DNA Cryptography Based on Symmetric Key Exchange

Tausif Anwar[#1], Abhishek Kumar[#2], Sanchita Paul[#3]

[#]Dept. of Computer Science & Engg.
Birla Institute of Technology, Mesra Ranchi, 835215, India
[1]tausifanwar30@gmail.com
[2]abhikmr012@gmail.com
[3]sanchita07@gmail.com

Abstract: - DNA cryptography is a technology of bio science to encrypt large message in compact volume. Now a day, researchers are going to research in the field of secure data transmission. Hiding the encrypted message is important part of Cryptography. Hidden message is in the form of DNA sequence, image, audio and video, which is used to prevent important data from the intruders.

In this paper, a new cryptography technique is proposed using Symmetric Key Exchange, one-time pad scheme and DNA hybridization to minimize time complexity.XOR operation with OTP DNA sequence is used as encryption technique based on DNA cryptography. Symmetric Key Exchange is presenting a secure key generation scheme. This method is very efficient in encrypting, hiding, transmitting and preventing powerful attacks.

Keywords: -DNA Cryptography, One time pad, DNA technologies, Hiding data.

I. INTRODUCTION

DNA cryptography is a new field of technology for encrypting any kind of message. Nowadays researchers are focusing on different DNA technologies. There are two ways to realize DNA technology - DNA computing and conventional cryptography. DNA computing uses molecular biology which consists of DNA hybridization, DNA fragmentation and micro biology. According to Adleman, DNA computing is used to solve Hamiltonian path problem [1]. Hamiltonian path problem is finding shortest path to reach from source to destination. He solved seven vertices graph and encoded in molecular structure form, further extend by Lipton to solve NP-complete problem [2]. It has a parallel processing capability with molecular biology and new data structure. DNA cryptography has parallel computing properties to perform the encryption and decryption of the public and private keys. In Public key cryptography same key is used for encrypting and decrypting message and provides security, confidentiality and integrity. A traditional cryptography like DES can be broken by the use of DNA computing [4]. Adleman and Lipton performed DNA polymerase, PCR amplification on DNA strands to encoding of plaintext into binary string [6]. One time pad technique can be used for splitting the DNA sequence and extended in steganogaphy. In modern technology, there is a need of high storage requirement of huge amount of information [7]. DNA cryptography stores huge amount of data in small volume with the combination of only these four letters A, C, G, and T. These bases form the structure of DNA strands by forming hydrogen bonds with each other to keep two strands intact [3]. DNA cryptography based on conventional cryptographic consists of key generation, encryption and decryption process. DNA cryptography achieved the higher level of security while sending data over network. The storage capacity of DNA molecules is (1gm= 10^{21} DNA bases) which is equal to (1gm=10^{8}tera bytes). This much amount of data is stored, which is efficient for DNA cryptography to reduce space complexity.

There are few DNA technologies used in DNA cryptography like polymerase chain reaction (PCR), DNA coding, DNA synthesis. Polymerase chain reaction (PCR) technique is used for encoding a message between two primers. It is difficult to encode a message without knowing the correct primers. Plaintext is encoded in binary code, which is combination of 0 and 1and then it is convert into DNA sequence. DNA coding is based on four nucleotides for encrypting binary to DNA sequence such as adenine ‘A’, cytosine ‘C’, thymine ‘T’ and guanine ‘G’ [9]. Combination of these nucleotides stores information present in all living organisms. The cipher text is completely different from plain text, which is not easily detectable by intruders. James Watson discovered the DNA structure [10]. DNA molecules combined of two single strands which form a double helix structure. There are double hydrogen bond present in between adenine (A) and thymine (T) whereas triple hydrogen bond present in cytosine (C) and guanine (G) [11]. A paired with T and C paired with G to form base pairs to create DNA structure. DNA strands have polarity 5 at the top and 3 at the bottom. A single DNA strands forms a double strands DNA using Hybridization. This paper describes an encryption key exchange method to convert large message into DNA sequence, which reduces time complexity.

II. LITERATURE REVIEW

In 2003, Jie Chen [2] proposed DNA cryptographic algorithm on carbon nano-tube and DNA based system. DNA based cryptosystems are used to convert message into segments. One-time-pad is used code book to convert plain text into cipher text. Code book should be random and must be unique. Jie Chen presenting a DNA encryption and decryption images bio-molecular method based on proposed algorithm.

In 2004, Sabari Pramanik1 et al. [3] presented cryptography methodologies using DNA hybridization and DNA digital coding, one time pad, which minimize time complexity. DNA technologies require huge computing time, high computational complexity and extensively laboratory depended. They used parallel technique to decrypt the message in less time.

In 2005, Kazuo Tanaka et al. [5] presented cryptographic algorithm based on public key. This is helpful for encryption and decryption technique. After generating public key message are encoded in DNA sequence. They used immobilization process and PCR amplification to decode the conceded DNA sequence.

In 2006, Sherif T. Amin et al.[6] used symmetric key algorithm in DNA cryptographic approach, where key is estimated in DNA sequences are obtained from genome and stored large DNA sequence in compact space. DNA cryptographic approach has great storing capabilities than other conventional cryptography algorithm. In this Author described symmetric DNA based cipher approach and effectively scalable for large digital information products.

In 2008, Guangzhao Cui et al. [7] proposed the encryption scheme using DNA coding, PCR amplification and DNA synthesis. The PCR amplification two primers pair was used as key and does not design by sender and receiver. This encryption algorithm is used for increase security purpose. Using this method we can get different cipher text, which can prevent from intruder as PCR primers. This encryption scheme shows that high confidential strength.

In 2008, Lai Xin-she et al. [8] explained novel generation key scheme based on DNA cryptographic approach. It uses matrix operation to increase computational speed. They generated key expansion matrix M and generate encryption between two key using XOR operations. In this paper they uses the DNA sequence as a randomized database, reduce the computation and influence of matrix operation to the computed speed.

In 2009, Xing Wang, et al. [11] applied cryptography approach in many field and solve many hard problem. In this paper author applied new technique to work cryptography with DNA computing and RSA algorithm is used to connect with DNA computing to encrypt message efficiently. DNA computing is a method to solve some hard problem and work faster than electronic computer. This paper introduced a new encryption algorithm combine with RSA algorithm. DNA computing and model can't used in laboratory but this method of parallel computing is a new method of computation.

In 2010, Lai, XueJiaet al. [9] proposed DNA sequence as asymmetric encryption and signature method with DNA technology matrix is obtained for encoding the image. Divide the DNA sequence matrix into block and addition operation is performed between block. In this paper original image are scrambled by addition and complement operation, which provides large secret key space and high sensitive to secret key of encryption algorithm. This algorithm resists exhaustive attack, statistical attack and differential attack.

In 2011, Deepak Kumar et al. [10] presented secret data writing using DNA sequence. They focused on DNA computing, DNA sequence, which have large storage capacity, extraordinary information density. Author present encryption and decryption algorithm based on one time pad technique through which one can secure our data in DNA sequence. Steganogaphy is used in this paper to hide message in double strand DNA sequence microdots. Author designed data hiding algorithm by using DNA sequence and traditional cryptography. This algorithm is easy to use and efficient.

In 2012, Yunpeng Zhang et al. [12] proposed DNA cryptographic approach based on DNA digital coding and DNA fragment assembly. They provide high security analysis and prove that the algorithm has high confidential strength. In this paper author design symmetric encryption algorithm using DNA technology.DNA technology has unique advantages than traditional cryptography. It has low energy consumption and high storage capacity.

In 2013, Wang Zhong et al. [13] proposed a new index based symmetric algorithm. This algorithm encrypts plain text using block cipher and index of string. Algorithm converts each character into ascii code and according to the nucleotide sequence convert into DNA sequence. This algorithm stores position as a cipher text. The researchers should prove efficiency and time complexity of this algorithm through simulation and theoretical analysis.

In 2013, TusharMandge et al. [4] proposed DNA cryptographic approach based on matrix manipulation for making data much secure. They used mathematical manipulation and scrambling in cycles to make data non readable. XOR operation is performed with the initial key. The benefit for this proposed algorithm is that it always generates different cipher text for same plain text and key.

In 2014 K. Monika Borda et al. [14] presented DNA secret writing techniques of bio molecular computation and different algorithm for cryptography and steganogaphy. In this paper author used XOR operation, DNA chromosomes indexing for encoding message. Algorithm uses bioinformatics toolbox and not requiring laboratory experiments.

III. DNA STRUCTURE, DNA TECHNOLOGIES, DNA CODING METHOD

A. DNA Structure

Deoxyribonucleic Acid (DNA) sequence consisting of four alphabets: A, C, G and T. It has two base pairs (A, T) and (C, G) a sugar and phosphate group. The combination of two base pairs is formed double helix like structure of DNA containing double hydrogen bond with (A, T) and triple hydrogen bond with (C, G). Watson-Crick base complementary principle (A, T) and (C, G) are complement to each other. The combination of the bases results in purines and pyrimidines. The sequence of these bases stores information of living organisms, which is unique for all living organisms. There are two strands of DNA sequence represent an individual strand as single stranded DNA (ssDNA) and double stranded DNA (dsDNA) [16]. An ssDNA can form double strand DNA (dsDNA) with other ssDNA. SsDNA and dsDNA are complementary with each other. This process is called Hybridization. The two strands DNA molecules are anti parallel to each other.

B. DNA Technologies

DNA cryptography uses different type of technologies to encrypt data through secure channel, as for example- DNA polymerase chain reaction (PCR), bio molecular, one-time-pad. DNA cryptography technology determines the order of four DNA sequence (A, C, T, G). OTP is randomly generated key which is used only one time for encryption and it is to be changed for another time. PCR is a molecular biology technique to amplify several copies of DNA up to order of magnitude of particular DNA.

Table I. Different Types of DNA Technologies

Types of DNA Technologies	Explanation
1. DNA Bio Molecular	• DNA Bio molecular stores genetic instruction as DNA sequence. • DNA Bio molecular structure has three dimensional shapes which are formed by protein, DNA and RNA. • Bio molecular structure decomposed into primary structure, secondary structure, tertiary structure, quaternary structure.
2. OTP (One-Time Pad)	• OTP is randomly generated key which is used only one time for encryption and it is to be changed for another time. • Size of key is greater than or equal to plaintext message. Key should be defined uniquely and kept secret. • One-time-pad technique is difficult to guess the right key to obtain plaintext.
3. DNA Chip Technology	• DNA chip technology is defined independently in biological sample. • DNA chip technology support by the method of micro printing using large number of DNA probes and then hybridization with labeled sample and obtained genetic information. • DNA chip is also known as Gene chips, DNA array and oligonucleotide array.
4. DNA Fragmentations	• DNA fragmentation is essential to library construction for DNA sequence. • DNA fragmentation is used to split of DNA sequence into small pieces.
5. Polymerase chain reaction (PCR)	• Polymerase chain reaction (PCR) is defined as enzymatic replication and DNA fragment. • PCR is a molecular biology technique to amplify several copies of DNA up to order of magnitude of particular DNA. • PCR is used to amplify a specific region of DNA strand.

C. DNA Coding Method

DNA coding method is a procedure for conversion of plain text to ASCII code and subsequent conversion of ASCII code to DNA sequence. There are two methods to encode a plain text.

Plain text is encoded to binary number, which is expressed in 8 bits. For example ASCII code for plain text 'S' is 83, which is further convert into binary number $(83)_2$= 01010011.

Binary plain text 'S'=01010011is converted into DNA sequence using table 2given below.

For example, scanning two left most bits in the binary sequence and further convert to DNA sequence according to table 2. A=00, C=01, G=10, T=11 [15].

Table II. DNA sequence to Binary Conversion

DNA Sequence	Binary
A	00
C	01
G	10
T	11

IV. A New Encryption Key Exchange Algorithm

Proposed algorithm is based on Symmetric Key Exchange and XOR operation technique, which encrypts plain text message into DNA cipher text. To avoid possible attacks on cipher text by intruders modified message are checked at the receiver side. Two parties involved in communication are sender and receiver. Sender encrypts the plain text using symmetric key into DNA sequence and sends through insecure channels like internet.

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

Receiver decrypts the cipher text into plain text using DNA key sequence.

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

A. Key Generation

In this algorithm, Symmetric key exchange technique is used to calculate one time pad (OTP) DNA sequence to facilitate secure communication. Randomly generated OTP DNA sequence is used only once for encryption and decryption process. It gives unique result for a particular statistical calculation. In this paper we used Symmetric key exchange technique to calculate symmetric key k.

Sender 'A' and receiver 'B' agree on two larges prime numbers(g and n).x and y are any two number chosen by sender 'A' and receiver 'B'. A key exchange algorithm is used to calculate symmetric key K.

(a)Calculate A= (g*x) mod n and B= (g*y) mod n.

Sender sends value of A to receiver and receiver sends value of B to sender.

(b) Sender computes secret key K1= (B*x) mod n.

(c) Receiver compute secret key K2= (A*y) mod n.

(d) Finally we get value of K, K=K1= K2.

Value of K is the number of Oligonucleotide present in a DNA sequence. For example if value of K=6 then DNA sequence is ATCGCG consisting of six oligonucleotide. The length of final key is obtained by multiplying numbers of K oligonucleotide in the DNA sequences with length of binary plain text. DNA sequence is obtained from pseudo random generator on the basis of key length.

Take complement of (K) right most nucleotides from DNA sequence and pretend it with 0, 1, 2, 3…..and substitute them with A, C, T, G correspondingly up to end of DNA sequence.(An example illustrate in section 5).

Sender and receiver uses DNA key sequence for encryption and decryption, further it destroyed it. It is impossible for intruder to know about correct sequence.

B. Steps for Encryption

Step 1- Choose the plaintext say 'SE' to be sent and convert it into ASCII code and then to convert binary code.

Step 2- Arrange binary plain text column wise from left to right in a 4*4 matrix say A.

Step 3- Right shift the columns to obtained a mirror image of above matrix, say A'.

Step 4-Convert OTP DNA sequence to its binary form and arrange it column wise in a 4*4 matrix say 'B'.

Step 5- Apply XOR operation between matrices A' and B to get new matrix say AB.

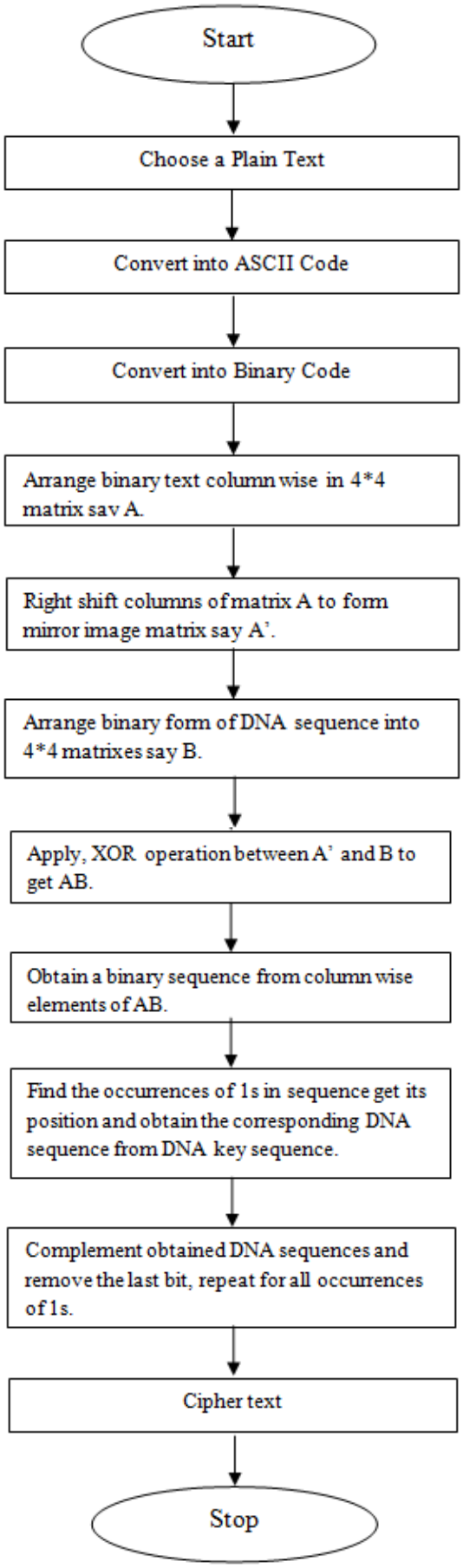
Step 6-Take the column wise matrix elements from AB and put them in a row to obtain a binary sequence.

Step 7-Start scanning the binary sequence from left to right to find the occurrences of 1s. Once a '1' is found, gets its position in the DNA key sequence and get the corresponding DNA sequence from the generated DNA key sequence. Compute this DNA sequence and remove the last bit from it.

Step 8-Repeat step7 for all the occurrences of 1s and put them all together to obtain the final cipher text.

Step 9-Sender sends the ssDNA sequence in the form of packets to the receiver.

C. Flow chart for Encryption technique



D. Steps for Decryption

Decryption Algorithm decrypts the message at receiver side will consists of the following step:

Step 1:-Take leftmost K bits from cipher text, complement it. Find the corresponding sequence from DNA key sequence and attach the position bit.

Step 2:-Repeat step1 for the subsequent k bit sequence in the cipher text till end**.**

Step 3:-Find the position of DNA sequences obtained in step2 in OTP DNA sequence and form a binary sequence by potting 1s for all such occurrences, other positions in binary sequence should be 0.

Step 4-Arrange the obtained binary sequence column wise in 4*4 matrix say AB.

Step 5:-Convert OTP DNA sequences to its binary form and arrange column wise in a 4*4 matrix say B.

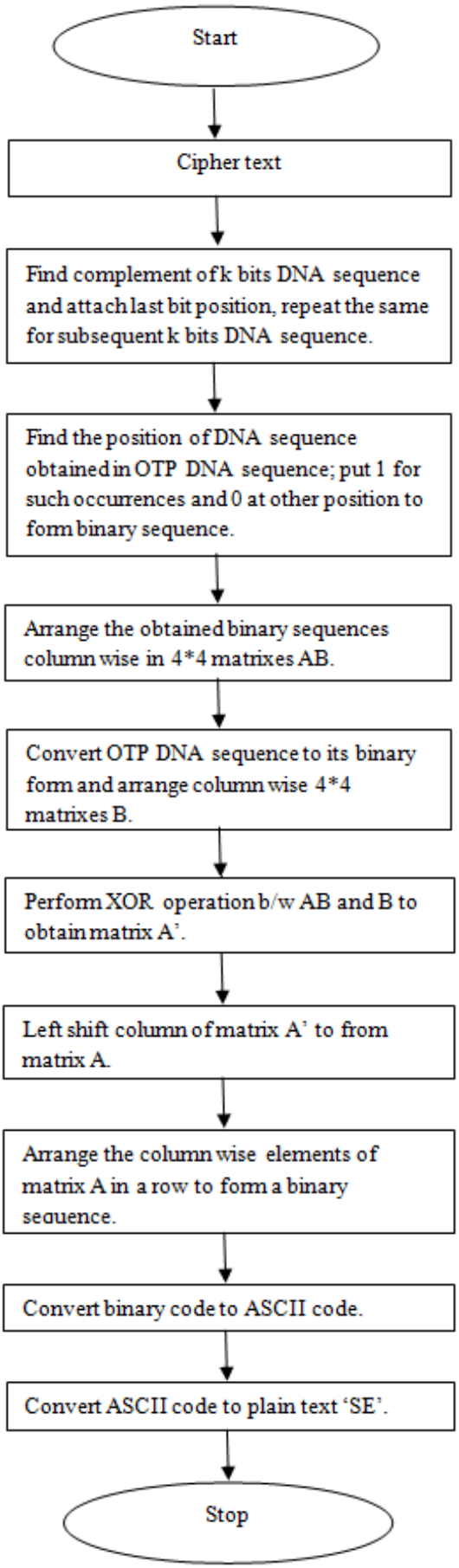
Step 6-Perform XOR operation between AB and B to obtained matrix A'.

Step 7- Left shift, column wise of matrix A' to form matrix A.

Step 8-Arrange the column wise elements of matrix A in a row to form a binary sequence.

Step 9-Convert the binary sequence to ASCII code which in turn will be converted to plain text 'SE'.

E. Flow chart for decryption technique



V. Illustration

A. Key Generation

Let us take plain text (SE) to encrypt and decrypt using our proposed method and convert into ASCII code and subsequent binary code i.e. 01010011 01000101=16 bits.

Now the length of plain text 'SE' is 16 bits. We take prime number g=5, n=11 and sender takes any value x=3 and receiver takes y=4.

(a)Calculate A= (g*x) mod n and B= (g*y) mod n.

A= (5*3) mod 11= 4 and

B= (5*4) mod 11= 9

Sender sends value of A to receiver and receiver sends value of B to sender.

(b) Sender computes secret key K1= (B*x) mod n= (9*3) mod 11=5

(c) Receiver compute secret key K2= (A*y) mod n =(4*4)mod 11=5

(d) Finally we get value of K, K=K1= K2=5.

Now DNA sequence become (16*5) = 80 bits.

OTP generate DNA sequences:
CGTACTAAGGGCGTACCTTTAAAGCATCGGAACCCGTACGGGCGTAATTGGGATTCGGTACGCCA
AATTCGACCGTAGGC

Take complement of 5 right most nucleotides from DNA sequence and pretend it with 0, 1, 2, 3…..and substitute them with A, C, T, G correspondingly up to end of DNA sequence. Ex- ATCCGA CTGGCC TTAAGG GCGGTT GCCATA CCTAAC TTAACG GCGCAT CATGCA TTGGGC TAGCCG TTTCGT GGAAAA CGCATC ATTCCG GCATGT.

B. Encryption

a) Let binary plain text (SE) be -01010011 01000101. Arrange binary plain text column wise in matrix A.

Step 1- Arrange binary plain text column wise in 4*4 Matrix say A.

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

Step 2- - Right shift the columns to obtained a mirror image of above matrix, say A'.

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

Step 3 – Convert OTP DNA sequence to its binary form and arrange it column wise in a 4*4 matrix say B. Ex- OTP DNA sequence is CGATTAAG and its binary number is 0110001111000010.

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

Step 4- Apply XOR operation between matrices A' and B to get new matrix say AB.

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

b) Arrange elements of matrix in a row, result will be (0011011111110111). Start scanning the binary sequence from left to right to find the occurrences of 1s. Once a '1' is found, gets its position in the DNA key sequence and get the corresponding DNA sequence from the generated DNA key sequence. Compute this DNA sequence and remove the last bit from it.

c) SsDNAsequences-
TTAAGGGCGGTTCCTAACTTAACGCCGCTCATGCATTGGGCTAGCCGTTTCGTCGCATC
ATTCCG GCATGT. Find its complement and replace last attached DNA sequence. Final result will be AATTCCGCCAGGATTAATTG GGCGTGTACGAACCCATCGGAAAGC GCGTA TAAGG CGTAC. This is our cipher text.

C. Decryption

a) Once received cipher text DNA sequence i.e AATTC CGCCA GGATT AATTG GGCGT GTACG AACCC ATCGG AAAGC GCGTA TAAGG CGTAC. Take left most 5 bits from cipher text, complement it. Find the corresponding sequence from DNA key sequence and attach the position bit. Result will be TTAAGG GCGGTT CCTAAC TTAACG CCGCT CATGCA TTGGGC TAGCCG TTTCGT CGCATC ATTCCG GCATGT.

b) Find the position of DNA sequences obtained in step I in OTP DNA sequence and form a binary sequence by putting 1s for all such occurrences, other positions in binary sequence should be 0.
Result will be (0011011111110111).

Step 1- Arrange the obtained binary sequence column wise in 4*4 matrix say AB.

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

Step 2- Convert OTP DNA sequences CGATTAAG to its binary form is 0110001111000010 and arrange column wise in a 4*4 matrix say B.

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

Step 3- Perform XOR operation between AB and B to obtained matrix say A'.

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

Step 4- Left shift column wise of matrix A' to form matrix say A.

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

c) Arrange the column wise elements of matrix A in a row to form a binary sequence, which is (01010011 01000101) and obtained desire plain text SE.

VI. Pseudo Code

A. Key Generation

```
1) begin
2) Select two large prime number g and n, also x and y are any two numbers chosen by sender and receiver, respectively
3) A← (g*x) mod n  //sender computes A
4) B← (g*y) mod n   //receiver computes B
5) A and B are exchanged between sender and receiver
6) K1← (A*x) mod n  //sender computes K1
7) K2← (B*y) mod n  //receiver computes K2
8) K=K1=K2
9) Kdna←(K * Length of binary plain text(M))
10) Random_DNA← (char choice[i], char temp, char choice[j])
11)      for i:= 0 to 4 step 1 do
12)           for  j:= 0 to 4 step 1 do
13) Print(temp, choice[i],choice[j]);
14)           end for
15)      end for
16) strcpy(base(k),temp)
17)      for  i:=0 to n step 1 do
18) Print(base[i])
19) end for
20) seqk end left← end right
21) position ←position+1
22) concate(DNA to position)
23) end
```

B. Encryption

```
1)  Begin
2)  Select a plain text 'SE'
3)  DNA_binary(int result, i, r,n)
4)    while(n>0) do
5)  r ← n%2
6)  result← result+(i*r)
7)  n← n/2
8)   end while
9)     i← i*10
10) Generate4*4 matrix
11)    Right-Shift the columns of matrix
12) binary_xor(inti,char string[8], char string1[8])
13)     for i:=0 to 8 step 1 do
14) string[i]← string[i]^string1[i]
15) print string[i]
16)      end for
17) cd←output({'00','01','10','11'},{'A','C','G','T'})
18) end
```

C. Decryption

```
1)  Begin
2)  dna_number(string s)
3)  num=0
4)      for n:=0 to s step 1 do
5)  end for
6)      if (s[n]='A') then
7)  num+=0
8)  end if
9)      if(s[n]='C') then
10) num+=1
11) end if
12)     if(s[n] ='G')
13) num+=2
14) end if
15)     if(s[n] ='T') then
16) num+=3
17) end if
18) print d_num("TAGGC")
19) bitxor(int x ,int y)
20) btodecimal(intbno, dno=0, j=1, r)
21)     while(bno!=0) do
22) r ← bno%10
23) dno←dno + r *j
24)  j ←j*2
25) bn←bn/10
26) end while
27) Return num
```

Table III. Time complexity comparisons of existing algorithm

Algorithm	**Plain text**	**Cipher text**	**Demerits**	**Time complexity for Encryption**	**Time complexity for Decryption**
Secret data writing using DNA sequence	Hello	350 bits DNA sequence	Size of key and cipher text is large, It increases time complexity	**O(n)**	**O(n)**
An encryption scheme using DNA technology	DNA	210 bits DNA sequence	Message sends packet takes more time.	**O(n)**	**O(n)**
A DNA encryption technique based on matrix manipulation and secure key generation scheme	DNA	128 bits DNA sequence	Two part of encryption mechanism is performed	**O(n)**	**O(n)**
Symmetric Key Exchange Based on DNA Cryptography	**1.SE** **2.Hello** **3.DNA**	**80 bits DNA sequence** **200 bits** **120 bits DNA sequence**	Two part of key generation scheme is performed.	**O(n)**	**O(n)**

D. Encryption Time

a) Plain text to ASCII code- O (n).
b) ASCII code to Binary code- O (logn).
c) Substitute of Binary code- O (n).
d) Binary to XOR operation- O (n).
e) Scanning of binary code with DNA sequence- O (n).
f) Encryption DNA sequence- O (n).

Total time complexity for encryption T (n) = O (n).

E. Decryption Time

a) Decryption of DNA cipher text to binary code- O (n).
b) Binary to XOR operation - O (n).
c) Substitute of Binary code- O (n).
d) Binary code to ASCII code- O (log n).
e) ASCII code to desired Plain text- O (n).

Total time complexity for encryption T (n) = O (n).

VII. Conclusion & Future Scope

We implemented a new DNA encryption scheme based on symmetric key exchange, matrix operation and XOR technique. Any message is converted in DNA sequence. DNA sequence stored large message in compact volume. In this paper, a new cryptography technique is proposed using Symmetric Key Exchange, one-time pad scheme and DNA hybridization to minimize the time complexity. Matrix form operations reduce time complexity of encryption and decryption. DNA cryptography can be combined with traditional cryptography to provide hybrid security. So there is a lot of scope for future works in this area. Different traditional cryptography techniques combined with DNA cryptography may lead to better hybridization. The use of higher dimension matrices for encryption and decryption can further minimize the time complexity and hence can be considered as future scope of this work.

References

[1] L. M. Ad leman, "Molecular computation of solution to combinatorial problems Science, (1994) 11, (266): 1021-1024
[2] Chen Jie, “A DNA-based bio molecular cryptography design,” Proceedings of IEEE International Symposium, Vol. 3, pp. III-822, (2003).
[3] Borda, Monica, and Olga Tornea, "DNA secret writing Techniques," In Communications (COMM), 8th IEEE International Conference on, pp. 451-456, (2010).
[4] TusharMandge, Vijay Choudhary. “A DNA encryption technique based on matrix manipulation and secure key generation scheme”. Information Communication and Embedded Systems (ICICES), International Conference on 21-22 Feb. (2013).
[5] Kazuo Tanaka, Akimitsu Okamoto, and Isao Saito, “Public-key system using DNA as a one-way function for distribution”.Bios stems 81, 1, pp. 25-29, (2005).
[6] Sherif T. Amin, MagdySaeb and El-Gindi Salah, “A DNA-based implementation of YAEA encryption algorithm,” In Computational Intelligence, pp. 120-125, (2006).
[7] Cui, Guangzhao, Liming 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).
[8] Lai Xin-she, Zhang Lei, “A novel generation key scheme based on DNA”. Computational Intelligence and security, IEEE, International conference on 13-17 Dec. (2008).
[9] Lai, XueJia, "Asymmetric encryption and signature method with DNA technology," Science China Information Sciences 53.3, page 506-514, (2010).
[10] 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).
[11] Xing Wang,QiangZhang“DNA computing-based cryptography”. Key Laboratory of Advanced Design and 1ntelligent Compuling (Dalian university), Ministry of education, Dalian, 116622, China IEEE in 2009.
[12] 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).
[13] Wang Zhong, Zhy Yu, “Index-based symmetric DNA encryption algorithm”. Image and Signal Processing (CISP), 2011 4th International congress on image and signal processing, 15-17 oct.(2011).
[14] Olga Tornea, and Monica E. Borda, "Security and complexity of a DNA-based cipher," IEEE Roedunet International Conference (RoEduNet), 11th, pp. 1-5, (2013).
[15] Borda, Monica, and Olga Tornea, "DNA secret writing Techniques," In Communications (COMM), 8th IEEE International Conference on, pp. 451-456, (2010).
[16] Tausif Anwar, Sanchita Paul and Shailendra Kumar Singh “Message Transmission Based on DNA Cryptography: Review” in International Journal of Bio-Science and Bio-Technology. Vol 6, No.5, Issue 30, October 2014, pages 215-222.

Authors

Tausif Anwar[1] obtained his B.Tech degree in Computer Science and Engineering from Bhadrak Institute of Engineering & Technology, Odisha in 2010. He completed Master of Engineering in Software Engineering from Birla Institute Of Technology, Mesra, Ranchi (India). He has 2 years of industry experience as a software developer.

Abhishek Kumar[2] is pursuing his M.E in Software Engineering from Birla Institute of Technology, Mesra, Ranchi, India .He has B.E. degree in Information Science & Engineering from C.M.R.I.T Bangalore, India. His research areas include Internet of Things, Cloud computing, Internet Security. He has also 3 years (approx.) of industry experience as software developer in web based projects.

Dr.Sanchita Paul[3] is an Assistant Professor in Department of Computer Science & Engineering, Birla Institute of Technology, Mesra, Ranchi (India). She obtained B.E, M.E and Ph.D Degree in Computer Science and Engineering. Her area of Interests is Artificial Intelligence, Cloud Computing, Bioinformatics, NLP, Automata Theory, Design and Analysis of Algorithms.