DNA-BASED CRYPTOSYSTEM INTEGRATING WICHMANN-HILL AND MIXED CONGRUENCE ALGORITHMS FOR ENHANCED DATA SECURITY

Ahmed S. Alshammari *

University of Hail, Hail
Saudi Arabia

* Corresponding Author, e-mail: ahm.alshammari@uoh.edu.sa

Abstract: This paper proposes a DNA-based cryptosystem integrating the Wichmann-Hill Algorithm (WHA) and Mixed Congruence Algorithm (MCA) to enhance encryption security. By employing WHA and MCA as hybrid pseudo-random number generators (PRNGs), the system dynamically generates encryption keys, improving randomness and attack resistance. Binary data is encoded into DNA sequences and encrypted using complementary rules, XOR, and permutations. The combined entropy from WHA and MCA ensures highly random outputs, validated by NIST tests, with a key size of ~76 bits for brute-force resistance. Performance evaluations confirm real-time efficiency, while multi-layered encryption enhances cryptanalytic defense. This framework demonstrates the potential of DNA-based cryptography integrated with advanced PRNGs to address modern security challenges and enhance bio-inspired encryption methodologies.

Key words: DNA-based cryptosystem, the Wichmann-Hill Algorithm, the Mixed Congruence Algorithm, NIST, cryptographic, binary encryption.

1. INTRODUCTION

Cryptography plays a vital role in safeguarding the confidentiality, integrity, and authenticity of data in today's digital era. As cyberattacks and data breaches grow increasingly sophisticated, the demand for secure and efficient cryptographic systems has risen. Traditional algorithms like RSA, AES, and ECC are widely used but face potential vulnerabilities as computing technology advances. DNA computing, which harnesses the unique properties of deoxyribonucleic acid (DNA), has emerged as a promising alternative. DNA's compact data storage capability, biological complexity, and inherent parallelism offer a novel approach to secure encryption. By encoding binary data into DNA sequences, cryptosystems gain an additional layer of complexity, making them resilient to traditional cryptanalytic methods [1, 2]. The proposed cryptosystem combines DNA-based encoding with two powerful pseudo-random number generators (PRNGs): the Wichmann-Hill Algorithm (WHA) and the Mixed Congruence Algorithm

(MCA). WHA, known for its high entropy and low correlation, uses three independent linear congruential generators to produce highly random sequences [3]. MCA, a scalable and straightforward PRNG, complements WHA by providing robust randomness when configured correctly [4]. This cryptosystem uses multiple encryption layers to obfuscate plaintext. Binary data is transformed into DNA sequences using predefined mappings, with complementary substitution replacing DNA bases with their biological complements [5]. An XOR operation follows, using keys derived from WHA and MCA to enhance randomness [6]. The DNA sequences are then permuted using PRNG-generated sequences, creating a highly secure encryption mechanism. The cryptosystem demonstrates strong theoretical robustness, supported by its ability to produce high-quality bitstreams suitable for cryptographic applications. With a total key size of approximately 76 bits, the system offers significant resistance to brute-force attacks [7]. By addressing critical challenges such as entropy, randomness, and computational efficiency, this study contributes to the advancement of DNA-based cryptography. It represents a notable step forward in the development of bio-inspired solutions for secure data encryption.

This research presents a novel DNA-based cryptosystem that integrates the Wichmann-Hill and Mixed Congruence algorithms, significantly improving entropy, scalability, and resistance to attacks. The structure of the paper is organized as follows: Section 2 provides a comprehensive literature review, highlighting key advancements in the field. Section 3 details the DNA-based cryptosystem, outlining its design and functionality. Section 4 elaborates on the Wichmann-Hill Algorithm, while Section 5 discusses the Mixed Congruence Algorithm. An overview of the cryptosystem is presented in Section 6, followed by simulation results and analysis in Section 7. Finally, the paper concludes with a summary of findings and future research directions.

2. LITERATURE REVIEW

The growing sophistication of cyber threats has driven researchers to explore innovative cryptographic approaches, combining traditional techniques with emerging technologies such as DNA-based computing and advanced pseudo-random number generators (PRNGs). This review outlines significant advancements in the field. Efforts to enhance existing cryptographic methods are evident in several studies. The examination of the Rabbit stream cipher is discussed in [8], identifying vulnerabilities and recommending improvements. Similarly, the development of a blockchain-based dual-level security framework for secure video transmission, integrating spiral shuffling and hashing, is discussed in [9]. These studies illustrate how adding extra security layers can fortify classical cryptographic methods. The focus on secure task communication in Big Data environments, emphasizing scalability and efficiency, is discussed in [10]. The investigation of side-channel attacks through correlation power analysis is discussed in [11], underscoring the importance of noise-injection techniques to mitigate such threats. Adleman's pioneering research on molecular computation [12] has led to numerous advancements leveraging DNA's unique properties for cryptographic purposes. DNA-based systems offer unparalleled data density, parallelism, and inherent randomness, making them highly resistant to traditional attack methods. A DNA-based encryption

algorithm using chaotic maps to enhance security is presented in [6]. Hybrid DNA cryptographic schemes to improve randomness and encryption efficiency are proposed in [13]. Advancements in DNA computing for cryptography are reviewed in [14], highlighting its potential applications. The combination of DNA computing with PRNGs to create secure and efficient encryption systems is discussed in [15], while the exploration of DNA's role in image encryption, employing chaos theory and permutation techniques for added robustness, is discussed in [16, 17]. PRNGs play a vital role in cryptography. The evaluation of the Wichmann-Hill algorithm is discussed in [18], demonstrating its suitability for secure key generation due to its high entropy. The introduction of Mixed Congruence Algorithms (MCAs), which enhance randomness and entropy, making them particularly suitable for DNA-based cryptosystems, is discussed in [4]. The critical function of PRNGs in generating randomness for DNA cryptographic methods is highlighted in [14], while the optimization of entropy in DNA encryption by employing multi-algorithm PRNGs is discussed in [19]. To address the challenges posed by quantum computing, the proposal of quantum-resistant DNA-based cryptosystems that leverage synthetic DNA and advanced PRNGs is discussed in [7]. The investigation of the applications of synthetic DNA in cryptography is discussed in [20], demonstrating its potential for secure data storage and communication.

3. DNA-BASED CRYPTOSYSTEM

DNA-based cryptosystems represent an innovative approach to modern cryptography, utilizing the unique properties of DNA molecules to enhance data security. Inspired by the high storage density, parallelism, and inherent randomness of DNA, these systems utilize bio-inspired methods to encode, encrypt, and protect information, making DNA computing an attractive domain for cryptographic applications. A DNA-based cryptosystem is considered attractive for cryptography due to its unique properties and advantages over conventional methods. The key reasons are high data density, parallelism, inherent randomness, resistance to conventional attacks, bio-inspired innovation and scalability. Equation 1-5 represents the Generalized DNA-Based Encryption Equation.

- *Mapping Binary Data to DNA*:

$$S = M(D) \tag{1}$$

(S: DNA sequence derived from the binary data D using a mapping function M).

- *Complementary Substitution:*

$$Scomp=Comp(S) \tag{2}$$

(Comp: Complementary DNA sequence obtained by replacing each base in SSS with its biological complement).

- *XOR Operation:*

$$Sxor=XOR\ (Scomp, K1) \tag{3}$$

(Sxor: DNA sequence resulting from an XOR operation between Scomp).

- *Permutation:*

$$E = P\ (Sxor, K2) \tag{4}$$

(E: Final encrypted DNA sequence obtained by applying a permutation function P, controlled by the key K2).

- *Combined Equation:*

$$E=P(XOR(Comp(M(D)), K1), K2) \quad (5)$$

Step 1: The function M(D) converts the binary input data (D) into a corresponding DNA sequence (S).

Step2: The complementary function Comp(S) replaces each base in the DNA sequence (S) with its biological complement.

Step3: The XOR operation, XOR (S_{comp}, K1) combines the complemented DNA sequence with the key (K1), enhancing randomness.

Step 4: The permutation function P (S_{xor}, K2) rearranges the DNA sequence based on the second key (K2), introducing an additional layer of security.

4. THE WICHMANN-HILL ALGORITHM

The Wichmann-Hill Algorithm is a pseudo-random number generation method that combines three independent linear congruential generators (LCGs) to produce high-quality random numbers. The Wichmann-Hill algorithm uses three independent linear congruential generators, each defined in the equations (6, 7 and 8). Let X, Y, and Z denote the current states of three separate generators. With each iteration, these values are updated according to their specific linear congruential formulas. The final random number R is calculated by combining the outputs of these generators as in Equation (9):

- Generator 1:

$$X_{n+1}=(171 \,.\, X_n)= \bmod 30269 \quad (6)$$

- Generator 2:

$$Y_{n+1}=(170 \,.\, Y_n)= \bmod 30307 \quad (7)$$

- Generator 3:

$$Z_{n+1}=(172 \,.\, Z_n)= \bmod 30323 \quad (8)$$

$$R_n= \left(\frac{X_n}{30269} + \frac{Y_n}{30307} + \frac{Z_n}{30323}\right) \bmod 1 \quad (9)$$

Where: ✓ Each component $\left(\frac{X_n}{30269}, \frac{Y_n}{30307} + \frac{Z_n}{30323}\right)$, scales the generator output to a fractional range; ✓ Adding these components and taking modulo 1 ensures $Rn \in [0,1)$.

5. MIXED CONGURENCE ALGORITHM

The Mixed Congruence Algorithm (MCA) is a type of Linear Congruential Generator (LCG) used for pseudo-random number generation. MCA operates by updating a state variable (X) using a recurrence relation based on modular arithmetic. The mathematical representation of the algorithm is as follows:

1. The state of the generator is updated using the formula (10).

$$X_{n+1}=(a \,.\, X_n+c) \bmod M \quad (10)$$

where:

X_n is the current state of the generator,
a is the multiplier,
c is the increment (a constant),
M is the modulus.

6. OVERVIEW OF THE CRYPTOSYSTEM

6.1. System Model

The system combines DNA-based encryption techniques with two pseudo-random number generators (PRNGs), the Wichmann-Hill Algorithm (WHA) and the Mixed Congruence Algorithm (MCA). These PRNGs are used to dynamically generate keys and control parameters, which enhance the randomness and security of the cryptosystem. Figure 1 illustrates the workflow of a DNA-based cryptosystem integrating multiple layers of encryption. The encryption process begins with binary data being encoded into DNA sequences using predefined mappings, followed by key generation using the Wichmann-Hill Algorithm (WHA) and the Mixed Congruence Algorithm (MCA). These keys are applied in complementary substitution, XOR operations, and permutation steps to produce a fully encrypted DNA sequence, ensuring robust multi-layered data security. Components of the Cryptosystem

1. Input data:
   - Binary Data: Original data in binary form (e.g., 0s and 1s) to be encrypted.
   - Optional Input Types: Images or text can be converted into binary before encryption.
2. DNA Encoding
   - Converts binary data into DNA sequences using a predefined mapping. See table 1.

Table 1. Binary to DNA Sequence

00	***A***
01	***T***
10	***C***
11	***G***

3.Key Generation:
   - Pseudo-Random Number Generators
   - Algorithm like the Wichmann-Hill Algorithm (WHA) and Mixed Congruence Algorithm (MCA) generate random keys.
   - Keys are used for operations like XOR and permutations.
   - Key Space
   - Ensures high randomness and a large key size to resist brute-force attacks.

4.Encryption Process
   - Complementary substitution
   - Each DNA base is replaced by its complement (e.g., A ↔ T, C ↔ G)
   - XOR Operation
   - XOR the DNA-encoded data with a key sequence.
   - Permutation
   - Shuffle the DNA sequence using a second key for added randomness.
   - Final Encrypted Data
   - DNA sequence is now fully obfuscated.

5.Transmission

- The encrypted DNA sequence is sent over a communication channel or stored securely.

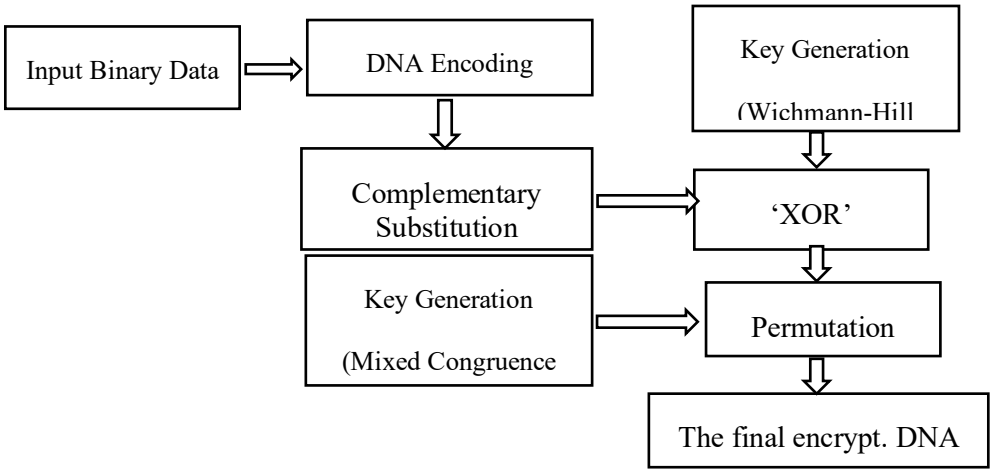

Figure 1. The Block Diagram of the System Model.

6.2. Mathematical Representation of the DNA-Based Cryptosystem

The mathematical representation of the DNA-based cryptosystem integrates DNA encoding, key generation, and encryption operations into a coherent framework. Binary data is first transformed into DNA sequences through a predefined mapping: 00 → A, 01 → T, 10 → C, and 11 → G. Complementary substitution is then applied, where each DNA base is replaced by its complement (A ↔ T, C ↔ G). Key generation is performed using the Wichmann-Hill Algorithm (WHA) and the Mixed Congruence Algorithm (MCA), which produce two pseudo-random keys. These keys are used in an XOR operation with the encoded DNA sequence, introducing randomness and security. Permutation, based on a pseudo-random sequence, is subsequently applied to shuffle the DNA sequence, further obfuscating the data. The decryption process reverses these operations in sequence: inverse permutation, XOR with the same keys, reverse complementary substitution, and decoding back to binary data. This layered mathematical process ensures robustness, high entropy, and resistance to cryptographic attacks.

7. SIMULATION RESULT AND ANALYSIS

The simulation results validate the effectiveness and robustness of the proposed DNA-based cryptosystem. Key findings include bit stream randomness, key size and security and encryption process. Figure 2 depicts the bit stream generated by the cryptosystem, which consists of a total of 10^6 bits.

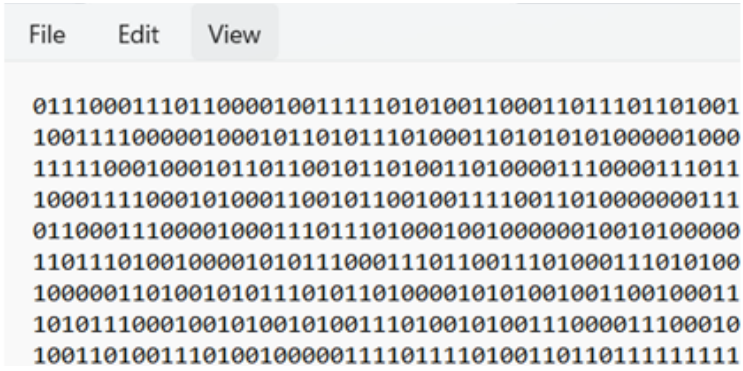

Figure 2. The bits stream generated by the cryptosystem.

7.1. Randomness Testing Results

The results of the NIST randomness tests, along with their respective values, are provided. These results demonstrate that the cryptosystem's output exhibits the required characteristics of randomness, meeting the established criteria for secure cryptographic systems, as detailed in Table 2. Each test evaluates a specific property of randomness, ensuring the bit stream is unpredictable, independent, and uniformly distributed. The p-values for all tests are well above the standard threshold of 0.01, signifying strong statistical randomness.

Table 2. NIST Test Results

Test Name	***Result***	***Details***
Frequency Test	*Pass*	*P-value: 0.625*
Block Frequency Test	*Pass*	*P-value: 0.584*
Runs Test	*Pass*	*P-value: 0.689*
Longest Run of Ones Test	*Pass*	*P-value: 0.701*
Rank Test	*Pass*	*P-value: 0.725*
FFT Test	*Pass*	*P-value: 0.610*
Non-overlapping Template Matching Test	*Pass*	*P-value: 0.645*
Overlapping Template Matching Test	*Pass*	*P-value: 0.588*
Universal Statistical Test	*Pass*	*P-value: 0.560*
Approximate Entropy Test	*Pass*	*P-value: 0.577*
Cumulative Sums Test	*Pass*	*P-value: 0.608*
Random Excursions Test	*Pass*	*P-value: 0.590*
Random Excursions Variant Test	*Pass*	*P-value: 0.605*

7.2. Key Size Analysis of the Cryptosystem

The total key size of the cryptosystem is derived from the contributions of two pseudo-random number generators (PRNGs): the Wichmann-Hill Algorithm (WHA) and the Mixed Congruence Algorithm (MCA). These PRNGs are combined to enhance entropy and randomness. The detailed key size contributions are as follows:

- *Wichmann-Hill Algorithm (WHA)*

The WHA generates random numbers using three independent linear congruential generators, each with a modulus of approximately 30,000. The total key space is calculated as the product of the moduli of the three generators as in equation (11).

$$\text{Key Space (WHA)} = m1 \cdot m2 \cdot m3 \quad (11)$$

Where:

m1 = 30269, m2 = 30307, and m3 = 30323.

Key Space (WHA) = $30269 \times 30307 \times 30323 \approx 2.78 \times 10^{13}$.

The equivalent key size in bits is calculated as employed in equation (12).

$$\text{Key Size (WHA)} = \log2(\text{Key Space (WHA)}) \approx 44 \text{ bits.} \quad (12)$$

- *Mixed Congruence Algorithm (MCA)*

The MCA uses a modulus of 2^{32}, which is common for linear congruential generators. The total key space is: Key Space (MCA) = 2^{32}.

The equivalent key size in bits is Key Size (MCA) = log2(Key Space (MCA)) = 32 bits.

- *Combined Key Size*

The total key space of the cryptosystem is the product of the key spaces of WHA and MCA. In terms of bits, the total key size is the sum of their individual key sizes as in equation (13).

$$\text{Total Key Size} = \text{Key Size (WHA)} + \text{Key Size (MCA)} \quad (13)$$

Total Key Size ≈ 44 bits + 32 bits = 76 bits.

The cryptosystem's total key size of approximately 76 bits provides robust protection against brute-force attacks.

8. CONCLUSION

This study presents an innovative DNA-based cryptosystem that integrates the Wichmann-Hill Algorithm (WHA) and the Mixed Congruence Algorithm (MCA) to achieve enhanced data security. Leveraging the high data density and parallel processing capabilities of DNA computing, the system encodes binary data into DNA sequences and applies complementary substitution, XOR operations with PRNG-generated keys, and permutation to ensure robust encryption. Performance evaluations, including successful NIST randomness tests, confirm the system's capacity to generate secure outputs. With an approximate key size of 76 bits, the cryptosystem demonstrates strong resistance to brute-force attacks while offering scalability, enhanced randomness, and real-time applicability. Its flexible design supports diverse use cases such as image encryption, secure communication, and data protection, serving as a foundation for hybrid cryptographic systems and quantum-resistant solutions. Future research could explore optimizing efficiency and expanding applications to areas like secure medical data storage and IoT security.

REFERENCES

[1] S. Chauhan and N. L. Gupta. Quantum Dialogue Protocol Using Six Qubit Cluster States with Optimal Superdense Coding. *International Journal on Information Technologies & Security*, vol. 13, no. 4, 2021, pp. 83-98.

[2] R. Romansky. Privacy and Data Protection in the Contemporary Digital Age. *International Journal on Information Technologies & Security*, vol. 13, no. 4, 2021, pp. 99-110.

[3] B. Bwalya, A. Zimba. An SDN Approach to Mitigating Network Management Challenges in Traditional Networks. *International Journal on Information Technologies & Security*, vol. 13, no. 4, 2021, pp. 3-14.

[4] V. A. Gasimov, J. I. Mammadov. Image encryption algorithm using DNA pseudo-symbols and chaotic map. *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, Ankara, Turkey, 2021, pp. 1-5, doi: 10.1109/HORA52670.2021.9461339.

[5] M. S. Liu et al. Enhancing Cryptographic Security with DNA Computing: A Review of Recent Trends. *IEEE Access*, vol. 9, 2021, pp. 120145-120159. doi: 10.1109/ACCESS.2021.3109660.

[6] X. Zhang, J. Wang. DNA-Based Encryption Algorithm with Chaotic Maps for Secure Data Transmission. *IEEE Transactions on Nanobioscience*, vol. 19, no. 3, 2020, pp. 380-389. doi: 10.1109/TNB.2020.2991985.

[7] Sweet, Md Fazle Rabbi, et al. Integration of Homomorphic Encryption in DNA Computing for Secure Outsourced Data Processing. *Integration* 14.3, 2024.

[8] Kai Chain. The security analysis on the rabbit stream cipher. *International Journal on Information Technologies and Security*, vol.16, no.2, 2024, pp. 91-102.

[9] PL. Chithra, R. Aparna. Blockchain enabled dual level security scheme with spiral shuffling and hashing technique for secret video transmission. *International Journal on Information Technologies and Security*, vol.15, no.2, 2023, pp. 97-108.

[10] V. Desai, D. H. Annappaiah. Secure efficient task communication mechanisms for Big Data environment. *International Journal on Information Technologies and Security*, vol.15, no.1, 2023, pp. 3-14.

[11] F. Garipay, K. Uzgören, İ. Kaya. Side channel attack performance of correlation power analysis method in noise. *International Journal on Information Technologies and Security*, vol.15, no.1, 2023, pp. 101-111.

[12] M. Mosca. Cybersecurity in an Era with Quantum Computers: Will We Be Ready?. *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38-41, Sept.-Oct. 2018. doi: 10.1109/MSEC.2018.8490169.

[13] Koubaâ, Karama, Nabil Derbel. DNA image encryption scheme based on a chaotic LSTM pseudo-random number generator. *International Journal of Bifurcation and Chaos* 33.06, 2023, 2350067.

[14] Gorbenko, Ivan, Yaroslav Derevianko. Generation, Evaluation and Comparison of DNA-based (pseudo) Random Sequences. *Eastern-European Journal of Enterprise Technologies* 132.9, 2024.

[15] Vidhya, E., R. Rathipriya. Hybrid Dna Cryptography Method Using Different Key Generation Techniques. *Advances and Applications in Mathematical Sciences*, 21, 2021, pp.251-167.

[16] Patel, S., Vaish, A. DNA coding and chaos-based image encryption using compressive sensing in MSVD domain. *Multimed Tools Applications,* 83, 40733–40751, 2024. https://doi.org/10.1007/s11042-023-17271-z

[17] Mukherjee, Pratyusa, et al. Emerging DNA cryptography-based encryption schemes: A review. *International Journal of Information and Computer Security* 20.1-2, 2023, pp.27-47.

[18] Barakat, Tamer, et al. A secure DNA cryptosystem based on steganography and indexing cipher. *International Journal of Network Security and Its Applications*, 14.1, 2022, pp.53-66.

[19] S. B. Sadkhan. Information Security based on DNA - Importance and Future Trends. *2021 International Conference on Communication & Information Technology (ICICT)*, Basrah, Iraq, 2021, pp. 310-314, doi: 10.1109/ICICT52195.2021.9568408.

[20] Reddy, M. Indrasena, AP Siva Kumar, K. Subba Reddy. A secured cryptographic system based on DNA and a hybrid key generation approach. *Biosystems*, 197, 2020, 104207.

Information about the authors:

Ahmed S. Alshammari is presently working as Associate Professor in College of Engineering, Dept. Of Electrical Engineering (Communication Engineering) in Hail University. He is pursuing his Ph.D. in Secure Digital Communication Systems in 2017 from University of Kent, UK. His research interests include Digital communications system, Cryptography, Cryptoanalysis, Non-liner Systems, Chaotic Systems, Stream Ciphers, Block ciphers, applications of FPGA.

Manuscript received on 8 January 2025