Journal of Engineering Science and Technology Review 9 (3) (2016) 86 – 92

Research Article

JOURNAL OF
Engineering Science and Technology Review

www.jestr.org

Information Coding and its Retrieval using DNA Cryptography

A. Ruhan Bevi*, S Malarvizhi and Kathan Patel

Department of Electronics and Communication Engineering, SRM University, Kattankulathur-603203, India.

Received 18 February 2016; Accepted 10 June 2016

Abstract

DNA Cryptography is used to encrypt messages for secure end to end communication over a network. DNA is a well-known information carrier from one generation to another. DNA cryptography is preferred due to information density and parallelism that are inherent in any DNA molecule.In this paper, we propose a new algorithm based on DNA cryptography which enhances the security aspects of the data being sent over a network. This is achieved by introducing feistel inspired structure and adding complex operations to it. Furthermore, this paper discusses DNA cryptosystem concepts based on the classic Vigenere cipher for substitution. One Time Pad is used for generation of the key which provides unique key every time using a random function. This makes the algorithm complex and prevents the attackers/adversaries to perform any brute force attacks. The results indicate that the confidentiality and integrity of the data is maintained and the feistel inspired structure for DNA cryptography using one time pad for key generation achieves a better encryption rate.

Keywords: DNA, Cryptography, DNA sequences, Random funtion, One time pad, Encryption.

1. Introduction

With the growing pace of Internet and network technology day by day, the security threats are also increasing due to lot of information flow on the network. There are various kinds of attackers/adversaries who always try to break into the system either to retrieve the crucial information or to destroy the integrity of data. So, the information security becomes necessary for modern computing systems. Generally, the secret data hiding techniques are used to protect the data from the adversaries. Cryptography and steganography are most common and widely used methods to prevent data from invaders. 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 which may be shared public/private.

Increasing the bit size of encryption reduces the risk of being attacked. A 512 bit encryption seemed to be safe compared to 64/128 bit encryption. So, with the failure of modern cryptographic algorithm like DES and MD5, new 2. methods of information security are needed to protect the data. 3.

Efforts are taken continuously to improve the encryption methods while staying within the limits of available technology.

In the process of cryptography, the algorithm and the key play vital role to ascertain the secrecy of data while saving 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. The general process of cryptography involving both encryption and decryption is shown in the Figure 1.

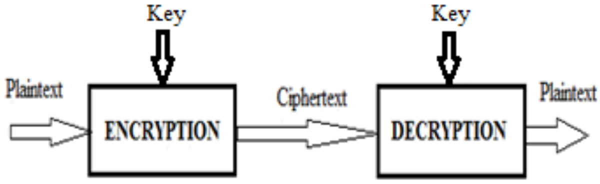


Fig. 1. Flow Diagram of Cryptography

In this paper, section 2 deals with the related works. Section 3 deals with DNA cryptography where DNA sequences, its properties and the concepts of DNA coding are discussed. The proposed method is conferred in section 4 with experimental results listed in section 5. Conclusions are drawn in section 5.

2. Related Work

In 1994, Adleman [1] proposed solution of Hamiltonian path problem using DNA. This resulted into the discover of new field of research known as bio- computing. In 2006, Sherif T. Amin et al. [2] proposed the DNA cryptographic approach based on symmetric key, where key sequences are obtained from the genetic database and remain same at both ends while sending and receiving. Message/plaintext is first converted into binary format and then into a DNA format using substitution. Once the substitution has been performed and message is in the form of DNA sequence, a quadruple is

* E-mail address: ruhan.b@ktr.srmuniv.ac.in

ISSN: 1791-2377 © 2016 Eastern Macedonia and Thrace Institute of Technology.

chosen from the sequence obtained and a match is done with the key sequence. The position of match is used for encrypting/retrieving the message. Random position for each character in the plaintext are obtained this way and the file which contains these positions are defined ciphertext which is send to the receiver where decryption is performed in reverse order.

Deepak Kumar and Shailendra Singh [4] in 2011 proposed a new secret data writing techniques based on DNA sequences. A simple string is transmitted and a ssDNA One-time pad (OTP) key of 350 bits is generated which is 70 times longer than the plaintext and is used to perform encryption and decryption on the plaintext using symmetric key. 4^{350} different ssDNA strings should be addressedby the attacker to explore the key.

Bibhash Roy et al.[5] in 2011 proposed an improved symmetric key cryptography with DNA based strong cipher. A DNA computational logic is discussed for encrypting, storing and transmitting the data.

In 2013, Wang Zhong et al.[6] proposed an Index based DNA encryption algorithm. Block cipher and Index of string is used for encrypting message into DNA sequences, which is send to the receiver by a secure communication medium. The message was converted into ASCII and binary which is further converted into DNA sequence to perform searching in the key sequence.

Ashish Kumar Kaundaland A.K Verma [8] in 2014 proposed a DNA cryptographic approach based on symmetric key using OTP. A fiestel inspired structure for DNA cryptography was proposed using genetic database.

MohammadrezaNajaftorkaman, Nazanin Sadat Kazazi [11] in 2015 proposed a new DNA cryptography algorithm based on the classic Vigenere cipher. OTP key was generated and plain text was encrypted in DNA format using substitution method.

In our proposed method based on DNA cryptography, the plaintext is hidden in the DNA digital form.DNA cryptography uses DNA for storing data. DNA cryptography enables the confidentiality of data more high than the modern methods with the use of OTP keys and its size.

3. DNA Cryptography

In this section, basic concepts of DNA sequences and its properties are discussed first. These concepts are essential to understand the DNA coding techniques which are discussed later in this section.

3.1 DNA Sequences and it's Properties

Deoxyribonucleic Acid (DNA) is the heredity unit and also a information carrier of all living organism ranging from small viruses, chromosomes to complex human beings. DNA is a long polymer of small units called nucleotides. Each nucleotide consists of the following three components: a nitrogenous base, a five carbon sugar and a phosphate group. There are four different nucleotides classified upon the type of nitrogenous base which are A, C, T, G called Adenine, Cytosine, Thymine and Guanine respectively. Watson-Crick proposed a complimentary rule for DNA sequences that is "A combines with T through double bound A=T and C combines with G through triple bound C≡G. Adenine and Guanine are called purines and Thymine and Cytosine are called pyrimidines in biological terms**.** DNA is a double helical structure with two strands running anti parallel as shown in figure 2 below.

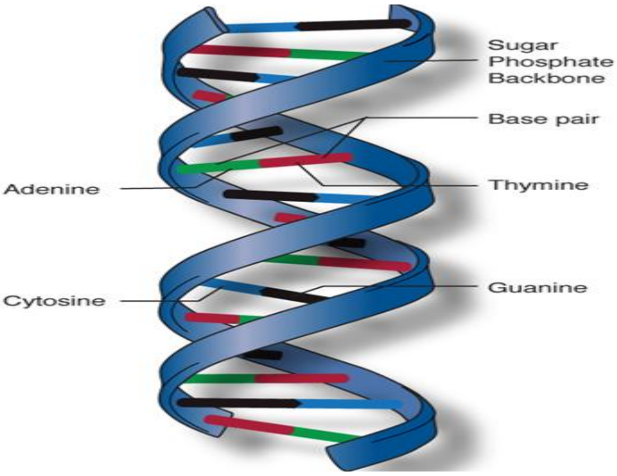


Fig. 2. Double Helical Structure of DNA *Courtesy:www.microbe.net*

3.2 DNA Coding

DNA cryptography is either based on molecular theory or on conventional approach. DNA Coding is a new way for storing large amount of data in the small fragment of DNA and providing security to it. DNA structure provides vast parallelism, exceptional energy efficiency and extra ordinary storage capacity. A 1 gm of DNA can store about 10^8tera bytes of digital data [9]. It provides security by using the properties of DNA and good number of arithmetic operations.

The proposed method employs DNA cryptography consisting of regular key generation, encryption and decryption process [3,10]. The DNA cryptography differs from the conventional cryptography in following ways:

i) Key generation: The key sequence is in a DNA format say ATCGCCAG which is purely based on OTP.
ii) Cipher text: The cipher text produced during encryption process by converting plaintext is also in DNA form.
iii) 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.DNA Cryptography based on symmetric key [7] is shown below:

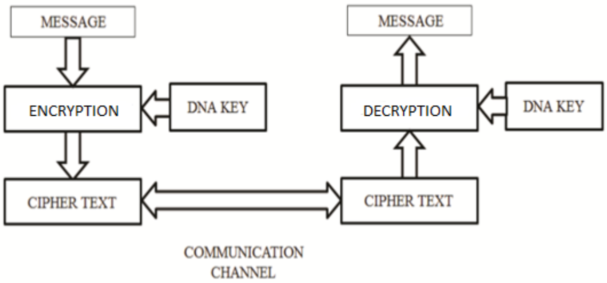


Fig. 3. DNA Cryptography: An overview

The key generation is based on the OTP and according to the Shannon's theory,

$K_{size} \geq P_{size}$

whereK_{size} => Size of the key.
P_{size} => Size of the plaintext.

The encryption block involves the process of shifting, confusion and substitution which are performed on the feistel structure of the message. The decryption block involves the process which is just the reverse of the encryption process and it uses the symmetric DNA key for decryption of the cipher text to obtain the plain text. The methodology for DNA encryption is described below:

1) Set fixed number of nucleotides adaptive for any length of plaintext P.

2) Devise an algorithm inspired on feistel inspired structure and Vigenere cipher in order to make the ciphertext.

3) MATLAB will be used for simulating the proposed algorithm.

4) Variable length plaintexts consists of numeric, alphanumeric and alphabets are simulated to deliver corresponding ciphertext.

5) Validate this algorithm with the conventional cryptographic algorithms for parameters like security, encryption and decryption time.

4. The Proposed Method

The input to the encryption algorithm will be a plaintext which is entered by the user. Encryption algorithm converts the plaintext into ciphertext where it is coded as DNA sequence using a DNA key. The obtained ciphertext is given as a input to the decryption algorithm which converts it back into plaintext using the same DNA key. There are five main steps in implementing the proposed DNA cryptography algorithm: data pre-processing, key generation, encryption, decryption, and data post-processing.

A. DATA PRE-PROCESSING

1. The plaintext Pis converted intoASCII, P_{ASCII} and then to binary plaintext, P_B.

2. Re-ordering of binary plaintext is done as follows:

a) The first byte of P_B is shifted left by 2 bits and the last byte is shifted right by 4 bits to obtain P_{B1}.
b) After shifting, XOR operation is performed on P_{B1} to obtain P_{B2} as shown in figure 4.

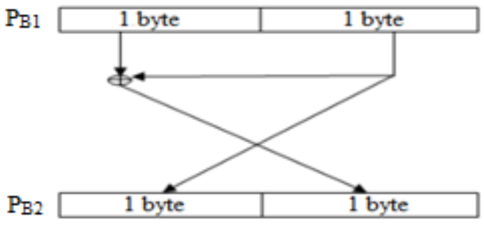


Fig. 4. .Reordering of the plaintext.

B. KEY GENERATION

A random key sequence based on OTP uses pseudo-random generator to provide a seed of 32 bytes. This is used to provide a DNA sequence as an input from the genetic database (Genbank) and keeps 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. For the implementation of the proposed algorithm, the Bioinformatics Toolbox provided by the MATLAB is used. The getgenbank function retrieves sequence information from GenBank database. This database is maintained by the National Center for Biotechnology Information (NCBI) [12].

NCBI bank is the master bank of all human genome and search for different kinds of DNA string are performed. It provides a sample database of DNA strings and MATLAB is used to extract from the NCBI database. The following function extracts the DNA sequence from the NCBI bank:

```
M= getgenbank('NC_001807','SequenceOnly',true);
```

where the variable M is returned with 32 bytes of DNA sequence. To produce a DNA key a 'Rand' function is used to identify the start index of the DNA secret key.

```
startindex=fix(10*rand);
```

After that some value are added to the "startindex" variable to identify the end index of the DNA strand. All the DNA nucleotides from start index to end index are extracted to obtain the key. In this paper, the length of DNA secret key depends upon the length of the plain text.

C. ENCRYPTION

1. DNA substitution is performed on P_{B2} with DNA key (K). P_{B2} is scanned from left to right and key is scanned from right to left. The substitution is explained in following pseudocode.

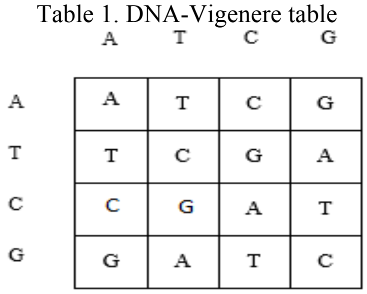
Pseudocode: Encryption

```
for  i:=1 to length(P_B2) do
{
if P_B2(i) = '1'
then
    Pick 5-mer nucleotides from DNA key
if P_B2(i) ='0'
then
    Skip 5-mer nucleotides from DNA key
}
end
```

DNA sequence is obtained at the end of above process.

2.P_{B2} is processed based on the Vigenere cipher, to obtain a sequence P_{B3} through the following steps. The DNA-Vigenere table based on the properties of the Vigenere cipheris shown in table below:

Table 1. DNA-Vigenere table



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

The characters of the P_{B2} show the row number of the DNA-Vigenere table and the characters of the key (K) shows the column number of the table.

P_{B2} is scanned from left to right and K too is scanned from left to right and P_{B3} is obtained.

For example, if the first character of P_{B2} is 'A' and the first character of K is 'G' that means row 1, column 4. Therefore, we replace the first character of P_{B2},A with G.

- The process continues up-to the length of P_{B2}.

3. Now $P_{B3}$is converted into its Watson Crick's complementary (W) to produceciphertext (C).

4. Sender sends the DNA sequence in the form of packets to the receiver.
The process flow of A,B,C is illustrated in figure 5.

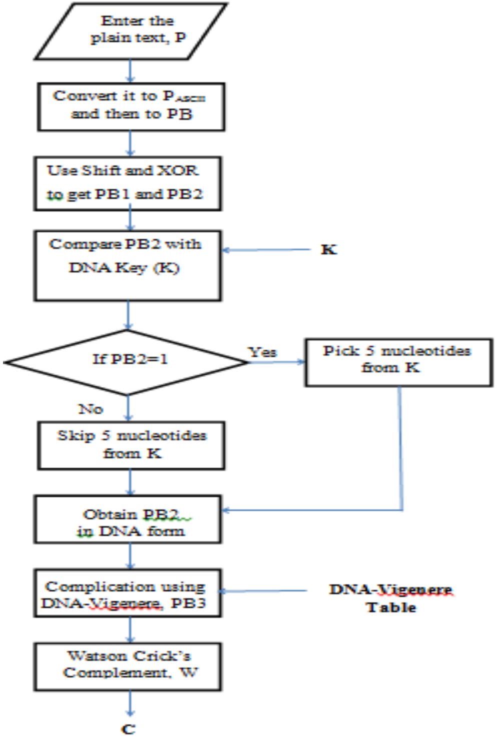

Enter the plain text, P
Convert it to P_{ASCII} and then to PB
Use Shift and XOR to get PB1 and PB2
Compare PB2 with DNA Key (K)
K
If PB2=1
Yes
Pick 5 nucleotides from K
No
Skip 5 nucleotides from K
Obtain PB2 in DNA form
Complication using DNA-Vigenere, PB3
DNA-Vigenere Table
Watson Crick's Complement, W
C

Fig 5. Proposed DNA Encryption Flow Diagram.

D. DECRYPTION

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

1. Receiver receives the packets, arranges them and obtains the ciphertext.

2. Watson Crick's complementary form of ciphertext is done to obtain DNA sequence.

3. This DNA sequence is processed using Vigenere Cipher table to obtain D_{B1}. Both the key and the DNA sequence obtained from step (2) are scanned from left to right. This process is just the reverse of that of the encryption process.

4. The reverse process of substitution is performed on D_{B1} with the help of DNA key as follows:
D_{B1} is scanned from left to right and key from right to left.

```
Pseudocode: Decryption
for   i:=1 to length($D_{B1}$) do
{
if $D_{B1}(i)$ = 5-mer nucleotides in DNA key
then
Insert '1'
if$D_{B1}(i) \neq$ 5-mer nucleotides in DNA key
then
Insert '0'
}
end
```

The result of the above process is a data in binary form D_{B2}.

E. DATA POST-PROCESSING

1. The reverse process of reordering is performed on D_{B2} using two feistel inspired structure in order to obtain $D_{B3}$and D_{B4} as shown in figure 6.

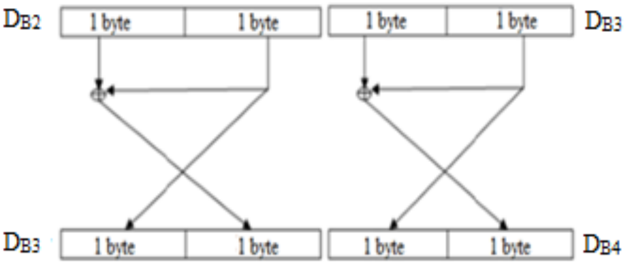


Fig 6. Reordering of ciphertext

2.The first byte of D_{B4} is then shifted right by 2 bits whereas the last byte is shifted left by 4 bits.

3. Finally the result of step (2) is converted into ASCII format and then to the desired plaintext.

The process flow of D and E is illustrated in figure 7.

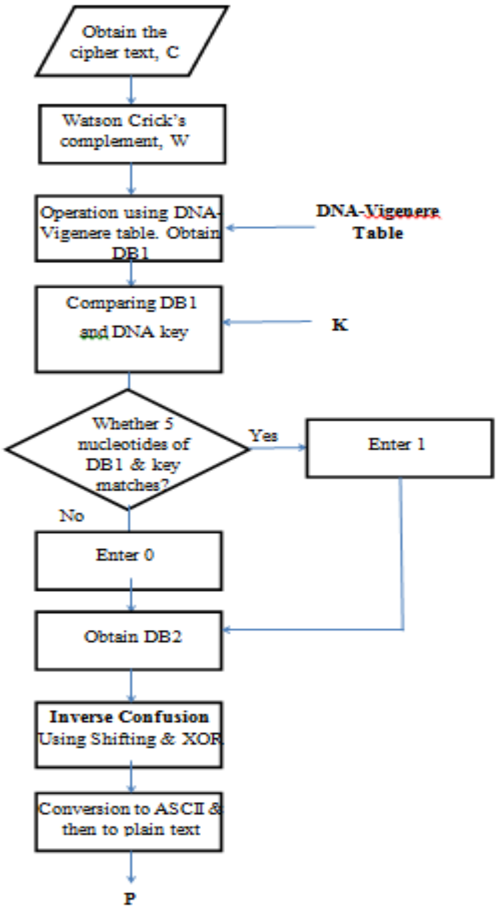

Obtain the cipher text, C
Watson Crick's complement, W
Operation using DNA-Vigenere table. Obtain DB1
DNA-Vigenere Table
Comparing DB1 and DNA key
K
Whether 5 nucleotides of DB1 & key matches?
Yes
Enter 1
No
Enter 0
Obtain DB2
Inverse Confusion Using Shifting & XOR
Conversion to ASCII & then to plain text
P

Fig. 7.Proposed DNA Decryption Flow Diagram.

5. Experimental Results

Validation for the encryption and decryption of the proposed method is demonstrated below. The entire simulation was done using MATLAB 7.10.0.499 (R2010A). The Bioinformatics toolbox provided by MATLAB is used for the generation of the key.

Key Generation

In our proposed algorithm, K depends upon P and 5-mer nucleotides.
Since the length of P_B is 16, DNA key sequence length becomes: P_B * 10 => 16*10 => 160.
Now OTP generates DNA key of length: 160.
Let the obtained key, K be=>

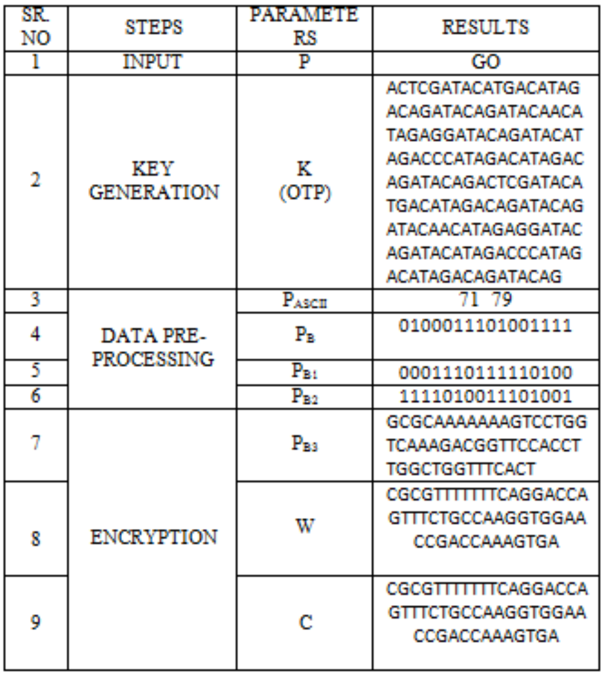
ACTCGATACATGACATAGACAGATACAGATACAAC
ATAGAGGATACAGATACATAGACCCATAGACATAG
ACAGATACAGACTCGATACATGACATAGACAGATA
CAGATACAACATAGAGGATACAGATACATAGACCC
ATAGACATAGACAGATACAG

This DNA key is shared between both the sender and the receiver for this session.

Encryption

The results of all the steps involved in encryption are depicted in the table 2 below:

Table 2. Encryption Results



SR. NO	STEPS	PARAMETERS	RESULTS
1	INPUT	P	GO
2	KEY GENERATION	K (OTP)	ACTCGATACATGACATAG ACAGATACAGATACAACA TAGAGGATACAGATACAT AGACCCATAGACATAGAC AGATACAGACTCGATACA TGACATAGACAGATACAG ATACAACATAGAGGATAC AGATACATAGACCCATAG ACATAGACAGATACAG
3	DATA PRE-PROCESSING	P_{ASCII}	71 79
4		P_B	0100011101001111
5		P_{B1}	0001110111110100
6		P_{B2}	1111010011101001
7	ENCRYPTION	P_{B3}	GCGCAAAAAAAGTCCTGG TCAAAGACGGTTCCACCT TGGCTGGTTTCACT
8		W	CGCGTTTTTTTCAGGACCA GTTTCTGCCAAGGTGGAA CCGACCAAAGTGA
9		C	CGCGTTTTTTTCAGGACCA GTTTCTGCCAAGGTGGAA CCGACCAAAGTGA

The re-ordering of P_B is done to get P_{B1}. We have:
P_B – 0100011101001111

The first byte of P_B is shifted left by 2 bits and the last byte of P_B is shifted right by 4 bits to obtain P_{B1}.

P_{B1}- 0001110111110100

Now XOR operation shown in figure 8 is performed on P_{B1} to obtain P_{B2}.

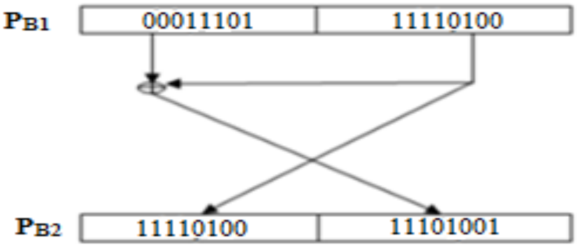
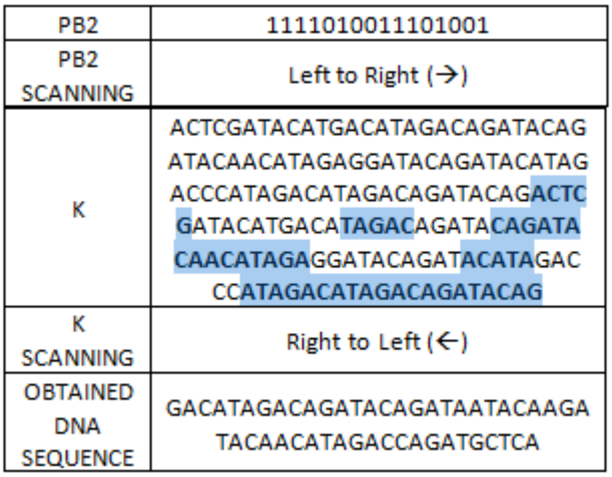


Fig 8. Re-ordering of plaintext

Substitution is performed on $P_{B2}$with the help of K. $P_{B2,}$ which is binary form is converted into DNA form using K. Table 3 shows this process. The shaded region in K shows 5-mer nucleotides which are selected out of the entire key depending upon $P_{B2.}$

Table 3.Comparison of P_{B2} and K



PB2	1111010011101001
PB2 SCANNING	Left to Right (→)
K	ACTCGATACATGACATAGACAGATACAG ATACAACATAGAGGATACAGATACATAG ACCCATAGACATAGACAGATACAGACTC GATACATGACATAGACAGATACAGATA CAACATAGAGGATACAGATACATAGAC CCATAGACATAGACAGATACAG
K SCANNING	Right to Left (←)
OBTAINED DNA SEQUENCE	GACATAGACAGATACAGATAATACAAGA TACAACATAGACCAGATGCTCA

Hence, P_{B2} in DNA form-

GACATAGACAGATACAGATAATACAAGATACAACA
TAGACCAGATGCTCA

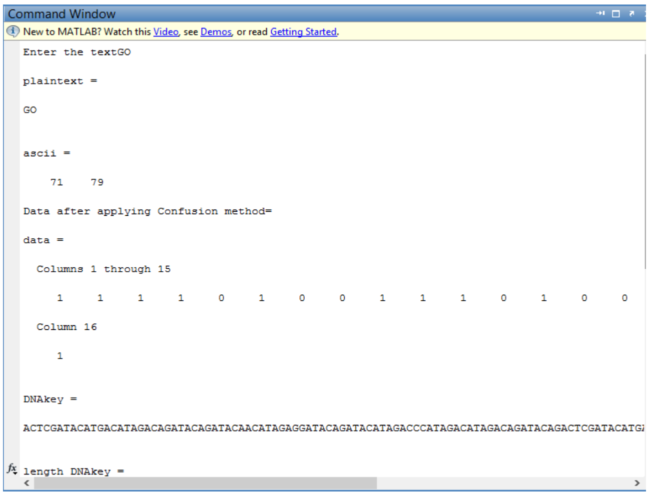
The DNA sequence obtained is processed based on the Vigenere cipher to obtain a new DNA sequence P_{B3}. This operation is based on table 1 shown previously.

P_{B3}-
GCGCAAAAAAAGTCCTGGTCAAAGACGGTTCCACC
TTGGCTGGTTTCACT

Now DNA sequence is converted into its Watson Crick's complementary formwhich represents Cipher text, C.
Thus we get,

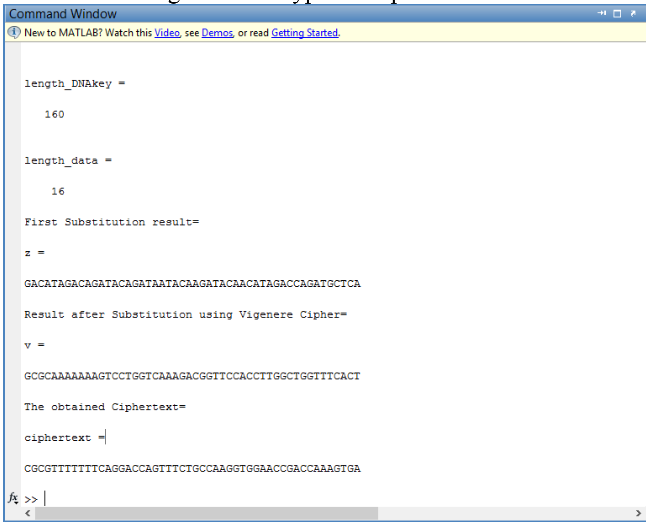
**CGCGTTTTTTTCAGGACCAGTTTCTGCCAAGGTG
GAACCGACCAAAGTGA**

The simulation of the above encryption in MATLAB is shown in figure 9 and figure 10. Figure 9 shows the entered plaintext, result after confusion and shifting and the DNA key. Figure 10 shows the result after substitution, result after Vigenere cipher operation and the obtained ciphertext.


Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.

```
Enter the textGO

plaintext =

GO


ascii =

    71    79

Data after applying Confusion method=

data =

  Columns 1 through 15

     1     1     1     1     0     1     0     0     1     1     1     0     1     0     0

  Column 16

     1


DNAkey =

ACTCGATACATGACATAGACAGATACAGATACAACATAGAGGATACAGATACATAGACCCATAGACATAGACAGATACAGACTCGATACATGA

length DNAkey =
```

Figure 9. Encryption of plaintext


Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.

```
length_DNAkey =

   160


length_data =

    16

First Substitution result=

z =

GACATAGACAGATACAGATAATACAAGATACAACATAGACCAGATGCTCA

Result after Substitution using Vigenere Cipher=

v =

GCGCAAAAAAAGTCCTGGTCAAAGACGGTTCCACCTTGGCTGGTTTCACT

The obtained Ciphertext=

ciphertext =

CGCGTTTTTTTCAGGACCAGTTTCTGCCAAGGTGGAACCGACCAAAGTGA

>> |
```

Fig. 10. Encryption of plaintext

Decryption

Receiver receives the ciphertext, C and the results of various operations are shown in table 4 below.

Table 4. Decryption Results

SR. NO	STEPS	PARAMETERS	RESULTS
1	INPUT	C	CGCGTTTTTTTCAGGACC AGTTTCTGCCAAGGTGGA ACCGACCAAAGTGA
2	DNA KEY	K	ACTCGATACATGACATAG ACAGATACAGATACAACA TAGAGGATACAGATACAT AGACCCATAGACATAGAC AGATACAGACTCGATACA TGACATAGACAGATACAG ATACAACATAGAGGATAC AGATACATAGACCCATAG ACATAGACAGATACAG
3	DECRYPTION	W	GCGCAAAAAAAGTCCTG GTCAAAGACGGTTCCACC TTGGCTGGTTTCACT
4		D_{B1}	GACATAGACAGATACAG ATAATACAAGATACAACA TAGACCAGATGCTCA
5		D_{B2}	1111010011101001
6	DATA POST-PROCESSING	D_{B3}	1110100100011101
7		D_{B4}	0001110111110100
8		$D_{B4shift}$	0100011101001111
9		P	GO

The Watson Crick's complement, W is processed using Vigenere cipher shown in table 1 to obtain D_{B1}.
This process is just the opposite of that done in encryption.

D_{B1}-
GACATAGACAGATACAGATAATACAAGATACAACA
TAGACCAGATGCTCA

Now Inverse substitution is performed on D_{B1} using the key as discussed above to obtain D_{B2}. Thus we get:

D_{B2}-1111010011101001

Now D_{B2} is moved to the feistel inspired structures for further processing in order to obtain the desired plaintext as shown in figure 11.

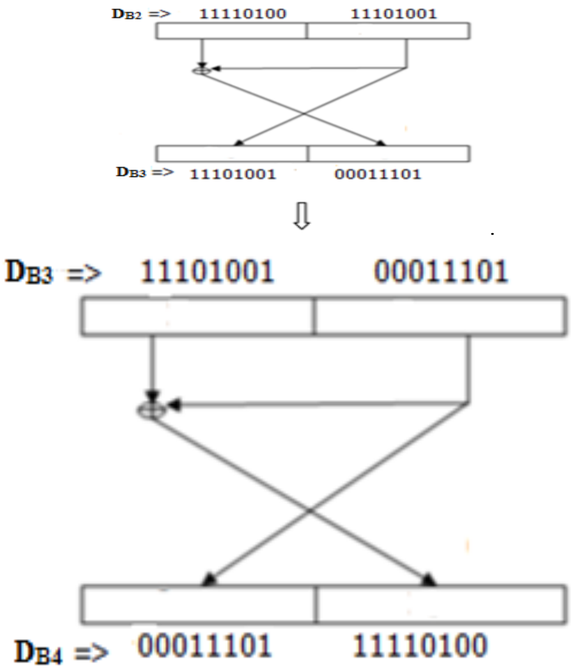


Fig. 11. Reverse process of confusion for decryption

Once D_{B4} is obtained, the process of shifting is done. The direction of shifting is just the opposite of that done in encryption.

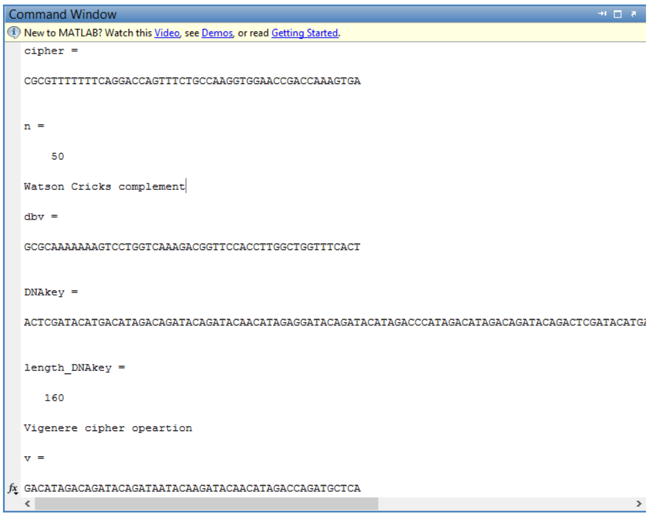
Thus we get,

D_{B4}shift- 0100011101001111

After getting the value of D_{B4}shift, it is converted into its ASCII form and then to the desired plaintext: - "GO".

Decrypted text- GO

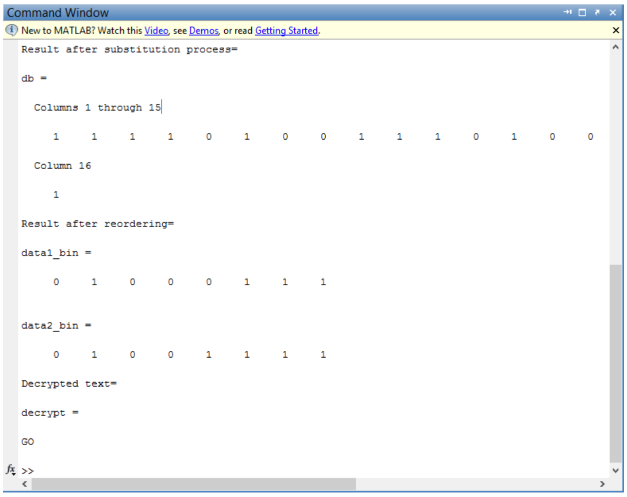
The simulation of above decryption in MATLAB is shown in figure 12 and figure 13. Figure 12 shows the obtained ciphertext, its Watson's Crick Complement, the DNA key and the result after Vigenere operation. Figure 13 shows the result after substitution, result after shifting and confusion and the obtained plaintext.



Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.

```
cipher =

CGCGTTTTTTTCAGGACCAGTTTCTGCCAAGGTGGAACCGACCAAAGTGA


n =

    50

Watson Cricks complement

dbv =

GCGCAAAAAAAGTCCTGGTCAAAGACGGTTCCACCTTGGCTGGTTTCACT


DNAkey =

ACTCGATACATGACATAGACAGATACAGATACAACATAGAGGATACAGATACATAGACCCATAGACATAGACAGATACAGACTCGATACATG


length_DNAkey =

   160

Vigenere cipher opeartion

v =

GACATAGACAGATACAGATAATACAAGATACAACATAGACCAGATGCTCA
```

Fig 12.. Decryption of ciphertext



Command Window
New to MATLAB? Watch this Video, see Demos, or read Getting Started.

```
Result after substitution process=

db =

  Columns 1 through 15

     1     1     1     1     0     1     0     0     1     1     1     0     1     0     0

  Column 16

     1

Result after reordering=

data1_bin =

     0     1     0     0     0     1     1     1


data2_bin =

     0     1     0     0     1     1     1     1

Decrypted text=

decrypt =

GO

>>
```

Fig. 13. Decryption of ciphertext

Entire encryption and decryption process is secure and if the adversary wants to apply brute force method in order to compute the key sequence from ciphertext then 4^{160} different computations should be performed for DNA key sequences.

6. Conclusions

In this paper, a DNA cryptographic approach was a feistel network with Vigenere cipher substitution. The addition of OTP in DNA cryptography makes the technique strong enough to protect from brute force attacks. So, if the attacker wants to know the exact key sequence then the attacker has to search $4^{\text{key length}}$ different DNA key sequences which are very difficult and time consuming.

The shifting, confusion and substitution concepts used in the approach makes the algorithm secure and easy to use. Further the invention of energy efficient DNA nanochip for computers opens new horizons for the researchers in the field of DNA computing and information security.

References

1. L. M. Adleman, "Molecular computation of solutions to combinational problems," Science,**vol. 266**, pp. 1021–1024 (1994) .
2. Sherif T. Amin, Magdy Saeb and El-Gindi Salah, "A DNA-based implementation of YAEA encryption algorithm," Computational Intelligence,pp. 120-125, (2006).
3. Deepak Kumar and Shailendra Singh, "Secret data writing using DNA sequences", Emerging Trends in Networks and Computer Communications (ETNCC), IEEE International Conference, pp. 402-405, (2011)
4. Bibhash Roy, PratimSingha, "An improved symmetric key cryptography with DNA based strong cipher", IEEE International Conference on Devices and Communications (ICDeCom),(2011).
5. Wang Zhong, Zhy Yu, "Index-based symmetric DNA encryption algorithm", Proceedings of Image and Signal Processing (CISP), 4th International congress on image and signal processing, (2011).
6. Ashish Kumar Kaundal and A.K Verma, "DNA Cryptography : A Review", International Journal of Information & Computation Technology, ISSN 0974-2239 **Volume 4**, Number 7, pp. 693-698, (2014).
7. MohammadrezaNajaftorkaman, Nazanin Sadat Kazazi, "A Method to Encrypt Information with DNA-Based Cryptography", International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(3), pp. 417-426, (2015).
8. Tausif Anwar, Dr. Sanchita Paul and Shailendra Kumar Singh, "Message Transmission Based on DNA Cryptography: Review", International Journal of Bio-Science and Bio-Technology **Vol.6, No.5**, pp.215-222, (2014)
9. M. X. Lu, "Symmetric-key cryptosystem with DNA technology", Science in China Series F: Information Sciences,**vol. 3**, pp. 324–333, (2007)
10. Shipra Jain and Vishal Bhatnagar, "Bit Based Symmetric Encryption Method Using DNA Sequence", 5th International Conference of The Next Generation Information Technology Summit (Confluence), (2014).
11. Naveen Jarold K, P Karthigaikumar, N M Sivamangai, Sandhya R, Sruthi B Asok, "Hardware Implementation of DNA Based Cryptography",Proceedings of 2013 IEEE Conference on Information and Communication Technologies (ICT), (2013).
12. http://www.ncbi.nlm.nih.gov/Genbank/