IJCTA, 9(33), 2016, pp. 49-59
© International Science Press

Encryption Algorithm Based On DNA Strand Technology

Prashanth Mogali* and Neha Kaura**

Abstract : We live in a world where large corporations and small companies are flooding the market place with their products for a varied consumer base. Also digitization is a revolution fast catching up with even the most common government offices which hold records. The highlight of the two trends mentioned above is that both are increasing the amount of data present online. Since the nature of this data is sensitive, its security is paramount. Hence, adoption of multiple data encryption algorithms to make sure the confidentiality and integrity of the data is not compromised. Among the plethora of methods include techniques like hashing, usage of public or private keys and upcoming areas of research like DNA and quantum cryptography. Except for the one-time pad, there is no other known unbreakable method but can only be classified as stronger than another that is tougher to break into by the attacker. This paper attempts to propose another encryption algorithm influenced by DNA cryptography which makes use of the advantages of a one-time pad, merging it with the use of a private keys as used in symmetric encryption to offer stronger security to data through encryption.

Keywords : DNA cryptography, DNA.

1. INTRODUCTION

Data security is the practice of protecting data from corruption or unauthorized access. Every organization practices some form of cryptography. The process of securing information is Cryptography. Cryptography has come a long way from what it was in the time of Julius Caesar. As internet widely spread throughout the world so did the need for securing the data available online. Researchers began developing algorithms to create unbreakable security; hence advancement of cryptography was inevitable. Based on the encryption and decryption process, cryptography is symmetric or asymmetric. Symmetric key algorithms use the same key for encryption and decryption, where it's quite the contrary in asymmetric algorithms / public key cryptography which use separate keys for both encryption and decryption. The oldest type of cryptography is the traditional cryptography. For current technologies these methods of cryptography are not strong enough to offer the data security effectively [1,2].

The above mentioned methods fall into the set of techniques grouped under traditional cryptography. These methods though undeniably popular for practical uses are still breakable at different extents of force applied by an attacker. Hence researchers have started looking in other directions to offer a secure environment for data transfer. Some of the avenues which have shown hopes of feasibility are quantum cryptography and DNA cryptography. Quantum cryptography is still far from the execution phase[3,4]where a live demonstration of the DNA model by Adleman[5]sprouted different algorithms and expanded the computational capabilities in the laboratory environment.

* Dept. of Information Technology SRM University Chennai, India Chennai, India, m.prashanth54@gmail.com.

** Dept. of Computer Science & Engg. SRM Universitynehakaura243@gmail.com.

DNA encryption involves encrypting of data in a DNA strand form to simulate arithmetic and logical operations[6]. The key elements of DNA based cryptography are namely DNA computing, sequencing, gel electrophoresis, hybridization and PCR (Polymerase Chain Reaction). Deoxyribonucleic Acid (DNA) is a self-replicating material which performs calculations many times quicker than any other computer existing in the world. The complex structure of the living body consists of human parts which are the result of applying simple operations to the first information encoded in a DNA sequence called genes. Likewise, the complicated mathematical operation are combinations of simple addition and subtraction.

DNA exists as double-stranded molecules, the two complementary DNA strands are held together to form a double helix structure by hydrogen bonds containing four bases, Adenine (A), Thiamine (T), Guanine (G) and Cytosine(C). According to Watson Crick[7] complement condition, in a double helix DNA, the oligonucleotides or DNA strands with the four bases bind together A is double bonded with T, C is triple bonded with G. The process of computing DNA sequences is DNA computing. Since DNA exhibits vast parallelism and addition properties[8], it could act as a microprocessor which could replace the silicon processors in the future. DNA and RNA are enticing media to store data which exceeds the storage capacity of electronic, physical and optical media.

Most of the encryption methods use the sequencing property and secretly select a publicly available sequence (S) as its reference[9]which is known only by its sender and receiver. The sequence undergoes a transformation into another sequence by addition of extra information and the encoded message (M). This newly transformed sequence is the cipher text sent to the receiver along with several other sequences.

Most of the methods follow the convention of representing the bases into bits. Taking the values as follows:

A – 00, C – 01, G – 10 and T – 11

S-DNA = AAGCTTACAGACTCCAGGTATGGACTTCAAGT .

S-DNA = 0000100111110001001000011101010010101100111010000111110111110100001011.

2. PROPOSED ALGORITHM

In this paper the authors attempt to propose a new encryption algorithm which uses the One Time Pad and the Huffman Encoding to enhance its security.

Also known as the Vernam Cipher, one-time pad is the only unbreakable algorithm present for encryption till date. For usage, plaintext encryption done using a key which is random in nature[10]. The algorithm's requirement is that 1) the sequence is random; 2) Sequence once used cannot be reused hence the name one-time pad. This algorithm is unbreakable till date.

Huffman Encoding is a technique used for compression of data in a way such that no loss of data occurs. Characterization is by an ideal prefix code found using the Huffman coding algorithm as developed by David A. Huffman.[11]

An understanding of the One Time Pad and Huffman Encoding is vital for this proposed algorithm. In the first step, the available plaintext undergoes a compression using the Huffman Technique. After compression the new compressed text is represented in the form of blocks. After which a certain encryption key along with a pre-generated OTP performs the rotation and encryption on the data. The type of rotation is dependent on the OTP bits. Thus the data in the matrix can experience square rotation, double square rotation, 90-degree rotation, etc. Hence, plaintext transforms to cipher text. The next step is conversion to DNA sequence representation i.e. a sequence of letters representing double bonded nuclear base pairs AG and CT.

The encrypted data is then transferred to the receiver through any means seen comfortable by both the parties. Once the receiver obtains the data, decryption follows for his/her understanding of the data. Decryption of the proposed algorithm follows steps similar to those followed in encryption but in a reverse way. The receiver uses the private key in his possession (same as the one used by the sender) to do

rotations on the key and finally get it back to the binary representation. After getting the binary form, decompression back to the original data using Huffman decompression. Thus cipher text transforms to plaintext.

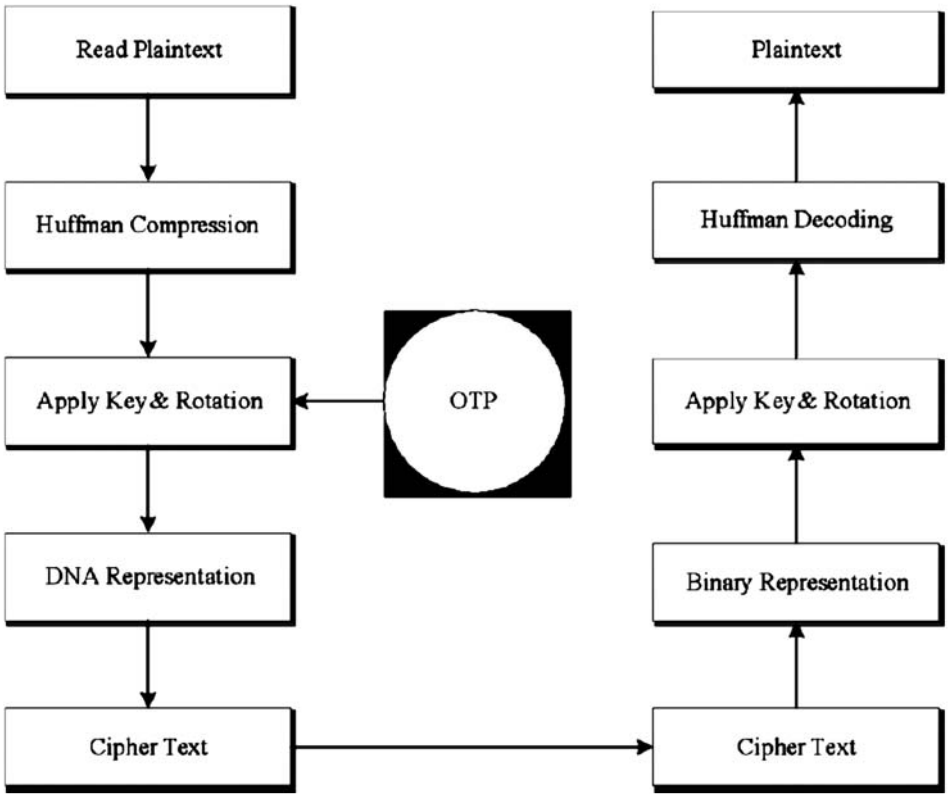

Figure 1: Various operations to be applied on the plaintext to get the cipher text and vice-versa

The encryption process is explained in a more detailed manner in section IV of the paper.

3. DNA CRYPTOGRAPHY : A LITERATURE SURVEY

As mentioned above efforts made to make a method to put the qualities of DNA to a practical use in the area of data encryption. A concise mention of many of the suggested techniques till date are found below:

A. Yet Another Encryption Algorithm (YAEA)[12]

This technique suggested by M.Saeb and A.Baith performs data encryption through a symmetric approach to DNA cryptography. The plaintext transformation is by keeping in mind that every four DNA nucleotide sequences represent a binary octet. A sequential search technique used to find and return position of the binary octets. The security based on several possible assumptions such as there is no potential interceptor to distinguish between the dummies and the message strand and that each possible key has the same probability of occurrence which does not mean each sequence inevitably occurs.

B. DNA cryptography using One Time Pad[13]

Prof. Gehani, T.LaBean and J.Reif formalized two designs for encryption based on one time pads in a DNA. In the first method he suggested to translate the fixed length DNA plain code sequence cell to a DNA sequence according to a defined mapping graph, calling it the mapping substitute. The other is the exclusive OR technique involving DNA computing to perform the exclusive operations on the plain code to the cipher code. Even though this method is absolutely secure it's very critical to settle down the encryption mapping graph or cipher key carrier (called DNA material) between the two communicators properly and ensure this material can't be altered or replicated.

C. DNA based bimolecular design[14]

In this method Jie Chen Proposed a DNA based cryptosystem using Carbon Nano Tubes (CNT) to alter the messages at an atomic scale. DNA chips have microscopic arrays of immobilized strands of DNA from which grouping of multiple copies of a single sequence and DNA synthesis performs in parallel. The Y-shaped CNTs produced by CVD growth in branched Nano-channel alumina templates[15]. The Y-shaped tube has proven promising as it can act both as a connection and an active device.

D. Cryptography with DNA binary strands[16]

This method suggested by Leier, Richter, Banzhaf and Rauhe discusses about graphical subtraction of binary gel images. It is a steganography approach to encipher and decipher data. Steganography means hiding of secret messages among other information to conceal their existence[17,18]. The DNA strand contains primers which are essential and there are no other ways of reading them. The message strand corresponding to the binary encoded plaintext mixed with other strands called dummy strands in equimolar proportions to prevent reading the strand by sequencing. Along with this a unique identification key sequence is also attached to the message strand. This could be any of the terminator sequences or the start sequences.

E. Public Key System using DNA as a one way function for key distribution[19]

This encryption algorithm suggested by the authors uses an asymmetric approach inspired by[20]. The method provides easy evaluation in the forward direction but impracticable in reverse direction. Restoration of the message encoded in the DNA dummies is by PCR amplification followed by sequencing[21]. These operations are a one way function to hide the message but are impossible to extract the encoded message without knowing the right primer sequence. This method ensures that only the possessor of the public key will be able to decode the message.

F. An Encryption Scheme Using DNA Technology[22]

The approach provides a safe way to transfer data between two people using RSA as pre-processes to the plaintext. Supposing Alice and Bob have encryption key K_A and decryption key K_B. Alice uses her key to transform the plaintext into a cipher text C. Bob can decrypt that cipher text using his key. Assume

$$\text{Message} = M, \text{Cipher text} = C.$$

$$C = Ek\alpha\,(M) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad {}^{22}$$

$$DKb\,(C) = DKb\,(EK\alpha\,(M)) = M \quad \ldots\ldots\ldots\ldots \quad {}^{22}$$

E_{KA} is a pre-process of any of the traditional cryptography approaches, but this method focuses on RSA. After which C converts to a DNA sequence form using the coding convention. Finally, the DNA sequence is inserted between dummies which are of 60 – 160 oligonucleotides of sonicated human DNA and denaturing it. This DNA mixture is received by the receiver in an open channel.

G. DNA Encryption Using Tiles[23]

O. Tornea and M.E Borda have utilized XOR OTP, RSA and public key encryption in their method. DNA tiles are created synthetically by taking individual oligonucleotides chains which hybridize in one helix and cross over and hybridize in another. To hide the message the author chooses the technique used in [24]. To decrypt, the receiver needs to have knowledge of the OTP, primers and the medium containing the message.

H. DNA indexing using Chromosomes [25,26]

The author suggests generation of an OTP using the large size of a DNA chromosome which is selected from a public database for every session. The equivalent binary value of the OTP is converted into the form of bases and then analyzed. For every 4 – letter sequence, it's indexed from the chromosomal sequence and stored in an index array. A random number is selected from the array which is the encrypted character. This makes the cipher text an array of random indexes.

I. Data hiding methods based upon DNA sequences [27]

In this method the author suggests three techniques for data hiding namely insertion method, substitution method and complementary pair method. In insertion the author takes a reference sequence S and a message M = 01001100. S is given as ACGGTTCCAATGC. As the name suggests extra bits are added to the message to form the cipher text, by doing so security is enhanced. In complementary pair method a pair of bases is combined (AC) (CG) (GT) (TA) and a counter part is assigned to each one. The author has used a string of "AATGC" so the complementary will be "CCATG". The substitution method uses a complementary rule such that for all x, C(x), C(C(x)) and C(C(C(x))) are not equal, where C(x) represents the compliment of x. This is to ensure that the complementary rule follows injective mapping.

J. Indexed based symmetric DNA [28]

Here, the authors have given importance to block cipher and index of string. This method follows a symmetric approach towards encrypting and decrypting with a key generator based on logistic mapping initialized by x_0 and μ. The key space in this method is found to be very large minimizing the chances of a successful attack. Key can be divided into two parts, the first part of the key is selected from the GenBank[29],the other part of the key is used to control the key generator to create a chaos sequence.

K. Using DNA microdots to hide messages[30]

The author has used a steganography approach in hiding information in microdots. A microdot is a compressed form of a photograph pasted over a full stop[31]. The author developed a doubly based steganography approach where the encoded message is initially camouflaged within numerous and enormous complexity of the human DNA. Then the sample is concealed within a microdot. The author uses a simple substitution cipher for encryption. The recipient is to know about the secret message DNA PCR sequence and the encryption key in order to decode.

L. Using DNA hybridization for secret writing[32]

The author uses OTP's as a single strand DNA (ssDNA) for the encryption process. The length of the OTP is decided by the size of the message. The author follows Viviana Risca's idea to hide the message. Scan the sequence in reverse taking 10 bases at one. The hybridized segments represent binary ones and the unchanged are zeroes. The encrypted message is given by the set of segments that are complementary to the ssDNA. Using microdot steganography approach, it's extremely difficult to identify the encoded message[33]. Only by knowing the correct primer sequences it is possible.

M. Encrypting Information using DNA Computing[34]

The author in[34] uses bimolecular finite automata for the ciphering purposes and solve a hard problem[35,36]. A new kind of a restriction nuclease was used as the hardware to control it. This concept of bimolecular finite automata was developed from that proposed by Bennet in 1972[37]. Assume an input molecular aaT. After certain transitions the sticky end CTGG matches none of the existing transition molecular in the solution, forcing it to halt then the string "aa" is the summation of the finite automata. The mechanism of the finite automata is certain but the sequence of states and symbols needn't be, hence if there are N states and M symbols the bio molecular automata will have $M \times N \times N$ transition molecules.

N. Secure Communication Protocol[38]

A DNA primer is a short DNA sequence used to recognize genes) used as keys by the author to send messages. The two parties involved may be the sender and the receiver. Suppose both the sender and the receiver are in possession of a common codebook that contains a collection of DNA sequences all of which can code a unique predefined message each. The sender transfers the primers to the receiver who then anneals it a sequence to get the message.

O. Data Hiding [39]

The author attempts to make the data available in the cloud environment more secure. For this, DNA sequences and the complementary base rules have been applied. The original data is essentially hidden using a DNA sequence and pair rules. The same DNA sequence can be used to get the original data back.

P. DNA Cryptography based on DNA Fragmentation Assembly[40]

The authors have used the concept of DNA fragmentation and assembly. Here a long chain DNA sequence is broken into fragments and then they are incorporated with the original long chain of DNA. This strategy of fragmenting the sequence and recombining back into the original chain after overlap removal I called Shotgun sequencing.

Q. Message Encoding Scheme for Small Text Files[41]

In this method the author proposes an algorithm for small text files where the encoding process is coupled with other processes like message transformation and message compression. This method can be used to store data which is needed for a long term in fields like military, biological hereditary research etc.

R. Data Hiding using DNA Coding[42]

Most of the conventional methods in cryptography almost always transfer the entire key directly through some channel, hence risking the safety of the encryption. He Has suggested a novel algorithm which does not send the entire key but share session keys. Session keys contain information about the actual keys.

4. DETAILED ALGORITHM

The algorithm described by the authors in this paper has two striking features. The first being that the key required for encryption is taken in the form of a matrix. This allows for more complex operations to be performed on it as opposed to a sequence. Secondly, the key changes multiple times during the course of encryption due to different types of rotation performed on it based on an OTP in the form of an DNA sequence. The type of rotation for each corresponding base is given in Table 1.

Table 1

The rotations to be applied for each particular DNA character encountered

DNA Character	*Binary Equivalent*	*Type of Rotation*
A	00	Square Rotation
T	01	Rotate 90
C	10	Rotate 180
G	11	Square Rotation × 2 × 2

A detailed description of the algorithm is provided below

Suppose Alice needs to send Bob an encrypted text using a key (KEY) known to both of them. Let the data be represented by M. The steps followed by Alice for encryption and Bob for decryption are

Step 1 : Generate a random OTP from the EBI database[43]. Let it be represented by the variable **OTP.** The OTP is basically a sequence of DNA bases and represent the different rotations that need to be performed on the key.

Step 2 : Encode the given plaintext M using Huffman to get the compressed binary form M'.

Step 3 : Convert the key into the string form taking row wise from matrix (key).

Step 4 : Split M' into several smaller chunks of lengths equal or lesser than key

$$\text{Lenght (M'[}i\text{])} = \text{Length(M) / Length (key)}$$

Step 5 : Generate random junk values equivalent to the length of the key in binary and prepend it to M'. This is done to provide security against brute force attacks by using junk to dilute the contents of the message.

Step 6 : Iterate over M' to find the count of 1 say "C" in every chunk and perform the below operation. Let OTP sequence be iterated with o

$$M'[i+1] = M'[i+1][:C\% \text{ length}(M'[i+1])] + OTP[o] + M'[i+1][C\% \text{ length}(M'[i+1]):]$$

$$o = o + 1$$

If OTP [o] = = OTP[last]:

$$o = 0$$

Here, the main action performed is the process of counting the number of 1's in the previous block to get the bit location where the data must be stored and extracted in to the next block.

Step 7: Iterate over M' and perform the below operations

If i = = 0:

$$C = M'[i].\text{ count ("1")}$$

Perform XOR between M'[i] and key

Else : $Rot = M'[i][C\% (\text{length}(M'[i+1]) - 2): C\% (\text{length}(M'[i+1]) - 2) + 2]$

Perform XOR between M'[i] and key

Apply Rotation to the key based on Rot from the table

$$C = M'[i].\text{ count ("1")}$$

Here, we authors have elaborated two cases namely when we consider the first two blocks and operation for the rest of the blocks. The first block requires no rotation on the key but before encrypting the location on the OTP sequence on the next block is identified. The next block will also not require any rotation but this time the location of the next sequence as well the rotation for the key is extracted. The subsequent blocks will undergo rotations in the key by extracting the OTP bit in its previous blocks.

Step 8 : Convert M' to its DNA sequence (M'') and send the data.

Step 9 : Generate another random OTP sequence and repeat the process to encrypt the Huffman decoding table and send the data.

5. DECRYPTION

Decryption essentially being the reverse process of encryption perform the following operation taking M' as the ciphertext and convert into binary form and split the data.Iterate over M' and perform the below operations :

If = = 0 :

Perform XOR between M'[i] and key

$$C = M'[i].\text{ count ("1")}$$

Else :

Perform XOR between M'[i] and key

$$Rot = M'[i][C\% (\text{length}(M'[i+1]) - 2): C\% (\text{length}(M'[i+1]) - 2) + 2]$$

Apply Rotation to the key based on Rot from the table

$$C = M'[i].\text{ count ("1")}$$

After iteration slice out the first chunk of data and the resultant is the plaintext. Perform the same for the second file of Huffman decoding table and decode the data.

Working Example

Given PT : Wish you a many returns of the day Bob !

Given Key : 1 2 3 00110001 00110010 00110011

4 5 6 00110100 00110101 00110110

7 8 9 00110111 00111000 00111001

The above key can be collectively viewed as :

Key : "00110001 00110010 00110011 00110100 00110101 00110110 00110111 00111000 00111001"

OTP : "atacaacggtatctccacct"

Random Junk Data: '01100010 00100111 01011100 01111000 01100110 00110001 01011100 01111000 01100110'

Splitting plaintext into smaller chunks : ['01100010 00100111 01011100 01111000 01100110 00110001 01011100 01111000 01100110', '01100 00100 0100 11100 10 1101 011001 11111 10 1100 10 01101 1100 0101 1101 10 1', '1110 0001 0011 11111 11110 0101 010010 10 0111 00101 10 0011 11100 0001 10 11101', '1 1100 1101 10 111010 0111 00000 10 0000001 ']

Table 2

Huffman Decoding Table for retrieving the plaintext

Chars	***Huffman***
"	10
'!'	00001
'B'	111010
'W'	01100
'*a*'	1100
'*b*'	00000
'*d*'	111011
'*e*'	0001
'*f*'	00101
'*h*'	11100
'*i*'	00100
'*m*'	01101
'*n*'	0101
'*o*'	0111
'*r*'	11110
'*s*'	0100
'*t*'	0011
'*u*'	11111
'*y*'	1101

Ciphertext :

AAAAAAATAAAAAAATAAAAAAAAAAATAAATAAAAAAAAAAAAAAAAAAT
AAAAAATAAAAAAATAAAAAAAAAAATAAATAAAAAAATAAATAAATAAAT
AAAAAAAAAATAAAAAAAAAATAAATAAAAAAAAAAAAAAAAATAAAAAAT
AAAAAAAAAATAAATAAAAAAAAAAAAAAAAAAAAAAAAAATAAATAAAT
AAAAAAAAAATAAATAAAAAAATAAAAAAATAAATAAAAAAAAAATAAAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAATAAAAAAATAAATAAATAAATAA
ATAAAAAAATAAAAAAATAAAAATAAAAAAAAAATATATAAAAAAAAAATATAAAT
AAATAAAAAAATATAAATATAAATAAATAAATAAATATAAAAATAAATATATATAT
AAATAAAAAAAAATATAAAAAAAAAAAATAAAAATAAAAATATAAAAAAAAAAAAT
AAAAAAATATATATATAAAAATAAAAAAAAAAAAAAAAAAATATATAAATAT
AAATAAAAAAAAAAAAAAAAAAAAAATATAAAAATATAAAAAAAAAATATAAAT
AAAAAAAAAAATATAAATATAAATAAAAAAAAATATAAAAAAAAATAAAAAAAAT
AAATAAAAAAATATAAAAATAAAAAAAAATATATAAAAAAAAATAAAAAAATAT
AAAAATAAAAATATAAATAAATATATAAAAAAATAAATAAAAAAAAAAAAAAAAAT
AAATAAAAATAAAAATAAAAAAATATAAAAATAAAAATATAAAAAAAAATAT
AAAAAAAAATATAAATATAAAAAATAAATAAATAAAAAAAAAAATATATAT
AAAAATAAAAATAAATAAAAAAATATAAAAATATATAAATAAAAAAATATAT
AAATAAAAAAAAAAAAAAAAAAAAATAAAAATATAAAAATAAAAAAAT
AAATAAATATAAAAAAAAAAAAATAAAAATAAAAATATATAAAAAAATATAT
AAAAAAAATATAAAAAAAAATATAAAAAAATAAATATATAAAAAAAAAAATAAAT
AAAAAAAAAAAAAATAAATAAATATAAAAATAAATAAAAAAAAAAAAAATAAAT
AAAAAAATAAATATAT

Table 3

Performance and runtime according to different file sizes

S.No.	*File Size*	*Binary File Size*	*Key Matrix*	*Time to Encrypt plain text (sec)*
1.	68 kb	377 kb	4 × 4	4.62120795249939
2.	5 kb	28 kb	4 × 4	0.33630251884460
3.	2 kb	6 kb	4 × 4	0.06701827049255

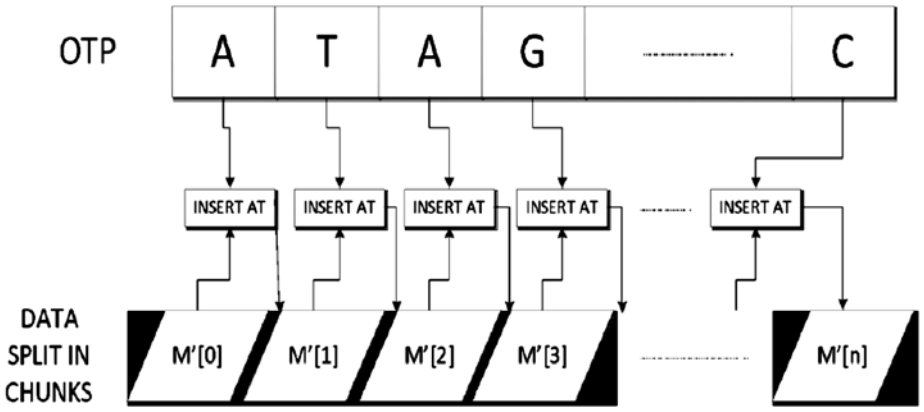

Figure 2: Data Pre-treatment with OTP

6. CONCLUSION

In this paper the authors have suggested a novel algorithm for data encryption using DNA cryptography. Also the list of existing methods that incorporates DNA technology for data security has been compiled and elaborated. Although much research has been done in the field of DNA cryptography it is apparent that it still remains a relatively new area of research. However, the literature shows that DNA cryptography is inter dependent on research of DNA computing. Current scenario is such that the cost of securing the data is higher than the data itself. With advanced research in the near future DNA technology shows promise of reducing complexity for encryption and providing robust security all the while bridging the gap between feasibility and security.

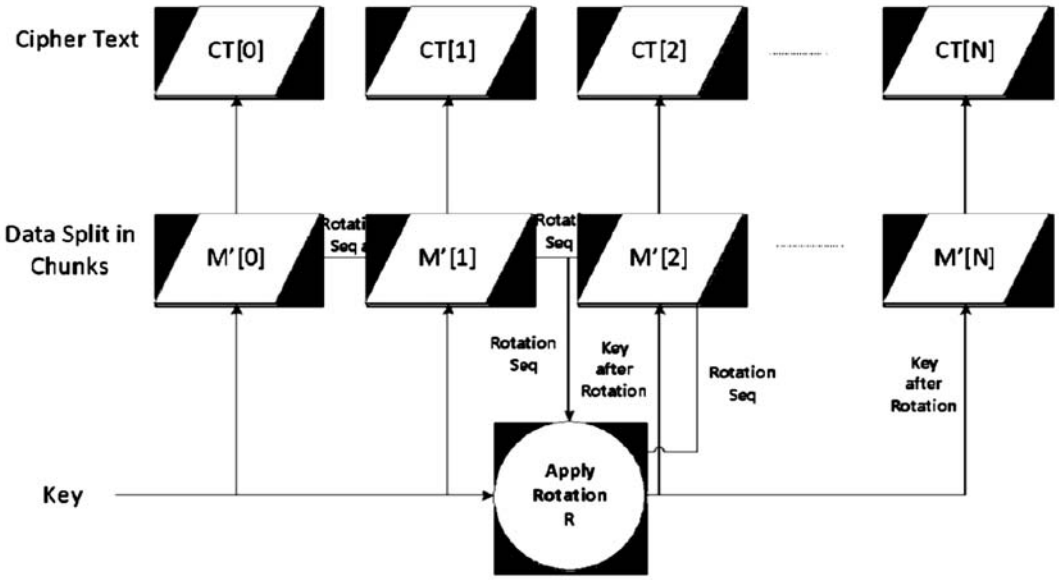

Fig. 3. Data Flow in the Encryption Process.

7. ACKNOWLEDGMENT

The authors would like to thank Dr. Harish Ramani for his contribution and support towards the completion of this paper. His advice has been highly beneficial for the authors in their attempts at research in the field of Cryptography and Security.

8. REFERENCES

1. G. Cui, L. Qin, Y. Wang, and X. Zhang. Information security technology based on dna computing. In Proceedings of the 2007 IEECui G, Qin L, Wang Y, Zhang X (2007) Information Security Technology Based on DNA Computing. 2007 International Workshop on Anti-Counterfeiting, Security and Identification (ASID). doi: 10.1109/iwasid.2007.373746
2. A. Gehani, T. LaBean, and J. Reif. Dna-based cryptography. DIMACS Series in Discrete Mathematics and Theoritical Computer Science, 54:233–249, 2000.
3. Hemmer PWrachtrup J (2009) Where Is My Quantum Computer?. Science 324:473-474 4. Shor P W. Algorithms for quantum computation: discrete log and factoring. In: Goldwasser S, ed. Proceedings of the 35th Symposium on Foundations of Computer Science. Los Alamitos, CA: IEEE Computer Society Press, 1994. 124–134
5. Adleman L (1994) Molecular computation of solutions to combinatorial problems. Science 266:1021-1024
6. S. V. Kartalopoulos. Dna-inspired cryptographic method in optical communications, authentication and data mimicking. Proc. of the IEEE on Military Communications Conference, 2:774–779, 2005.
7. J. D. Watson, F. H. C. Crick, "A structure for de oxy ribose nucleic acid", Nature, vol. 25, pp. 737-738, 1953
8. Leonard M. Adleman "Molecular Computation of solution to combinatorial problems" Science, New Series, Vol. 266, No. 5187. pp. 1021-1024 Nov. 11, 1994
9. H. Hsu and R.C.T.Lee. Dna based encryption methods. In The 23rd Workshop on Combinational Mathematics and Computation Theory, pages 145–150. National Chi Nan University Puli, Nantou Hsies, Taiwan 545, April 2006.
10. Gehani, Ashish, Thomas LaBean, and John Reif. "DNA-based cryptography." Aspects of Molecular Computing. Springer Berlin Heidelberg, 2004. 167-188.
11. Huffman, D.A.: A method for the construction of minimum-redundancy codes. Proceedings of IRE 40(9), 1098–1101 (1952)
12. M. Saeb, A. Baith, "An Encryption Algorithm for Data Security," Recent Advances in Information Science & Technology, N.E. Mastorakis, (editor), World ScientificPublishing Company, pp. 350-354, 1998.
13. Gehani, Ashish, Thomas LaBean, and John Reif. "DNA-based cryptography." Aspects of Molecular Computing. Springer Berlin Heidelberg, 2004. 167-188.

14. J.Chen, "A DNA-Based, Biomolecular Cryptography Design", Proceedings of the 2003 Internationa[Symposium on Circuits and Systems 2003 ISCAS'03, Vol. 3,pp. 822-825,2003.
15. J. Li. C. Papodopouloa, J . M. Xu. and M. Moikavitr. ". Applied Physics Letter. vol. 75, pp. 367.. 1999.
16. A Leier,C.Richter,W.Banzhaf,H.Rauhe, "Cryptography with DNA Binary Strands",Biosystems, Vol. 57, Issue No. 1, pp. 13-22,2007.
17. Kahn, D., 1967. The Codebreakers. Macmillan Publishing Company, New York.
18. Schneier, B., 1996. Applied Cryptography, second ed. John Wiley, New York.
19. K.Tanaka"A. Okamoto, I. Saito, "Public-Key System Using DNA as a One-Way Function for Public Key Distribution", Biosystems, Vol. 81(1), pp. 25-29,2005.
20. Rivest, R.L., Shamir, A., Adleman, L., 1978. A method for obtaining digital signatures and public- key cryptosystems. Commun.ACM 21, 120–126.
21. Clelland, C.T., Risca, V., Bancroft, C., 1999. Hiding messages in DNA microdots. Nature 399, 533–534.
22. G.Cui, L.Qin,Y. Wang" X.Zhang,"An Encryption Scheme Using DNA Technology",3rd International Conference on Bio-Inspired Computing: Theories and Applications 2008, Adelaide SA, pp. 37-42,2008.
23. O.Tornea, M.E.Borda, "DNA Cryptographic Algorithms", International Conference on Advancements of Medicine and Health Care through Technology IFMBE Proceedings, Vol. 26, pp. 223-226,2009.
24. C. Taylor, V. Risca, and C. Bancroft, "Hiding messages in DNA microdots", Nature, vol. 399, pp. 533-534, 1999.
25. S. T. Amin, M. Saeb, S. El-Gindi, "A DNA-based Implementation of YAEA Encryption Algorithm", IASTED, pp. 120-125, 2006.
26. M. E. Borda, O. Tornea, T. Hodorogea, M. Vaida, "Encryption System with Indexing DNA Chromosomes Cryptographic Algorithm", IASTED Proceedings, pp. 12 – 15, 2010.
27. H.J.ShiuKL. Ng,J.F. Fang, R.C.T.Lee,R. and C.H.Huang,"Data Hiding Methods Based Upon DNA Sequences", Information Sciences: An International Journal, Vo1.1 80, Issue No. II,pp. 21 96-2208,2010
28 Z.Yunpeng"Z.Yu.W.,Zhong,R.O.Sinnott, "Index-Based Symmetric DNA Encryption Algorithm", 14th International Congress on Image and Signal Processing (CISP) 20 II ,Shanghai, Vol. 5, pp. 2290-2294, 20 II.
29. (2016) National Center for Biotechnology Information. In: Ncbi.nlm.nih.gov. http://www.ncbi.nlm.nih.gov. Accessed 3 Sep 2015
30. Clelland, Catherine Taylor, Viviana Risca, and Carter Bancroft. "Hiding messages in DNA microdots." Nature 399.6736 (1999): 533-534.
31. Hoover, J. E. Reader's Digest 48, 1–6 (April 1946).
32. Borda, Monica, and Olga Tornea. "DNA secret writing Techniques." IEEE conferences. 2010.
33. C. T. Taylor, V. Risca, and C. Bancroft, "Hiding messages in DNA microdots" Nature, 399:533-534, 1999.
34. Z. Zhang.Z,"A Method to Encrypt Information with DNA Computing", 3rd International conference on Bio-Inspired Computing: Theories and Applications BICT A 2008, pp. [55-160,2008.
35. Pan Linqiang, Xu Jin, Liu Yachun, A Surface-Based DNA Algorithm for the Minimal Vertex Problem, Progress In Natural Science. 13(1)(2003), 81-84.
36. Linqiang Pan, ArtiomAlhazov, Solving HPP and SAT by P systems with Active Memabrabes and Separation Rules, ActaInformatica, 43(2006), 131-145.
37. Bennett C. H.: On Constructing a Molecular Computer. IBM Journal of Research and Development,17 (1973) 525~532
38. Q.Gao,"A Few DNA Based Security Techniques", IEEE Long Island Systems Applications and Technology Conference (LiSAT) 2011 " Farmingdale NY, pp. 1-5,2011.
39. M.R.Abbasy, B. Shanmugam,"Enabling Data Hiding for Resource Sharing in Cloud Computing Environments Based on DNA Sequences", 'IEEE World Congress on Services (SERVICES) 2011', Washington DC, pp. 385-390,20 II.
40. Y.lhang" B.Fu, X.Zhang,,"DNA Cryptography Based on DNA Fragment Assembly", 8th International Conference on Information Science and Digital Content Technology (ICIDT)2012. Jeju, Vol. I, pp. 179-182,2012
41. R.Vishwakarma, N.Amiri,"High Density Data Storage in DNA Using An Efficient Message Encoding Scheme", International Journal of Information Technology Convergence and Services,VoI.2, Issue No. 2, pp.41-46,2012.
42. K.Nirmalya. et.al. ,"An Improved Data Security using DNA Sequencing", Proceedi
43. (2016) GenBank Home. In: Ncbi.nlm.nih.gov. http://www.ncbi.nlm.nih.gov/genbank. Accessed 30 Nov 2015.