Journal of Sustainability Science and Management
Volume 17 Number 5, May 2022: 165-178
eISSN: 2672-7226

A THEORETICAL COMPARATIVE ANALYSIS OF DNA TECHNIQUES USED IN DNA BASED CRYPTOGRAPHY

NIK AZURA NIK ABDULLAH[1*], NUR HAFIZA ZAKARIA[1], AZNI HASLIZAN AB HALIM[1], FARIDA HAZWANI MOHD RIDZUAN[1], AZUAN AHMAD[1], KAMARUZZAMAN SEMAN[1] AND SURIYANI ARIFFIN[2]

[1]Faculty of Science and Technology, Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia. [2]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Jalan Ilmu 1/1, 40450 Shah Alam, Selangor, Malaysia.

**Corresponding author: azura@cybersecurity.my*
Submitted final draft: 23 January 2022 *Accepted: 11 March 2022* http://doi.org/10.46754/jssm.2022.05.014

Abstract: Cryptography has been extensively employed in the information security field for the purpose of providing security for confidential data. The field of cryptography has recently considered a hybrid cryptographic implementation that combines conventional cryptographic techniques with the knowledge of DNA technologies to formulate what is known as DNA cryptography. DNA based cryptography is considered a branch of sustainability science as it combines transdisciplinary structures from natural sciences (biology) and technological sciences (information security). This paper discusses the various biological DNA techniques that have been implemented in recent DNA cryptographic algorithms. Among them are the Watson-Crick Complementary Rules, DNA Encoding/Decoding Rules, DNA Operation Rules, the Triplet Codon DNA Code, DNA Segmentation, DNA Hybridisation (DNA Annealing) and DNA Transcription and DNA Replication from the Central Dogma Molecular Biology process. A description of the algorithms and a theoretical comparative analysis of these DNA cryptographic algorithms is also presented in this research paper. Comparisons have also been made based on the following parameters: Conventional cryptographic techniques vis-a-vis the techniques used by DNA cryptographic algorithms, the application of these algorithms, their limitations and a security analysis to see how well DNA cryptography perform as against current conventional cryptography.

Keywords: Cryptography, DNA computing, comparative analysis.

Introduction

What distinguishes humans from other species is their ability to think, process information, communicate and exchange that information with each other. The valuable data that they share may need to be made in secret or privately. Given the rapid development of digital communications, electronic data exchanges and network technologies, private and confidential information can potentially be shared widely over the world wide web. With the widespread use of the Internet, the risk of shared information being exposed to or compromised by unintended recipients is increasing. The security of data in transit is not the only concern, data at rest can also be stolen by unauthorised users. At this point, the confidentiality and integrity of the invaluable information can be destroyed. To overcome this, cryptography has been used to anticipate and address the issue of securing confidential data.

The use of cryptography satisfies the information security triad of confidentiality, integrity and authentication (CIA). Modern cryptography also emphasises an additional characteristic of basic information security called non-repudiation. Cryptography involves the process of transforming a readable information (plain text) into an unreadable format (cipher text). This process is called encryption. Whereas the reverse process of converting the cipher text back to its plain text format is called decryption.

Implementation of cryptography over the Internet enables users to communicate and transfer information securely. It has also been a crucial instrument that allows users to store confidential data in electronic storage units.

There are many cryptographic algorithms currently available ranging from Symmetric Block Cipher, Symmetric Stream Cipher, Asymmetric Cryptographic, Hash Function and so on. However, the continual advancement of technology, has seen an increase in people who consider the art and science of defeating the protections offered by cryptography. The security of most cryptographic algorithms and the infrastructure or platform they are executed on have become more vulnerable to attacks, therefore it is getting easier to break these algorithms. Conventional cryptographic algorithms implemented in binary computers have various physical constraints, especially in data storage and computational processes. It is a common approach for a cryptographic algorithm to have large key space and complicated algorithm to strengthen its security, however, the cryptographic key generation, key retrieval, data encryption and data decryption process becomes more time consuming. The quality of the algorithms used also contribute to the causes for concern. Therefore, since conventional cryptography has severe security problems, the field of information security focuses to new ways of protecting confidential information.

Over the years, there have been many studies by researchers and cryptographers on improving the security and performance of cryptographic technologies. Among them are quantum cryptography and DNA cryptography. DNA cryptography is a new cryptographic method that is inspired by DNA computing that uses DNA molecules as an information carrier and DNA techniques to replace the operations and mathematical computations which exist in conventional cryptography. Due to DNA's natural properties of massive parallelism and huge storage capacity, sustainable solutions to support cybersecurity and privacy can be achieved using DNA cryptography.

This paper will discuss DNA cryptography and work that has been done in the field of DNA cryptography. This paper is organised into four sections as follows: The first section is an introduction to DNA, DNA computing and DNA-based cryptography. The second section describes the basic DNA concepts and techniques that are widely implemented in DNA cryptography field. The third section provides a theoretical comparison of recent works based on DNA cryptography. The final section discusses the conclusions of this research paper.

What is DNA?

DNA, the abbreviation of Deoxyribose Nucleic Acid (DNA) is a complex molecule which contains the genetic information of all living creatures and organisms ranging from the smallest viruses to creatures as complex as human beings. DNA contains information to assemble and maintain cells and instructions to carry out cell activities. Each and every cell of an organism has a complete set of DNA. Each individual has a unique set of DNA.

These unique properties make it possible to identify any living creature individually. For human beings, DNA represents their biological information such as skin colour, hair colour and type, nose and eye shape and even their weight and size. The uniqueness of human DNA structures are passed on from parents to their children and then on to future generations.

The monomer units of DNA, called nucleotides, are the organic molecules that act as the building blocks of nucleic acids. Each nucleotide is composed of a five-carbon sugars called deoxyribose, a phosphate group and one of the four nitrogenous bases which are Adenine(A), Guanine(G), Cytosine(C) and Thymine(T) (Parker *et al.,* 2016). As shown in Figure 1 below (BioNinja), Adenine and Guanine are Purine types of nitrogenous bases whereas Cytosine and Thymine are Pyrimidine types of nitrogenous bases. The polymer unit of DNA, called a polynucleotide, which is made up of nucleotides bonded together to form a chain is known as a DNA strand.

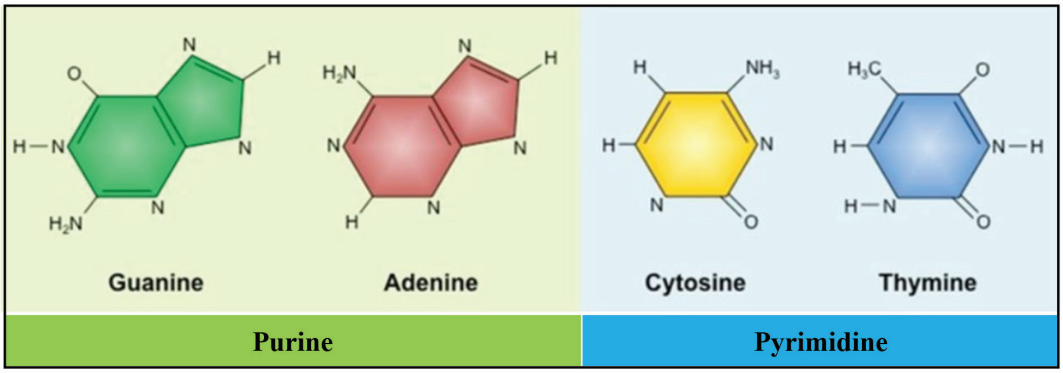

Figure 1: Nitrogenous bases

DNA is combined using base pairing rules known as the Watson-Crick Complementary Rules. These base pairing rules state that each base pair is joined together by hydrogen bonds. Thymine pairs up with Adenine through two hydrogen bonds, whereas Cytosine pairs up with Guanine through three hydrogen bonds. This is shown in Figure 2 (BioNinja).

The DNA structure is usually presented as a double helix with two DNA strands as shown in Figure 3 below (Miller School of Medicine). The double helix structure of DNA was revealed by James Watson and Francis Crick with the help of two other DNA scientists, Rosalind Frankline and Mourice Wilkins in 1953 (Kennepohl *et al.,* 2020). This structure resembles a twisted ladder

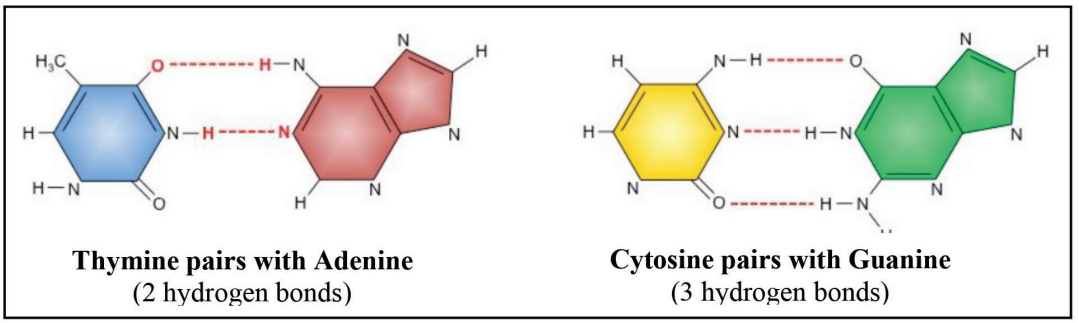

Figure 2: Complementary base pairing of nitrogenous bases

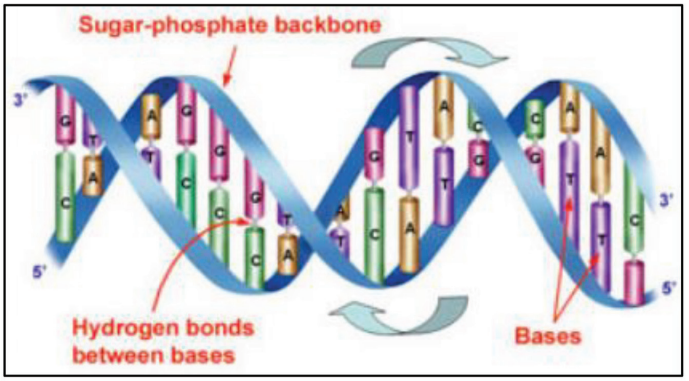

Figure 3: The double helix structure of DNA

with two backbone sides and stairs between these two sides. The backbone sides which wind around each other are formed from carbon sugar and phosphate, whereas the stairs of the ladder are formed from the complementary pairs of nitrogenous bases that are joined together by hydrogen bonds.

The two DNA strands have a beginning and an end, which are 5' (five prime) and 3' (three prime). One strand is known as the sense strand, whereas the other strand which run in the opposite direction and is antiparallel to the sense strand is known as the antisense strand. An individual strand of DNA is referred to as single strand DNA (ssDNA), but when the sense strand and antisense strand are combined together in Watson-Crick complementary manner, it is referred to as double stranded DNA (dsDNA) (Nafea & Ibrahem, 2018).

DNA Computing and DNA Based Cryptography

DNA computing is the combined discipline of bio-computing which concerns the use of DNA molecules in computational processes. It is an emerging branch of computing technology, which is able to solve problems that a traditional electronic computing cannot. In DNA computing, performing logical and arithmetic computations are done using biological molecules properties of DNA instead of using the traditional carbon/silicon chips (Jayakumar, 2020; Martyn, 2019).

The idea of using molecules and atoms for computations was first introduced by Richard Feynman way back in 1959. Many years later, in 1994, Prof. Leonard Adleman, a computer scientist from University of Southern California, who is the 'A' of RSA algorithms described the capability of biological molecular computation to solve complex computational problem (Loeffier, 2019; Naidu, 2019). Prof. Leonard Adleman is then known as the pioneer of DNA computing. He built the first DNA based computer to solve a mathematical and computer science problem, the directed Hamiltonian Path Problem also known as the "Travelling Salesman Problem".

DNA computing technology has many advantages when compared with traditional electronic computing. Among the most important advantages that DNA computing has to offer is its massive parallelism properties. This property of DNA is derived from the biding properties between nucleotides bases (A pairs up with T and C pairs up with G) that offer the possibility to create self-assembly structures. With a considerable amount of self-replicating DNA, computations will become much more efficient compared to traditional computers which would require a lot more hardware. Because of DNA's massive parallelism, complex mathematical equations or computational problems can potentially be solved more efficiently in much less time. 10^{18} processors working in parallel can easily be handled, which means huge problems can potentially be solved by parallel search (Mondal & Ray, 2019).

Another important advantage of DNA computing is its huge storage capacity. Each DNA molecule or group of molecules can store up to billion times more data than the best capacity of any traditional storage media whether it is magneticoptical, electronic and or physical. One gramme of DNA contains 10^{21} DNA bases, which can store nearly equal to 10^{8} terabytes of data (Mondal & Ray, 2019). A single gramme of DNA may have the potential of storing the same amount of information that could fit in one trillion Compact Discs (CDs). In other words, a few grams of DNA molecules have the capacity to retain all the data stored in the world. DNA stores memory at a density of about 1 bit/nm3, whereas conventional storage media requires up to 10^{12} nm^3/bit (Kolate & Joshi, 2021).

Besides the two advantages mentioned above, DNA computing is highly energy efficient. DNA computing requires almost no power efficiency during computation, therefore the consumption of power is low, which is around 2×10^{19} operations per joule (Kaur, 2012). This technology is clean as no toxic materials are used. It is also inexpensive because readily available materials are used and it is smaller in size than any existing computers.

DNA cryptography, a relatively new field of cryptology has emerged from the outstanding developments in the field of DNA computing. It is a technique of hiding data in the form of DNA and combining it with any conventional cryptographic algorithms to enhance the security of cryptographic algorithms. The properties of DNA are an important element, which allow it to be used to meet all kinds of cryptographic purposes such as encryption/decryption, authentication, signature or verification and others. In DNA cryptography, DNA chemistry is used to replace the mathematical aspects of cryptography, therefore it is immune to attacks from super computers. DNA cryptography was first established by Gehani, LaBean and Reif in 2004 when they published a paper entitled DNA-based Cryptography (Raj *et al.,* 2016; Zhang *et al.,* 2017).

Basic DNA Concept and Techniques Implemented in DNA Cryptography

Eight DNA concepts and techniques will be discussed in this section. However, there are many more concepts and techniques which will not be covered in this paper. The eight DNA concepts and techniques selected for discussion in this research paper were chosen because they are the most common and have been extensively used in most DNA cryptography. They also feature similar structures and components of normal block ciphers used in conventional cryptographic algorithms and are more practical to implement when designing new DNA cryptographic methods.

Watson-Crick Complementary Rules

A DNA sequence consists of four nitrogenous bases: Adenine(A), Guanine(G), Cytosine(C) and Thymine(T). In total, there would be 4! = 24 possible types of combinations of these DNA bases (Zhang *et a*l., 2014; Nafea & Ibrahem, 2018). These combinations are as follows:

CTAG CTGA CATG CAGT CGTA CGAT
TCAG TCGA TACG TAGC TGAC TGCA
ATCG ATGC ACTG ACGT AGCT AGTC
GTAC GTCA GATC GACT GCTA GCAT

According to Watson-Crick complementary rule, A and T are complementary and G and C are complementary. Therefore, to fulfil this complementary relationship between DNA nitrogenous bases, only eight types of DNA combinations are considered suitable (Gupta & Jain, 2014):

For pair A and T: CTAG CATG GTAC GATC

For pair G and C: TCGA TGCA ACGT AGCT

Either one from these eight DNA combinations can be used in the implementation of DNA cryptography.

DNA Encoding or Decoding Rules

DNA encoding or decoding is the process of mapping two binary bits to DNA representation and vice-versa. The eight encoding/decoding rules of the above DNA combinations are as shown in Table 1 below. In this paper, Rule 1 is considered; 00 – C, 01 – T, 10 – A, 11 – G.

Table 1: DNA encoding or decoding rules

	Rule 1	**Rule 2**	**Rule 3**	**Rule 4**	**Rule 5**	**Rule 6**	**Rule 7**	**Rule 8**
00	C	C	G	G	T	T	A	A
01	T	A	T	A	C	G	C	G
10	A	T	A	T	G	C	G	C
11	G	G	C	C	A	A	T	T

DNA Operation Rules: DNA XOR, DNA Addition and DNA Subtraction

The rules of DNA operation such as DNA XOR, DNA addition and DNA subtraction are altered using traditional binary XOR, binary addition and binary subtraction respectively. If the DNA addition rule is implemented in the encryption algorithm, the DNA subtraction rule needs to be implemented in the decryption algorithm and vice-versa. Table 2 shows the DNA XOR, DNA addition and DNA subtraction rules.

DNA Triplet Codon Code

A codon is made of three consecutive nucleotides sequence or called trinucleotide sequence. These codons correspond to a specific amino acid and the combination of different amino acids makes protein (Karimi & Haider; 2017). In DNA cryptography, triplet codon code is used as a substitute. The substitutions properties are met by using the DNA triplet codon code and their corresponding values, which are arranged randomly in a lookup table (Patnala & Kumar, 2019).

DNA Hybridization (DNA Annealing)

As described above, the DNA structure is presented in a double helix structure with two DNA strands, the sense strand and the antisense strand. These individual two strands are known as single stranded DNA (ssDNA). DNA hybridisation or also known as DNA annealing is the process of combining two antiparallel ssDNA to form one double stranded DNA (dsDNA). The combining process must satisfy Watson-Crick complementary rule where A always binds with T and G always binds with C. In DNA cryptography, hybridisation or annealing is performed by concatenating the antisense strand after the sense strand to form a larger DNA sequence.

DNA Transcription and DNA Replication

These two are the operations of converting DNA sequence to protein sequence in Central Dogma process. Transcription of dsDNA sequence to single stranded RNA (Ribonucleic Acid) sequence is by swapping the Thymine (T) nitrogenous base in DNA to Uracil (U) base. Translation is the process of transforming the RNA sequence to its protein form. In this process, RNA is read in three letters codon formed from four RNA bases, which gives a combination of 64 codons. These codons form 20 different amino acids. Combinations of amino acids in sequence form proteins (Karimi & Haider, 2017).

Theoretical Comparison of Recent Works Based on DNA Cryptography

In January 2016, Raj, Vijay and Mahalakshmi proposed a secure data transfer through DNA cryptography using symmetric algorithms. In the proposed algorithm, input plain text is converted to ASCII, then converted to decimal and to DNA sequence. A random key lookup table of length 256 is generated. The ciphertext is the index of the DNA sequence from the random key lookup table.

Table 2: DNA operation rules

DNA XOR Rule					**DNA Addition Rule**					**DNA Subtraction Rule**				
	C	**T**	**A**	**G**		**C**	**T**	**A**	**G**		**C**	**T**	**A**	**G**
C	C	T	A	G	**C**	C	T	A	G	**C**	C	G	A	T
T	T	C	G	A	**T**	T	A	G	C	**T**	T	C	G	A
A	A	G	C	T	**A**	A	G	C	T	**A**	A	T	C	G
G	G	A	T	C	**G**	G	C	T	A	**G**	G	A	T	C

In October 2016, Rathi, Bhaskare, Kale, Shah and Vaswani proposed a data security method using DNA cryptography. The proposed method utilised 16-byte block size and a 16-byte key size. The DNA technique was applied to the key generation. In the key scheduling algorithm, the key matrix is randomly generated and is arranged in a 4 by 4 2D array. The values of the key matrix range from 0 to 127. Mod 2 is applied to the generated key matrix. For the storage and transmission of the key, the key is converted into different combinations of the four bases that make up the DNA sequence.

The encryption algorithm for this proposed method makes use of the concept of poly substitution and the byte-rotation technique. First, the plain text is divided into blocks of 16 bytes each and the ASCII value of the plain text is arranged in a 4 by 4 2D matrix. If the plain text is smaller than the block size, '.' is padded into the matrix. The matrix is then transposed. The plain text matrix is added to the key matrix and rows rotation and then columns rotation is applied to the matrix to get the ciphertext.

In 2016, Kamaraj, Bhrintha and Bhavithara proposed a DNA based encryption and decryption using Field-Programmable Gate Array (FPGA). For this encryption algorithm, input message is read by FPGA in ASCII codes and is then converted to the triplet codon code using a codon lookup table. The triplet codon code is encrypted with a key using Vigenere cipher where DNA encoding or decoding rules are applied.

In June 2017, Karimi and Haider proposed a cryptographic algorithm using DNA nucleotides. This algorithm operates in a random number of rounds and utilizes key size which varies based on length of user's password. In the key schedule algorithm, password in binary form is first converted to its DNA nitrogenous bases. DNA Hybridiszation or DNA Annealing is then applied to the single stranded DNA sequence to form double stranded DNA sequence. Next, DNA Transcription is applied to convert the DNA sequence to RNA sequence.

The keys are created by separating the RNA sequence with the stop codon. In the encryption algorithm, binary messages are shifted to the left and XORed with the keys generated from key scheduling process to produce the ciphertext.

In 2017, Kolte, Kuhalli and Shinde created a DNA cryptography algorithm using Index-Based symmetric DNA encryption. This algorithm adopts the symmetric block cipher and index string techniques. A real DNA sequence obtained from the NCBI database, which uses the China rose nucleotide as a One Time Pad symmetric key. In the encryption algorithm, plain text is converted to DNA sequence using the DNA encoding or decoding rules, where one plain text character in ASCII gives four characters of DNA.

The four characters of the DNA sequence are searched in the One Time Pad which is the DNA sequence obtained from NCBI database. The indexes of the four characters of DNA sequence are memorised. Number of indexes is the frequency of the four characters of the DNA sequence found throughout the One Time Pad. Using a random sequence, the index for each four characters of DNA sequence is chosen to become the ciphertext.

In July 2018, using the Feistel Network and dynamic DNA encoding, Zhang, Zhou and Niu proposed an image encryption method. To determine the digest of the plain text image, this proposed method used the SHA-3 algorithm and to produce sequence that is to be used to construct the Hill encryption matrix, this method makes use of the hyper-chaotic system. The input image pixel will be substituted with the constructed Hill encryption matrix. The F function of the Feistel network uses DNA operations. A DNA sequence database obtained from the GenBank is used as the key of Feistel network. In this proposed method, diffusion property is achieved by the Feistel network, dynamic DNA encoding and chaotic index sequences. Confusion and further diffusion properties are met through the ciphertext feedback and three-round circulation.

In November 2018, Nafea and Ibrahem suggested a cryptographic algorithm based on DNA and RNA properties. In the key generation algorithm, a DNA-OTP sequence is randomly generated with sequence equal to the plain text length. DNA Hybridisation or DNA Annealing is then applied to the single stranded DNA-OTP sequence to form double stranded DNA sequence. The DNA sequence is then turned into an RNA sequence, a DNA Transcription process is then applied, to convert the RNA sequence to a 3-letter amino acid or the protein sequence, DNA Translation is then used. The key, which is the 3-letter amino acid is then converted into binary code. In this encryption algorithm, the key is XORed with plain text. The ciphertext is the XORed sequence in a DNA format.

In January 2019, using DNA codons, Patnala and Kumar proposed a level-based DNA security algorithm. In this algorithm, the substitution properties are met using the DNA triplet codon code with their corresponding values which are arranged randomly in a lookup table. The encryption process of this algorithm operates in three rounds only. The security strength of the algorithm increases as the number of rounds increases. In the first level, plain text is converted to ASCII values and then converted to its binary value and its DNA nitrogenous bases. In the second round, the DNA triplet codon code is formed. Then, using a DNA triplet codon lookup table, the DNA triplet codon code is replaced with its equivalent values. In the final round, the ciphertext is obtained by replacing values from the second round with its equivalent ASCII values and converting them to binary representations. Finally, the ciphertext is created by converting the binary sequence back to its DNA nitrogenous bases.

In May 2019, using XOR based data segments Kishore, Suneetha and Pradeep suggested an improved method of DNA data encryption. The proposed encryption algorithm used a random approach, a key is generated based on the length of the plain text*4. The original plain text and the key in binary form are divided into four equal parts. The plain text and randomly generated key are binary XORed, then the resulting XOR operation is then converted into a DNA sequence.

The DNA sequence is then mapped to a 256 DNA ASCII table to obtain the decimal values. The decimal values are again converted to DNA sequence. The ciphertext is the DNA sequence converted to ASCII characters.

In June 2019, Aishwarya and Sreerangaraju made a proposal to enhance security using DNA cryptography. In this proposal, authors combine the compressive sensing techniques with DNA encoding and decoding in Linear-Feedback Shift Register (LFSR)-based stream cipher. In this algorithm, the key is created using a lookup table containing the triplet codon code (DNA base triplets) which corresponds to alphabet, values and numbers. The DNA codon sequence is XORed with the input bit using DNA XOR to produce the ciphertext.

In July 2019, Das, Sarma and Deka proposed a DNA cryptography data security method. The proposed method is able to detect and prevent attacks aimed at modifying the data. In the key generation algorithm, an input string is converted to ASCII values and then converted to its binary value and its DNA nitrogenous bases. Then DNA hybridization or DNA annealing is performed using Watson-Crick complementary rules. The resulting DNA sequence is concatenated with the initial DNA sequence. Next, a DNA transcription is performed. The longest length of string between stop codon is obtained, which becomes the protein key.

In February 2020, using Message Queuing Telemetry Transport (MQTT) protocol, Hussein and Shujaa came up with a DNA computing-based stream cipher for the Internet of Things (IoT). Their proposed encryption algorithm makes use of a binary sequence of plain text message, which is encoded to a DNA sequence using DNA coding or encoding rules. The binary sequence of the cipher key is generated using 16-bit LFSR with a length equal to plain text message in binary, which is then encoded to a DNA sequence using the same DNA coding or encoding rules. The DNA sequence of plain text

and the DNA sequence of the key are then added together using DNA addition rules.

Another binary sequence is then generated using LFSR equal the length to the DNA sequence. Using the Watson-Crick complementary rule, if a bit '0' is found, complement A = T and G = C. The result of this complementary process is the ciphertext. The decryption process is the encryption process in reverse using the DNA subtraction rule instead of the DNA addition rule.

In August 2020, Al-Wattar planned a new lightweight cryptography method for IoT devices. This method is based on a public key cryptography principle and utilises data segments taken from GenBank. The proposed algorithm considers the public key of the receiver the location of the chosen DNA segment within a specific GenBank data segment. The key, which can be just a number or a code without any meaning is used to specify a location within the GenBank.

Meanwhile, the private key of receiver is the value of the chosen DNA segment within the GenBank data segment with a specific length. The receiver chooses the value of the DNA segment to calculate its private key.

In September 2020, Leelavathy and Sugumar proposed an enhanced user data security framework using DNA cryptography in cloud computing environment. The new security framework operates using a genetic algorithm with a smaller block size which increases the level of security provided by framework.

In December 2020, Zaid, Kubba and Hoonod recommended a DNA-based block cipher algorithm, DPRESENT (Developing a Lightweight Cryptographic Algorithm Based on DNA Computing). This algorithm is based on a famous lightweight cryptographic algorithm, PRESENT. DPRESENT utilises a 64-bit plain text, 80-bit or 128-bit key and operates in 20 rounds instead of 31 rounds as in PRESENT. The substitution and permutation properties of DPRESENT are met using PRESENT's S-box layer and PRESENT's P-layer respectively. DNA cryptography techniques were added in the round function after the S-box layer and P-layer. DPRESENT aims to produce a more complex ciphertext but at the same time to preserve minimal computation time.

Table 3 below shows the comparative review of the recent work based on DNA cryptography considered in this study using the following parameters.

(1) Conventional cryptographic techniques used.

(2) DNA concepts and techniques used.

(3) Applications.

(4) Other descriptions of the work (its limitations or analysis of effectiveness as security protocols).

Table 3: Comparative review of recent works based on DNA cryptography

	Reference	Cryptographic Technique Used	DNA Enc/ Dec Rules	DNA Concept and Technique Used	Application	Other Description
1.	Raj *et al.,* January 2016	Symmetric stream cipher	ACGT	4 DNA bases lookup table	Wireless network	Limitation: DNA chromosome required
2.	Rathi *et al.,* October 2016	Symmetric block cipher, byte rotation technique from BREA algorithm	ACGT			

	Reference	Cryptographic Technique Used	DNA Enc/ Dec Rules	DNA Concept and Technique Used	Application	Other Description
3.	Kamaraj *et al.,* 2016	Vigenere cipher	ATCG	DNA triplet codon lookup table		
4.	Karimi & Haider, June 2017	Symmetric key generation, XOR operation, left circular shift	ACGT	DNA hybridization, DNA transcription		Limitation: Not suitable for small network
5.	Kolte *et al.,* 2017	Symmetric block cipher, OTP key generation	ACGT	NCBI	Text encryption	Limitations: Distribution of key is a hectic problem
6.	Zhang *et al.,* July 2018	SHA3, Fiestel network	All 8 DNA rules	DNA operation rules, GenBank	Image encryption	Security analysis: Key Space and Its Sensitivity Analysis - has a strong key sensitivity and it can resist violent attacks Gray Histogram Analysis - grayscale distribution of the encrypted image very uniform Correlation Coefficient Analysis - correlation between the pixels is greatly reduced Differential Attack Analysis - good ability to resist differential attack Information Entropy Analysis - information leakage of the ciphertext is very small
7.	Nafea & Ibrahem, November 2018	Symmetric stream cipher, XOR operation, OTP key generation	ACGT	DNA-OTP, DNA hybridization, DNA transcription, DNA translation		Security analysis: NIST Statistical Analysis - Pass all 13 tests Performance Analysis - Lesser encryption and decryption time compared to Triplet DES algorithm

	Reference	Cryptographic Technique Used	DNA Enc/ Dec Rules	DNA Concept and Technique Used	Application	Other Description
8.	Patnala & Kumar, January 2019	-	AGCT	DNA triplet codon lookup table	Text encryption	Limitation: Able to process 64 characters only
9.	Kishore *et al.,* May 2019	Symmetric, XOR operation	ACTG	DNA ASCII Table		Security analysis: Performance measurement - very less execution time
10.	Aishwary *et al.,* June 2019	LFSR based stream cipher	-	DNA triplet codon code, DNA operation rules	Lightweight	
11.	Das *et al.,* July 2019	XOR operation, left circular shift	ACGT	DNA hybridization, DNA transcription		
12.	Hussein & Shujaa, February 2020	One Time Pad, LFSR for PRNG key generator	ATCG	DNA operation rules, Watson-Crick complementary rules	IoT	
13.	Al-Wattar, August 2020	Public key	ACGT	Data segment from GenBank	IoT	
14.	Leelavathy *et al.,* September 2020	AES-256, ECC to encrypt the shared key			Cloud Computing	
15.	Zaid, Kubba & Hoonod, December 2020	Symmetric block cipher – SPN structure, substitution, permutation	ATGC	-	Lightweight	Security analysis: NIST Statistical Analysis - DPRESENT has a significant level of randomness as PRESENT and P-values produced by DPRESENT are higher than PRESENT

It can be concluded that all 15 DNA cryptographic methods listed in Table 3 incorporate conventional and DNA cryptographic techniques and concepts and all 15 cryptographic methods discussed employ the DNA Encoding or Decoding Rules.

Recommendations regarding the suitable application of the 15 DNA cryptographic methods and their limitations as data security tools as analysed and provided in the table for future reference. It is hoped that this will help researchers find appropriate solutions for secure and reliable cryptographic algorithms.

Conclusion

In this paper, we have discussed various DNA techniques that have been implemented in recent DNA cryptographic algorithms. We have also provided a brief description of some of the DNA cryptographic algorithms. A comparative analysis of conventional cryptographic techniques and DNA techniques used by these cryptography tools and its application, limitations and security analysis has also been looked at. The findings of this theoretical comparative analysis will benefit academic researchers and cryptography developers by enabling them to find the best, most suitable and most sustainable solution for secure and reliable cryptographic algorithms to be adopted into the information security field.

Acknowledgements

The authors would like to thank the Universiti Sains Islam Malaysia (USIM) for funding the fundamental research by way of Grant FRGS/1/2020/ICT04/USIM/03/1. This research is part of a dissertation which was submitted as partial fulfilment of the requirements for a Doctor of Philosophy degree in Science and Technology at Universiti Sains Islam Malaysia (USIM).

References

Aishwarya, R. U., & Sreerangaraju, M. N. (2019). Enhanced Security using DNA Cryptography. *International Research Journal of Engineering and Technology (IRJET), 6*(6), 3193-3196.

Al-Wattar, A. H. (2020). A new lightweight proposed Cryptography Method for IoT. *International Journal of Advanced Trends in Computer Science and Engineering, 9*(4), 4954-4958.

BioNinja. *Nitrogenous Bases*. Retrieved from Nitrogenous Bases | BioNinja

Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., Seurin, Y., & Vikkelsoe, C. (2007). PRESENT: An Ultra-Lightweight Block Cipher. *Lecture Notes in Computer Science (LNCS), 472,* 450-466.

Das, A., Sarma, A. K., & Deka, S. (2019). Data security with DNA Cryptography. *Proceedings of the World Congress on Engineering 2019.*

Gupta, R., & Jain, A. (2014). A new image encryption algorithm based on DNA Approach. *International Journal of Computer Applications, 85*(18), 27-31.

Hammad, B. T., Sagheer, A. M., Ahmed, I. T., & Jamil, N. (2020). A comparative review on symmetric and asymmetric DNA-based Cryptography. *Bulletin of Electrical Engineering and Informatics, 9*(6), 2484-2491.

Hussein, N. A., & Shujaa, M. I. (2020). DNA computing based stream cipher for internet of things using MQTT Protocol. *International Journal of Electrical and Computer Engineering (IJECE), 10*(1), 1035 – 1042.

Jayakumar, A. (2020, August 5). *Introduction to DNA Computing and its Applications*. https://www.section.io/engineering-education/dna-computing/

Kamaraj, A., Bhrintha, A. P., & Bhavithara, M. (2016). DNA Based Encryption and Decryption using FPGA. *International Journal of Current Research and Modern Education (IJCRME),* 89-94.

Karimi, M., & Haider, W. (2017). Cryptography using DNA Nucleotides. *International Journal of Computer Applications, 168*(7), 16-18.

Kaur, M. (2012). DNA Computing: Its advantages and future. *Journal of Teaching and Education, 1*(7), 51-59.

Kennepohl, D., Farmer, S., Schaller, P., & Jakubowski, C. (2020, August 11). *Base Pairing in DNA- The Watson-Crick Model.* https://chem.libretexts.org/@go/page/36494

Kishore, D., Suneetha, D., & Pradeep, G. G. S. (2019). An improved method of DNA Data Encryption using XOR Based Data Segments. *International Journal of Recent Technology and Engineering (IJRTE), 8*(1), 1834-1838.

Kolate, V., & Joshi, R. B. (2021). An Information Security Using DNA Cryptography along with AES Algorithm. *Turkish Journal of Computer and Mathematics Education, 12*(1), 183-192.

Kolte, N. S., Kulhalli, K. V., & Shinde, S. C. (2017). DNA Cryptography using Index-Based Symmetric DNA Encryption Algorithm. *International Journal of Engineering Research and Technology, 10*(1), 810-813.

Leelavathy, L., & Sugumar, R. (2020). EUDSFDNA: Enhanced User Data Security Framework using DNA Cryptography in Cloud Computing Environment. *Journal of Shanghai Jiaotong University, 19*(9), 568-574.

Loeffier, J. (2019, March 11). *What is DNA Computing, How Does It Work and Why It's Such a Big Deal.* https://interestingengineering.com/what-is-dna-computing-how-does-it-work-and-why-its-such-a-big-deal

Martyn, A. (2019, February 11). DNA Computing. *Encyclopaedia Britannica*. https://www.britannica.com/technology/DNA-computing.

Miller School of Medicine. *Genetics Basics.* http://hihg.med.miami.edu/code/http/modules/education/Design/page.asp?CourseNum=1&LessonNum=1&index=1&hcb=1

Mondal, M., & Ray, K. S. (2019). Review on DNA Cryptography. *ArXiv(1904.05528v1).* https://arxiv.org/abs/1904.05528

Nafea, S. S., & Ibrahem, M. K. (2018). Cryptographic Algorithm based on DNA and RNA Properties. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 7*(11), 804-811.

Naidu, V. (2019, May 8). *DNA Computing for Neuromorphic Intelligence.* https://www.linkedin.com/pulse/dna-computing-neuromorphic-intelligence-victor-naidu

Parker, N., Schneegurt, M., Thi Tu, A. H., Lister, P., & Forster, B. M. (2016). Chapter 10.2: Structure and Function of DNA. In *Microbiology*. https://openstax.org/books/microbiology/pages/10-2-structure-and-function-of-dna

Patnala, B. D., & Kumar, R. K. (2019). A Novel Level-Based DNA Security Algorithm Using DNA Codons. *SpringerBriefs in Forensic and Medical Bioinformatics.* https://www.researchgate.net/publication/327545604_A_Novel_Level-Based_DNA_Security_Algorithm_Using_DNA_Codons_Applications_in_Bioinformatics

Raj, B. B., Vijay, J. F., & Mahalakshmi, T. (2016). Secure Data Transfer through DNA Cryptography using Symmetric Algorithm. *International Journal of Computer Applications, 133*(2), 19-23.

Rathi, M., Bhaskare, S., Kale, T., Shah, N., & Vaswani, N. (2016). Data Security Using DNA Cryptography. *A Monthly Journal of Computer Science and Information Technology, 5*(10), 123-129.

Singh, G., & Yadav, R. K. (2019). DNA Based Cryptography Techniques with applications and limitations. *International Journal of Engineering and Advanced Technology (IJEAT), 8*(6), 3997-4004.

Zaid, M., Kubba, J., & Hoonod, H. K. (2020). Developing a Lightweight Cryptographic Algorithm Based on DNA Computing. *AIP Conference Proceedings 2290, 040013.*

Zhang, J., Fang, D. X., & Ren, H. (2014). Image Encryption Algorithm Based on DNA Encoding and Chaotic Maps. *Mathematical Problems in Engineering.* http://dx.doi.org/10.1155/2014/917147

Zhang, X., Zhou, Z., & Niu, Y. (2018). An Image Encryption Method based on the Feistel Network and Dynamic DNA Encoding. *IEEE Photonics Journal.* https://www.researchgate.net/publication/326598560_An_Image_Encryption_Method_Based_on_the_Feistel_Network_and_Dynamic_DNA_Encoding

Zhang, Y., Liu, X., Ma, Y., & Cheng, L.C. (2017). An Optimized DNA Based Encryption Scheme with Enforced Secure Key Distribution. *Cluster Computing, 20*(4), 3119-3130.