ISSN: 2321-7782 (Online)
e-ISJN: A4372-3114
Impact Factor: 7.327

Volume 6, Issue 10, October 2018

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

DNA Cryptography: A Novel Approach for Data Security Using Genetic Algorithm

Madhvi Popli
Research Scholar, Department of Computer Science
Punjabi University
Patiala, India.

***Abstract:** The dependency on computers for Secure communication from one machine to another connected virtually has been grown. Cryptography helps to minimize such data security issues and change information into an unreadable form based on the key. This paper is based on the new technique based on the DNA cryptography along with Genetic Algorithm. Keys are generated using Genetic Algorithms that is considered as one of the most optimization technique. Each letter and the numerical value is encoded and converted into DNA sequence of nucleotides bases (As, Cs, Gs, Ts). In proposed work, a method is introduced for generating a key using Genetic Algorithm and implementation of Encryption and Decryption using DNA cryptography. The proposed method is conceptually based on the translation and transcription of DNA into proteins and implemented at the digital level. The random and unbreakable key is generated using Genetic Algorithm for the encryption process. The Algorithm is completely based on the new cryptosystem where a key is generated using an optimized technique and applied to the text using DNA cryptography. Every individual has unique DNA and the transmission of genes from one generation to another and DNA based algorithms are considered as a revolutionary technique.*

***Keywords:** Cloud Computing; Cryptography; DNA Computing; DNA Cryptography; Genetic Algorithm.*

I. INTRODUCTION

Cloud computing becomes a promising technology by providing on-demand storage and computing services at affordable rates. The modern cloud technologies have changed every one perception regarding infrastructure architecture, development and delivery models. The user needs to pay for the services they used and they can access data and service anywhere/anytime via internet. Today in the information system, security and ethical issues become the most important concern for most of the organizations.

The US National Institute of standards and technology (NIST) defines Cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal effort or service providers interaction [3].In Recent times, owing to the information explosion, information has become a crucial strategic resource and hence the requirement for information security is of utmost importance. The dependency on computers for transmitting information from one machine to another connected virtually has been grown and this also increases the need for security. Secure communication is required for transferring information between a sender and receiver. Many techniques are developed for encoding and decoding plain text in mathematical cryptography.

Cryptography is an art of science for transferring information through a secure channel. So the main purpose is to secure the data from unintended and unauthorized users. Cryptanalysis is a specific task that is run parallel to cryptography in order to break protection technique used in cryptography. So we can say cryptography techniques should be stronger. Cryptography plays a vital role in network security and communication. Cryptography is a fundamental technique that uses some mathematical formulas for converting a message to unreadable form and provide security aspects such as information security, confidentiality, integrity, and authentication. It is a method of sending information in masked form so that only intended receiver can read this message.

A new method is proposed for text encryption and decryption using DNA cryptography. In DNA cryptography text is transformed to nucleotides bases (A, G, C, T). The proposed encryption method is basically based on the translation and transcription of DNA into proteins. The complete decryption process is a reverse procedure of encryption process. The complete method is implemented at the digital level, not at the molecule level, Genetic Algorithm is used for generating a Random and unbreakable key for the encryption process. The Algorithm is completely based on the new cryptosystem where a key is generated using an optimized technique and applied to the text using DNA cryptography.

II. Related Works

Several approaches have been devoted by authors to protect data from intruders using different techniques. Many researchers are working on DNA Cryptography and Genetic algorithm and they are using DNA properties to implement data security algorithms. This section discusses different DNA and genetic techniques used by various authors.

Majumdar et al. [14] proposed DNA based encryption algorithm with 256-bit key is used. Round key selection and message encryption method is used for this algorithm. 256-bit random key is used for encryption. Datta et al.[16] implemented algorithm using genetic algorithm. Pseudo random function is used for encryption and decryption of binary data. Blum Blum Shub PRNG function is used to generate pseudorandom sequence for encryption and decryption method.

Jhingran et al. [17] provides analysis on different image encryption methods used by many authors using genetic algorithms. Author also proposed a modified encryption algorithm using Genetic algorithm and RSA cryptography. Authors in [5] proposed a model where data is encrypted using RSA and hash function is calculated along with the owner finger print. However, the major problem is the key is only managed by data owner. Authors in [6] proposed a Bidirectional DNA algorithm where data is encoded by DNA and converted into ASCII values and later in binary values. The authors in [8,9,10] implements image encryption algorithm using DNA and chaotic maps. The plain image is encoded using DNA matrix and then encrypted using chaotic maps.

DNA based encryption algorithm is proposed by Sukumaran et al.[15]. The encryption algorithm is implemented using a bio-computational technique. DNA steganography and indexing is used along with binary coding rule for making algorithm more secure and increases computational complexities. The algorithm suggested by authors in [7] uses DNA steganography and indexing techniques with binary coding to provide additional layer of security.

A new security concept is proposed by Hammami et al.[18]. The security schema allows the distant users to migrate their data in cloud. Author categorized paper into three levels. First level describes the literature survey of security mechanism used for data security, second level provides the encryption algorithm implemented using DNA cryptography, and the third level presents the security analysis of the proposed work. The algorithm works in two phases; first phase encode data into DNA nucleotides forming genetic information. The second phase is encryption and migration phase. In this genetic codes are further divided into 256 sub-blocks. Sbox is used to encrypt the 256 sub-blocks.

III. Cryptography and DNA Computing

Cryptography is an art of achieving security to protect data from unauthorized access by making it to non-readable by applying encryption at the sender side and transform into a readable form by decrypting it at the receiver side. To ensure the confidentiality of the data encryption is necessary. Cryptography becomes more complex and used advanced mathematical procedures during encryption and decryption processes.

Suppose Person A wants to send the simple message to Person B and Person C in between wants to read that message but could not able to do so as the message is in an unreadable form that is secured using some cryptographic algorithm. The message is simple and can be understood by anyone is called plain-text. The process of converting a simple message to unreadable form which is not understood by all is called encryption and the unreadable form is cipher-text. By use of special knowledge and applying methods, the unreadable form can be converted to plain-text this process is known as decryption.

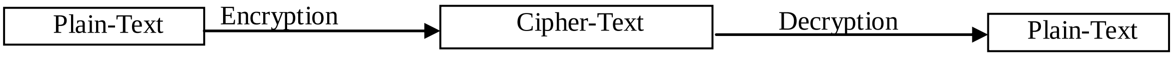


Fig 1: Cryptography

Symmetric and Asymmetric are two main algorithms. The basic difference between the two encryption techniques is the use of secret keys. A Symmetric key algorithm requires a secured exchange of secret keys and uses the same key for encryption and decryption process. These methods are computationally low cost and require fewer resources whereas Asymmetric uses different keys for encryption and decryption process. It uses the public key for encryption and private key for the decryption process. These methods are computationally high cost and require more resources. With the evolution of information technology, network security issues become acute. When a massive amount of data is transferred from one place to another then in that case field of security and encryption become very important. Fig 2 represents the structure for Symmetric Key Process and Fig 3 represents Asymmetric Encryption Process.

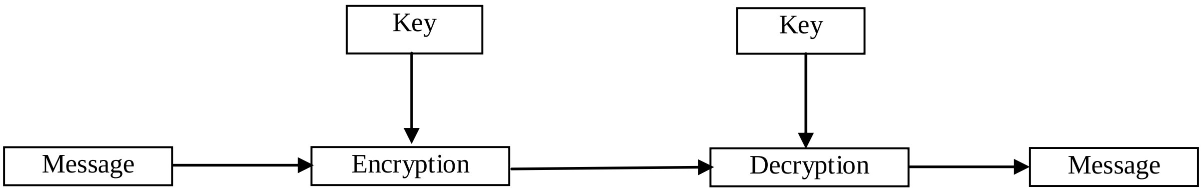


Fig 2: Symmetric Key

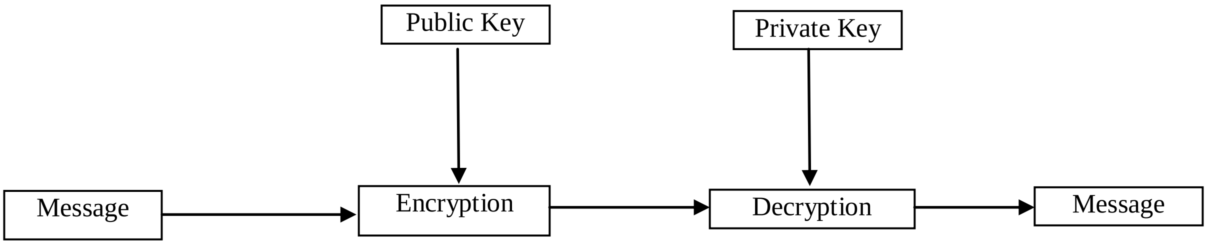


Fig 3: Asymmetric Key

There are various types of cryptography techniques used that are based on difficult mathematical equations. This paper is based on the new technique based on the DNA cryptography with keys are generated using Genetic Algorithms. Genetic Algorithms is considered one of the most optimized techniques used for generating a key for encryption and decryption. When Genetic algorithm and DNA cryptography are used then it produces a new technique that is completely based on biological operations and feasible.

Deoxyribonucleic Acid(DNA) shapes the extinct organism and is incomparable for each individual. DNA cryptography is based on the biological concept of DNA molecules. A single strand of DNA consists of four different nucleotides bases namely A- adenine, G-guanine, C-cytosine, T-thymine. DNA bases generate Complimentary pairs such as A with T, C with G by making bonding by hydrogen bonds. A traditional computer represents information in the form of (0,1) but DNA represents information in the form of (A, G, C, T) that means DNA can store much more information.

Every individual has unique DNA and the transmission of genes from one generation to another. DNA based algorithms are considered as a revolutionary technique based on the surplus features such as large storage capability, ultra-low power consumption and massive parallelism [4]. since DNA uses four strands (A, C, T, G) rather than binary strand (0,1) that means a traditional computer can store much more information. In 1994, Aldeman L. introduces a concept of DNA computation based cryptography. This paper is logically and conceptually based on DNA cryptography where DNA processes like transcription and translation are applied on text for encryption and the reverse process for getting original text.

IV. Genetic Algorithm

Genetic Algorithm is one of the famous evolutionary methods proposed by John Holland in 1975 to solve different optimization problems. It is one of the important soft computing algorithms that play a vital role in generating encryption keys in any type of encryption techniques. Genetic Algorithms are heuristic search based on the theory of natural selection and one of the optimized searching techniques where chromosomes are treated as a main parametric. It deals with the Randomness and randomness increases the security level and are used for generating keys.

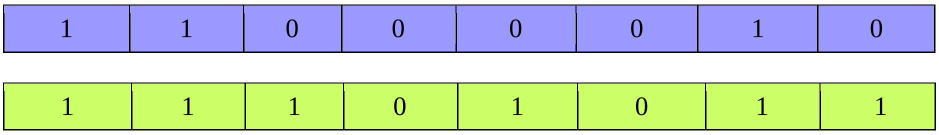
Genetic programming provides a way to create computer program to resolves high-level problems the main difference in the development of sciences and genetic programming is that in case of science development environment are changing permanently without any definite objective while in genetic programming development is defined by fitness functions and genetic programming have unlimited structures for producing fixed length of chromosome to find suitable solutions when searching for a problem.

The algorithm usually starts with a set of solutions usually created randomly and the adaptation of each generation is evaluated by applying fitness functions. Some individuals are selected for the next generation and mutated or crossover to form a new population that is used as new input for the next iteration. The algorithm starts with the population of individuals which are randomly generated. The fitter chromosomes are selected for reproduction based on the probability that is directly proportional to fitness value [12]. To produce offspring, mutation and crossover operations are applied on these chromosomes. Population Initialization, Crossover, and Mutation are basic operations in GAs.

Chromosomes. The first step is to create an initial population randomly from the set of terminals and functions. It is very crucial to determine population size. If the population size is small then it will increase the risk for converging to local minima.[2]

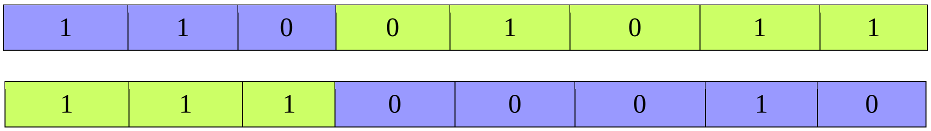
Fitness Function. In order to addresses, the approximate solution of the problems fitness function is used. Fitness function is a key mechanism to determine the quality of the individuals. In this paper, a Run test has been used to evaluate the fitness of random chromosome. It is hard to identify the randomness of any number. By just a simple look no one can say this is random data. The Run test is used to calculate randomness of the number. The procedure of the run test is to calculate the number of runs in the chromosomes. The procedure is based on the number of ones presents in the chromosome that is generated using Genetic Algorithm.

Crossover. In binary chromosomes, two offspring are created by combining two parent chromosomes at random position and new individuals are created by swapping these crossover points. There are several ways of performing crossover. The most common crossover operators are single point crossover and K-Point crossover [12]. In single point crossover, a point is randomly picked on both parent chromosome that is designated as the crossover point. New offspring individuals are generated by swapping the bits to the right of that crossover points between the parents. Crossover lets to find new solutions by making small random changes in the representation. [1] For example in the fig. 3 two parent chromosomes are selected and the crossover point is generated randomly to accomplish crossover and to obtain new offspring. In this example, the crossover point is 3 so the chromosomes are crossed after the third place to produce new offspring as shown in Fig. 4 and Fig. 5.



1	1	0	0	0	0	1	0
1	1	1	0	1	0	1	1

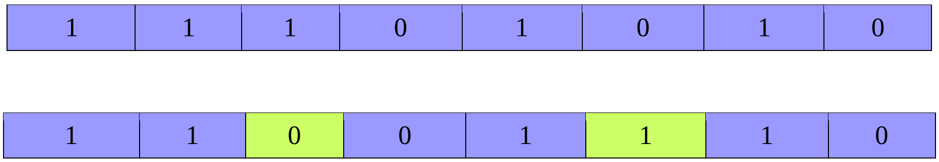
Fig 4: Randomly two chromosomes are selected for Crossover



1	1	0	0	1	0	1	1
1	1	1	0	0	0	1	0

Fig 5: New offspring after Crossover

Mutation. Mutation is defined as the flipping of bits at random position to obtain a new solution. It alters one or more values of the chromosome and solution is entirely changed from the previous solutions. In this, one or more than one bit from the parent chromosome is flipped by converting 0 to 1 or 1 to 0.



1	1	1	0	1	0	1	0
1	1	0	0	1	1	1	0

Fig 6: Mutation by flipping bits

Genetic Algorithm is a powerful randomized search optimization technique that is reliable and follows natural selection. It can be applied to both image and the text.[3] In this paper, the genetic algorithm is applied text only. The algorithm generates the chromosome that as best fitness value that is minimum fitness value. The basic principle of Genetic Algorithm technique is to generate the best chromosome that contains optimize fitness value. The generated chromosome act as a Key1 and this Key1 fitness value is matched against the fitness value of the keys generated and stored in the repository. The key with highest fitness value is act as Key2. Key1 and Key2 are XOR-ed to a create a final key. This final key is stored in the repository and used for encryption and decryption process. The process is iterated over 100 times.

V. Our Proposed Approach

In this paper, Genetic Algorithm generates best chromosomes that contain an optimized value. The Random generator is used to generate random binary numbers which will act as an initial population of chromosomes, Each chromosome has some fitness value which is calculated by applying some fitness algorithm. Randomness factor is the basic principle of generating a unique Key for the encryption process.

A. Key Generation using Genetic Algorithm

Initial Population. An initial population of a binary string is generated using a Random Generator that is known as Chromosomes. In this paper, 100 chromosomes are generated randomly by a random generator. The population is transformed into a new population by applying different methods that occur in Genetic Procedures. The fitness value of each chromosome is calculated by applying the fitness algorithm.

Crossover. Two parent chromosomes are selected randomly from the set of 100 chromosomes. The Crossover uses different ways to produce offspring. In this algorithm, K-point crossover is used for producing two new offspring. Two chromosomes are selected and the k-point crossover is applied on both and calculate the new fitness value of new offspring.

Mutation. Mutation is used to produce a new solution by applying random tweaks in chromosomes. It maintains the diversity in genetic population and usually applied in low probability [11]. A random point is selected for mutation and flipping is applied by changing bit value i.e. 1 becomes 0 and 0 becomes 1 leaving other bits without any change.

Fitness functions calculate the fitness of chromosomes and also increases the possibility of generating better results. The Fitness value is calculated for the new chromosomes.

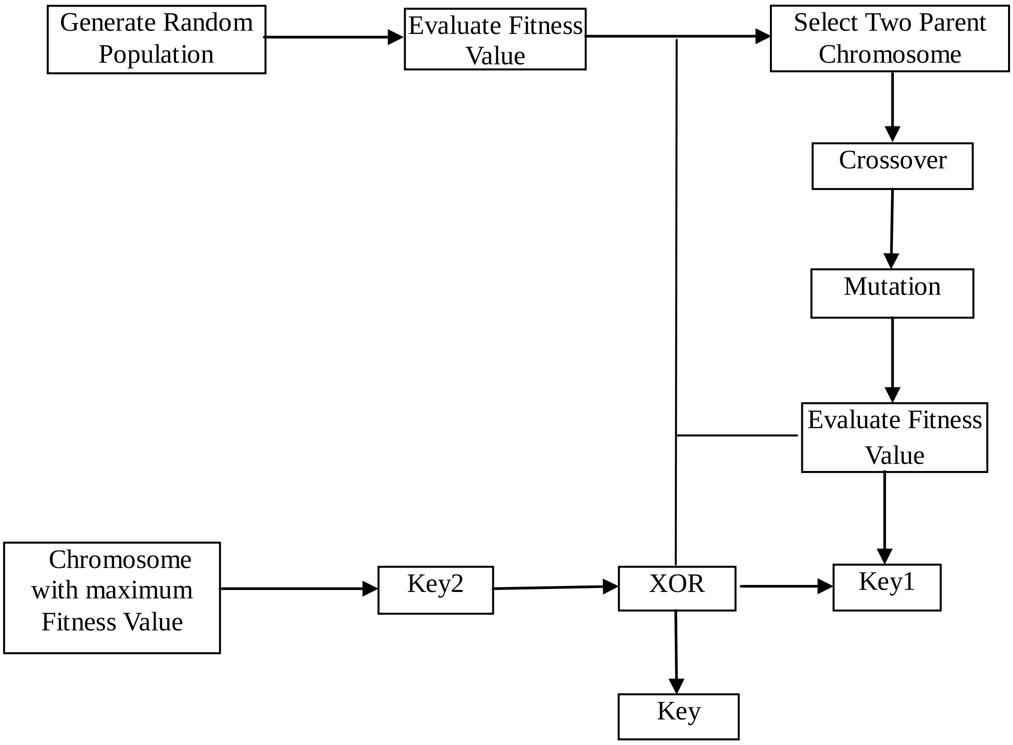

Generate Random Population
Evaluate Fitness Value
Select Two Parent Chromosome
Crossover
Mutation
Evaluate Fitness Value
Chromosome with maximum Fitness Value
Key2
XOR
Key1
Key

Fig 7: Key Generation Process Using Genetic Algorithm

B. *DNA Cryptography with Genetic Algorithm*

Each letter and a numerical value is encoded and converted into a DNA sequence of nucleotides bases (As, Cs, Gs, Ts). The Random sequence of four DNA nucleotide is generated for English alphabets and for numerical digits which means we can utilize these four sequences to encode information which is more than for a traditional computer which only understands binary sequence.

For example, the text “hello world” is encoded in the form of DNA sequence as:

T = CTAGTAGCCTGACTGATGCAGCATTAAGTGCATGCTCTGACATG

TABLE I RANDOM DNA SEQUENCE

Value of a is ATGC	Value of b is TGCA	Value of c is GCAT
Value of d is CATG	Value of e is TAGC	Value of f is AGCT
Value of g is GCTA	Value of h is CTAG	Value of i is GATC
Value of j is ATCG	Value of k is TCGA	Value of l is CTGA
Value of m is CATG	Value of n is ATGC	Value of o is TGCA
Value of p is GCAT	Value of q is TAGC	Value of r is TGCT
Value of s is TAGT	Value of t is GCGG	Value of u is ACCA
Value of v is TAAT	Value of w is TAAG	Value of x is AGAG
Value of y is GGCC	Value of z is GGTT	Value of 0 is TTGG
Value of 1 is AGTC	Value of 2 is ACCT	Value of 3 is TAAC
Value of 4 is CACT	Value of 5 is TACA	Value of 6 is AGGA
Value of 7 is CGGC	Value of 8 is CGCG	Value of 9 is CTTA

After data is encoded in the DNA sequence the data is transcripted into DNA complementary strand. T and T’ represents the text in the DNA and DNA complementary strand. The complementary strand of DNA sequence is shown in the table given below:-

TABLE II COMPLEMENTARY DNA SEQUENCE

DNA Nucleotides Bases	Complimentary DNA
A	U
C	G
G	C
T	A

T = CTAGTAGCCTGACTGATGCAGCATTAAGTGCATGCTCTGACATG

T’=GAUCAUCGGACUGACUACGUCGUAAUUCACGUACGAGACUGUAG

DNA complementary strand T’ is converted into Binary form. The binary form of the sequence is shown in the table given below.

TABLE III BINARY SEQUENCE OF DNA NUCLEOTIDES BASES

DNA Nucleotides Bases	Binary Sequence
U	11
C	01
G	10
A	00

After converting sequence in to binary form the sequence is divided in to blocks of 8-bit each

T’=1000110100110110100001111000011100011011011011000011110100011011000110001000011110110010

T’=10001101 00110110 10000111 10000111 00011011 01101100 00111101 00011011 00011000 10000111 10110010

Right shift each byte by 2 bits each

T’’= 01100011 10001101 11100001 11100001 11000110 00011011 01001111 11000110 00000110 11100001 10101100

The sequence obtained after the right shift is XOR-ed with the key from the repository generated through the genetic algorithm.

01100011	10001101	11100001	11100001	11000110	00011011	01001111	11000110	00000110	11100001	10101100

XOR

01000001	10001111	10101101	11001101	11101101	11111011	11001111	11000111	11110111	10101010	11001100

The result is then converted into decimal and then further converted into equivalent hexadecimal that is equivalent to cipher-text. The final Key is stored inside the repository that is being used for the decryption. The decryption process is just a reciprocal of an encryption process. The cipher-text that is hexadecimal is converted into decimal and then multiply the key which is stored in the repository. The result is then transformed to binary form and then converted into equivalent DNA sequence. The DNA sequence is again mapped to decode into Original Text.

C. *Encryption/Decryption Flowchart for DNA Cryptography with Genetic Algorithm*

The plain text is encrypted using the key that is generated using Genetic Algorithm. The key generation flowchart is shown in Fig 7 and this key is stored in Repository for further use in encryption and decryption process. The text is then encrypted using Key as shown in Fig 8 and Decryption process is an exact reverse process of Encryption as shown in Fig 9

The detailed description and implementation is provided in flowcharts and algorithm is implemented using Python for both key and DNA computation. 100 chromosomes are generated randomly and several operations are applied for generating an optimized key. A Run test is used for the fitness value of the chromosome and it also depicts the randomness. The lowest fitness value chromosome is compared with the highest fitness value chromosome. These two are XOR-ed to obtained final chromosome which acts as a key and stored in the repository. The process is reiterate over 100 times to generate optimized and non-repeatable solution key used for encryption.

A random table for alphabets and numbers are generated using four nucleotides bases A, C, T, G, and plain text is encoded using these bases. The encoded text is further converted into binary form and translation and transcription process is applied on the binary sequence. Key taken out from the repository are applied and convert the text into an encrypted form. The reverse process is applied to the cipher-text to obtained original text.

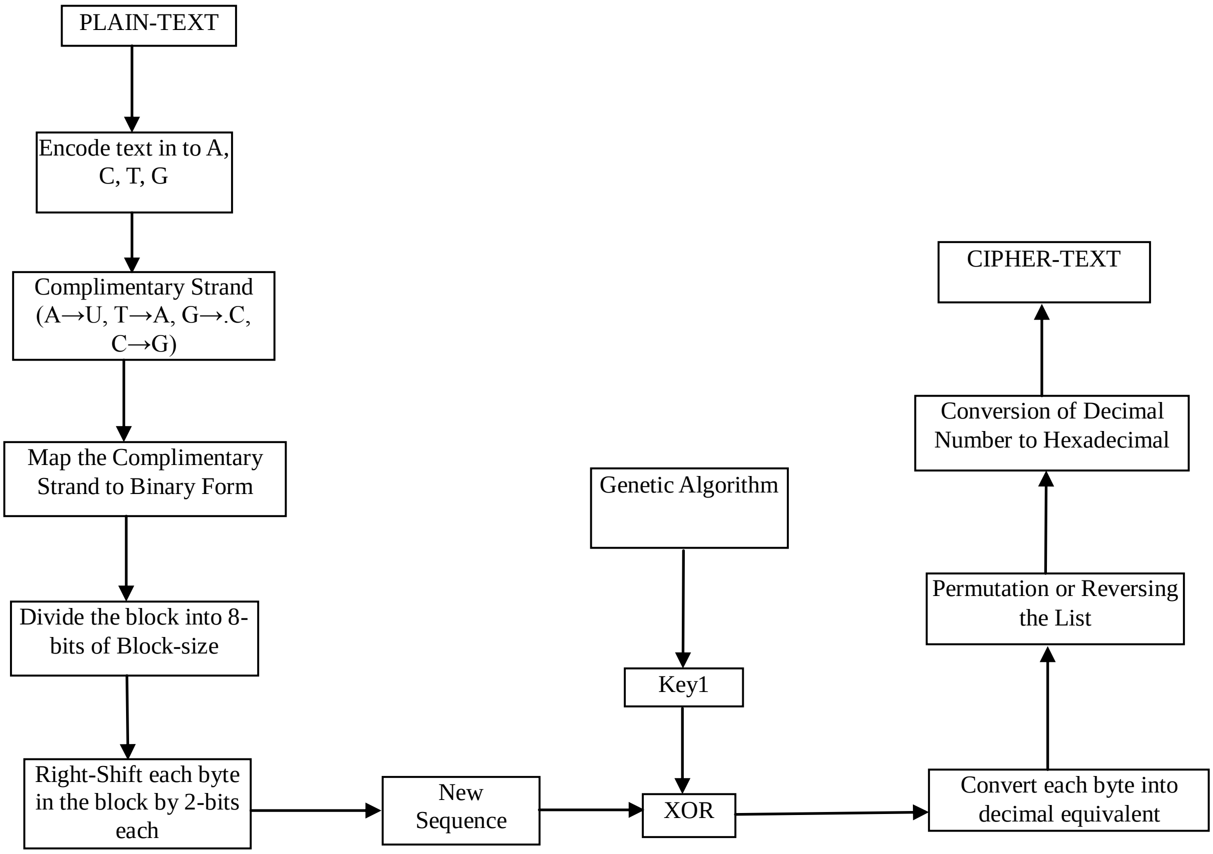

PLAIN-TEXT
Encode text in to A, C, T, G
Complimentary Strand (A→U, T→A, G→.C, C→G)
Map the Complimentary Strand to Binary Form
Divide the block into 8-bits of Block-size
Right-Shift each byte in the block by 2-bits each
New Sequence
Genetic Algorithm
Key1
XOR
Convert each byte into decimal equivalent
Permutation or Reversing the List
Conversion of Decimal Number to Hexadecimal
CIPHER-TEXT

Fig 8: Encryption Process

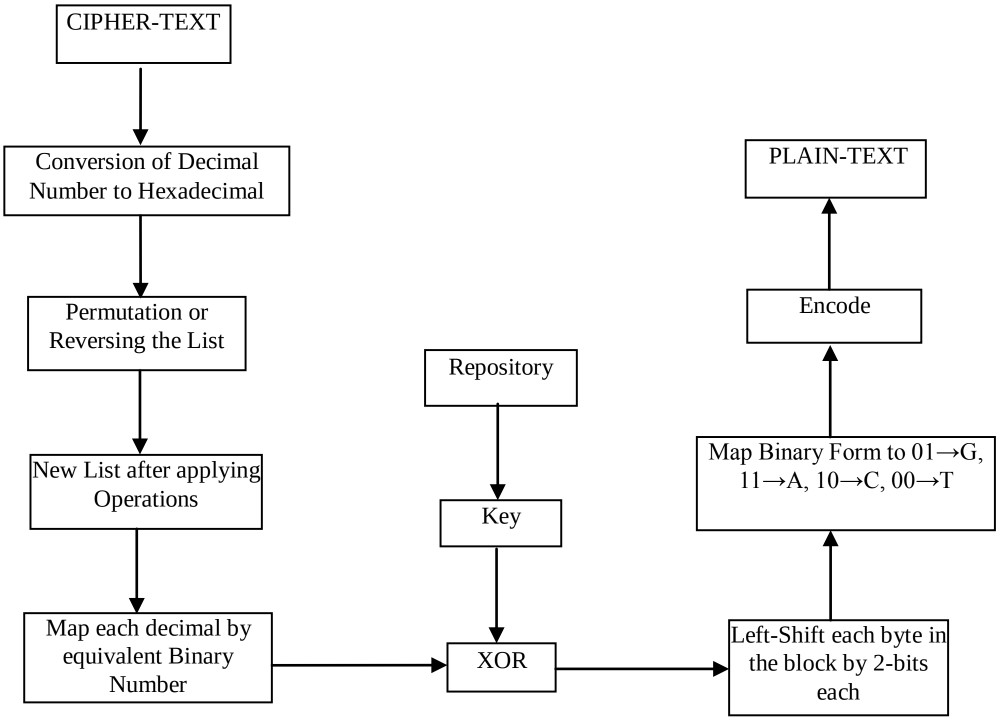

CIPHER-TEXT
Conversion of Decimal Number to Hexadecimal
Permutation or Reversing the List
New List after applying Operations
Map each decimal by equivalent Binary Number
Repository
Key
XOR
Left-Shift each byte in the block by 2-bits each
Map Binary Form to 01→G, 11→A, 10→C, 00→T
Encode
PLAIN-TEXT

Fig 9: Decryption Process

VI. Results

The experimental analysis and detailed description has been implemented using python. A random 100 binary strings are generated that act as initial population and various operations are applied to obtain the final key. The fitness value is calculated using run test and is compared with the other fitness values. Minimum is the fitness value more is the optimized solution. The analysis is done by providing detail of time taken by algorithm for encryption and decryption process.

TABLE IV TIME TAKEN FOR ENCRYPTION AND DECRYPTION PROCESS

File Size	Encryption(ms)	Decryption(ms)
1 KB	0.0113	0.0223
2 KB	0.0243	0.0420
3 KB	0.0331	0.0551

Chi- square test and Cosine functions are calculated to determine the feasibility and the dissimilarity index of the code.

For example, the text "hello world" is taken as input and encoded in the form of DNA sequence as:

T = CTAGTAGCCTGACTGATGCAGCATTAAGTGCATGCTCTGACATG

hello world contains 11 characters and the encoded text contains 44 characters

I. Chi-square value is calculated from the number of characters in encoded text and from the original text chi-square= ((44-11)^2)/(44+11). The value comes out to be 19.8 that means which is not nearer to one that indicates the higher dissimilarity value. Higher is the dissimilarity index more is the feasibility.

II. Cosine test calculate the feasibility and dissimilarity of the method. Cos(44,11) and the value comes out to be 0.9918 which is nearer to 1 as cos lies between [0,1]. so the results shown the method is quite feasible increases the trust factor of users.

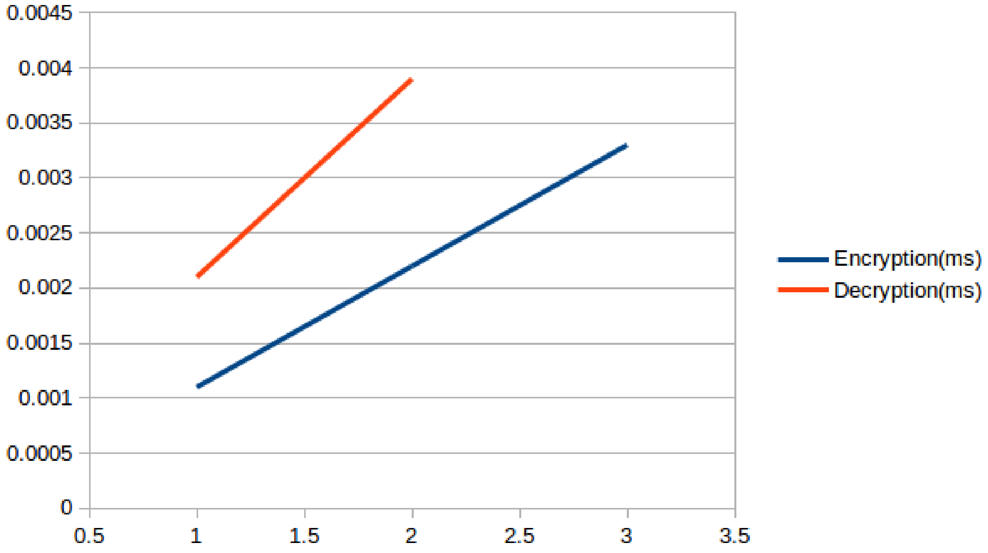


Fig:10 Encryption and Decryption time with File size

VII. Conclusion and Future Work

The modern cloud technologies have changed every one perception regarding infrastructure architecture, development and delivery models. Cryptography is not the mathematical science of transferring data into unreadable form but also getting original data from cipher-text. This paper introduces a concept of DNA cryptography along with the key generation using Genetic Algorithm. Each letter and a numerical value is encipher and converted into a DNA sequence of nucleotides bases (As, Cs, Gs, Ts). In the first method, Data is encoded in the DNA sequence and then transcripted into DNA complementary strand. The complementary strand is further converted into binary digits and operations are applied for generating encrypted text. Randomly 100 chromosomes have generated that act as an initial population. The two parent chromosomes are selected for applying operations such as crossover and mutation and fitness value is calculated. The minimum the fitness value more is the optimized solution. The Key is generated by applying Genetic Algorithm are stored in the repository for further use for encryption and decryption in DNA cryptography.

The work presented in this paper can be summarized in the following points:

A. Literature survey of data security mechanism used by various researchers using DNA cryptography, Genetic algorithm. Through this we have study various research papers published in recent era which inspired us to contribute and to implement in this area.

B. A concept of DNA cryptography is introduced in which key is generated using Genetic Algorithm. Data is encoded and converted in to DNA sequence which are further converted into binary digits and operations are applied on this binary data with the key generated randomly by Genetic Algorithm

C. Finally, result analysis is provided from which we have tried to present that the approach used in this paper is secure and feasible.

The proposed work has increases the level of security because of the randomization. This work is completely based on the random numbers and no one can predict the randomization. The time complexity for encryption and decryption determines the feasibility of the algorithm The security parameters are calculated using chi-square test and cosine functions and they provide the highest dissimilarity index value that indicates the high security and trust factor. The proposed work is a novel encryption approach for storing data in cloud environment. Currently we have mainly focused on DNA cryptography and Genetic algorithm. In future, it might be possible to add DNA cryptography with other soft computing algorithms in order to provide more secure cloud environment.

References

1. Mozaffari Saeed. Parallel image encryption with bitplane decomposition and genetic algorithm. Multimedia Tools and Applications, Springer, 2018, pp 1-21,doi: 10.1007/s11042-018-5817-8
2. Kumar Ankit, Chatterjee Kakali. An Efficient Stream Cipher using Genetic Algorithm. IEEE International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), 2016, pp 2322 – 2326, doi: 10.1109/WiSPNET.2016.7566557
3. Kalaiselvi K., Kumar Anand. Enhanced AES cryptosystem by using genetic algorithm and neural network in S-box. IEEE International Conference on Current Trends in Advanced Computing (ICCTAC),2016, doi: 10.1109/ICCTAC.2016.7567340
4. Chen Junxin, Zhu Zhi-liang, Zhang Li-bo, Zhang Yushu, Ben-qiang Yang. Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption. Signal Processing, Elsevier, 2018,pp 340-353, doi: 10.1016/j.sigpro.2017.07.034.
5. Chidambaram N., Raj P., Thenmozhi K. , Amirtharajan, R. Enhancing the Security of Customer Data in Cloud Environments Using a Novel Digital Fingerprinting Technique. International Journal of Digital Multimedia Broadcasting, 2016, pp 1-6, doi: 10.1155/2016/8789397.
6. B. Ashishkumar Prajapati, Barkha P. Implementation of DNA cryptography in cloud computing and using socket programming. IEEE International Conference on Computer Communication and Informatics (ICCCI), 2016, pp 1-6, doi: 10.1109/ICCCI.2016.7479930.
7. Sukumaran SC, Mohammed Misbahuddin. DNA Cryptography for Secure Data Storage in Cloud.International Journal of Network Security, pp 447-454, 2018, doi: 10.6633/IJNS.201805.20(3).06
8. Kumar, M., Iqbal A., Kumar, P. A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography. Signal Processing, Elsevier , 2016, pp 187-202., doi: 10.1016/j.sigpro.2016.01.017
9. Wang X., Liu, C. A novel and effective image encryption algorithm based on chaos and DNA encoding. Multimedia Tools and Applications, Springer US, 2017, pp 6229-6245, doi: 10.1007/s11042-016-3311-8
10. Chai X., Chen, Y., Broyde L. A novel chaos-based image encryption algorithm using DNA sequence operations. Optics and Lasers in Engineering, Elsevier, 2017, pp 197-213, doi: 10.1016/j.optlaseng.2016.08.009
11. Kalsi S, Kaur H, Chang V. DNA Cryptography and Deep Learning using Genetic Algorithm with NW algorithm for Key Generation. Journal of Medical Systems, Springer, 2018, pp 1-12, doi: 10.1007/s10916-017-0851-z
12. Afarin R, Mozaffari S. Image encryption using genetic algorithm. 8th IEEE Iranian Conference on Machine Vision and Image Processing (MVIP), 2013, doi: 10.1109/IranianMVIP.2013.6780026
13. P. Mell, and T. Grance. The NIST definition of cloud computing. Computer Security Division Information Technology Laboratory National Institute of Standard and Technology Gaithersburg, pp 1-7, 2011
14. Majumder Atanu, Majumdar Abhishek, Podder Tanusree, Kar Nirmalya, and Sharmas Meenakshi. Secure Data Communication and Cryptography Based on DNA Based Message Encoding, IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), pp 360-363, 2014
15. Sukumaran Sreeja Cherillath, and Misbahuddin Mohammed. DNA Cryptography for Secure Data Storage in Cloud, International Journal of Network Security, Vol.20, No.3, pp.447-454, May 2018
16. Dutta Suvajit, Das Tanumay, Jash Sharad, Patra Debasish, and Paul Dr. Pranam. A Cryptography Algorithm Using the Operations of Genetic Algorithm & Pseudo Random Sequence Generating Functions, International Journal of Advances in Computer Science and Technology, Vol. 3, No. 5, pp 325-330, May 2014
17. Jhingran Rajat, Thada Vikas and Dhaka Shivali. A Study on Cryptography using Genetic Algorithm, International Journal of Computer Applications, Vol. 118, No.20, pp 10-14, May 2015
18. Hammami Hamza, Brahmi Hanen, and Yahia Sadok Ben. Secured Outsourcing Towards a Cloud Computing Environment Based on DNA Cryptography, IEEE International Conference on Information Networking (ICOIN), pp 31-36, Janurary 2018, doi: 10.1109/ICOIN.2018.8343079.