An Improved Method of Dna Data Encryption using Xor Based Data Segments

D.Ratna Kishore, D.Suneetha, G.G.S.Pradeep

Abstract: Internet is developing each day. One of the most important factors is to provide security for data in internet. In fact that there are numerous number of security algorithm were proposed at the same time hackers are also working with various technique and introduced so many new algorithm to break the security. DNA cryptography is one of the rising regions of computer science. In this paper we proposed a new technique to provide security for data using DNA cryptography. In this we use 256 DNA ASCII table instead of 64 lookup table and key is generated in random manner based on the length of the plaintext*4. In this proposed technique the original plaintext and key was divided into 4 equal parts. The proposed algorithm produces better results when compared to other existing algorithm in terms of encryption and decryption times.

Keywords: DNA Cryptography, Encryption, Decryption, PCR

I. INTRODUCTION

Data and information has become very important resource in present centaury and the process of providing security is also important parameter. So many ways are present to provide security to the data[1-4]. Cryptography is also one of the most important components in computer security. There are multiple number of cryptography algorithm of multiple number of types are available. There are so many defects are present in some existing conventional and classical cryptography techniques. So the attackers easily break the cipher text and create many problems to the authorized persons. There is no relation in between cryptography and molecular biology. Originally there are not relevant to each other but in depth study of molecular biology and also modern biotechnology DNA computing is present these two areas are work together to provide security for data[5]. DNA cryptography is the new field of science in the area of providing security for data. Many researchers introduced so many security algorithms with the help of DNA cryptography to hide the sensitive secret data [6-7]. Completely DNA cryptography is based on the biological problem. Generally the DNA computer not only performs computing just like a compute system it is also able to perform potency and function which a traditional computer system cannot perform. DNA computing is huge scale of parallelism and its computing speed is very huge like 1 billon times per second. Secondly DNA computing has large capacity of storage. In one cubic decimeter of DNA solution have tera bytes of data. Third DNA cryptography has low power consumption. So many techniques are used to carry DNA computation .Some of these techniques are

Gel electrophoresis: In this technique separate DNA fragments are used according to their length. A gel is prepared. The negatively charged molecules are placed are one side of this gel. The negatively charged molecular are moved to the positive gel[8].

Polymerge chain reaction: PCR is having high amplification affection. This is used to amplify DNA molecules [11].

In DNA we can add binary segments to interpret data. Those are

A-00 C-01 G-10 and T-11

In this binary format is used For the purpose of data storage and transmission from one place to another place.

II. RELATED WORK

Adi et al proposed a new scenario to link E-DNA for identify the DNA molecules and it is dynamic in nature. IT attempts to link the unit and to identify the interaction profile in the data communication. Mousa et al propose a new approach for data hiding using DNA cryptography. It uses the concept of reversible contrast mapping. This scheme uses two words to achieve reversibility on the contrast mapping [9].

Jin taur et al proposed a new advanced scheme in data hiding based on the look up table and it is called as Table lookup table substitution method. In this the plain text is replaced with the values of look up table and that replaceable data is transferred to the receiver as a cipher text and the look up table was modified randomly for every data transmission[10].

Mohamed [12] proposed a new innovation in the asymmetric cryptographic technique based on the protocol. The main advantage of the proposed algorithm is that it uses innovative DNA cryptography for sharing secret key among sender and receiver throughout the unsecured transmission.

Banahmed[13] discusses a new reference DNA sequence shared in two parties. Not only the sequence shared and the data is accessed from NCBL and EBI databases and the hacker is not able to access the database because the database is virtually created and accessed randomly. Yamuna [14] present a different encryption technique based on the binary strings. In this 4 different algorithms are present.

Revised Manuscript Received on 30 May 2019.
* Correspondence Author

Dr.D.Ratna Kishore* ,Professor, Department of CSE, NRIIT, Vijayawada, A.P, India.

D.Suneetha, Associate Professor, Department of CSE, NRIIT, Vijayawada, A.P, India.

Dr.G.G.S.Pradeep, Professor, Department of CSE, Malla Reddy Institute of Science and Technology, A.P, India

Kenunta [15] proposed another algorithm consists of different stages because if numbers of stages are increased the hacker does not understand the original message. Kencl [16] proposed a new algorithm for solving concealing problem in DNA sequence. This algorithm works on the principle of repeating sequences and it is stress less. The output of the algorithm is also consist of repeats has no other similarities are having in a given DNA structure. Reza Nazif [17] proposed a new algorithm which uses asymmetric cryptography and increase in the usage of DNA cryptography based on the DNA sequence. Mitras[8] discussed a new algorithm based on DNA molecular sequence with the help of look up table and it provides a better security with respect to various existing algorithm.

III. PROPOSED ALGORITHM

The Proposed Model is shown in Fig 1

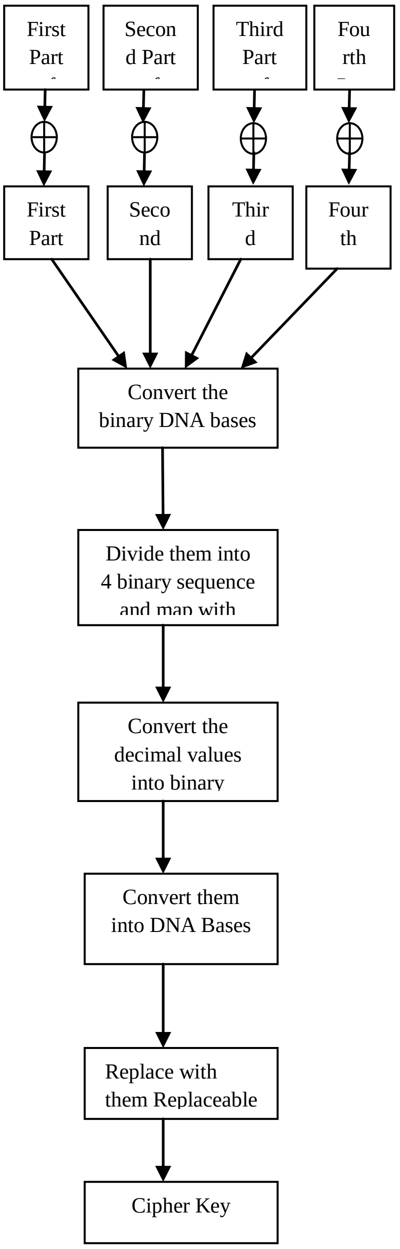

First Part
Secon d Part
Third Part
Fou rth
First Part
Seco nd
Thir d
Four th
Convert the binary DNA bases
Divide them into 4 binary sequence and map with
Convert the decimal values into binary
Convert them into DNA Bases
Replace with them Replaceable
Cipher Key

Fig 1: Model for Proposed System

ALGORITHM FOR ENCRYPTION

1. Convert the given plaintext M into its equivalent binary value
2. Divide the plain text into 4 equal parts(M1,M2,M3,M4)
3. Generate random key and the length of the key is equal to the n*4 where n is the size of the plain text
4. Divide the key into 4 equal parts (K1,K2,K3,K4)
5. Perform XOR operations M1with K1, M2 with K2, M3 with K3 and M4 with K4
6. Plain text is obtained after concatenation 4 XOR operations
7. Transform plain text into DNA bases
8. Split the plain text with respect to ASCII values and assign decimal values according to the DNA ASCII table
9. Convert Decimal values into binary values
10. Replace the binary values with DNA bases
11. Obtain the values and replace them with replaceable characters of DNA ASCII table and that is final cipher key

ALGORITHM FOR DECRYPTION

The reverse operation was performed to get the plain text from cipher text

Empirical Analysis:

Process of Encryption:

Original plain text message M= Welcome

W=87=01010111

e=101=01100101

l=108=01101100

c=99=01100011

o=111=01101111

m=109=01101101

e=101=01100101

010101110110010101101100011000110110111101101101
01100101

Divide the original plain text 4 equal parts: We lc om e

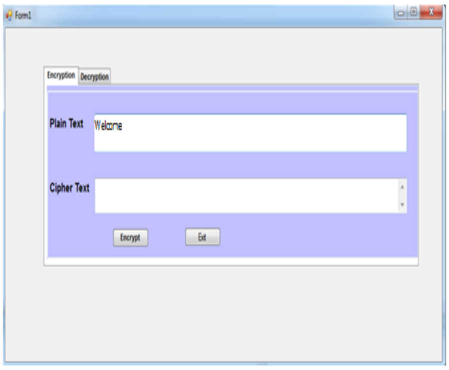
The generated random key K is =1001011010101010110110101010

K1=1001011

K2=01001011
K3=1011011
K4=0101010

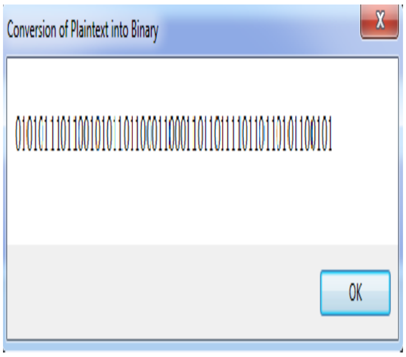
Perform XOR operation: M1 with K1 and the result is 1111111110101110
M2 with K2 and the result is 0101100011001000
M3 with K3 and the result is 0110001100110100
M4 with K4 and the result is 01011111
Concatenation results of all XOR operation is: 111111111010111001011000110010000110001100110100 01011111
The DNA codon sequence is GGGGTTGTCCTAGATACCAGAGCACCGG
Replaceable Decimal values are: 25512822269118295
255=11111111=GGGG
12=00001100=AAGA
82=01010010=CCAT
226=11100010=GTAT
91=01011011=CCTG
182=10110110=TGTT
95=01011111=CCGG
GGGGAAGACCATGTATCCTGTGTTCCGG= ÿ®X È S0_=Cipher Text
Process of Decryption:
The given cipher text is ÿ®X È S0_= GGGGAAGACCATGTATCCTGTGTTCCGG
GGGG=11111111=255
AAGA=00001100=12
CCAT=01010010=82
GTAT=11100010=226
CCTG=01011011=91
TGTT=10110110=182
CCGG=01011111=95
25512822269118295
Then the DNA codon sequence is GGGGTTGTCCTAGATACCAGAGCACCGG =111111111010111001011000110010000110001100110100 01011111
Then obtained Plain Text is =Welcome

IV. RESULTS



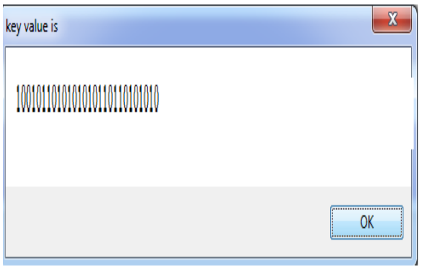
Plain Text: Welcome
Cipher Text:

Fig 2: Encryption Screen



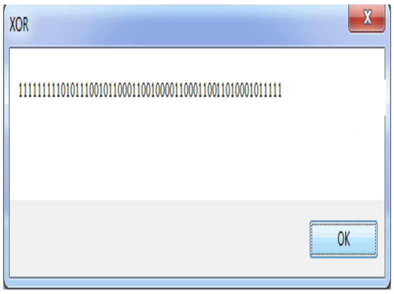
01010111011001010110110001100011011011110110110101100101

Fig 3: Conversion of Plaintext to Binary form



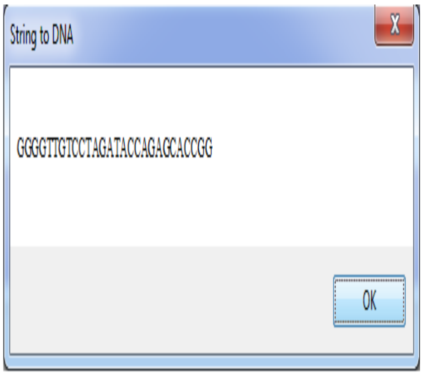
100101101010101010110110101010

Fig 4: Key Value



11111111101011100101100011001000011000110011010001011111

Fig 5: XOR(Plaintext, Key)



GGGGTTGTCCTAGATACCAGAGCACCGG

Fig 6: Conversion of XOR values into DNA Form

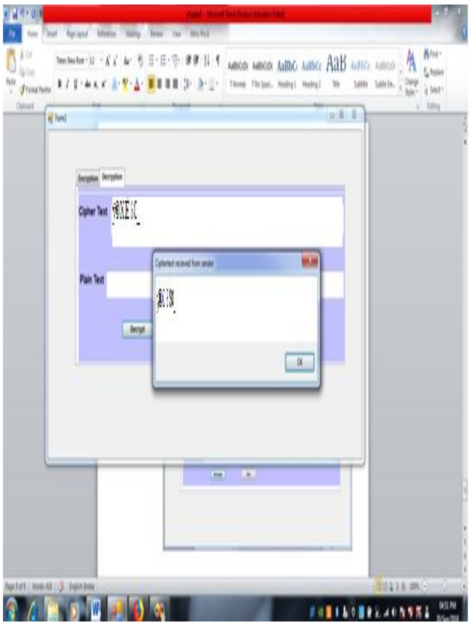


Fig 8: Final Cipher text

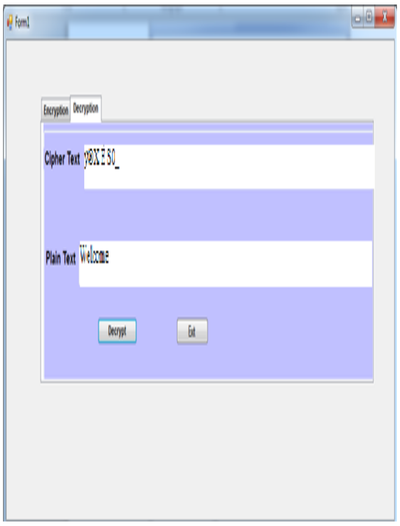


Fig 9: Conversion of Cipher text to Plaintext

Performance Measurement

The analysis of an algorithm measured in intel i3 processor in DOTNET environment with 4GB RAM in Windows7 Platform for the string “Welcome”. The simulations noted down various message lengths in terms of bytes in relation with the time taken for encryption and decryption process. This model is compared with the previous proposed model “Level Based DNA Security Mechanism using DNA Codons” and found that this model suits for all the message lengths which has very less execution time.

Table 1: Comparison of Encryption time between Proposed and Level based DNA Cryptosystem using DNA Codons

Sl.No	Number of Bytes	Encryption time(in ms) of Proposed Algorithm	Encryption time(in ms) of DNA cryptosystem using Codons
1	10	0.0019423	0.0043409
2	100	0.0050861	0.0123234
3	1000	0.0299623	0.1116644
4	10000	0.0861128	14.0743528
5	20000	0.1932413	23.1862541
6	30000	0.8734091	31.2265894

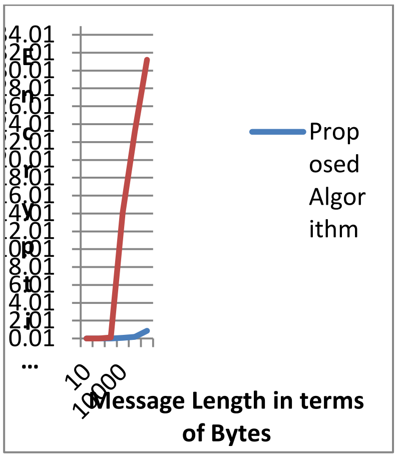


Fig 9: Performance analysis for encryption process of various Message lengths

Table 2: Comparison of Decryption time between Proposed and Level based DNA Cryptosystem using DNA Codons

Sl.No.	Number of Bytes	Decryption time(in ms) of Proposed Algorithm	Decryption time(in ms) of DNA cryptosystem using Codons
1	10	0.0001862	0.0001647
2	100	0.0010924	0.0006071
3	1000	0.0161892	0.0020742
4	10000	0.1296585	0.0333596
5	20000	1.9865942	3.2569877
6	30000	5.4730824	8.1528588

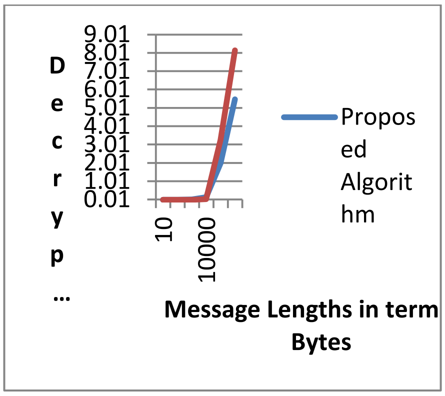


Fig 10: Performance analysis of Decryption Process of Various Message Lengths

V. CONCLUSION

In the proposed algorithm as the key is created randomly, it is an incomprehensible undertaking to the intruder to figure out the plaintext. At first, both sender and receiver affirm to the spiral pattern. The randomly created key by the sender is exchanged to the recipient through the safe medium. The proposed technique has three level securities. In the principal level, the cross join of XOR performed with the plaintext and the key i.e., XOR(M_1,K_1),XOR(M_2,$K_{2)}$,XOR(M_3,$K_{3)}$and XOR(M_4,K_4) is performed. In the following level the DNA Sequence which is of length four is mapped to DNA ASCII Value. Another DNA ASCII Table is planned with the goal that the mapping can be distinguished in 256! ways making the activity of intruder more complex. In the last level the DNA Sequences are arranged in a spiral design. The information is sent row wise to the receiver. The proposed algorithm expanded the level of confusion and diffusion to deliver a higher security framework.

REFERENCES

1. G. Cui, L. Qin, Y. Wang and X. Zhang, "An encryption scheme using DNA technology," *2008 3rd International Conference on Bio-Inspired Computing: Theories and Applications*, Adelaide, SA, 2016, pp. 37-42.
2. An Elliptical Curve Cryptography (ECC) Primer-Why ECC is the next generation of public key cryptography, The Certicom catch the curve-White Paper Series, June, 2014.
3. Gilles Brassard, Norbert Lutkenhaus, Tal Mor and Barry C.Sanders, “Limitations of Practical Quantum Cryptography, Physics Review Letters, Vol.85, Issue.6, pp.1330-1333, 2000
4. https://cs.stanford.edu/people/eroberts/courses/soco/projects/dna-computing/adleman_bio.htm.
5. Gehani A., LaBean T., Reif J., “DNA-based Cryptography. Aspects of Molecular Computing”. Lecture Notes in Computer Science, vol 2950. Springer, Berlin, Heidelberg, 2013
6. N.Galbreath, Cryptography for Internet and Database Applications: Developing Secret and Public Key Techniques with Java, New York, USA: John Wiley and Sons, Inc., 2014.
7. A.Menezes, P.Oorschot, and S.Vanstone, Handbook of applied cryptography, CRC Press, 1996.
8. Mitras, "What is cryptography?," in *IEEE Security & Privacy*, vol. 4, no. 1, pp. 70-73, Jan.-Feb. 2006.
9. Adi, Cryptography and Network Security: Principles and Practices, 4th edition, Pearson Education, Prentice Hall, NJ, 2009.
10. Jin, "Cryptography and security - future challenges and issues," *15th International Conference on Advanced Computing and Communications (ADCOM 2007)*, Guwahati, Assam, pp. xxxii-xxxiii, 2017.
11. Hamdan.O.Alanazi,B.B.Zaidan, A.A.Zaidan, Hamid.A.Jalab, M.Shabbir and Y.Al-Nabhani, “New Compartive Study Between DES, 3DES and AES with Nine Factors”, Journal of Computing, Vol.2, Issue3,pp.152-157, 2010.
12. Mohmamed Cryptography and network security, Express Learning, ITL Education Solution ltd.
13. Jahmmed D.R., Cryptography: Theory and Practice, CRC Press, Third Edition, 2016.
14. Yamuna Sharma, “Implementation and Analysis of Various Cryptosystmes”, Indian Journal of Science & Technology, Vol.3, No.12, pp.1173-1176, 2011.
15. Kerntent, “Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures”, International Journal of Computer Science and Management Studies, Vol.11, Issue.3, pp.60-63, 2012.
16. TKencil, "A study of DES and Blowfish encryption algorithm," *TAs study of DNA ENCON 2009 - 2009 IEEE Region 10 Conference*, Singapore, pp.1-4, 2014.
17. Nazefi “ A Study of DNA Cryptography” International conference of computer Vision , 2016