Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2026 (44)** : 1–7.
ISSN-0037-8712
doi:10.5269/bspm.81388

# A Security Comparison of Cryptosystems Based on DNA

Atwar Ahmed Abboodi, Ameera Nema Alkiffai and Hassan Rashed Yassein

ABSTRACT: This study presents three previously introduced coding systems, examining their mathematical structures and the tools used in their three phases, and then offers a comparative analysis of their security. The first system, ATDNA, uses DNA encoding and polynomials, while the second system, LPDNA, relies on polynomials ring, DNA encoding, and the Laplace transform. The third system, DNPL is based on DNA structure, permutations, and the Laplace transform.

Keywords: DNA, Polynomial rings, Laplace transform, permutation, security analysis.

## Contents



## 1. Introduction

Modern approaches utilize algebraic structures, such as polynomial rings, permutation, and Laplace transform, to improve key generation and resistance to attacks. Combining these with DNA coding results in multi- layered cryptosystems with enhanced security. In 1994, Adleman conducted a pioneering experiment demonstrating the ability of DNA molecules to perform computational tasks, thereby laying the foundation for DNA computing as a multidisciplinary research field [1]. In 2008, Doleskani et al. introduced a public-key encryption scheme based on the symmetric groupS_n, resistant to discrete logarithm attacks, while requiring relatively higher memory and bandwidth [2]. In 2011, Yunpeng et al. proposed a symmetric DNA-based cryptosystem that relies on sequence indexing combined with block cipher techniques to encode and secure messages [3]. In 2012, Church et al. presented a technique for encrypting and storing digital data within DNA molecules [4]. In 2013, Hewarikar proposed an innovative mathematical encryption method based on the Laplace transform, using its inverse for decryption, thereby enhancing data transmission security [5]. In 2017, Erlich and Zielinski presented a more efficient

2020 *Mathematics Subject Classification:* 94A60, 11T71.
Submitted January 16, 2026. Published June 05, 2026.

model using DNA techniques, which improved the effectiveness of data storage and retrieval [6]. In 2018, Vidhya and Rathipriya increased the complexity of DNA sequence encoding to enhance security levels [7]. In 2020, Farhan et al. developed an innovative mRNA-based substitution box (S-box), generating the required number of boxes using a secret key [8]. Several researchers have presented a number of encryption methods based on polynomials ring in their construction phases [9,10,11,12,13,14,15]. In 2024, Abidalzahra presented the PDNA system, based on polynomial rings and DNA codons [16]. In 2025, Albakaa and Yassein proposed the FDNA system, a high-security scheme utilizing truncated polynomial rings and DNA codons [17].

## 2. Previously Cryptosystems

### 2.1. ATDNA Cryptosystem

The ATDNA encryption method combines DNA sequences with polynomial operations and substitution tables based on the four nucleotides (A, T, C, G), enhancing data security and randomness. Since the discovery of the DNA double-helix, researchers have explored its potential for storing and encoding information, giving rise to DNA computing that merges molecular biology with computer science. The ATDNA system provides an effective and secure model for textual data encryption.

*2.1.1. Key Generation.* The key consists of two independent components:

1. DNA Strand: A DNA strand is selected from reliable databases such as GENBANK and EMBL.
2. Polynomial Key $f(x)$: A polynomial is chosen from the truncated ring $Z[x]/(x^N - 1)$ with specific coefficients and a multiplicative inverse $f_p^{-1}$.

Coding tables are used to convert letters of the original message into DNA codons. Each codon represents a specific letter from the message according to the table, forming the basis of the encryption process.

*2.1.2. Encryption.* To encrypt a message $M$:

1. Convert the original text into DNA codons using the encoding table.
2. Using the key generated in the key generation step and the codons obtained from the previous step, they are converted into English letters according to the coding table.
3. Convert symbols into a binary sequence and transform the binary sequence into a polynomial $g$.
4. Compute $C \equiv f * g(mod\ p)$. Convert $C$ to binary system and the binary system into a string of nitrogenous bases that represents the ciphertext E.

*2.1.3. Decryption.* To decryption the ciphertext E:

1. Convert the DNA sequence back to binary using the encoding tables. And transform the binary sequence into a polynomial of length N.
2. Compute $\mathcal{A} \equiv f_p^{-1} * \theta\ (mod\ p)$ and convert to binary chain.
3. Convert the binary sequence to plaintext symbols, then to DNA codons, and finally recover the original message $M$.

### 2.2. LPDNA Cryptosystem

The LPDNA cryptosystem is introduced as a hybrid scheme that combines DNA sequences, polynomial rings, and the Laplace transform to address modern security challenges. This design leverages the inherent randomness of DNA, the algebraic structure of polynomials, and the mathematical transformation of Laplace to achieve secure encryption and decryption.

*2.2.1. Key Generation.* Key generation consists of three components:

1. DNA sequence key: A DNA strand is selected from publicly available databases such as GENBANK or EMBL. This strand introduces high randomness due to the four nucleotide bases (A, T, C, G).

2. Polynomial key: A truncated polynomial $g(x) \in Z[x]/x^N - 1$ of degree $N-1$ is chosen with integer coefficients. Certain coefficients are set to 1 or -1, while others are zero. The polynomial must have a multiplicative inverse modulo $p$, denoted $g_p^{-1}$, where $p$ and $N$ are positive integers.

3. Laplace function key: A function $f(x)$ with a Taylor series, (e.g. $t^l \cosh(rt)$), is selected. This function provides an additional layer of transformation to enhance the security of the cryptosystem

Finally, coding schemes are established to convert plaintext into DNA codons, translate codons into English letters, and represent nucleotide sequences in binary format.

*2.2.2. Encryption.* To encrypt a message $M$, the following steps are performed:

1. The plaintext is encoded into DNA codons according to a predefined encoding rule.

2. The resulting codons are converted into English letters using the specified DNA sequence according to the established coding table.

3. The English letters are transformed into a binary representation according to their alphabetical order.

4. The obtained binary sequence is represented as a polynomial $B$ of degree $N$.

5. Compute $C \equiv g * B \ (mod\ p)$.

6. The polynomial C is converted into binary form and then into decimal form to obtain a numerical sequence.

7. The Laplace transform of the selected mathematical function is applied, and the resulting coefficients are reduced modulo 26.

*2.2.3. Decryption.* To decrypt the ciphertext E:

1. Convert the received ciphertext into a binary representation and then into decimal values $G_i$.

2. Apply the key $k_i$ to compute $q_i = 26k_i + G_i$ and perform the inverse Laplace transform to obtain the values $G$.

3. Convert the obtained values $G$ into a binary sequence and then into a polynomial of length $N$.

4. Compute $D \equiv g_p^{-1} * \theta \ (mod\ p)$ and convert $D$ into a binary sequence.

5. Convert the binary sequence into English letters and then into codons.

6. Convert the codons into the plaintext message.

### 2.3. DNPL Cryptosystem

The proposed DNPL system (DNA-Permutation-Laplace) is based on the combination of three fundamental concepts: DNA structure, the permutation group $(S_n, ^\circ)$ and the Laplace transform of certain special functions. This system combines the security features of DNA with the precision of mathematical operations in permutations and the Laplace transform, enhancing overall efficiency and making code-breaking more difficult. The steps for constructing the system are presented below:

*2.3.1. Key Generation.* The system uses three main keys:

1. DNA Key: A DNA sequence is selected from genetic databases or generated randomly.
2. Permutation Key: An element from the permutation group is chosen to reorder the message components.
3. Mathematical Function Key: A function with a Taylor series expansion is used, for example: $f(t) = t^l \sinh(rt)$, Coding tables are used to convert letters to codons, convert nucleotide pairs to English letters, and represent nucleotides in binary form, which facilitates key application.

*2.3.2. Encryption.* To encryption the original message $M$ and produce an unintelligible ciphertext for unauthorized parties, the following steps are applied:

1. DNA Representation of the Message: The original message M is converted into DNA codons using the predefined coding table. These codons are then transformed into English letters according to the coding scheme based on the selected DNA sequence.
2. Permutation Process: The resulting text is divided into blocks of length $n$ according to the permutation group $S_n$. If the last block is shorter than $n$, the character $x$ is appended repeatedly until the required length is reached. The characters within each block are then rearranged using a selected permutation key. After that the letters are converted into numerical values based on their alphabetical order $(a = 0, b = 1, \ldots, z = 25)$, producing the numerical encrypted message $G_i$.
3. Mathematical Processing Using the Laplace transform: The function $f(t) = G_i \sinh(rt)$,
4. Binary and DNA Encoding: The obtained coefficients are reduced using the operation mod 26. The resulting values are converted into a binary sequence, which is subsequently represented as a DNA nucleotide sequence using the predefined coding table, yielding the final ciphertext E.

*2.3.3. Decryption.* Upon receiving the ciphertext, the receiver performs a sequence of reverse operations to recover the original message as follows:

1. Conversion from DNA to Numerical Form: The DNA nucleotide sequence is converted into a binary sequence using the predefined coding table. The binary sequence is then divided into fixed-length segments, and each segment is converted into its corresponding decimal value.
2. Inverse Mathematical Processing: The numerical values are computed using the relation $q_i = 26k_i + G_i$.
3. Recovery of Alphabetic Representation: The resulting numerical values are converted into English letters according to their positions in the English alphabet.
4. Inverse Permutation Process: The letters are divided into blocks of length n according to the permutation group $S_n$. The inverse permutation key is then applied to restore the original order of letters within each block.
5. Retrieval of the Original Message: The resulting English letters are converted into DNA codons using the DNA sequence and the coding table. Finally, the original message is recovered from the obtained codons using the predefined decoding table.

## 3. Security Comparison of Cryptosystems

### 3.1. Security Comparison between ATDNA and LPDNA

The ATDNA system employs two primary keys: one derived from a DNA sequence and the other from a polynomial, providing a high level of security within its mathematical design. In contrast, the LPDNA system uses a DNA sequence, a polynomial, and a Laplace-based key, forming a multi-layered cryptographic structure that enhances the security of the encryption process and increases resistance against various potential attacks. Consequently, LPDNA is considered more secure than ATDNA while

maintaining efficient encryption and effective protection of sensitive data, making it highly suitable for applications requiring the highest level of cryptographic security. Table 1 presents the security comparison between the two cryptosystems.

Table 1: Comparison of ATDNA and LPDNA

| Cryptosystem | Security space |
|---|---|
| ATDNA | $\frac{4^{\alpha}N!}{d_f\ ((d_f-1)!)^2\ (N-2d_f+1)!}$, |
| LPDNA | $\frac{4^{\alpha}N!\ 359l}{d_f\ ((d_f-1)!)^2\ (N-2d_f+1)!}$ |

### 3.2. Security Comparison between ATDNA and DNPL

The ATDNA system employs two primary keys: one derived from a DNA sequence and the other from a polynomial, providing a high level of security within its mathematical design. In contrast, the DNPL system relies on a DNA sequence, a permutation from the symmetric group, and a Laplace-based key, which enhances its cryptographic strength by expanding the possible key space. The security comparison indicates that ATDNA is more secure than DNPL if $\frac{N!}{d_f((d_f-1)!)^2(N-2d_f+1)!} > (n!-1)(359l)$; otherwise, DNPL demonstrates superior security. Table 2 presents the security comparison between the two cryptosystems.

Table 2: Comparison of ATDNA and DNPL

| Cryptosystem | Security space |
|---|---|
| ATDNA | $\frac{4^{\alpha}N!}{d_f\ ((d_f-1)!)^2\ (N-2d_f+1)!}$, |
| DNPL | $(4^{\alpha})(n!-1)(359l)$ |

### 3.3. Security Comparison between PLDNA and DNPL

The LPDNA system has three main keys: a DNA sequence, a polynomial key, and a Laplace transform key, providing a cryptographic structure based on the algebraic properties of those keys. In contrast the DNPL system also uses three keys: a DNA sequence, a permutation key, and a Laplace transform key, which expands the possible key space due to the permutation element. The security comparison indicates that if the following condition is satisfied: $\frac{N!}{d_f((d_f-1)!)^2(N-2d_f+1)!} > (n!-1)$, then LPDNA is more secure than DNPL, otherwise DNPL remains the more secure. Table 3 presents the security comparison between the two cryptosystems.

Table 3: Comparison of LPDNA and DNPL

| Cryptosystem | Security space |
|---|---|
| LPDNA | $\frac{4^{\alpha}N!359l}{d_f((d_f-1)!)^2(N-2d_f+1)!}$, |
| DNPL | $(4^{\alpha})(n!-1)(359l)$ |

Thus, the LPDNA system is more secure than the ATDNA system due to its three keys, and it becomes more secure than the DNPL system if the following condition is satisfied: $\frac{N!}{d_f((d_f-1)!)^2(N-2d_f+1)!} > (n!-1)$, otherwise, the DNPL system is the most secure. As for the systems ATDNA and DNPL, the ATDNA system is more secure if the following condition is satisfied: $\frac{N!}{d_f((d_f-1)!)^2(N-2d_f+1)!} > (n!-$

1)(359$l$); otherwise, the DNPL system remains the most secure. Table 4 presents the security comparison between the three cryptosystems.

Table 4: Comparison of ATDNA, LPDNA, and DNPL

| Cryptosystem | Security space |
|---|---|
| ATDNA | $\frac{4^{\alpha}N!}{d_f((d_f-1)!)^2(N-2d_f+1)!}$, |
| LPDNA | $\frac{4^{\alpha}N!359l}{d_f((d_f-1)!)^2(N-2d_f+1)!}$, |
| DNPL | $(4^{\alpha})(n!-1)(359l)$ |

## 4. Conclusion

The security analysis of the three cryptosystems indicates that the LPDNA system is the most secure due to its three primary keys (DNA, Polynomials, Laplace), providing the highest resistance against mathematical and analytical attacks and enhancing overall data protection. The ATDNA system outperforms DNPL if the specified mathematical condition is satisfied; otherwise, DNPL retains the highest security level. Direct comparisons between the systems show that LPDNA surpasses both ATDNA and DNPL when the security conditions are met, and the overall ranking of the systems in terms of security is: LPDNA first, followed by ATDN, and then DNPL. This reflects the critical role of the number and type of keys in strengthening the overall cryptosystem security, confirming that a multi-key design is essential for resisting advanced attacks, maintaining encryption efficiency, and protecting sensitive data effectively.

## References

1. L.M. Adleman. Molecular computation of solutions to combinatorial problems. *science*, 266(5187):1021–1024, 1994.
2. J. N. Doliskani, E. Malekian, and A. Zakerolhosseini. A cryptosystem based on the symmetric group. *IJCSNS International Journal of Computer Science and Network Security*, 8(2):273–277, 2008.
3. Y. Zhang, Y. Zhu, Z. Wang, and R.O. Sinnott. Index-based symmetric dna encryption algorithm. In *2011 4th International Congress on Image and Signal Processing*, volume 5, pages 2290–2294. IEEE, 2011.
4. G.M. Church, Y. Gao, and S. Kosuri. Next-generation digital information storage in dna. *Science*, 337(6102):1628–1628, 2012.
5. A. P. Hiwarekar. Application of laplace transform for cryptographic scheme. In *Proceedings of the World Congress on Engineering 2013, Vol. I*, WCE 2013, pages 1–6, London, U.K., 2013.
6. Y. Erlich and D. Zielinski. Dna fountain enables a robust and efficient storage architecture. *Nature Biotechnology*, 35(5):441–446, 2017.
7. E. Vidhya and R. Rathipriya. Two level text data encryption using dna cryptography. *International Journal of Computational Intelligence and Informatics*, 8(3):106–118, 2018.
8. A.K. Farhan, R.S. Ali, H.R. Yassein, N.M.G. Al-Saidi, and G.H. Abdul-Majeed. A new approach to generate multi s-boxes based on rna computing. *Int. J. Innov. Comput. Inf. Control*, 16(1):331–348, 2020.
9. S. H. Shahhadi and H. R. Yassein. NTRsh: A new secure variant of ntruencrypt based on tripternion algebra. *Journal of Physics: Conference Series*, 1999(1):012092, 2021.
10. H. H. Abo-Alsood and H. R. Yassein. QOTRU: A new design of NTRU public key encryption via qu-octonion subalgebra. *Journal of Physics: Conference Series*, 1999(1):012097, 2021.
11. S. H. Shahhadi and H. R. Yassein. An innovative tripternion algebra for designing NTRU-like cryptosystem with high security. *AIP Conference Proceedings*, 2386(1):060009, 2022.
12. F. R. Atea and H. R. Yassein. PMRSA: Designing an efficient and secure public-key similar to RSA based on polynomial ring. *Applied Mathematics and Information Sciences*, 17(3):535–538, 2023.
13. N. N. Abass and H. R. Yassein. Design of an alternative to polynomial modified RSA algorithm. *International Journal of Mathematics and Computer*, 19(3):693–696, 2024.
14. S. M. Abboud, H. R. Yassein, and R. K. Alhamido. Improvement of a multi-dimensional public-key OTRU cryptosystem. *Computer Science*, 19(4):1071–1076, 2024.

15. H. R. Yassein and H. A. Ali. Hudtru: An enhanced NTRU for data security via quintuple algebra. *International Journal of Mathematics and Computer Science*, 2:199–204, 2023.

16. A.A. Abidalzahra. *Designing Secure Public Key Cryptosystem Based on NTRU and DNA*. M.sc. thesis, University of Al-Qadisiyah, Iraq, 2024.

17. F. H. Albakkaa and H. R. Yassein. A new encryption scheme based on DNA and polynomials with more security. *International Journal of Mathematics and Computer Science*, 20(1):383–386, 2025.

*Atwar Ahmed Abboodi,*
*Department of Mathematics,*
*Faculty of Education for Women, University of Kufa*
*Iraq.*
*E-mail address:* atwara.alkoofee@student.uokufa.edu.iq

*and*

*Ameera Nema Alkiffai,*
*Department of Mathematics,*
*Faculty of Education for Women, University of Kufa*
*Iraq.*
*E-mail address:* ameeran.alkiffai@uokufa.edu.iq

*and*

*Hassan Rashed Yassein,*
*Department of Mathematics,*
*Collage of Education, University of Al-Qadisiyah,*
*Iraq.*
*E-mail address:* hassan.yaseen@qu.edu.iq