International Journal of Mathematics and Computer Science
Volume **20,** Issue no. 1, (2025), 383–386
DOI: https://doi.org/10.69793/ijmcs/01.2025/albakaa

A New Encryption Scheme Based on DNA and Polynomials with More Security

Fatimah H. Albakaa[1], Hassan Rashed Yassein[2]

[1]Department of Mathematics
Faculty of Education for Women
University of Kufa
Al Najaf, Iraq

[2]Department of Mathematics
College of Education
University of Al-Qadisiyah
Al-Qadisiyah, Iraq

Email: fatema.albakaa@atu.edu.iq, hassan.yaseen@qu.edu.iq

(Received October 20, 2024, Accepted November 22, 2024, Published November 23, 2024)

Abstract

In this paper, we develop a new method of encryption, using DNA and polynomials as public and private keys, which gives a very high level of security for both the private keys and the original message.

1 Introduction

It is known that one gram of DNA stores about 10 terabytes, as its ability to store information exceeds all known storage methods (electrical, optical, magnetic) [1]. DNA encryption is applied in information security and storage. Encryption carries and hides information and transmits data from one party to another. In 1999, Jehani et al. [2] proposed the idea of creating an encryption system based on DNA molecules. In 2011, Yunpeng et al.

Key words and phrases: DNA, polynomials, security level.
AMS (MOS) Subject Classifications: 94A60, 68P25.
ISSN 1814-0432, 2025, https://future-in-tech.net

proposed a symmetric cryptosystem based on the DNA cryptosystem [3]. In 2022, Rahutomo et al. introduced the DNA encryption system integrated with the NTRU encryption system to enhance the security level [4].

2 FDNA Encryption

The proposed method FDNA can be described in follows:

2.1 Key Generation

First, a truncated polynomial ring $\varphi = Z[x]/(x^N - 1) = \{$polynomial of degree $N-1$ with integer coefficients$\}$ is selected. Next, the recipient randomly chooses two polynomials $f \epsilon l_f$ and $g \epsilon l_g$ where $l_f = \{f \in \varphi | f$ has d_f coefficients equal 1,($d_f - 1$) equal -1, and 0 for other values$\}$, $l_g = \{g \in \varphi | g$ has d_g coefficients equal 1, $(d_g - 1)$ equal -1 and 0 for other values $\}$ as private keys such that a polynomial f should have a multiplicative inverse with modulo p referred to as f_p, where p and N are relatively prime.

After that, the public key $\kappa = f_p * g_p \,(mod\ p)$ is computed. Choosing a private key $\mathcal{X}$ in the form of a DNA sequence from databases in global centers specialized in genetic engineering and websites (GENBANK, EMBL, NCBI) (using Tables 1, 2, and 3 in [5]).

2.2 Encryption

The ciphertext is computed by the sender as follows:
1. According to Table 1, by converting a message $\mathcal{M}$ into codons and using the key $\mathcal{X}$ in Table 2 to get the English letters.
2. Writing the alphabetical sequence of English letters as a series of binary numbers.
3. Converting the binary series obtained from step 2 into a polynomial called $\mathcal{T} \in \varphi$.
4. Using the public key κ to obtain C by the following formula:

$$\mathsf{C} = \kappa * \mathcal{T} \ (\ mod\ p).$$

5. Converting C into a chain of series of binary numbers.
6. Converting the result of step 5 into a string of nitrogenous bases by Table 3 that represents the ciphertext $\mathcal{E}$.

2.3 Decryption

After receiving the ciphertext $\mathcal{E}$ from the recipient, the original message is obtained through the following steps:
1. Converting the string of nitrogenous bases $\mathcal{E}$ into the binary system chain by Table 3.
2. Converting the result of step 1 to polynomial $\mathtt{C}$.
3. Computing $\mathcal{D} = g * f * \mathtt{C}$ ($mod\ p$).
4. Converting the polynomial $\mathcal{D}$ to binary series.
5. Using key $\mathcal{X}$ with English alphabet according Table 2 to getting codons.
6. Using Table 1, converting codons to English letters to get the message m.

3 Security Analysis

The three private keys in the proposed method are:
1) The key $\mathcal{X}$ which is represented by codons and of length n with randomness.
2) The polynomials f and g of degree n with non-zero coefficients that determine the security level.
3) Given that there are only four letters A, C, G, and T in DNA, the key space is 4^n. For keys f and g, their spaces are $\frac{N!}{d_f!(d_f-1)!(N-2d_f+1)!}$ and $\frac{N!}{d_g!(d_g-1)!(N-2d_g+1)!}$.

Therefore, through a brute force attack, the security level is either $4^n\frac{N!}{d_f!(d_f-1)!(N-2d_f+1)!}$ or $4^n\frac{N!}{d_g!(d_g-1)!(N-2d_g+1)!}$.

References

[1] G. Cui, Y. Liu, X. Zhang, New direction of data storage: DNA molecular storage technology, Computer Engineering and Application, **42,** no. 26, (2006), 29–32.

[2] A. Gehani, T. LaBean, J. Reif, DNA-based cryptography, Proceedings pf the 5th DIMACS Workshop on DNA Based Computers, (1999).

[3] Z. Yunpeng, Y. Zhu, W. Zhong, R. O. Sinnott, Index-based symmetric DNA encryption algorithm. In the 2011 4th International Congress on Image and Signal Processing, (2011), 2290–2294.

[4] U.Y. Satriyo, F. Rahutomo, B. Harjito, H. Prasetyo, DNA Cryptography Based on NTRU Cryptosystem to Improve Security. In the 2022 IEEE 8th Information Technology International Seminar, (2022), 27–31.

[5] A.A. Abidulzahra, Designing Secure Public Key Cryptosystems Based on NTRU and DNA, M. Sc. thesis, University of Al-Qadisiyah, Iraq, (2024).