DNA Based Cryptography Techniques with Applications and Limitations

Gambhir Singh, Rakesh Kumar Yadav

Abstract:Cryptography techniques and systems have been developed for data security.DNA cryptography techniques are much better as compared to Quantum cryptography techniques and modern cryptography techniques. This type's cryptography is a fresh and growing paradigm in the field of cryptography for secure communication on a different application. DNA cryptography is based on genetic information transfer from one generation to the next generation. This type of cryptography uses DNA molecules which have very high dense storage capacity and large scale parallelism. So, this technique provides fast and secure data transfer from one end to another end with low power consumption. In this paper, many approaches based on DNA cryptography have been discussed with applications and limitations.

Keywords* : *Cryptography, DNA, DNA Based cryptography.

I. INTRODUCTION

The geographical area and users of the internet are increasing rapidly with the development of network technology. A large number of users transferring a lot of information on the network. With the growth of users and internet security challenges, it is necessary to protect the data from unauthorized access. Unauthorized access can steal valuable information of the users or destroy the confidentiality and integrity of data. There are many fields like military, banking, email systems e-commerce, and government who cannot tolerate any confidentiality and integrity of data. Cryptography [37] is used to protect the information by transferring it into an unreadable format. The authorized user can convert this unreadable format in readable is known as decryption of data. There are private, and public keys are used to encode or decode the information. DNA based cryptography is an innovative and growing paradigm in the study to have secure communication on a network. DNA cryptography exists more secure than the Quantum cryptography and modern cryptography because it hides the data in DNA digital form.DNA cryptography ensures security data with the use of cryptographic algorithms.

II. DNA COMPUTING

In 1994, A.Adleman [2] suggested things similar to DNA based computing is growing to a "molecular revolution," which finally will have a theatrical effect on the world. A. Adleman explained the use of DNA in computer science, and he provides the solution of 7 node Hamiltonian Graph Problem which an NP-complete problem like traveling salesman problem. Although the result to a seven- node instances are trivial. It was the first practical which explains the use of DNA in the field of computing. That was the to shown have potential as a means to solve some other large scale problems.

In 1997, Mitsunori Ogihara [1], Animesh Ray two scientists recommended and explained the Boolean based circuit with its implementation. In 2002, Rehovot, Israel, from scientists belonged to Weizmann Institute of Science proposed a programmable molecular computing device in which enzymes and DNA molecules were used in its place of silicon microchips. In, 2004, Shapiro, Benenson,Binamin Gil,Ben-Dor,and Adar belong to Weizmann Institute publicized in the journal Nature that they designed a new DNA based computer which has input and output device would academically be skilled of identifying cancerous deceases within a cell of the living organism and providing drug to encounter cancer. In, 2013, scientists provide DNA digital data storage which was capable of storing a JPEG picture, a set of Shakespearean sonnets, and an audio file of Martin Luther King, Jr's speech...

In, 2013, scientists designed a biological transistor(transcriptor).

III. DNA

DNA-Deoxyribonucleic acid contains genetic information needed to carry out cell activities.DNA is a natural molecule known as nucleic acid. The nucleic acid is molecules consists of a linking chain of repeating molecules, which is also known as polymers. Chain of repeating molecules is called monomers. Nucleotides are monomers of nucleic acid which made up of three portions: a phosphate group, a sugar, and nitrogenous base. Deoxyribonucleic acid is a double standard revealed by Watson and Crick, and so it is also known as the structure of double-helical DNA. The composition of monomers made nucleic acid also called as deoxyribonucleotides.

Revised Manuscript Received on October 30, 2019.

* Correspondence Author

Gambhir Singh*, Research Scholar, Computer Science and Engineering, IFTM University, Moradabad, India. Email: gambhirmtech@gmail.com

Dr.Rakesh Kumar Yadav, Department of Computer Science and Engineering, IFTM University, Moradabad, India. Email: rkyiftmuniversity@yahoo.com

A phosphate group, the sugar deoxyribose, and one of four nitrogenous bases made up deoxyribonucleotide.DNA has four adenine-A,thymine-T, cytosine-C and guanine –G different nitrogenous bases. These four A, T, C, and G are different nitrogenous bases contain the genetic information of a living organism. After transcribed into messenger RNA and finally read at the ribosome to make a protein. There are two types of nitrogenous base based on their shape, thymine and cytosine are made a single carbon ring skeleton called pyrimidines, and adenine and guanine are made of two carbon ring skeletons together called purines.

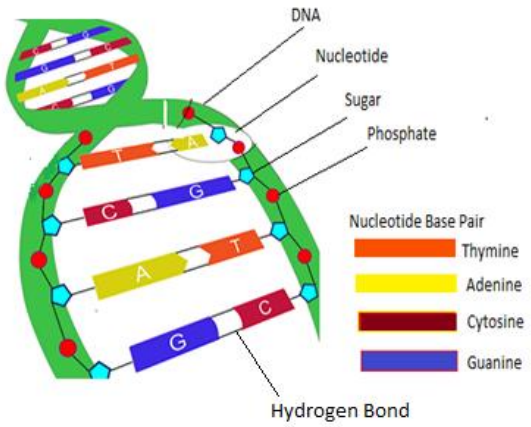

Fig. 1.The structure of double-helical DNA.

A. Operations on DNA

Many biological operations [3, 5, 6] 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. Addition and subtraction are the basic arithmetic operations which can be applied on DNA nucleotides.DNA nucleotides have nitrogenous bases adenine-A,thymine-T,cytosine-C and guanine–G represented as 00, 01, 10 and 11 respectively. Addition and subtraction can be applied on DNA nucleotide's bases according to the binary rules for example binary addition of 10 and 01 will be 11 similarly addition of C and T will be G.If 00 is subtracted from 10 then the result will be 10. Similarly, A is subtracted from C the result will be Different logical operations can be implemented on DNA sequence.

IV. DNA CRYPTOGRAPHY

In 1994, A.Adleman [2] said things similar to DNA based computing is growing to a "molecular revolution," which finally will have a theatrical effect on the world. A. Adleman explained the use of DNA in computer scince ,and he provide the solution of 7 node Hamiltonian Graph Problem which a NP-complete problem like traveling saleman problem. Although the result to a seven- node instances are trivial. It was the first practical which explains the use of DNA in the field of computing. That was to shown have potential as a means to solve some other large-scale problems. Now it has been discovered that DNA computing [2] having several following advantages:

- A single gram of DNA contains 700 terabytes of information.so it is a very compact way to store the massive amount of data.
- DNA Computers are very fast as Compare to electronic computers..
- DNA computer needs very fewer power requirements as compared to modern-day electronic machines.

DNA based Cryptography [2] is the branch of computing.DNA based cryptography is the technique of hiding data and information using biological structure. Nowadays researcher is working on the field of cryptography is concentrated on the use of DNA code to encode binary information in one form or another form. So, DNA computing may be other techniques for securing data and information. DNA encryption is a technique to convert the plain text into ciphertext with the use of DNA sequence. There are following four DNA encryption techniques.

A. DNA random One Time Pad Based

In this technique, a set of randomly organized non-repeating characters used for implementing one-time pad because if an input ciphertext is used once it is not used again to increase the security. In this scheme, the size of the plain text should be equivalent to a one-time pad. To convert the short segments of plain text messages to ciphertext, DNA onetime pad process is used. A random and unique codebook is taken into account for replacing the plain text. This technique is applicable only on short messages due to hardware limitations. The large size of the message increases the complexity of DNA mapping.

B. DNA chip-based cryptography

The DNA chip is also called microarray. This DNA chip made of nucleic acid and electronic circuit designed by semiconductors. This technology provides excellent progress in the field of DNA based cryptography. A DNA-chip is used for storing handling and maintaining a large amount of genome and biological information. Biochemical processes are used to encrypt the text and images. The limitation of this technique is the sudden change in physical factor provides negative results.

C. DNA Fragmentation

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

D. DNA Steganography

DNA Steganography is used for hiding one message inside another message. Image, audio, and video reused to protect a large amount of data, but data can be damaged due to the sudden change in environment.

V. DNA BASED CRYPTOGRAPHIC TECHNIQUES (LITERATURE SURVEY)

In 2003, Chen et al. [7] proposed a DNA Based cryptographic technique uses molecular theory to encrypts/decrypts the two-dimensional images using a one-time pad(OTP).

In 2004, Gehani et al. [8] provide a platform for DNA cryptographic technique based upon molecular theory using a one-time pad (OTP) for complete secrecy, Vernam's and Shannon: originator of one -time pad(OTP). Authors have offered a secure scheme in which it was challenging to guess the encrypted message. They used DNA- Chip, and OTP.

In 2005, Tanaka et al. [9] offered DNA cryptography, which uses Public Key. In this method, they discussed the generation of public keys through solid mixture or PkA and ODN mixture for PkB. After the generation of keys, the data is converted into DNA code by using one of the public key synthesized with the DNA synthesizer and then converted message sequence is produced with the one more public key. The result of the earlier process is now transferred to the immobilization procedure, and then for PCR amplification, this PCR amplification is completed by using secret sequence, for decoding the converted/encrypted DNA sequence.

In 2006,Amin et al. [10] offered the DNA based cryptographic method which is based on the symmetric key cryptography, In this technique keys, are accessed from genetic database system which will be same for encrypting and decrypt at the ends.

In 2008, Verma et al. [11] suggested a Pseudo-DNA cryptographic technique for providing security for routing protocol in Mobile Ad hoc Networks.This DNA based cryptography technique uses the central dogma of molecular biology. In this technique routing information are stored in the form of DNA code then convert into messenger RNA. Messenger RNA convert into proteins which are known as cipher text.The cipher text is transferred to the recipient through the secure channel. The same key with OTP will be applied at both ends for encryption and decryption.

In 2008,Cui et al. [12] suggested the DNA based cryptographic method uses the public key, DNA synthesizer, digital coding of DNA and PCR amplification which provides the safety precaution during the excellent confidential strength communication between sender and receiver.

In 2010, Xuejia et al. [13] suggested asymmetric DNA cryptography technique using DNA-chip technology. The chip is fabricated with probes. There are two types of inquiries used; one at the sender side for encryption and another probe is used at receiver side for decryption of the message.

In 2011, Deepak Kumar et al. [14] suggested a data writing technique which was secrete based on DNA cryptography. Authors took a sample of "HELLO" as a message, and an ssDNA OTP key will be 70 times longer than message size gets generated and performed encryption and decryption on the plaintext using the same key. Due to the large size of key the hacker has to search among 4310 different ssDNA string, which is terrible for the hacker.

In 2012, Pramanik et al. [15] suggested a parallel and less time-consuming DNA cryptography technique. This technique uses DNA sequence and hybridization. Authors explained how fast and secure message is transferring between two sides.

In 2012, Zhang et al. [16] suggested the DNA based cryptography technique which uses DNA fragment assembly. In this process, authors demonstrated how the plaintext is changed into binary code by the sender, and it transformed into a long chain of DNA code, this DNA is again divided into small size DNA chains. In this method Key of shortchain placement is in the fragments which is forwarded to the recipient as encoded text and then recipient decode encoded text and starts small part reassembly to decrypt the plaintext.

In 2013, Tornea et al. [17] suggested a DNA cryptographic technique which uses DNA indexing. Authors access a random DNA code from the database which contains genetic information as an OTP key, and this sequence sent to a receiver via a secure communication channel. To encrypt the plain text is converted its ASCII code form and then to the binary code again transformed it into the adenine -A, thymine -T, cytosine -C) and guanine –G. This form of DNA is to be searched in the key sequence; along with index numbers are noted. The array of integer numbers obtained is the required cipher text. This cipher text is decoded by the receiver using key and index pointer.

In 2015, N. S. Kazazi et al.[18] provided a five-stage algorithm which is DNA based cryptography used to encrypt information. In this technique, five stages include data preprocessing, key generation, and encryption process at the sender end and decryption and data post-processing at the receiver end. This technique is based on vigenere cipher and provides a double layer of security. This is a secret key cryptographic technique takes huge running time.

Anwar et al. [4] provide an XOR operation based method which uses the symmetric key to encrypt plain text. This technique can be used for an insecure channel like the internet. This technique is very easy and strong. DNA hybridization and matrix calculations are used to decrease the running time of this technique. This technique is very cost-effective.

Bama et al. [19] proposed a method which uses DNA sequence and substitution techniques. Plain text is encoded using the substitution technique and DNA sequence, which is selected from 55 million. So, this selection of DNA sequence and substitution make it very secure, simple, efficient, and 5nalyzin. The proposed algorithm is already implemented in an Electronic Medical Record System.

In,2014 Raj et al.[21] proposed a DNA-based cryptography technique which used random key generation and permutation. This technique uses the idea of DNA pattern generation in a random fashion. Initially, input data is transformed into 7-bit ASCII code format then this form of data is transformed into binary form.

Table-I: Transformation of binary code format to a DNA sequence

DNA Sequence	Binary code
00	**A**
01	**C**
10	**T**
11	**G**

A DNA sequence is selected as a key and gathered in blocks where each block contains four characters. A table is formed on the basis of how the characters occupy the block positions. Finally, from this table, the randomly selected DNA sequence gets converted into an encrypted form. The cipher sequence and key is transfer to the receiver through the communication medium. The DNA sequences are decoded by following Table-I. The reverse steps are applied to get back the same 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,2016 Mahalaxmi ,et al.[22] proposed a DNA based symmetric key cryptography for secure data transfer over the communication channel. Firstly Input data, image or text converted into ASCII value, ASCII value is transformed into its binary form, Binary form transformed into DNA code then this code is randomly allocated based on a private key and is converted to the extended ASCII code. At last, the input is encrypted using DNA code, and clinical permutation is done with the private key. Java is used to implement this modern symmetric key encryption technique. DNA chromosome is required for data transmission over the communication medium.

In 2016, Gulati et al. [23] suggested a new technique based on DNA cryptography, this technique uses XOR operation and one-time pad (OTP) for secure data transmission. This algorithm provides three levels of security because it consists of arithmetic operation or XOR operation, one-time pad, and DNA complementary rule. This technique is very easy and secured to random OTP.OTP is hard to guess by the hacker. This technique is not so userfriendly because of some preconditions applied, so need to take the precaution of the preconditions while picking the OTP.

In 2016, Sravanan et al. [24] suggested a technique which is based on the modified Shamir's secret algorithm and DNA-based encryption and decryption technique. A large no. of user are sitting on receiver's end. Some added security is merged in the algorithm. Decryption only possible when the entire clients are involved in the decryption process, only then the secret message can be decoded. The message is converted into ASCII values using Mathematical calculations. ASCII value converted 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 technique implemented in Java and Python. The technique is useful for a group, and if anyone is not involved, then the message decryption is impossible.

In 2016, Kamaraj et al. [25] proposed a symmetric key algorithm with double-layer security. In this technique, plain text is encoded twice at sender end with a key size 100 and applied the reverse process at the receiver. In this algorithm first step is encryption, which converts plain text into ciphertext, and the second step is decryption, which provides original data from the ciphertext. Here, Palin text is given to the FPGA(Field-Programmable Gate Array) through PS2 keyboard which is read by the FPGA as ASCII value codes. Then it is converted to the codon by a codon table, and Vigenere cipher is used for the encryption of the codon. The distribution of key is not discussed here; hence, it can be a hectic problem for the algorithm.

In 2014,Darbari et al. [26] proposed a trust-based approach which provides a new structure for distributed system security with the assistance of DNA cryptography. It is reputation, and rule-based approach evaluates the trustmanagement.This approach contains three phases, i.e., proof collection, reputation factor approximation, and reputation confidence. The trust-based distributed systems are tremendously secure in dealing with security features. DNA based cryptography enhance the security trust-based distributed system. Data post-processing method is combined into this technique to deal with many cyber-attacks. This technique is appropriate to only trust-based distributed systems but not applicable for all.

In 2011, Roy et al. [27] proposed a method in which keys are generated based on DNA synthesis. This system improves the encryption and decryption process. Two-levels of keys are used in this technique; the first level of the key is used to transform the plain text into primary ciphertext with the encryption algorithm. The second level key is used to enhance the security of this method. Due to two level of keys, this method is robust against brute force attack. A hacker would take to break the ciphertext more than six-month using the computer. Running time and space taken in this method is very high.

In 2014, Aggrawal, et al.[28] proposed a complementary pair technique which is different from traditional DNA encryption method. In first step DNA's four different DNA sequence A,T,C and Gare complemented A with T, G with C ,C with A, and T with G. after that in second step DNA reference sequence is selected and named as sender and reciever are awre with S. In the third step, S is then complemented and named as S'. This S' is then sent to the receiver by using any stenographic technique. The receiver will decrypt ciphertext S' with the help of S. Application of steganography enhances the security of the proposed method. To decrypt the message, an attacker has to guess the randomly generated sequence S. approximately 55 million publicly DNA sequences exist. Hence it will be substantial to crack S. This makes the algorithm a robust and reliable one.

In2014, Rani et al. [29] proposed a DNA cryptographic technique which uses XOR operations. In these techniques, plain text is selected, which has to be encrypted, then a random key is generated. A Randomized codon list is also generated and XOR-ed with the random key. Swap complement operation is applied to create the encrypted message. The key is made based on DNA properties and biotechnology. Due to the XOR operation, this technique is speedy, and time complexity is O (log N). But space complexity can be improved in the future.

In 2016, E. Suresh Babu et al. [33] proposed an inspired pseudo biotic DNA cryptography. It uses the central dogmas of biology. This is dissimilar to DNA cryptography but only uses terminology and mechanism of DNA. In this method, encryption and decryption are performed using transcription, splicing, and translation. These steps of encryption are used to improve security. In this method, the key is generated randomly to increase the degree of confusion and diffusion, which makes this algorithm challenging to break the ciphertext. Robustness analysis is performing to justify that the algorithm is very much secured against attacks. The implementation of this algorithm requires high tech biocomputational laboratories.

In 2005, Tanaka et al. [31] suggested an asymmetric DNA encryption algorithm in which two public keys using ODN mixture and solid mixture. This algorithm uses the public key. So the data is encrypted in a DNA form using one the public key. After that, It is synthesized and ligated together with DNA synthesizer and remaining public key. To decipher the DNA sequence, PCR Amplification used with the assistance of a secret series is done. This algorithm provides excellent security, but it takes a high cost to implement.

In 2015, Barman et al. [9] suggested a hybrid scheme to secure a DNA cryptography technique using elliptic curve cryptography (ECC). It uses encoding phase for encoding and ECC for encryption so is provides two levels of security. In this scheme, the key size is used for encoding is very small. This technique is fast, takes a low memory, and uses small size keys. This is hard to unbreakable by eavesdropper because of two-levels of security. It is strong against a brute force attack.FPGA based embedded system required to verify the practical implementation of this DNA-ECC cryptographic scheme.

In 2015, Basha, et al.[32] proposed a modern and secure DNA-based encryption algorithm which uses BIG data. In this method, an unauthorized person can access ciphertext of the message without essential nobody can read this cipher. This algorithm is used to encrypt a large amount of data using big data. In this method the encryption process uses DNA encoding table and PHP language. This algorithm used to solve significant data challenges and big data analysis.

In 2017, Zhang et al.[34] suggested DNA based cryptography, which uses hamming code and a block cipher to provide security for a key. It is crucial symmetric cryptography, which is used to optimize a DNA based technique. In this technique, the maximum length matching technique has also been established to protect against different attacks.

In 2018, Tiwari et al.[35] recommended a scheme in which the DNA mapping technique was offered for ECC. In this method the DNA code is random, and non-repetitive subsections are allotted to alphabets. Then these alphabets are used for encoding and decoding at the two ends.. This scheme was effectively employed and used in real-time internet of things devices.

In 2018, Sohal et al.[30] introduced a new method with the cryptographic technique. In this technique, client-side data is encrypted before storing it in the cloud. This is a symmetric-key cryptography scheme which uses DNA cryptography. Apart from presenting the thorough design of this approach, and comparing it with the present symmetric-key algorithms (DNA, AES, DES, and Blowfish), the experimental results show that this method leaves behind the traditional algorithms based on ciphertext size, encryption time, and throughput. Hence this new method is much more efficient and performs better.

In 2019, El-Latif et al.[36] suggested a method which has two rounds of encryption. This scheme is the same as the existing technique named the Data Encryption Standard (DES) algorithm. In this method, two keys are used for encoding the plaintext. These two keys are made up of the elliptic curve cryptography (ECC), and Gaussian kernel function (GKF) and another key is created on random based injective mapping on the second characters repeated in the first key. At last, the encryption message arbitrarily hides in the second DNA sequence based on the numbers from GKF.

Table- II: Comparison of Different DNA based Cryptographic algorithm (Related Work History)

S.No	Year of proposed	Algorithm Name	Cryptographic Method	Technique Used	Applications	Limitations
1	2003	DNA-based, Bimolecular Cryptography Design [7]	Symmetric key cryptography	OTP, Bimolecular	Short message sequences, two-dimensional images	A short message can be encrypted
2	2004	DNA-based cryptography, In Aspects of Molecular Computing [8]	Symmetric key cryptography	Bimolecular, OTP,	Encoding of messages	A short message can be encrypted
3	2005	A public-key system using DNA as a one-way function for key distribution [9]	Asymmetric key cryptography	Biomolecular, PCR amplification, DNA synthesis.	Encoding of messages	High running time
4	2005	A public key system using DNA [31]	Asymmetric key cryptography	The DNA sequence, PCR Amplifier, DNA synthesizer	Encoding of messages	High cost required
5	2006	A DNA-based implementation of YAEA encryption algorithm [10].	Symmetric key cryptography	Substitution method, OTP	Multi-level security applications	High running time
6	2008	DNA cryptography: a novel paradigm for secure routing in MANETs [11].	Symmetric key cryptography	The central dogma of biomolecular biology, OTP	To encrypt routing information	Only for short message

7	2008	An encryption scheme using DNA technology, In Bio-Inspired Computing: Theories and Applications, [12].	Asymmetric key cryptography	Synthesis, digital coding, PCR amplifier.	Message encryption	High time &space complexity
8	2010	Asymmetric encryption and signature method with DNA technology [13].	Asymmetric key cryptography	DNA- chip-based, Hybridization Technology	Message encryption	Based on hardware
9	2011	Secret Data Writing Using DNA [14].	Symmetric key cryptography	OTP	secret data writing	Once the detected message is known, format-specific
10	2011	Enhanced key generation scheme based on DNA logic[27]	Symmetric key cryptography	DNA synthesis, Two-level key	Message encryption	High time & space complexity
11	2012	DNA based Cryptography [15].	Symmetric key cryptography	OTP, Hybridization technology.	Message encryption	High computational complexity
12	2012	DNA based Cryptography Based on Fragment Assembly [16].	Symmetric key cryptography	The DNA sequence, Fragment assembly.	Internet application	An early stage of DNA cryptography
13	2013	Security and Complexity of DNA Cipher [17].	Symmetric key cryptography	DNA Index is used, OTP,	Message encryption for real-time applications	High time complexity
14	2014	Secure data transmission using DNA sequencing[19]	Symmetric key cryptography	The DNA sequence and substitution techniques	Electronic Medical Record System	Application-Specific
15	2014	DNA cryptography using permutation and random critical generation method [21]	Symmetric key cryptography	random key generation and permutation	Message encryption	Single level security
16	2014	A new framework of distributed system security using DNA and trust-based approach [26]	Symmetric key cryptography	Trust-based approach	trust-based distributed systems	Not applicable to all applications
17	2014	Secure data transmission using DNA encryption [28]	Asymmetric key cryptography	DNA Sequence, stenographic technique	Message encryption	High time complexity
18	2014	Enhancing asymmetric encryption using DNA-based cryptography [29]	Asymmetric key cryptography	DNA Sequence, XOR operations	Text encryption	High space complexity
19	2015	A method to encrypt information with DNA cryptography,[18]	Symmetric key cryptography	Vigenere cipher, DNA chip	Binary data can be encoded	Huge running time
20	2015	DNA based cryptography based on the symmetric key exchange [4].	Symmetric key cryptography	DNA hybridization, matrix calculations, and XOR operation	Internet	Two-part of a key generation scheme
21	2015	An efficient hybrid ECC system with DNA encoding [9]	Asymmetric key cryptography	elliptic curve cryptography (ECC)	Text encryption	FPGA based embedded system required to verify
22	2015	Survey on molecular cryptographic network DNA (MCND) using big data[32]	symmetric key cryptography	DNA Sequence, BIG data	to solve significant data challenges and big data analysis	High Time complexity
23	2016	Secure data transfer through DNA cryptography using symmetric key [22]	symmetric-key cryptography	The DNA sequence and random key generation	Data, text, and image	DNA chromosome required
24	2016	Pseudo-DNA cryptography technique using a one-time pad for secure data transfer[23]	symmetric-key cryptography	XOR operation and OTP	Secure information transmission	Preconditions while picking the OTP
25	2016	DNA-based secret sharing algorithm for multicast group[24]	symmetric-key cryptography	The DNA sequence and modified Shamir's secret algorithm	Tightly secure message transmission for multicast application	Only for text
26	2016	DNA based encryption and decryption using FPGA [25]	symmetric-key cryptography	Field-Programmable Gate Array, Vigenere cipher	Text encryption	Distribution of key is a hectic problem

27	2016	pseudo biotic DNA based cryptographic mechanism against adaptive attacks [33]	symmetric-key cryptography	central dogmas of biology	Text encryption	Implementation cost is high
28	2017	An Optimized DNA Encryption Scheme with Enforced Secure Key Distribution[34]	symmetric-key cryptography	Ham-ming code and a block cipher mechanism	Information encryption	High Time complexity
29	2018	B DNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing [30]	symmetric-key cryptography	Binary DNA	Cloud computing	High time complexity
29	2018	Novel Method for DNA-Based ECC for IoT Devices[35]	Asymmetric key cryptography	D Elliptic curve cryptography (ECC) NA DNA Sequence, Elliptic curve cryptography (ECC)	IoT real-time Applications	High time complexity
30	2019	Information hiding using artificial DNA sequences based on Gaussian kernel function(GKF) [36]	Asymmetric key cryptography	ECC, and Gaussian kernel function (GKF)	Data hiding	High time complexity

VI. CONCLUSION

DNA Cryptography is the branch of computing. One gram of DNA contains 700 terabytes of data. So it is a very compact way to store the massive amount of data.DNA Computers are very fast as compare to electronic computers.DNA computer needs very fewer power requirements as compared to modern-day automatic machines. Hybridization of DNA, DNA synthesis technology, DNA –chip-based technology, the Central dogma of molecular biology, PCR amplification technology, and OTP are used in DNA cryptography to makes it secure then old-style cryptographic schemes which are indestructible by the attackers, due to molecular calculation inherent in it. Symmetric and asymmetric keys are used to provide security to the application.DNA cryptography has a wide range of applications and can be implemented in various fields like mobile networks, cloud computing, IoT devices, Real-time applications, Internet, multicast applications to secure plain-text messages, images, videos, servers, etc. There are some limitations of DNA cryptography depend upon the technology used, keys used, and size of data.

REFERENCES

1. M. Ogihara and A. Ray, "Simulating Boolean circuits on a DNA computer." Algorithmica 25:239–250, 1999.
2. L. M. Adleman, "Molecular computation of solutions to combinatorial problems," Science, vol. 266, no. 5187, pp. 1021-1025, 1994.
3. 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.
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. R. Nag, A. Nath, D. Roy, "Image encryption using DNA encoding techniques: A brief overview," International Journal of Advanced Research in Computer Science and Management Studies, vol. 4, pp. 112-119,2016.
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. Chen Jie (2003), A DNA-based biomolecular cryptography design, Proceedings of IEEE International Symposium, Vol. 3, pp. III-822.
8. Ashish Gehani, LaBean Thomas and John Reif (2004), DNA-based cryptography, In Aspects of Molecular Computing, Springer Berlin Heidelberg, pp. 167-188.
9. Kazuo Tanaka, Akimitsu Okamoto, and Isao Saito (2005), Public-key system using DNA as a one-way function for key distribution, Biosystems 81, 1, pp. 25-29.
10. Sherif T. Amin, Magdy Saeb, and El-Gindi Salah (2006), A DNA-based implementation of YAEA encryption algorithm, In Computational Intelligence, pp. 120-125.
11. A.K. Verma, Mayank Dave, C. Joshi (2008), DNA cryptography: a novel paradigm for secure routing in MANETs, Journal of Discrete Mathematical Sciences and Cryptography, Vol. 11, No. 4, pp. 393-404.
12. Cui Guangzhao, Limin Qin, Yanfeng Wang, and Xuncai Zhang (2008), An encryption scheme using DNA technology, In Bio-Inspired Computing: Theories and Applications, BICTA, 3rd IEEE International Conference on, pp. 37-42.
13. Lai XueJia, MingXin Lu, Lei Qin, Han JunSong, and Fang XiWen (2010), Asymmetric encryption and signature method with DNA technology, Science China Information Sciences 53, no. 3, pp. 506-514.
14. Deepak Kumar, and Shailendra Singh (2011), Secret data writing using DNA sequences, In Emerging Trends in Networks and Computer Communications (ETNCC), IEEE International Conference on, pp. 402-405.
15. Pramanik Sabari and Kumar Sanjit Setua (2012), DNA cryptography, In Electrical & Computer Engineering (ICECE), 7th IEEE International Conference, pp. 551-554.
16. Yunpeng Zhang, Bochen Fu, and Xianwei Zhang (2012), DNA cryptography based on DNA Fragment Assembly, Information Science and Digital Content Technology (ICIDT), 8th IEEE International Conference, Vol. 1, pp. 179- 182.
17. Olga Tornea, and Borda E. Monica (2013), Security and complexity of a DNA-based cipher, In Roedunet International Conference (RoEduNet), 11th IEEE International Conference, pp. 1-5.
18. 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.
19. 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.
20. K. G. Raju, P. S. Varma, "Cryptography based on DNA using random key generation scheme," International journal. Gehlot, R. Shinde, "A survey on DNA-based cryptography," International Journal of Advanced Research in Computer Engineering and Technology.
21. 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.

22. T. Mahalaxmi, B. B. Raj, J. F. Vijay, "Secure data transfer through DNA cryptography using a symmetric algorithm," International Journal of Computer Applications, vol. 133, no. 2, pp. 19-23, 2016.
23. 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.
24. T. Purusothaman, K. Saravanan, "DNA-based secret sharing algorithm for a multicast group,” Asian Journal of Information Technology, vol. 15, no. 15, pp. 2699-2701, 2016.
25. 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.
26. M. Darbari, V. Prakash, "A new framework of distributed system security using DNA cryptography and trustbased approach," International Journal of Advancements in Research and Technology, vol. 3, no. 3, pp. 1-4.
27. 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.
28. 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.
29. 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.
30. Sohal, Sharma, "BDNA-A DNA inspired symmetric key cryptographic technique to secure cloud computing" Journal of King Saud University - Computer and Information Sciences Available online 29 September 2018.
31. 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, 2005.
32. 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.
33. 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.
34. Yunpeng Zhang, Xin Liu, Yongqiang Ma, Liang-Chieh Cheng "An Optimized DNA Based Encryption Scheme with Enforced Secure Key Distribution" Springer Science+Business Media, LLC 2017.
35. Harsh Durga Tiwari, Jae Hyung Kim "Novel Method for DNA-Based Elliptic Curve Cryptography for IoT Devices.ETRI Journal, Volume 40, Number 3, June 2018.
36. Eman I. Abd El-Latif & M. I. Moussa “Information hiding using artificial DNA sequences based on Gaussian kernel function” Journal of Information and Optimization Sciences ISSN: 0252-2667 (Print) 2169-0103 (Online) .

AUTHORS PROFILE

Gambhir Singh received his B.E. degree in Computer Science and Engineering from Krishana Institute of Engineering and Technology,Ghaziabad in 2003.M.Tech degree in Computer Science and Engineering from Shobhit University,Meerut and pursuing Ph.D. in Computer Science and Engineering from IFTM University Moradabad.Currently, he is working in the Department of Computer Science and Engineering of H.R. Institute of Technology,Ghaziabad; He has 14 years of teaching experience. He has published 4 research papers in International Journal and 2 research papers in National and International Conferences. He has attended 7 seminars and workshops. His areas of interests are Network Security, MANETs, Algorithms,and Computer Networks.

Dr. Rakesh Kumar Yadav pursed Bachelor of Technology from Utter Pradesh Technical University, Lucknow ,India, Master of Technology from Singhaniya University Rajasthan and Ph.D. from IFTM University, Moradabad. He has also served at Pant Nagar University of Agriculture & Technology. He is working as an Assistant Professor in Department of Computer Science & Engineering, IFTM University, Moradabad since 2007. He has published more than 19+ research papers in reputed international journals and conferences. His main research work focuses on Biometric, Image Processing, Computer Vision, Soft Computing and Artificial Intelligence. He has 13+ years of teaching experience in higher education.