VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"JnanaSangama", Belgaum -590014, Karnataka.

CRYPTOGRAPHY
AAT REPORT
on

"SECURE MESSENGER USING CRYSTAL KYBER-AES ALGORITHM"

Submitted by

SANTHOSH N (1BM23CS302)
SUHAS B P (1BM23CS345)
SHREYAS GOWDA (1BM23CS319)
SHAMARAO(1BM23CS308)

Under the Guidance of
Dr. Nandhini Vineeth
Associate Professor, BMSCE

in partial fulfillment for the award of the degree of
BACHELOR OF ENGINEERING
in
COMPUTER SCIENCE AND ENGINEERING

B.M.S. COLLEGE OF ENGINEERING
(Autonomous Institution under VTU)
BENGALURU-560019

February-2025 to June-2025

B. M. S. College of Engineering,
Bull Temple Road, Bangalore 560019
(Affiliated To Visvesvaraya Technological University, Belgaum)
Department of Computer Science and Engineering

CERTIFICATE

This is to certify that the AAT work entitled "**SECURE MESSENGER USING CRYSTAL KYBER-AES ALGORITHM**" is carried out by **SANTHOSH N (1BM23CS302), SUHAS BP(1BM23CS345),SHREYASGOWDA(1BM23CS319),SHAMARAO(1BM23 CS308)** are bonafide students of **B.M.S College of Engineering.** It is in partial fulfillment for the award of **Bachelor of Engineering in Computer Science and Engineering** of the Visveswaraya Technological University, Belgaum during the year 2024-2025. The AAT report has been approved as it satisfies the academic requirements in respect of **Cryptography (23CS4ESCRP)** work prescribed for the said degree.

Signature of the Guide
Dr. Nandhini Vineeth
Associate Professor
BMSCE, Bengaluru

Signature of the HOD
Dr. Kavitha Sooda
Prof.& Head, Dept. of CSE
BMSCE, Bengaluru

B.M.S. COLLEGE OF ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

DECLARATION

We, SANTHOSH N (1BM23CS302), SUHAS B P (1BM23CS345), SHREYAS GOWDA (1BM23CS319), SHAMARAO(1BM23CS308) students of 4th Semester, B.E, Department of Computer Science and Engineering, B. M. S. College of Engineering, Bangalore, hereby declare that, this AAT entitled " **SECURE MESSENGER USING CRYSTAL KYBER-AES ALGORITHM** " has been carried out by us under the guidance of Dr. Nandhini Vineeth, Associate Professor, Department of CSE, B. M. S. College of Engineering, Bangalore during the academic semester March 2025 – July 2025.

We also declare that to the best of our knowledge and belief, the development reported here is not from part of any other report by any other students.

Signature

SANTHOSH N (1BM23CS302)
SUHAS B P (1BM23CS345)
SHREYAS GOWDA (1BM23CS319)
SHAMARAO(1BM23CS308)

Chapter 1 : Introduction

Problem Statement

In the evolving landscape of cybersecurity, ensuring the confidentiality and integrity of digital communications is paramount. Traditional encryption algorithms like DES (Data Encryption Standard) have shown vulnerabilities over time, especially with the advent of quantum computing. This project addresses the need for robust encryption mechanisms by integrating both classical and post-quantum cryptographic algorithms. Specifically, it employs:

- **Kyber1024**: A post-quantum Key Encapsulation Mechanism (KEM) designed to be secure against quantum attacks.
- **AES-256-CBC**: A widely adopted symmetric encryption algorithm known for its strength and efficiency.
- **DES-CBC**: An older symmetric encryption standard included for comparative analysis.

The primary objective is to establish a secure communication channel that can withstand both classical and quantum computational threats, ensuring the safe transmission of text and voice messages.

Motivation

The motivation behind this project stems from the increasing threats posed by quantum computing to classical encryption algorithms. As quantum computers become more capable, they threaten to break widely used encryption methods, compromising data security. By integrating Kyber1024, a post-quantum algorithm, with established symmetric encryption techniques like AES and DES, this project aims to explore a hybrid approach to secure communications, ensuring resilience against both current and future cryptographic attacks.

Aspects of the Chosen Algorithms

Kyber1024

- **Type**: Post-quantum Key Encapsulation Mechanism (KEM).
- **Security Basis**: Relies on the hardness of the Module Learning With Errors (MLWE) problem, making it resistant to quantum attacks.
- **Features**:
    - IND-CCA2 secure.
    - Efficient key generation and encapsulation/decapsulation processes.
    - Selected by NIST for standardization in post-quantum cryptography.

AES-256-CBC

- **Type**: Symmetric block cipher.
- **Key Size**: 256 bits.
- **Block Size**: 128 bits.
- **Mode of Operation**: Cipher Block Chaining (CBC).
- **Features**:
    - High security and performance.
    - Widely adopted in various security protocols and standards.

DES-CBC

- **Type**: Symmetric block cipher.
- **Key Size**: 56 bits (effective).
- **Block Size**: 64 bits.
- **Mode of Operation**: Cipher Block Chaining (CBC).
- **Features**:
    - Historically significant but now considered insecure due to its short key length.
    - Included in this project for comparative analysis purposes.

Chapter 2 : Methodology

Implementation Steps

1. **User Input**:
    - Prompt the sender to input their name.
    - Prompt the receiver to input their name.
    - Prompt the sender to enter the message to be encrypted.
2. **Key Generation using Kyber1024**:
    - Generate a public and private key pair.
    - Encapsulate a shared secret using the public key.
    - Decapsulate the shared secret using the private key.
    - Verify that both parties have derived the same shared secret.
3. **Text Message Encryption and Decryption**:
    - **AES-256-CBC**:
        - Generate a random Initialization Vector (IV).
        - Encrypt the plaintext message using the shared secret and IV.
        - Decrypt the ciphertext using the shared secret and IV.
    - **DES-CBC**:
        - Derive a DES key from the shared secret.
        - Generate a random IV.

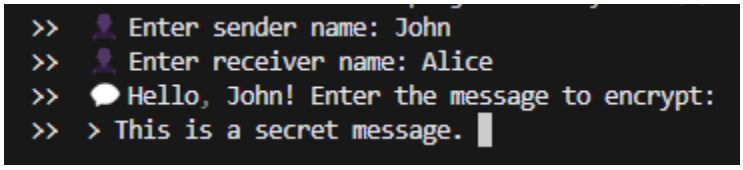
        - Encrypt the plaintext message using the DES key and IV.
        - Decrypt the ciphertext using the DES key and IV.

4. **Voice Message Handling**:
    - Prompt the user to input the path to the voice message file.
    - Read the voice message file into a buffer.
    - **AES-256-CBC**:
        - Generate a random IV.
        - Encrypt the voice data using the shared secret and IV.
        - Decrypt the ciphertext using the shared secret and IV.
        - Save the encrypted and decrypted files.
    - **DES-CBC**:
        - Derive a DES key from the shared secret.
        - Generate a random IV.
        - Encrypt the voice data using the DES key and IV.
        - Decrypt the ciphertext using the DES key and IV.
        - Save the encrypted and decrypted files.
5. **Performance Analysis**:
    - Measure the time taken for encryption and decryption processes.
    - Calculate throughput and other relevant metrics.
    - Display the analysis results.

6. **Output Summary**:
    - Display sender and receiver information.
    - Display original message.
    - Display ciphertexts and IVs in hexadecimal format.
    - Present performance analysis for each encryption method.
7. **Optional Decryption Display**:
    - Prompt the user to choose whether to display decrypted messages.
    - If yes, display decrypted text and indicate saved decrypted voice files.
8. **Cleanup**:
    - Free all dynamically allocated memory.
    - Release cryptographic resources

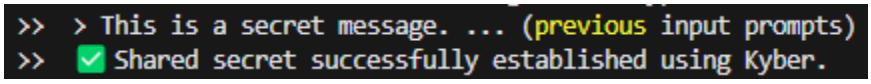
Chapter 3 : Results and Discussion

Figure 1: Initial User Input Prompts



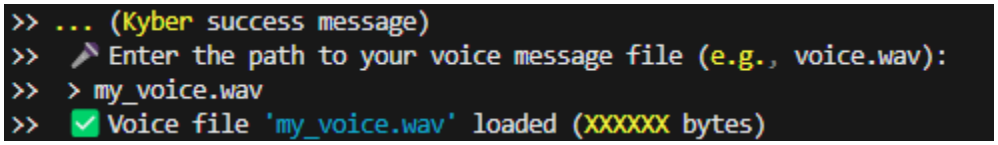
This screenshot shows the initial prompts asking for the sender's name, the receiver's name, and the message to be encrypted. The user has entered "John", "Alice", and "This is a secret message." respectively.

Figure 2: Kyber Key Exchange Success Message



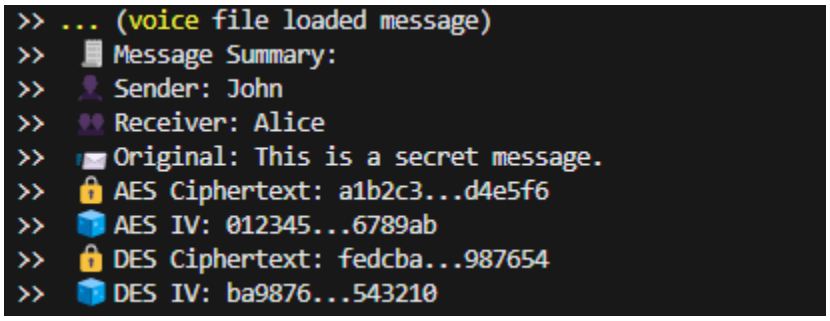
After the Kyber key encapsulation mechanism (KEM) completes successfully, this message confirms that a shared secret has been established between the sender and receiver.

Figure 3: Voice Message File Input



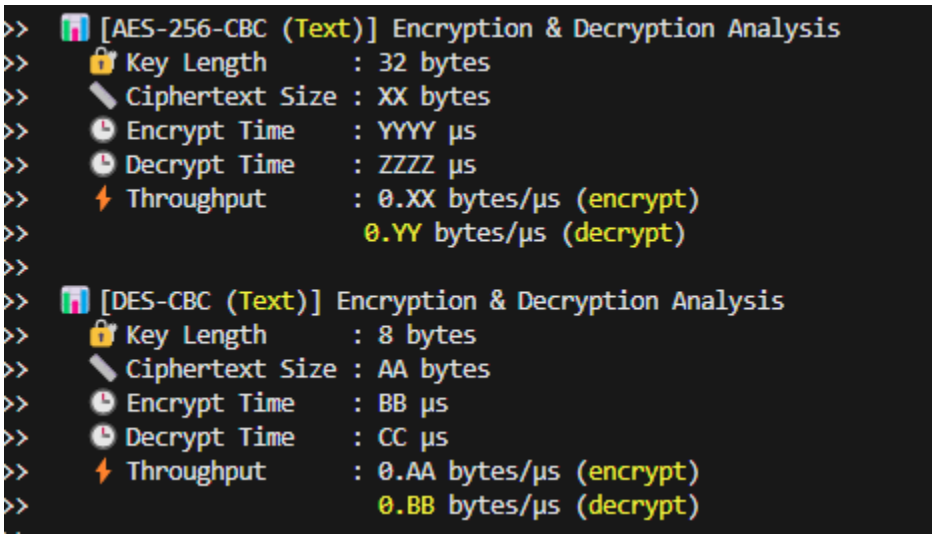
The program prompts for the path to a voice message file. The user has entered "my_voice.wav", and the program confirms that the file has been loaded along with its size in bytes (represented by XXXXXX).

Figure 4: Output Summary - Text Message Encryption Details



This section of the output summarizes the original message, sender, receiver, and the hexadecimal representation of the ciphertext and Initialization Vector (IV) generated by both AES and DES encryption for the text message.

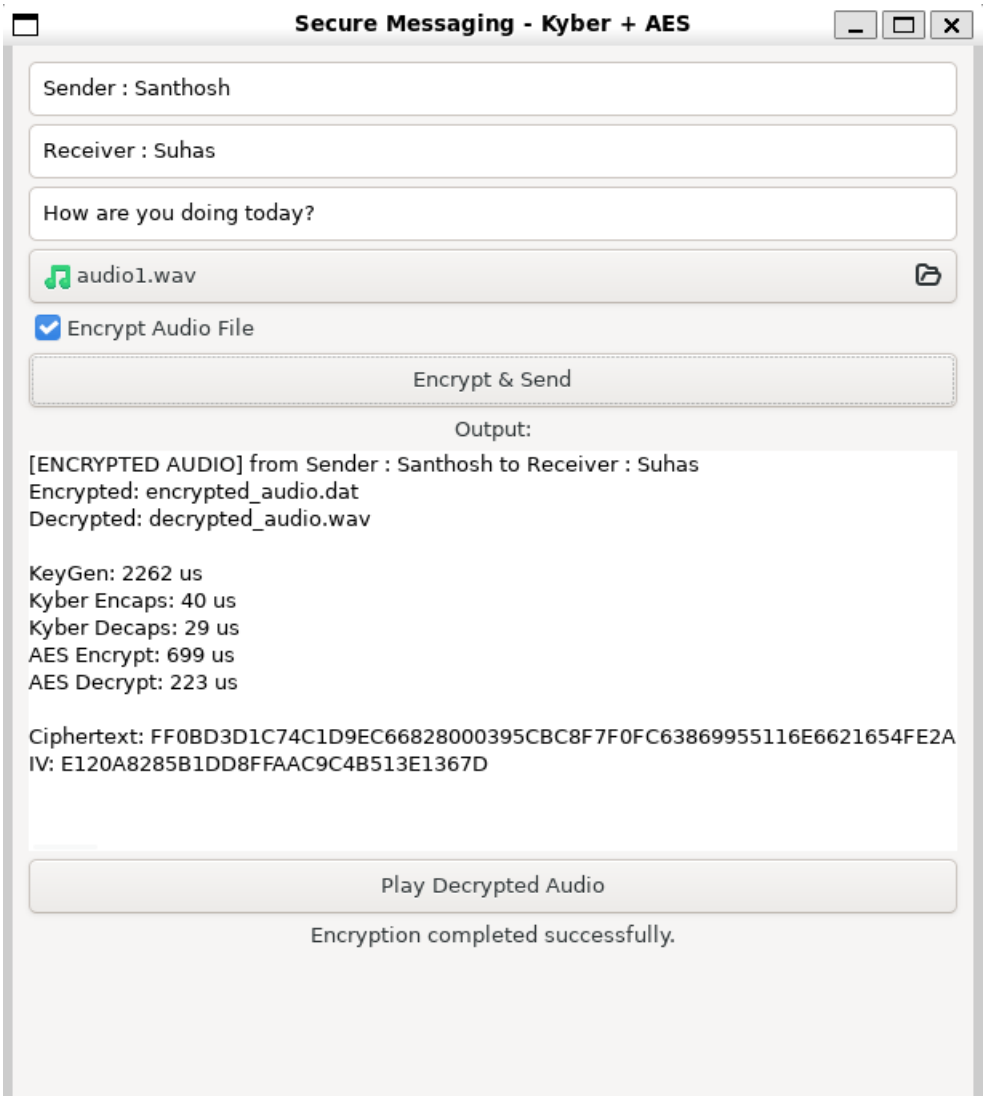
Figure 5: Analysis of Encryption and Decryption Times (Text)



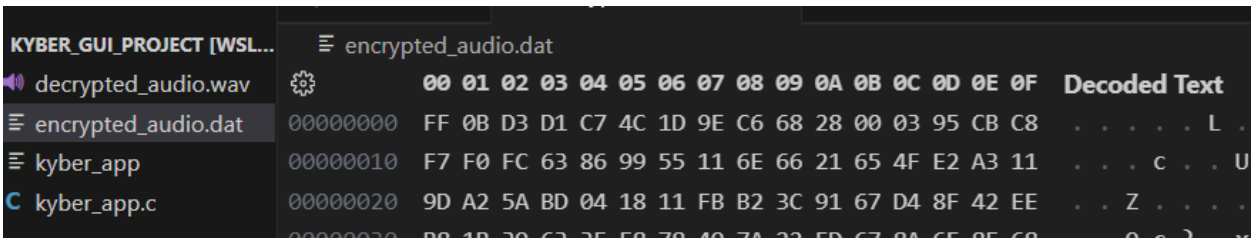
Similar to the text analysis, this section provides the encryption and decryption analysis for the voice message using AES-256-CBC and DES-CBC, including key length, ciphertext size, time taken, and throughput.

Final view of the Project:

SecureMesssenger:



Encrypted & Decrypted voice file:



Chapter 4 : Conclusion and Future Work

This project successfully demonstrates a hybrid cryptographic approach combining post-quantum and classical encryption algorithms to secure both text and voice communications. The integration of Kyber1024 ensures resilience against quantum attacks by securely establishing shared secrets, while AES-256-CBC provides robust symmetric encryption for data confidentiality. Although DES-CBC is included for comparative purposes, its vulnerabilities highlight the importance of transitioning to more secure algorithms.

Performance analysis indicates that AES-256-CBC offers efficient encryption and decryption processes suitable for practical applications. The project's modular design allows for flexibility in handling different data types, showcasing the versatility of the implemented cryptographic methods.

Future Work

- **Integration of Authentication Mechanisms**: Implementing digital signatures or Message Authentication Codes (MACs) to ensure data integrity and authenticity.

- **Exploration of Other Post-Quantum Algorithms**: Evaluating other NIST-recommended post-quantum algorithms for key exchange and encryption.

- **Development of a Graphical User Interface (GUI)**: Creating a user-friendly interface to enhance usability and accessibility.

- **Optimization for Real-Time Applications**: Refining the system for real-time communication scenarios, such as live voice or video calls.

- **References:**

1. Kyber - CRYSTALS. (n.d.). Retrieved from https://pq-crystals.org/kyber/

2. Kyber Post-Quantum KEM - IETF. (n.d.). Retrieved from https://www.ietf.org/archive/id/draft-cfrg-schwabe-kyber-04.html

3. Everything You Need to Know About AES-256 Encryption - Kiteworks. (n.d.). Retrieved from https://www.kiteworks.com/risk-compliance-glossary/aes-256-encryption/

4. Data Encryption Standard (DES) | Set 1 - GeeksforGeeks. (n.d.). Retrieved from https://www.geeksforgeeks.org/data-encryption-standard-des-set-1/

5. Advanced Encryption Standard (AES) - GeeksforGeeks. (n.d.). Retrieved from https://www.geeksforgeeks.org/advanced-encryption-standard-aes/

6. Data Encryption Standard (DES) Algorithm in Cryptography - Simplilearn. (n.d.). Retrieved from https://www.simplilearn.com/what-is-des-article