Journal of Theoretical and Applied Information Technology
30th April 2026. Vol.104. No.8

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CRYPTOSYSTEM USING RNA COMBINED WITH DATA SEQUENCE AND AFFINE CIPHER FOR SECURE DATA COMMUNICATION

KAMERAN ALI AMEEN [1], ASO AHMED MAJEED[2], YALMAZ NAJM ALDEEN TAHER[3], YOUSIF MOHAMMED WAHAB [4], KAWA M KAKY[5]

[1,3,4]Computer Science, College of Computer Science and Information Technology, University of Kirkuk, Kirkuk, Iraq
[2]Department of Basic Science, College of Nursing, University of Kirkuk, Kirkuk, Iraq
[5]Al-Nisour University College, Baghdad, Iraq

E-mail: [1]kameran.ameen@uokirkuk.edu.iq,[2]asoalsalihi@uokirkuk.edu.iq, [3]yalmaz.science@uokirkuk.edu.iq, [4]yosfmw@uokirkuk.edu.iq, [5]kawa.mudher@gmail.com

ABSTRACT

The 21st century has experienced an information surge due to rapid technological advancement, rendering knowledge a much more vital strategic asset, particularly when transmitted across insecure means and vulnerable to intrusions. Cryptosystems are commonly employed methods for safeguarding user data from undesirable access over communication networks. Moreover, it is essential to devise cryptographic solutions that are equilibrated in terms of security and efficiency. Bio cryptography is a new and promising cryptographic research area. Besides, Ribonucleic Acid (RNA) cryptography has exhibited considerable effectiveness. Moreover, research indicates that integrating the Affine Cipher with RNA sequence-inspired encoding, which depends on data sequences, is effective. The proposed cryptosystem utilizes an Affine Cipher initially to encrypt the original message through several procedures. The output is subsequently encoded into data sequences by generating a six-bit sequence. Ultimately, it encodes it according to the fundamental Biological RNA sequence. Comparative studies have been performed to validate the efficacy of our concept. The proposed method met the security requirements and showed the capability to counter many security threats. The results indicate that our method surpasses its alternative in terms of time and complexity, thereby meeting the majority of security objectives while ensuring high levels of privacy, security, and a respectable IC. It is also robust against certain recognized attacks. Moreover, the proposed algorithm yields faster execution times and enhanced performance relative to other algorithms during the encryption and decryption of 24B and 27B texts.
Keywords: *Affine Cipher, XOR operation, Data Sequence, RNA Sequence, Cryptography, Security*.

1. INTRODUCTION

The rapid and quick development and advancement in the specialized field of information technology, which includes the use of computers, software, and telecommunications, in recent years has made it possible for people to communicate, connect, and interact with each other in an easy, smooth, and effortless manner, without much difficulty or effort, and in a manner that is free from restrictions. This ability to communicate has become vital in our daily lives and activities. One of the primary ways this interaction occurs is through the exchange of information, such as data, messages, or knowledge, and visual representations like pictures, between individuals or groups over various network channels, which are pathways or communication links used to transmit data. However, these network channels or communication pathways can sometimes be unreliable, meaning they might not always be consistent, stable, or secure and could experience issues like interruptions, data loss, or unauthorized access. This results from the major security risks hackers create on channels of communication [1] [2]. On the other hand, the topic of genetics is currently undergoing extensive research because of its applicability in a variety of sectors, particularly in the realm of information security [3] [4]. In addition to its application in the dissemination and transmission of data via communication networks. This data is liable to alteration and modification. Consequently,

academics are attempting to discover novel ways and algorithms to enhance communication security. They are endeavoring to mitigate various vulnerabilities in the network environment to safeguard information from intruders [1] [3] [5].

Scientific research has shown that ribonucleic acid (RNA) possesses a wide range of versatile and impactful applications within the field of nanotechnology. Beyond its well-known biological role, RNA is being increasingly utilized in the development of nanoscale devices due to its unique structural properties and ability to fold into complex shapes. Furthermore, RNA has also found promising use in the emerging area of optical computing, where it plays a part in systems that use light rather than electrical signals to perform data processing tasks. In addition to these innovative applications, RNA is being explored as a tool for data encryption, secure information storage, reliable transmission of digital data, and even in the execution of complex. computational processes. These capabilities highlight RNA's potential in fields beyond biology, bridging the gap between molecular biology and information technology. As the global volume of data continues to grow at an unprecedented rate spanning scientific, commercial, and personal domains the ability to effectively manage, analyze, and interpret this vast sea of information has become increasingly essential. Automated data analysis systems are now considered highly valuable, providing insights that support decision-making across various sectors. Consequently, these advancements have heightened the importance of information security. The safeguarding data from unauthorized access, corruption, or loss is now a critical priority, and the use of novel molecular tools like RNA could play a pivotal role in developing future security technologies [6] [7] [8]. So, the primary purpose of RNA encryption in security is to ensure the best possible degree of secrecy, integrity, and authenticity while transmitting data across a network and to safeguard it from brute-force attacks [3] [9] [7].

Cryptography is a specialized technique and set of methods used for transforming, converting, or encoding data from its original, understandable form, known as plaintext, into an encrypted and unintelligible form called cipher text, which can only be read, understood, or accessed by individuals or parties who have the proper authorization, permissions, or cryptographic keys. After the encrypted data, or cipher text, reaches its intended destination or recipient, cryptography also involves decrypting or decoding this cipher text back into its original, readable form, known as plaintext, so that the authorized recipient can understand and use the information securely [10]. And, researchers have used a variety of methods and procedures to keep information safe. These include cryptographic methods, chaotic methods, RNA and DNA sequences, and hybrid encryption systems, among others. As a result, data may be changed and amended without the usage of these techniques [11] [12] [13]. The rest of this paper is structured as follows. Section 2 describes the RNA. In section 3, we provide essential information about the related works. Section 4 introduces our proposed technique. Section 5 presents an example of implementing the technique. In section 6, we evaluate our technique's security robustness via a series of experiments and comparisons. Finally, in section 7, we conclude by summarizing this paper's findings.

2. LITERATURE REVIEW

Bioinformatics refers to the application of computer-based techniques and algorithms to analyze and interpret complex biological information. This includes working with molecules such as ribonucleic acid (commonly abbreviated as RNA), across various fields within computer science such as data analysis, algorithm development, and machine learning. One important genetic component, the RNA sequence, is a linear molecule composed of smaller units known as ribonucleotides. These ribonucleotides are chemically bonded together through strong covalent bonds called phosphodiester linkages, forming the backbone of the RNA strand [14] [15]. Furthermore, it consistently exists as a single-stranded molecule. RNA consists of four bases: adenine (A), cytosine (C), guanine (G), and uracil (U). Each nucleotide will assume a binary value as outlined in Table 1 [16] [17] [18] [19].

Table 1: The RNA Representation of Bit Values

RNA sequences	Bit 1	Bit 2
Adenine (A)	0	0
Cytosine(C)	0	1
Guanine(G)	1	0
Uracil (U)	1	1

A data sequence refers to an ordered collection of data elements that forms a core or essential type of data structure in the field of computer science. This concept is widely employed in modern cryptographic frameworks and systems to facilitate secure data transmission and processing. Examples of data sequences encompass various forms of structured data, such as plain text documents, queue-

based structures for task management, stack-based structures for memory operations, and character strings used for textual information. These sequences can be represented as ordered streams or lists consisting of alphabetic characters (letters), numerical values such as real numbers or binary digits (0s and 1s), sequences of discrete events, and other similar ordered entities. That is arranged coherently. It may represent a diverse array of information. Data sequences are a primary category of biological data; for instance, RNA, DNA, and proteins are sequences of nucleotides or amino acids [20] [21] [22]. The sequence involves a special name for the two ends. Sequences have several styles, such as empty objects as one object [a] , more objects [a, b, c], or[$a_0, a_1, \ldots, a_n$]. In addition, it writes in a row similar ($x_1, x_2, \ldots, x_n$) [20] [22]. Moreover, The evolution of bio-cryptography has expanded to address the resource constraints of modern networks, such as the Internet of Things (IoT). Khan et al. recently proposed 'RNA-Trans Crypt,' a novel scheme that successfully integrates the bio cryptographic properties of RNA encoding with the unpredictability of chaos theory. Their work demonstrates that combining RNA sequences with transformative substitution techniques can yield highly secure, lightweight encryption models with optimal execution time [23].

The affine cipher is classified as a type of classical mono alphabetic substitution cipher utilized within cryptographic systems [24]. The cipher text is generated from the original text by mapping each alphabetic character to its respective numeric value. This value undergoes encryption through a modular arithmetic procedure, after which it is converted back into a letter. The employed formula indicates that each character in the text is substituted with a different character. The encryption process is outlined by Equation 2, while Equation 3 outlines the decryption process [25] [26].

Where: y_E is cipher text. y_D is plain text. x is the numerical value of the original letter. (a and b) are integer numbers (keys) of the cipher. p is the size of the number of letters (alphabet). Moreover, a must be a relatively prime value with p, or in other words, (a, p) =1 for congruence to be expressed in its inverse [25] [26] [27].

In [28] Rashid developed a secure text encryption scheme that leverages the central dogma of molecular biology. By sequentially converting plaintext into binary, DNA, RNA, and ultimately amino acid sequences, the proposed framework creates a highly complex ciphertext. Performance evaluations indicated that this multi-stage biological encoding yields fast execution times, making it a highly effective procedure for secure data transfer.

[29] A novel encryption scheme has been presented, comprising two steps. The encryption process has six stages. Initially, the original text is transformed into its corresponding ASCII representation and subsequently turned into binary integers. Subsequently, binary numbers are transformed into their corresponding complementary DNA sequences. Subsequently, they are transformed into RNA sequences. Ultimately, the RNA sequences are transmuted into amino acids, regarded as the ciphertext transmitted to the recipient. The decryption phase has six steps, the same in number to the encryption steps, executed in reverse order. The efficacy of the suggested approach is assessed by the measurement of encryption and decryption durations. The results indicated that they are efficient and rapid, as well as effective in enhancing data security during transfers between parties.

In [30], A novel message encryption method for wireless networks is suggested by integrating the Knapsack algorithm with the Diffie-Hellman (DH) approach. The suggested solution incorporates a shared key generated via the DH algorithm to secure access to the plaintext. Subsequently, each node authenticates one another using the message authentication code (MAC). The concept permits regular updates of the shared key for all nodes to prevent the compromise of certain nodes. Consequently, it guarantees that the message is sent just by legitimate nodes. The analytical results indicate that the plan effectively achieves certain security objectives by offering enhanced privacy and security. It is also impervious to some recognized attacks.

In [31] A novel hybrid encryption technique has been introduced, integrating the concepts of the Caesar cipher and DNA encryption while preserving their functionality and classification. The message is first encrypted with the Caesar cipher. Subsequently, k bits are added to the messages. The result of the preceding step is encrypted using DNA bases. The proposed solution is more secure than several alternative strategies. Accessing the plaintext is a challenge for hackers, and it demonstrates resilience against certain assaults. Consequently, it guarantees the integrity and secrecy of data throughout transmission.

[32] Proposed a unique RNA-based encryption system uses pixel depth to encode the RNA

sequence, serving as a potential solution for secure communication among users. This approach utilizes characteristics of RNA sequences that their complementary sequences transform into certain forms. This process involves the conversion of complementary RNA sequences into specific forms. Subsequently, it assigns a pixel value to each nucleotide in the RNA sequence. Subsequently, employ the pixel depth of these values to encode the message. The original message can only be retrieved via a complementary RNA sequence. The proposal is vulnerable to active attacks such as replay and repudiation.

[33] A scheme is put forth that guarantees compression and a sufficient degree of protection for secret data before transmission. The suggested approach utilizes specially constructed keys to enhance security using the Move-To-Front Transform (MTF) for compression and employs RNA coding with the MTF encoding methodology to ensure sufficient security. The primary purpose of specifically constructing these keys is to safeguard them against unauthorized users' guesses. The security of the suggested technique is robust due to the substantial probability associated with certain keys. The suggested scheme contribution is encrypting the plaintext with an Affine Cipher before encoding the output into data sequences using a six-bit sequence. Finally, it encodes it using the fundamental Biological RNA sequence, by using any data type through two keys based on the RNA sequence to get secure Message exchange.

3. THE PROPOSED SCHEME

The proposed cryptographic scheme is systematically divided into two main operational phases. The first phase involves the encryption of the message, during which the original data or plaintext is transformed into an unreadable or encoded format known as ciphertext. This process ensures that the information remains secure and inaccessible to unauthorized parties while in transit or storage. The second phase focuses on the decryption of the message, in which the previously encrypted data is converted back into its original, readable form. This allows the intended recipient, who possesses the correct decryption key or method, to access and understand the original message content. In the subsequent subsections, a comprehensive and detailed explanation of each of these two phases encryption and decryption is provided. This includes a step-by-step breakdown of the procedures, algorithms, and techniques utilized in each stage to achieve secure communication. In the beginning, the data sequence will be created, which encompasses six-bit binary numbers that are used in the encryption and decryption process, and this is done by following some of the following steps:

1. A sequence consists of R x W.
2. Alter each element of the sequence in base 6. W is the number of binary values, like R = 36 and W = 6 bits. 4. and it can be denoted as a matrix named M_{RW} [36 x 6] [16] [17] as shown in the Table 2.

3.1 Encryption Message Phase

This section is situated on the sender's side. It comprises three processes: Affine Cipher Encryption, Application of Data Sequence, and XOR logical operation, and Application of RNA Cryptography, explained as follows:

1. Each S_i and R_i select (a, b), where S is the sender, R is the receiver, and (a, b) are secret keys, $i \geq 1 \ni z$.
2. S_i picks p, where $p \ni z, 0 \leq p \geq SA$, p the plaintext value, and SA is plaintext alphabetic according to the Table 3.
3. Apply $y_E = \big((a.x) + b\big) \, mod \, p$ for each alphabet.
4. f= Converts y_E to data sequence according to the Table 2.
5. $d_j = f_j \oplus k$, where k is a secret consisting of random 6 bits,$\oplus$ is an XOR operation, j is the order of the alphabet.
6. h=CRH($d_1||d_2||d_3||...||d_n$) where CRS is Circular Right Shift by one and n is an integer number, || is the concatenation operation.
7. w= convert each 2 bits of h to $RNA_{sequence}$ according to theTable 1.
8. q=convert w to $RNA_{complement}$ according to Table 5.
9. x= convert q to digits according to Table 3.
10. m = convert each digit to five binary bits.
11. $c=m||k$, where c is the cipher message sent to R_i.

The table below (Table 5) demonstrates the encryption steps. In addition, the result of plaintext (go) after applying encryption steps, as clarified in the 3.1 will be a series of binary bits (010110000000000010010110000110010110010101).

***Table 4**: Complement of RNA*

$RNA_{sequence}$	$RNA_{complement}$
A	U
C	G
G	C
U	A

3.2 Decryption Message Phase

In this section, which is located on the other side (R_i) future, the application includes several procedures to obtain the original text by following the following steps.

1. Firstly, c'=separate *k* from c, where *k* is the secret random key.
2. m' = convert the rest of *c* (each five binary bits to digits).
3. *x'* =convert *m'* to digits according to Table 3.
4. q' = convert x'to $RNA_{complement}$ according to theTable5.
5. w' = convert each 2 bits of w' to $RNA_{sequence}$ according to Table 1.
6. h' = CLH($w_1||w_2||w_3||\ldots||w_n$) where LRS is Circular Left Shift by one and n is an integer number, || is the concatenation operation.
7. $d_j = w_j \oplus k$, where *k* is a secret consisting of random 6 bits,⊕ is an XOR operation, *j* is the order of the alphabet.
8. *f'*= convert dj to data sequence according to the Table 2.
9. Apply $yE = ((a.x) + b) \mod p$.
10. Finally, convert each value to alphabetical according to the Table 3.

4. EXECUTION AND ANALYSIS OF THE PROPOSED METHOD

The proposed scheme is simulated on a PC equipped with an Intel(R) Core (TM) i3-2328M CPU @ 2.20GHz processor, 8.00 GB of RAM, and a 64-bit Windows 10 Ultimate operating system, using the C# programming language. The performance analysis of our proposed scheme is based on various aspects, including security requirements and potential attacks, followed by a comparison with other schemes. Moreover, Figure 1 is the result of executing the proposed scheme, whose steps are explicated in 3.1.

4.1 Updating 6-bit Key Value

In order to enhance the overall effectiveness and operational efficiency of the proposed system, while simultaneously minimizing the potential risk of malicious attacks or unauthorized access attempts, it is crucial to periodically modify the cryptographic key, which in this case is represented by a six-bit binary value. This key is systematically refreshed at regular intervals, which are predetermined and mutually agreed upon by the involved parties. Furthermore, the validity period of each key is deliberately kept very short significantly shorter than the estimated amount of time an attacker would require to successfully carry out a brute-force or similar type of attack. This strategy ensures that any attempt to compromise the key within its limited active timeframe becomes impractical and ineffective, thereby strengthening the system's overall security.

4.2 Two Cryptosystems Used

The encryption in this proposal uses two keys. The first is a predefined key in the Affine Cipher, which costs less. The second key is when applying XOR, which can be updated continuously. Thus, this increases the security strength.

4.3 Index of Coincidence (IC)

The proposed cryptosystem uses RNA sequencing and the affine cipher, after measuring it by the index of coincidence (IC) with different lengths, showing its robustness as shown in theTable 6.

4.4 Proposed Execution Time

The results show the performance of the proposed method and measure it by analyzing the encryption and decryption time of the original text. The encryption and decryption time is calculated using two file sizes. Therefore, the proposed algorithm was compared in terms of its performance with other algorithms as shown in Table 7, figures 1 and 2 which shows the proposal scheme is better than [31] and [34] in term of time for (24B,27B) text size in encryption and decryption. Finally, as shown in Table 8; The proposed scheme is compared with other algorithms in terms of the number of approaches: results to given high level of security and fast execution compared with other algorithms.

4. CONCLUSION

Prior to transmitting sensitive data and communication signals across a computer or digital network, the information is encrypted to ensure that unauthorized users, such as malicious attackers or eavesdroppers, are unable to access, interpret, or tamper with the content. Encryption serves as a fundamental mechanism for preserving data integrity, ensuring confidentiality, and verifying the authenticity of the information being transmitted. In this study, a novel hybrid encryption technique is proposed, which integrates the classical affine cipher with an innovative encryption scheme inspired by biological RNA data sequences. The encryption process begins by transforming the original message using standard encryption methods, after which the resulting cipher text is further processed through a series of affine encryption operations. The final encrypted output is structured as a six-bit binary data

sequence, which is encoded based on patterns derived from biological RNA sequences drawing parallels between molecular biology and cryptographic encoding. To evaluate the effectiveness of this proposed method, it was systematically compared with existing encryption techniques and rigorously analyzed in terms of its ability to meet essential security requirements and resist various types of cryptographic attacks. The findings demonstrate that the proposed hybrid approach not only satisfies key criteria for security and authentication but also achieves superior performance in ensuring the secure transmission of data across networks.

REFERENCES

[1] A A Majeed, B A Mahmood, A C Shakir, "A secure and energy saving protocol for wireless sensor networks," *Bulletin of Electrical Engineering and Informatics,* vol. 10, no. 6, pp. 3353-3360, 2021.

[2] K. Vinayakan, V. Alamelu Mangayarkarasi, Dr. A. Dinesh Kumar, M. Vasuki, R. Jayakumar, "End-to-end secure communication in for wireless multimedia sensor networks via modified gorilla troops optimizer driven data compression with encryption approach," *Journal of Theoretical and Applied Information Technology,* vol. 104, no. 4, pp. 51-68, 2026.

[3] D S Phanindra, K V Rao and PVGD P Reddy, "Cryptography and Reference Sequence Based DNA/RNA Sequence Compression Algorithms," *Ingenierie des Systemes d'Information,* vol. 27, no. 3, p. 509, 2022.

[4] J Rodríguez, B Corredor and C Suárez, "Genetic operators applied to symmetric cryptography," *International Journal of Interactive Multimedia and Artificial Intelligence,* vol. 5, no. 7, p. 2019, 39-49.

[5] C N Ganesh, G Mamatha, V Veeraiah , V R Roy , A Adgaonkar , S S Ajagekar , A Gupta, P A Madhukar, "Privacy-Preserving Customer Data Management Using Hybrid Ai-Cryptography Models," *Journal of Theoretical and Applied Information Technology,* vol. 104, no. 4, pp. 389-405, 2026.

[6] S O Obado, M P Rout and M C Field, "Sending the message: specialized RNA export mechanisms in trypanosomes," *Trends in parasitology,* vol. 38, no. 10, pp. 854-867, 2022.

[7] Q Q Thabit, A A Al-Saffar and I A Abed, "A new DNA strand-based encryption algorithm using symmetric key generation table," *Al-Qadisiyah Journal for Engineering Sciences,* vol. 15, no. 1, pp. 32-37, 2022.

[8] D Midhunchakkaravarthy , G M Nagamani, V L Narayana, "Quantitative Benchmarking And Cross-Modal Analysis Of Deep Learning, Machine Learning, And Biosensor Frameworks For Early Colorectal Cancer Diagnosis And Prognosis," *Journal of Theoretical and Applied Information Technology ,* vol. 103, no. 18, pp. 7544-7564, 2025.

[9] F A H E Mohamed, W El-Shafai, H M. A. Elkamchouchi, A ELfahar; A Alarifi, M Amoon, "A cancelable biometric security framework based on RNA encryption and genetic algorithms," *IEEE Access,* vol. 10, pp. 55933--55957, 2022.

[10] Supiyanto and S A Mandowen, Advanced hill cipher algorithm for security image data with the involutory key matrix, IOP Publishing, 2021.

[11] R S Devi, ARN Aravind, J C Vishal, D Amritha, K Thenmozhi, JBB Rayappan, A Rengarajan, "Image encryption through RNA approach assisted with neural key sequences," *Multimedia Tools and Applications, springer,* vol. 79, pp. 12093-12124, 2020.

[12] S S Nafea and , M K Ibrahem, "Cryptographic Algorithm based on DNA and RNA Properties," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* vol. 7, no. 11, pp. 804-811, 2018.

[13] V NAMIREDDY , T FATIMA , U GOGATE, L BENNJIMA , R S S R BATTULA , G S KUMAR6, "DNA-Mapped Optical Cryptography For Robust And Efficient IOT Security," *Journal of Theoretical and Applied Information Technology ,* vol. 104, no. 2, pp. 403-413, 2026.

[14] S M Kadhem and D W M Ali, "Proposed Hiding Text in Text Based On RNA for Encoding Secret Information," *Iraqi Journal of Science,* vol. 58, pp. 562-573, 2017.

[15] Wen, Heping and Kang, Shenghao and Wu, Zhuxi and Lin, Yiting and Huang, Yiming, "Dynamic rna coding color image cipher based on chain feedback structure," *Mathematics,* vol. 11, no. 14, p. 3133, 2023.

[16] J. M. Al-Tuwaijari, "Multi-Cipher Technique based on RNA and Chebyschev Map."," *Iraqi*

Journal of Information Technology, vol. 7, no. 1, pp. 114-125, 2015.

[17] A. K. A. Hassan, "Proposed Approach for Key Generation Based on the RNA," *journal of the college of basic education,* vol. 20, no. 87, pp. 101-111, 2015.

[18] N M Abbas and M E Abdulmunim, "mRNA Approach Image Encryption Using LUC Algorithm," *Iraqi Journal of Science,* vol. 64, no. 5, pp. 2545-2560, 2023.

[19] E M R Hamed, A E Taha and I Hammoodi, An Advanced Data Security Algorithm Using cryptography and DNA-Based steganography, 2014 24th International Conference on Computer Theory and Applications (ICCTA),IEEE, 2014.

[20] A A Majeed and ,K A Ameenand, , A C Shakir and , Y Alyeksyeyenkov, "The Enhanced data sequence method for ECC cryptosystem," *Applied Mathematical Sciences,* vol. 8, no. 112, pp. 5553-5564, 2014.

[21] S Thorvaldsen and O Hössjer, "Estimating the information content of genetic sequence data," *Journal of the Royal Statistical Society Series C: Applied Statistics,* vol. 72, no. 5, pp. 1310-1338, 2023.

[22] A A Majeed and B A Qader, "An improved vigener algorithm based on circular-left-shift key and MSB binary for data security.," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 23, no. 1, pp. 431-437, 2021.

[23] MS Khan, J Ahmad, A Al-Dubai, B Ghaleb, N Pitropakis, WJ Buchanan, "RNA-TransCrypt: Image Encryption Using Chaotic RNA Encoding, Novel Transformative Substitution, and Tailored Cryptographic Operations," *In Cybersecurity, Cybercrimes, and Smart Emerging Technologies,CRC Press,* pp. 353-362, 2024.

[24] A Ihsan and N Doğan, "Improved affine encryption algorithm for color images using LFSR and XOR encryption," *Multimedia Tools and Applications,* vol. 82, no. 5, pp. 7621-7637, 2023.

[25] K Kumar, M Sharan and I Singh, "Image encryption and decryption using affine-RSA cryptosystem," *International Journal of Statistics and Applied Mathematics,* vol. 9, no. 2, pp. 113-115, 2024.

[26] S. Y. Wulandari, "Cryptography: A Combination of Caesar and Affine Cipher to Conceal the Message."," in *In Proceeding International Conference on Science and Engineering*, 2020.

[27] Arroyo, Jan Carlo T., and Allemar Jhone P. Delima, "A Keystream-Based Affine Cipher for Dynamic Encryption," *International Journal,* vol. 8, no. 7, pp. 2919-2922, 2020.

[28] O. F. Rashid, "Text Encryption Based on DNA Cryptography, RNA, and Amino Acid," *In The 5th International Multi-Conference on Artificial Intelligence Technology (MCAIT) ,* 2021.

[29] O. F. Rashid, "Text Encryption Based on DNA Cryptography, RNA, and Amino Acid," in *In The 5th International Multi-Conference on Artificial Intelligence Technology (MCAIT 2021)*, 2021.

[30] B. A. M. a. Y. N. T. K A Ameen, "Secure message transmission scheme in wireless sensor networks," *Bulletin of Electrical Engineering and Informatics,* vol. 10, no. 3, pp. 1514-1523, 2021.

[31] Y N A Taher, K A Ameen, and A M Fakhrudeen, "An efficient hybrid technique for message encryption using Caesar cipher and deoxyribonucleic acid steganography," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 28, no. 2, pp. 1096-1104, 2022.

[32] M Aoun, T Mazhar, M A Nadeem, T Shahzad, S Ur Rehman, and A Ur Rehman, "A novel encryption scheme for secure communication based on rna," *CSI Transactions on ICT,* vol. 12, no. 4, pp. 71-80, 2024.

[33] E. K. Gbashi, "Text Compression & Encryption Method Based on RNA and MTF," *Iraqi Journal of Science,* vol. 58, no. 2C, pp. 1149-1158, 2017.

[34] K A Ameen, W k Abdulwahab, and Y N A Taher, "Encryption Technique Using a Mixture of Hill Cipher and Modified DNA for Secure Data Transmission," *International Journal of Computing,* vol. 17, no. 1, pp. 1-9, 2025.

[35] J M Al-Tuwaijari, "Multi-Cipher Technique based on RNA and Chebyschev Map," *Iraqi Journal of Information Technology,* vol. 7, no. 1, pp. 114-125, 2015.

Table 2: Data Sequence Generator

Number of bits = 6						Equivalent	Number of bits = 6						Equivalent	Number of bits = 6						Equivalent
0	0	0	0	0	0	0	0	0	1	0	0	1	9	0	1	0	0	1	0	18
0	0	0	0	0	1	1	0	0	1	0	1	0	10	0	1	0	0	1	1	19
0	0	0	0	1	0	2	0	0	1	0	1	1	11	0	1	0	1	0	0	20
0	0	0	0	1	1	3	0	0	1	1	0	0	12	0	1	0	1	0	1	21
0	0	0	1	0	0	4	0	0	1	1	0	1	13	0	1	0	1	1	0	22
0	0	0	1	0	1	5	0	0	1	1	1	0	14	0	1	0	1	1	1	23
0	0	0	1	1	0	6	0	0	1	1	1	1	15	0	1	1	0	0	0	24
0	0	0	1	1	1	7	0	1	0	0	0	0	16	0	1	1	0	0	1	25
0	0	1	0	0	0	8	0	1	0	0	0	1	17	0	1	1	0	1	0	26

Table 3: Alphabet values

Plaintext alphabetic	a	b	C	D	e	f	G	H	i	j	k	l	m	n
Plaintext value	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Plaintext alphabetic	o	p	Q	R	s	t	U	V	w	x	y	z	spac e	
Plaintext value	14	15	16	17	18	19	20	21	22	23	24	25	26	

Table 5: Encryption message process

Plain text (Message)	Digit Value	Secret keys	Apply Affine Cipher	Convert to the Data Sequence	The 6-bit key XOR used	Result in XOR operation	Concatenation operation	Circular Right Shift
G	6	a = 7	18	010010	010101	000111	000111000010	001110000100
O	14	b = 2	22	010110	010101	000010		

Convert to RNA sequence	Complement of RNA sequence	Convert to Digit Number	Convert to binary value	Attach key XOR to result	Cipher Message
AUGACA	UACUGU	200220620	010110000000 00001001011 00001100101 10	010101	01011000000000 00100101100001 10010110010101

Table 6: Index of coincidence for the proposed scheme

Plain text	IC	Cipher text	IC
Computer is a good device	0.04285	o i y d c a i j q g u p q q q u f q k w u a u e y r h c a x a c n o d c o a l u f q v a u e y t v b f s m s f y u z	0.04030
Information technology	0.05238	e y q d u a c L d c o k g b c e a q q u e y v d c a a g q u f q v b c m k g d u o y q h u o y v a c a y y f	0.04919

Table 7: Comparison between the proposed scheme and others in term of time consumption

Algorithms	Text file size (Byte)	Cipher file size (Byte)	Encryption time (ms)	Decryption time (ms)
[31]	24	54	17.3232	30.5047
	27	81	20.3049	47.4209
[34]	24	68	13.0481	18.0343
	27	83	17.1542	21.4729
The Proposal scheme	24	65	9.3232	12.5047
	27	78	11.3049	15.4209

Table 8: Comparison between proposed algorithm and several algorithms

Schemes	Cryptography mechanisms	Kind data	Key-value used	XOR used	Encryption Technique used other than RNA	Security level	Execution time
Proposal scheme	Symmetric key	Any data	Two keys used	XOR used	RNA and Affine Cipher based on the data sequence	High	Fast
[29]	Symmetric key	Any data	Not used	Not used	DNA with RNA sequence	Middle	Moderate
[31]	Symmetric key	Any data	One Key used	Not used	DNA based Caesar Cipher	Middle	Moderate
[32]	Symmetric key	Any data	One Key used	XOR used	DNA with RNA sequence	Middle	Moderate
[35]	Symmetric key	Any data	One Key used	Not used	DNA and RNA with a chaotic sequence	Low	Slow
[33]	Symmetric key	Any data	More one Key used	Not used	RNA and MTF	Low	Moderate
[30]	Symmetric key	Any data	One Key used	Not used	DH and Knapsack Algorithm	Middle	Slow
[26]	Symmetric key	Any data	Two keys used	Not used	Caesar and Affine Cipher	Low	Slow

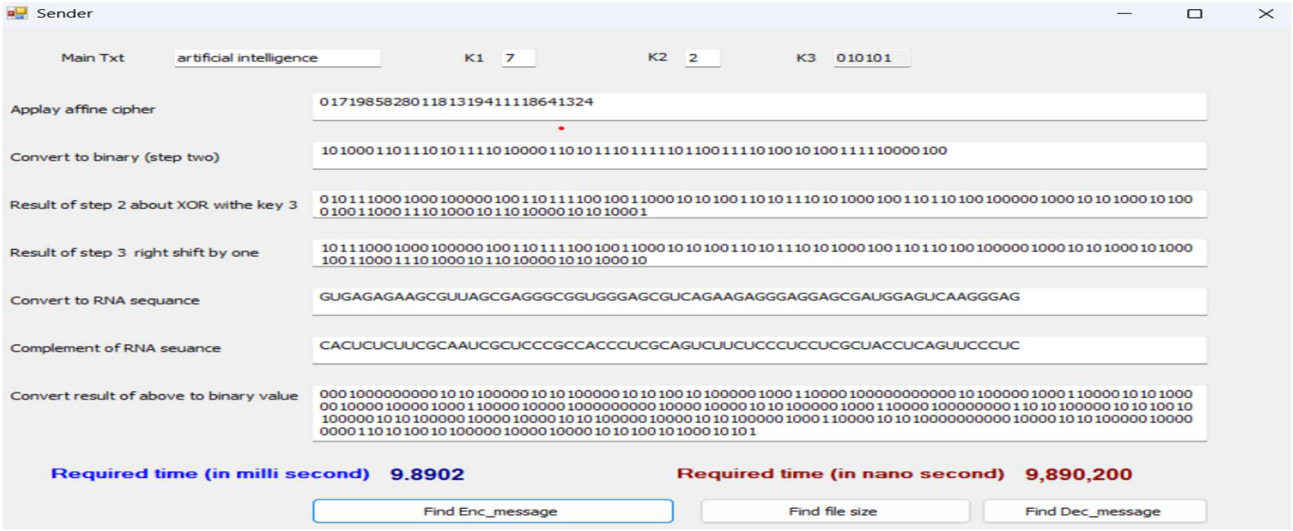

Figure 1: Simulation of the proposed approach.

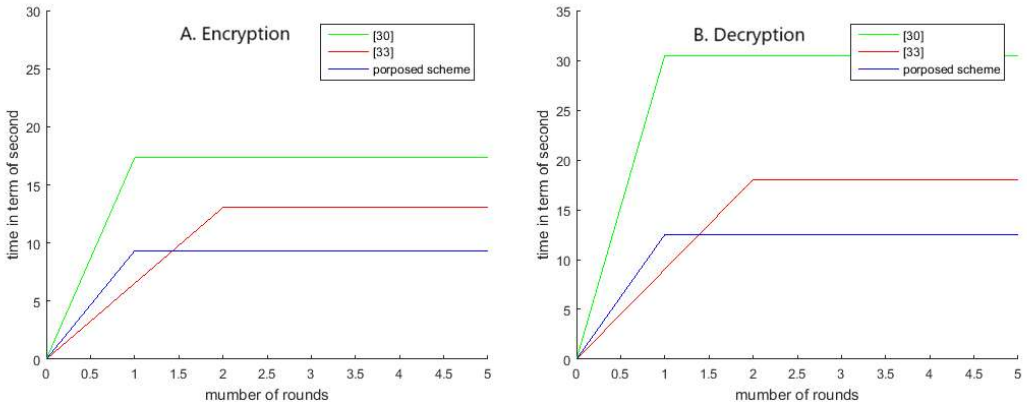

Figure 2: Comparison in term of time consumption for Text file size 24B A: Encryption B: Decryption

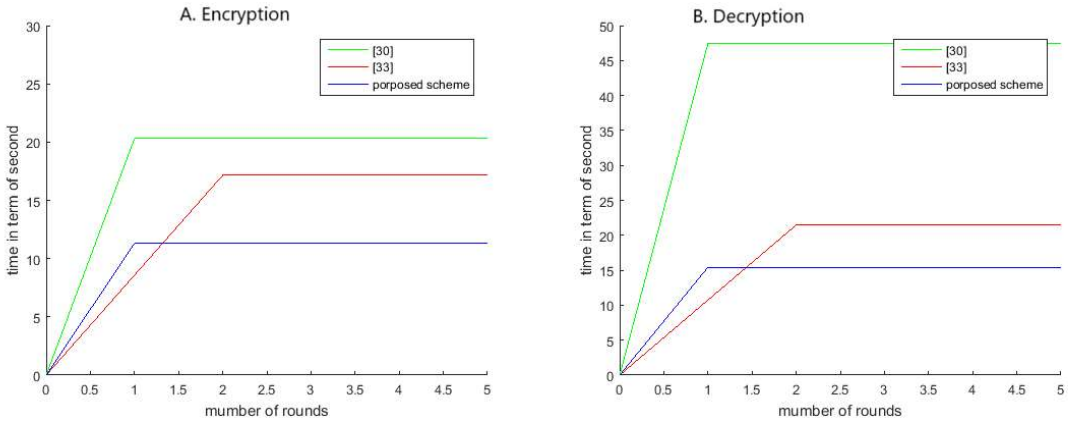

Figure 3: Comparison in term of time consumption for Text file size 27B A: Encryption B: Decryption