Available online at www.garmian.edu.krd

Passer Journal of Basic and Applied Sciences

Passer 8 (Issue 2) (2026) 962-968

Original Article

A Secure and Efficient PDNA Cryptosystem: A Novel DNA and Polynomial Based Encryption Approach

Hassan Rashed Yassein[1], Nadia Mohammed Ghanim Al-Saidi[*2], Suzan Jabbar Obaiys[3], Asia Aqeel Abidalzahra[1]

[11]*Department of Mathematics, College of Education, University of Al-Qadisiyah, Al-Qadisiyah, 58002, Iraq.*
[2]*Department of Applied Sciences, University of Technology, Baghdad, 10066, Iraq.*
[3]*Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur, 50603, Malaysia.*

Received 17 April 2025; revised 05 November 2025;
accepted 20 November 2025; available online 19 August 2026

DOI: 10.24271/PSR.2025.517523.2090

ABSTRACT

The security of sensitive data has become a major concern today due to the transmission of data over public communication channels. Encryption has been relied upon to transmit protected data, which requires continuous improvement. To enhance the security of the transferred data, this paper presents the PDNA cryptosystem, a novel encryption method that integrates Deoxyribonucleic acid (DNA) encryption with truncated polynomial-based encryption. DNA cryptography is a new advancement in the field of cryptography due to its important features, including the ability to store large amounts of information and the random nature of the sequences of nitrogenous bases that make up DNA. In this paper, a new DNA cipher is presented, combining the idea of using encoding tables to convert plaintext into codons and truncated polynomials. This integration provides a high level of security and a significant increase in the randomness of the ciphertext, particularly when selecting secret key methods and their mathematical construction. According to the security analysis, the large key space generated by the DNA sequence and polynomial functions makes the proposed cryptosystem highly resistant to brute-force attacks. Moreover, it significantly improves data confidentiality and advances this growing field of encryption techniques.

Keywords: DNA cryptography, PDNA cryptosystem, Truncated polynomial encryption, Biomolecular security, Genetic-based encryption.

1 Introduction

Deoxyribonucleic acid (DNA) encryption is the new trend in cryptography. Combining DNA computing theories with cryptography concepts presents a promising direction in cryptography research, thanks to the large storage capacity. Due to its unique properties, such as high storage capacity, randomness, and parallelism, DNA is considered a promising substitute for traditional encryption techniques [1]. DNA is used in cryptography and information security due to its properties that enable it to carry and conceal a significant amount of information. In 1994, the scientist Edelman [2] conducted the first successful experiment with DNA computing to solve the problem of finding the best path. Since Adleman's pioneering work to solve this combinatorial problem, several encryption techniques based on DNA have emerged. In 1995, Boneh et al. [3] used DNA to break the Data Encryption Standard (DES). Following that, numerous attempts were made to develop encryption systems based on DNA encryption, which leveraged the randomness inherent in the bases of nucleic acid sequences and viewed it as the key to a one-time encryption system [4]. In 2010, Sabry et al. [5] proposed a significant modification to the classic Playfair cipher by incorporating DNA-based and amino acid-based structures into the core of the ciphering process. NTRU cryptosystem is one of the public key systems that is based on a truncated polynomial ring of degree $(N-1)$ with integer coefficients belonging to $Z[x]/(x^N-1)$.

This makes it extremely resistant to factorization and lattice attacks. It is based on the security of the Shortest Vector Problem (SVP) in lattices, which is believed to be computationally intractable even for quantum computers. NTRU is widely used in cryptographic schemes due to its robustness against certain hard attacks, and moreover, it offers encryption and decryption speeds with guarantees of strong security. This polynomial-based cryptosystem has been significantly improved based on various mathematical structures [6-10]. In 2021, Bhoi et al. discussed

* Corresponding author
E-mail address nadia.m.ghanim@uotechnology.edu.iq (Instructor).
Peer-reviewed under the responsibility of the University of Garmian.

various techniques applied to a random DNA sample and image encryption using different algorithms [11].

In 2022, Satriyo et al. [12] introduced combining DNA cryptography methods depending on the NTRU cryptosystem to enhance data confidentiality. Additionally, Hagras et al. presented an encryption algorithm based on DES-DNA, utilizing a 64-nucleotide secret key [13]. Patidar and Kaur describe DNA encryption and the corresponding operations used in the image encryption algorithm, as well as the method for generating pseudo-random sequences [14]. Amin and Ahmed explain that open source firewalls bring security benefits to SD-WAN [15], and Hama et al. proposed an analysis of the security level of VANETs [16].

In this paper, the PDNA encryption method is presented, a new encryption method that integrates Deoxyribonucleic acid (DNA) encryption with truncated polynomial-based encryption. The main contribution of this work focuses on applying of customized codon table to obtain a new encryption method with high complexity and high resistance to statistical attacks. It is accomplished by converting text into codons, utilizing the chosen encoding tables as secret keys between the two ends of the transmission, and then applying the truncated polynomial ring to generate the key based on the NTRU cryptosystem technique. This hybridization process led to an increase in data transmission security due to key space expansion. The constructs of the unique encoding tables used to map plaintext characters to codons according to their position help increase the randomness of the encryption process. The effectiveness of the proposed PDNA technique is illustrated through a step-by-step example that demonstrates its applicability. Finally, the security is analyzed to demonstrate its resistance to emerging quantum computing attacks.

The remaining parts of the paper are organized as follows: Section 2 presents the main structure of the DNA sequences to show their nitrogenous bases. Section 3 proposes the new cryptosystem PDNA with its three parts. The security of the proposed system is analyzed in Section 4 to demonstrate its resistance to main attacks. Section 5 concludes the paper.

2 DNA Structure

Deoxyribonucleic acid (DNA) is a molecule responsible for storing and translating genetic information in living organisms. It is shaped like a double helix structure with two parallel opposite strands, as shown in Figure 1, and is composed of small units called nucleotides. Each nucleotide consists of three components:

- Nitrogenous bases.
- Five-carbon sugar.
- Acid phosphate.

DNA contains four different types of nitrogenous bases, including:

Adenine, symbolized by A, thymine, symbolized by T, cytosine, symbolized by C, and guanine, symbolized by G, where the nitrogenous bases are linked to each other in pairs. Adenine bonds with thymine (A-T), and guanine bonds with cytosine (G-C) [17].

3 The Proposed PDNA Cryptosystem

The PDNA cryptosystem is based on using the idea of Deoxyribonucleic Acid (DNA) cryptography. PDNA cryptosystem will be described as follows:

3.1 Key Generation

- Choosing a polynomial $f \in \varphi = Z[x]/x^N - 1$, such that φ is the truncated polynomial ring of degree $N-1$ with integer coefficients and has d_f coefficients equal 1, $d_f - 1$ equal -1, and 0 for the other values. The polynomial f should have a multiplicative inverse with modulo p referred to as f_p^{-1}, such that p and N are positive integer numbers.
- Selecting a strand of Deoxyribonucleic Acid (DNA), and this information is available in databases in international centers specialized in genetic engineering and studying the functioning of genes, as well as many internet sites (GENBANK, EMBL, NCBI).
- Create a set of coding tables (compensatory coding methods) as shown in Tables 1, 2, and 3.

Table 1: Encoding the plain letter into symbols according to its location.

Odd character	Codon	Odd character	Codon	Even character	Codon	Even character	Codon
a	TTC	n	TTA	A	TTG	N	TCT
b	TCC	o	TCA	B	TCG	O	TAT
c	TAC	p	TGT	C	TGC	P	TGG
d	CTT	q	CTC	D	CTA	Q	CTG
e	CCT	r	CCA	F	CAG	S	CGT
f	CAC	s	CAA	F	CAG	S	CGT

g	CGC	t	CGA	G	CGG	T	ATT

From the table above, we notice that a letter that is located in an odd position (referred to as a small character) symbolizes a different codon than the encoding of the same letter, but which is located in an even position (referred to as a capital character) within the chain of letters of the message.

Table 2: The process of encoding two nitrogenous bases into an English letter.

DNA chain resulting from plain letter coding	Agreed on the DND chain	The English letter resulting from the two chains	DNA chain resulting from plain letter coding	Agreed on the DND chain	The English letter resulting from the two chains
T	T	B	A	T	D
T	G	H	A	G	I
T	A	K	A	A	R
T	C	M	A	C	P
G	G	V	C	G	W
G	A	Y	C	A	Z
G	C	E	C	C	F

The rule for creating Table 2 is the result of a codon with another codon that produces one letter of the English alphabet without repetition. For example, the letter resulting from T with T is B, while another user can choose the letter F, and so on.

Table 3: Encoding nitrogenous bases into the binary system.

Nitrogen base	Binary system
A	00
C	01
G	10
T	11

3.2 Encryption

To encrypt the message $\mathcal{M}$, the sender takes the following steps:

- Converting the message $\mathcal{M}$ into codons according to Table 1.
- By using the DNA strand that was chosen in the key generation phase in Table 2, we obtain English letters.
- Convert English letters into a binary system chain based on their alphabetical sequence.
- Convert the binary system chain into a polynomial called $\mathcal{B}$ belonging to the φ based on length N.
- Using the key f that was chosen in the key generation phase, we obtain $\mathcal{C}$ through the following formula:

$\mathcal{C} = f * \mathcal{B}\ (mod\ p)$.

- Convert $\mathcal{C}$ to a binary system.
- Using Table 3, convert the binary chain into a string of nitrogenous bases that represents the ciphertext E.

3.3 Decryption

To decrypt the message E, the recipient performs the following steps:

- Using Table 3, convert a string of nitrogenous bases into the binary system chain.
- Convert the binary system chain into a polynomial θ of length N.
- Compute $\mathcal{D} = f_p^{-1} * \theta\ (mod\ p)$.
- Convert $\mathcal{D}$ into the binary system chain.
- Convert the binary system chain into letters based on their sequence in the English alphabet.
- Convert letters into codons according to Table 2.
- Convert the codons into a message $\mathcal{M}$ according to Table 1.

Figure 1 illustrates the workflow of the PDNA cryptosystem.

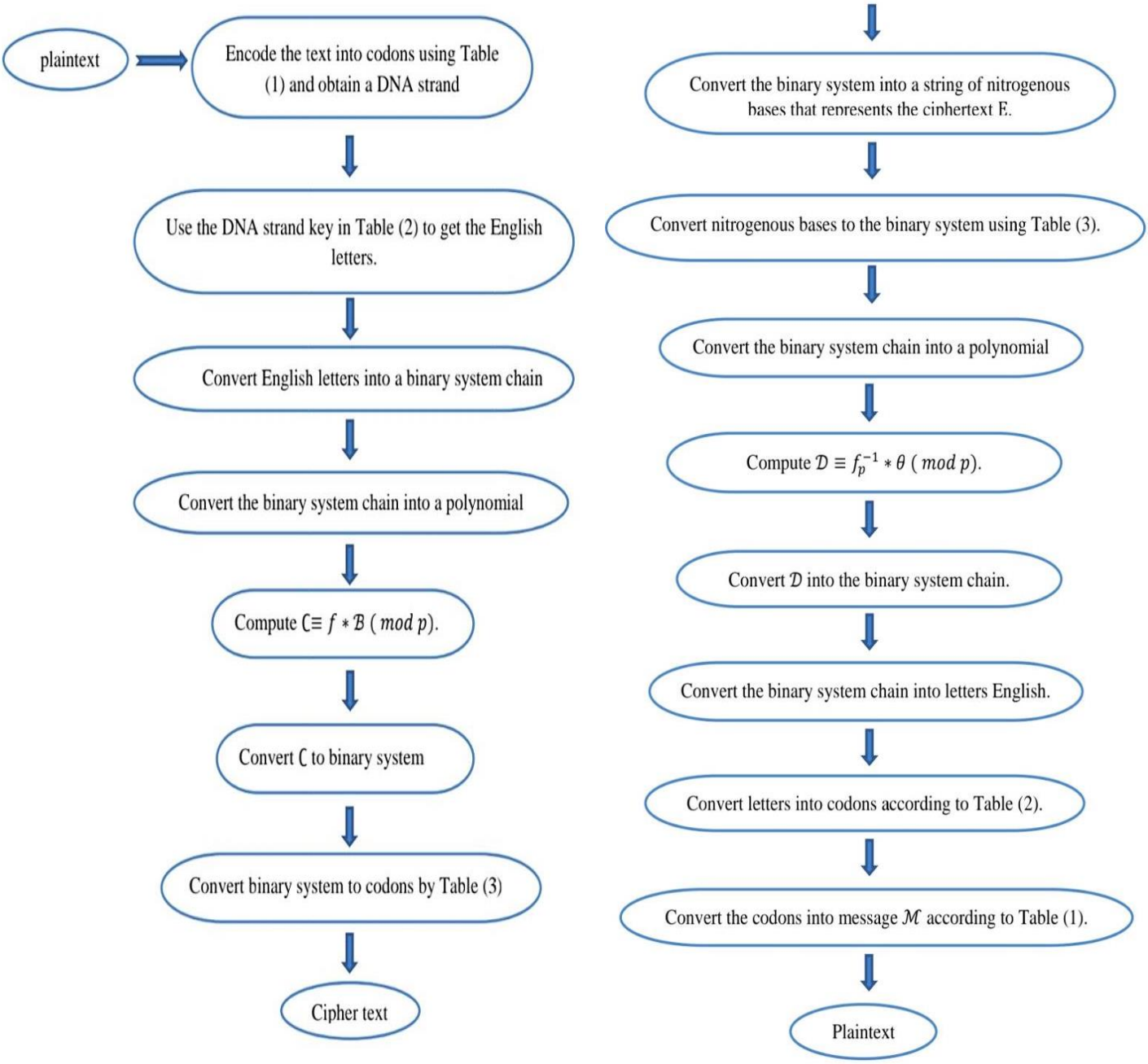

Figure 1: PDNA workflow.

4 Example of PDNA

Take $N = 11$ and $p = 3$

4.1 Generate Keys

- Choose $f = -1 + x + x^2 - x^4 + x^6 + x^9 - x^{10}$,
- Selection of bacteria E. coli taken from the EBI website, where

$\mathcal{G} = ATGTGCGAA\ldots$ as the DNA strand.

4.2 Encryption

- Take the message $\mathcal{M} = a$
- Encoding message $\mathcal{M} = a$ into codons TTC, according to Table 1, because a is located in an odd position.
- Encoding the nitrogenous bases of the two DNA chains into English letters using Table 2, as shown:

Codons	$\mathcal{G}$	English letter
T	A	D
T	T	B
C	G	E

- Convert English letters into a binary number chain based on their alphabetical sequence

Letter	Sequenced in the alphabet	Binary number
D	4	00100
B	2	00010
E	5	00101

Thus, the chain of binary numbers is: $\mathcal{B} = 001000001000101$

- Convert the chain $\mathcal{B}$ into a polynomial based on the length 11, so you will divide $\mathcal{B}$ into two parts (because the length of the chain is greater than 1).

$\mathcal{B}_1 = x^2 + x^8$ and $\mathcal{B}_2 = x + x^3$

Now, the encryption formula is applied as follows:

$$C_1 = f * \mathcal{B}_1 \ (mod\ p)$$

$$= 1 + x + 2x^2 + 2x^3 + x^4 + 2x^7 + x^9 + x^{10} \ \ (mod\ 3),$$

$$C_2 = f * \mathcal{B}_2 \ (mod\ p)$$

$$= 2 + x^4 + x^9 + x^{10} \ (mod\ 3).$$

Such that C_1 represents the encryption of $\mathcal{B}_1$ and C_2 represents the encryption of $\mathcal{B}_2$.

From C_1 and C_2 we get the following binary chain:

000010000100010000100000100000000000001000000000010000100000000000000000

0010000000000000000000000100001

- Using Table 3, convert the binary chain into a string of nitrogenous bases that represents the ciphertext E.

E = $AAGACACAAGAAGAAAAAAGAAAACAAGAGAAAAAAAA$

$AACAAAAAAAAAAAACAAG$.

4.3 Decryption

- Using Table 3, convert a string of nitrogenous bases into the binary system chain

E = $AAGACACAAGAAGAAAAAAGAAAACAAGAGAAAAAAAA$

$ACAAAAAAAAAAAACAAG$.

- Convert the binary system chain into a polynomial θ of length 11, so you will divide θ into two parts (because the length of the chain is greater than 11).

$\theta_1 = 1 + x + 2x^2 + 2x^3 + x^4 + 2x^7 + x^9 + x^{10} \ \ (mod\ 3)$

and

$\theta_2 = 2 + x^4 + x^9 + x^{10}\ (mod\ 3)$.

- Compute:

$$\mathcal{D}_1 = f_p^{-1} * \theta_1\ (mod\ 3)$$
$$= x^2 + x^8\ (mod\ 3),$$
$$\mathcal{D}_2 = f_p^{-1} * \theta_2\ (mod\ 3)$$
$$= x + x^3\ (mod\ 3).$$

- Convert $\mathcal{D}_1$ and $\mathcal{D}_2$ to the binary system chain

001000001000101.

- Convert the binary system chain into letters based on their sequence in the English alphabet. It is divided 001000001000101 into cells, each cell consisting of five units as shown in the table below:

Binary string	number	English letter
00100	4	D
00010	2	B
00101	5	E

- Convert letters into codons according to Table 2

English letter	$\mathcal{G}$	Codons
D	A	T
B	T	T
E	G	C

- Convert the codons TTC into message $\mathcal{M}$ according to Table 1, thus $\mathcal{M} = a$.

5 Performance Analysis

5.1 Security Analysis

The security of the PDNA encryption system depends on the two keys: $\mathcal{G}$ of length n, which represents a specific sequence of DNA, and the key f, which is a polynomial belonging to the ring of the

integers, a truncated polynomial with degree N. The level of security for the key $\mathcal{G}$ depends on great randomness in the selection, which makes it difficult to perform a statistical analysis of the text due to the use of only four letters, unlike what happens in the letters of known languages. Therefore, the space for the key $\mathcal{G}$ is equal to 4^n because of the use of the four letters A, C, G, and T only.

As for the security of the key f depends on the degree of the polynomial N and the number of non-zero coefficients whose space is equal to $\frac{N!}{(d_f!)^2(N-2d_f)!}$, and therefore the total space of the key security level is $4^n \frac{N!}{(d_f!)^2(N-2d_f)!}$, which gives a high level of security for the transmitted data. Since the security of NTRU depends on polynomials only, this means PDNA is more secure than NTRU.

5.2 Speed Analysis

The speed of PDNA depends on the time taken to perform the multiplication polynomial operation and the codons merging operation. Suppose t_1 represent the time of multiplication of polynomials and t_2 represent the time to merge the codons, then the total time of FDNA is shown in Table 4.

Table 4: Execution time of PDNA.

Key generation	Encryption	Decryption	Total time
t_1	$t_1 + t_2$	$t_1 + t_2$	$3t_1 + 2t_2$

Since the speed of NTRU depends on multiplication and addition of polynomials, this means PDNA is faster than NTRU.

Conclusion

In this paper, a new encryption method is presented based on DNA encryption. A set of substitution coding tables was constructed and utilized in conjunction with a coding method based on truncated polynomials. This work's main contribution is the combination of polynomial encryption and biomolecular cryptography to create a hybrid post-quantum cryptographic architecture. The PDNA cryptosystem ensures a larger key space and enhanced resistance to factorization-based cryptanalysis by generating keys using a truncated polynomial ring. Message obfuscation is enhanced by the use of DNA-based encoding tables, which render it impossible for attackers to reassemble the plaintext without knowledge of the encoding technique. According to the security analysis, the PDNA cryptosystem is highly resistant to both algebraic and statistical attacks, making it a viable option for private conversations, cloud storage encryption, and secure data transfer. Additionally, the detailed encryption and decryption demonstration highlights the effectiveness and efficiency of the proposed approach. Using this technique opens some future directions, such as enhancing the resistance to quantum decryption techniques through integration with quantum-safe cryptographic frameworks ·The extension of DNA-based authentication systems utilizes biological encryption techniques to ensure secure identity verification ·It can also be applicable in biomedical data encryption and secure cloud computing, offering cutting-edge security for private genetic and medical data.

Appendix A (Polynomials Calculation)

If

$$f = -1 + x + x^2 - x^4 + x^6 + x^9 - x^{10},$$

$$\mathcal{B}_1 = x^2 + x^8,$$

$$\mathcal{B}_2 = x + x^3,$$
$$\theta_1 = 1 + x + 2x^2 + 2x^3 + x^4 + 2x^7 + x^9 + x^{10},$$

and

$$\theta_2 = 2 + x^4 + x^9 + x^{10}$$

are truncated polynomials then

$f_3^{-1} = 1 + 2x + 2x^3 + 2x^4 + x^5 + 2x^7 + x^8 + 2x^9$ *such that* $f * f_3^{-1} = 1 \, mod \, 3$,

$$\mathcal{C}_1 = f * \mathcal{B}_1 \, (mod \, 3)$$

$$= (-1 + x + x^2 - x^4 + x^6 + x^9 - x^{10}) * (x^2 + x^8) \, (mod \, 3)$$

$$= 1 - 2x - x^2 + 2x^3 + x^4 - x^7 + x^9 + x^{10} \, (mod \, 3)$$

$$= 1 + x + 2x^2 + 2x^3 + x^4 + 2x^7 + x^9 + x^{10} \, (mod \, 3),$$

$$\mathcal{C}_2 = f * \mathcal{B}_2 \, (mod \, p)$$

$$= (-1 + x + x^2 - x^4 + x^6 + x^9 - x^{10}) * (x + x^3) \, (mod \, 3)$$

$$= -1 + x^4 + x^9 + x^{10} \, (mod \, 3)$$

$$= 2 + x^4 + x^9 + x^{10} \, (mod \, 3).$$

Also,

$$\mathcal{D}_1 = f_p^{-1} * \theta_1 \, (mod \, 3)$$

$$= (1 + 2x + 2x^3 + 2x^4 + x^5 + 2x^7 + x^8 + 2x^9) * (1 + x + 2x^2 + 2x^3 + x^4 + 2x^7 + x^9 + x^{10}) \, (mod \, 3)$$

$$= x^2 + x^8 \, (mod \, 3),$$

$$\mathcal{D}_2 = f_p^{-1} * \theta_2 \ (mod\ 3)$$

$$= (1 + 2x + 2x^3 + 2x^4 + x^5 + 2x^7 + x^8 + 2x^9) * (2 + x^4 + x^9 + x^{10})(mod\ 3)$$

$$= x + x^3 \ (mod\ 3).$$

References

[1] Chen, J. A., DNA-Based, Biomolecular Cryptography Design. *IEEE Int. Symp. Circuits Syst.*, **2003**, Bangkok, Thailand, doi:10.1109/ISCAS.2003.1205146 (2003).

[2] Adleman, L. Molecular computation of solutions to combinatorial problems. *Science* **266**, 1021–1024, doi:10.1126/science.7973651 (1994).

[3] Boneh, D., Dunworth, C. & Lipton, R. J. Breaking DES using a molecular computer. *DIMACS Ser Discrete Math Theor Comput Sci* **27**, 37–65, doi:10.1090/dimacs/027/04 (1996).

[4] Cui, G., Qin, L., Wang, Y. & Zhang, X. An encryption scheme using DNA technology. *Proc 3rd Int Conf Bio-Inspired Computing: Theories and Applications (BIC-TA)*, 37–42, doi:10.1109/BICTA.2008.4656701 (2008).

[5] Sabry, M., Hashem, M., Nazmy, T. & Khalifa, M. E. A DNA and amino acids-based implementation of Playfair cipher. *Int J Comput Sci Inf Secur* **8**, 129–136 (2010).

[6] Yassein, H. R., Abidalzahra, A. A. & Al-Saidi, N. M. G. A new design of NTRU encryption with high security and performance level. *AIP Conf Proc* **2334**, 080005, doi:10.1063/5.0042312 (2021).

[7] Yassein, H. R. & Al-Saidi, N. M. G. A comparative performance analysis of NTRU and its variant cryptosystems. *Proc Int Conf Current Research in Computer Science and Information Technology (ICCIT)*, 115–120, doi:10.1109/CRCSIT.2017.7965544 (2017).

[8] Yassein, H. R., Reshan, A. H. & Al-Saidi, N. M. G. AHQTR: A new NTRU variant based on quaternion algebra. *Proc 8th Int Cryptology and Information Security Conf (CRYPTOLOGY)*, 100–108 (2022).

[9] Yassein, H. R., Al-Saidi, N. M. & Farhan, A. K. A new NTRU cryptosystem outperforms three highly secured NTRU-analog systems through an innovational algebraic structure. *J Discrete Math Sci Cryptogr* **25**, 523–542, doi:10.1080/09720529.2020.1741218 (2022).

[10] Albakaa, F. H. & Yassein, H. R. A new encryption scheme based on DNA and polynomials with more security. *Int J Math Comput Sci* **20**, 383–386, doi:10.69793/ijmcs/01.2025/albakaa (2025).

[11] Bhoi, G., Bhavsar, R., Prajapati, P. & Shah, P. A review of recent trends on DNA based cryptography. *Proc 3rd Int Conf Intelligent Sustainable Systems (ICISS)*, 815–822, doi:10.1109/ICISS49785.2020.9316013 (2020).

[12] Satriyo, U. S. D., Rahutomo, F., Harjito, B. & Prasetyo, H. DNA cryptography based on NTRU cryptosystem to improve security. *Proc IEEE 8th Inf Technol Int Seminar (ITIS)*, 27–31, doi:10.1109/ITIS57155.2022.10010152 (2022).

[13] Hagras, T., Salama, D. & Youness, H. Anti-attacks encryption algorithm based on DNA computing and data encryption standard. *Alex Eng J* **61**, 11651–11662, doi:10.1016/j.aej.2022.05.033 (2022).

[14] Patidar, V. & Kaur, G. A novel conservative chaos driven dynamic DNA coding for image encryption. *Front Appl Math Stat* **8**, 1–21, doi:10.3389/fams.2022.1100839 (2022).

[15] Zhang, M., Tao, W., Tarn, T. & Xi, N. Interactive DNA sequence and structure design for DNA nanoapplications. *IEEE Trans Nanobiosci* **3**(4), 286 - 292, doi:10.1109/TNB.2004.837918 (2004).

[16] Hama, D. K., Mubarek, F. S. & Abdullatif, F. A. Enhanced Security Taxonomy for Fog-Enabled VANETs: A Comprehensive Survey on Attacks, Challenges, Applications and Architectures. *Passer Journal* **7**, 27-32, 10.24271/psr.2024.488319.1811, (2025).

[17] Zhang, M., Sabharwal, C. L., Tao, W., Tarn, T., Xi, N. & Li, G. Interactive DNA sequence and structure design for DNA nanoapplications. *IEEE Transactions on Nanobioscience* **4**, doi: 10.1109/TNB.2004.837918 (2004).