A Review on DNA Based Cryptographic Techniques

Article *in* International Journal of Network Security · November 2018

DOI: 10.6633/IJNS.201811_20(6).10

3 authors, including:

Animesh Hazra
Jalpaiguri Government Engineering College
20 PUBLICATIONS **288** CITATIONS
SEE PROFILE

Soumya Ghosh
Jalpaiguri Government Engineering College
2 PUBLICATIONS **18** CITATIONS
SEE PROFILE

A Review on DNA Based Cryptographic Techniques

Animesh Hazra[1], Soumya Ghosh[2], and Sampad Jash[2]
(Corresponding author: Animesh Hazra)

Department of Computer Science and Engineering, Jalpaiguri Government Engineering College[1]
Jalpaiguri, West Bengal 735102, India
(Email: hazraanimesh53@gmail.com)
Department of Information Technology, Jalpaiguri Government Engineering College[2]

(Received May 12, 2017; revised and accepted Oct. 28, 2017)

Abstract

Today, data security has become a great concern. The increase in digitalization and e-commerce has encouraged more and more people to use the Internet. As a result, the web has become a part of our life. Hence the need of data security is evident. In order to enhance the data security, researchers have come up with new concepts. The use of DNA cryptography along with various encryption techniques is one of the major trends used in modern data security. Experimental results show that several biological operations and encoding techniques can be applied on DNA. This paper gives a brief review of the methods used in DNA cryptography and real time implementation of those techniques. Computational advantages along with the limitations regarding DNA cryptography is also addressed.

Keywords: Data Security; Decryption; DNA Cryptography; E-Commerce

1 Introduction

Cryptography [38] can be defined as the art of achieving security with the help of encoding messages in order to make them non-readable. The technique of decoding the non-readable messages into readable one is known as cryptanalysis and it can be said that cryptology is defined as the combination of cryptography and cryptanalysis. Before the age of computers, the art of cryptography was performed my manual techniques. Some of the techniques involved are substitution technique and transposition technique. Caesar cipher, modified version of Caesar cipher, mono alphabetic cipher, polygram substitution cipher, Vigenere cipher are different examples of substitution technique. Some transposition techniques include rail-fence technique, simple columnar transposition technique, vermin cipher *etc.* The introduction of computer made it possible to use more complex cryptographic algorithms. Technical terms like encryption and decryption came into existence. Encryption is defined as the process involved in the encoding of plain text to cipher text and decryption is the reverse process of encryption [13].

There are two aspects in respect to this encryption and decryption process. One is the algorithm that is involved in the encryption process and another one is the key used in the algorithm. Key is the most important attribute on which the security of the encryption technique depends. It can be classified into two categories. If the same key is used for both encryption and decryption procedure then the key is known as symmetric key whereas in asymmetric key different keys are used for both encryption and decryption algorithm. There are various methods to implement these techniques like data encryption standard (DES), International data encryption algorithm (IDEA) [29, 31], RC4, RC5, blowfish, advanced encryption standard (AES) [30, 45], RSA [14, 33], ElGamal [18, 19, 42, 43], and ECC cryptography [36, 54] *etc.*

There are some challenges involved in traditional cryptography. One such problem is the sharing of key because it may fall prey to attacks like eavesdropping or man in the middle. It has been found out that the ultimate power of a cipher depends on three important factors *i.e.* the size of the key, the infrastructure on which the key is running and last one is the algorithm on which it is designed. Today the most secure key length is 2028 bits. A famous symmetric key algorithm known as DES which uses a 5-bit key size is no more considered as safe. The increase in computational power has compromised the safety of the traditional cryptographic techniques. This problem is solved with the use of DNA cryptography.

1.1 Operations on DNA

Many biological operations [5, 6, 46] can be done on DNA molecules which will aid us in solving mathematical and computational problems. Some of the arithmetic and logical operations performed on DNA are as follows.

The basic arithmetic operations which can be imposed on DNA nucleotides are addition and subtraction. They are described in the following section.

1) Addition Operation: The addition operation on DNA nucleotides are performed according to the traditional binary addition rules. For example, if two binary numbers 10 and 11 are added then it will result the value 01. Now, suppose the four DNA nucleotide bases A, T, C and G are encoded as 00, 01, 10 and 11 respectively. Then it can be concluded that when C is added with G, it results into T.

2) Subtraction Operation: The subtraction operation on DNA sequences are performed according to the traditional binary subtraction rules. For example, if 01 is subtracted from 11 then the result is 10. Now, suppose the four DNA nucleotide bases A, T, C and G are encoded as 00, 01, 10 and 11 respectively. Then it can be concluded that when T is subtracted from G, it results into C.

The logical operations which can be implemented on DNA sequences are NOT, OR, AND, XOR, NOR, NAND and XNOR. They are described below in details.

Deoxyribonucleic acid (DNA) has a number of characteristics that enables us to mimic the traditional logical operations. DNA prefers to be in double stranded form, so single stranded DNA sequences naturally migrate towards complementary sequences to form double stranded complexes. Complementary sequences pair the bases adenine (A) with thymine (T) and cytosine (C) with guanine (G). DNA sequences pair in an anti-parallel manner.

In each DNA-based logic operation, the input is represented by a single stranded DNA sequence with the requirement that the sequence representing a true evaluation is complementary to the sequence representing a false evaluation for a single gate. For example, ACCTAG can be represented as true whereas CTAGGT is represented as false, since CTAGGT is the reverse complement of ACCTAG. This enables sequence assignment to be dynamic in nature. A user could arbitrarily assign a new set of representative sequences for each gate in a circuit.

DNA's preference to be in double stranded form enables the implementation of traditional logic operations in a very convenient way. For each respective DNA-based gate design, a predetermined mixture is supplied containing a specific single stranded sequence to induce the appropriate chemical reaction which is known as the base mixture. If the gate input sequence provided is complementary to the base sequence then the corresponding double stranded DNA sequence will form. Thus, the presence or absence of a double stranded sequence is used to evaluate the gate output whereas the presence of a double stranded sequence represents a true evaluation and it's absence represents a false evaluation.

Fluorescent labels can be used to detect the presence or absence of the double stranded sequence. In this process fluorescent molecules are attached to the nucleotide sequence, which absorbs and emits light at a particular wavelength. Thus, by attaching the fluorescent molecule to one of the strands of the double stranded sequence, the double stranded sequence can be detected. It's presence can be identified by examining the sequence solution at the fluorescent probe's characteristic wavelength.

The presence of a fluorescently labelled double stranded sequence only works if the single stranded labelled sequences are removed. Deoxyribonuclease (DNase) is an enzyme that breaks down the single stranded DNA sequences by degrading the sugar bonds connecting adjacent to nucleic acids.

The final step of the DNA-based logic gates is to use the output observed at the previous gate as the input into the next logic gate in the circuit.

The representative sequences can be dynamically assigned and a new set of complementary sequences can be substituted between evaluation of the previous gate and the insertion of the representative sequence in the next proceeding gate. Each DNA-based logic gate design is built on the preceding set of procedures. Individual gate logic is achieved through the introduction of a specific complementary sequence in the base mixture provided to each gate. Specific gate construction for the traditional DNA-based Boolean logic gates for NOT, OR, AND, XOR, XNOR, NAND and NOR are discussed in the following section. All Boolean logic gates can be easily derived from the three fundamental logic gates AND, OR and NOT.

1) NOT Gate: The NOT gate often referred to as an inverter, is one of the simplest DNA-based logic gate. Only one input is supplied to the gate and the output is the corresponding complementary sequence. Because the output should evaluate true only in the presence of a false input and the base mixture provided to the gate contains the representative true sequence. DNase is supplied to destroy any single stranded sequences. If a double stranded sequence is observed then the result is true otherwise the result is false.

2) OR Gate: The OR gate evaluates true if at least one of the gate input is true. DNase is supplied to destroy any single stranded sequences. If a double stranded sequence is observed then the result is true otherwise the result is false.

3) AND Gate: The AND gate evaluates true if both inputs are true. DNase will destroy any single stranded sequence in the mixture. If a double stranded sequence is observed then the result is true otherwise the result is false.

4) XOR Gate: The XOR gate evaluates true only if exactly one of the input sequences evaluate true. With binary inputs, XOR is defined as evaluating true if input values are opposite. In DNA-based logic gates the XOR gate has the most simplistic design since no

base sequence needs to be supplied to the gate. Opposite input sequences are complementary and will bind together to form a double stranded sequence. If the inputs are not opposite then the sequences will not be able to bind with each other and DNase will destroy both input sequences.

5) XNOR Gate: The XNOR gate which evaluates true when both inputs are the same, is created by applying the NOT gate to one of the inputs then applying the XOR gate to the result and the other input. Like the preceding gate designs, the presence of a double stranded sequence indicates a true evaluation of the gate while the absence of a double stranded sequence indicates a false evaluation of the gate.

6) NAND Gate: The NAND gate evaluates true if both inputs are not true. The DNA-based NAND logic gate is similar to the OR gate presented previously except the base sequence contains the sequence representing value true rather than false. Thus, at least one of the inputs must be false in order to form a double stranded sequence. DNase will destroy any single stranded sequence in the mixture. If a double stranded sequence is observed then the result is true otherwise the result is false.

7) NOR Gate: Finally, the NOR gate which evaluates true when both inputs are false, is implemented by applying the NOT gate to the output of the OR gate.

2 DNA Cryptography

DNA computing can be defined as a new technique for securing information with the help of biological structures. Leonard Max Adleman [2] can be considered as the pioneer of the DNA computing. He used this in 1994 for solving complex algorithmic problems. Now it is discovered that DNA can be used to store and transmit data. There are several advantages of DNA computing out of which a few of them are discussed as follows.

1) Minimum storage requirement: In a compact volume large amount of data can be stored. Calculations suggest that 1 gram of DNA contains 10^8 terabytes of data.

2) Speed: DNA computing techniques are almost 100 times faster than the modern-day fastest computer.

3) Minimum power requirements: DNA computing needs very less or no power at all compared to modern day computers.

DNA cryptography is defined as a process of hiding data in terms of DNA sequence. At present, the work in the field of DNA cryptography is focused on the use of DNA sequences to encrypt binary data in some form or other. In the near future, DNA computing will become as one of the leading techniques for securing information. Some of the DNA cryptographic techniques are discussed as follows.

2.1 DNA Complement Operation

In DNA complement operation the four nucleotide bases adenine(A), cytosine(C), thymine(T) and guanine(G) are substiuted according to the complementary rule and antiparallel manner where A is substituted with T and vice-versa. Similarly C is substituted with G and vice-versa. For example, if the input DNA sequence is ACTGACTG, then it's complemented DNA sequence will be TGACTGAC.

2.2 DNA Digital Coding

It is a technique of mapping the 4 different bases of DNA that are A, C, T and G with 0 and 1. Plain text messages can be easily encoded using this scheme. There are 24 such patterns possible but only 8 unique combinations are considered which fit the complimentary rule. This will be clear with the following example. Suppose someone wants to send the number 97 using DNA encoding. He or she can convert 97 to binary, by breaking 9 to 4 bit binary form 1001 and 7 is converted into 0111. Then both the binary forms of 9 and 7 are joined together. The resulting binary number will be 10010111.

Table 1: Conversion scheme for binary form to DNA nucleotide

Binary Form	DNA Nucleotide
00	A
01	T
10	C
11	G

Starting from the left most bit, two consecutive binary digits are taken and converted to corresponding DNA nucleotide bases following the scheme described in Table 1. In this way finally, the number "97" will be encoded as "CTTG". Now the encrypted message "CTTG" will be sent through a channel to the receiver. The receiver then decodes it and extracts the original message.

2.3 Hao's Permutation and Fractal Sequence Representation

Hao *et al.* [32] designed and proposed a DNA fractal sequence representation approach. A complete genome of length N is given which may be circular or a linear DNA sequence composed of N letters from the alphabets A, C, G and T. The authors designed a mapping technique that maps the four letters A, C, G and T to the base 4 number system. α: {G,C,A,T}→{0,1,2,3}.

$$x = \Sigma_{i=1}^{k} 2^{k-i}[\alpha(s_i) >> 1] \quad (1)$$
$$y = \Sigma_{i=1}^{k} 2^{k-i}[\alpha(s_i) \& E] \quad (2)$$

In Equations (1) and (2) E means a binary number 1, ">> 1" indicates the right shift by one bit, symbol "&" is bitwise AND operator and s stands for the chosen DNA sequence. Here is a mapping function which converts the selected sequence into its corresponding base 4 number system.

This permutation approach is robust and provides high security, particularly in image encryption. Using this approach authors have proposed a new key generation process for image encryption [56].

2.4 Polymerase Chain Reaction (PCR)

It is a technique using molecular biology which amplifies the DNA. The steps followed in PCR operation is denaturation, primer annealing and primer extension. In denaturation, a two single stranded DNA is formed from a double-stranded molecule. This is done by heating the sample at a very high temperature of about 94 to 96 degree Celsius. Then primer annealing is done at about 50 to 65 degree Celsius where the primers which are designed to amplify the DNA regions are attached to the complimentary sequences. Finally, primer extension is performed. In this step, the temperature is again raised to about 72 degree Celsius. Here, nucleotides are added to the strand of a short primer on the base of original DNA strand using polymerase enzyme.

Apart from traditional methods some of the hybrid DNA cryptographic techniques which are evolving in this era are discussed as follows.

2.5 Elliptic Curve Cryptography Using DNA Encoding

It is one of the most efficient public key cryptography methods [34,35] . There are several benefits and facilities of this technique such as reduced key size. The security provided by this algorithm is similar to the security provided by RSA algorithm but the key used is much smaller compared to the RSA algorithm. Elliptic curve arithmetic is used for this technique. The security is increased by encoding the message with a DNA encryption technique. Elliptic curve cryptography is implemented over this DNA encoded message, thereby making the method more robust and a hybrid one.

2.6 Quantum Cryptography Using DNA Encoding

Quantum cryptography can be explained as emerging security technique in which the receiver and the sender communicate through a quantum channel. Quantum cryptography is based on Heisenberg's uncertainty principle and no-cloning theorem. This is purely based on the laws of applied physics. DNA encoding can be applied in the encryption technique of the plain text that is being sent through the quantum channel. The process is tough to crack and has given birth to a new hybrid technique.

3 DNA Encryption Techniques

The technique of converting the plain text to cipher text with involvement of DNA is known as DNA encryption. In the following section four DNA encryption techniques are discussed.

3.1 DNA Random One-Time Pad Based

This encryption technique is implemented using a set of randomly organized non-repeating characters. These act as the input ciphertext. It is named as one-time pad because if an input ciphertext is used once it is not used again. This helps in increasing the security. In this scheme the length of the one-time pad should be equal to the length of the plain text. In order to convert the short segments of plain text messages to cipher text, DNA one-time pad process is used. A random and unique codebook is taken into account for replacing the plain text. The problem in this method is that it is applicable only on short messages. For large messages the current hardware is not suitable enough for one-time pad. The increase in size of the message escalates the complexity of DNA mapping.

3.2 DNA Chip Based

The introduction of DNA chip technology has been a great progress in the field of DNA cryptography. It is helpful for the manipulation of a huge amount of genome sequences along with storing and handling of biological information. The DNA chip is commonly known as microarray. The microarray is made of nucleic acid and its electronic circuit is composed of semiconductors. Encryption and decryption occur using biochemical processes and it can be applied in encryption of plain text messages and images. Since the DNA chip is a biological element, its properties may change due to other physical factors. This sudden change will have a negative impact on encrypted messages.

3.3 DNA Steganography

The technique of hiding messages inside another message is known as steganography. When DNA is used in steganography it is known as DNA steganography. The scheme allows the message to be hidden in an image, audio or even a video file. It is a new emerging technique in the field of DNA cryptography. This is ideal for hiding a large amount of data. The process involves biological strands hence the data can get corrupted due to the sudden change of environment.

3.4 DNA Fragmentation

This method is used for library construction in DNA sequence. It is used to split the DNA sequence into small pieces. Many encryption algorithms use this as a second layer of security. It is also implemented in encryption of the key.

4 Literature Survey

There are several research papers which explore the DNA based cryptographic techniques. In this section the summaries of some of them are presented in a nutshell.

These papers are further categorized into five classes. They are DNA-based symmetric cryptography technique, DNA-based asymmetric cryptography technique, DNA-based elliptic curve cryptography technique, DNA-based quantum cryptography technique and DNA-based cloud cryptography technique respectively. It is described below in details.

Zhang *et al.* [25] proposed a DNA cryptographic algorithm. The method is based on DNA fragment assembly. Authors have implemented the features of DNA digital coding, DNA molecular key and some software techniques in their algorithm. This technique follows the concept of symmetric key cryptography. The encryption mechanism is done here using DNA digital coding. The main disadvantage of this algorithm is the implementation of the DNA molecular key.

In [24] the authors have mentioned a new encryption scheme on data security and cryptography, based on DNA sequencing. In the proposed system the message is converted into its binary form. Prior to communication establishment, the session key is shared through a secure channel between sender and receiver. Two rounds of encryption are used in this technique. The security is increased by breaking the sequence into blocks which is followed by hexadecimal addition and subtraction. The encoding method used here is based on symmetric key cryptography. This concept can be implemented in real-time security of distributed network systems. The sharing of key during distribution is a real difficulty in this algorithm.

Ibrahim *et al.* [1] proposed a technique to enhance the security of data hiding using double DNA sequences. The main idea behind the designed scheme is the encryption of secret message to ensure security and robustness. The encryption is done in two phases. The encrypted message is hidden into another DNA reference sequence. Overall a new data hiding algorithm based on DNA sequences has been recommended. In this scheme hiding of data in repeated characters minimizes the modification rate. On analysing the security aspect of this algorithm, it can be concluded that it would be difficult for the attacker to identify the secret message. But, if somehow the attacker manages to obtain the secret message then the method can be broken down easily.

In [39] the authors have proposed a method to encrypt information with DNA-based cryptography which is performed on five main stages. The first stage is data preprocessing where binary data is converted into a DNA string. The second step is the key generation followed by the encryption process. The fourth step is the decryption process where the DNA strand cipher text acts as the input and the output is DNA plaintext. The secret key is used to decrypt the cipher text. The last step is data post-processing where the obtained DNA sequence plain text is converted into binary plaintext. This algorithm is very much secured since it has a double layer of security and is based on vigenere cipher. The time complexity involved in this algorithm is huge.

Anwar *et al.* [4] proposed a new DNA cryptographic algorithm. This encryption technique is a combination of XOR operation and symmetric key exchange. It is very simple but powerful algorithm. The scheme encrypts plain text message into DNA cipher text. In order to increase security, the message is checked at the receiver end. Sender uses the symmetric key technique and encrypts the plain text into DNA sequence. The message is then sent to the receiver through various insecure channels like the Internet. At the receiver end, the receiver decrypts the cipher text into plain text using the DNA sequence. The concept of DNA hybridization and matrix calculations are done here to minimize the time complexity. DNA sequences can store large messages in very compact form which is one of the major advantage of this algorithm. Implementation of this method in real life is very cost effective.

Bama *et al.* [49] provided an interesting algorithm for secure data transmission using various properties of DNA sequencing and substitution techniques. The encryption technique is mainly dependent on a substitution scheme and a selected DNA sequence. The DNA sequence is selected out of 55 million possibilities which make the algorithm very much secured. Some intelligent binary logic and reverse substitution techniques are used to recover the message during the decryption phase. This method is very simple, efficient and reliable. The proposed algorithm is already implemented in an Electronic Medical Record System. The substitution scheme used here needs to be protected because if the scheme is compromised then the whole method will be vulnerable.

In [52] the authors proposed a cryptographic algorithm based on DNA, random key generation scheme and matrix multiplications. This generated key is XOR-ed with the outcome of the scrambled matrix. As a result even though the same key and same message is used, each and every time this technique will generate a different cipher text. Here, a total of three keys are used *i.e.* the initial key, primer key and the generated key. The performance and security of the DNA-based algorithm is suitable for multilevel security. This DNA cryptographic algorithm can resist exhaustive attack, statistical attack and differential attack. For single level security this method unnecessarily increases the time complexity.

Raj *et al.* proposed a technique on DNA-based cryptography using random key generation and permutation [51] . The above algorithm uses the concept of DNA pattern generation in a random manner. The method is very simple where the encryption starts by first converting the plain text into ASCII code and then into binary form. Table 2 is used here to convert the binary data into DNA sequences.

Table 2: Conversion formula for binary code to DNA nucleotide

Binary Form	DNA Nucleotide
00	A
01	T
10	C
11	G

A DNA sequence is selected as a key and grouped in blocks where each block consists of four characters. A table is created on the basis of how the characters occupy the block positions. Finally, from this table the randomly selected DNA sequence gets converted into encrypted form. The cipher sequence along with the key is sent to the receiver. The DNA sequences are decoded by following Table 2. The reverse steps are applied to get back the original message. This algorithm is somehow different from others, since traditional mathematical operations or data manipulation techniques are not used. Hence this method cannot be applied for multilevel security.

In [44] the authors presented a method which gives a secure data transfer mechanism using symmetric algorithm through DNA cryptography. Initially, the input data, text or image is converted to ASCII value and then it is again converted into its binary equivalent. Now, the binary value is converted to DNA code. The DNA code is randomly assigned on the basis of a private key and is converted to the extended ASCII code. Finally, the message is encrypted using DNA code and clinical permutation is done with the private key. The proposed system is implemented using Java and falls in the category of modern symmetric key encryption technique. DNA chromosome need to be used during the data transmission. On deep analysis of the algorithm, we can conclude that this method uses a much faster and better encoding scheme than conventional cryptographic techniques. This scheme can be used to increase the security mechanism of wireless networks. However, the use of DNA chromosome increases the overall implementation cost of the algorithm.

Researchers in [28] came up with a new technique for secure data transmission using the process of XOR operation, one-time pad (OTP) scheme and DNA cryptography. OTP scheme is applied here by a suitable method which has some preconditions. XOR operation is applied between the OTP and binary form. The binary digits are converted into DNA sequence by the following scheme: 00=A, 01=T, 10=C and 11=G. After complementing DNA bases, the DNA sequence is reversed from right to left. Then resulting encrypted data is sent to the recipient. This algorithm provides three levels of security *i.e.* arithmetic operation or XOR operation, one-time pad and DNA complementary rule. Overall the process is very simple to understand but highly secured as the randomly generated OTP is very much hard to guess for an attacker. Since there are some preconditions applied, therefore the method is not so user friendly as the user always has to take care of the preconditions while choosing the OTP.

Sravanan *et al.* [50] proposed an algorithm based on the modified Shamir's secret algorithm as well as DNA-based encryption and decryption technique. In the receiver end, a group is involved instead of a single user. Some added security is incorporated in the algorithm. When all the clients in the group are involved in the decryption process, only then the secret message can be decoded. Mathematical calculations are performed to convert the message into ASCII values. It is then altered into DNA bases. The message is transmitted to the group of clients and then the message is decrypted using DNA encoding to increase the security of message transmission for multicast applications. The proposed protocols can be implemented in Python and Java. This process can be used in trust-based image encryption system in future. The method is suitable only for a group and if someone is missing then the message cannot be decrypted.

Kamaraj *et al.* [11] proposed a new cryptography algorithm based on DNA computing. The algorithm is divided into two stages namely encryption and decryption. The first step converts the data into the corresponding cipher text and then it is sent to the receiver. At the receiver end, the encrypted code is decoded into original data. Here, the input message is in the form of normal text which is given to the FPGA(Field-Programmable Gate Array) through PS 2 keyboard. The message is read by the FPGA as ASCII value codes. Then it is converted to the codon by a codon table provided by the authors. Vigenere cipher is used for the encryption of the codon. This algorithm gives an idea of double layer security with a symmetric key. The distribution of key is not discussed here hence it can be a hectic problem for the algorithm.

In [22] the authors proposed a new structure for distributed system security with the help of DNA cryptography and trust-based approach. A rule-based approach for evaluating the trust-management has been designed. It is processed using the reputation approach. The reputation approach contains three phases *i.e.* proof collection, reputation factor approximation and reputation confidence. In the rule-based approach, the authors have used a DNA-based cryptographic method where detailed rules for encryption and decryption are laid out. The trust-based distributed systems used here are extremely robust in dealing with the security aspects. The introduction of DNA-based cryptography in this type of system will make the system highly secured. Data post-processing approach is integrated into this method to deal with various cyber-attacks. This method cannot have wide applications and is applicable to only trust-based distributed systems.

Roy *et al.* [17] designed a method to improve the key generation based on DNA synthesis. This system optimizes the encryption and decryption process. The plain text is converted to the primary cipher text by a first level key (PK1) along with an encryption algorithm. The concept of second level key is introduced which increases the security of this technique. The second level private key add primers and positions of introns which strengthen the cipher text. On analysing the proposed method against brute force attack, excellent results are achieved. It would take more than half a year for the hacker to decrypt the cipher text with the help of modern day computer. Time and space complexity associated with this method is very high.

In [3] the authors have introduced a complimentary pair approach instead of traditional DNA encryption method. Initially, the DNA bases are complemented in the following manner: A-T, C-A, G-C and T-G. Then a DNA reference sequence is selected and named as S. This S will be known to both sender and receiver. S is then complemented and named as S'. This S' is then sent to the receiver by using any steganographic technique. The receiver will decrypt cipher text S' with the help of S. Application of steganography enhances the security of the proposed method. The algorithm is implemented in Java. In order to decrypt the message, an attacker has to guess the randomly generated sequence S. There are roughly 55 million publicly DNA sequences are available, hence it will be very hard to crack S. This makes the algorithm a robust and reliable one. The distribution of S is not discussed properly and if the receiver does not know S from before then the algorithm cannot be applied in that case.

Rani *et al.* [37] developed a DNA-based encryption technique using XOR operations. Initially, the plain text is selected and a random key is generated. A Randomized codon list is created and XOR-ed with the key. Swap complement operation is applied to create the encrypted message. The key is generated on the basis of DNA properties and biotechnology. The XOR operation is very fast hence it is implemented in O (log N) time. In future, more work can be done on decreasing the space complexity of the algorithm.

Zhang *et al.* [53] designed a method on index-based encryption algorithm which follows the concept of symmetric key cryptography. The proposed technique is based on the index of string and block cipher. The plaintext is encrypted twice with the help of the key. First, the plain text is converted to ASCII code and then it is expressed in 8-bit binary value. DNA encoding technique is performed to convert the binary form into DNA sequences using the scheme described in Table 3.

Table 3: Conversion scheme from binary form to DNA nucleotide

Binary Form	DNA Nucleotide
00	C
01	T
10	A
11	G

In the next step, the key is selected and it is divided into two parts. Finally, the encryption process takes place. The uniqueness of this algorithm is that it gives a huge key space and an extremely complex encryption algorithm. The chaos mapping added in this algorithm increases the mathematical security. Key generation ensures that the huge key space is fully optimized and can prevent extensive attacks. The space complexity associated with this method is huge.

Borda *et al.* [12] proposed a method on secret writing with the help of DNA hybridization. The algorithm hides the data in artificial or real DNA digital form. It is based on the one-time pad (OTP) scheme. In the designed method the receiver and transmitter will have a set of such non-repeating strands. Each ssDNA from the set will be used once and then destroyed. The concept of OTP is applied with ssDNA key in order to encrypt the message. This message is hidden with the help of Viviana Risea's idea. The actual message is changed to ASCII value and then in binary form. One time pad is applied and finally the encrypted message is a set of segments which is complementary to the ssDNA. The encoded message will be transmitted in a compact form and is hidden using DNA steganography technique. The message recovery is possible for someone who has the knowledge of the medium containing the message, the one-time pad and the primer sequences which are used for the encryption process. This algorithm has the advantage of parallel computing. It's implementation is done using Bioinformatics Toolbox present in Matlab software. The use of this method requires high tech laboratories.

In [7], the authors proposed a new concept on DNA cryptography. It is based on Yet Another Encryption Algorithm (YAEA). YAEA was first proposed by Saeb and Baith. Symmetric key cryptography is used here. This method uses sequential search algorithm. Then it locates and returns one of the many positions of quadruple DNA nucleotides. These nucleotides represent the binary octet of each plain text characters. The decryption process is done with the help of pointer file and random binary file. This binary file is available to both sender and receiver from beforehand. In order to get a higher order of security, larger genome sequence is used. The technique can be used in large digital information products. If the receiver does not have the binary file from beforehand then he or she cannot apply this algorithm.

In networking and data communication the main concern is security. Mobile networks are becoming vulnerable day by day. In [20] the authors have proposed a method to secure mobile networks through DNA-based cryptography. The message to be sent is initially converted into 8 bit extended ASCII code and then to binary form. DNA encoding, mRNA sequence, amino acid and some mathematical concepts are used for encryption procedure. The algorithm is implemented using C++ environment in Windows Vista machine. The proposed technique is secured enough to endure the brute force method as the permutations used in this methodology are very strong. This process can be applied as a hardware solution. The method can only be used in wireless communications.

Shinde *et al.* [26] proposed a new DNA-based cryptography technique. The method comprises of traditional cryptographic technique along with new approaches for enhancing the data security. Initially, the plaintext is converted into ASCII value then consequent binary strings. Further, the binary strings are converted into hexadecimal values and simultaneously using MD5 algorithm a 128 bit key is generated. This key is converted into the hexadecimal string of length 32 characters which are mapped to 16 dynamic values. The binary values are encoded with the help of mapping table. Some mathematical and logical operations are performed after encoding. An insecure transmission channel is used for data transfer. Here decryption is not exactly the reverse process of encryption. Some extra parameters are required for decryption procedure. This technique is very fast and efficient one. The algorithm is implemented on Java platform. The security provided in this algorithm is not suitable for multilevel applications.

Chavan designed a new DNA cryptographic technique based on DNA hybridization and one-time pad (OTP) scheme [15] . Here, same keys are used in encryption and decryption process, hence making the algorithm symmetric. One of the keys is a randomly chosen string of nucleotides forming a ssDNA sequence. The second key is a binary sequence that is used for the OTP. The length of the ssDNA sequence key should be half of the length of binary key. XOR technique, OTP, ssDNA sequence and oligonucleotides are used for encryption method. DNA hybridization is implemented in decryption procedure. Experiment results show that the security of this algorithm is very high. About 1 in 1.94 X 10^{84} combinations can be right while guessing the key. The main advantage of this technique is scalability and reusability. Nevertheless, as the data for encryption increases, the computational complexity also increases. However, in future with the increase in processing power of computers, this problem may be solved.

Verma *et al.* [23] have proposed an index based DNA encryption algorithm. The plain text messages are encrypted into DNA sequences with the help of index of strings and block cipher. The DNA sequence is then sent to the receiver through a secure communication channel. Initially, the plain text or message is converted into ASCII code and then converted into binary code. This binary code is further encoded into DNA sequence. An algorithm is designed to search the key sequence among the encoded DNA sequences. Finally, the sequences are given an index number which acts as the cipher text. It is very hard for any attacker to guess the real message. The main difficulty of this algorithm is to find a secure communication channel in order to send the DNA sequence.

Paspula *et al.* [16] proposed a unique cipher text generation procedure as well as a new key generation method. The key generation method has two rounds. A conventional cryptographic technique generates an intermediate form of cipher text and in the second round the intermediate form of cipher text is converted into final cipher text. The method generates a fake DNA sequence inorder to confuse an intruder. If the application requires a single layer of security then this algorithm unnecessarily increases the time and space complexity.

In [8] biotic pseudo DNA cryptography method has been proposed. The methodology uses splicing system to improve the security. The key is generated in a random fashion, due to this reason the degree and confusion of the algorithm increases and makes the resulting cipher text difficult to de-cipher. Robustness analysis of the method shows that the method is very much secured from common cipher attacks. The implementation of this algorithm requires high tech bio-computational laboratories.

Tanaka *et al.* [47] proposed a DNA cryptographic algorithm which is based on one-way public key. The keys are generated using ODN mixture for Pk_B and solid mixture for Pk_A where Pk_A and Pk_B are public keys A and public key B respectively. The plain text or message is encoded in a DNA sequence with the help of one of the public key. It is furthermore synthesized and ligated both with DNA synthesizer and the remaining public key. In order to decode the DNA sequence, PCR amplification with the help of a secret sequence is done. This is an asymmetric method which has a high level of security but very costly to implement.

Lai *et al.* [41] designed a method which is based on the asymmetric key algorithm. The proposed method uses DNA chip technology where the DNA chip is fabricated with probes. The probes are used for encryption and decryption purpose. This algorithm uses the National Engineering Centre for Biochip at Shanghai as the bank for generating the keys. On the basis of intensity of probes, the value of probes are assigned. If intensity is greater than some threshold, then the value is fixed to 1 else it is 0. The process uses two keys for encryption, one by the sender and another one by the receiver. In first step, the plaintext is converted to ASCII value and then to its equivalent binary code. These binary codes are arranged in the form of a matrix. For 0 and 1 in the matrix, probe 0 and probe 1 are selected respectively. These probes are spotted on the DNA chip and then fabricated. This fabricated chip now becomes the cipher text. The receiver uses hybridization technique and the decryption key to decrypt the cipher text. A light spot in the key indicates high intensity that means 1 and dark spots correspond to 0. The use of two keys in the encryption process increases the complexity of the algorithm.

In [21] the authors have implemented a method which is based on the asymmetric key. The algorithm uses PCR amplification along with DNA digital coding and digital synthesis for encryption of the plain text. PCR amplification is added here to provide security and safeguard during the communication phase. This encryption scheme has high confidential strength and at the same time is very cost effective.

Vijayakumar *et al.* [55] have proposed a technique using DNA cryptography and hyper elliptic curve cryptography to enhance the level of security. In DNA-based elliptic curve cryptographic technique the key size used is quite large hence the message encryption and decryption time increases. The concept of DNA strands is used in order to remove the above limitation. In this method converting the original text message into DNA nucleotide is the first level of security. Koblitz method provides the second level of security. The encoded nucleotide is converted into numbers and then the numbers are mapped into points. These points act as plaintext for encryption using hyper elliptic curve cryptography. This method can be implemented using MATLAB simulation tool. Real time implementation of the algorithm will be a challenging one.

Barman *et al.* [9] have proposed a new method to develop a DNA cryptography technique through a hybrid approach. The technique is composed of traditional DNA cryptography and elliptic curve cryptography (ECC). In this method, the plain text is converted first to ASCII value and then to binary form. A DNA nucleotide is taken from publicly available sequences which will be known to both sender and receiver. These nucleotide bases are converted to binary form using DNA encoding scheme. Several pairs of binary numbers are produced and all these pairs are concatenated to generate a long binary number. Encoding is done here by following some tables. The Koblitz method is used to convert the decimal numbers into elliptic curve points. These points are again encrypted to another elliptic curve point with the help of ECC encryption expression. The encrypted points are in the form of cipher text points which are sent to the receiver. This DNA-ECC hybrid method is more efficient in terms of security than the present DNA cryptography techniques. It uses a small key size and at the same time has two levels of security. The proposed method can be implemented on FPGA-based embedded system. Since the key size is small, so this method is not very much secured from the brute force attack.

Gogte *et al.* [27] presented a new type of DNA cryptography system based on quantum cryptography for secure communication. Quantum cryptography can be explained as an emerging security technique in which two parties communicate through a quantum channel. It is based on Heisenberg's uncertainty principle and no-cloning theorem. Initially, a simulation of quantum key exchange along with authentication is done. This step is followed by an application of a DNA-based algorithm. The proposed system consists of the following steps. The first step is authentication, which is based on both the traditional and quantum cryptographic methods. Secure key exchange using the BB84 protocol is done in the second step. This protocol is purely a quantum cryptography based method. The designed algorithm follows this protocol as it is except for the method through which random bits and basis are generated. The DNA encryption algorithm uses a symmetric block cipher where the input is a 128 bit key. The method is perfectly secured from the man in the middle attack, eavesdropping, replay-attack, packet sniffing and spoofing. The technique is very expensive to implement in real life.

Cloud computing has become very popular. It has many features like cost effectiveness, resource-ness, sharing and easy to use. Nevertheless, the security provided in the cloud data is one of the main concerns. In [40], the authors have proposed a new DNA-based cryptography method to increase the security of cloud data. The proposed algorithm uses a symmetric key for the encryption process. Initially, the original text is encrypted using a key and then converted to binary text. DNA sequences are selected and converted to the corresponding DNA base pair cipher. Though the algorithm looks simple yet it is very much secured.

As the field of cloud computing started emerging, many companies are embracing this technique. Eventually, there are many risks involved in this technique like theft of data, data leakage *etc.* The concept of multi-cloud has evolved in order to cope up with the problems of cloud computing. In multi-cloud technique, the users' data are split into different parts and uploaded into multiple clouds. In [48] the authors have described a DNA-based cryptographic technique which can be used in multi-cloud computing environment to enhance the security. The proposed strategy is divided into two phases, namely data embedding and data extracting. Initially, the data is converted into binary form and then into DNA sequence. The base pairing rule is applied to the message. The index of nucleotides is searched and matched from the reference. The data is then sent over the cloud. Data extracting phase follows the reverse steps of data embedding phase. The cipher text is converted back to the original text. This step takes place at the receiver side. The security of this algorithm is very strong. The probability for the attacker to guess the message correctly is less than 1 in million chances. This algorithm is implemented using Microsoft Visual Studio 2010 and Microsoft SQL 2008 on Windows 8 platform. This strategy is proved to provide the cloud user with more secured storage. The method has huge time complexity.

In [10] the authors have proposed a DNA-based encryption method using BIG data. The idea is very innovative and tough to crack. If a third party or any unauthorized person tries to retrieve the message, then he or she will only be able to get the DNA sequences, without the key nobody can break the encryption algorithm. When a large amount of data is to be stored using BIG data then the use of this encryption technique is suggested. The designed method uses PHP language and a DNA encoding table for the encryption process. So far BIG data analysis is facing many challenges. Therefore this encryption process can be used to solve some of the problems in BIG data analysis.

5 Discussion

The use of cutting edge technologies and the computational properties of DNA are bringing several cryptographic methods into existence. The key used in these techniques is one of the main factors. It helps to determine the strength of the algorithm. Most of these methods are designed using a symmetric key. These algorithms are efficient, fast and reliable. Nevertheless, if the key is known to the attacker then the method will be cracked in few minutes. The use of an asymmetric key is one solution to this problem. Even if one of the keys is known, without the private key it is impossible to break the algorithm. But asymmetric key increases the computational complexity and making the process slow down. If the data to be encrypted is huge then an asymmetric key is not at all preferred. These disadvantages have paved the way for hybrid cryptographic methods. The use of DNA encryption techniques with quantum cryptography and hyper elliptic curve cryptography methods have become the new area of research. But implementation of these methods will be very costly as well as a challenge to the computer engineers.

6 Conclusion

DNA cryptography provides a medium of ultra-compact information storage. A few grams of DNA can hold about 10^8 terabytes of data. Effective and efficient algorithms are implemented in order to bring DNA computing on a digital level and use it on large scale. In future, DNA encryption will replace the need of digital signature, authorization and digital timestamps as DNA itself is a unique signature. It is fast, reliable and can work in a parallel manner. DNA cryptography has a wide range of applications and can be implemented in various fields like mobile networks, cloud computing, multi-cloud computing, plain-text messages, images, videos, servers *etc.* Exploring the various characteristics of DNA molecule and using it in the field of cryptography is one of the main concerns among the researchers. In order to increase more security, work can be done on developing asymmetric keys which will make the system more secure. The encryption schemes used in the four cryptography techniques *i.e.* traditional cryptography, DNA cryptography, elliptic curve cryptography and quantum cryptography is being interchanged with each other and as a result new hybrid techniques are being invented. DNA has the potential to explore the further biological molecule based computation methods. The invention of energy efficient DNA computer chip by IBM has opened up new gates for a bright future in this field. DNA cryptography is in its primary phase and hence it's implementation will need bio-molecular labs and costly instruments which are major constraints for the smooth progress in this field.

References

[1] H. M. Abdelkader, F. E. Ibrahim, M. I. Moussa, "Enhancing the security of data hiding using double DNA sequences," in *Industry Academia Collaboration Conference (IAC'15)*, 2015. (https://www.researchgate.net/publication/278028006_Enhancing_the_Security_of_Data_Hiding_Using_Double_DNA_Sequences)

[2] L. M. Adleman,"Molecular computation of solutions to combinatorial problems," *Science*, vol. 266, no. 5187, pp. 1021-1025, 1994.

[3] A. Aggarwal, P. Kanth, "Secure data transmission using DNA encryption," *International Journal of Advanced Research in Computer Science*, vol. 5, no. 6, pp. 57-61, 2014.

[4] T. Anwar, A. Kumar, S. Paul, "DNA cryptography based on symmetric key exchange," *International Journal of Engineering and Technology (IJET'15)*, vol. 7, no. 3, pp. 938-950, 2015.

[5] B. Arazi, C. M. Gearheart, E. C. Rouchka, "DNA-based active logic design and its implications," *Journal of Emerging Trends in Computing and Information Sciences*, vol. 3, pp. 756-766, 2012.

[6] M. A. Athitha, M. A. Akshatha, B. Vandana, "A review on DNA based cryptographic techniques," *International Journal of Science and Research*, vol. 3, no. 11, pp. 2819-2824, 2015.

[7] S. T. Amin, S. E. Gindi, M. Saeb, "A DNA-base implementation of YAEA encryption algorithm," in *International Conference on Computational Intelligence*, pp. 120-125, 2006.

[8] E. S. Babu, M. H. M. K. Prasad, C. N. Raju, "Inspired pseudo biotic DNA based cryptographic mechanism against adaptive cryptographic attacks," *International Journal of Network Security*, vol. 18, no. 2, pp. 291-303, 2016.

[9] P. Barman, B. Saha, "An efficient hybrid elliptic curve cryptology system with DNA encoding," *International Research Journal of Computer Science*, vol. 2, no. 2, pp. 33-39, 2015.

[10] M. S. S. Basha, I. A. Emerson, R. Kannadasan, "Survey on molecular cryptographic network DNA (MCND) using big data," in *Procedia Computer Science of 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)*, vol. 50, pp. 3-9, 2015.

[11] M. Bhavithara, A. P. Bhrintha, A. Kamaraj, "DNA-based encryption and decryption using FPGA," *International Journal of Current Research and Modern Education (IJCRME'16)*, pp. 89-94, 2016.

[12] M. E. Borda, T. Hodorogea, O. Tornea, "Secret writing by DNA hybridization," *ACTA TECHNICA NAPOCENSIS*, vol. 50, pp. 21-24, 2009.

[13] Z. Cao, L. Liu, Z. Guo, "Ruminations on attribute-based encryption," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 9–19, 2018.

[14] C. C. Chang, M. S. Hwang, "Parallel computation of the generating keys for RSA cryptosystems", *Electronics Letters*, vo1. 32, no. 15, pp. 1365–1366, 1996.

[15] S. Chavan, "DNA cryptography based on DNA hybridization and one time pad scheme," *International Journal of Engineering Research and Technology (IJERT'13)*, vol. 2, no. 10, pp. 2679-2682, 2013.

[16] K. Chiranjeevi, S. L. Kumar, R. Paspula, "Hidden data transmission with variable DNA technology," *International Journal of Electronics and Information Engineering*, vol. 7, pp. 41-52, 2017.

[17] R. Chakraborty, G. Rakshit, B. Roy, "Enhanced key generation scheme based on cryptography with DNA logic," *International Journal of Information and Communication Technology Research*, vol. 1, no. 8, pp. 370-374, 2011.

[18] T. Y. Chang, M. S. Hwang, J. W. Li, C. C. Yang, "Simple generalized group-oriented cryptosystems using ElGamal cryptosystem," *Informatica*, vol. 14, no. 1, pp. 111-120, 2003.

[19] C. C. Chang, M. S. Hwang, K. F. Hwang, "An ElGamal-like cryptosystem for enciphering large messages," *IEEE Transactions on Knowledge and Data Engineering*, vol. 14, no. 2, pp. 445-446, 2002.

[20] K. Chugh, H. Dhaka, H. Singh, A. K. Verma, "DNA based cryptography: An approach to secure mobile networks," *International Journal of Computer Applications*, vol. 1, no. 19, pp. 77-80, 2010.

[21] G. Cui, L. Qin, Y. Wang, X. Zhang, "An encryption scheme using DNA technology," in *IEEE International Conference of Bio Inspired Computing: Theories and applications*, pp. 37-42, 2008.

[22] M. Darbari, V. Prakash, "A new framework of distributed system security using DNA cryptography and trust based approach," *International Journal of Advancements in Research and Technology*, vol. 3, no. 3, pp. 1-4.

[23] M. Dave, R. C. Joshi, A. K. Verma, "Securing Ad hoc networks using DNA cryptography," in *IEEE International Conference on Computers and Devices for Communication*, pp. 781-786, 2006.

[24] S. Deb, N. Kar, A. Majumder, M. C. Pal, A. Saha, "Data security and cryptography based on DNA sequencing," *International Journal of Information Technology and Computer Science (IJITCS'13)*, vol. 10, no. 3, pp. 24-32, 2013.

[25] B. Fu, Y. Zhang, X. Zhang, "DNA cryptography based on DNA fragment assembly," in *IEEE International Conference Information Science and Digital Content Technology (ICICDT'12)*, vol. 1, pp. 179-182, 2012.

[26] L. Gehlot, R. Shinde, "A survey on DNA-based cryptography," *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET'16)*, vol. 5, no. 1, pp. 107-110, 2016.

[27] S. Gogte, T. Nemade, P. Nalawade, S. Pawar, "Simulation of quantum cryptography and use of DNA-based algorithm for secure communication," *IOSR Journal of Computer Engineering*, vol. 11, no. 2, pp. 64-71, 2013.

[28] N. Gulati, S. Kalyani, "Pseudo DNA cryptography technique using OTP key for secure data transfer," *International Journal of Engineering Science and Computing*, vol. 6, no. 5, pp. 5657-5663, 2016.

[29] T. Gulom, "The encryption algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 59-71, 2017.

[30] T. Gulom, "The encryption algorithm AES-PES16-1 and AES-RFWKPES16-1 based on network PES16-1 and RFWKPES16-1," *International Journal of Electronics and Information Engineering*, vol. 3, no. 2, pp. 53–66, 2015.

[31] T. Gulom, "The encryption algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4," *International Journal of Electronics and Information Engineering*, vol. 8, no. 1, pp. 20–31, 2018.

[32] B. L. Hao, H. C. Lee, S. Y. Zhang, "Fractals related to long DNA sequences and complete genomes," *Chaos Solitons Fractals*, vol. 11, pp. 825-836, 2000.

[33] M. S. Hwang, K. F. Hwang, I. C. Lin, "Cryptanalysis of the batch verifying multiple RSA digital signatures", *Informatica*, vol. 11, no. 1, pp. 15-18, Jan. 2000.

[34] M. S. Hwang, P. C. Sung, C. S. Tsai, "Blind signature scheme based on elliptic curve cryptography," *Journal of Computer Society of India*, vol. 34, no. 3, pp. 58-60, July 2004.

[35] M. S. Hwang, C. S. Tsai, S. F. Tzeng, "Generalization of proxy signature based on elliptic curves," *Computer Standards and Interfaces*, vol. 26, no. 2, pp. 73-84, Mar. 2004.

[36] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of Proxy Signature Based on Elliptic Curves", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73–84, 2004.

[37] S. Jain, M. Rani, Asha, "Enhancing asymmetric encryption using DNA-based cryptography," *International Journal of Computer Science Trends and Technology (IJCST'14)*, vol. 2, no. 3, pp. 7-11, 2014.

[38] A. Kahate, *Cryptography and Network Security*, Third Edition, Mc Graw HIll, 2016.

[39] N. S. Kazazi, M. R. N. Torkaman, "A method to encrypt information with DNA-based cryptography,"

International Journal of Cyber Security and Digital Forensics (IJCSDF'15), vol. 4, no. 3, pp. 417-426, 2015.

[40] A. Kumar, V. K. Pant, "DNA cryptography a new approach to secure cloud data," *International Journal of Scientific and Engineering Research*, vol. 7, no. 6, pp. 890-895, 2016.

[41] X. Lai, "Asymmetric encryption and signature method with DNA technology," *Science China Information Sciences*, vol. 53, no. 3, pp. 506-514, 2010.

[42] C. C. Lee, M. S. Hwang, L. H. Li, "A new key authentication scheme based on discrete logarithms", *Applied Mathematics and Computation*, vol. 139, no. 2, pp. 343-349, July 2003.

[43] L. H. Li, S. F. Tzeng, M. S. Hwang, "Generalization of proxy signature based on discrete logarithms", *Computers & Security*, vol. 22, no. 3, pp. 245–255, 2003.

[44] T. Mahalaxmi, B. B. Raj, J. F. Vijay, "Secure data transfer through DNA cryptography using symmetric algorithm," *International Journal of Computer Applications*, vol. 133, no. 2, pp. 19-23, 2016.

[45] A. Mersaid, T. Gulom, "The encryption algorithm AES-RFWKIDEA32-1 based on network RFWKIDEA32-1," *International Journal of Electronics and Information Engineering*, vol. 4, no. 1, pp. 1–11, 2016.

[46] R. Nag, A. Nath, D. Roy, "Image encryption using DNA encoding techniques: A brief overview," *International Journal of Advance Research in Computer Science and Management Studies*, vol. 4, pp. 112-119, 2016.

[47] A. Okamoto, I. Saito, K. Tanaka, "Public key system using DNA as a one way function for distribution," *Biosystem*, vol. 81, no. 1, pp. 25-29, 2015.

[48] B. D. Phulpagar, R. H. Ranalkar, "DNA based cryptography in multi cloud security strategy and analysis," *International Journal of Emerging Trends and Technology in Computer Science (IJETICS'14)*, vol. 3, no. 2, pp. 189-192, 2014.

[49] K. Priyadarshani, R. Bama, S. Deivanai, "Secure data transmission using DNA sequencing," *IOSR Journal of Computer Engineering (IOSRJCE'14)*, vol. 16, no. 2, pp. 19-22, 2014.

[50] T. Purusothaman, K. Saravanan, "DNA-based secret sharing algorithm for multicast group," *Asian Journal of Information Technology*, vol. 15, no. 15, pp. 2699-2701, 2016.

[51] B. B. Raj, V. Panchami, "DNA-based cryptography using permutation and random key generation method," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 3, no. 5, pp. 263-267, 2015.

[52] K. G. Raju, P. S. Varma, "Cryptography based on DNA using random key generation scheme," *International Journal of Science Engineering and Advance Technology*, vol. 2, no. 7, pp. 168-175, 2014.

[53] R. O. Sinnot, Z. Yupeng, Z. Yu, W. Zhong, "Index based symmetric DNA encryption algorithm," in *IEEE 4th International Congress on Image and Signal Processing*, pp. 2290-2294, 2011.

[54] S. F. Tzeng, M. S. Hwang, "Digital signature with message recovery and its variants based on elliptic curve discrete logarithm problem", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 61–71, Mar. 2004.

[55] P. Vijayakumar, V. Vijayalakshmi, G. Zayaraj, "Enhanced level of security using DNA computing technique with hyper elliptic curve cryptography," *ACEEE International Journal on Network Security*, vol. 4, no. 1, pp. 1-5, 2013.

[56] X. Wei, Q. Zhang, S. Zhou, "An efficient approach for DNA fractal based image encryption," *Applied Mathematics and Information Sciences*, vol. 5, no. 3, pp. 445-459, 2011.

Biography

Animesh Hazra is working as Assistant Professor in Jalpaiguri Government Engineering College, India. He has received master degree in Computer Science and Engineering from Jadavpur University in 2005. His area of expertise includes network security, cryptography, data mining, computer graphics and image processing. He has published several papers in international journals and conferences.

Soumya Ghosh is pursuing B.Tech. in Information Technology from Jalpaiguri Government Engineering College, India. His area of interest includes network security, cryptography and data mining.

Sampad Jash is pursuing B.Tech. in Information Technology from Jalpaiguri Government Engineering College, India. His area of interest includes network security and cryptography.