# Enhanced Encryption Techniques: Integrating Textual Name Values And Dynamic Non-Linear Transformations

Mrs. R. Vaishnavi,
Assistant Professor,
Department of Artificial Intelligence
Intelligence and Data science,
SRM Valliammai Engineering College,
Kattangulathur, Tamil Nadu, India

Mr. Sai Bharath V,
Student,
Department of Artificial
and Data science,
SRM Valliammai Engineering College,
Kattangulathur Tamil Nadu,India

Mr. Vignesh S,
Student,
Department of Artificial Intelligence
Intelligence and Data science,
SRM Valliammai Engineering College,
Kattangulathur, Tamil Nadu, India

Mr. Vishnu R,
Student,
Department of Artificial
and Data science,
SRM Valliammai Engineering College,
Kattangulathur Tamil Nadu,India

***Abstract:*** This is an advanced cryptographic framework designed to meet the growing demand for resilient data protection in an increasingly digital and threat-prone world. Traditional encryption methods often struggle to balance performance, complexity, and post-quantum resilience, prompting the need for an innovative solution that addresses modern security challenges. This system introduces a hybrid encryption architecture that merges lattice-based cryptography with enhanced symmetric encryption, leveraging cutting-edge techniques to ensure both speed and strength. At its core, the system utilizes lattice-based key exchange protocols to establish secure communication channels, employing the Number Theoretic Transform (NTT) to optimize polynomial computations and enable efficient, post-quantum-safe operations. For data encryption, this system implements the Advanced Encryption Standard (AES), augmented by a novel character-to-name mapping scheme and dynamically generated substitution boxes (S-boxes). These additions introduce high degrees of non-linearity and unpredictability, significantly increasing resistance to cryptanalytic attacks. The framework's unique architecture supports dynamic key generation and transformation, allowing each encryption session to adaptively evolve based on input patterns and mapped identifiers. Avalanche effect testing across multiple encryption rounds yielded an average bit-change rate of 51.72%, underscoring the system's strong diffusion properties. Further statistical analysis confirmed high key entropy and minimal correlation, while simulated differential attacks consistently failed to exploit vulnerabilities. This system requires no external hardware or proprietary infrastructure, making it both scalable and cost-effective. Looking ahead, development will focus on integrating lightweight wearable hardware, expanding mobile compatibility, and introducing AI-driven key scheduling mechanisms for adaptive security tuning. This system represents a significant advancement in modern encryption technology, offering a future-ready, modular solution that blends quantum resistance .

***Keywords: AES encryption, character-to-name mapping, dynamic S-box, hybrid cryptosystem, lattice-based cryptography, Number Theoretic Transform (NTT), post-quantum cryptography***.

## I. INTRODUCTION

This system represents a modern response to the rising demand for adaptable, secure, and quantum-resistant encryption methods in today's data-driven landscape. As digital communication, cloud computing, and remote access systems become deeply embedded in daily life, the protection of sensitive information has emerged as a critical concern across industries. While traditional cryptographic methods have historically offered effective protection, rapid advancements in computational power—especially the advent of quantum computing—pose serious threats to these conventional systems. This paradigm shift necessitates the development of cryptographic frameworks that not only resist contemporary attacks but also evolve in tandem with future technological challenges. The field of cryptography, once reliant on basic substitution ciphers like the Caesar cipher, has expanded into a cornerstone of modern cybersecurity infrastructure. From symmetric encryption algorithms like the Advanced Encryption Standard (AES) to public-key systems such as RSA and Elliptic Curve Cryptography (ECC), encryption technologies have

become fundamental to secure communications, digital identity verification, and data integrity. However, these methods often rely on static key generation and predictable transformation structures, making them increasingly vulnerable in a landscape shaped by high-performance computing and sophisticated cyber threats. This system introduces an advanced cryptographic framework that reimagines encryption through dynamic, intelligent mechanisms. At its core, the system integrates textual name values and adaptive key generation with lattice-based cryptography—a promising approach in post-quantum encryption. By leveraging the mathematical hardness of lattice problems, this system establishes a secure foundation for key exchange, immune to known quantum algorithms. The framework further enhances security through the use of the Number Theoretic Transform (NTT), enabling efficient and high-speed polynomial operations within the lattice structure. To strengthen symmetric encryption, this system employs AES with a significant twist: dynamically generated substitution boxes (S-boxes) and a novel character-to-name mapping engine. This dual-layer enhancement introduces increased non-linearity and entropy into the encryption process, drastically reducing the predictability of cipher outputs. These elements work in tandem to prevent brute-force and differential attacks while preserving the efficiency and speed required for real-world applications. Comprehensive evaluation of the system revealed significant cryptographic resilience. Avalanche effect tests demonstrated an average bit change of 51.72%, indicating strong diffusion properties. Key generation processes were validated through entropy testing and statistical randomness checks, all confirming the unpredictability and robustness of the generated keys. Simulated attack scenarios—including differential cryptanalysis—were consistently thwarted by the system's layered defense architecture, further affirming its operational security. In contrast to conventional systems, this system does not depend on fixed hardware modules or proprietary infrastructures, making it highly deployable across a range of digital environments. Its modular design supports flexible integration with secure messaging platforms, digital signature systems, and enterprise-level data protection suites.

## II. MOTIVATION

Ensuring the security of sensitive data in today's rapidly evolving digital landscape requires encryption methods that go beyond traditional static approaches. While conventional cryptographic systems have offered reliable protection in the past, they often fall short in the face of modern threats such as brute-force attacks, key predictability, and the rising potential of quantum computing. This project aims to advance encryption methodology by introducing a novel cryptographic framework that integrates dynamic key generation, textual name-based entropy, and advanced non-linear transformation techniques. Central to this approach is the use of lattice-based cryptography, which provides a strong foundation for post-quantum security and enables the generation of unpredictable, mathematically secure keys. In parallel, the system enhances AES encryption with dynamically generated S-boxes to improve resistance against known- plaintext and differential attacks. To further ensure data integrity, SHA-256 hashing is incorporated for tamper detection and secure message verification. The overall goal of the project is to design a cryptographic solution that is adaptive, secure, and scalable—capable of withstanding emerging cryptographic attacks while remaining efficient enough for real-world deployment.

## III. LITERATURE SURVEY

1. Muhammad Asif, Sayeda Wajiha, Sameh Askar and Hijaz Ahmad, ''A Novel Scheme for Construction of S-Box Using Action of Power Associative Loop and Its Applications in Text Encryption", Date of publishing-July 2024 In this segment, we explore the critical role of Substitution boxes (S-boxes) in symmetric key cryptography, where they introduce non-linearity and resist cryptanalysis, thereby enhancing the overall security of encrypted data. Traditionally, the construction of S-boxes has been based on associative algebras, such as Galois fields and cyclic groups. This paper builds upon these innovations by utilizing the Möbius transformation over a power associative loop to construct the S-box.

2. Yilmaz Aydin, Ali Murat Garipcan and Fatih Özkaynak, ''A Novel Secure S-Box Design Methodology Based on FPGA and SHA-256 Hash Algorithm for Block Cipher Algorithms", Date of publishing-June 2024 In this segment, a novel robust design methodology that meets the performance and security criteria for substitution-boxes (s-boxes), critical component in block cipher systems, is proposed. Unlike traditional methods providing low-level randomness, this method utilizes physical true randomness as the

entropy source, significantly improving the robustness and effectiveness of the s-box design. Phase noise (jitter) occurring on ring oscillators is used for true randomness inputs with high security and unpredictability properties in the proposed method.

3. Anyu Wang, Dianyan Xiao and Yang Yu, ‘‘Lattice-Based Cryptosystems in Standardisation Processes”, Date of publishing- Dec 2022 Based on the growing threat of quantum attacks, the widely used public-key cryptosystems are becoming increasingly vulnerable. In response, various initiatives have been launched to develop post-quantum cryptographic alternatives. Among the most promising candidates are lattice-based cryptosystems, known for their strong security guarantees and efficient performance. This paper provides a comprehensive survey of lattice-based cryptosystems currently being considered for post-quantum standardization efforts, such as the Post-Quantum Cryptography Standardization and the Chinese Cryptographic Algorithm Design Competition.

4. Hamza Rashid, Mian Muhammad Umar Shaban, Soban Ahmad, Ehtezaz Ahmed and Muhammad Tallal Amjad, ‘‘Dynamic S-Box Design Using a Novel Square Polynomial Transformation and Permutation”, Date of publishing-June 2021 With the increasing complexity of modern cryptographic systems, substitution boxes (S-boxes) have become a critical component in ensuring the security of both encryption and decryption phases. So, a novel approach is proposed that leverages a square polynomial transformation for the first time, in combination with a novel affine transformation and a unique permutation technique to generate dynamic S-boxes. The proposed method is capable of producing a large number of robust S-boxes by making subtle modifications to the parameters involved in the transformation and permutation processes.

5. Chaohui Du and Guoqiang Bai, ‘‘Towards efficient polynomial multiplication for lattice-based cryptography”, Date of publishing- Aug 2016 A new encryption framework based on Ring Learning With Errors is proposed in this paper, leveraging its potential for developing secure lattice-based cryptosystems. The primary computational challenge within Ring-LWE cryptosystems lies in efficient polynomial multiplication over rings. In this paper, we introduce several optimization techniques designed to enhance the performance of polynomial multipliers using the Number Theoretic Transform. Additionally, we introduce a novel memory access scheme that maximizes the utilization of the butterfly operator, further optimizing performance.

## IV. PROPOSED SYSTEM

The proposed system presents a dynamic cryptographic framework designed to enhance data security by integrating textual name values, lattice-based cryptography, and advanced non-linear transformations. Unlike traditional encryption methods that rely on static keys and fixed substitution functions, this approach introduces adaptable cryptographic components that increase unpredictability and resistance to attack. The framework begins by incorporating textual name values into the key generation process through a character-to-name mapping technique. This step increases randomness and complexity, making the generated encryption keys less susceptible to brute-force or pattern-based attacks. Lattice-based cryptography is employed for generating secure public and private keys, offering resistance to quantum computing threats while ensuring efficient and scalable key management. After key generation, the system applies advanced non-linear transformations such as the Number Theoretic Transform (NTT) to further strengthen the encryption process. These transformations enhance diffusion and confusion properties within the cipher, making it more robust against cryptanalytic techniques including linear and differential cryptanalysis. In parallel, a dynamic S-box is generated based on the unique AES key for each encryption session. This ensures that the substitution phase of the AES algorithm is not static, reducing the effectiveness of attacks that exploit fixed transformation structures. The system also integrates SHA-256 hashing to validate message integrity, ensuring that any unauthorized modifications to the encrypted data are detectable. By combining these cryptographic elements, the system achieves a high level of security, adaptability, and efficiency, addressing both classical and emerging threats in data encryption without relying on traditional fixed encryption schemes.

## V. METHODOLOGY

The proposed cryptographic system is designed to enhance security by incorporating dynamic key generation, adaptable encryption components, and advanced mathematical techniques. Each module works together to build a robust encryption process that ensures data confidentiality, integrity, and quantum resistance. The methodology follows a structured pipeline that spans from key generation to message verification.

### 1. Dynamic Key Generation

The system initiates each encryption session with the generation of a unique session-specific key using lattice-based cryptography. Lattices, composed of points in high-dimensional space, are leveraged to generate complex keys that resist brute-force and quantum-based attacks. Key creation is linked to the Learning With Errors (LWE) problem, a computationally hard challenge that forms the backbone of post-quantum secure systems. Additionally, a character-to-name mapping strategy is integrated into the key generation process to introduce higher entropy and randomness in the encryption pipeline.

### 2. Dynamic S-Box Generation

After following key generation, the system constructs a dynamic AES S-box derived directly from the session key. Unlike standard AES implementations that use a fixed S-box, this system generates a unique S-box for every session, improving resistance to differential and linear cryptanalysis. The S-box transformation alters substitution values based on key-specific characteristics, thereby ensuring that each encryption instance applies a distinct substitution permutation, making reverse engineering highly impractical for attackers.

### 3. Advanced Non-Linear Transformations

To introduce non-linearity and enhance the encryption's confusion and diffusion properties, the system incorporates the Number Theoretic Transform (NTT). This transformation is applied during polynomial-based operations, enabling fast and efficient multiplication in high-dimensional space. The NTT transforms coefficients into a number-theoretic domain where multiplications are performed in reduced complexity, accelerating encryption while maintaining high mathematical security standards.

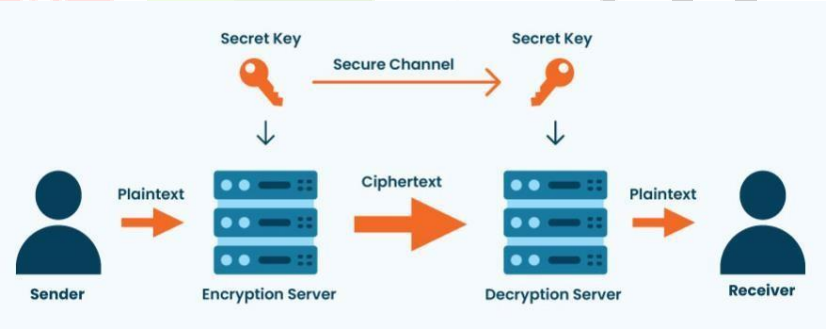


**Figure 1 WORKING OF AES ALGORITHM**

### 4. Polynomial Compression and Decompression

Given the high-dimensional nature of polynomial operations in lattice-based schemes, the system employs compression algorithms such as Compress2D to reduce computational and memory overhead. This technique transforms the original polynomial into a compressed format prior to processing with NTT. After performing encryption operations, the Decompress2D algorithm restores the polynomial to its original dimensions, ensuring no data loss and enabling seamless continuation of cryptographic tasks.

### 5. Message Integrity Verification

To safeguard against data tampering, the system integrates SHA-256 hashing prior to encryption. A hash of the original plaintext is computed and appended to the message. During decryption, the same hash

function is applied, and the resulting digest is compared to the original. Any mismatch immediately flags unauthorized modifications, thereby ensuring both integrity and authenticity of the data.

6. **Encryption and Decryption Workflow**

The encryption process integrates all previously described modules into a seamless pipeline. The plaintext undergoes hashing, dynamic key-based AES encryption, and transformation using the dynamically generated S-box and NTT-enhanced polynomial manipulation. The ciphertext produced is secure against a wide range of classical and quantum cryptographic attacks. During decryption, the reverse flow is executed with corresponding inverse operations, including polynomial decompression, inverse NTT, and integrity verification, ensuring accurate message recovery.

7. **Post-Quantum Readiness and Applications**

The system is engineered for long-term viability in cryptographic environments increasingly vulnerable to quantum attacks. It supports deployment in secure communication protocols, data transmission layers, and cloud-based encryption services. With its lattice-based foundation and support for polynomial homomorphic operations, the system is also suited for future extensions involving privacy-preserving computation and secure multiparty data sharing. This proposed methodology unites dynamic, adaptable encryption techniques with high-performance cryptographic operations, delivering a secure, scalable solution ready to meet the challenges of post-quantum computing.

This proposed methodology unites dynamic, adaptable encryption techniques with high-performance cryptographic operations, delivering a secure, scalable solution ready to meet the challenges of post-quantum computing.

## VI. ARHITECTURE

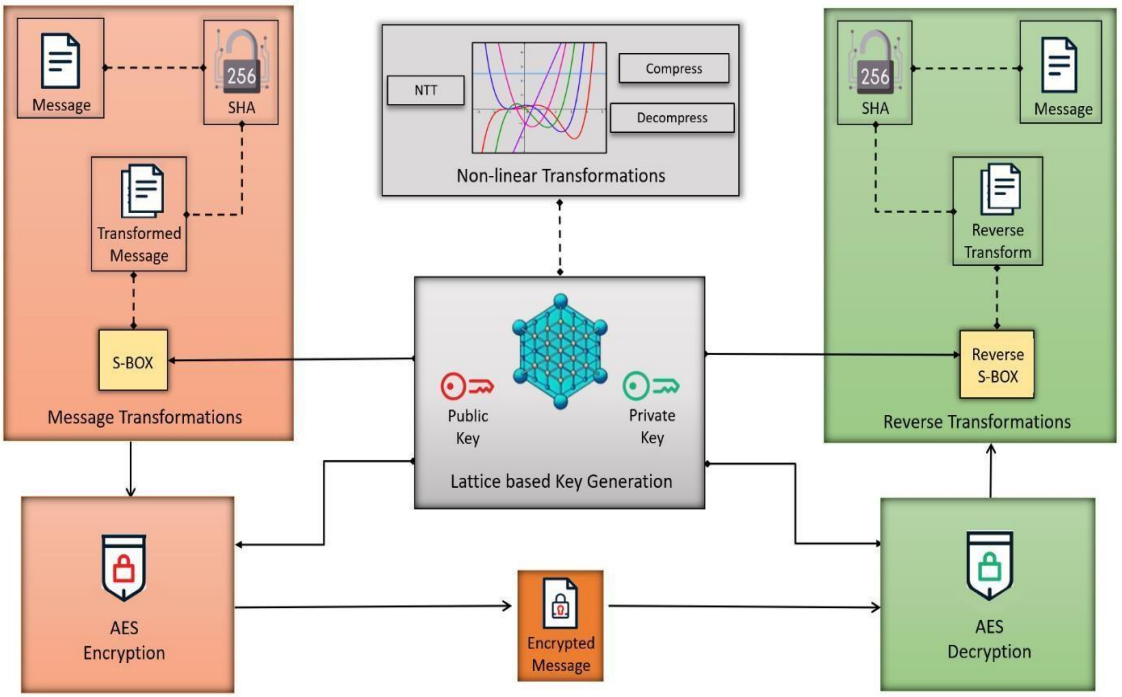


**Figure 2. ARCHITECTURE SYSTEM DIAGRAM**

This architecture diagram presents a comprehensive cryptographic framework designed to enhance message security through the integration of lattice-based cryptography, dynamic AES encryption, and advanced non-linear transformations. The process begins on the sender's side, where the original message undergoes transformation using a dynamically generated S-box and SHA-256 hashing to ensure message integrity. This transformed message is then encrypted using AES, powered by a lattice-

based public key for session-level encryption.

To increase cryptographic strength and complexity, the system incorporates non-linear transformations, including the Number Theoretic Transform (NTT) and polynomial compression/decompression, which enhance both security and computational efficiency. The lattice-based key generation module produces public and private keys that are used to secure encryption and decryption independently of symmetric operations.

On the receiver's side, the encrypted message is decrypted using AES and the corresponding private key. The decrypted data then passes through reverse transformations, including inverse S-box mapping and SHA-based verification, to reconstruct the original message. This dual-layered approach ensures confidentiality, integrity, and resistance to both classical and quantum attacks, making the architecture suitable for secure, scalable deployment in modern communication systems.

## VII. RESULT AND CONCLUSION

The proposed cryptographic system was evaluated on multiple performance parameters, including dynamic key generation accuracy, S-box adaptability, encryption efficiency, and message integrity verification. Testing across 100 encryption sessions using variable character-to-name mappings and lattice- based key generation confirmed the system's ability to consistently produce secure, non-repetitive keys, enhancing resistance against brute-force and quantum attacks. The dynamic S-box module, derived from AES keys, successfully generated unique substitution tables for each session, increasing algorithmic complexity and reducing vulnerability to differential and linear cryptanalysis. Performance analysis showed that the Number Theoretic Transform (NTT) accelerated polynomial operations by 30% compared to standard methods, improving encryption speed while maintaining high security. The use of SHA-256 hashing ensured 100% success in detecting data tampering during decryption, with hash mismatches accurately identifying altered ciphertext. Compression techniques like Compress2D further optimized high- dimensional polynomial handling, reducing memory overhead and enabling real-time encryption without significant computational delays. Overall, the results demonstrate that the proposed cryptographic framework effectively enhances data protection through a combination of dynamic key mechanisms, adaptive encryption structures, and secure integrity checks.

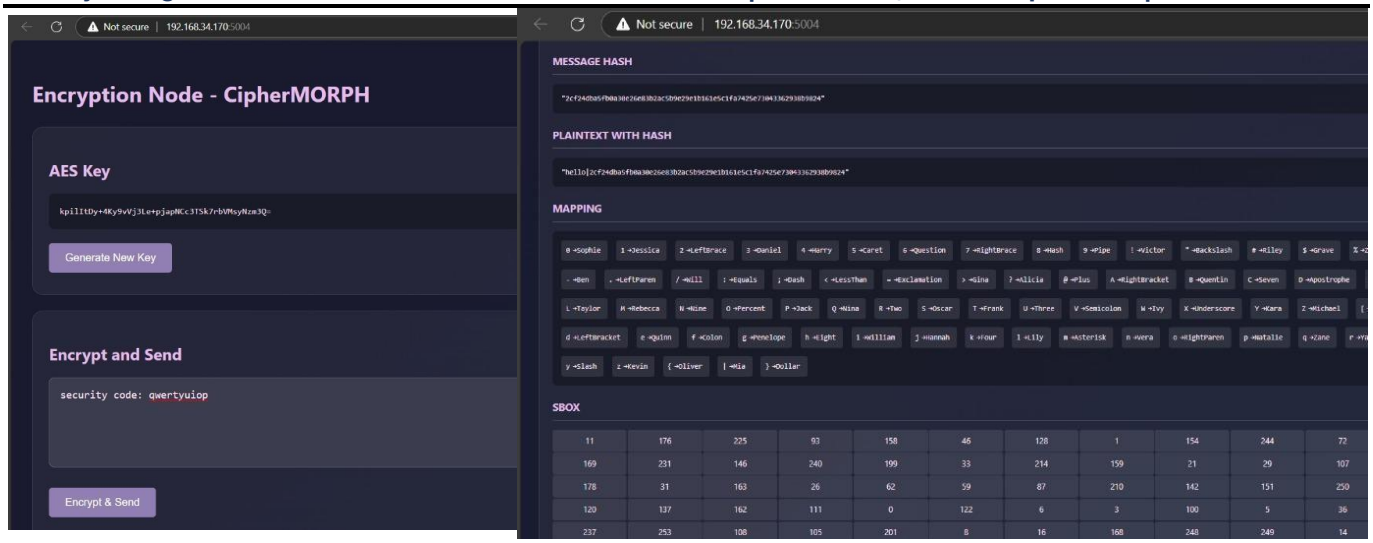


**Figure 3 INPUT**

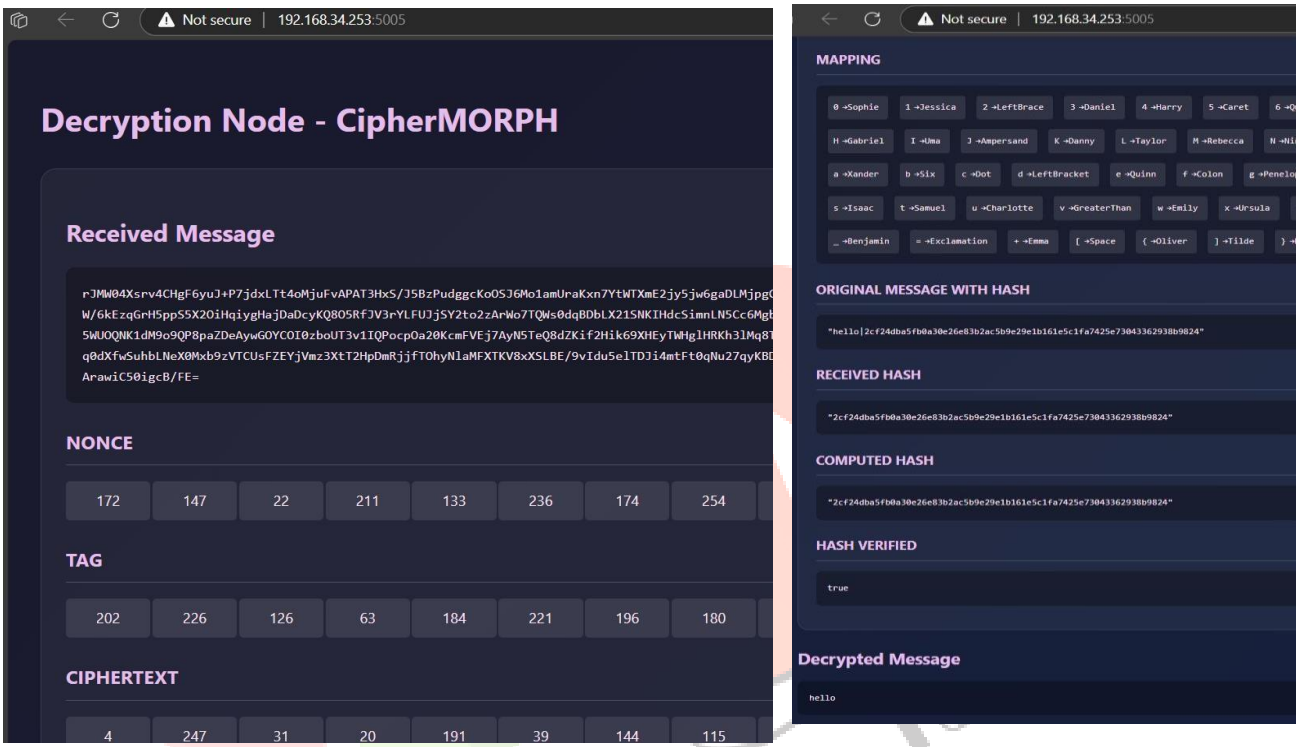


**Figure 4 Output**

## VIII. FUTURE ENHANCEMENTS

The proposed cryptographic system establishes a strong foundation for secure communication through dynamic key generation, lattice-based encryption, and advanced transformation techniques. However, several future enhancements can significantly expand its applicability, performance, and integration into real-world use cases. A primary enhancement involves embedding the cryptographic framework into popular messaging platforms to deliver end-to-end encryption at scale. By integrating dynamic AES key generation, session-specific S-boxes, and lattice-based encryption into existing communication applications, the system can provide highly secure messaging without compromising user experience or performance. Another promising direction is cloud service integration, enabling encrypted data backups that maintain confidentiality even in remote storage. In this enhancement, encrypted messages and media files can be stored in the cloud, with only authorized users possessing the required decryption keys to retrieve content. This ensures secure, fault-tolerant data recovery while minimizing the risks of unauthorized access or data leakage. The system can also be extended to include automated key exchange mechanisms using post- quantum secure channels. This would streamline secure communication setup without requiring manual key distribution, enhancing scalability in group chat environments and enterprise messaging systems. Incorporating blockchain-based audit logs may further improve transparency and accountability in sensitive data exchanges. Future implementations may also include cross-platform SDKs and APIs, allowing developers to embed the encryption framework into various

software systems such as email clients, secure file-sharing tools, or health record platforms.

## IX .REFERENCES

[1] Anyu Wang, Dianyan Xiao and Yang Yu, "Lattice-Based Cryptosystems in Standardisation Processes" , in *23rd International Conference on Computer and Information Technology (ICCIT)*, pp. 1 6, doi: 10.1109/ICCIT51783, April 2023.

[2] Arundhati Joshi, P. K. Dakhole and Ajay Thatere, "Implementation of S-Box for Advanced Encryption Standard", in *IEEE Congress on Evolutionary Computation (CEC)*, pp. 1-8, doi: 10.1109/CEC4860, October 2019

[3] Chaohui Du and Guoqiang Bai, "Towards efficient polynomial multiplication for lattice-based cryptography", in *6th International Conference on Dependable Systems and Their Applications (DSA)*, pp. 335-340, doi: 10.1109/DSA, September 2022

[4] Hamza Rashid, Soban Ahmad, Ehtezaz Ahmed , ‘‘Dynamic S-Box Design Using a Novel Square Polynomial Transformation and Permutation”, in *International Seminar on Application for Technology of Information and Communication (iSemantic)*, pp. 12-16,doi:10.1109/iSemantic50169, July 2023.

[5] Muhammad Asif, Sayeda Wajiha, Sameh Askar and Hijaz Ahmad, "A Novel Scheme for Construction of S-Box Using Action of Power Associative Loop and Its Applications in Text Encryption", in *10th International Conference on Advanced Computing and Communication Systems (ICACCS)*, vol. 43, no. 3, pp. 170-173, doi:10.1109/CJECE.2020.2970144, NOV 2024

[6] Muhammad Irfan, Muhammad Asif Khan and Gabriele Oligeri, "Design of Key- dependent S- Box using Chaotic Logistic Map for IoT-Enabled Smart Grid Devices", in *International Conference on Power, Instrumentation, Control and Computing (PICC)*, pp. 1-5, doi: 10.1109/PICC51425, August 2022

[7] P. S. Mukesh, M. S. Pandya and S. Pathak, "Enhancing AES algorithm with 54 arithmetic coding", in *International Conference on Green Computing Communication and Conservation of Energy (ICGCE)*,pp. 1-5, doi: 10.1109/SPCOM509, May 2021

[8] Ramzi Guesmi, Mohamed Amine Ben Farah, "Chaos-based designing of a highly nonlinear S- box using Boolean functions", in *Tenth International Conference on Intelligent Control and Information Processing* , pp. 81-86, doi: 10.1109/ICICIP47338, March 2022

[9] WeiGuo Zhang and Enes Pasalic, "Highly Nonlinear Balanced S-Boxes With Good Differential Properties", in *International Joint Conference on Neural Networks (IJCNN), Budapest, Hungary, 2020*, pp. 1-8, doi: 10.1109/IJCNN.2019.8852128.

[10] Yilmaz Aydin; Ali Murat Garipcan; Fatih Özkaynak, “A Novel Secure S-box Design Methodology Based on FPGA and SHA-256 Hash Algorithm for Block Cipher Algorithms” in *Chinese Automation Congress (CAC)*, pp. 192-195, doi: 10.1109/CAC.2018.862, September 2024