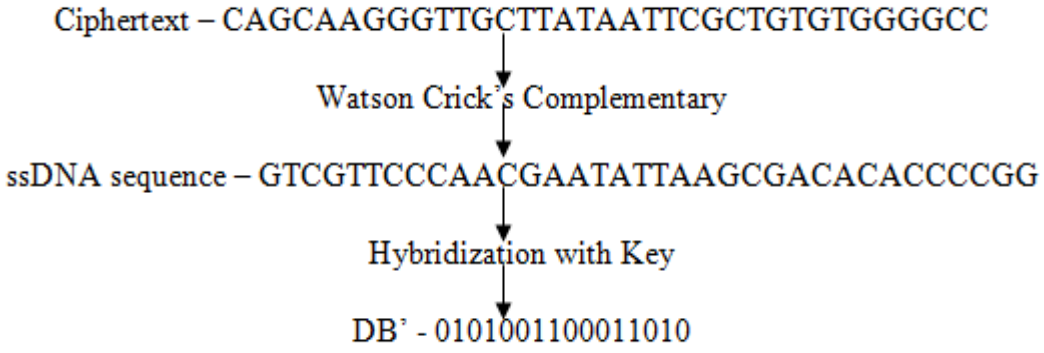
Now ssDNA sequence is converted into its Watson Crick's complementary form which represents the ciphertext.

Ciphertext - CAGCAAGGGTTGCTTATAATTCGCTGTGTGGGGCC

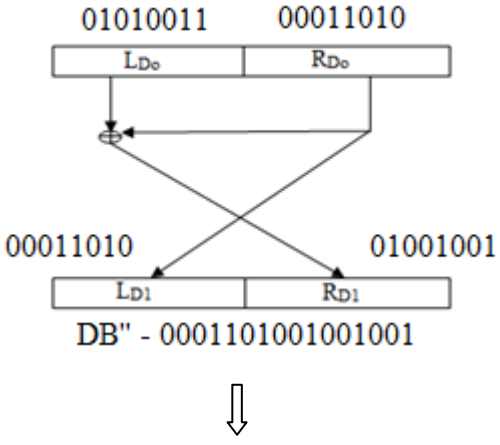
Alice sends this ciphertext to Bob through some insecure channel.

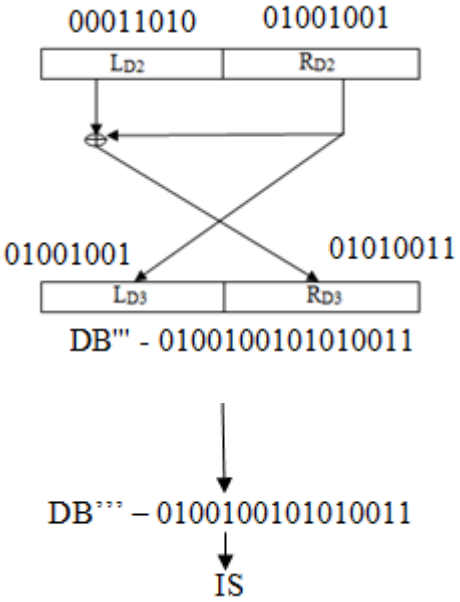
Step 3: Decryption

Bob receive the ciphertext and apply the concept of confusion and diffusion to it based on the above discussed decryption process.



Now DB' is moved to the feistel inspired structures for further processing in order to obtain the desired plaintext.





After getting the value of DB”’ it is converted into its ASCII form then to the desired plaintext: - “**IS**”.

Whole encryption and decryption process is secure enough that if adversary wants to apply brute force method in order to compute the key sequence from ciphertext then he has to compute 4^{80} different ssDNA key sequences. So computing that much sequences is very hard for the adversaries and hence represents high confidentiality level.

CHAPTER 5

SIMULATION AND RESULTS

5.1 Simulation Using Vb.Net Framework

In this chapter proposed approach is simulated with the help of simulator developed in Vb.NET framework using Intel core i5 processor, 2GB RAM. The design of the simulator which is named as DNA cryptosystem is shown below:

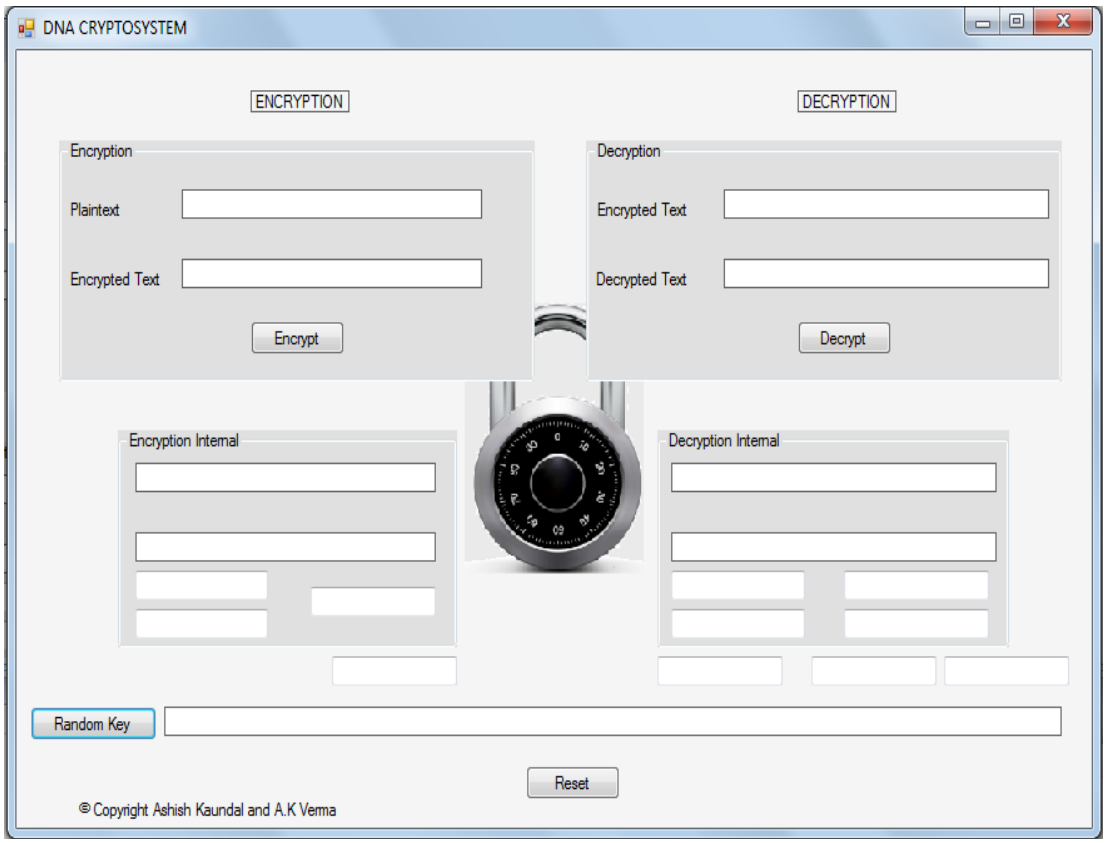


Figure 5.1 DNA Cryptosystem

This application is capable of performing encryption in DNA form (A, C, T, G) by using a symmetric key and will be decrypted by the receiver only, who have secret key. Like other traditional cryptosystem, DNA cryptosystem consists of key generation, encryption and decryption which are explained below:

(a) Key Generation

One time pad which has perfect secrecy and most secure, according to Vernam's and Shannon approach in modern cryptographic theories. Key used in DNA cryptography is based on the randomness feature of one time pad, according to which each and every

session a unique key is used, which is destroyed after its use. So there is no chance for the adversary to predict any guess about the key. In proposed work symmetric key is used which is same at both the ends (sender and receiver), therefore after performing the encryption process by the sender key is transferred to the receiver using a secure channel.

Single stranded DNA (ssDNA) which acts as a one time pad here. Size of single stranded DNA key generally depends upon the size of the plaintext bit and fixed number of oligonucleotides. Here we are using fixed 5-mer oligonucleotides.

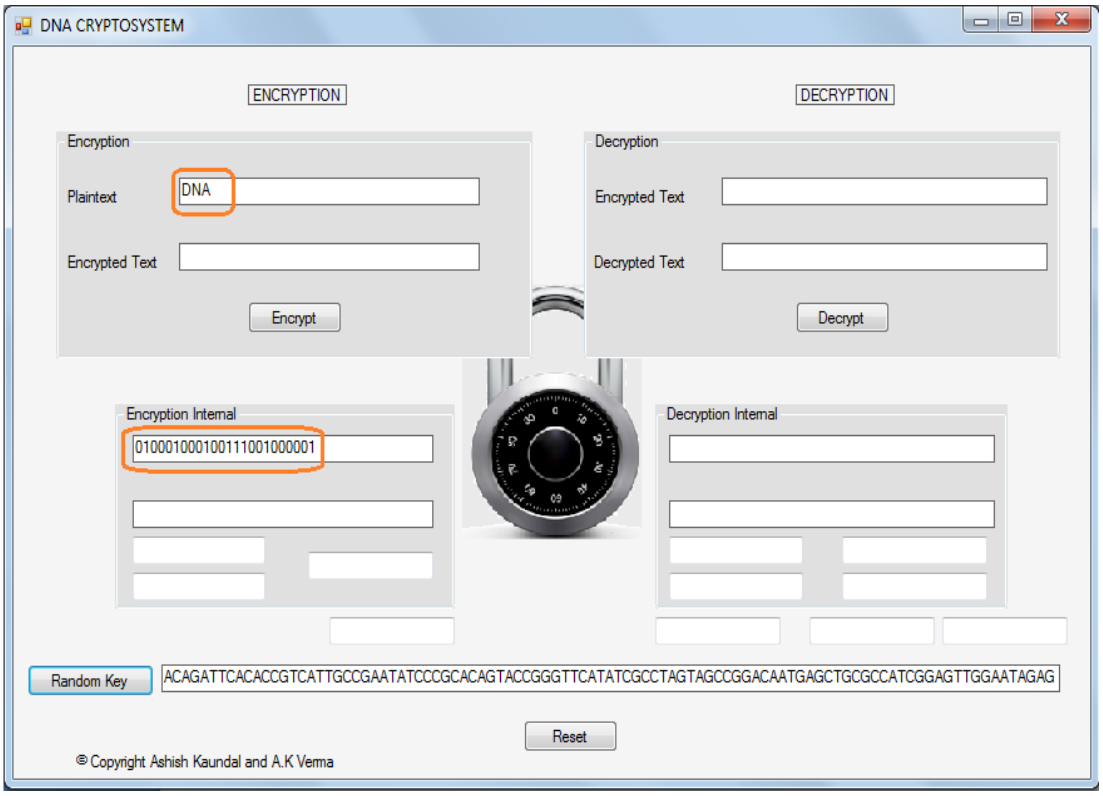


Figure 5.1 (a) Key Generation step 1

Now length of this unit is multiplied with the length of binary plaintext every time when the plaintext is generated. The final length produced after the multiplication is our key length. On the basis of this key length pseudo-random generator will generate the ssDNA key sequence. Since our approach is purely based on symmetric key cryptography, ssDNA key is same at both the ends: sender (Alice) and receiver (Bob) and destroyed after its use. So it is impossible for the adversary to have an idea of the correct key sequence.

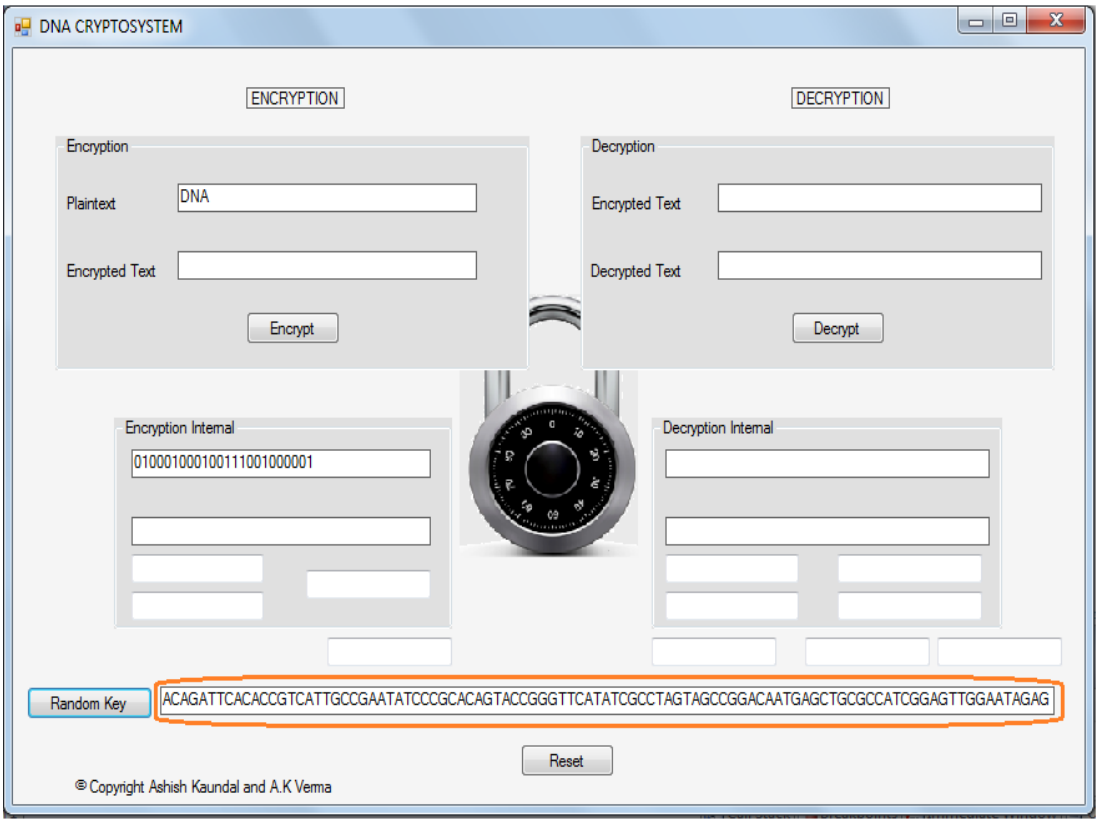


Figure 5.1 (a) Key Generation step 2

The above figures clearly shows about the key generation process that how plaintext "DNA" is entered, converted to binary plaintext and then to ssDNA key sequence.

(b) Encryption

When user enter the plaintext, it is transformed into its ASCII and then to its binary plaintext. Binary plaintext is then forwarded to the feistel inspired structure where some sort of permutation is performed. Now the output of feistel inspired structure is scanned from left to right and Key from right to left.

The encryption algorithm will read the feistel output from left, if the first bit of the feistel output is "0", then string of 5-mer oligonucleotide is skipped from the reverse side of the ssDNA key. Now the algorithm read the next bit of the feistel output and checks the remaining length of the key. If the next bit is "1", then string of 5 mer-oligonucleotides is selected from the remaining length of the key. Like this, process goes on selecting and skipping the DNA strings till the last bit of the feistel output. Once we obtained all the strings, algorithm will takes the Watson-Crick complementary of the string and put it into the encrypted textbox, which is our ciphertext in DNA form. Internal operations are also shown in the figure 5.1(b).

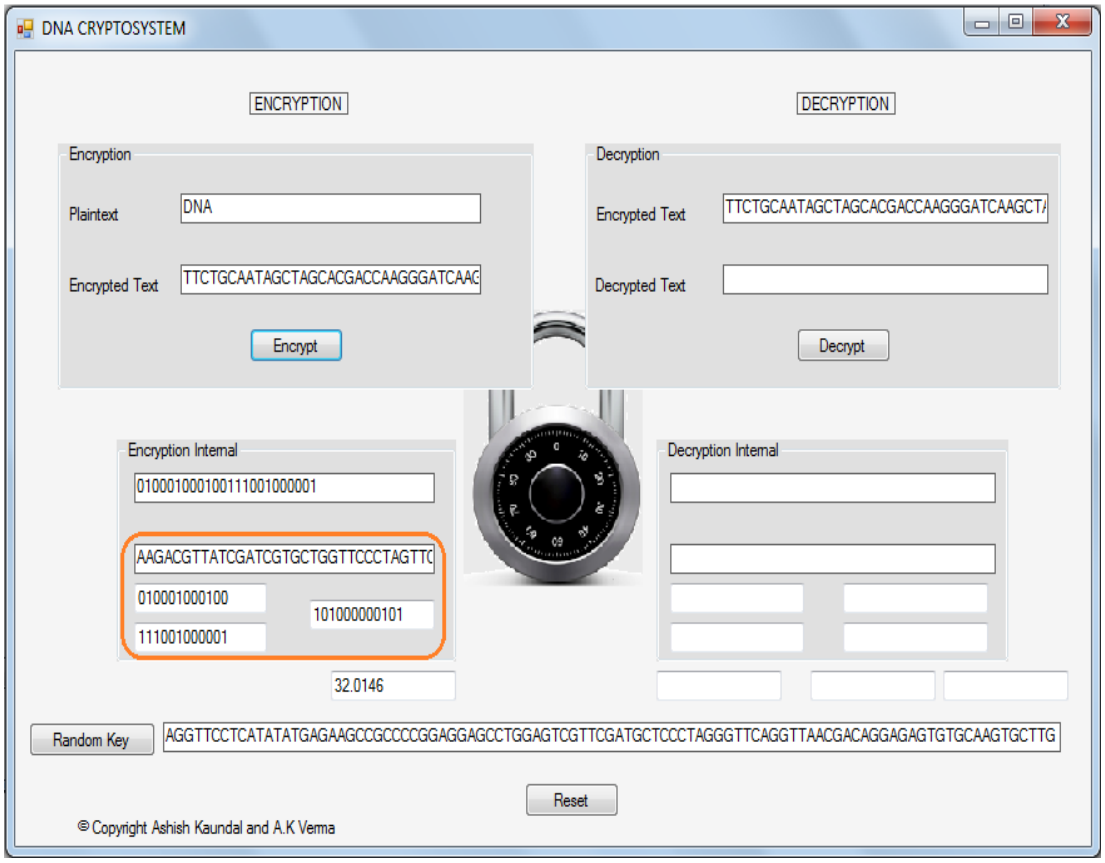


Figure 5.1 (b) Encryption step 1

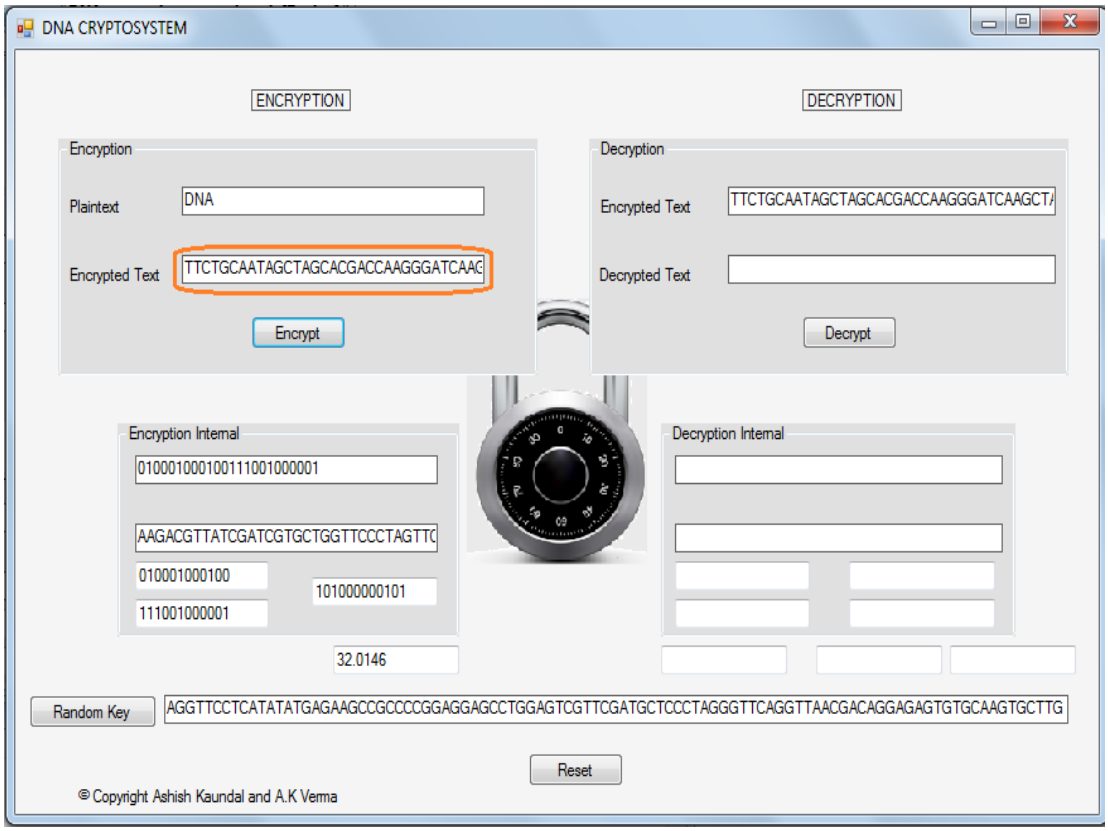


Figure 5.1 (b) Encryption step 2

(c) Decryption

The decryption algorithm will decipher the ciphertext obtained from the sender, this process is just the reverse of the encryption process. Decryption algorithm will first convert the ciphertext into its Watson-Crick complementary form as shown in the fig. below. Then ciphertext is scanned from left to right and key from right to left. As the key is symmetric, it is same at both the ends (sender and receiver). Decryption algorithm will read the string of 5-mer oligonucleotide from the left side of ciphertext and hybridize with the key starting from the right hand side. If the string matched, the binary digit "1" is printed at that position in the key and if the string mismatched, then the binary digit "0" is printed at that position in the key. Similarly all the process goes on till we get the final result, which holds all the binary digits. Now these binary digits are forwarded to the feistel inspired structure for further its processing and then its output is converted into string form which is our plaintext. Hence, receiver obtained the same plaintext which was send by the sender, without any loss of confidentiality.

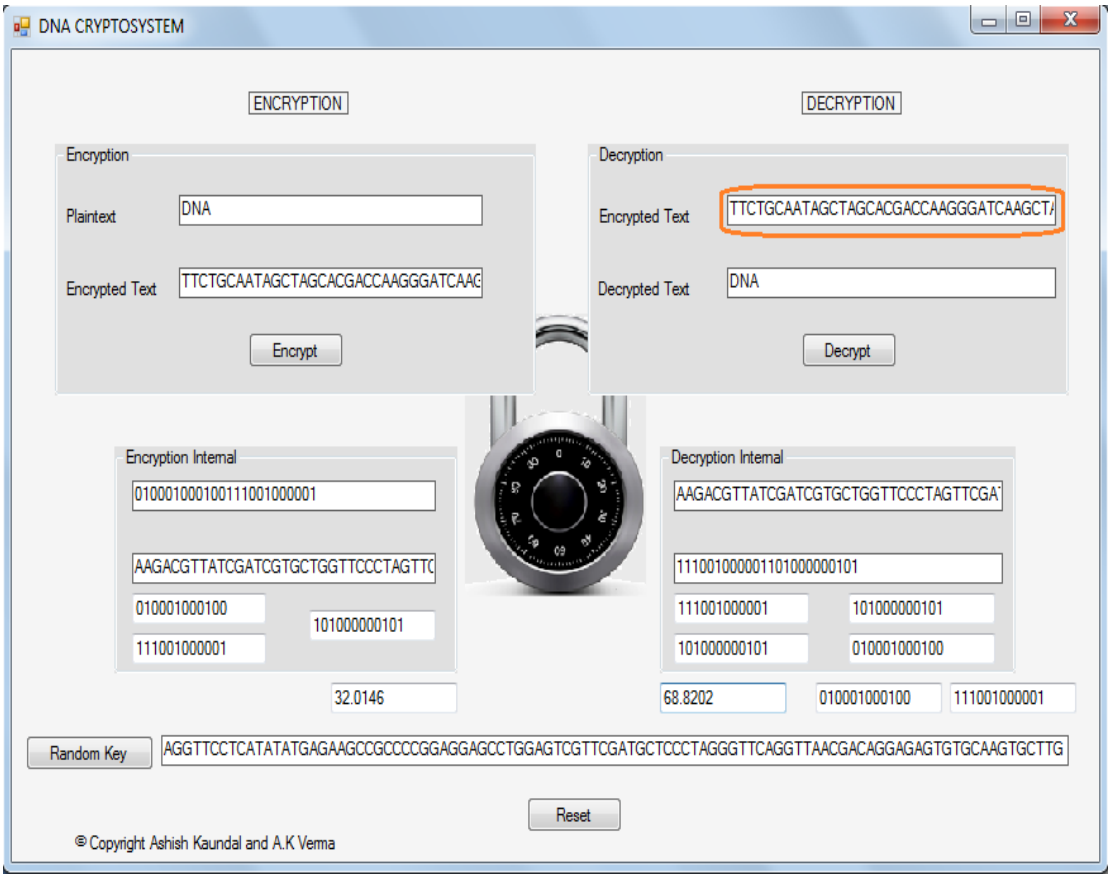


Figure 5.1 (c) Decryption step 1

Whole process is complex enough that if adversary wants to apply some brute force method to know the key sequence then he has to compute 4^{120} different key sequences

which is impossible for the adversary. Only the receiver who has the right key can only perform the decryption of ciphertext.

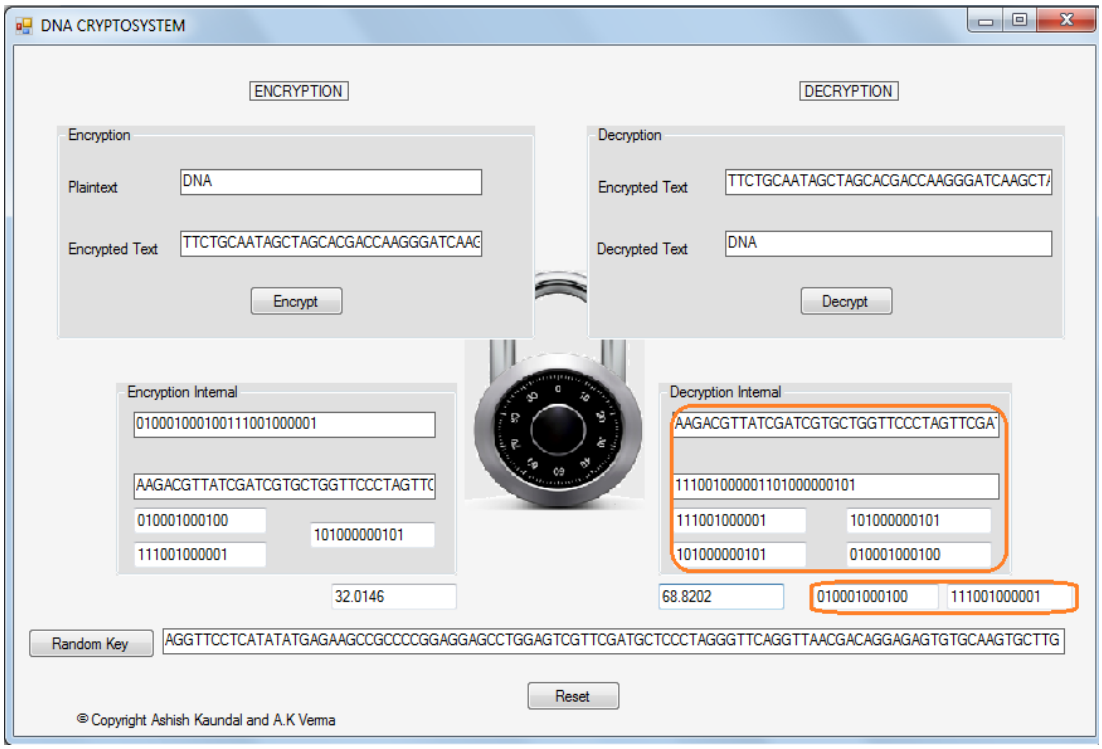


Figure 5.1 (c) Decryption step 2

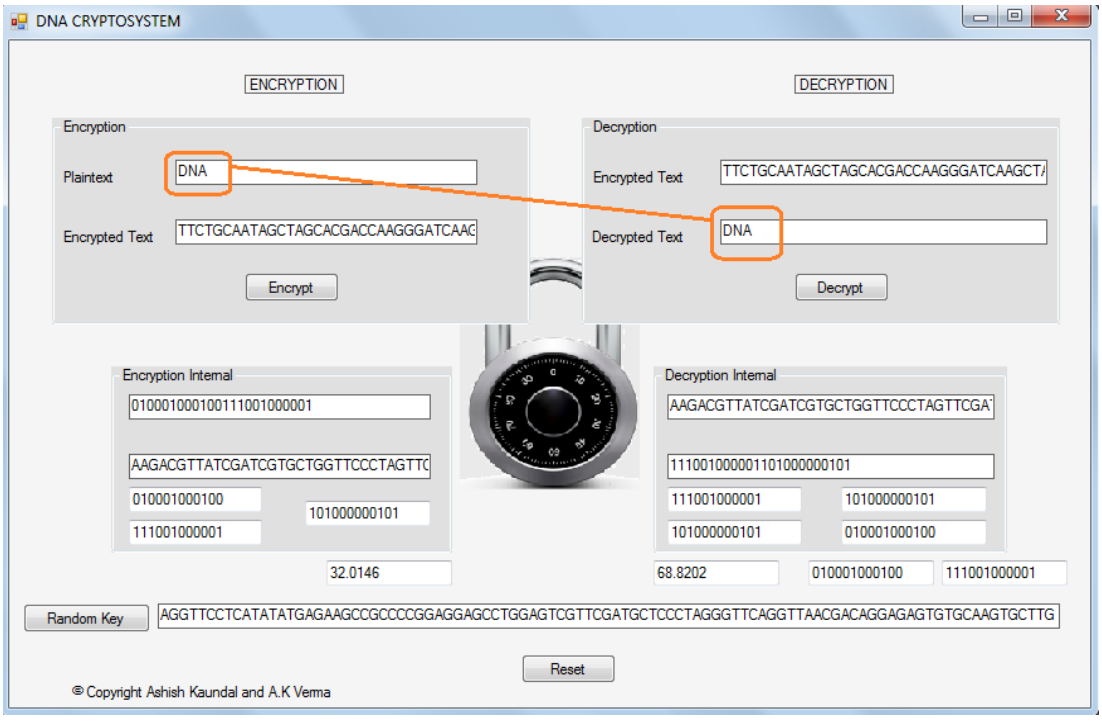


Figure 5.1 (c) Decryption step 3

5.2 Time Complexity

5.2.1 Encryption Time

According to our proposed algorithm if we calculate the encryption time, complexity exists as follows:

1: Plaintext to ASCII conversion – O(h)

2: ASCII to binary plaintext – O(logn)

3: Binary plaintext to feistel inspired structure output – O(n)

4: Scanning EB'' – O(n)

5: Encryption using DNA key sequence - O(n)

So, the overall time complexity at the encryption side is:

$$T(n) = O(n)$$

5.2.2 Decryption Time Complexity

According to our proposed algorithm if we calculate the decryption time, complexity will be as follows:

1: Decryption of ciphertext to binary form using key sequence – O(n)

2: Dividing binary data to feistel inspired structures – O(n)

3: Converting final output of feistel inspired structure to ASCII – O(h)

4: ASCII to plaintext – O(logn)

So, the overall time complexity at the decryption side is:

$$T(n) = O(n)$$

5.3 Results

In this section variable length plaintexts consisting of alphabetical characters, alphanumeric characters, digital characters are used for simulation purposes and results obtained are compared with previous algorithm [22]. Encryption and decryption process is performed ten times and average encryption and decryption time is considered for four different plaintexts with increasing size.

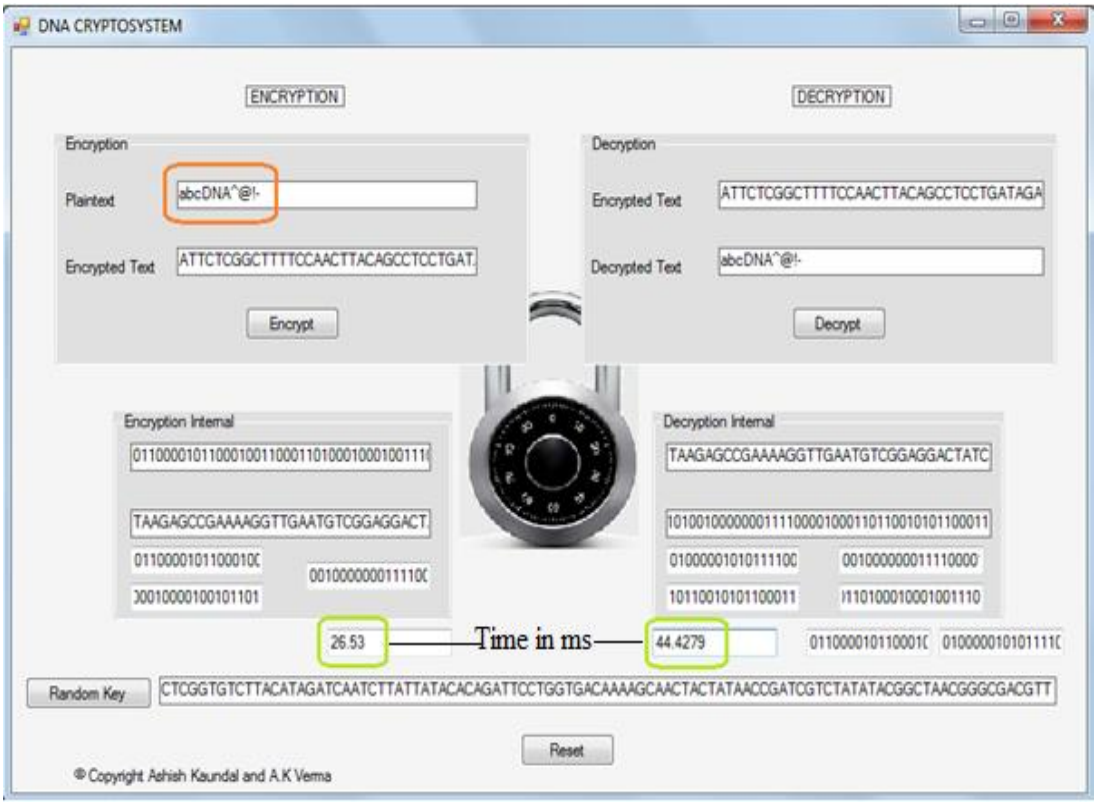


Figure 5.3 (a) Encryption and decryption time for plaintext of length 10

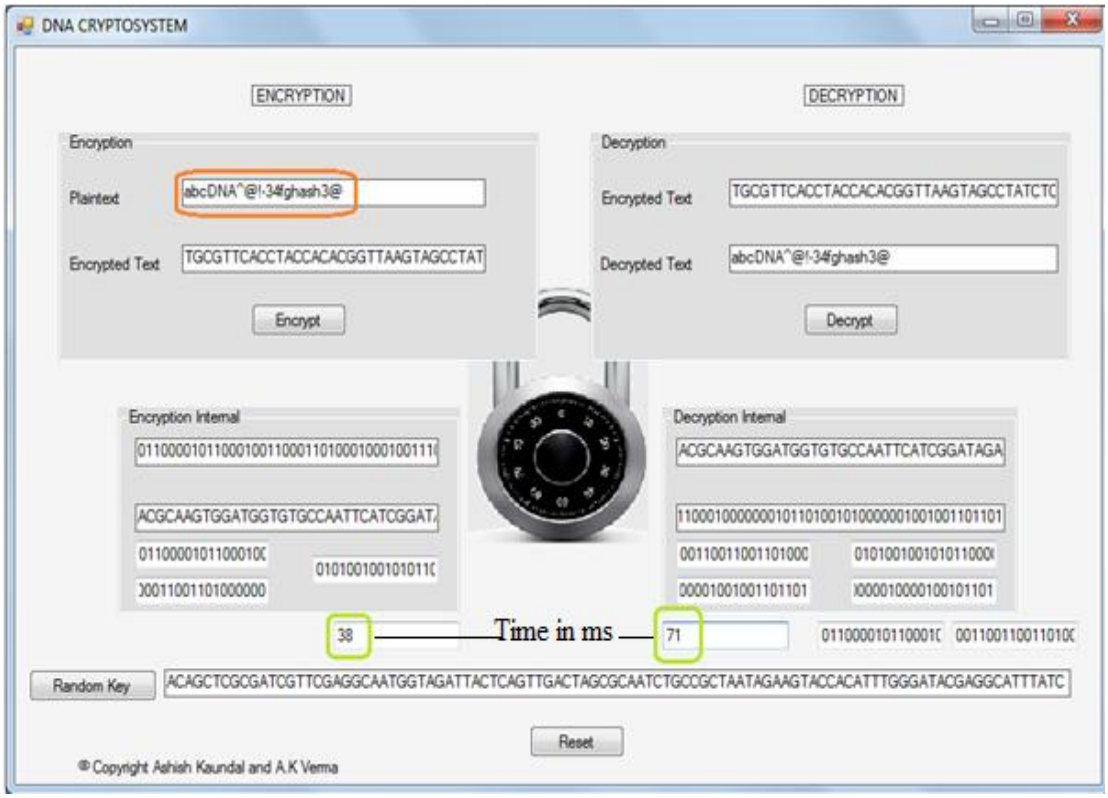


Figure 5.3 (b) Encryption and decryption time for plaintext of length 20

Table 5.3 (a) Encryption Time Analysis

Test Patterns	Size of Plaintext time (Bytes)	Size of Ciphertext (Bytes)	Size of Key (Bytes)	Encryption Time of Previous Algo. [22] (ms)	Encryption Time of Proposed Approach (ms)
Test1	10	160	400	15	20
Test2	20	324	800	27	35
Test3	40	635	1600	38	49
Test4	80	1281	3200	70	96

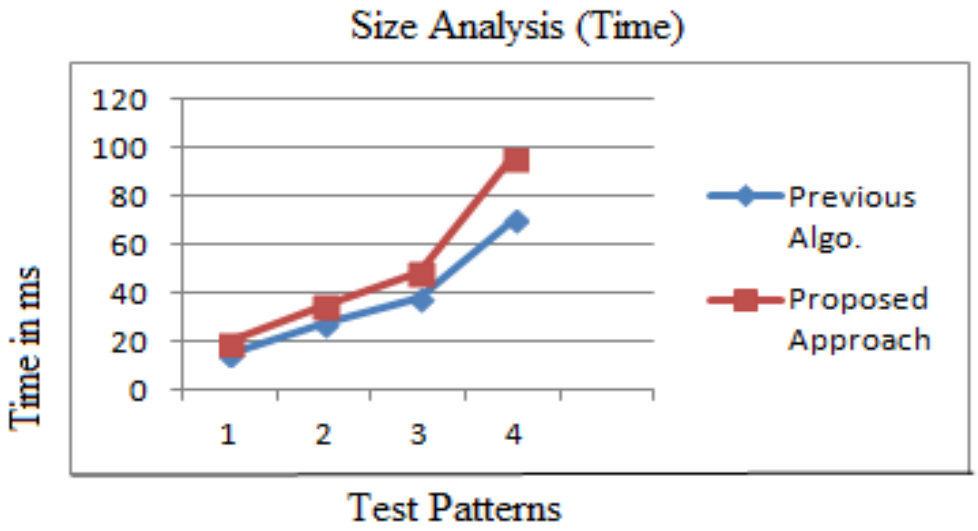


Figure 5.3 (c) Comparison of Encryption Time

As we can clearly observed from the figure above that as the size of plaintext increases encryption time of proposed algorithm is also increases slightly more than it's competitor.

Table 5.3 (b) Decryption Time Analysis

Test Patterns	Size of Plaintext time (Bytes)	Size of Ciphertext (Bytes)	Size of Key (Bytes)	Decryption Time of Previous Algo. [22] (ms)	Decryption Time of Proposed Approach (ms)
Test1	10	160	400	37	49
Test2	20	324	800	44	68
Test3	40	635	1600	110	159
Test4	80	1281	3200	270	414

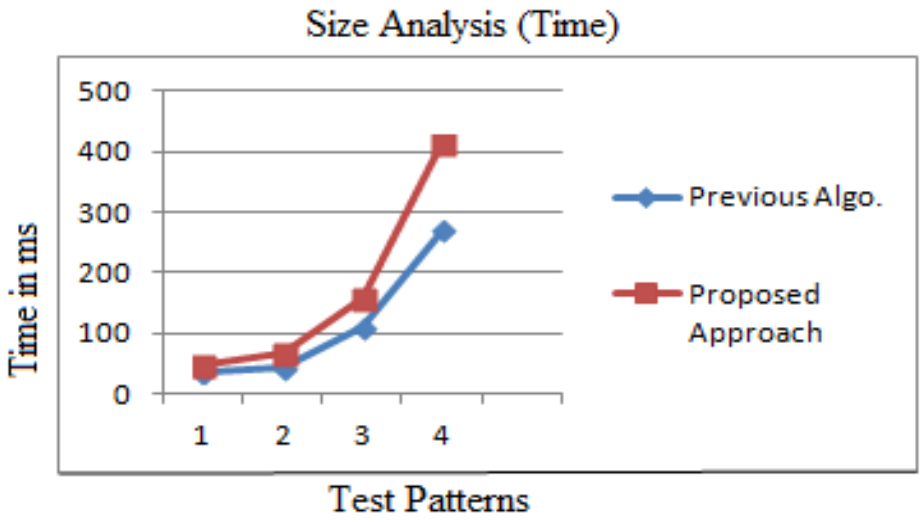


Figure 5.3 (d) Comparison of Decryption Time

As we can clearly see from the graph that decryption time of our proposed algorithm is little bit more than the previous algorithm but it promises greater security than the previous algorithm.

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

In this thesis we have presented DNA cryptographic approach based on feistel inspired structure, implemented and compared with previous algorithm. Further with the addition of One Time Pad in DNA symmetric key cryptography makes it enough strong to protect from brute force attacks. So, if the adversary wants to know the exact key sequence then adversary has to search $4^{\text{key length}}$ different ssDNA key sequences which is very difficult and time consuming. Concept of confusion and diffusion in the proposed method of DNA cryptography also make this unique from other traditional DNA cryptographic approaches.

Further the invention of energy efficient DNA nanochip for computers opens new vistas for the researchers in the field of DNA computing and information security. Though DNA has many positive aspects in different fields which fascinate the researchers, some of the aspects like- requirement of bio molecular labs, environment impact, and quantum attacks are some of the issues that need to be addressed.

6.2 Future Scope

DNA cryptography is a promising field for doing research and some quantum of contribution(s) can be made to the following:

- Looking into the integrity factor of this algorithm.
- Can be extended for steganography, to provide more layer of protection.
- Improving space complexity of this algorithm.

REFRENCES

[1] Adleman, Leonard M, "Molecular computation of solutions to combinatorial problems," *Science-AAAS-Weekly Paper Edition 266*, no. S5187, 1994.

[2] A.K. Verma, R. C. Joshi, and Mayank Dave, "DNA cryptography: a novel paradigm for secure routing in Mobile Adhoc Networks(MANETS)," *Journal of Discrete Mathematics Sciences and Cryptography*, vol.11, 2008.

[3] A. K. Verma, Mayank Dave, R.C. Joshi, "Securing Ad hoc Networks Using DNA Cryptography", *IEEE International Conference on Computers and Devices for Communication (CODEC06)*, pp. 781-786, Dec. 18-20, 2006.

[4] Ashish Gehani, Thomas LaBean, and John Reif, "DNA-based cryptography," *In 5th DIMACS workshop on DNA Based Computers, MIT*. 1999.

[5] Behrouz A. Forouzan, "Cryptography and Network Security", Special Indian Edition, TMH Inc., New York, Chapter 1, pp. 2-13, 2010.

[6] Boneh Dan, Christopher Dimworth, Lipton, Richard J. "Breaking DES Using a Molecular Computer," *DNA based computers* 27, 37: 1996.

[7] Borda, Monica, and Olga Tornea, "DNA secret writing Techniques," In Communications (COMM), *8th IEEE International Conference* on, pp. 451-456, 2010.

[8] Chen Jie, "A DNA-based bio molecular cryptography design," *Proceedings of IEEE International Symposium, Vol. 3*, pp. III-822, 2003.

[9] Cox, Jonathan PL. "Long-term data storage in DNA," *TRENDS in Biotechnology* 19.7: 247-250, 2001.

[10] Cui, Guangzhao, Limin Qin, Yanfeng Wang, and Xuncai Zhang, "An encryption scheme using DNA technology," In Bio-Inspired Computing: Theories and Applications, *IEEE International Conference* on, pp. 37-42, 2008.

[11] Deepak Kumar, and Shailendra Singh, "Secret data writing using DNA sequences," In Emerging Trends in Networks and Computer Communications (ETNCC), *IEEE International Conference* on, pp. 402-40, 2011.

[12] Eric Conrad, " Explanation of Three Types of Cryptosystem", *http://www.giac.org/cissp-papers/52.pdf*, October, 2006.

[13] G. Rozenberg and A. Salomaa, "DNA computing: New ideas andparadigms," Lecture Notes in Computer Science (LNCS), *Springer-Verlag*, Vol. 7, pp. 188-200, 2006.

[14] Jonathan Katz and Yehuda Lindell, *"Introduction to modern cryptography"*. Chapman and Hall/CRC, 2008.

[15] J. Lipton Richard, "DNA solution of hard computational problems", *Science* 268.5210: 542-545, 1995.

[16] Kazuo Tanaka, Akimitsu Okamoto, and Isao Saito, "Public-key system using DNA as a one-way function for distribution," *Biosystems 81*, *1*, pp. 25-29, 2005.

[17] Lai, XueJia, "Asymmetric encryption and signature method with DNA technology," *Science China Information Sciences* 53.3, 506-514: 2010.

[18] M.X. Lu, "Symmetric-key cryptosystem with DNA technology," *Science in China Series F: Information Sciences*, vol.3, pp. 324-333, 2007.

[19] Nathan S Lewis, "Concept of DNA and RNA and Its Structure", *http://www.biologymad.com/resources/DNA.pdf*, March, 2005.

[20] Olga Tornea, and Monica E. Borda, "Security and complexity of a DNA-based cipher," *IEEE Roedunet International Conference (RoEduNet)*, 11th, pp. 1-5, 2013.

[21] Ouyang Qi, D. Peter Kaplan, Liu Shumao and Albert Libchaber, "DNA solution of the maximal clique problem," *Science* 278, 5337, 446-449, 1997.

[22] Pramanik Sabari, and Sanjit Kumar Setua, "DNA cryptography," In Electrical & Computer Engineering (ICECE), *7th IEEE International Conference* on, pp. 551-554, 2012.

[23] Sherif T. Amin, Magdy Saeb and El-Gindi Salah, "A DNA-based implementation of YAEA encryption algorithm," *In Computational Intelligence*, pp. 120-125, 2006.

[24] William Stallings, Cryptography and Network Security, Principles and Practices, Forth Edition, Pearson Education, 2008.

[25] 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.

LIST OF PUBLICATIONS

[1] Ashish Kumar Kaundal, A.K Verma, "DNA Based Cryptography: A Review," International J. Information and Computational Technology, Volume 4, Number 7, pp. 693-698, 2014.

[2] Ashish Kumar Kaundal, A.K Verma, "Quick Review on DNA Based Cryptographic Approaches," In National Conference on Cyber Pollution Problem and Remedy, pp. 75-76, April 4th, 2014.

[3] Ashish Kumar Kaundal, A.K Verma, "Extending Feistel Structure to DNA Cryptography," communicated in J. Discrete Mathematics Sciences and Cryptography, Taylor & Francis.

[4] Ashish Kumar Kaundal, A.K Verma, "DNA Based Cryptography using Feistel Inspired Structure," In Proceedings of Second International Conference on Emerging Research in Computing, Information, Communication and Applications, Elsevier. (Status - Accepted)