International Journal of Future Generation Communication and Networking
Vol. 13, No. 3, (2020), pp. 3191–3196

# A Survey On Information Security Using DNA Cryptography Along With AES Algorithm.

**Varsha Hari kolate[1], Dr.R.B.Joshi[2]**

*[1] Department of computer engineering, JSPM's RSCOE Tathawade, ,Pune, India*
*[2]Professor, Department of computer engineering, JSPM's RSCOE Tathawade, ,Pune, India*
*[1]varshakolate08@gmail.com, [2]ramjoshi.comp@gmail.com*

***Abstract***

*Securing information is the most important need of not only the business world but also its 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 survey paper DNA based security technique is proposed as an information transporter, the latest data securing process can be adopted by harnessing the benefits of DNA based AES. This technique will provide multilevel security. The proposed system aims to secure transaction data during communication as it is essential when a message or data transmit between sender and receiver should be private along with integrity and availability.AS the detail hiding needs a carrier to hold the data, therefore in order to increase data security and make the data more private effectual encryption algorithm is proposed using DNA cryptography. DNA molecules, holds an ability to accumulation, 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 nonvulnerable communication. The current features with reference to DNA cryptography are reviewed and presented here.*

***Keywords:*** *Information security, Time varying delay, DNA cryptography, Data protection, AES*

## 1. 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 scholarly 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 anxious with the protection of information while transmitting top of the network. In this paper DNA based AES algorithm is proposed to be used for the aim 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 hold 1021 DNA bases = 108 Terabytes of data. 2 ]Speed:Execute more intricate crypto algorithms,It brings forward new hope to break strong algorithms.This is because DNA compute offers better momemtum,High storage. 3 ]Storage:DNA stores memory at a density of about 1 bit/nm3 where established storage media requires 1012nm3/bit. 4 ]Power Requirements:No power essential for DNA storage. 5 ]Authenticity:Confirms that data is coming from right per- son.

## 2. 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 safety for the information through DNA encoding methods 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 prevailing security with high volume and low revision rate. A novel data security scheme can be established by capti- vating the benefits of DNA basics 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 a new DNA sequence. This hybrid technique providing three level security to the private message. This hybrid technique provides three level security using DNA based algorithm as the secret message. They mention encryption algorithm proposed is based on the amalgamation idea of DNA encoding and AES encryption.

In[3] Author Sudipta Singha Roy and etc had proposed and explained a new encryption methods. It is proposed using delayed chaotic neural network with a subsequent DNA cryptog- raphy. The binary sequence need to a execute XOR operation with message blocks to form a key by passing it through permutation function whose dependency is over the binary series made from chaotic neural network. The proposed process performs better-quality in section of security by including DNA cryptography and ensure secure between end to end users. The supplementary DNA cryptographic approach is castoff over the cipher text acquired from the initial level encryption to strengthen the security of the proposed model.

In[4] Authors K.KALAISELVI and etc has proposed methods to increase the performance of convential AES and using make the current cryptosystem more difficult and powerful 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 protection and the quickness of the algorithm. In order to strengh then 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 improved AES cryptosystem by employ genetic algorithm because genetic operations are perform inconsequential and benefit of this algorithm were increase efficiency. The presented complication rises the completing time of the algorithm that tends to monitor attacks. This paper proposed two improved AES cryptosystem by using Genetic algorithm in SP boxes and alteration of AES by employing non linear neural network in SP network to enhance security in

contradiction of timing attack and lessen the count time of the offered system. Both GA and NN are appiled in key elaboration and key dispensation of the AES algorithm.

In[5] Authors Panagiotis Papadimitratos suggested that wire- less secure data communication also protocols are widely applicable. They provide lightweight end to end security 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 of secure and fault-tolerant communication in the presence of adversaries across a multi-hop wireless network with fre- quently 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. Rafiul Biswas and etc had proposed DNA cryptographic technique which is using dynamic DNA en- coding 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 and the safety levels are enhanced. An empirical analysis carried out by using RSA, ElGamal and Paillier cryptosystems.

## 3.Structure of DNA

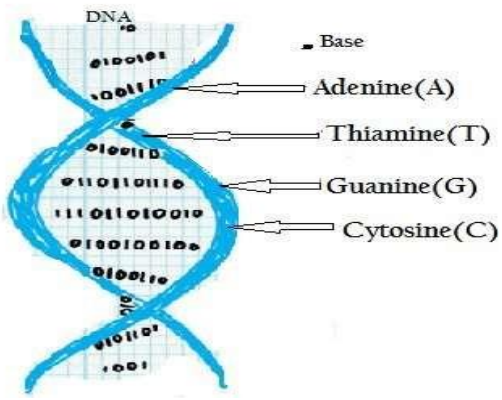


**Fig 1.Structure of DNA**

De-oxyribo nucleic acid (DNA) is a theme like sequence of molecules known as nucleic acid. They have used for transmit and receive DNA genetic commands which in turn is used in growth, improvement, functioning and reproduction of all living organism [1]. One of the primary benifit of DNA molecule is that, it is a group of four bases:

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

**Fig. 2. DNA digital Encoding**

These four kind of bases collaborates in dissimilar order to form:[G],[A],[T] and[C] These bi- strands of DNA molecules are inverse-similar and they can move in the opposite directions also DNA bases are transformed into two bit binary value[1]. 1) Encryption: The plaintext is sent to encryption process and number of steps to produce DNA encrypted form. 2) Decryption: 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.

## 4. 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 of sample and test the results.[1] Due to an added security features Advanced Encryption Standard (AES), usage became widespread in the field of commercial transactions, e-business also it support and provide security for wireless transmission and encrypted information storage etc. AES is more safe and quicker as compare to three times 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. Here [TEN] rounds for [128-bit],12 rounds for [192-bit ] KEY and 14 rounds for [256-bit key]. Varied round keys, acquired from AES key are utilized round wise. AES algorithm considers bytes for the section of data so in case of 128 bits of simple 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 procedure involved in the proposed DNA encryption and decryption [2].

3] The Authors explain a cryptographic pattern model, which is suggested text for messages by applying chaotic neural network along with transmogrify delay for encryption to first step DNA cryptography[3]. A. Binary Strands usage for DNA cryptosystem:

A.DNA binary strands to perform cryptography in their paper They specified that, both the sender and recipient hold the secret data along with 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 shown:
Fig .3 point of the compatible 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 as well as encrypted strands are combination in multiple quantity.
Step 5: The resulting output is send to the expected recipient by medium for transferring information or server. Step 6: Decryption by the receiver. Using the key arrange series as one of the primers and the consequent [bits] .
C. Binary Strands Representation: The Figure illustrates the DNA sequence form which is the represented of the compatible digital binary string sequence.

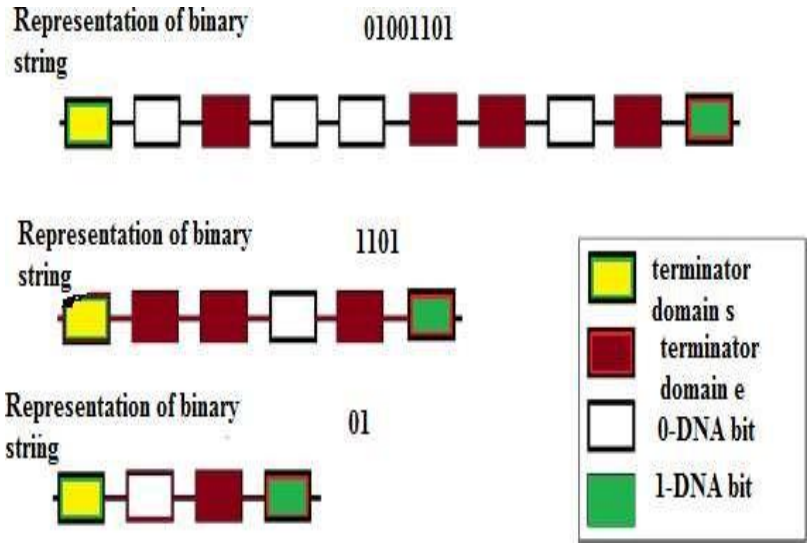


**Fig. 3. DNA Strands**

## 5. Algorithm Explanation

DNA base algorithm(AES) The solution will be a series of four bases. The first priorty is an AES algorithm takes data in sections of 64 bases. The key of 128 bit [64 DNA]is used for encoding.[2]
Orderly to receive the coded message, the method has to perform 10 rounds of procedure. These tasks are performed in DNA stages.
1) AddRoundKey: It is an first phase.It is a easy function that adds XoR of the factor of the position with the comparable Round key. The derive set round keys are produced by key elaboration stage[2].
2) SubBytes: In the second stage, every [four] DNA in [state] stream will be substitute information put in the s-box[2] .
3) Rows: In third stage conversion are exchange row to row on [state]. The main task is differentiated all rows after that shifting rows in left direction [2] .
4) MixColumn: This task is the most hardest. The process individually to produce a new column In Mix Column task, a prearranged column pattern is XoRed with all, proceed

tocolumn of insert as declared by the 10 rounds . This operation is only available in initial eight rounds.
encryption and decryption steps help to avoid problem of data breach.DNA based AES algorithm increase integrity level of data.This platform will be best using for data security in any stream.

## 6. Conclusion

DNA cryptography is a favorable and fast developing arena in data protection. These kind 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 confer various stage of security along with DNA based AES encryption. Compression method can also be applied with DNA cryptography using AES.It can be used are secure data sensitive data like military purposes.Main purpose use by DNA cryptography has secure share and receive your data.

## 7. Future work

The big tech giants, may take an initiative to commercial- ize DNA computers in near future. Hopefully, in years the practically un-hackable DNA cryptography performance will be an effectual choice to standard cryptosystem. The security of real time information flow among the distributed network system will be area of research.

## References

[1] Bonny B.Raj, Sharmila, V Ceronmani "An Survey on DNA Based Cryptography "International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR) - Ernakulam (2018.7.112018.7.13)] 2018
[2] Saijisha K S ;Mathew,sheena" An encryption based on DNA cryptography and steganography" International conference of Electronics, Communication and Aerospace Technology (ICECA)- COIMBATORE, India (2017.4.20-2017.4.22)] 2017
[3] Roy, Sudipta Singha; Shahriyar, Shaikh Akib; Asaf- Uddowla, Md.; Alam, Kazi Md. Rokibul; Morimoto, Yasuhiko "A novel encryption model for text messages using delayed chaotic neural network and DNA cryptography." 20th International Conference of Computer and Information Technology (ICCIT) - Dhaka, Bangladesh (2017.12.222017.12.24)] 2017 .
[4] K.KALAISELVI "Enhanced AES Cryptosystem by using Genetic Algorithm and Neural Network in S-box 978-1- 50901936-6/16/2016 [5] Panagiotis Papadimitratos". Secure Data Communication in Mobile Ad Hoc Networks" IEEE 0733-8716 [6] Md. RafiulBiswas ; Kazi Md. RokibulAlam ; 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.