International Journal of Science Engineering and Advance Technology

A Novel DNA Encryption Technique Using Efficient Key Generation Method For Secure Data

[1.]Mrs. Ardhani Siva Sravanthi [2.]S. Sushma
[1,2] Dept. of CSE, Kakinada Institute of Engineering and Technology for women, Kakinada

ABSTRACT:

Information innovation is creating orderly, meanwhile security of information is genuine concern. There are diverse customers and affiliations who need to keep their vital data from attackers and software engineers. Diverse cryptographic systems are made in past years. Another field of cryptography is ascending in perspective of DNA figuring on account of high stockpiling cut-off, limitless parallelism and phenomenal vitality capability of natural DNA. This field is in starting stage so an extensive measure of investigation must be done yet. In this we are showing a DNA encryption methodology in light of cross section control and secure key time arrangement.

KEYWORDS: Overlay network, resource allocation.

I. INTRODUCTION:

DNA cryptography is another promising heading in cryptography ask about that rose with the progression of DNA figuring field. DNA can be used to store and transmit the information, and also to perform computation. The expansive parallelism and exceptional information thickness inbuilt in this particle are abused for cryptographic purposes. A couple DNA based calculations are proposed for encryption, verification and so on.

Cryptography is considered and it has attempted to make sense of the stray pieces of DNA Cryptography that how DNA cryptography field created and how DNA computational method of reasoning can be used as a piece of cryptography for encoding, securing and transmitting the information i.e. the claim to fame of cryptography security to make anyone message confounded by encoding it. It has been shown that how DNA cryptography uses DNA as the computational instrument with different sub-nuclear routines to control it close by distinctive algorithms for encryption.

For applying cryptography operations, data can be encoded to DNA groupings. In the essential encryption handle, a message or data is taken as a DNA strand and DNA cryptography strategies are connected on it to change information into cipher content. A definitive target is to scramble information in the way that the individual who doesn't know the key, can't read or alter information. In DNA cryptography, message is encoded as DNA nucleotide succession. Utilizing DNA steganography any data can be covered up by blending DNA strands with other DNA strands like customary calculation where data is stow away inside another medium or document, for example, picture, sound or video[6]. A few procedures are utilized for DNA steganography and cryptography, for example, DNA advanced coding.

Due to nonappearance of continuous executions of DNA based structures; it is illogical to do positive relationship of conventional cryptography and DNA cryptography. As showed by couple of properties of DNA, a general relationship can be presented. To the extent limit DNA is much capable than silicon based structures. For beneficial use of DNA in enrolling and cryptography silicon chips can be supplanted by DNA chips or bio-chips future.

II. RELATED WORK:

As of late few works are proposed by scientists on DNA cryptography and steganography. Viviana I. Risca proposed a DNA steganographic strategy in which DNA scrambled message strand is put between mystery preliminaries and covered up in a microdot. Ashish gehani et al introduced techniques in light of one-time cushions; one is substitution strategy where pair astute mapping is performed between plaintext word and figure word. He likewise exhibited another thought of DNA chip-based technique for encryption and decoding for 2D picture with one-time cushion furthermore proposed an enhanced DNA steganography framework by diminishing the distinction between the plaintext and distracter strands. Monica borda et al proposed new techniques for secret composing by DNA hybridization, DNA chromosome indexing and DNA XOR OTP encryption utilizing tiles. Pankaj Rakheja planned another system by coordinating DNA figuring in International Data Encryption Algorithm. D.Prabhu and M.Adimoolam Bi-serial DNA Encryption Algorithm taking into account number change, DNA coding, PCR enhancement and XOR operation. These calculated

works can be helpful in the advancement of this new conceived innovation of cryptography to satisfy the future security necessities.

III. LITERATURE SURVEY:

THE AUTHOR, Lenuta Alboaie, (ET .AL), AIM IN [1] elective security routines in view of DNA. From the accessible option security routines, symmetric DNA calculations were created and executed. The principal symmetric DNA calculation was executed in the Java dialect, while the second DNA calculation was actualized in Bio Java and MatLab. Examinations have been made between the exhibitions of distinctive standard symmetrical algorithms and the DNA proposed algorithms. As another stride to upgrade the security, a topsy-turvy key era inside a DNA security calculation is displayed. The lopsided key era calculation begins from a secret word phrase. The uneven DNA algorithm proposes a component which makes utilization of more encryption innovations. In this manner, it is more dependable and more intense than the OTP DNA symmetric algorithms.

THE AUTHOR, Grasha Jacob (ET .AL) AIM IN [2], with the development of mechanical advancements, the dangers managed by a client become exponentially. Consequently security has turned into a discriminating issue in information stockpiling and transmission. As conventional cryptographic frameworks are presently vulnerable against attacks, the idea of utilizing DNA Cryptography has been distinguished as a conceivable innovation that presents another trust in unbreakable algorithms. This paper dissects the distinctive methodologies on DNA based Cryptography.

IV. PROBLEM DEFINITION:

Lately few works are proposed by scientists on DNA cryptography and steganography. Viviana I. Risca proposed a DNA steganographic strategy in which DNA encoded message strand is set between mystery ground works and covered up in a microdot. Ashish gehani et al displayed techniques in view of one-time cushions; one is substitution strategy where pair shrewd mapping is performed between plaintext word and figure word. He additionally showed another thought of DNA chip-based technique for encryption and decoding for 2D picture with one-time cushion furthermore proposed an enhanced DNA steganography framework by decreasing the distinction between the plaintext and distracter strands. Monica borda et al proposed new techniques for mystery composing by DNA hybridization, DNA chromosome indexing and DNA XOR OTP encryption utilizing tiles. Pankaj Rakheja composed another system by coordinating DNA figuring in International Data Encryption Algorithm. D.Prabhu and M.Adimoolam Bi-serial DNA Encryption Algorithm taking into account number transformation, DNA coding, PCR intensification and XOR operation. These calculated works can be valuable in the advancement of this new conceived innovation of cryptography to satisfy the future security necessities.

V. PROPOSED APPROACH:

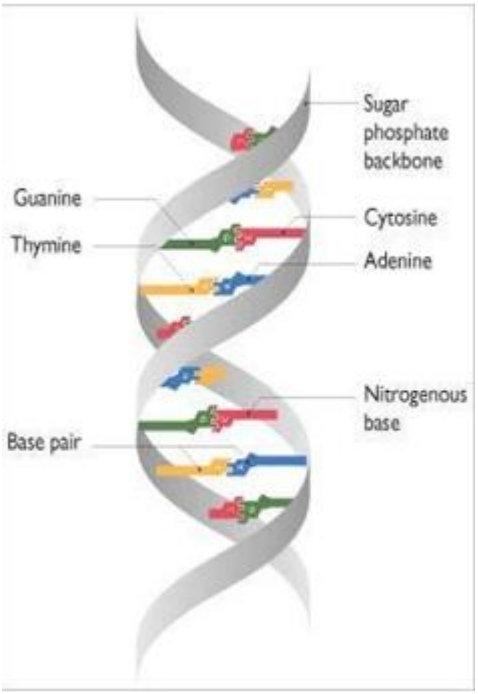
We planned a DNA encryption method taking into account matrix controls and utilizing a key era plan which makes information much secure. Here instant message is changed over to ASCII code and put in a 4*4 matrix. On this matrix, numerical control and scrambling is performed in cycles and XOR operation is performed with the beginning key in every cycle to scramble information legitimately to make message non-lucid.

A safe key era plan is likewise utilized as a part of this encryption framework. Utilizing produced key we XOR the consequence of matrix control to create smaller than normal cipher. The advantage of utilizing this plan is that it generally creates distinctive figure content for same message content and notwithstanding for same key. So it doesn't give any insight or clue to make surmises about plain content.

DNA computerized coding is performed on the smaller than usual figure result to create DNA nucleotide based codes which are as A, C, T and G. Preliminary sets are utilized as keys to change the nucleotide arrangement. Amino corrosive succession is created utilizing DNA codes as a last figure content. This succession to some degree helps sequestered from everything the presence of DNA coding utilization from aggressor. Along these lines this outline gives a straightforward and secure framework taking into account lattice calculations. The utilization of 2 keys like beginning key, created key in light of our plan makes encryption prepare much productive. This new instrument depends on the blend of scientific and organic operations and ideas.

In our proposed framework there are two sections of our system. To begin with part fits in with scientific controls of information matrix while second part fits in with DNA encryption process where DNA advanced coding adjustment is performed to make information secure.

VI. DNA STRUCTURE:



VII. PROPOSED METHODOLOGY:

CIPHER TEXT GENERATION:

In first part of encryption process, up to 128 bit data and 128 bit key can be processed. In the first step original plaintext is converted to ASCII codes, after that data is placed in a 4 X 4 data matrix. Matrix manipulation operation is performed in cycles where first of all row shifting is performed as operated in AES algorithm.

In each cycle after matrix manipulation, XOR operation is performed between the results of first three steps of cycle with the initial key. This cycle is based on the length of initial key. If the length of initial key is n then the number of cycles will be equivalent to 2*n. The output of matrix manipulation cycle is XORed with result of first part of our algorithm. Mini cipher will be always different for same plaintext and same key because of our secure key generation scheme. This feature makes data safe because it does not give any hint due to its different outputs. In the second part, base- 4 conversion is performed which is a sequence of 0, 1, 2, 3. On this data reshaping operation is performed to modify the data sequence.

SECURE KEY GENERATION SCHEME:

The Secure Key Generation scheme takes initial key as input and generates a new key. This newly generated key consists of a random number followed by a set of numbers which are generated by adding the random number generated with their corresponding Fibonacci sequence values.

MESSAGE RECOVERY:

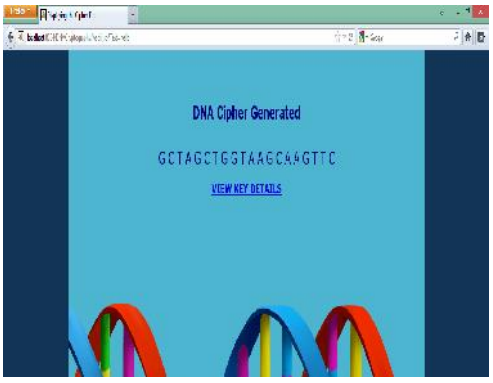
Message recovery of original plaintext is a reverse process of encryption. In the decryption process only the secure key generated is shared with the receiver and the initial key is generated from secure key.

INITIAL KEY GENERATION SCHEME:

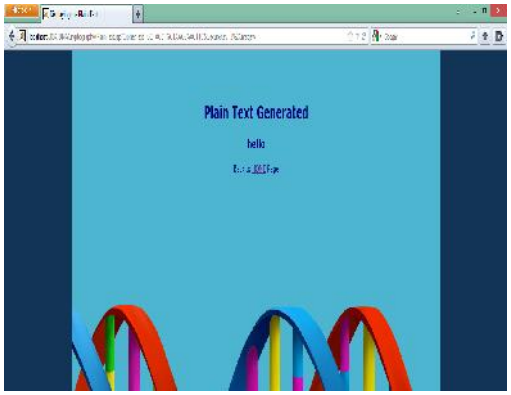
In Secure Key Generation Scheme we added the Fibonacci sequence values. Now generating initial key is a converse of that process. We simply subtract the Fibonacci sequence values from random number generated.

IX. RESULTS:

To select Encryption or Decryption



DNA cipher generated from the given text is “G C T A G C T G G T A A G C A A G T T C”.



Plain Text generated : hello

XII. CONCLUSION:

DNA parallel strands support feasibility and congruity of DNA-based Cryptography. The security and the execution of the DNA based cryptographic calculations are pleasing for multi-level security employments of today's framework. Certain DNA computations can contradict far reaching ambush, quantifiable strike and differential attack. The field of DNA figuring is still in its start and the applications for this development have not yet been totally gotten on. DNA handling is suitable and DNA affirmation strategies have shown great assurance in the business focus of today and it is assumed that its applications will continue developing. DNA Cipher is the helpful supplement to the current numerical figure. If the nuclear word can be controlled openly, it may be possible to achieve unendingly better execution for information stockpiling and security.

XII. FUTURE WORK:

The future work can contain examining and differentiating the execution of all the DNA cryptographic techniques in perspective of secure data transmission shapes. The DNA Cipher obliges a more drawn out execution time for encryption and unscrambling, about to substitute figures. We would expect these results because of the sort changes which are required by virtue of the symmetric Bio algorithm. All settled encryption calculations technique display of bytes while the DNA Cipher talks reality strings. The additional changes from string to show of bytes and back make this figure to oblige more open door for encryption and unravelling then other incredible algorithms. Regardless, this inconvenience should be comprehended with the execution of full DNA counts and the usage of Bio-processors, which would make use of the parallel taking care of power of DNA estimations. As future progressions, we might need to make some test for the asymmetric DNA algorithm and lessening its execution time.

XIII. REFERENCES:

[1] Atul Kahate, Cryptography and network security (New Delhi: Tata McGraw Hill, 2012).
[2] B. Anam, K. Sakib, Md. A. Hossain, K. Dahal, Review on the Advancements of DNA cryptography, 2010.
[3] http://ghr.nlm.nih.gov/handbook/basics/dna Genetic home reference, a service of the U.S. National Library of Medicine,
[4] DNA Structure, http://ijarovic.wordpress.com, 2012.
[5] Learn Genetics, University of Utah, http://learn.genetics.utah.edu/content/begin/tour, 2012.
[6] Nucleotide base pairing of strands, http://dedunn.edublogs.org, 2012.
[7] D.Prabhu and M.Adimoolam, Bi-serial DNA Encryption Algorithm (BDEA), Cornell university library, http://arxiv.org/abs/1101.2577, 2011.
[8] L. Adleman, "Molecular computation of solutions to combinatorial problems", Science, JSTOR, vol. 266, 1994, 1021–1025.
[9] R. J. Lipton, "Using DNA to Solve NPComplete problems", Science, vol. 268, 1995, 542-545.
[10] Boneh, C. Dunworth, and R. Lipton, "Breaking DES using a molecular computer", Proceedings of DIMACS workshop on DNA computing, 1995, 37–65.
[11] Taylor Clelland, "Hiding messages in DNA Microdots", Nature Magazine vol.399, June 1999.
[12] Gehani, T. LaBean, and J. Reif, "DNABased Cryptography", Lecture Notes in Computer Science, Springer, 2004.
[13] G. Cui, L. Qin , Y. Wang , X. Zhang, "An Encryption Scheme Using DNA Technology", IEEE, 2008.
[14] S. Jeevidha, Dr. M. S. Saleem Basha and Dr. P. Dhavachelvan, "Analysis on DNA based Cryptography to Secure Data Transmission", IJCA, Volume 29– No.8, September 2011.
[15] Monica Borda and Olga Tornea, "DNA secret writing Techniques", IEEE conference, 2010.
[16] M. Borda , O. Tornea and T. Hodorogea, "secret writing by DNA hybridization", acta technical napocensis Electronics and Telecommunications, Volume 50, Number 2, 2009.
[17] Pankaj Rakheja, "Integrating DNA Computing in International Data Encryption Algorithm", IJCA, Volume 26– No.3, July 2011.

Smt.s.sushma is a student of Kakinada institute of Engineering and Technology for Women,kakinada. Presently she is pursuing her M.Tech [computer science engineering] from this college and she received her B.Tech from pragati engineering college, affiliated to JNT University, Kakinada in the year 2011. Her area of interest includes computer networks, computer graphics, mobile computing, all current trends and techniques in Computer Science.

Mrs. Ardhani Siva Sravanthi, well known and excellent teacher Received B.Tech and M.Tech(CSE) from JNTU Kakinada University is working as Assistant Professor, Department of B.Tech, M.Tech Computer science engineering, in Kakinada institute of Engineering and Technology for Women, She is an active member of CSI. She has 6 years of teaching experience in various engineering colleges. To her credit participated workshops conducted by IIT BOMBAY, IBM. Her area of Interest includes Mobile computing, information security, Unix and Shell Programming, Computer Graphics, Operating Systems and Object oriented Programming languages flavors of computer networks, cloud computing, and other advances in computer Applications.