DNA Based Security System Based On DNA ASCII Table Using 16x16 Keymatrix

Ravindra Ponugumati[1], P.Bharathi Devi[2]
[1,2]Asst.Professor, Department of Computer Science, KBN College, Vijayawada
[1]ravindraponugumati@gmail.com, [2] bharathipatnala@gmail.com

Article Info
Volume 83
Page Number: 5742 - 5747
Publication Issue:
May - June 2020

Article History
Article Received: *19 November 2019*
Revised: *27 January 2020*
Accepted: *24 February 2020*
Publication: *17 May 2020*

Abstract

In the present internet age, the number of threats is increased with the advancements in technology and also massive usage of the internet. It is the responsibility of the provider to give security to the information whether it is in a cloud or whether it is in storage media that was transmitted through a network. It is also important to observe whether the provider gives the authenticity of the information to the client or not. To overcome this problem, there is a need for encrypting the information before transmitting or storing it. In the browser itself, if we encrypt the data and then transmitted through the network results in better security. To achieve this, DNA Cryptography plays a prominent role in providing end-to-end security to the information which is in the form of DNA Strands while transmitting data through the network. Cryptography with the help of DNA creates confusion for the attacker. In this paper, the authors proposed a novel algorithm that is based on DNA ASCII, conversion of DNA bases based on the key matrix of size 16x16 with hexadecimal values and also applied XOR function with the randomly generated key matrix. By observing the results, the proposed model has taken more time when compared to the existing algorithm because of increasing the number of levels to enhance the security.

Keywords: *DNA, DNA Cryptography, Encryption, Decryption, DNA ASCII*

I. INTRODUCTION

The process of producing unscrambled data from the given data is known as Encryption and revert is known as Decryption. It is a branch of study in Cryptography [1]. To provide security to the information, many algorithms developed based on mathematical equations as well as quantum computing. But those are having some limitations [2,3]. To overcome these limitations, DNA Cryptography plays an important role in the present era to give security to the information. DNA can store huge information in a single gram DNA cell and it was also proven fact by the students of Harvard University [4]. DNA Cryptography is nothing but the unscrambled message is in the form of DNA bases. Each DNA strand contains four nitrogen bases named as Adenine(A), Thymine(T), Cytosine(C) and Guanine(G). Out of these four, A & T are Complimentary bases and C& G are other Complimentary bases according to Watson Crick double helix structure [5,6]. The DNA Digital coding can be represented in the table1 which is used to transmit the binary information of plaintext into DNA form. In the process of protein synthesization, the DNA strand converted into RNA and then converted into Protein form. This can be done in two phases one is Transcription and the other one is Translation. In the transcription, the DNA strand converted as mRNA means messenger RNA that is the base Thymine is converted as Uracil(U)[7,8].

Table 1. DNA Digital Coding

DNA Base	Digital Code
A	00
C	01
G	10
T	11

TEST Engineering & Management
May – June 2020
ISSN: 0193-4120 Page No. 5742-5747

After that, the mRNA is converted into Protein according to the standard DNA Codons table, which is called as Translation Phase. The codon is a combination of 3 nucleotide bases formed among four DNA bases. Each codon is equal to one amino acid. These amino acids are used in the process of protein synthesis (Fig 1) .

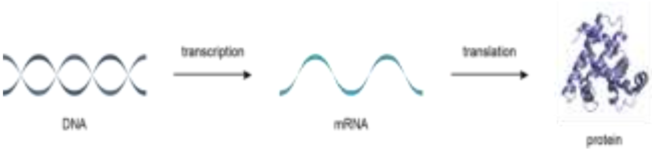

Fig 1. Protein Synthesis

A total 64 codons are formed among four DNA bases. Out of which 61 are amino acids and three are stop signals. These codons play an important role in the filed DNA cryptography. The Figure2 shows the structured codon table which is used in the process of protein synthesis[9].

first base in codon	second base in codon: T	C	A	G	third base in codon
T	TTT Phe	TCT Ser	TAT Tyr	TGT Cys	T
	TTC Phe	TCC Ser	TAC Tyr	TGC Cys	C
	TTA Leu	TCA Ser	TAA stop	TGA stop	A
	TTG Leu	TCG Ser	TAG stop	TGG Trp	G
C	CTT Leu	CCT Pro	CAT His	CGT Arg	T
	CTC Leu	CCC Pro	CAC His	CGC Arg	C
	CTA Leu	CCA Pro	CAA Gln	CGA Arg	A
	CTG Leu	CCG Pro	CAG Gln	CGG Arg	G
A	ATT Ile	ACT Thr	AAT Asn	AGT Ser	T
	ATC Ile	ACC Thr	AAC Asn	AGC Ser	C
	ATA Ile	ACA Thr	AAA Lys	AGA Arg	A
	ATG Met	ACG Thr	AAG Lys	AGG Arg	G
G	GTT Val	GCT Ala	GAT Asp	GGT Gly	T
	GTC Val	GCC Ala	GAC Asp	GGC Gly	C
	GTA Val	GCA Ala	GAA Glu	GGA Gly	A
	GTG Val	GCG Ala	GAG Glu	GGG Gly	G

Fig 2. Structured Codon Table

So much research work is going on in the field of DNA cryptography by using this protein synthesis action and also this DNA cryptography applied all the media for providing security that is whether the transmitted data may be a piece of information, an image, an audio or a video file. The input file may be changed according to the needs but the output of this contains only DNA bases.

II. RELATED WORK

In the year 1994, Adleman experimented Hamiltonian path problem [10]. It is an NP problem solved by assigning short DNA sequences to each city. By using DNA Computing the massive parallelism concept achieved. In the field of cryptography after the introduction of DNA Computing, many researchers turned their interest in DNA cryptography and hid the information in the form of DNA. Lipton [11] created a Boolean equation to understand the satisfiability problem which as the SAT by using DNA with the motivation of Adleman. It sets a trademark and so many researchers did the number of works based on this DNA as a medium to transmit information in an encoded format. Some sample works related to DNA Cryptography discussed in this section. Jie Chen [12] proposed an encryption model with the help of Carbon nanotube-based information. Pankaj Rajkheja [13] added a DNA Cipher layer to the conventional cryptography algorithm that is IDEA. In this algorithm, the Key size is augmented to invulnerable the data from cryptanalytic attacks. S.Sadeg, et al. [14] proposed another symmetric encryption model propelled from DNA by re-enacting thoughts from translation technique (get mRNA from DNA), in this work, the analysts attempted to consolidate DNA Ciphering with an existing encryption calculation which is Rijndael to make another encryption algorithm as in crafted by X. Wang [15] in which they process the plaintext by mapping its substance into DNA coding, at that point encoded it through a Rijndael algorithm. Without the use of public Key Harry C. Shaw

May – June 2020
ISSN: 0193-4120 Page No. 5742-5747

et.al., [16] designed a novel encryption scheme using DNA that contributes to the security of mobile, ad-hoc networks. Mona Sabry [17] designed a Playfair DNA model that has some limitations and those can be overridden by many other researchers like Atito [18], Kiran K Reddi et.al [19]. Kiran K Reddi et.al [20]. mentioned DNA ASCII table based cryptosystem with a spiral approach gives more security when compared with some other existing techniques. A Novel DNA based Cryptosystem using DNA Codons designed by Kiran K Reddi et.al. [21] is the base model for this proposed system. In this model, they implemented the security model in three levels and they considered the DNA Code book which comprised only 64 values. This can be extended in the proposed model up to 256 values and also this model did not generate any random key value. They considered the codebook as a key value.

III. PROPOSED ALGORITHM

Before sending the information, the sender & receiver must agree on the terms of key-value and the Key matrix (Table 2). The Key matrix is a matrix of size 16X16 and it contains all possible combinations of DNA bases A, C, G, T. There are a total of 256 values occurred out of four bases. The DNA box arrangements can be done in 256! Permutations. And also consider the DNA ASCII table which was proposed by Kiran K Reddi et.al., in the paper entitled "A Novel Encryption Scheme to Secure the Data Using DNA Based Play fair Cipher Technique". Initially, the message was converted into its equivalent ASCII value and in turn, converts into binary and then converts into DNA by using the DNA Binary code table. After getting DNA bases, the strand divided into four bases each. Find the position of each base in the key matrix in the form of hexadecimal values. In the next level, these Hexadecimal values converted into binary and then converted into DNA. Then retrieve the ASCII Value from the DNA ASCII table. In the final level convert the ASCII Values of DNA base which is of length four to binary value and perform cross XOR with Key-value which was initially agreed by both that is $ML = ML \oplus KR$ and $MR = MR \oplus KL$. Concatenate both ML and MR and convert them in the form of DNA bases which is cipher text. Doing the same in reverse at receiver end will give the original message. The elaborated process can be depicted in the figure 3.

Table 2. KeyMatrix

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	CGTG	CGCA	CGTT	CACA	CATG	CGCT	TTTA	TTTC	TTTG	TTTT	TTCA	TTCC	TTCG	TTCT	TCTA	TCTC
1	TCTG	TCTT	TTGA	TTGC	TTGG	TTGT	TTAA	TTAC	TTAG	TTAT	TCCA	TCCC	TCCG	TCCT	TCAA	TCAC
2	TCAG	TCAT	TCGA	TCGC	TCGG	TCGT	TATA	TATC	TATG	TATT	TACA	TACC	TACG	TACT	TGTA	TGTC
3	TGTG	TGTT	TAGA	TAGC	TAGG	TAGT	TAAA	TAAC	TAAG	TAAT	TGCA	TGCC	TGCG	TGCT	TGAA	TGAC
4	TGAG	TGAT	TGGA	TGGC	TGGG	TGGT	ATTA	ATTC	ATTG	ATTT	ATCA	ATCC	ATCG	ATCT	ACTA	ACTC
5	ACTG	ACTT	ATGA	ATGC	ATGG	ATGT	ATAA	ATAC	ATAG	ATAT	ACCA	ACCC	ACCG	ACCT	ACAA	ACAC
6	ACAG	ACAT	ACGA	ACGC	ACGG	ACGT	CATA	CATC	CATT	CACC	CACG	CACT	CGTA	CGTC	CAGA	CAGC
7	CAGG	CAGT	CAAA	CAAC	CAAG	CAAT	CGCC	CGCG	CGAA	CGAC	CGAG	CGAT	CGGA	CGGC	CGGG	CGGT
8	CTTA	CTTC	CTTG	CTTT	CTCA	CTCC	CTCG	CTCT	CCTA	CCTC	CCTG	CCTT	CTGA	CTGC	CTGG	CTGT
9	CTAA	CTAC	CTAG	CTAT	CCCA	CCCC	CCCG	CCCT	CCAA	CCAC	CCAG	CCAT	CCGA	CCGC	CCGG	CCGT
A	AATA	AATC	AATG	AATT	AACA	AACC	AACG	AACT	AGTA	AGTC	AGTG	AGTT	AAGA	AAGC	AAGG	AAGT
B	AAAA	AAAC	AAAG	AAAT	AGCA	AGCC	AGCG	AGCT	AGAA	AGAC	AGAG	AGAT	AGGA	AGGC	AGGG	AGGT
C	GTTA	GTTC	GTTG	GTTT	GTCA	GTCC	GTCG	GTCT	GCTA	GCTC	GCTG	GCTT	GTGA	GTGC	GTGG	GTCT
D	GTAA	GTAC	GTAG	GTAT	GCCA	GCCC	GCCG	GCCT	GCAA	GCAC	GCAG	GCAT	GCCA	GCGC	GCGG	GCGT
E	GATA	GATC	GATG	GATT	GACA	GACC	GACG	GACT	GGTA	GGTC	GGTG	GGTT	GAGA	GAGC	GAGG	GAGT
F	GAAA	GAAC	GAAG	GAAT	GGCA	GGCC	GGCG	GGCT	GGAA	GGAC	GGAC	GGAT	GGGA	GGGC	GGGG	GGGT

TEST Engineering & Management
May – June 2020
ISSN: 0193-4120 Page No. 5742-5747

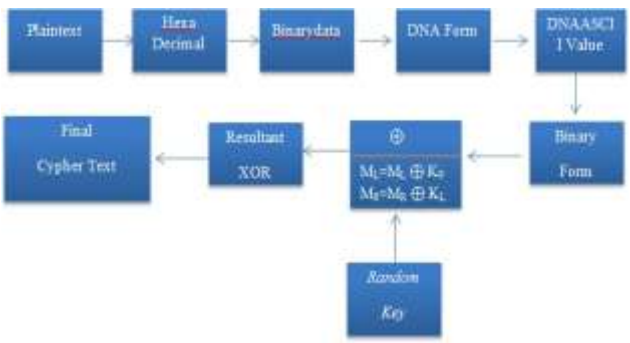

Fig 3. DNA Based Cryptosystem using DNA ASCII Table

The suggested model is developed using .NET environment and the simulations were noted on various plaintext messages of length in terms of bytes. The screenshots and the simulations are tabulated in the following table(Table 3). The encryption and decryption process results can be shown in figure 4 and figure 5.

Fig 4. Encryption of Text Document with the Keyword "dna playfair"

Fig 5. Reverting back the Original Text

Table 3. Time Analysis of Proposed and Existing Models

Message Length(in terms of bytes)	Encryption Time(in terms of ms) Proposed Algorithm	Encryption Time(in term of ms) Existing Algorithm	Decryption Time(in terms of ms) Proposed Algorithm	Decryption Time(in terms of ms) Existing Algorithm
10	2.2543211	0.0043409	1.9236548	0.0001647
100	3.3521648	0.0123234	3.6254893	0.0006070
1000	4.0532165	0.1116644	4.1652013	0.0020742
10000	20.2468594	14.0743528	19.936025	0.0333596
100000	32.1203245	25.0124862	30.268592	5.2224898

The proposed method has taken time complexity more than the existing model by observing the results tabulated in Table 3. Even though it has taken much time, security wise good because the number of functionality in each layers increased when compared to existing model because the arrangement of key matrix and making of DNA ASCII Table was also taken much time. The existing model was also compared with some other models discussed in the related work and proved it was having lesser time complexity to encrypt and decrypt the information. The following figures 6 and 7 showed the comparison of time taking for encryption and decryption for the existed and proposed model

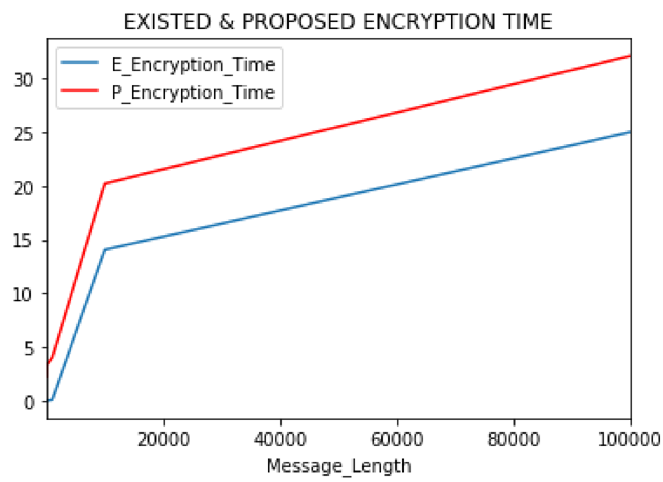

Fig 6. Comparison of Time taking to encrypt the message for various message lengths

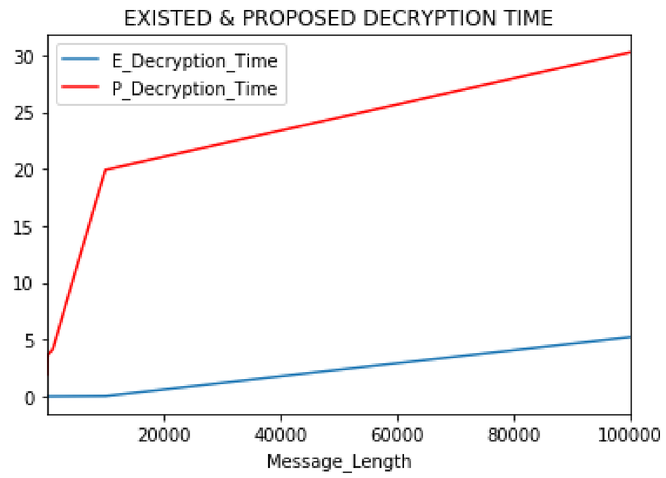

Fig 7. Comparison of Time taking to decrypt the ciphertext4 Implementation and Discussions

IV.CONCLUSIONS

This model ensures better security because of randomly generated key and the prediction rate increased when the values are randomized. Not only the key and also this model performed cross XOR function on message and a key. The XOR function also not done directly on both the message and key. The XOR function done on the right part of message with left part of key and the left part of message with right part of key so that it strengthen the security feature to the algorithm to one more credit. Finally, the DNA box arrangement is also done in 256! Ways so that the intruder identifies the sequence in brute force attack is also difficult.

9 References

[1] W. Stallings, Cryptography and Network Security: Principles and Practices, 3rd edition, Prentice Hall, NJ, 2003.

[2] Noorul Hussain UbaidurRahman, Chithrealekha Balamurugan and Rajapandian Mariappan, “A Novel DNA Computing based Encryption and Decryption Algorithm”, In International Conference on Information and Communication Technologies, pp. 463-475, 2015

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

[4] https://www.extremetech.com/extreme/134672-harvard-cracks-dna-storage- crams-700-terabytes-of-data-into-a-single-gram.

[5] Ashish Gehani, LaBean Thomas and John Reif, “ DNA-based cryptography, In Aspects of Molecular Computing”, Springer Berlin Heidelberg, pp. 167-188, 2004.

[6] Cui Guangzhao, Limin Qin, Yanfeng Wang, and Xuncai Zhang , “An encryption scheme using DNA technology, In Bio-Inspired Computing: Theories and Applications”, BICTA, 3rd IEEE International Conference on, pp.37-42, 2008..

[7] Tausif Anwar, Abhishek Kumar, Sanchita Paul, “DNA Cryptography based on Symmetric Key Exchange”, International Journal of Engineering and Technology, Vol.7,No.3, pp.938-950, 2015.

[8] R.Pradeep Kumar Reddy, C.Nagaraju and N.Subramanyam, “Text Encryption through level based privacy using DNA Steganography”, International Journal of Emerging Trends & Technology in Computer Science(IJETTCS) Vol.3, Issue 3, May-June 2014.

[9] E. Suresh Babu , C. Naga Raju and Munaga H.M Krishna Prasad, ”Inspired Pseudo Biotic DNA Based Cryptographic Mechanism Against Adaptive Cryptographic Attacks”, International Journal of Network Security,Vol.18, No.2,PP.291-303, 2016.

[10] Leonard Adelman, “Molecular Computation of Solution to Combinatorial Problems”, Science, New Series, Vol.266, No.5187, pp.1021-1024, 1994.

[11] R.J.Lipton, “Using DNA to solve NP-Complete Problems”, Science, Vol.268, pp.542-545, 1995.

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

[13] Pankaj Rakheja,“Integrating DNA Computing in International Data Encryption Algorithm(IDEA),”, International Journal of Computer Applications, Vol.26, No.3, pp.1-6, 2011.

[14] S. Sadeg, M. Gougache, N. Mansouri, and H. Drias, "An encryption algorithm inspired from DNA," in Machine and Web Intelligence (ICMWI), 2010 International Conference on, pp. 344-349, 2010.

May – June 2020
ISSN: 0193-4120 Page No. 5742-5747

[15] X. Wang, Q. Zhang, and X. P. Wei, "A New Encryption Method Based on Rijndael Algorithm and DNAComputing," Applied Mechanics and Materials, vol. 20, pp. 1241-1246, 2010
[16] H. Shaw and S. Hussein, "A DNA-Inspired Encryption Methodology for Secure, Mobile Ad-Hoc Networks(MANET)‖," in Proceedings of the First International Conference on Biomedical Electronics and Devices, BIOSIGNALS, pp. 472-477, 2008.
[17] Mona Sabry, Mohammed Hasheem, TaymoorNazmy and Mohamed EssamKhalifa " A DNA and Amino Acids-Based Implementation of Playfair Cipher. International Journal of Computer Science and Information Security", Vol.8(3):129-136, 2010.
[18] Atito A, Khalifa A, Rida SZ, "DNA-based data encryption and hiding using Play fair and insertion techniques," Journal of Communications & computer Engineering, pp.44-49, 2012.
[19] Kiran K Reddi, Bharathi P Devi, "A Novel Encryption Scheme to Secure the Data using DNA Based Playfair Cipher Technique, i-Mangers Journal of Information Technology, Vol.7, Issue 3, pp.1-9[2018].
[20] Bharathi P Devi, Kiran K Kumar, 2018, "A Novel Text Encryption Algorithm using DNA ASCII Table with Spiral Approach", International Journal of Recent Scientific Research, Vol.9, Issue 1, pp.23588-23595.
[21] Patnala, Bd, R K Kumar, "A Novel Level-Based DNA Security Algorithm Using DNA Codons" Computational Intelligence and Big Data Analytics, pp.1-13, 2019.