Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 5, pp. 1895–1901
DOI : 10.47974/JDMSC-2350

Hybrid secure encryption scheme via polynomials ring and DNA

Atwar Ahmed Abboodi *
Ameera Nema Alkiffai †
Department of Mathematics
Faculty of Education for Women
University of Kufa
Kufa
Iraq

Hassan Rashed Yassein §
Department of Mathematics
College of Education
University of Al-Qadisiyah
Al-Diwaniyah 58001
Al-Qadisiyah
Iraq

Abstract

In this study, a novel encryption system is proposed that uses four nucleotide bases instead three in the original system DNA, which provides a high secure that helps to protect the data from surges and makes it suitable for many information that require high secure when transmitted through in unsecure conductive medium due to the significant randomness resulting from the increased number of bases in DNA.

Subject Classification: *11T71, 92D20.*

Keywords: *Polynomials ring, DNA, PDNA, Security analysis.*

1. Introduction

The discovery of DNA revolutionized medicine, genetic engineering, crime detection and analysis, identification, and massive data storage instead of disks. Researchers interested in cryptography have also worked with this

* *E-mail:* **Atwara.alkoofee@student.uokufa.edu.iq (Corresponding Author)**
† *E-mail:* **ameeran.alkiffai@uokufa.edu.iq**
§ *E-mail:* **hassan.yaseen@qu.edu.iq**

structure to encrypted data. We will review several studies that present DNA-based data encryption methods. The authors in [1] presented the first use of DNA for computational operations, which paved the way for extensive research in this field. The authors in [2] introduced an index-based symmetric DNA cryptosystem via an index of a block cipher and a string to encode a message [2]. A technology for storing data inside DNA was developed in 2012 [3]. In 2017, a more efficient model was proposed, emphasizing the use of DNA technology to improve data storage and retrieval efficiency [4]. In 2018, further work focused on increasing the complexity of DNA sequencing [5]. After two years, a new mRNA-based S-box was introduced, generating the required number of boxes using a secret key [6]. Comparative studies between asymmetric and symmetric DNA cryptosystems were also conducted [7]. Additionally, a DNA cryptosystem integrated with the NTRU system was proposed to enhance security [8]. In 2025, a PDNA encryption system based on coding theory and polynomials was introduced [9]. In 2020, an FDNA encryption scheme with high security was proposed, utilizing DNA and a truncated polynomial ring [10]. Furthermore, several encryption systems have been developed based on specific mathematical structures [11].

2. PDNA Cryptosystem

Deoxyribonucleic acid (DNA) is made up of small units is said nucleotide. A nucleotide consists of three parts: nitrogenous bases, a five-carbon sugar, and a phosphate acid. Each set of three nitrogenous bases is called a codon [9]. The PDNA based on the truncated polynomials ring $\mathcal{T} = Z[x] / (x^N - 1)$ = {polynomials of degree $N-1$ with coefficients of integer}, subset $\ell_{\mathfrak{f}}$ ={ $\mathfrak{f} \in \mathcal{T} \setminus \mathfrak{f}$ has $d_{\mathfrak{f}}$, and $d_{\mathfrak{f}}$ -1 coefficients equal positive one, and negative one, respectively, and equal zero to the others, $\ell_{\mathfrak{g}}$ = { $\mathfrak{g} \in \mathcal{T} \setminus \mathfrak{g}$ has $d_{\mathfrak{g}}$, and $d_{\mathfrak{g}}$ -1, coefficients equal positive one, and negative one, respectively, and zero to the other, and one public key and two private keys. The security of PDNA on one polynomial and the standard DNA strand.

3. Suggested Method

Assume that every four nitrogenous bases form a codon, which is the basis for building the new encryption method, since there are four nucleotides that make up DNA (there are 256 different codons, as shown in the following Table 1, allowing all keyboard symbols to be covered in comparison of the DNA and PDNA methods. Also, Tables 2, 3, and 4 are created for use in the system phases.

Table 1

Shows the process of encoding the four codons.

First rule		Second rule				Third rule	Four rule
		T	C	Λ	G		
	T	TTTT	TCTT	TΛTT	TGTT	T	T
		TTTC	TCTC	TΛTC	TGTC	C	C
		TTTΛ	TCTΛ	TΛTΛ	TGTΛ	Λ	Λ
		TTTG	TCTG	TΛTG	TGTG	G	G
		TTCT	TCCT	TΛCT	TGCT		
		TTCC	TCCC	TΛCC	TGCC		
		TTCΛ	TCCΛ	TΛCΛ	TGCΛ		
		TTCG	TCCG	TΛCG	TGCG		
		TTΛT	TCΛT	TΛΛT	TGΛT		
		TTΛC	TCΛC	TΛΛC	TGΛC		
		TTΛΛ	TCΛΛ	TΛΛΛ	TGΛΛ		
		TTΛG	TCΛG	TΛΛG	TGΛG		
		TTGT	TCGT	TΛGT	TGGT		
		TTGC	TCGC	TΛGC	TGGC		
		TTGΛ	TCGΛ	TΛGΛ	TGGΛ		
		TTGG	TCGG	TΛGG	TGGG		
	C	CTTT	CCTT	CΛTT	CGTT	T	T
		CTTC	CCTC	CΛTC	CGTC	C	C
		CTTΛ	CCTΛ	CΛTΛ	CGTΛ	Λ	Λ
		CTTG	CCTG	CΛTG	CGTG	G	G
		CTCT	CCCT	CΛCT	CGCT		
		CTCC	CCCC	CΛCC	CGCC		
		CTCΛ	CCCΛ	CΛCΛ	CGCΛ		
		CTCG	CCCG	CΛCG	CGCG		
		CTΛT	CCΛT	CΛΛT	CGΛT		
		CTΛC	CCΛC	CΛΛC	CGΛC		
		CTΛΛ	CCΛΛ	CΛΛΛ	CGΛΛ		
		CTΛG	CCΛG	CΛΛG	CGΛG		
		CTGT	CCGT	CΛGT	CGGT		
		CTGC	CCGC	CΛGC	CGGC		
		CTGΛ	CCGΛ	CΛGΛ	CGGΛ		
		CTGG	CCGG	CΛGG	CGGG		
	Λ	ΛTTT	ΛCTT	ΛΛTT	ΛGTT	T	T
		ΛTTC	ΛCTC	ΛΛTC	ΛGTC	C	C
		ΛTTΛ	ΛCTΛ	ΛΛTΛ	ΛGTΛ	Λ	Λ
		ΛTTG	ΛCTG	ΛΛTG	ΛGTG	G	G
		ΛTCT	ΛCCT	ΛΛCT	ΛGCT		
		ΛTCC	ΛCCC	ΛΛCC	ΛGCC		
		ΛTCΛ	ΛCCΛ	ΛΛCΛ	ΛGCΛ		
		ΛTCG	ΛCCG	ΛΛCG	ΛGCG		
		ΛTΛT	ΛCΛT	ΛΛΛT	ΛGΛT		
		ΛTΛC	ΛCΛC	ΛΛΛC	ΛGΛC		
		ΛTΛΛ	ΛCΛΛ	ΛΛΛΛ	ΛGΛΛ		
		ΛTΛG	ΛCΛG	ΛΛΛG	ΛGΛG		

		ΛTGT ΛTGC ΛTGΛ ΛTGG	ΛCGT ΛCGC ΛCGΛ ΛCGG	ΛΛGT ΛΛGC ΛΛGΛ ΛΛGG	ΛGGT ΛGGC ΛGGΛ ΛGGG			
	G	GTTT GTTC GTTΛ GTTG GTCT GTCC CTCΛ GTCG GTΛT GTΛC GTΛΛ GTΛG GTGT GTGC GTGΛ GTGG	GCTT GCTC GCTΛ GCTG GCCT GCCC GCCΛ GCCG GCΛT GCΛC GCΛΛ GCΛG GCGT GCGC GCGΛ GCGG	GΛTT GΛTC GΛTΛ GΛTG GΛCT GΛCC GΛCΛ GΛCG GΛΛT GΛΛC GΛΛΛ GΛΛG GΛGT GΛGC GΛGΛ GΛGG	GGTT GGTC GGTΛ GGTG GGCT GGCC GGCΛ GGCG GGΛT GGΛC GGΛΛ GGΛG GGGT GGGC GGGΛ GGGG	T C Λ G	T C Λ G	

Table 2

Coding of plaintext characters into codons according to their position.

Odd	Codon	Odd	Codon	Even	Codon	Even	Codon
a	TTTC	n	GTΛC	A	TΛTG	N	GΛCG
b	TCCΛ	o	GTCΛ	B	TGCΛ	O	GCCC
c	ΛΛTG	p	ΛCGΛ	C	ΛGTT	P	ΛGGΛ
d	ΛTCC	q	ΛCCΛ	D	ΛΛCΛ	Q	ΛTTΛ
e	ΛTΛΛ	r	ΛCΛG	E	ΛGΛG	R	ΛΛGΛ
f	GTTC	s	CΛCΛ	F	GΛCC	S	CGCΛ
g	GGΛC	t	CCTG	G	GΛGΛ	T	CTTΛ
h	TCΛC	u	TGΛΛ	H	TΛΛΛ	U	TΛCΛ
i	TGGC	v	TΛGC	I	TCGG	V	TTGG
j	CCΛT	w	TTΛC	J	CΛGC	W	TTCC
k	CGGT	x	CΛΛΛ	K	CGΛC	X	CCCΛ
l	ΛTGG	y	CCGT	L	ΛΛΛΛ	Y	CTGC
m	ΛCTΛ	z	CTCΛ	M	ΛGCΛ	Z	CTΛΛ

For example, a in the word (are) is odd because the sequence of a in the word (are) is odd, r is even because its sequence is even, and e is odd.

Table 3

The 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	Λ	D
G	T	H	G	Λ	I
Λ	T	K	Λ	Λ	R
C	T	M	C	Λ	P
T	G	S	T	C	X
G	G	V	G	C	W
Λ	G	Y	Λ	C	Z
C	G	E	C	C	F

Table 4

Coding of nitrogenous bases in the binary system

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

The ATDNA (Atwar DNA) cryptosystem relies on the concept of DNA-based cryptography. The ATDNA encryption system is explained as follows:

3.1 *Key Generation*

Selecting polynomial $\mathbb{f} \in \varphi = Z[x] / x^N - 1$, such that φ is ring of truncated polynomial of degree $N - 1$ with coefficients of integers and has $d_{\mathbb{f}}$, $d_{\mathbb{f}}$ -1 coefficients equal 1, -1, respectively and other values are zero. The polynomial $\mathbb{f}$ should have inverse of multiplicative modulo $\mathcal{P}$ denoted by $\mathbb{f}_{\mathcal{P}}^{-1}$, such that $\mathcal{P}$ and N are positive integer numbers. Selecting a strand of DNA and this information is available in databases at international centers in genetic engineering and studying the functioning of genes, as well as many internet sites (GENBANK, EMBL).

3.2 *Encryption*

In order to encrypt the message M, the sender proceeds with the following steps:

1- The plaintext consists of multiple sequences of English alphabet letters, which include 26 characters, which are encoded into codons according to

Table 2 where each letter is assigned a specific codon based on its position (odd or even) in the text.

2- Using the key in step (2) of the key generation phase with the codons from the last step, we obtain the English letters based on Table 3, these letters are converted into binary form based on their order in the English alphabet.

3- Convert the binary system chain into a polynomial called g, belonging to the φ based on length N. By utilizing the key $\mathbb{f}$ selected during the key generation phase, c is derived using the following formula $c \equiv \mathbb{f} * g \, mod \, \mathcal{P}$. Transform c into the binary system. By Table 4, convert the binary chain to string of nitrogenous which is the ciphertext E.

3.3 *Decryption*

The recipient carries out the following steps to decrypt the message E:

1- With the help of Table 4, transform the nitrogenous base string into a binary chain. Transform the binary chain into a polynomial θ of length N.

2- Compute $\mathcal{A} \equiv \mathbb{f}_{\mathcal{P}}^{-1} * \theta \pmod{\mathcal{P}}$, then convert $\mathcal{A}$ into the binary system chain. Convert the binary system chain into letters based on their sequence in the English alphabet, then convert letters into codons according to Table 3.

3- Convert the codons into message M according to Table 2.

4. Security Analysis

The security of the ATDNA encryption scheme relies on access to the DNA string key and the truncated polynomial key, requiring an attacker to search the edge space f and the DNA string convolutionally (taking each polynomial key with all possible DNA string key probabilities) based on the polynomial degree, nonzero coefficients, and DNA string length, respectively. Furthermore, the fact that each of the four bases contains four characters instead of three edges increases the randomness of this method, making it difficult for an attacker to access the keys, thus providing high security for data transmitted over an insecure medium.

5. Conclusion

In this paper, we present a new method, ATDNA, for data encryption based on DNA sequences and polynomials. This method develops a set of substitution codon tables, providing a higher level of security than DNA-based encryption methods, polynomial-ring-based methods such as NTRU, or hybrid methods that combine polynomial rings and DNA, such as PDNA. This approach is particularly effective against guesswork-based attacks, such as brute-force attacks, because of its random nature. This makes it effective and suitable for many electronic transactions that transmit highly sensitive data that could cause significant damage if viewed by an unauthorized third party.

References

[1] L. M. Adleman, "Molecular computation of solutions to combinatorial problems," *Science*, vol. 266, no. 5187, pp. 1021–1024 (1994).

[2] Y. Yunpeng, Z. Yu, W. Zhong, and R. O. Sinnott, "Index-based symmetric DNA encryption algorithm," in *Proc. 2011 4th Int. Congr. Image Signal Process., IEEE*, vol. 5, pp. 2290–2294 (2011).

[3] G. M. Church, Y. Gao, and S. Kosuri, "Next-generation digital information storage in DNA," *Science*, vol. 337, no. 6102, pp. 1628–1628 (2012).

[4] Y. Erlich and D. Zielinski, "DNA Fountain enables a robust and efficient storage architecture," *Science*, vol. 355, no. 6328, pp. 950–954 (2017).

[5] E. Vidhya and R. Rathipriya, "Two level text data encryption using DNA cryptography," *Int. J. Comput. Intell. Inform.*, vol. 8, no. 3, pp. 106–118 (2018).

[6] 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*, vol. 16, no. 1, pp. 331–348 (2020).

[7] B. T. Hammad, A. M. Sagheer, I. T. Ahmed, and N. Jamil, "A comparative review on symmetric and asymmetric DNA-based cryptography," *Bull. Electr. Eng. Inform.*, vol. 9, no. 6, pp. 2484–2491 (2020).

[8] U. S. D. Satriyo, F. Rahutomo, B. Harjito, and H. Prasetyo, "DNA cryptography based on NTRU cryptosystem to improve security," in *Proc. 2022 IEEE 8th Int. Inf. Technol. Int. Semin. (ITIS)*, Surabaya, Indonesia, pp. 27–31 (Oct. 2022).

[9] F. H. Albakaa and H. R. Yassein, "A New Encryption Scheme Based on DNA and Polynomials with More Security," *Int. J. Math. Comput. Sci.*, vol. 20, pp. 1–14 (2017).

[10] A. Chillali and M. Sahmoudi, "SCC-Cryptosystem on an algebraic closure ring," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 23, no. 8, pp. 1475–1485 (2020).

[11] D. K. Verma, M. Rani, R. K. Tyagi, and B. B. Sagar, "Baptista chaotic cryptosystem based on alternate superior dynamic lookup table," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, no. 8, pp. 1383–1392 (2019).

Received May, 2025