International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Information Security using DNA Cryptography Along with AES Algorithm

Miss.Varsha Hari Kolate and Dr.R.B.Joshi

Department of information Technology JSPM rajarshi Shahu college of engineering

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

Securing information is the most important need of not only the business world but also it's highly essential in all the other major sectors. The secured data storage capacity along with security during data transit is also an important factor. In this paper DNA based security technique is proposed as an information carrier, The new data securing method can be adopted by harnessing the advantages of DNA based AES. This technique will provide multilayer security. The proposed system aims to secure transactional data during communication as it is required when message or data transfer between sender and receiver should be confidential along with integrity and availability.AS the data hiding needs a carrier to hold the data, therefore in order to enhance data security and make the data more confidential effective encryption algorithm is proposed using DNA cryptography. DNA molecules, holds an ability to store, process and transfer data, stimulates the notion of DNA cryptography. This amalgamation of the chemical features of genetic DNA structures along with cryptography confirms the non-vulnerable communication. The current features with reference to DNA cryptography are reviewed and presented here.

Keywords: *Information security, Time vary- ing delay DNA cryptography,Data security;Encoding and decoding;AES*

Introduction

It's obvious that a new tactic to secure valuable information is required, if ecommerce and internet users would like to stay ahead of the invaders and more efficiently shield their intellectual property, files, client information and personnel then the employed strategies to secure the information must be virtuous and adequate to challenge the ever-changing data breaches. However this the scenario that demands secure ambiance for the information along with encryption of data which is static one or stored data and the data which is in transit over the network.As per the understanding from the various literatures term cryptography stands for securing your information by writing it in some specific secret format to make it difficult to understand and retrieve the meaning just by simply reading it.The need of current generation to secure the huge amount of data produced and continuous transition over the network has raised the demand for securing this transit data from the hackers. Hence protecting the data which is static in the repository or data ware house and some data which is on the wire or transit needs to be protected is the biggest challenge for the corporate world and also for many organizations. Cryptography applies mathematical approach and techniques for securing this information as per the CIA triad of Confidentiality, Integrity and Availability. DNA cryptography is inspired from biological science. In biological science DNA is an information carrier from one generation to another. Security is concerned with the protection of information while transmitting over the network. In this paper DNA based AES algorithm is proposed to be used for the purpose of encrypting the information or data and provide protected secured original data to user. The security needs that include confidentiality, Integrity, Availability Non repudiation and Authentication are all together are implemented through this novel approach.

A: Benefits of DNA storage of data:

1 A gram of DNA contains 1021 DNA bases = 108 Terabytes of data.
2 Speed:Implement more complex crypto algorithms,It brings forward new hope to break unbreakable algorithms.This is because DNA computing offers more speed,minimal storage and power requirments.
3Storage:DNA stores memory at a density of about 1 bit/nm3 where conventional storage media requires 1012nm3/bit.
4Power Requirements:No power required for DNA computing while the computation is taking place.
5 Authenticity:Confirms that data is coming from right person.

Review of Literature

In[1] Author Raj, Bonny B; Sharmila and etc had suggested the use of DNA encoding methods. Use of generic traditional approach to harness the power of cryptography along with DNA as an information carrier. In this approach the author highlighted the ability of De-oxyribo Nucleic Acid(DNA) for use as an upcoming technique. The use of DNA cryptog- raphy enhanced parallelism along with incomparable energy efficiency, storing and computing abilities. In[2] Authors Saijisha K S and etc had implemented the amal- gamation of cryptography and steganography which delivers more security for the information thorough DNA encoding. prevailing security with high volume and low revision rate. of secure and fault-tolerant communication in the presence method and DNA based AES algorithm .This technique will enable to encrypt the data in a very complex. Here DNA is discovered as a new transporter for securing the information during transit since it accomplishes higher protection and features includes are collaborative support of basic networking function such as routing and data network functions also wire- less security protocol stop undesirable parties from connecting to your wireless network. They also addressed the problem. A novel data security scheme can be established by captivating the benefits of DNA based AES (Advanced Encryption Standard) cryptography and DNA steganography. This method offers multilayer security to confidential information. In this approach initially text encoded to DNA bases then DNA based AES algorithm used over it. As a final point the encoded DNA will be masked in another DNA sequence. This hybrid technique provides triple layer security to the secret message. This hybrid technique provides triple layer security using DNA based algorithm as the secret message. They mention encryption algorithm proposed is based on the combination idea of DNA encoding and AES encryption. In[3] Author Sudipta Singha Roy and etc had proposed and explained a novel encryption methods. It is proposed using delayed chaotic neural network with a posterior DNA cryptography. The binary sequence need to a perform XOR operation with message blocks to form a key by passing it through permutation function whose dependency is over the binary sequence made from chaotic neural network. The proposed method performs superior in field of security by including DNA cryptography and ensure secure between end to end users. The supplementary DNA cryptographic approach is of adversaries across a multi-hop wireless network with frequently changing topology. In this approach to commendably handle with random nasty interruption of data transmissions, authors propose and assess the secure message transmission (SMT) protocol and its substitute, the secure single-path (SSP) protocol. Amongst the noticeable characteristics of SMT and SSP is their capability to function uniquely in an end-to-end method and without limiting rules on the network conviction and security associations.

In [6] authors Md. RafiulBiswas and etc had proposed DNA cryptographic technique which is using dynamic DNA en- coding along with asymmetric cryptosystem for performance enhancement in terms of data security. By applying the math- ematical approach to divide the plaintext in the specific format of some fixed size length of text called chunk. Apply the algorithm on each of these chunks and merge the cipher text of each using dynamic DNA encoding. They applied the concept of converting the text into ASCII equivalent then separated it to a finite one. During encryption equivalent binary is considered for DNA bases. Finally to carry out the merging operation on each chunk, sufficient random strings are produced to diffuse and confuse. Fibonacci series is used for these random strings castoff over the cipher text acquired from the first level and the security levels are enhanced. An empirical analysis encryption to strengthen the security of the proposed carried out by using RSA, ElGamal and Paillier cryptosystems. model. In[4] authors K.Kalaiselvi and etc has proposed methods to increase the performance of convential AES and using make the existing cryptosystem more complex and stronger against attacks. In traditional cryptosystems they uses block ciphers and also use Key-dependent ciphers for securing the data were found to be weaker in terms of efficiency as they rely on the security and the speed of the algorithm. In order to strengthen encryption process by making them adaptive and dynamic so that they can tackle cryptanalytic attacks. Adding confusion and diffusion is one of the way to complicate the algorithm and avert the attacks. They enhanced AES cryptosystem by employing genetic algorithm because genetic operations are perform inconsequential and benefit of this algorithm were increase efficiency. The presented complication rises the execution time of the algorithm that tends to timing attacks. This paper proposed two improved AES cryptosystem by using Genetic algorithm (GA) in SPboxes and alteration of AES by employing nonlinear neural network (NN) in SP network to enhance

Proposed Methodology

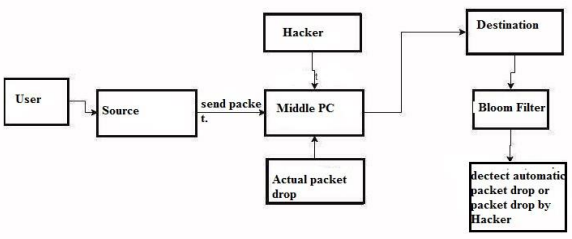

Fig. 1. System Architecture

1) **Source(System1)**: Source is sending a file to destination .If the file is single then any one can hack this file in the network so we are sending the file in encrypted format and this file is divided into three packets and also sharing the secret key to decrypt file. 2 2) **Destination(system2)**:Destination is checked he/she geta original file or not.If the file is changed from hacker then it will denote the packet.It is drop or changed so user will not get original file .The use of secret key user will download original file encrypt and decrypt the file. 3) **Hacker**:Hacker will drop the any packet or changed destination address.If the address is changed then original file not send to destination

Structure of DNA

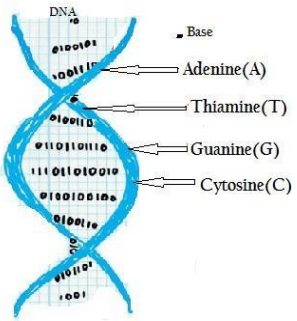

Fig. 2. Structure of DNA

DNA stands for Deoxyribose nucleic acid is a thread like chain of molecules known as nucleic acid. They are used for transmitting genetic instructions which in turn is used in growth, development, functioning and reproduction of all living organism [1]. One of the major advantage of DNA molecule is that, it is a combination of four bases:

A. Table DNA digital encoding

These four bases combines in different order to form: Purines (Guanine and Adenine)and Pyrimidines (Thymine and Cytosine). These bi- strands of DNA molecules are anti parallel and they can moves in the reverse directions also DNA molecule are convertedinto two bit binary value[1]. 1)Encryption:The plaintext is sent to encryption process and number of steps to produce DNA encrypted form. 2)De- cryption:The encrypted ambiguity sequence is first encrypted using AES to require key sequence.After using this key the amino sequence is decrypted to sequence.This is converted to binary,then corresponding ASCII values.

Four Bases	Binary Value
Adenine(A)	00
Thiamine(T)	01
Guanine(G)	10
Cytosine(C)	11

Fig. 3. DNA digital encoding

Related Work

1]The proposed algorithm were developed by researchers not only to ensure data security but also to enhance the performance. The researchers suggested that using DNA based encryption algorithm it's possible to accomplish the goal. When DNA Based encoded data received then apply PCR amplification(polymer chain reaction). Which is often used to examine extremely small amount ofsample and test the results.[1] Due to an added security features Advanced Encryption Standard (AES), usage became widespread in the field of commercial transactions, ebusiness also it support and provide security for wireless communication and encrypted data storage etc. AES is more safe and quicker as compare to triple DES both in hardware and software. The flexibility provided in terms of key size and number of rounds makes it more viable solution as compared to other symmetric key ciphers. There are 10 rounds for 128-bit key, 12 rounds for 192-bit key and 14 rounds for 256-bit key. Different round keys, obtained from AES key are utilized round wise. AES algorithm considers bytes for the block of data so in case of 128 bits of plain text is considered as 16 bytes. 2]The authors suggested that DNA based AES algorithm provide triple layer security.They also discuss about methods and steps involved in the proposed DNA encryption and decryption[2].
3]Authors explain a cryptographic model,which is proposed for text messages by using chaotic neural network along with transmogrify delay for encryption to first step DNA cryptography[3].

A.Binary Strands usage for DNA cryptosystem : Leier et al. used DNA binary strands to perform cryptography in their paper [Leieret al.,2000]. They specified that, both the sender and recipient hold the secret data.The same technical potentials then the projected cryptosystem mechanisms shows remarkable results.
B.Using Dummy Strands: The DNA binary strands with 's' denoting start and 'e' denoting end are used as sticky ends for varying length binary string in between them. For encoding digital text with different lengths with representation of 0-DNA bit and 1-DNA bit is done by using DNA oligonucleotides with sticky ends. The concatenation of the encoding bits is modeled as show

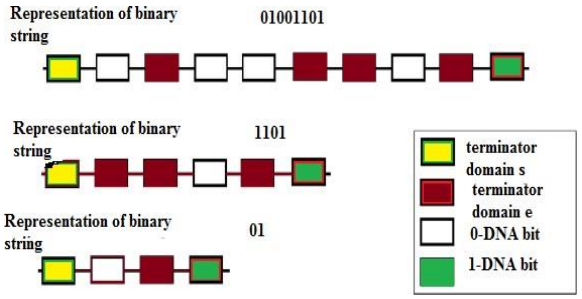

Fig .3 shows the DNA binary strands which ar

the representative of the corresponding digital binary strings. The cryptosystem based on DNA steganography
follows :
Step 1: Sharing Encryption Key.
Step 2: Formation of the digital binary string and then encrypted to obtain DNA sequence.
Step 3: Generating dummy DNA for confusion and diffusion process.
Step 4: The dummy strands and the encrypted strands are mixed in equimolar amounts.
Step 5: The resultant solution is sent to the intended receiver through open communication channel

tep 6: Decryption by the recipient. Using the key sequence as one of the primers and the corresponding 0-
DNA bit or 1-DNA bit as another primer PCR is performed.

A. Algorithm Explanation

DNA based AES algorithm DNA encoding, the result will be a sequence of nitrogen bases. The DNA based AES
algorithm [2] takes data in blocks of 64 bases. A key of 128 bit (64 DNA) is used for encryption as well as decryption.
Inorder to obtain the cipher text, the input has to undergo
10 rounds of operation where each round involves the following functions:
1)DNA AddRoundKey: This is a first phase.It is a simple operation that involves XOR of elements of the STATE with
the corresponding Round key. The derive set round keys are
generated through key expansion process .
2) DNA SubBytes: In this step, each 4 DNA in STATE streams will be an input to the function transposition in the SBox[2] .
3) DNA Rows: It is a transformation that operates row by row
on STATE. It is basically a function of separating each row
in a separate stream then left rotation by 4 DNA characters
according to each row number[2] .
4) DNA MixColumn: This operation is the most difficult the process separately to produce new columnIn MixColumn
function, a predefined column matrix is XORed with each
column of input as per the round number. This function is
only present in first eight rounds The decryption procedure
involves the inverse of all the encryption round functions.
During decryption, the inverse[2]

B DNA Encryption steps:

• Convert the message to binary form from its ASCIIvalue.
• Use 4-bit binary coding rule to convert the message in binary form to DNA. Then check whether the length of DNA form obtained is divisible by three, to divide them to codons (each codon contains three bases). If not, append nitrogen base 'A' at the end of obtained DNA form till the codons can be formed.
• Convert DNA form obtained from the previous step to amino acid, based on amino table. During this process record the corresponding ambiguity bits , which will be used in DNA decoding step.
• Perform swapping in amino acid form of the message and again convert it into DNA. Inorder to performDNA based AES encryption [2], the obtained DNA form need to be divided into blocks or states (where each state contains 64 DNA bases). For that check the length of DNA bases whether it is divisible by 64. If not, append base 'A' at the end of obtained DNA form till the states can be formed. Then randomly generate the key and perform key expansion.

- Apply DNA based AES algorithm .
- Convert the DNA cipher to binary[2].

C DNA decryption steps:

- Convert the binary form of cipher text to DNA. Also obtain the DNA form of key extracted. Then perform key expansion.
- Decrypt the DNA cipher with DNA based AES algorithm.
- Converted the output obtained from the previous step to amino acid. Before the conversion check whether the DNA form obtained can be divide into codons. For that exclude the bases at the end one by one till the formation of codons is possible (here the extra bases appended during encryption get removed).
- Perform reverse swapping in amino form thus obtained.
- Convert amino to DNA with the help of ambiguity bits, then convert to binary.
- Obtain the original message from ASCII value after ASCII conversion of binary.[2]

Both encryption and decryption steps helps to avoid problem of data breach.DNA based AES algorithm increase integirty level of data.This paltform will be best using for data security in any stearm.

Characters	DNA Triple
A	CGA
B	CCA
C	GTT
D	TTG
E	GGT
G	TTT
..	..
..	..
..	..
V	CCT
W	CCG
X	CTA
Y	AAA

Fig. 5. DNA encoding

Implementation

The plaintext message is encrypted with AES algorithm. The security of this algorithm is given by the computational difficulty of factoring large numbers. To be secure, very large numbers must be used as primes, 100 decimal digits at the very least. Product of such large prime numbers is an easy mathematical operation, but reverse process is a very hard task. It is extremely difficult, nearly impossible, to determine derived keys called round keys.these are apiled along with other operations,on an aaray of data to be encrypted. These are the following steps of encryption for a 128-bit block..

1.Derive the set of round keys from the cipher key.

2.Initialize the state array with the blockdata(plaintext) 3.Add the initial rounds key to the starting state array. 4 perform nine rounds of state manipulation.

5 perform the tenth and final round of state.

6 Copy the final state array out as the encrypted data(ciphertext). The encrypted message with AES is a set of numerical values. These numbers will be converted using substitution in artificial DNA strand. All resulted peaces of DNA strands are bind together using a special ligase protein and the complementary strand as a template. The encrypted message can be transmitted in a compact form on DNA chip.

Algorithm steps: Step 1: Binary data, text or image, is visualized like ASCII cod or brightness levels. For example original message: “my secret !” in ASCII will be: 109 121 32 115 101 99 114 101 116 33.

Step 2: This numeric values are arranged in a string and taken by several digits at once, number of digits rise together with the public keys length. In this example we’ll take seven digits at once and obtain: 1091213 2115101 9911410 111633. Step 3: These numbers, seven digits long will be encrypted with public key (public key will be relatively short 224 O. Tornea and M.E. Borda IFMBE Proceedings Vol. 26 in order to make the example easer to follow) and the result is another set of numbers: 417310496328959; 129126952185213; 373906236380070; 367568882589235.

Step 4: Encrypted sequence is trans- formed in binary form: 417310496328959Æ 0101111011100010101010101111100101000011001 11111
11.

Step 5: Binary sequence using substitution is transformed
in DNA sequence: A – 00 C – 01 G – 10 T – 11 0101111011100010101010101111100101000011001 1111
1111Æ Æ CCTGTGAGGGGGTTGCCAATATTTT

Step 6: All sequences are bind together in a single strand, the ciphertext: CCTGTGAGGGGGTTGCCAATATTTTCTCCC- TAAG TCGACTCGGTCCTTCCTCCCTAAGTCGACTCG-GTCC TTCCCCCAACAATCCACGCGACATGGCGCCC-CAAC AATCCACGCGACATGGCGCCATGCATCCATAG-GTC CCTGATAT. Decryption is a reverse process: the DNA strand is cleaved in original peaces using restriction enzymes and transformed in numerical values using the same substitution as for encryption. The last step of decryption is done using the private AES key

Result

Input:Here, Whole System taken many more attribute for the input purpose but here author mainly focuses on the accuracy, time, storage and energy cost of system. Based on this attributes we getting following analytical result for our proposed system with respect to existing system. Expected results:

	Existing	Proposed
Accuracy	8	10
Storage	10	2
Energy	8	4
Time	10	6

Fig. 6. DNA digital encoding

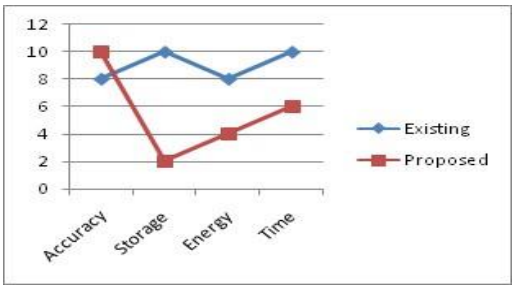

Fig. 7. DNA digital encoding

Conclusion

DNA cryptography is a favorable and fast developing arenain data security. The uses of four bases A,T,G and C for encoding the info helps in to improve the performance in terms of parallelism and also huge capacity to store the data. .A secured DNA based cryptographic algorithms provides multi-levels of security along with DNA based AES encryption.Compression techniques can also be applied with DNA cryptography using AES. It can be used are secure sensitive data like military purposes.Main purpose use by DNA cryptography has secure share and receive your data. VII.

Future Work

The big tech giants, may take an initiative to commercial- size DNA computers in near future. Hopefully, in years the virtually un-hackable DNA cryptography techniques will be n effective alternative

to classical cryptosystem. The security of real time information flow among the distributed network system will be area of research.

References

[1]. B.Raj, V. Ceronmani sharmimila," An Survey on DNA Based Cryptography" IEEE 2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR) - Ernakulam

[2]. (2018.7.11-2018.7.13)] 2018.

[3]. Saijisha K S,S.Mathew," An encryption based on DNA cryptography and steganography"IEEE 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)COIMBATORE, India (2017.4.202017.4.22)] 2017 .

[4]. S.ROY, Shaikh Akib Shahriyar,Md.Asaf-Uddowla,kazi md.Rokibul Alam,Yasuhiko Morimoto," A novel encryption model for text messages using delayed chaotic neural network and DNA cryptography"[IEEE 2017 20th International Conference of Computer and Information Technology (ICCIT) - Dhaka, Bangladesh (2017.12.222017.12.24) 2017.

[5]. K.KALAISELVI "Enhanced AES Cryptosystem by using Genetic Algorithm and Neural Network in S-box" 978-15090-1936-6/16/$31.00 ©2016 IEEE.

[6]. Panagiotis Papadimitratos," Secure Data Communication in Mobile Ad Hoc Networks", IEEE journal on selected areas in communications 0733-8716.

[7]. Md. Rafiul Biswas , Kazi Md. Rokibul Alam ,Ali Akber , Yasuhiko Mori- moto "A DNA cryptographic technique based on dynamic DNA encoding and asymmetric cryptosystem " Published in: 2017 4th International Conference on Networking, Systems and Security (NSysS)978-1-5386-3288-8/17/$31.00(2017)IEEE.