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

(3s.) **v. 2026 (44) 5** : 1–4.
ISSN-0037-8712
doi:10.5269/bspm.80983

DNA and MAL-eleven Algebra to Design an Efficient Encryption Cryptosystem

Mariam Yosef Almustafa, Basel Hamdo Alarnous and Hassan Rashed Yassein*

ABSTRACT: In this paper, we present an innovative encryption method based on DNA and MAL-eleven algebra, where both are used to generate public and private keys.This method provides a high level of security by enhancing key confidentiality and ensuring the protection of the original message from any potential threat.

Keywords: DNA, MAL-eleven algebra, security analysis.

Contents

1. Introduction

DNA encryption is one of the most prominent modern innovations in the field of encryption, due to its unique characteristics, most notably its superior ability to store huge amounts of data, in addition to the random nature of the sequence of nitrogenous bases that make it up. In 1994, Adelman demonstrated the use of DNA for computational purposes, paving the way for the improvement of bio-computing [1]. In 2000, Banzhaf et al. [2] proposed two different coding methods via double- stranded DNA series, where binary information is encoded and hidden within DNA strands for secure data storage. DNA cryptography has since gained wide attention due to its unique characteristics, including the ability to store vast amounts of data and the inherent randomness of nitrogenous base sequences. The combination of DNA computing theories with cryptographic principles offers a highly promising direction in research [3,4]. In 2011, Yunpeng and others introduced a symmetric encryption via DNA techniques, utilizing string indexing and block cipher methods to encode messages into DNA sequences [5].

In 2015, UbaidurRahman et al. [6] proposed a novel encryption and decryption algorithm used DNA computing, leveraging the unique characteristics of molecular biology to enhance cryptographic security. In 2019, Barman and Banani [7] introduced a system combining DNA encoding with elliptic curve cryptography (ECC), utilizing modern biological techniques in the design. In 2024, Abidalzahra introduced PDNA via polynomial and DNA codon [8]. In 2025, Albakaa and Yassein relied on truncated polynomials ring and DNA codons to propose the FDNA cryptosystem [9].

2. The Proposed MDNA Cryptosystem

In this section, we present the MDNA system, a multidimensional coding system based on the MAL-eleven algebra [10] with deoxyribonucleic acid (DNA). The following is a description of how the proposed system works:

* Corresponding author.
2020 *Mathematics Subject Classification:* 11T71, 92D20.
Submitted December 22, 2025. Published February 14, 2026

2.1. Key Generation

The recipient randomly selects two polynomials $f, g \in M_{ae}$ as private keys, such that f has d_f coefficient equal 1 and a $d_f - 1$ coefficient equal -1 with the remainder being zeros. Similarly, g has d_g coefficient equal 1 and a $d_g - 1$ coefficient equal -1 with the remainder being zeros. Both f, g have inverses of measure p, denoted as f_p^{-1} and g_p^{-1} respectively. The recipient then calculates the public key $H = f_p^{-1} * g_p^{-1}$. Finally, the recipient selects the key χ which is a DNA sequence obtained from databases at international centers specializing in genetic engineering. These databases can also be accessed online (e.g., GENBANK, EMBL, NCBL).

Then it creates a set of encoding tables as shown in the following Tables 1-3.

Table 1: Encoding plaintext characters into codons according to their position.

Codon	Even position	codon	Even position	codon	odd position	codon	odd position
TCT	N	TTG	A	TTA	n	TTC	a
TAT	O	TCG	B	TCA	o	TCC	b
TGG	P	TGC	C	TGT	p	TAC	c
CTG	Q	CTA	D	CTC	q	CTT	d
CAT	R	CGG	E	CCA	r	CCT	e
CGT	S	CAG	F	CAA	s	CAC	f
ATT	T	CGG	G	CGA	t	CGC	g
ACT	U	ATG	H	ATA	u	ATC	h
AAT	V	ACG	I	ACA	v	ACC	i
AGC	W	AGT	J	AAG	w	AAC	j
GTC	X	GTT	K	AGG	x	AGA	k
GCC	Y	GCA	L	GTG	y	GTA	l
GAC	Z	GAT	M	GCG	z	GCA	m

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

The English letter code for the two bases	DNA sequence agreed upon by both parties	A DNA strand generated from plaintext encoding	The English letter code for the two bases	DNA sequence agreed upon by both parties	A DNA strand generated from plaintext encoding
A	T	D	T	T	B
A	G	I	T	G	H
A	A	R	T	A	K
A	C	P	T	C	M
C	T	X	G	T	S
C	G	W	G	G	V
C	A	Z	G	A	Y
C	C	F	G	C	E

Table 3: Coding of nitrogenous bases in the binary system.

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

2.2. Encryption

The sender calculates the ciphertext as follows:

1. Convert the message M into codons according to Table 1. Using the DNA strand chosen during the key generation stage and denoted by the symbol χ they obtain the English letters according to Table 2.
2. Convert the English letters into a binary system sequence according to their alphabetical order.
3. Convert the binary number sequence into a polynomial called $\Phi \in M_{ae}$.
4. Use the public key H to obtain the formula $C = H * \Phi \ (mod\ p)$.
5. Convert C into a binary system sequence.
6. Convert the resulting binary system sequence from the previous step into a sequence of nitrogenous bases according to Table 3. This sequence represents the ciphertext E.

2.3. Decryption

After the receiver receives the ciphertext E, it performs the following steps to access the message M:

1. Converts the sequence of nitrogenous bases into a binary sequence according to Table 3.
2. Converts the binary sequence into a polynomial B.
3. Computes $D = f * g * \mathcal{B}$.
4. Converts D back into a binary sequence.
5. Converts the binary sequence into letters according to their alphabetical order. Using the key χ with the letter sequence, it obtains a sequence of codons according to Table 2.
6. Converts the codons back into English letters to obtain the message M according to Table 1.

3. Security of the Proposed MDNA System

The security of the MDNA encryption system depends on:

1. The key χ which is represented by codons and has a length of n. Since there are only four letters in DNA (T, C, G, and A), the sample space for this key is 4^n.
2. Polynomials g, f where the sample space for each is:

$$\left(\frac{N!}{d_f!\,(d_f-1)!\,(N-2d_f+1)!}\right)^{11}, \left(\frac{N!}{d_g!\,(d_g-1)!\,(N-2d_g+1)!}\right)^{11} \text{ respectively.}$$

An attacker who wants to access message M must search for the key χ along with one of the keys f or g, because if they obtain f, they can access g, and vice versa. Therefore, the overall system security level is:

$$4^n \left(\frac{N!}{d_f!\,(d_f-1)!\,(N-2d_f+1)!}\right)^{11}$$

or

$$4^n \left(\frac{N!}{d_g!\,(d_g-1)!\,(N-2d_g+1)!}\right)^{11}$$

4. Conclusions

Encryption methods that rely on combining multiple mathematical structures are more efficient. Here, two structures were used: one mathematical (binary algebra) and the other biological (DNA) in all stages of building the proposed encryption method. This significantly increased its security level, making it a popular method for many applications that focus on securely transmitting data, protecting it from hackers.

References

1. Leonard M. Adleman. Molecular computation of solutions to combinatorial problem. *Science*, 266(5187):1021–1024, 1994.
2. Wolfgang Banzhaf, H. Rauhe, and C. Richter. Cryptography with DNA binary strands. *BioSystems*, 57:13–22, 2000.
3. J. Chen. DNA-based biomolecular cryptography design. In *Proceedings of the 2003 International Symposium on Circuits and Systems (ISCAS'03)*, volume 3, Bangkok, Thailand, May 2003. IEEE.
4. G. Z. Cui, Y. Liu, and X. Zhang. New direction of data storage: DNA molecular storage technology. *Computer Engineering and Applications*, 42(26):29–32, 2006.
5. Y. Zhang, Z. Yu, W. Zhong, and Richard O. Sinnott. Index-based symmetric DNA encryption algorithm. In *Proceedings of the 4th International Congress on Image and Signal Processing (CISP)*, Shanghai, China, 2011. IEEE.
6. N. H. Ubaidur Rahman, C. Balamurugan, and R. Mariappan. A novel DNA computing-based encryption and decryption algorithm. *Procedia Computer Science*, 46:463–475, 2015.
7. P. Barman and B. Saha. DNA encoded elliptic curve cryptography system for IoT security. *International Journal of Computational Intelligence*, 2:7, 2019.
8. A. A. Abidalzahra. *Designing Secure Public Key Cryptosystem Based on NTRU and DNA*. M.sc. thesis, University of Al-Qadisiyah, Al-Qadisiyah, Iraq, 2024.
9. 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):383–386, 2025.
10. M. Y. Almustafa, B. H. Alarnous, and H. R. Yassein. ELTRU: Development of NTRU via newly eleventh-dimensional algebra. *Bol. Soc. Paran. Mat.*, 43(3s):1–7, 2025.

Mariam Yosef Almustafa,
Department of Mathematics,
College of Science, Homs University,
Syria.
E-mail address: mariamalmustafa588@gmail.com

and

Basel Hamdo Alarnous,
Department of Mathematics,
College of Science, Homs University,
Syria.
E-mail address: barnous@homs-univ.edu.sy

and

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