Contents lists available at http://qu.edu.iq

Al-Qadisiyah Journal for Engineering Sciences

Journal homepage: http://qu.edu.iq/journaleng/index.php/JQES

A new DNA strand-based encryption algorithm using symmetric key generation table

***Qabeela Q. Thabit*[a]*, *Alaa A. Al-saffar*[b] *and Issa Ahmed Abed*[b]**

[a] *Directorate of Education, Ministry of Education, Basrah,Iraq.*
[b] *Engineering Technical College, Southern Technical University, Basrah, Iraq*

ARTICLEINFO

Article history:
Received 23 February 2022
Received in revised form 5 April 2022
Accepted May 22, 2022

Keywords:
DNA-based Cryptography
Encryption
Decryption
Binary Code
DNA Bases

ABSTRACT

Due to the characteristics of Deoxyribonucleic acid DNA chain which contains a very wide range of parallelism mechanism, and the computing processing speed can arrive at 1 billion times per one second. It is worth only a billionth of a traditional computer. It became the focus of the attention of researchers in the field of encryption. The aim of this study is to find an efficient and safe algorithm for data encryption as well as decryption. A symmetric novel method is proposed in this paper depends on DNA encryption by applying a mixture of DNA oligonucleotide and new development of algorithm technology steps. It includes encoding each character to a predefined decimal number, converting it to its equivalent binary number and then converting it into DNA coding. Finally, converts each code of DNA to a number that represents a row and column numbers. Simulation all all text (words) is executed in parallel by using Visual Basic programming, obtained an excellent encoding result in terms of time because all the characters, so the algorithm is able to process the largest number of data, all of them encode at the same time. An efficient, fast and highly encoding scheme has been obtained due to the complete executing parallelism of the DNA-based algorithm.

1. Introduction

Initially, because of the great parallelization and excellent energy efficiency of Deoxyribonucleic DNA coding and the great density of information inherent in DNA molecules for data storage and coding, it is distinguished from other coding technologies. The DNA cryptography technique is a new encouraging path in cryptography science that has emerged as a result of advances in the field of DNA computing, the uses of DNA and RNA have multiple scientific applications within the field of DNA nanotechnology, as they have been used in optical computers [1,3] and in drugs that treat cancer [4], as well as their use in cryptography information because the world is witnessing an explosion of information in which The analysis of information has grown a very important mechanism source, and therefore the task of information field security is becoming increasingly important. cryptography is the most important part of telecom and computer security infrastructure [5]. Research continued in the science scope that related to cryptography field and steganography field using DNA in the past few years, in 2011 S. Jeevidha et.al. analyzed a proposal DNA computing approach with DNA depends cryptographic different approaches which produces the easy concept and constraints of all works that focus on this research [6] Z. Yunpeng et al., on the other hand, used simulation and theoretical research to demonstrate the algorithm's efficiency, biosecurity and math security are two examples. The used algorithm has a tremendous key space, plaintext has a high sensitivity, and encryption has a huge effect. In addition, the algorithm has been verified to work at the computing processing stage in the encryption security evaluation scheme [7]. After this offered innovative algorithm to communicate data securely by A. Atito et.al. in 2012. The Playfair-insertion the procedure is a construction

* *Corresponding author. Tel.: +964(0)787796310*
E-mail address: qabelh2010@gmail.com (Qabeela Q. Thabit)

https://doi.org/10.30772/qjes.v15i1.803

encryption and data concealment applying some features of Deoxyribonucleic Acid (DNA) structure sequences [8]. DNA cryptography applies Hybridization of DNA oligonucleotides, and the generic binary one-time pad methodology was mixed in this paper. [9]. Digital DNA encoding, rules of complementary, and biotechnological designs in this scheme [10]. Using DNA sequences for the encoded text message is a means of transmitting information, a process to transfer encrypted data through a secure communication channel. The time complexity of transferring encrypted messages is reduced by the message transmission process. Biomolecular and one time- pad technologies is done for secure message encryption [11]. An algorithm computation security using DNA cryptography suggested. In wireless communication, DNA cryptography is combined with a safe support layer (SSL) to create a secure channel for a more secure information replacement [12]. Cascaded DNA cryptography and steganography which represent hiding of data. Initially it performs DNA cryptography and then its hidden in a random frame of video [13]. Kevin Santoso et al. described a section-based DNA steganalysis approach that stores binary information in non-coding regions of the Nucleotide sequence. The goal of sector-based compression is to protect the organism's life data while maintaining a high level of protection, data performance, and error checking. A sector is made up of referencing bases, segmentation message bases, and parity bases [14]. DNA Cryptography introduced after that in many method some these traditional such as genetic algorithm [15,16] and Vigenere Cipher[17], data Encryption Standard (DES), Advanced Encryption Standard (AES), and Blowfish are examples of symmetric cryptographic techniques [18], and asymmetric key cryptographic algorithms like Rivest-Shamir-Aldeman RSA[19], but other encryption based on biological technologies such as DNA chips and Polymerase Chain Reaction PCR amplification[20-22], DNA Encryption Dependent on DNA Arithmetic and Biomedical Processes is a strategy for encrypting DNA[23]. Bimolecular cryptography emerged as field for data encryption which exploiting specific biomolecular interactions as a unique approach for information security [24].

A novel algorithm to communicate data securely is suggested in this paper. The technique is a combination of encryption using properties of DNA sequences and generation matrix as key for decryption process. Consequentially, the presented method includes mainly of three levels. The first level, plaint text convert to binary sequences. While the second level the safe data is encrypted using a DNA, and the third level, the encrypted data is hidden by convert it into matrix of number. The submitted algorithm can successfully work on any text writing that represents in decimal and then binary data since it is transformed into a string of DNA nucleotides adopting the code of DNA.

2. Related work

A summarized analysis of some associated works is discussed in this section as following:

Sirisha KS and Sheena Mathew [25] are merging cryptographic protocols and steganography techniques gave a new hybrid method that performs the device has multiple layers of authentication, including DNA-based Advanced Encryption Standard (AES) encryption. The Steganalysis schemes employed do not expand the original DNA sequence, and the encrypted data can be withdrawn without a real DNA known sequences.

In this work, the proposed encryption algorithm depends on the mixture of the conception of DNA encryption and DNA dependent AES DNA steganography is combined with encryption. The DNA-RSA Hybrid Cryptographic system proposed by Narendren S et al [19] integrates different appropriate algorithms used in existing DNA cryptography algorithms with the RSA algorithm, leading in a DNA-RSA Hybrid Cryptographic algorithm. The hidden message is translated to DNA before being passed via a rounded function. Transcription, translation, mutation, reverse transcription, and circular right shift are among the activities performed by a round method. The round function's output (i.e., the DNA sequence) is then translated to binary number format, with the decimal value of the binary sequence serving as the hidden message for the RSA algorithm. The cipher text fragments are then estimated using RSA, and as all the blocks are merged into a unified cipher text. This mixed cipher text is first compiled to binary numbers, then to DNA. As a response, this DNA sequence will be the last cipher text used during the contact. Vidhya and Rathi Priya [26] suggested method composes from the steps as following, the first step being to apply the encryption key to the original text by encrypting it by that key, then take ASCII number for each letter after that convert all decimal number into corresponding binary numbers and finally convert each pair of binary number to DNA sequences.

The sequence of DNA can be received by the receiver. Create a binary representation of the DNA sequence. Erase the suffix secret message afterward. Binary numbers are compared to ASCII numbers with an eight-bit weight. The ASCII numbers are transferred to ASCII values, and when the shift key is held, the plaintext is viewed by the receiver. B. Devi Patnala and R. Kiran Kumar [27] offered a DNA-based defense algorithm based on DNA Codon groups. This scheme utilizes the exchange process, in which transformations are performed using a Lookup table is a collection DNA Codon groups and their corresponding alphabet values. This table has a random number generator and should be sent to the recipient via secure media.

The main idea behind DNA molecules is that they can collect information for a long period of time. D.Ratna Kishore et. al [28] Because the key is generated at random, figuring out the plaintext is an unfathomable task for the intruder is presented. At first, both the transmitter and the recipient agree that the spiral pattern is correct. The sender's randomly generated key is sent to the receiver over the secure media. There are three levels of security in the proposed technique. XOR's cross join with the plaintext and the key, i.e., XOR(M1-K1), XOR(M2-K2), XOR(M3-K3), and XOR(M4-K4), is conducted at the primary level number. At the next level, the DNA sequence, which is four characters long, is mapped to a DNA ASCII value. Another DNA ASCII Table is being constructed with the goal of distinguishing the mapping in 256! distinct ways, increasing the complexity of the intruder's actions. The DNA string sequences are placed in a spiral form in the last level. The data is transmitted to the recipient in a row-by-row fashion. To provide a higher security framework, the proposed method increased the level of confusion and diffusion.

Anupam Das et al. [29] presented a detailed report, and the information provided here will greatly assist researchers in doing further research in this area. The modules for degenerative changes, cryptography, and decryption must commission need subsequent work on cryptographic techniques deployment. The current work will also aid in the development and integration of DNA-based cryptography and steganography methodologies. Prasanna Balaji Narasingapuram and M. Ponnavaikko [30] devised and implemented a novel security method to strengthen the user's level of security It's a user authentication strategy for any network or cloud application that requires it. In a protected data transfer application, the user authentication procedure is one of the most critical and vital activities. It certifies if the user is acceptable or malevolent, and whether the user has access to the information.

3. Proposed algorithm

The suggested system produces a secure key as matrix in new manner which increases difficulty to break the code of plaint text. Suggested a new encryption approach is implemented depended on three levels to get the cipher text. The entire operation of DNA encoding, and decryption illustrated in the following Fig. 1.

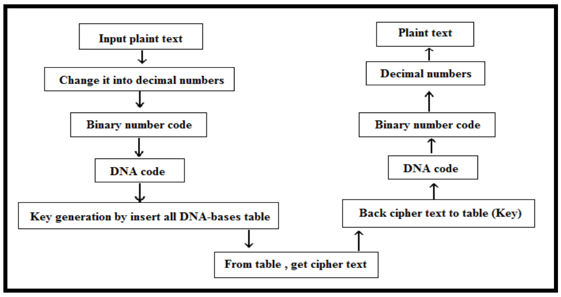

Input plaint text
Change it into decimal numbers
Binary number code
DNA code
Key generation by insert all DNA-bases table
From table , get cipher text
Back cipher text to table (Key)
DNA code
Binary number code
Decimal numbers
Plaint text

Figure 1. DNA encryption & decryption algorithm based on key generation

3.1. Algorithm for encryption

Level one: The encryption procedure is viewed in the following stages as:

1: Input data (plaint-text) separates into n-words (number of words), each one encrypted by converting it into a corresponding number (decimal Form) for each character by using Table 1 [31].

2: And all decimal values are subtracting from 25 at the same time.

3: Take the results from step2 and convert into character and a corresponding number also from Table 1.

4: Convert these number into form binary code (0's with 1's).

Table 1. Decimal number for each character

Letter	Code no.	Letter	Code no.
'A'	0	'N'	13
'B'	1	'O'	14
'C'	2	'P'	15
'D'	3	'Q'	16
'E'	4	'R'	17
'F'	5	'S'	18
'G'	6	'T'	19
'H'	7	'U'	20
'I'	8	'V'	21
'J'	9	'W'	22
'K'	10	'X'	23
'L'	11	'Y'	24
'M'	12	'Z'	25

Level two:

1: Add padded zero in front all binary numbers, and each block 6bit in binary, considered as blocks.

2: After that, through using (2) bit binary coding law, every 2 bit is convertible to nucleotide bases (DNA bases). [28] as shown in Table2, we get n-strings of DNA bases sequences.

Table 2. DNA code

Binary number	DNA code
00	A or (Adenine)
01	C or (Cytosine)
10	G or (Guanine)
11	T or (Thymine)

Level three (Key Generation):

1: Delete the padded zero in front all binary numbers.

2: Convert all binary numbers into decimal numbers.

3: Each number results from step 4 subtract from 25 and convert the result number into character by using Table 1. The design of the key table is done based on the process of entering the nitrogenous bases associated with a specific character. The table consists of three rows for each code belonging to a character where the first line represents the first base, so if the first base is Adenine A that is placed in the first column and if the first base is cytosine C it is placed in the second column, but if the base Guanine G placed in the third column and placed in the fourth column if they are Thymine T. And so on for the rest character codes as explain in Table 3. Therefore, the last form of cipher text as matrix all elements are two digits first is number that represent of row and the second is represented number of columns related to nitrogen base in each character code.

3.2. Algorithm for decryption

Analysis all number to corresponding nitrogen bases for each character code.

Convert the character code to binary code according Table2.

Delete the padded zero in front all binary numbers.

Convert all binary numbers into decimal numbers

Each number results from step 4 subtract from 25 and convert the result number into character by using Table 1.

Encryption procedure is a numerical description representation as the following example: Input data using is "SYMMETRIC ALGORITHM", the operation steps is explained as following Table 3:

Table 3. Two-level encryption

Level one						Level two		
S	18	25-18	7	H	00111	00111Ø	00-11-10	ATG
Y	24	25-24	1	B	00001	00001Ø	00-00-10	AAG
M	12	25-12	13	N	01101	01101Ø	01-10-10	CGG
M	12	25-12	13	N	01101	01101Ø	01-10-10	CGG
E	4	25-4	21	V	10101	10101Ø	10-10-10	GGG
T	19	25-19	6	G	00110	00110Ø	00-11-00	ATA
R	17	25-17	8	I	01000	01000Ø	01-00-00	CAA
I	8	25-8	17	R	10001	10001Ø	10-00-10	GAG
C	2	25-2	23	X	10111	10111Ø	10-11-10	GTG
A	0	25-0	25	Z	11001	11001Ø	11-00-10	TAG
L	11	25-11	14	O	01110	01110Ø	01-11-00	CTA
G	6	25-6	19	T	10011	10011Ø	10-01-10	GCG
O	14	25-14	11	L	01011	01011Ø	01-01-10	CCG
R	17	25-17	8	I	01000	01000Ø	01-00-00	CAA
I	8	25-8	17	R	10001	10001Ø	10-00-10	GAG
T	19	25-19	6	G	00110	00110Ø	00-11-00	ATA
H	7	25-7	18	S	10010	10010Ø	10-01-00	GCA
M	12	25-12	13	N	01101	01101Ø	01-10-10	CGG

Level three:

After reaching a sequence of three nitrogen bases representing each letter in the second level of coding, we distribute those bases on a table in a way that each sequence is built of three rows in each column from four columns, three bars representing the number of nitrogen bases for a minimum obtained from the last stage, and four columns representing all the possibilities of the bases Probable nitrogenous be any resulting sequence (A, C, G, T). The encrypted words are taken at the same time and the rules are entered into a table where we notice for each rule three lines for each word. The A was placed in the first row of the A column of the first word while T was placed in the second row of the T column of the first word and the base G was placed in the third row of the first word's G column, and so on for the rest. We put each nitrogen base in its place based on Table 4.

Table 4. Level three (key generation)

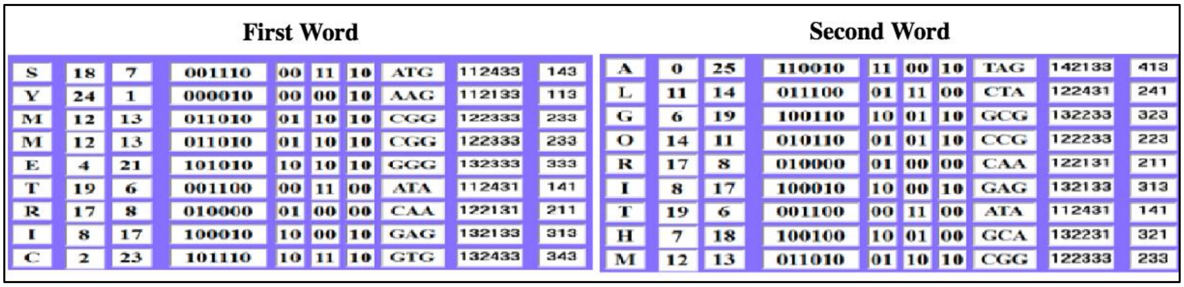
Character No.	C.A word1	C.A word2	C.C word1	C.C word2	C.G word1	C.G word2	C.T word1	C.T word2
1	A	A			G	G	T	T
2	A A	A		C	G			T
3			C	C	G G	G G		
4			C	C C	G G	G		
5		A A		C	G G G			
6	A A	A				G G		T
7	A A	A A	C					T
8	A	A		C	G G	G		
9				C	G G	G G		T

Table 5. Three level encryptions

First word			Cipher text		Second word		Cipher text
11	24	33	143	14	21	33	413
11	21	33	113	12	24	31	241
12	23	33	233	13	22	33	323
12	23	33	233	12	22	33	223
13	23	33	333	12	21	31	211
11	24	31	141	13	21	33	313
12	21	31	211	11	24	31	141
13	21	33	313	13	22	31	321
13	24	33	343	12	23	33	233

Table 6. Decryption operation.

		Step1				Step2	Step3	Step4	Step5	
Ch no.	Cipher text	R1	R2	R3	DNA code	Binary code	Delete padded zero	Deci. no.	Original character number	Original character
1	143	11	24	33	ATG	001110	00111	7	18	S
2	113	11	21	33	AAG	000010	00001	1	24	Y
3	233	12	23	33	CGG	011010	01101	13	12	M
4	233	12	23	33	CGG	011010	01101	13	12	M
5	333	13	23	33	GGG	101010	10101	21	4	E
6	141	11	24	31	ATA	001100	00110	6	19	T
7	211	12	21	31	CAA	010000	01000	8	17	R
8	313	13	21	33	GAG	100010	10001	17	8	I
9	343	13	24	33	GTG	101110	10111	23	2	C
1	413	14	21	33	TAG	110010	11001	25	0	A
2	241	12	24	31	CTA	011100	01110	14	11	L
3	323	13	22	33	GCG	100110	10011	19	6	G
4	223	12	22	33	CCG	010110	01011	11	14	O
5	211	12	21	31	CAA	010000	01000	8	17	R
6	313	13	21	33	GAG	100010	10001	17	8	I
7	141	11	24	31	ATA	001100	00110	6	19	T
8	321	13	22	31	GCA	100100	10010	18	7	H
9	233	12	23	33	CGG	011010	01101	13	12	M



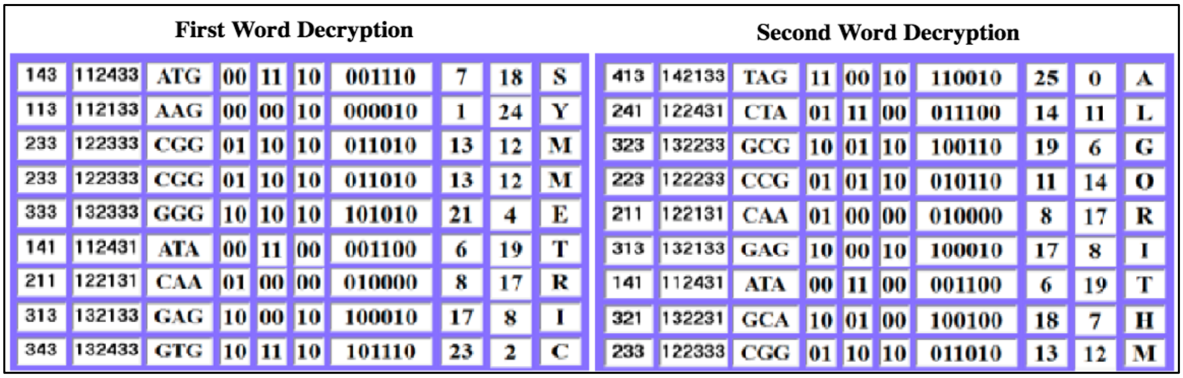
First Word

S	18	7	001110	00	11	10	ATG	112433	143
Y	24	1	000010	00	00	10	AAG	112133	113
M	12	13	011010	01	10	10	CGG	122333	233
M	12	13	011010	01	10	10	CGG	122333	233
E	4	21	101010	10	10	10	GGG	132333	333
T	19	6	001100	00	11	00	ATA	112431	141
R	17	8	010000	01	00	00	CAA	122131	211
I	8	17	100010	10	00	10	GAG	132133	313
C	2	23	101110	10	11	10	GTG	132433	343

Second Word

A	0	25	110010	11	00	10	TAG	142133	413
L	11	14	011100	01	11	00	CTA	122431	241
G	6	19	100110	10	01	10	GCG	132233	323
O	14	11	010110	01	01	10	CCG	122233	223
R	17	8	010000	01	00	00	CAA	122131	211
I	8	17	100010	10	00	10	GAG	132133	313
T	19	6	001100	00	11	00	ATA	112431	141
H	7	18	100100	10	01	00	GCA	132231	321
M	12	13	011010	01	10	10	CGG	122333	233

Figure 2. Simulation part of encryption process



First Word Decryption

143	112433	ATG	00	11	10	001110	7	18	S
113	112133	AAG	00	00	10	000010	1	24	Y
233	122333	CGG	01	10	10	011010	13	12	M
233	122333	CGG	01	10	10	011010	13	12	M
333	132333	GGG	10	10	10	101010	21	4	E
141	112431	ATA	00	11	00	001100	6	19	T
211	122131	CAA	01	00	00	010000	8	17	R
313	132133	GAG	10	00	10	100010	17	8	I
343	132433	GTG	10	11	10	101110	23	2	C

Second Word Decryption

413	142133	TAG	11	00	10	110010	25	0	A
241	122431	CTA	01	11	00	011100	14	11	L
323	132233	GCG	10	01	10	100110	19	6	G
223	122233	CCG	01	01	10	010110	11	14	O
211	122131	CAA	01	00	00	010000	8	17	R
313	132133	GAG	10	00	10	100010	17	8	I
141	112431	ATA	00	11	00	001100	6	19	T
321	132231	GCA	10	01	00	100100	18	7	H
233	122333	CGG	01	10	10	011010	13	12	M

Figure 3. Simulation part of decryption process

From Table 4, we take a two number, the first represent the number of rows, and the second number of columns, after that delete all numbers represent row number and get the following n-array, in each one the number of columns represents the number of characters in each word as shown in Table 5 which represent cipher text. Decryption: Analysis of all numbers to corresponding nitrogen bases for each character code. Then convert the character code to binary code according to Table2. After that delete the padded zero in front of all binary numbers, next step is converting all binary numbers into decimal numbers. Finally, each number results from step 4 subtract from 25, and convert the resulting number into character by using Table 1. Back each number in cipher text to row number, then retrieve to nitrogen base equivalent to pair number, after that convert it into binary code as Table 5.

4. Discussion and simulation results

In most of the research like this work, it goes through almost the same procedures, which is to convert the data into an ASCII code, then into a binary digital system, and finally get the code represented by a series of nitrogenous bases, or convert each number to a specific amino acid, and thus the encoding and decoding path is known in advance. As for the proposed work, there was a change in the encryption and decryption procedures, which is a departure from the norm by implementing the mentioned steps. This added advantages to the work where the path is safe for decryption. Also, relying on a table that can be read and written in an accurate manner recognized by the sender and the recipient, and provided a level of sobriety for the algorithm, in addition to that. It is possible to implement in a parallel way a full text and not just words, making a change in the efficiency of obtaining the largest amount of secure information. The implementation of the algorithm for encoding and decoding is by an easy and parallel mechanism, which supports an efficient system capable of executing an unlimited number of words. In this paper, we take an example consisting of two words as shown in Fig. 2, simulation part of encryption process for plaint text “SYMMETRIC ALGORITHM”. While Fig. 3, is shown simulation part of decryption process.

5. Conclusion

In recent years, many papers have focused on research into DNA encoding. DNA encoding has a huge data capacity in addition to the possibility of parallel implementation of represent and giving a high confidentiality of data that made it the focus of attention of researchers. In this work, we presented a model for an algorithm consisting of two dimensions: the first dimension is data encryption, which includes three levels, respectively, while the other dimension is decryption, which consists of five steps. A table has been added at the end of the encryption process and the beginning of the decryption process to serve as a strong security barrier to prevent tampering or obtaining the text by the eavesdropper of the process. It is noteworthy, we added DNA with this research in a new way that opens horizons to apply that within other asymmetric algorithms or even the ability to implement quantum cryptography by employing DNA strands that can be Polarized light-bearing bodies, such as chromo-pores.

REFERENCES

[1] Thabit Q.Q., and Al-Saffar A.A. DNA-strand molecular beacon optical processor, Heliyon 5(9) (2019), e02389.

[2] Alaa A. Al-Saffar and Qabeela Q. Thabit, Simulation of nanoscale optical signed digit addition based on dna-strands, proc. of 2018 International Conference on Advanced Science and Engineering (ICOASE),Duhok, Iraq.

[3] Alaa A. Al-Saffar and Qabeela Q. Thabit, Optical computing for a three-step binary modified signed-digit addition using DNA, Fourth International Conference on Computational Science and Technology of 2017, Kuala Lumpur.

[4] S. Li et al., A DNA nanorobot functions as a cancer therapeutic in response to a molecular trigger in vivo, Nature Biotechnology, 36 (2018) 258-264.

[5] Heba G. Mohamed, Dalia H. ElKamchouchi, and Karim H. Moussa, A Novel Color Image Encryption Algorithm Based on Hyperchaotic Maps and Mitochondrial DNA Sequences, Entropy, 22(158) (2020)1-15.

[6] S.Jeevidha, M.S.Saleem Basha, andP.Dhavachelvan, Analysis on DNA based Cryptography to Secure Data Transmission, International Journal of Computer Applications (0975 – 8887), 29(8) (2011) 16-20.

[7] Zhang Yunpengm,Zhu Yu,Wang Zhong,Richard O.Sinnott ,Index-Based Symmetric DNA Encryption Algorithm, 2011 4th International Congress on Image and Signal Processing, 9(2011)2290-2294.

[8] A. Atito, A. Khalifa, and S. Z. Rida, DNA-Based Data Encryption and Hiding Using Playfair and Insertion Techniques, J. of Commun. & Comput. Eng. ,2(3) (2012) 44- 49.

[9] Shreyas Chavan, DNA Cryptography Based on DNA Hybridization and One Time pad scheme, International Journal of Engineering Research & Technology (IJERT), 2 (10) (2013) 2679- 2682.

[10] Guangzhao Cui, Dong Han, Yan Wang, Yanfeng Wang, and Zicheng Wang, An Improved Method of DNA Information Encryption, BIC-TA 2014, CCIS, 472(2014)73–77.

[11] Tausif Anwar, Sanchita Paul, and Shailendra Kumar Singh, Message Transmission Based on DNA Cryptography: Review, International Journal of Bio-Science and Bio-Technology, 6(5) (2014) 215-222.

[12] Monikaa, and Shuchita Upadhyayaa, Secure communication using DNA cryptography with secure socket layer (SSL) protocol in wireless sensor networks, 4thInternational Conference on Eco-friendly Computing and Communication Systems, Procedia Computer Science, 70 (2015) 808 -813.

[13] Shweta and S. Indora. Cascaded DNA cryptography and steganography, In Green Computing and Internet of Things (ICGCIoT), 2015 International Conference, (2015)104–107.

[14] Kevin Santoso, Suk-Hwan Lee, Won-Joo Hwang, and Ki-Ryong Kwon, Sector-based DNA information hiding method, Security and Communication Networks, 9(2016)4210-4226.

[15] Anushree Raj, and Rio G L D Souza, DNA Cryptography Algorithm Using Genetic operaters, International Journal of Latest Trends in Engineering and Technology Special Issue SACAIM, (2017) 034-039.

[16] Kalsi, S., Kaur, H. and Chang, V., DNA Cryptography and Deep Learning using Genetic Algorithm with NW algorithm for Key Generation, J Med Syst 42(17) (2018).

[17] Akhil Kaushik, and Vikas Thada, VG1 Cipher – A DNA Indexing, Cipher, International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9(3) (2020).

[18] 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.

[19] Narendren S, Yashas B Yathish, and Chandra Mohan B, A Cryptosystem using Two Layers of Security-DNA and RSA Cryptography, International Journal of Pure and Applied Mathematics, 119(7) (2018) 217-224.

[20] Anupriya Aggarwal and Praveen Kanth, DNA Encryption, International Journal of Computer Science and Engineering (IJCSE), 3(3) (2014) 51- 66.

[21] Yun-peng ZHANG, Zhen-zhen WANG, Zhi-wen WANG, Yasin Hasan KARANFIL and Wei-di DAI, A New DNA Cryptography Algorithm Based on the Biological Puzzle and DNA Chip Techniques, International Conference on Biomedical and Biological Engineering (BBE 2016).

[22] Nikita Parab and Ashwin Nirantar, Survey of different DNA Cryptography based algorithms, International Research Journal of Engineering and Technology (IRJET), 4(12) (2017) 1100- 1104.

[23] Dilovan Asaad Zebari, Habibollah Haron, Subhi R. M. Zeebaree, and Diyar Qader Zeebaree, Multi-Level of DNA Encryption Technique Based on DNA Arithmetic and Biological Operations, 2018 International Conference on Advanced Science and Engineering (ICOASE), Kurdistan Region, Iraq (2018) 312-317.

[24] Yinan Zhang et al., DNA origami cryptography for secure communication, Nature Communication, (2019)1-8.

[25] Sajisha K S and Sheena Mathew, An Encryption based on DNA cryptography and Steganography, International Conference on Electronics, Communication and Aerospace Technology ICECA, (2017) 162-167.

[26] E. Vidhya and R. Rathipriya, Two Level Text Data Encryption using DNA Cryptography, International Journal of Computational Intelligence and Informatics, 8(3) (2018) 106-118.

[27] Bharathi Devi Patnala and R. Kiran Kumar, A Novel Level-Based DNA Security Algorithm Using DNA Codons, SpringerBriefs in Forensic and Medical Bioinformatics, In book: Computational Intelligence and Big Data Analytics, (2019) 1-13.

[28] D.Ratna Kishore, D.Suneetha, and G.G.S.Pradeep, An Improved Method of Dna Data Encryption using Xor Based Data Segments, International Journal of Recent Technology and Engineering (IJRTE), 8(1)(2019) 1834-1838.

[29] Anupam Das, Shikhar Kumar Sarma, Shrutimala Deka, Data Security with DNA Cryptography, Proceedings of the World Congress on Engineering, (2019)246-251.

[30] Prasanna Balaji Narasingapuram, and M. Ponnavaikko, DNA Cryptography Based User Level Security for Cloud Computing and Applications, International Journal of Recent Technology and Engineering (IJRTE), 8(5) (2020) 3738-3745.

[31] Alharith A. Abdullah, Rifaat Khalaf, and Mustafa Riza, A Realizable Quantum Three-Pass Protocol Authentication Based on Hill-Cipher Algorithm, Hindawi Publishing Corporation (Mathematical Problems in Engineering), 2015 (2015) 1-6.