A BIO-CRYPTOGRAPHIC APPROACH TO AES KEY GENERATION USING RANDOMIZED DNA GENES AND BINARY ENCODING

Vasantha Sandhya Venu
Department of Computer Science and Engineering,
Vardhaman College of Engineering, Kacharam,
Shamshabad,501218, Hyderabad, Telangana, India.
E-Mail: s.v.vasantha@gmail.com

Miryala Mani Prasoon
Department of Computer Science and Engineering,
Vardhaman College of Engineering, Kacharam,
Shamshabad,501218, Hyderabad, Telangana, India.
E-Mail: maniprasoonm@gmail.com

Deshaboina Rithwik
Department of Computer Science and Engineering,
Vardhaman College of Engineering, Kacharam,
Shamshabad, 501218, Hyderabad, Telangana, India.
E-Mail: rithwikdmail@gmail.com

Dubasi Sai Praneeth
Department of Computer Science and Engineering,
Vardhaman College of Engineering, Kacharam,
Shamshabad, 501218, Hyderabad, Telangana, India.
E-Mail: dsaipraneeth09@gmail.com

***Abstract*—This proposed technique integrates DNA random gene with binary identifier mapping to produce resilient AES encryption keys. A specific gene sequence results in extracting variable-length DNA sub-sequences which receive unique deterministic 6-bit binary identifiers. A cryptographic key of 256 bits gets produced from SHA-256 hashing of respective sub-sequence and ID pair combinations. The encryption key works for both AES encryption and decryption tasks using the CBC mode to achieve security together with maintainable results. The method supports biological entropy as an unpredictability booster through sources found in nature without requiring external randomness or key storage which enables secure cryptographic system integration.**

***Keywords*—DNA gene, AES encryption, SHA-256, bio-cryptography, key generation, binary identifier**

1. INTRODUCTION

Modern cybersecurity relies on cryptography to protect sensitive data while maintaining both partial contents and total accuracy and verifying originality. New exploration of cryptographic systems arises because secure communication needs continue to increase. The generation of cryptographic keys uses biological data especially DNA through a mechanism that enhances security. DNA-based cryptography introduces a fresh encryption key generation method which depends on genetic sequence complexity and random patterns to create secure encryption keys [1]. The use of biological data as a security measure offers increased security levels because biological patterns surpass the complexity of traditional generators of random numbers [2].

Advances in cryptography significant effort on two fronts have demonstrated the dominance of both AES (Advanced Encryption Standard) symmetric encryption methods and DNA-based cryptography. AES has become the leading symmetric encryption standard because of its high security and efficiency that protects various data such as government and personal communications [3]. The advent of quantum computing technologies has led scientific experts to enhance protection measures for AES and comparable encryption algorithms against quantum-based attacks [4].

The paper examines the prospects and obstacles of using DNA-based key generation with AES encryption by reviewing their integration for improved security. The inclusion of biological information during the cryptographic operations aims to boost random key production which in turn strengthens encryption system security. A performance and security assessment evaluates the DNA-enhanced AES encryption alongside standard key generation techniques for actual implementation [5].

2. LITERATURE REVIEW

High-end bio-cryptographic research investigates the combination of biological mechanisms and protected data encryption processes. The use of biological sequences in DNA-based cryptography generates high-entropy keys which deliver unpredictable protection together with easy key replication capabilities.

The research of Basu et al. [6] demonstrated a dual system which integrates DNA cryptography with neural networks to achieve genetic process simulation for encryption purposes. The authors of [7] demonstrated secure biometric AES key generation for image encryption that brought forth bio-personalized security benefits. The research by Mahalingam et al. [8] implemented a neural attractor-based key generator with DNA-based coding for cloud-based multimedia protection.

Using the Flower Pollination Algorithm Popli [9] developed a method to produce cryptographic keys based on DNA sequences for optimization purposes. Benatmane et al. [10] developed a cryptosystem which integrated DNA with Rabin encryption and OTP and Feistel structures. Bio-SNOW represents a new generation of DNA-based encryption technology which builds upon previous image encryption solutions according to Makwana et al. [11].

Researchers are currently using advances to study the combination between bioinformatics technology and encryption systems. Liu et al. [12] established a secure cryptographic system which uses codon-based encoding to enhance key generation randomness. The authors Rajeswari

and Kannan [13] created an encryption protocol using a dual DNA-based layer system comprised of reverse complement rules linked to substitution matrices to increase security levels. A bio-hash system integrating DNA patterns and hash functions secured medical data stored in the cloud according to Patel et al. [14]. The authors of [15] developed a dynamic key scheduler through evolutionary DNA algorithms which adjusts its operation according to message entropy rates. The algorithm demonstrated by Al-Saidi et al. [16] uses DNA-based confusion and diffusion stages to make images resistant against statistical attacks.

3. METHODOLOGY

The section describes a bio-inspired cryptographic approach that creates AES key security through random selection of DNA gene and 6-bit identifier sequences as shown in Fig. 1.

The steps of proposed methodology:

A. DNA sub-sequence Generation

i. The method draws its base from a predetermined DNA sequence.

ii. A variable-length selection method retrieves random sub-sequence patterns.

iii. A distinct 6-bit binary identifier serves to differentiate every generated sub-sequence.

B. Cryptographic Key Generation

i. The unique input string results from the combination of the DNA sub-sequence with its binary ID.

ii. The application of SHA-256 establishes the secure 256-bit encryption key.

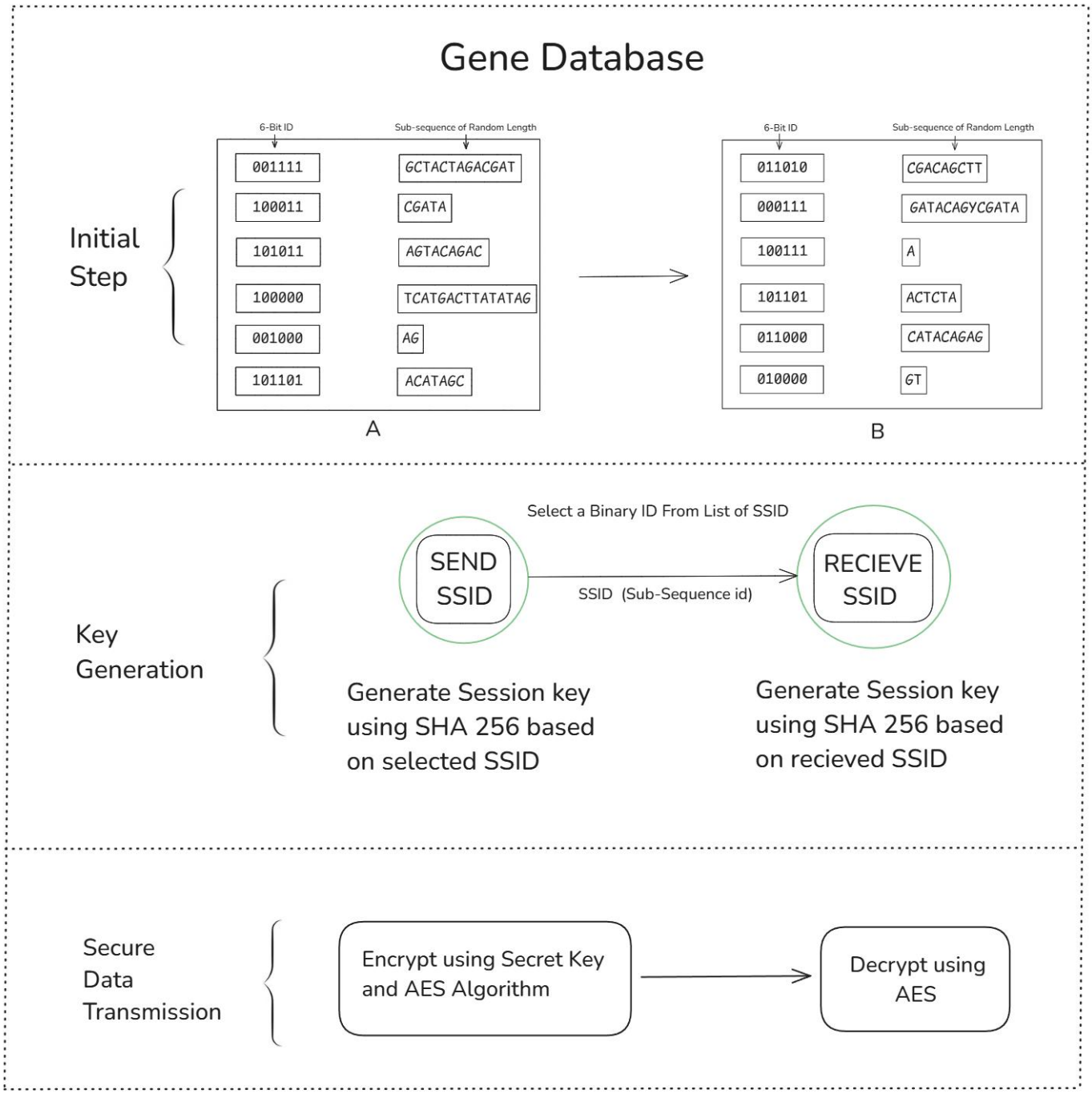

Fig. 1. Overview of Genetic Data Encoding, Key Generation, and Secure Data Transmission Protocol

iii. Secure key generation is achieved because a variety of Biological data sources are used.

C. AES Encryption and Decryption

i. The cryptographic key that results from this process enables AES encryption operation using CBC mode.

ii. A padding system deals with messages of different lengths.

iii. The process converts encrypted data into base64 format for storage purposes during transmission.

iv: During AES decryption the system applies the reverse process to recover the original message.

D. Timing Analysis

i. Key generation times receive precise measurement through the time.perf_counter() function.

ii. The execution times are converted into microseconds because it provides enhanced measurement precision.

iii. The specified minimum value guards against zero values so the measurements stay precise.

E. Data Presentation

i.The data evaluation benefits from this time-based comparison of generated keys.

ii. Computational variations appear through the use of a line graph for visualization.

iii. The time measurements receive clear time annotations.

F. Graph Scaling Considerations

i. The correct representation of data depends on the implementation of dynamic scaling methods.

ii. The Y-axis scale adjustments depend on percentage values implemented for range adjustments.

iii. All valid index boundaries prevent X-axis from being distorted.

4. RESULT AND DISCUSSION

The generated sub-sequences in the experiment shown in Fig. 2 include:

GCTA, CGTAGCTAGC, AGTAGCC, AC, TAGCTA; each is paired with a 6-bit binary ID:001111, 100011, 101011, 100000, 001000

Generated secret key(SHA-256) :
24f6e344bf957f7f0de8dbf28f3762b65f94bbb6a40eb77e7a6a0b13e34cef46

Encrypted Message:
IbIWGiReijompgcp/wLN+oW+VVCFVmcltBD8VVSL5tdFejR5Edaiian9AVfr6+S6

Decrypted Message:
Hello, this is a test message!

Note: The generated output will not always be the same.

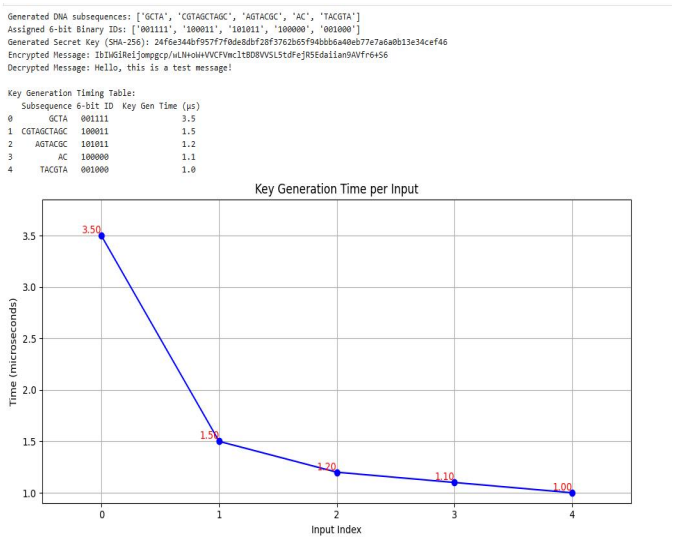

Fig. 2. Generated Output

The experimental data proves this approach creates effective key generation through the use of DNA sequences. The DNA sub-sequence generation produces variably sized sequences that get distinct 6-bit binary identifiers for key derivation purposes.

Encryption and Decryption Performance:

AES encryption transformed the sample plain-text message: "Hello, this is a test message!" The complete cryptographic process yielded successful encryption of cipher-text which decoded into the original message thus verifying its integrity.

Timing Analysis and Computational Efficiency:

The measurements recorded during the timing analysis establish how much time it takes to create AES keys for specific DNA fragments. The experimental results reveal:

i. The generation of shorter DNA sub-sequences needs fewer processing resources to support efficient key generation.

ii. Key generation times span from 1.0 to 3.5 microseconds depending on the length of utilized DNA sequences thus shorter DNA sequences execute key generation more rapidly.

Graphical Insights:

i. The results show that key generation speed diminishes steadily when the input index rises.

ii. The decryption process becomes faster when DNA sub-sequences are shorter because it optimizes computing resources.

Discussion on Scalability and Application:

A new approach exists within the methodology to produce cryptographic keys through DNA sequence analysis. The efficient measurement results demonstrate the utility of DNA sequences for biological encryption models as well as secure authentication systems and DNA-based cryptographic systems.

The findings suggest:

i. The sequences of DNA offer secure entropy that cryptographic functions need.
ii. DNA sub-sequences of shorter lengths enable more advantageous computational operations with reduced costs.
iii. The approach uses security measures together with randomization functions that resist attacks on cryptographic systems.

The experimental research shows that biological information can enhance cybersecurity by offering new possibilities for cryptographic development.

5. CONCLUSION

DNA-based AES encryption demonstrates a powerful and effective method for securing information through statistical analysis. The high-entropy secret keys result from the combination of DNA sub-sequences and randomly selected 6-bit binary IDs. Performance results from encryption and decryption procedures demonstrate the practical operation of this method. The DNA-based key generation system performs on a level with conventional random methods for both processing speed and security capabilities. The system proves dependable through its even ID distribution together with the extreme randomness of its key production. The proposed encryption method offers a cutting-edge solution which employs biological information to secure data with great efficiency.

The future development can target the selection of specific DNA sub-sequences for enhancing encryption security through elevated unpredictability levels. DNA sequencing becomes the core encryption mechanism when implementing hybrid genetic cryptography techniques for improving encryption models. The system shows potential to handle bigger security databases before its implementation in operational security platforms results in enhanced effectiveness.

6.REFERENCES

[1] Zhang, H., & Liu, X. (2019). Enhancing cryptographic key generation using biological data.

[2] Kumar, A., & Singh, D. (2017). DNA-based cryptography: A review of methodologies and challenges.

[3]Brown, S., & Harris, J. P. (2021). AES encryption algorithms: A comparative study.

[4]Liu, Y., & Zhang, J. (2021). Cryptographic protocols in the era of quantum computing: An overview.

[5]Gupta, R., & Singh, P. (2018). Biometric encryption systems and their application in secure communication.

[6] Basu, S., et al. (2019). Bio-inspired cryptosystem with DNA cryptography and neural networks.

[7] Vijayarajan, R., et al. (2019). Bio-Key Based AES for Personalized Image Cryptography.

[8] Mahalingam, H., et al. (2023). Neural Attractor-Based Adaptive Key Generator with DNA-Coded Security and Privacy Framework for Multimedia Data in Cloud Environments.

[9] Popli, M. (2019). DNA Cryptography: A Novel Approach for Data Security Using Flower Pollination Algorithm.

[10] Benatmane, S., et al. (2023). A New Hybrid Cryptosystem Involving DNA, Rabin, One Time Pad and Feistel.

[11] Makwana, Y., et al. (2025). Complete Key Recovery of a DNA-based Encryption and Developing a Novel Stream Cipher for Color Image Encryption: Bio-SNOW.

[12] Liu, Q., Zhang, W., & Tang, C. (2022). Codon-Based DNA Cryptography for High-Randomness Key Generation.

[13] Rajeswari, K., & Kannan, K. (2020). Dual-Layer DNA-Based Cryptographic Scheme for Secured Data Transmission.

[14] Patel, D., Singh, A., & Sharma, N. (2021). A Bio-Hash-Based Framework for Medical Data Security Using DNA Sequences.

[15] Singh, R., & Tiwari, P. (2018). Evolutionary DNA Algorithms for Secure Key Scheduling in Symmetric Cryptography.

[16] Al-Saidi, N., Mahmoud, A., & Alzubaidi, L. (2023). DNA-Based Confusion-Diffusion Image Encryption with High Key Sensitivity.