Various Cryptographic Techniques: An Overview
Vinay Jain¹, Sonam Baghel²,
Associate Professor, ETC³, Research Scholar²
Faculty of Engineering and Technology¹, Student of Engineering and Technology²
Shri Shankaracharya Technical Campus, Junwani, BHILAI, C.G, India

Abstract:
Since security is a standout amongst the most vital issues, the development of cryptography and cryptographic investigation are considered as the fields of ongoing exploration. The most recent advancement in this field is DNA cryptography. It has risen after the divergence of computational capacity of Deoxyribo Nucleic Acid (DNA). To give security to the data there are different calculations of conventional cryptography and steganography. New field DNA cryptography rises to give security to the information store in DNA. The DNA cryptography utilizes the bio-molecular computational capacities of DNA. DNA cryptography utilizes DNA as the computational apparatus alongside a few atomic procedures to control it. Because of the high stockpiling limit of DNA, this field is turning out to be exceptionally encouraging. Presently it is in the improvement stage and it requires a considerable measure of work and research to achieve a develop arrange. By assessing all the potential and bleeding edge innovation of ebb and flow inquire about, this paper demonstrates the bearings that should be tended to encourage in the field of DNA cryptography.

Keywords: DNA, Cryptography, Steganography, Bimolecular.

I. INTRODUCTION

Cryptography is one of the methods for enhancing security of data by scrambling the information in a way that the message gets to be non-readable (Cipher content) to an interloper. So that the information can't be perused or altered by outsiders. DNA cryptography is a branch of organic science, which has an expansive information stockpiling limit. It stores data of living beings. Living creatures have extraordinary DNA data. It is characterized as data stockpiling, monstrous parallel preparing and exceedingly secured information transmission. DNA cryptography depends on one-time-cushions conspire. Cryptography needs to join with sub-atomic science for more secure information transmission and information covering up. A plaintext message is encoded in DNA successions. DNA successions get intense, when consolidated with nucleotide base A-T and C-G. DNA cryptography innovation is required in data security to ensure and conceal information. In conventional cryptography (like as DES, RSA), encrypted messages are perceptible by an aggressor. DNA has the ability to store gigantic data as opposed to existing calculation. DNA is presented as another innovation for unbroken data. Genetic data is encoded as a grouping of nucleotides Guanine-G, Adenine-A, Thymine-T and Cytosine-C. Adenine, Thymine and Guanine, Cytosine are base sets, which are joined to a sugar and a phosphate to keep up helical structure. DNA strands consolidated with hydrogen bond. A and T DNA arrangements are joined with twofold hydrogen bond while C and G are consolidated with triple bond. Every nucleotide comprises of the accompanying three segments, A Nitrogenous Base, A five carbon Sugar, A Phosphate Group.

II. RESEARCH METHODOLOGY

DNA has for some time been examined as an advanced information stockpiling media by the scientists. This field of study has three sub domains in particular DNA, information stockpiling and Security. DNA is the field of biomedical sciences while information stockpiling and security are identified with Computer Science. So this field envelops three research regions and scientist in this field is required to concentrate every one of them. Parcel of research has been finished by different scientists here referring to the huge measure of information stockpiling limit DNA sees. Accordingly heaps of articles, journals and books were distributed giving the different research approaches and ebb and flow methods. Be that as it may, there has been an absence of gathering of this work as the information stockpiling system in DNA is exceptionally mind boggling and includes various strategies in different phases of improvement. The Creators did a thorough study on this point and gathered research material scattered over various assets. Different diaries, which were alluded are specified underneath:
The authors in this paper explore the different calculations for DNA cryptography and examine them as indicated by different classifications. The authors likewise give the classification of DNA security as per different cryptography procedures. Inquire about papers were sought in terms like 'DNA information stockpiling', 'Security in DNA', 'DNA Cryptography' and so forth. The papers gathered were looked into by the creators as far as pertinent to the subject and those papers which were discovered significant were incorporated into this paper. Evaluation criteria utilized for settling on consideration of research papers can be spoken to diagrammatically in figure.

Figure 2. Flowchart for evaluation and selection criteria of research papers [30].

III. OPERATIONS ON DNA

The procedure of DNA processing into a few stages which are considered as the primitive operations for DNA calculation. These operations are as per the following:

A. DNA Synthesis: Encoding of content written in any dialect is done more than four letters in order {A, C, G, T} to get a solitary strand of DNA.

B. Hybridization: In light of the corresponding hypothesis of Watson-Crick, single strands of DNA with inverse introduction combine so as to shape a twofold helical structure.

C. Cutting: A particular short length grouping of DNA is chosen called limitation chemical. This confinement protein is mapped with the twofold stranded DNA. The site where the event of this limitation catalyst found in a twofold stranded DNA grouping is known as confinement site. The protein cuts the DNA grouping from that area in a particular arrangement which is same as that of the catalyst. Accordingly, two "limit finished" twofold strands of DNA are left or two twofold stranded DNA with single-stranded shades known as "sticky-closures" are cleared out.

D. Ligation: This operation is the invert of cutting. In this, a chemical known as DNA ligase, repairs and rejoins the resultant double stranded DNA groupings of cutting operation.

E. Separation: This operation is done by utilizing gel electrophoresis method. In this, DNA atoms are sifted through as per their size (little or expansive).

F. Extraction: A single stranded DNA atom that contains the focused on subsequence of bases is removed by a procedure of proclivity decontamination.

G. DNA replication: It is finished with the assistance of polymerase chain response and a preliminary. In this, different duplicates of the supplemented portion of DNA format which begins with groundwork arrangement are created.

IV. ANALYSIS OF ALGORITHMS

In this area the authors investigated the different past calculations proposed by various specialists. The authors arranged the operations into various classes by altogether concentrating on the security:
<table>
<thead>
<tr>
<th>S.NO</th>
<th>AUTHOR</th>
<th>PAPER TITLE</th>
<th>CRYPTOGRAPHIC MECHANISM</th>
<th>METHODOLOGY USED</th>
<th>ADVANTAGES</th>
<th>DISADVANTAGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Sherif T Amin et al. 2006 [15]</td>
<td>A DNA based implementation of YAEA encryption algorithm</td>
<td>symmetric</td>
<td>1. DNA nucleotides , searching algorithms</td>
<td>1. Real message is not transfer over network 2. Scalable for large digital information products.</td>
<td>1. Size of plain text increases the encryption time and decryption time. 2. It provides only one level of security.</td>
</tr>
<tr>
<td>2.</td>
<td>L. MingXin, L. XueJia, X. GuoZhen and Qin. L., 2007 [8]</td>
<td>Symmetric key cryptosystem with DNA technology</td>
<td>symmetric</td>
<td>DNA fabrication DNA hybridization</td>
<td>Provide two level security biological and computational security</td>
<td>It has the possibility of attack from DNA computer in future.</td>
</tr>
<tr>
<td>3.</td>
<td>Guangzhao Cui et al., 2008 [4]</td>
<td>An Encryption Scheme Using DNA Technology</td>
<td>Asymmetric key</td>
<td>1. DNA synthesis. 2. DNA digital coding. 3. PCR amplification.</td>
<td>1. Prevent an attack from a possible word as PCR primers. 2. The complexity of Biological scheme and cryptography computing provide a double security safeguards for the scheme. 3. Cost of encryption scheme is low.</td>
<td>1. Security can depend only on decryption key. 2. The encryption scheme is still far away being a perfect scheme.</td>
</tr>
<tr>
<td>4.</td>
<td>LI Xin-she et al., 2008 [18]</td>
<td>A Novel generation key scheme based on DNA</td>
<td>Symmetric key</td>
<td>1. key expansion matrix</td>
<td>1. DNA sequence reduces the computation complexity. 2. Computation speed is increased.</td>
<td>1. Security depends upon the key.</td>
</tr>
<tr>
<td>5.</td>
<td>H.J.Shiu et. al. 2010[14]</td>
<td>data hiding methods based upon DNA sequences</td>
<td>symmetric</td>
<td>1. Insertion method 2. substitution method 3. complimentary pair method</td>
<td>1. easy to implement 2. flexible</td>
<td>1. security is depend upon the referred DNA sequences which are available on the internet</td>
</tr>
<tr>
<td>7.</td>
<td>Qinghai Gao et al.,2011 [10]</td>
<td>secure communication protocol with DNA primer</td>
<td>symmetric</td>
<td>1.decode message according to codebook</td>
<td>1. real message is never transmitted</td>
<td>1. difficult to send a message which is not present in the codebook</td>
</tr>
<tr>
<td></td>
<td>Authors</td>
<td>Title</td>
<td>Symmetric key</td>
<td>Advantages</td>
<td>Disadvantages</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---------</td>
<td>-------</td>
<td>---------------</td>
<td>-------------</td>
<td>---------------</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Zhang Yunpeng et al., 2011 [11]</td>
<td>Index-Based Symmetric DNA Encryption Algorithm</td>
<td>Symmetric key</td>
<td>1. XOR operation 2. Position Indexing</td>
<td>1. Exact position of DNA sequence is not identified. 2. Huge key space, high sensitivity to plaintext on encryption. 3. Proper random key sequence to improve security. 1. Higher security, could encrypt a longer DNA Sequence takes more time. 2. Security completely depends upon key.</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Yunpeng Zhang et al., 2012 [7]</td>
<td>DNA Cryptography Based on Fragment Assembly</td>
<td>Symmetric key</td>
<td>1. DNA Fragmentation</td>
<td>1. Length of cipher-text is secure and short. 1. Length of DNA Fragment is short, attacker can easily detect.</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>S. Dhawan and A. Saini et al., 2012 [12]</td>
<td>A new DNA encryption technique for secure data transmission</td>
<td>Symmetric key</td>
<td>1. Division 2. 10-base 4 conversion 3. Amino acid conversion</td>
<td>1. Provides computing difficulty 2. Provides double layer security 1. Encryption cost is high 2. Starting number in key array is starting from 255</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>T. Mandage et al., 2013 [5]</td>
<td>A DNA encryption technique based on matrix manipulation and secure key generation scheme</td>
<td>Symmetric key</td>
<td>1. Primers 2. Amino acid conversion 3. XOR operation 4. Mirror operation</td>
<td>1. Always get new cipher text for the same plain text and key 1. It includes only basic operation hence security completely depends upon key</td>
<td></td>
</tr>
</tbody>
</table>
### V. LIMITATIONS OF THE STUDY

- The parameters and the administrators are characterized just regarding the calculations creators alluded in this paper.
- These parameters and administrators give the significant gauge, which can be further broadened.
- The multifaceted nature of the calculation builds the security and cost of the calculation usage.
- Due to foundation of PCs, creators couldn’t confirm some natural terms and systems agreeable to them.
- Authors did exclude every one of the papers of security calculations.
- Authors did not have entry to the majority of the exploration papers and got to our decision in view of the theoretical and other supplementary archives accessible to them.

### VI. REFERENCES


