ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

A Combined Approach of Cryptography to Enhance the Security Using Traditional DNA and Tree Traversal Technique

Aayushi Saxena[1], Sushil Sharma [2], Lalit Mohan Gupta[3]

M.Tech. Scholar, Dept. of CSE, ITM, Aligarh, India[1]

Asst. Professor, Dept. of CSE, ITM, Aligarh, India[2]

Asst. Professor, Dept of CSE, VCTM, Aligarh, India[3]

ABSTRACT: The present paper is an approach to uplift the impregnability of the system at the time of communication through internet. With the help of this technique one can also become aware regarding the concept of DNA and tree traversal concepts in order to make the system more safe and secure without being accessed by the intruders. The efficiency of security is raised by the tree traversal algorithm which functions in the form of encrypted system for the conversion of original message in a secret form. Therefore, the derived text can be in the form of cipher text that is arbitrary to come out in its original message without having the knowledge of decryption method.

KEYWORDS: Encryption, Decryption , DNA cryptography ,tree traversal security, DNA base pairs

I. INTRODUCTION

In the post modern century, the use of internet services has facilitated all around the globe in a rapid way. Due to the impact of globalization, the demand of modern technology has also attained its utmost height .For this, security has became an imperative issue in the minds of researchers. Presently, there are vivid algorithms proposed by the multiple researchers in order to elevate the security of the system. Security has incline a dominant concern in our day today life. It inculpate communication and network as one of the standard to breach its services like confidentiality, authentication, authorization and integrity. For accommodating the security in our systems, there is a need of some mechanism which cease the intruders to attack them. Security can be violated by interrupting the confidentiality, integrity & availability of a data and the person who attempt to gain access to a system, is an intruder. There are three classes of intruders.1) masquerader 2) misfeasor 3) clandestine user [1]. **Masqueraders** are the person who pretends to be another person and takes a control over the account of authorized person. **Misfeasors** may be an authorized or unauthorized individual who can access the resources, if authorized they take the misuse of his or her privilege**. Clandestine users**, for escaping or avoiding the auditing or to forcibly put an end to the audit collection, an intruder stops the supervisory control of the system. These are the attacks for which the techniques for preventing and controlling them have been established. There are billion or trillion of devices which has been allied to the internet, to communicate and can share the data in a more convenient and efficient manner. But, with the convenience and efficiency another term that has been proposed is security. So, for providing the security there is a need of some major techniques and computational tools which oversight the vulnerabilities of the system. There are multiple techniques had been disclosed in order to secure data transmission by putting it together either with the help of DNA cryptography or by using tree traversal approach and distinct techniques had been put together using either the DNA cryptography or using the tree traversal approach. One prominent issue in the era of internet is the data transmission. Transmission is simply means to transfer information from one system to another. But the term which is utmost significant for the transmission is “security” i.e transferring of data which is confidential data over a secure channel. For this, we adopt the cryptography techniques which is the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

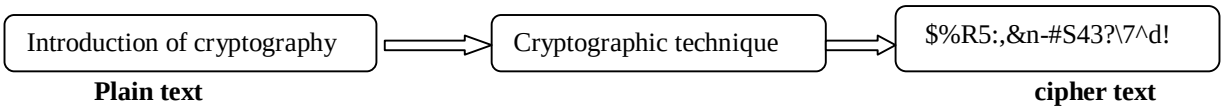
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

combination of both encryption and decryption methods. There are vivid symmetric key Algorithms [11]having same key for transmitter & the receiver for encryption and decryption such as AES, SHA-2, 3DES, RC4[12] and asymmetric key algorithms such as RSA[12]etc which doesn't provide a complex technique for augmenting security in our systems.
AES: It is also known as Rjindaels's algorithm. The formation of this algorithm is done by Vincent Rijmen and Joan Daemon in 1998. Two hashing algorithms are used SHA1 and MD5
SHA-2 :It is one of the hash function that provide the security services in integrity and with some changes in message size, word size, security bits, message hash size shares the similar functional structures.[10]
RSA: This algorithm is designed by Rivest, Adi Shamir and Leonard Adleman in 1977.It is one of the asymmetric pubic key cryptography system having different keys for encryption & decryption.
All those are the algorithms that foster the mathematical techniques but weakens the robustness of the cryptosystem which directly or indirectly hamper the security challenges. For yielding a more desirable functionality and more security we presume about a new data structure acknowledged as a TREE. A tree is a non linear data structure which uses the hierarchical order to carry out more enhanced complexity in clefting the cipher text. Exclusive tree has a special data item called as a root of the tree and respective node except the root node has their children. There are varied types of binary trees and distinct operations may enforce on binary tree .One of the utmost considerable operation is the TREE TRAVERSAL approach .Using tree traversal ,we can visit to each and every node exactly once in a precise manner.
There are three ways of binary tree traversal : 1)PREORDER 2) POSTORDER 3) INORDER
The following operations of traversal work or traverse a node as follows:
PREORDER: Root Left Right, INORDER: Left Root Right, POSTORDER: Left Right Root
With the support of tree traversal we audit or update every node in systematic order. Many researchers put an effort on tree traversal for procuring the high level of security in encryption and decryption.

CRYTOGRAPHY=ENCRYPTION+DECRYPTION



DNA(Deoxyribonucleic acid) is an hereditary substantial in human being and it is a key storage medium. The three-dimensional structure of DNA was explored in 1953 by Watson and Crick DNA is a double helix structure containing a base pairs. Helix is a curve in three dimensional aspect like a coil springs. A helix structure plays a vital role in the augmentation of secure data hauling. There are 4 chemical bases in which the information is stored in A, T ,C, G where A is Adenine is thymine, C is cytosine is guanine. A term base pair is used in which the bases frame a pair with each other i.e A with T and C with G to **f**orm a unit[6].DNA molecule has a two strands that are twisted all over each other like a twisted pair wire. When we avail a biological structure and amalgamate it with technical accession then the security as well as storage capacity of the system has been elevated.DNA approach having a helix structure assists in inventoring the authentic or a plain text into cipher text. By using the DNA in cryptography, we can conceal and store our data in a compact form. Vivid researchers recommend encryption techniques using DNA that remains static in the field of cryptography which is in course for the unique innovations and to retain security for the further encryption and decryption on the system.

II. LITERATURE SURVEY

Zhang Yunpeng [3] proposed an index based symmetric DNA encryption algorithm in which each and every character is encoded in ASCII characters and using nucleotide sequence it will converted into DNA coding and provide encryption by using key, created by a key generator.
Biphash Roy, Gautam rakshit [4]proposed an improved symmetric key cryptography with DNA based strong cipher in which the primary cipher obtained after encryption is divided into three unequal parts and to obtain the final cipher text

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

,the cipher is added by primer code, authentication code, integrity code file type code. The method proposed is much stronger by having a partial information contained in cipher text.

Emtious Md sazzad Hossain, Kazi Md. Rokibul Alam[5] proposed a dynamic DNA sequence table which assigns DNA sequence table for random ASCII characters.

Fasila K.A, Deepthy Antony [6] proposed a hybrid cryptosystem which is a combination of the encryption and key encapsulation mechanism and enhanced the security using strong key using DNA steganography. DNA stegnography is also used for encapsulation on the strong key for elevating the security. Some of the DNA techniques are used, like coding. In this technique, the cipher text is converted to colors which improves the level of security.

Bonny B Raj, Panchami V[14] proposed DNA based cryptography using permutation and random key generation method.

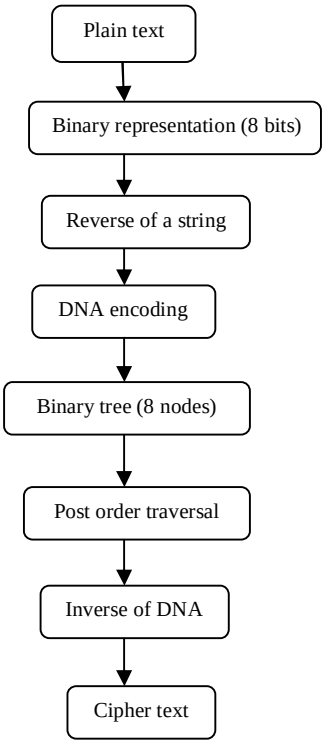
L.Eshwara Chandra Vidya Sagar proposed Data Security using tree traversal [7]in which BFS mechanism is used to arrange the original text to get a tree structure and apply any tree traversal scheme for encryption.

Sumit Sharma, Mrs. Shobha Bhatt[8] proposed encryption of message block using binary tree in block cipher system in which the binary tree concept is used to make the block cipher more complex for proving more security in encryption and decryption techniques. It shows that, using the binary tree for performing the encryption on the original text will converts or doubles the size of the cipher text (8 bytes into 16 bytes) and the cipher text length is equal to the length of the plain text, hence in this introduced algorithm, the cipher system increases the complexity and maintains the complications for the intruders to attack on the system.

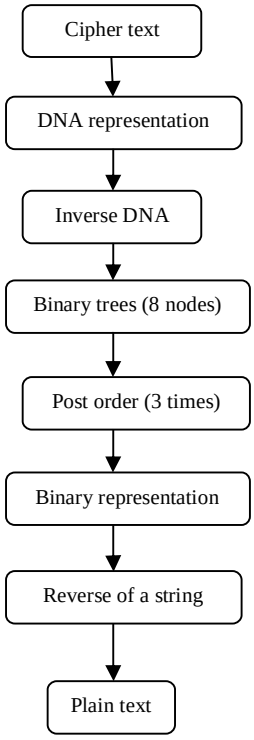
Sivakumar T,Humsharavarthini K, Jayasree M, Eswara M, proposed[9] data encryption using binary tree traversal which is having two level achieving of encryption ,by substitution and permutation.

Mansi Rathi, Sheryas Bhaskar Proposed [15], Data Security using DNA Cryptography, International Journal of computer science & mobile computing, vol.5, issue 10, pg. No 123-129, Oct. 2016

FLOW CHART:



ENCRYPTION PROCESS



DECRYPTION PROCESS

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

III. PROPOSED CRYPTOGRAPHY METHOD

The proposed cryptography method presents a contemporary way of encoding and decoding the data, through which we can relish our day to day entertainment with the cooperation of internet in a more impregnable manner. Hence, intension is to propose the tactic to assure the information. In this paper, we are using the amalgam of both the approaches i.e. DNA cryptography and one of the tree traversal operations. Tree traversal grants to traverse each node exactly once [13].

In this proposed method, we can take 4 nodes but we have taken 8 nodes for performing post order tree traversal which will have the maximum swapping of the nodes and it will serve more security for the sender in the transmission of the data to the receiver. we can perform tree traversal approach as pre order or in order also but both of these approaches will not provide the better security as comparing with the post order tree traversal.

Procedure for encryption by taking an example:

ENCRYPTION:
Step 1: Here, we are taking a plain text or an original text is "CODE" which has to be converted into a secure cipher text.
Plain text="CODE"
Step 2: By using the table of **ASCII** (**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange), find the ASCII values for the alphabets C,O,D ,E.
C=67, O=79, D=68, E=69
Step 3: Convert the ASCII values into 8 bit binary representation.
C=01000011, O=01001111, D=01000100, E=01000101
Original string=01000011010011110100010001000101
Step 4: Reverse the original string.
Reverse string=10100010001000101111001011000010
Step 5:using the base pairs of DNA, perform DNA encoding
Base Pairs: A=00, T=11, C=10, G=01
Coding= C C A C A C A C T T A C T A A C
Step 6: Constructing a binary tree having 8 nodes containing information in encoded form of DNA base pairs .
Binary tree:

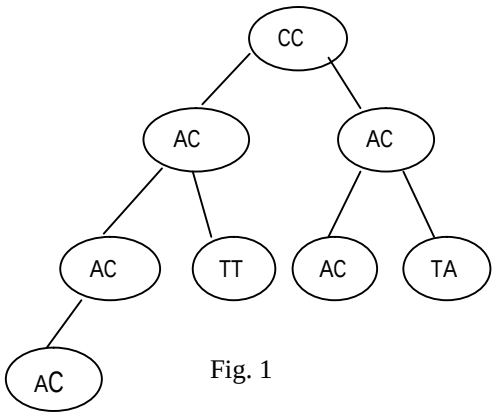


Fig. 1

Step 7: Find the post order tree traversal of a given binary tree.
Post order=LEFT RIGHT ROOT
POST ORDER of a binary tree: A C A C T T A C A C T A A C C C

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

Step 8: Exchange the base pairs of DNA with each other as:

A⟺T C⟺G

DNA Inverse: T G T G A A T G T G A T T G G G

Step 9: Hence, we get the Cipher text, is the encoded form of the original or the plain text and the message send by the sender to the receiver is the :

Cipher text: 1101110100001101110100111101010 1

DECRYPTION PROCESS:

Step 1: Receiver receives a cipher text as:

Cipher text: 1101110100001101110100111101010 1

Step 2: Convert this cipher text into the DNA base pairs representation:

DNA representation: T G T G A A T G T G A T T G G G

Step 3: Take an inverse of DNA base pairs

DNA INVERSE: A C A C T T A C A C T A A C C C

Step 4: Representation of DNA inverse in the form of 8 nodes of a binary tree .

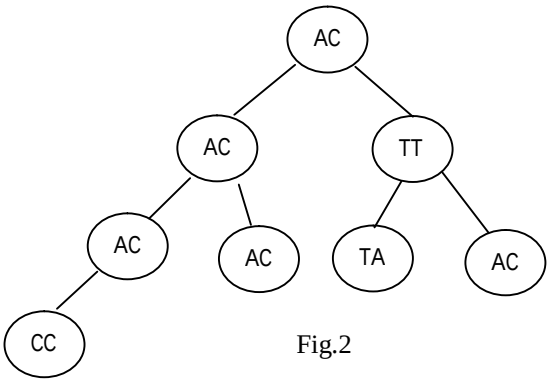


Fig.2

Step 5: Take a post order of a tree for three times to get the original sequence.

Post order 1: C C A C A C A C T A A C T T A C

Post order 2: A C A C T A A C A C T T A C C C

Post order 3: C C A C A C A C T T A C T A A C

Step 6: Give the binary representation of final post order of a binary tree.

Final post order: C C A C A C A C T T A C T A A C

Binary representation: 10100010001000101111001011000010

Step 7: Reverse of a string of binary representation.

Reverse string: 01000011010011110100010001000101

Step 8: Cipher text is converted into plain or original text using ASCII codes.

Plain text: C O D E

IV. COMPARATIVE SECURITY PERFORMANCE USING ALL TREE TRAVERSAL

Here, we are representing the comparison study of all three tree traversal approaches applying on a binary tree. Security is one of the vital issue in the field of computer science. So, there is a need to provide an efficient and more secure approach of traversing which is complex to breach the security.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

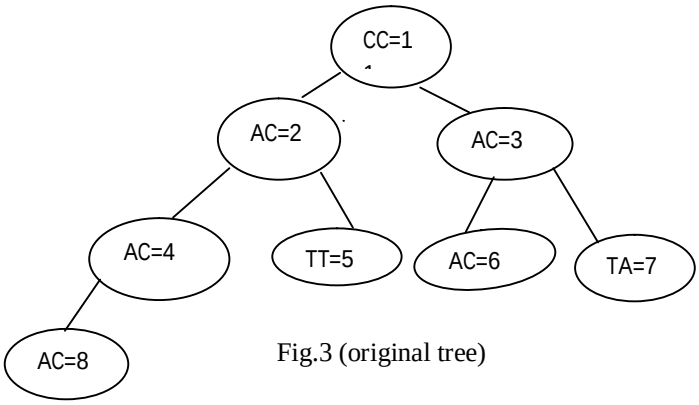


Fig.3 (original tree)

Original text = CC AC AC AC TT AC TA AC
1 2 3 4 5 6 7 8

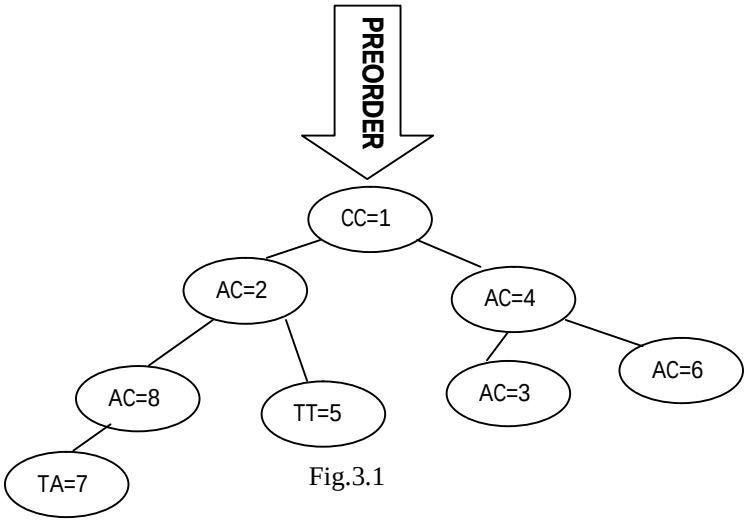


Fig.3.1

Pre order= CC AC AC AC TT AC AC TA
1 2 4 8 5 3 6 7

Comparing both sequence of original tree and pre order of original tree is given below:

1 2 4 8 5 3 6 7

Here, we observe that the positions of some of the nodes don't change its position like 1, 2 & 5 remains in the same position as in the original tree. So, the security is not as much sufficient, it will be easy for intruders to breach it.

For Inorder:

Original text = CC AC AC AC TT AC TA AC

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

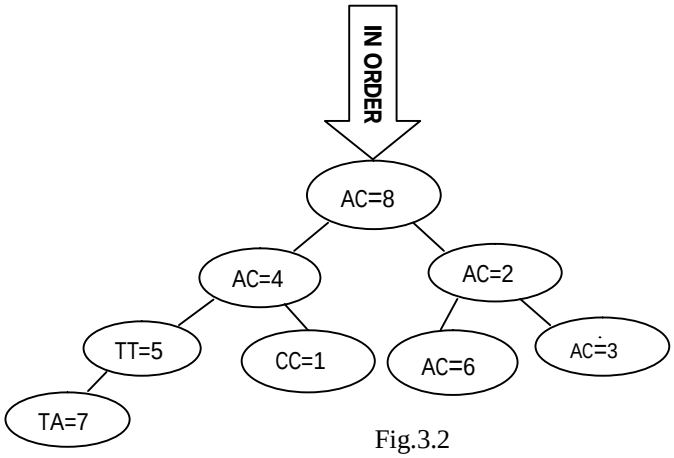


Fig.3.2

1	2	3	4	5	6	7	8
⇩	⇩	⇩	⇩	⇩	⇩	⇩	⇩
8	4	2	5	1	6	3	7

Comparing both the sequences of original tree and Inorder tree of an original tree is mentioned underneath:
We conclude that by using the in order on original tree, we get 6th node at the same position in the applied in order binary tree . So we didn't get strong security, which will be typical for intruders to find the original text .

For post order:
Original text = CC AC AC AC TT AC TA AC

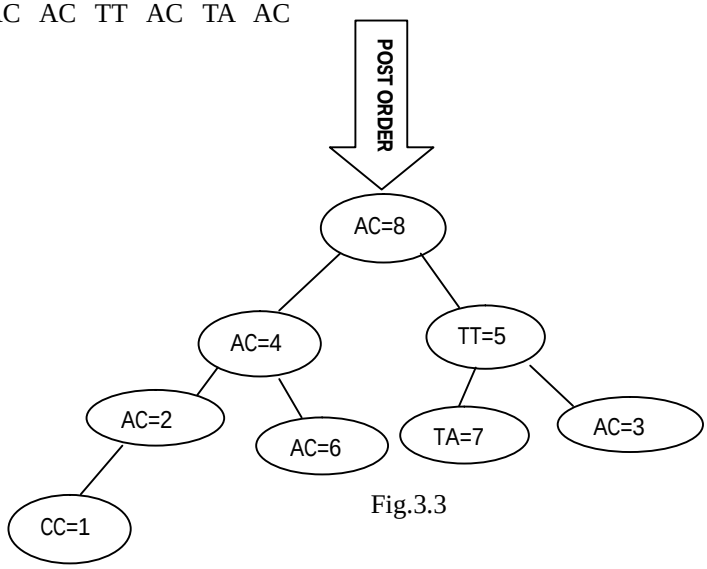


Fig.3.3

By applying the post order on original binary tree, we get the result which provides optimal solution for our security. Post order traversal is one of the major approach in which each and every node has a different position and do not have the similar position as in a binary tree.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

V. SIMULATION AND RESULTS

TABLE 1

DATASET FOR TESTING ON VARIABLE SIZE NODES:

	TYPE OF TREE TRAVERSAL APPROACH	NUMBER OF NODES HAVING CHANGED POSITION AFTER APPLYING TREE TRAVERSAL	PERCENTAGE OF SECURITY (100%)
TEST FOR 4 NODES	pre order	2	50
	In order	3	75
	Post order	2	50

	TYPE OF TREE TRAVERSAL APPROACH	NUMBER OF NODES HAVING CHANGED POSITION AFTER APPLYING TREE TRAVERSAL	PERCENTAGE OF DIFFERENT NODES (100%)
TEST FOR 8 NODES	Pre order	5	62.5
	In order	7	87.5
	Post order	8	100

Here the percentage of different nodes while applying tree traversal also shows the amount of security.

PERFORMANCE ANALYSIS OF PROPOSED ALGORITHM:

The comparisons between the tree traversal approaches have been interpreted in the above obtained datasets of TABLE, which provides a graph given below. This graph shows that the encryption is much stronger by using post order tree traversal approach. Post order presents the extravagant behavior when applied to the nodes on the original tree. When we apply all three tree traversal on 4 nodes, we observe that a tree shows minor swapping of nodes as correlate the traverse by using 8 nodes. Hence, the security is more in post order for 8 nodes.

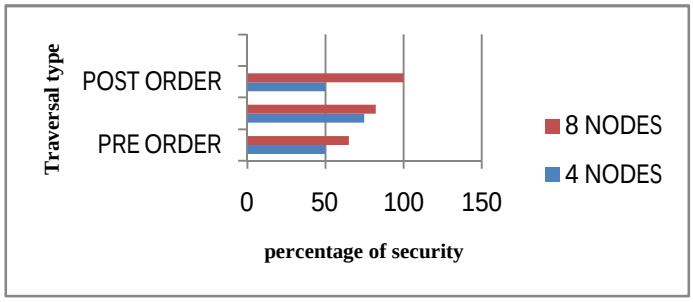


Figure 4. Percentage of security using 4 and 8 nodes

TABLE 2.

RUNTIME ANALYSIS ON VARIABLE LENGTH OF ORIGINAL FILE SIZE (KB) OF PROPOSED ALGORITHM:

S.NO	ORIGINAL FILE SIZE(KB)	CIPHER SIZE(KB)	ENCRYPTION TIME(ms)	DECRYPTION TIME(ms)
1.	1029	4103.7	3142	7591
2.	2058.01	8207.45	4164	7603
3.	3087.02	12311.18	6750	7716
4.	5129.36	20456.14	15185	15050

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

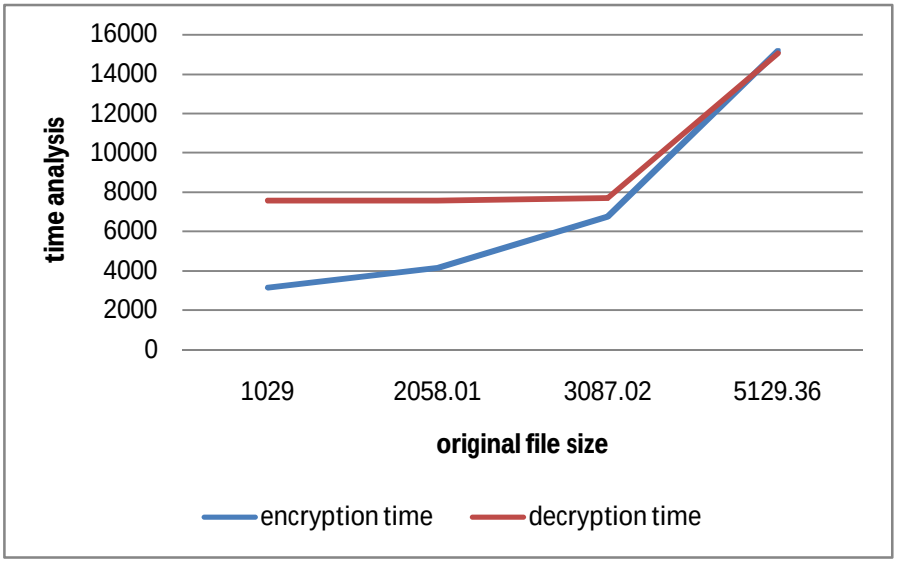


Figure 6. Encryption time vs decrypt time based on file size

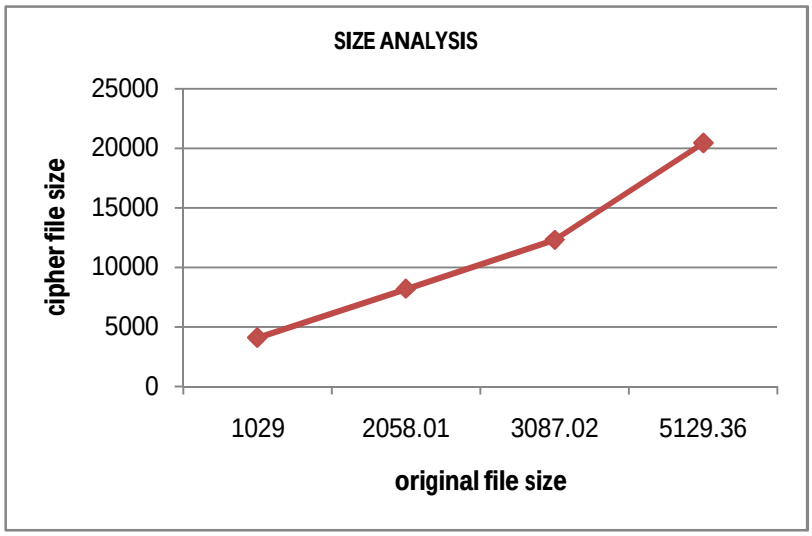


Figure 5. Original file size vs cipher file size

VI. CONCLUSION

The proposed cryptography approach included both the concepts of DNA & tree traversal cryptography . This approach is used to enhance the security more and more. Applying the DNA base pairs on a string, designing a binary tree and performing a tree traversal, became a complex structure for attackers to know the original plain text. All these steps shows that the new approach is suitable for providing security of data between transmitter and receiver in an integrity manner. We test the performance of our algorithm in terms of efficiency by running the plain text having different file size. We observe that the size of the cipher text becomes 3.988 times greater than the original file size.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 2, February 2019

Proceeding the paper, next we are trying to establish an algorithm in which we can minimize the size of our cipher text.

REFERENCES

[1] Stallings .William, "Cryptography & network security principle & practices", Prentice Hall:/PEARSON,Ed.4, 2006
[2] Kahati. Atul,"Cryptography & network security",Tata Mc Graw Hill,Ed.2,2008
[3] Zhang Yupeng, ,Zhu Yu, Wang Zhong ,Richard O. Sinnott, Index- Based Symmetric DNA Encryption Algorithm ,IEEE 4rth International congress on Image and signal processing,2011
[4 Bipash Roy, Gautam Rakshit, Pratim singha, Atanu Majumder, Debarata Datta," An improved symmetric key cryptograqphy with DNA based strong cipher" 978-1-4244-9190-2,2011,IEEE
[5] Emitous Md.Sazzad Hossain,Kazi Md.Rokibul Alam,Md.Raiful Biswas, Yasuhiko Morimoto,"A DNA Cryptographic Technique Based on Dynamic DNA Sequence Table",19th international conference of computer and information technology, Dec 18-20,2016,pg no.270-275
[6] Fasila K.A, Deepthy Antony, A Multiphase Cryptosystem With Secure Key Encapsulation Scheme based On Principles of DNA Computing, Fourth International Conference On Advances In Computing And Communication, IEEE, Pg.No 1-4, 2014
[7] L.Eswara Chandra Vidya Sagar, "Data Security Using Tree Traversal ",Global journal of computer science and technology (C) ,volume 15, issue 3.0 version 1,pg no.19-21, 2015
[8] Sumit Sharma, Mrs.Shobha bhatt," encryption of Message Block Using Binary Tree In Block Cipher System: An approach" International Journal Of Science technology & Engineering",vol 2,Issue 01, pg no.114-119, July 2015
[9] Sivakumar T, Humshavarthini K, Jaysree M, Eswaran M," Data Encryption using Binary Tree Treaversal",3rd International conference on latest trends in engineering science,humanities and management, pg no.151-160, 2017
[10] R. Guesmi, M.A.B. Farah, A.kachauri,M.Samet," A novel chaos based image encryption using DNA sequence operation and secure hash algorithm SHA-2" published on 14 sep 2015,springer publications
[11] N. Kumar and S.Agrawal," An efficient and effective loseless symmetric key cryptography algorithm for an image", 2014 IEEE international conference on advance in engineering & technology research (ICAETR-2014),Unnao,2014,pg no.1-5
[12] Ms Rashmi N, Dr Jyothy K,"An Improved Method For Reversible Data Hiding Stegnography Combined With Cryptography", proceeding of the second international conference on inventive systems and controls(ICISC 2018) IEEE,pg no.81-84
[13] Seymour Lipschutz, "Data Structures", Tata Mc Graw Hills, schaum's outlines
[14] Bonny B Raj,Panchami V," DNA based cryptography using permutation and random key generation method", International conference on innovative research in Science, Engineering and technology[IC-IASET 2014],vol.3,pg no.263-267, 2014
[15] Mansi Rathi, Sheryas Bhaskar, Data Security using DNA Cryptography, International Journal of computer science & mobile computing, vol.5, issue 10, pg. No 123-129, Oct. 2016