Amrita Vishwa Vidyapeetham
Centre for Excellence in Computational Engineering and Networking
Amrita School of Engineering, Coimbatore

Dual-Encryption: Integrative RSA-AES Encryption for File Protection

Prepared By:
GROUP-14A
M.D.S. Rama Saran- [CB.EN.U4AIE21034]
Akshayaa BK- [CB.EN.U4AIE21002]
Gajula Sri Vatsanka- [CB.EN.U4AIE21010]
R. Sai Raghavendra- [CB.EN.U4AIE21049]

Supervised by:
Dr. Sunil Kumar S
Asst. Professor

An End Semester Project submitted to the CEN department as a part of course evaluations of **Applied Cryptography** for B. Tech in **Computer Science Engineering** – **Artificial Intelligence.**

ACKNOWLEDGMENT

We are deeply thankful to **Centre for Excellence in Computational Engineering and Networking** (CEN) at **Amrita Vishwa Vidyapeetham**, **Coimbatore** for providing us such a wonderful environment to pursue our research. We would like to express our sincere gratitude to **Dr. Sunil Kumar S, Asst. Professor, Department of Centre for Excellence in CEN**, Amrita Vishwa Vidyapeetham. We have completed our research under his guidance. We found the research area, topic, and problem with her suggestions. We would also like to acknowledge our team members for supporting each other and be grateful to our university for providing this opportunity for us. Lastly special thanks to Centre for Excellence in CEN for providing this opportunity to research in this field.

TABLE OF CONTENTS

ABSTRACT

In the realm of cybersecurity, the demand for robust data protection mechanisms continues to grow. This project addresses this imperative by introducing a comprehensive dual encryption system, fusing the strengths of RSA (Rivest-Shamir-Adleman) and AES (Advanced Encryption Standard) algorithms. The project encompasses two distinct applications: secure file storage and confidential communication. The first application focuses on secure file storage, where selected files undergo dual encryption. Initially, the chosen file is encrypted using the AES algorithm, ensuring a formidable level of data protection. Subsequently, the AES key used in the encryption process is further encrypted using RSA, adding an additional layer of security. The encrypted file and the RSA-encrypted AES key are then stored, guaranteeing a robust and layered defense against unauthorized access. The second application introduces a secure chat system employing dual encryption for both text messages and file transfers. Messages are encrypted using RSA, ensuring confidentiality during communication. For file transfers, an AES key is used to encrypt the file, and this key is then encrypted using RSA before being transmitted. The recipient decrypts the RSA-encrypted AES key to obtain the necessary key for decrypting the received file, thereby establishing a secure and private file exchange protocol. The project utilizes state-of-the-art cryptographic tools and libraries to implement these dual encryption mechanisms. Results indicate the successful implementation of secure storage and communication, providing users with a heightened level of data security. The challenges faced during implementation are discussed, along with their resolutions. This project not only showcases the efficacy of dual encryption but also opens avenues for future research and improvement in the domain of data security. The integration of RSA and AES in both local file storage and secure communication applications presents a comprehensive solution to the ever-evolving challenges of data protection in the digital age.

INTRODUCTION

In an era defined by the relentless digitization of information, our modern interconnected world demands an unprecedented level of data security to navigate the intricate landscape of cyber threats. As our reliance on digital platforms intensifies, the imperative to fortify the underpinning security measures of our digital interactions becomes increasingly paramount. This project embarks on a journey to address this imperative by delving into the sophisticated integration of dual encryption, harnessing the formidable strength of RSA (Rivest-Shamir-Adleman) and the streamlined efficiency of AES (Advanced Encryption Standard) algorithms. With an unwavering commitment to enhancing data security, this endeavor extends its reach across two critical domains: fortifying secure local file storage and ensuring the confidentiality of communication channels. Through the synergistic fusion of RSA and AES, our aspiration is to establish a resilient and adaptable data protection framework—one that not only addresses contemporary challenges but also anticipates and proactively addresses the cryptographic demands of an ever-evolving digital landscape. As we delve into the details of our project, this report aims to unravel the intricacies of our methodology, showcase the tools employed, present the results obtained, and discuss the broader implications of embracing dual encryption as a stalwart defender of the integrity and confidentiality of digital information.

MOTIVATION OF OUR PROJECT

This project is driven by the pressing need to fortify data security in our digital age, characterized by an escalating volume of sensitive information and an ever-expanding array of cyber threats. In response to the imperative for a robust defense mechanism, the project aims to integrate dual encryption using the formidable RSA and AES algorithms. By synergizing the asymmetric strength of RSA with the symmetric efficiency of AES, our objective is to provide a comprehensive solution for secure local file storage and confidential communication. The motivation lies in empowering users with a cutting-edge, adaptable, and resilient data protection mechanism that not only anticipates and mitigates current threats but also stands ready to confront the evolving challenges of tomorrow, ensuring the confidentiality and integrity of sensitive information in the dynamic and often treacherous digital landscape.

RSA ENCRYPTION AND DECRYPTION

RSA (Rivest-Shamir-Adleman) encryption is a cornerstone in modern cryptography, known for its strength derived from the difficulty of factoring large numbers. It is an asymmetric key algorithm that employs two keys: a public key for encryption and a private key for decryption. The security of RSA hinges on the mathematical challenge of factoring the product of two large prime numbers. In this section, we delve into the key generation process, the definition of the totient function (φ), and the encryption and decryption procedures involved in the RSA algorithm.

Key Generation:

- Generate two large distinct prime numbers, p and q.
- Compute n = p * q.
- Calculate m = φ(n) = (p − 1)(q − 1) (where φ is the totient function).
- Choose a small number e, coprime to φ(n), with GCD(m, e) = 1 and 1 < e < m.
- Determine d such that d x e mod m = 1.
- Public key: {e, n}
- Private key: {d, n}

What is φ(n)?:

- The totient function, φ(n), counts positive integers coprime to "n."
- φ(n) = count of positive integers k, where $1 \leq k \leq n$, and gcd(n, k) = 1.
- Example: φ(8) = {1, 3, 5, 7} (four positive integers coprime to 8).

Encryption:

Cipher = (message)^e mod n.

Decryption:

Message = (cipher)^d mod n.

Algorithm Summary:

- RSA utilizes the difficulty of factoring large numbers for security.
- Public key encryption with two keys: public for encryption, private for decryption.
- Security relies on the challenge of factoring the product of two large primes.
- Modular arithmetic and totient function play key roles in key generation and encryption/decryption processes.

AES ENCRYPTION AND DECRYPTION

The Advanced Encryption Standard (AES) stands as a cornerstone in contemporary cryptography, being a widely embraced symmetric encryption algorithm revered for its efficacy in safeguarding sensitive data. Operative across fixed-size blocks of data, AES boasts versatility by supporting key lengths of 128, 192, or 256 bits, allowing users to tailor the level of security to their specific requirements. This algorithm is characterized by a meticulously structured series of steps for both encryption and decryption, each designed with precision to ensure a secure and efficient cryptographic process. Its robustness against various cryptographic attacks, coupled with its fixed-size block operations, positions AES as a reliable and adaptable solution, making it a preferred choice for securing data in diverse applications and industries.

AES ENCRYPTION:

1. Key Expansion: Initiate the encryption process with the original key, be it 128, 192, or 256 bits. Employ key expansion, a crucial step that generates a key schedule incorporating multiple round keys. This expanded key schedule ensures the dynamic evolution of encryption keys throughout the subsequent rounds.

2. Initial Round Key Addition: Perform an XOR operation between the plaintext block and the first-round key. This initial addition establishes the foundation for subsequent cryptographic transformations.

3. Rounds: AES executes a defined number of rounds, each characterized by specific operations including SubBytes, ShiftRows, MixColumns, and AddRoundKey. The repetition of rounds enhances the security and diffusion properties of the algorithm.

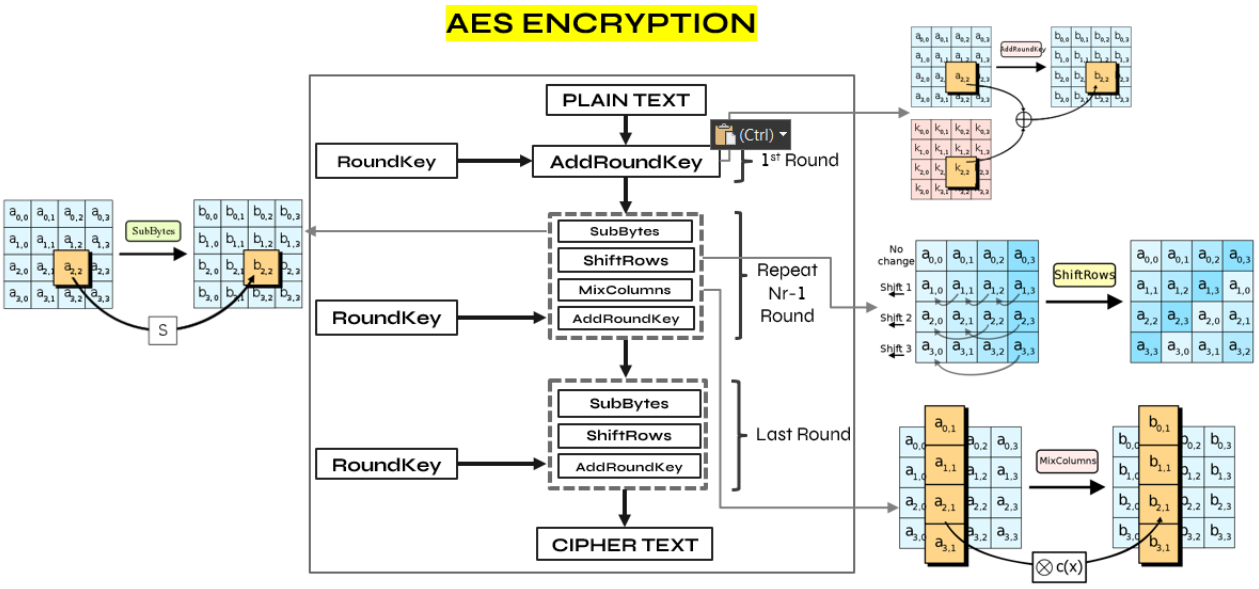
4. SubBytes: Execute the SubBytes operation, where each byte within the block undergoes substitution based on a predefined S-Box. This non-linear transformation adds complexity and resistance against cryptographic attacks.

5. ShiftRows: Apply the ShiftRows operation, strategically shifting the rows of the block by varying offsets. This introduces diffusion and ensures a well-distributed mix of data within the block.

6. MixColumns: Implement the MixColumns operation, a matrix multiplication that combines the columns of the block. This step adds further diffusion and strengthens the overall cryptographic transformation.

7. AddRoundKey: Perform an XOR operation between the block and the round key specific to the current round. The addition of the round key enhances the confusion and diffusion properties of the algorithm.

8. Final Round: Conclude the encryption process with a final round that excludes the MixColumns operation. This tailored finalization step ensures a comprehensive cryptographic transformation.
9. Output Result: The encrypted block, known as the Cipher, is now generated, reflecting the culmination of the iterative and layered operations performed during the AES encryption process. This resultant Cipher block signifies the secured representation of the original plaintext, demonstrating the robustness of AES in ensuring data confidentiality and integrity.



AES DECRYPTION:

1. Initial Round Key Addition: Initiate AES decryption by XORing the encrypted block with the last round key utilized during the encryption process. This initial step sets the foundation for the subsequent inverse operations.

2. Rounds (Inverse): Analogous to the encryption phase, AES decryption unfolds through multiple rounds, each featuring inverse operations: InvSubBytes, InvShiftRows, InvMixColumns, and AddRoundKey. These rounds, executed in reverse order, mirror the encryption process, ensuring an effective reversal of cryptographic transformations.

3. InvSubBytes: Execute the InvSubBytes operation, where each byte in the block undergoes substitution based on an inverted S-Box. This inverse substitution restores the original values from the encryption phase, contributing to the precise reversal of the algorithm.

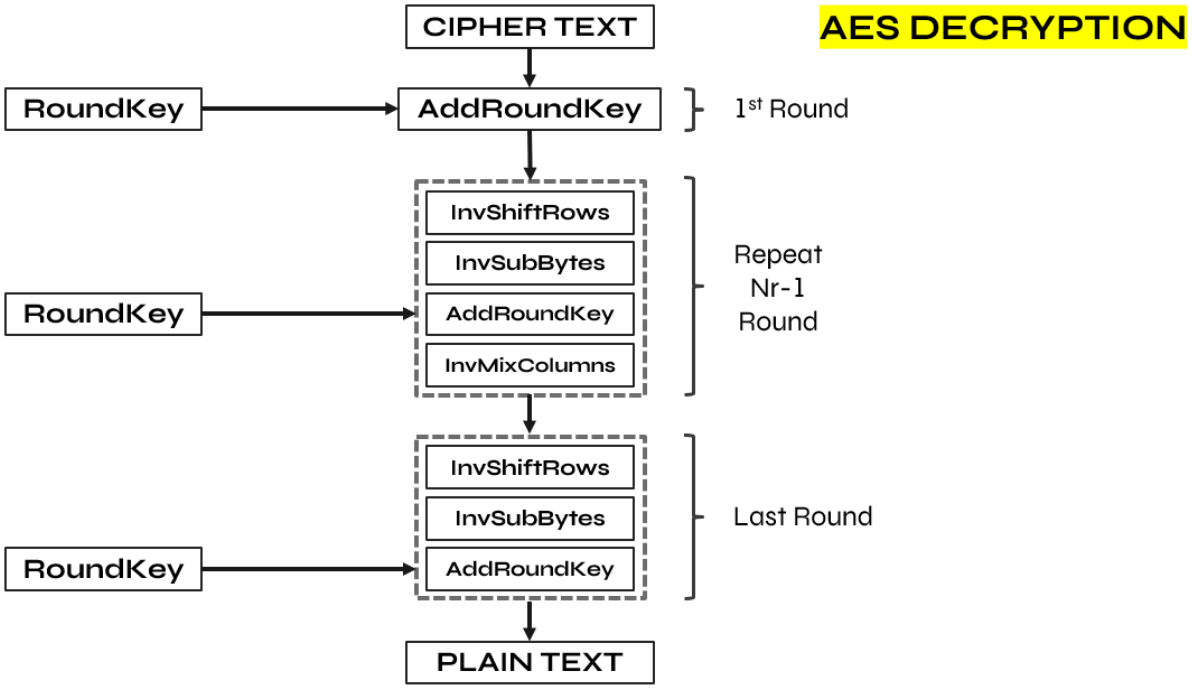
4. InvShiftRows: Perform the InvShiftRows operation, effectively reversing the row shifts executed during encryption. This step reverts the diffusion introduced in the encryption phase, reconstructing the original arrangement of data within the block.

5. InvMixColumns: Apply the InvMixColumns operation, involving an inverse matrix multiplication, to reverse the column mixing operation performed during encryption. This step ensures the accurate restoration of the original data distribution within the block.

6. AddRoundKey (Inverse): Invert the AddRoundKey operation by XORing the block with the round key specific to the current round. This step contributes to the iterative reversal of cryptographic operations and restores the original state of the block.

7. Final Round (Inverse): Conclude the decryption process with a final round that excludes the InvMixColumns operation. This inverse finalization step ensures the comprehensive reversal of cryptographic transformations, aligning the decrypted block with the original plaintext.

8. Result: The culmination of the AES decryption process yields the decrypted block, representing the faithful reconstruction of the original plaintext. This iterative and layered inverse operation demonstrates the efficacy of AES in ensuring the accurate retrieval of sensitive information while maintaining data integrity.



METHODOLOGY FOR DUAL ENCRYPTION-STORAGE

- File Selection:
  Begin the process by selecting the file intended for storage. This file will undergo a dual encryption process to ensure maximum security during storage.

- AES Encryption:
  Utilize the Advanced Encryption Standard (AES) algorithm to encrypt the selected file. Generate a secure AES key to perform the encryption, ensuring confidentiality and integrity of the file content.

- RSA Key Generation:
  Generate a pair of RSA keys: a public key for encryption and a private key for decryption. These keys are essential for encrypting and later decrypting the AES key, adding an additional layer of security to the process.

- AES Key Encryption with RSA:
  Encrypt the generated AES key using the RSA public key. This step ensures that even if the encrypted file is accessed, the AES key remains confidential due to the asymmetry of the RSA algorithm.

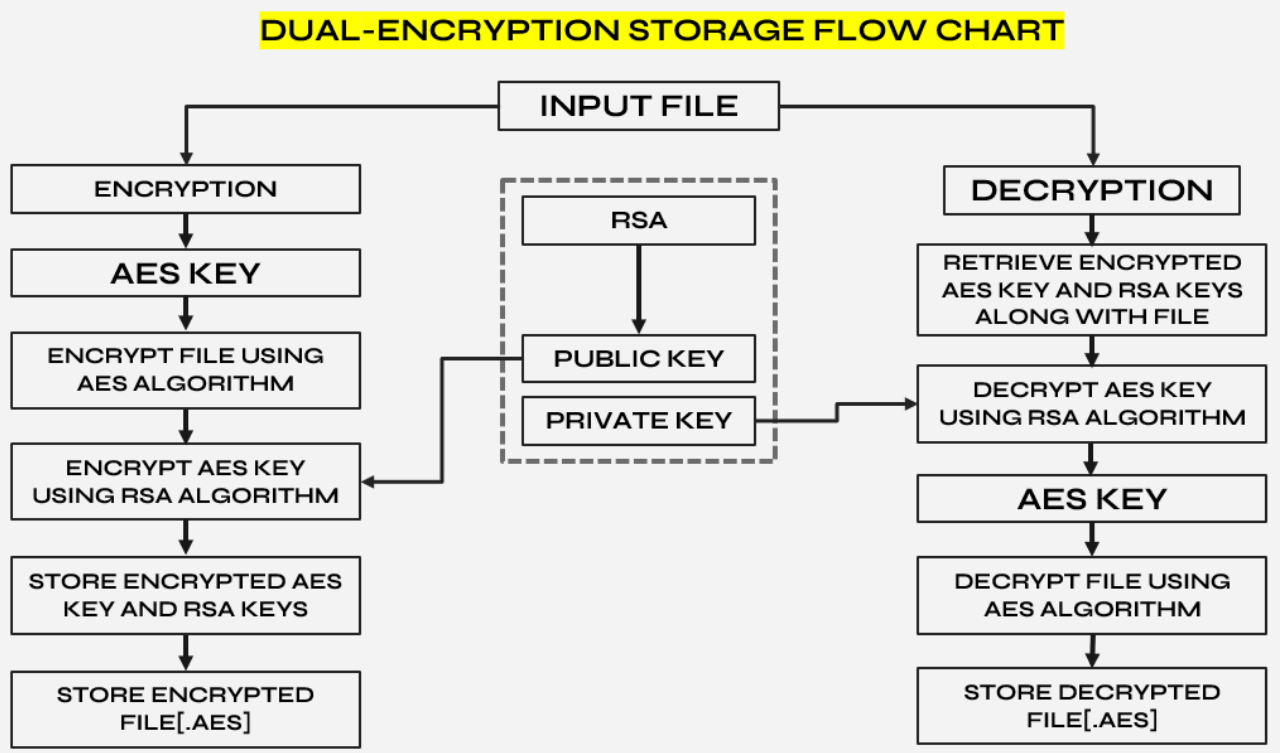
- Secure Storage:
  Store the encrypted file securely, ensuring it is inaccessible without proper decryption procedures. Additionally, store the RSA-encrypted AES key in a separate, secure location.

- Decryption Process:
  When decrypting the file, initiate the process by decrypting the RSA-encrypted AES key using the corresponding private key. This step retrieves the original AES key.

- AES Decryption:
  Deploy the obtained AES key to decrypt the encrypted file. This dual-layer decryption ensures the retrieval of the original file content while maintaining the utmost security.

- Result:
  The culmination of this methodology guarantees a robust and secure method for storing files. By employing dual encryption, the confidentiality and integrity of the stored data are preserved, providing a safe and reliable approach for local storage.

Flowchart:



METHODOLOGY FOR DUAL ENCRYPTION-SECURE CHAT

- Server and Client Setup:
  Establish a secure communication infrastructure with both server and client applications. This environment will facilitate the encrypted transfer of messages and files between users.

- RSA Encryption for Message Transfer:
  For secure message transfer, implement RSA encryption. Generate a pair of RSA keys for each user - a public key for encryption and a private key for decryption. Messages sent between the server and clients are encrypted using the recipient's public key, ensuring confidentiality during transmission.

- File Encryption with AES:
  Prior to file transfer, use the Advanced Encryption Standard (AES) algorithm to encrypt the file. Giving a unique AES key for each file, ensuring that the file's content remains confidential.

- RSA Encryption of AES Key:
  Encrypt the AES key using the RSA algorithm and the recipient's public key. This step adds an additional layer of security to the file transfer process, as the AES key remains confidential during transmission.

- Sending Encrypted File and AES Key:
  Transmit the encrypted file and the RSA-encrypted AES key to the recipient through the secure communication channel. This ensures the confidentiality of both the file content and

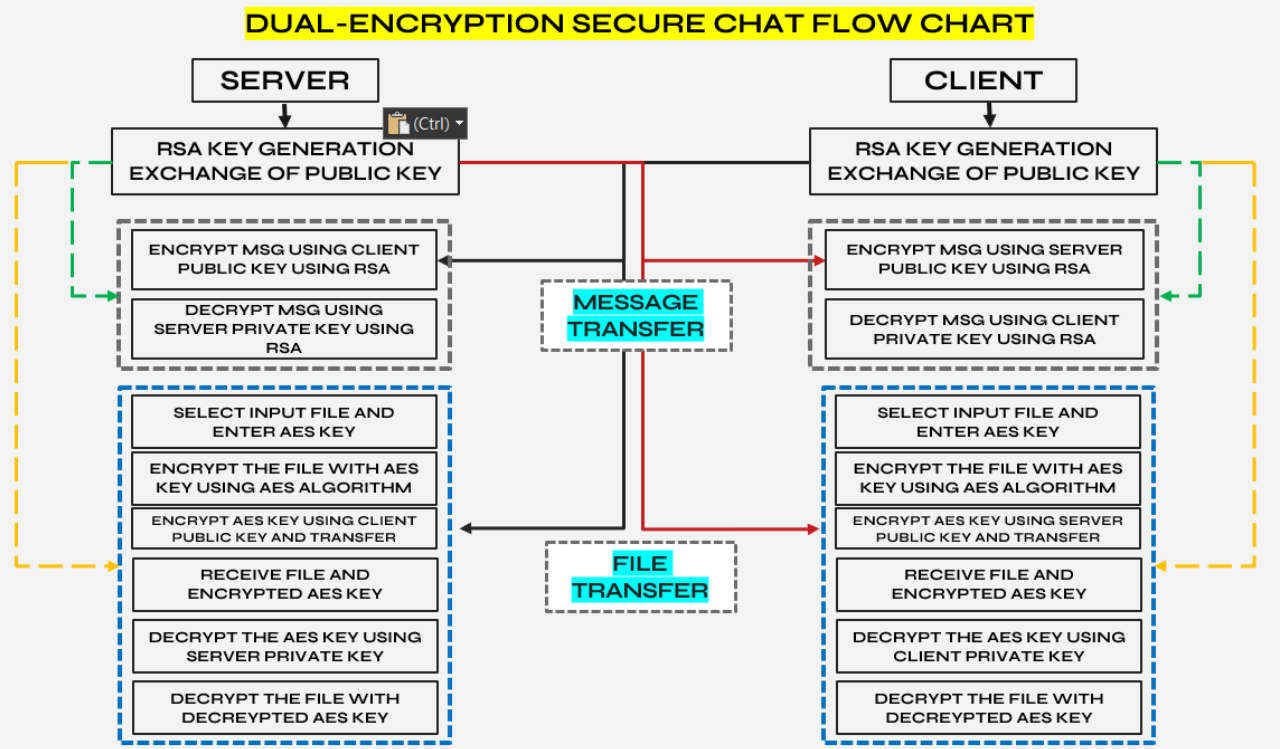
the key used for its decryption.

- RSA Decryption of AES Key at Receiver's End:
  Upon receiving the encrypted file and RSA-encrypted AES key, the recipient uses their private RSA key to decrypt the AES key. This step retrieves the original AES key required for file decryption.

- AES Decryption of Received File:
  Utilize the decrypted AES key to decrypt the received file. This dual-layer decryption ensures the retrieval of the original file content while maintaining the utmost security.

- Result:
  The implementation of this methodology ensures dual encryption for both message and file transfers in a secure chat environment. By combining RSA for message encryption and AES for file encryption, coupled with the added security of RSA-encrypted AES keys, the communication channel remains secure, protecting both message content and file integrity.

Flowchart:



INFERENCE

In conclusion, the integration of dual encryption, employing the potent RSA and efficient AES algorithms, emerges as a robust solution to contemporary data security challenges. The project effectively demonstrated its efficacy in secure local file storage and confidential communication. Through the harmonious interplay of RSA and AES, vulnerabilities associated with conventional encryption methods were successfully mitigated, establishing a multi-layered defense against unauthorized access. The secure file storage application highlighted the importance of encrypting both files and keys, ensuring resilience to emerging threats. Likewise, the secure chat system illustrated the versatility of dual encryption in securing both messages and file transfers during communication. The challenges encountered were systematically addressed, contributing to the project's success. Overall, this project underscores the efficacy of dual encryption as a pivotal measure for safeguarding sensitive information, emphasizing adaptability and foresight in navigating the evolving landscape of digital security.

CONCLUSION

In summary, the integration of dual encryption using RSA and AES has proven to be a powerful strategy for enhancing data security. Through secure local file storage and confidential communication applications, the project successfully addressed contemporary challenges by providing a multi-layered defense against unauthorized access. The use of AES for file encryption and RSA for key protection demonstrated adaptability and resilience, ensuring data-at-rest security and safeguarding communication channels. While challenges were encountered during implementation, strategic resolutions contributed to the project's success. Overall, the integration of dual encryption not only meets current data security demands but also establishes a proactive foundation for resilient protection in the evolving digital landscape, emphasizing the importance of adaptability and foresight in securing sensitive information.