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

(3s.) **v. 2026 (44)** : 1–8.
ISSN-0037-8712
doi:10.5269/bspm.79624

An Enhanced Encryption Scheme Employing Laplace Transform, DNA Coding, and Truncated Polynomial Rings

Atwar Ahmed Abboodi, Ameera Nema Alkiffai and Hassan Rashed Yassein*

ABSTRACT: This paper presents an advanced encryption algorithm, named LPDNA, which employs the algebraic structure of polynomial rings, the mathematical properties of the Laplace transform, and DNA coding as the foundation for key generation. The proposed algorithm features multi-structured keys, enhancing its resistance against various types of attacks while providing high and reliable performance. It is designed to secure data transmission in untrusted environments and over insecure communication channels, making it an effective solution to meet the increasing security demands of the digital age.

Keywords: Encryption, Laplace transform, polynomials ring, DNA coding, security.

Contents

1. Introduction

The rapid advancement of digital technologies has increased the need for the development of advanced encryption systems to address emerging security challenges. As adversaries gain greater capabilities in cryptanalysis, traditional methods have become less effective against complex and sophisticated attacks, prompting the ongoing search for stronger and more efficient encryption schemes to resist modern decryption attempts. In 1994, Adleman's pioneering experiment demonstrated the ability of DNA molecules to perform computational tasks, marking the beginning of DNA computing as a multidisciplinary scientific field [1]. In 2011, Zhang et al. proposed a symmetric encryption algorithm based on DNA, utilizing sequence indexing and block cipher techniques to secure messages [2]. In 2012, Som and Som developed a symmetric encryption system called DSWLT, notable for its high performance and efficiency in encrypting large-scale data files [3]. In 2013, Church et al. presented a method for encrypting and storing digital data within DNA molecules [4], while in the same year, Hewarikar introduced an innovative mathematical encryption technique based on the Laplace transform for encrypting plaintext and reversing it for decryption, thereby enhancing data transmission security [5]. In 2017, Ehrlich and Zelinski proposed a more efficient model through the DNA Fountion technique, which improved the efficiency 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 S-boxes using a secret key [8]. In 2021, Al-Azzani et al. proposed a new encryption system based on the Laplace transform using substitution boxes, where messages are encrypted over multiple rounds with the secret key applied in each round, providing a higher

* Corresponding author.
2020 *Mathematics Subject Classification:* 94A60, 11T71.
Submitted October 17, 2025. Published March 19, 2026

level of security against various attacks [9]. In 2022, Pranajaya and Soegiarto proposed an encryption system based on the Laplace transform and the maclaurin series, using numbers derived from the series as parameters for key and ciphertext generation. Decryption relies on the inverse Laplace transform, with adaptability to different alphabets [10]. In 2023, Sharba et al. introduced a novel encryption approach based on Taylor series coefficients of the logarithmic function, with decryption using the Laplace transform to reverse the function, resulting in innovative encryption and decryption formulas [11]. In the same year, Rasool and Mohan proposed an encryption method based on a Laplace equation and its inverse transform, converting messages from plaintext to ciphertext through multiple transformation rounds to ensure information confidentiality [12]. In 2024, Abidalzahra presented the PDNA system, based on polynomial rings and DNA codons [13]. In 2025, Albakaa and Yassein proposed the FDNA system, which utilizes truncated polynomial rings and DNA codons [14]. This paper, is structured as follows: Section two reviews the mathematical foundations; Section three presents the proposed encryption method; Section four analyzes the system's security; and Section five presents the conclusion.

2. Mathematical Preliminaries

Theorem 2.1 *[5] Consider standard expansion*

$$f(t) = Gt^j \cosh rt = \sum_{i=0}^{\infty} \frac{G_i r^{2i} t^{2i+j}}{2i\ !},$$

by writing G as a coefficient of $t^j \cosh rt$, when taking Laplace transform then G_i converted to $G_i' = q_i - 26k_i$, where $q_i = G_i r^{2i}(2i+1)(2i+2)\dots(2i+j)$ with $k_i = \frac{q_i - G_i'}{26}$ for $i = 0, 1, 2, 3\dots$ and $r, j = 1, 2, 3\dots$.

Theorem 2.2 *[5] Given G_i' and k_i for $i = 0, 1, 2\dots$ and taking inverse Laplace transform of*

$$G'\left(\frac{-d^j}{ds^j}\right)\left(\frac{1}{s^2 - r^2}\right) = \sum_{i=0}^{\infty} \frac{q_i}{s^{2i+j+1}},$$

then G_i' converted to $G_i = \frac{26k_i + G_i'}{r^{2i}(2i+1)(2i+2)\dots(2i+j)}$, where $q_i = G_i' + 26k_i$ with $k_i = \frac{q_i - G_i'}{26}$ for $r, j = 1, 2, 3\dots$.

The Laplace transform [15]: If $f(t)$ is a function defined for all positive values of t, then the Laplace transform of $f(t)$ is

$$L\{f(t)\} = F(s) = \int_0^{\infty} e^{-st} f(t)\, dt.$$

Provided that the integral exists. Here the parameter s a real or complex number. The corresponding inverse Laplace transform is $L^{-1}\{F(s)\} = f(t)$. Here $f(t)$ and $F(s)$ are called as pair of Laplace transform.

Truncated Polynomial Ring [16]: A truncated polynomial ring is defined as $\mathbb{Z}_p[x]/(x^N - 1)$, where the polynomials have integer coefficients modulo p and a degree less than N. In this ring, addition is performed by summing the corresponding coefficients. Multiplication follows the relation $x^N \equiv 1$, which means any term of degree $\geq N$ is reduced modulo $x^N - 1$, ensuring that the remains of degree less than N.

3. LPDNA Cryptosystem

The Laplace-Polynomial-DNA (LPDNA) encryption system relies on three distinct techniques that collectively enhance security: the Laplace transform for generating time-based keys, polynomial rings for providing an efficient algebraic framework, and DNA sequences for introducing high randomness. The system is implemented through structured phases designed to coordinate these components for secure and efficient encryption. These phases are as follows

3.1. Key Generation

The steps of the key generation algorithm are as follows:

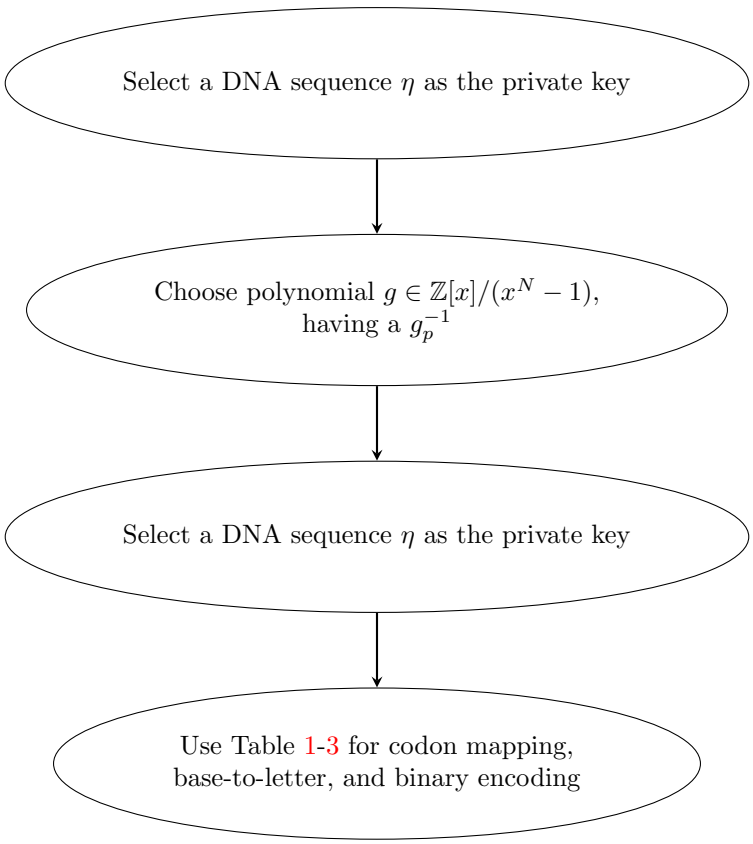

Figure 1: Key Generation

Table 1: Coding of plaintext characters into codons according to their position

Letter	Codon	Letter	Codon	Letter	Codon	Letter	Codon
a	TTTC	n	GTAC	A	TATG	N	GACG
b	TCCA	o	GTCA	B	TGCA	O	GCCC
c	AATG	p	ACGA	C	AGTT	P	AGGA
d	ATCC	q	ACCA	D	AACA	Q	ATTA
e	ATAA	r	ACAG	E	AGAG	R	AAGA
f	GTTC	s	CACA	F	GACC	S	CGCA
g	GGAC	t	CCTG	G	GAGA	T	CTTA
h	TCAC	u	TGAA	H	TAAA	U	TACA
i	TGGC	v	TAGC	I	TCGG	V	TTGG
j	CCAT	w	TTAC	J	CAGC	W	TTCC
k	CGGT	x	CAAA	K	CGAC	X	CCCA
l	ATGG	y	CCGT	L	AAAA	Y	CTGC
m	ACTA	z	CTCA	M	AGCA	Z	CTAA
0	TCTA	1	CGTG	2	GGTA	3	GAAA
4	GCGG	5	AGTA	6	CATT	7	TGTA
8	GCAA	9	GATG				

Table 2: The procedure of converting two nitrogenous bases into an English letter

Standard DNA strand	A DNA strand generated from plaintext encoding	The English letter encoded the two bases	Standard DNA strand	A DNA strand generated from plaintext encoding	The English letter encoded the two bases
T	T	B	T	A	D
G	T	H	G	A	I
A	T	K	A	A	R
C	T	M	C	A	P
T	G	S	T	C	X
G	G	V	G	C	W
A	G	Y	A	C	Z
C	G	E	C	C	F

Table 3: Coding of nitrogenous bases in the binary system

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

3.2. Encryption

The steps of the encryption algorithm are as follows:

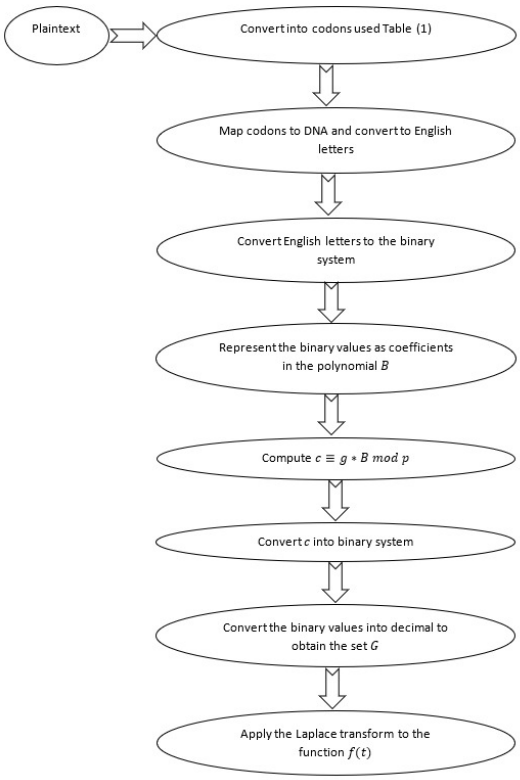

Figure 2: Encryption.

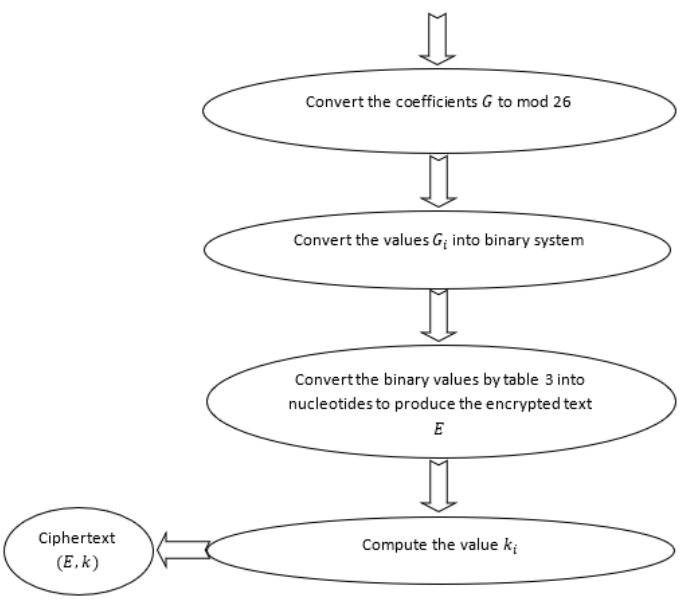

Figure 2: Encryption (Continued).

3.3. Decryption

The steps of the decryption algorithm are as follows:

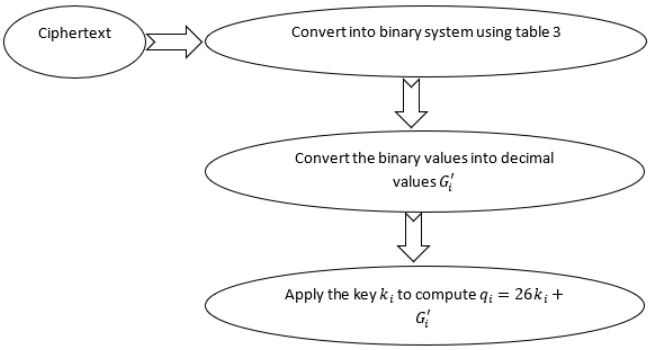

Figure 3: Decryption.

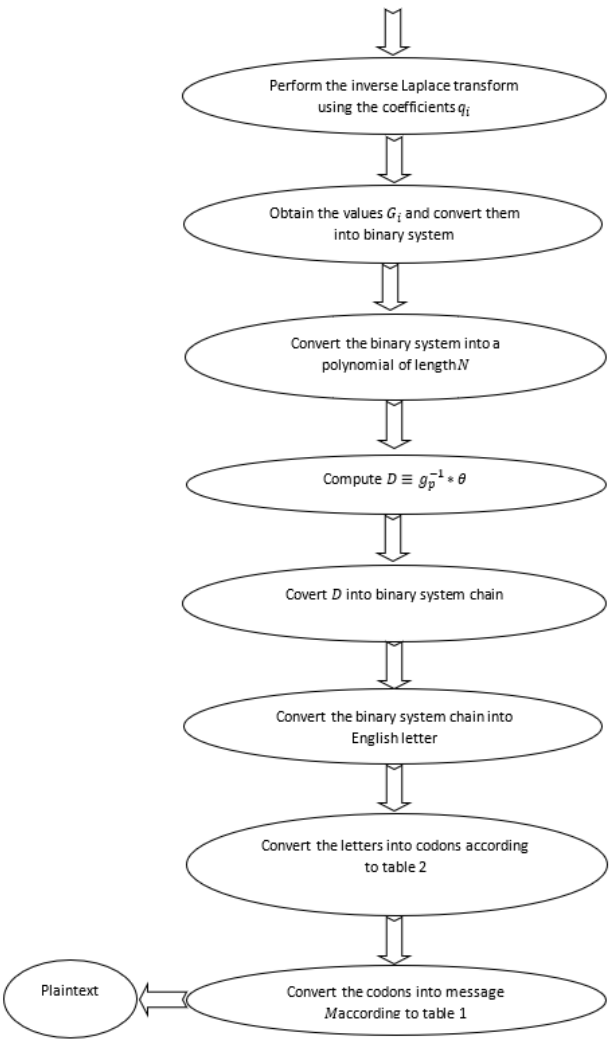

Figure 3: Decryption (Continued).

4. Security Analysis of the LPDNA Encryption System

The security of the LDNA encryption system is based on the combination of three independent keys: DNA sequences, a truncated polynomial ring, and nonlinear mathematical function. This multilayered key structure provides a high level of complexity, significantly enhancing the system's resistance to both classical and modern cryptanalytic attacks. The extensive key space, resulting from the combination of the individual security domains of all components, makes it computationally infeasible to perform an exhaustive exploration of all possible key combinations. The overall security strength of the system can be expressed mathematically as follows:

$$(4^n)\frac{N!}{(d_f!)^2\,(N-2d_f)!}\;(359k).$$

This expression reflects the security relationship between all three components of the system, indicating that the system's resistance increases exponentially with the growth of the sequence length and the number of nonzero polynomial coefficients.

5. Conclusions

The LPDNA system is built upon a combination of mathematical and biological concepts, providing it with the capability to safeguard financial transactions and sensitive information exchanged over the internet, thereby enhancing the level of trust in digital services. One of the primary applications of this system lies encrypting data stored on cloud services, ensuring that such information remains protected even if unauthorized parties gain access to the servers, as the encrypted data cannot be deciphered without the corresponding decryption keys. Furthermore, the system can be effectively employed in mobile devices, including smartphones and tablets, to secure personal information stored on these platforms, offering a reliable and robust layer of data protection.

References

1. L.M. Adleman. Molecular computation of solutions to combinatorial problems. *science*, 266(5187):1021–1024, 1994.
2. 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.
3. S. Som and M. Som. Dna secret writing with laplace transform. *International Journal of Computer Applications*, 50(5):44–50, 2012.
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*, volume 1, pages 3–5, 2013.
6. Y. Erlich and D. Zielinski. Dna fountain enables a robust and efficient storage architecture. *science*, 355(6328):950–954, 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. A.M. Al-Azzani, M.A.M. Rageh, and G.H. Al-Gaphari. A new cryptography scheme based on laplace transform and a substitution-permutation network. *International Journal of Advanced Trends in Computer Science and Engineering*, 10(4):2658–2663, 2021.
10. A.A. Pranajaya and I. Sugiarto. Simulation and analysis on cryptography by maclaurin series and laplace transform. *IAENG International Journal of Applied Mathematics*, 52(2):441, 2022.
11. B.A. Sharba, R.R. Al-Khalidy, and R.I. Hussein. A new approach of cryptography using taylor series of logarithm function. *Journal of Discrete Mathematical Sciences and Cryptography*, 26(7):1889–1895, 2023.
12. M. Rasool and K.R. Mohan. A cryptographic technique applying laplace transform and exponetial function. *Southeast Europe Journal of Soft Computing*, 12(2):10–14, 2023.
13. A.A. Abidalzahra. *Designing Secure Public Key Cryptosystem Based on NTRU and DNA*. M.sc. thesis, University of Al-Qadisiyah, Iraq, 2024.

14. F.H. Albakaa 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):83–386, 2025.

15. A.P. Hiwarekar. A new method of cryptography using laplace transform of hyperbolic functions. *International Journal of Mathematical Archive*, 4(2):208–213, 2013.

16. B. Brunel. *Implementation of NTRU for Constrained Devices*. M.sc. thesis, Catholic University of Leuven, 2008.

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