SECURE EMAIL SYSTEM

(A Cryptography-Based Secure Email System Integrating RSA, AES, and SHA-512 for Confidentiality, Integrity, and Authentication)

GROUP MEMBERS:

1. CHANDU CHERUPALLY 22CSB0C20
2. MANOJ KUMAR SAMUDRALA22CSB0C23

1. INTRODUCTION

In today's digital world, email has become an essential mode of communication for both personal and professional use. People exchange sensitive information such as financial data, business documents, and personal details through emails daily. However, traditional email systems are not inherently secure, making them vulnerable to cyber threats. Attackers can exploit various security loopholes to intercept, modify, or impersonate email communications, leading to serious consequences such as data breaches, financial fraud, and identity theft. These risks highlight the need for a secure email system that ensures confidentiality, integrity, and authentication of the exchanged messages.

To mitigate these security threats, modern secure email solutions incorporate cryptographic techniques that protect the contents of an email from unauthorized access. Encryption plays a vital role in securing communication by converting readable text into an unreadable format that can only be deciphered by the intended recipient. Existing solutions such as PGP (Pretty Good Privacy) and S/MIME (Secure/Multipurpose Internet Mail Extensions) use encryption and digital signatures to secure email contents. However, these approaches often come with complex key management requirements, dependence on external certificate authorities, and the need for users to manually configure security settings, making them difficult for non-technical users to adopt. There is a need for a more automated and user-friendly secure email solution that eliminates these complexities while ensuring robust protection.

Our project, Secure Email System, is designed to provide a practical, efficient, and easy-to-use approach for securing email communication. The system ensures Confidentiality, Integrity, and Authentication (CIA) using a combination of RSA, AES, and SHA-512 hashing algorithms. Each user generates a unique pair of RSA keys (public and private) based on a password during login, ensuring that key pairs remain consistent for authentication. When User A sends an email to User B, the email content is first hashed using SHA-512 to create a unique fingerprint of the message. This hash value is then digitally signed using A's private RSA key, ensuring that the message has not been tampered with. Next, an AES encryption key is generated, which is encrypted using B's public RSA key and sent alongside the email. The actual email body is encrypted using AES encryption, ensuring that even if intercepted, it remains unreadable to unauthorized users.

Upon receiving the email, User B decrypts the AES key using their private RSA key, which allows them to decrypt the email body. To verify the authenticity of the message,

B uses A's public key to verify the signature and checks the integrity of the email by recomputing the SHA-512 hash of the decrypted content. If the computed hash matches the original signed hash, it confirms that the message has not been altered in transit.

In addition to securing email text, our system extends these security measures to file and attachment encryption, ensuring that sensitive documents and media files are also protected. This approach makes the Secure Email System comparable to standard email services but with added security layers, preventing unauthorized access or tampering. By seamlessly integrating these cryptographic techniques, our system ensures a balance between security and usability, making encrypted communication accessible without the need for advanced configurations.

2. OBJECTIVES

- Enhance Security and Data Integrity:

Develop a secure email system that ensures confidentiality, integrity, and authentication by leveraging RSA for key management, AES for message encryption, and SHA-512 for data hashing. This approach guarantees that both email content and attachments remain secure during transmission.

- Simplify Key Management and User Experience:

Implement an automated key generation mechanism that derives consistent RSA key pairs from user passwords during login, streamlining the encryption and decryption processes while providing a user-friendly interface for secure communication.

3. IMPLEMENTATION AND RESULTS ANALYSIS

3.1 Implementation Overview

The Secure Email System integrates layered cryptographic techniques to safeguard email communications. The system leverages RSA for asymmetric key management, AES for symmetric encryption, and SHA-512 for hashing to ensure message integrity and authenticity. Each user generates a unique RSA key pair derived from their login password, which guarantees consistent key usage throughout sessions. The system's core

functions include message signing, key encapsulation, encryption, decryption, and signature verification.

3.2 System Architecture and Module Breakdown

Key Generation Module

Purpose: Generate a consistent RSA key pair for each user based on their password.

Process: On login, a password-based key derivation algorithm produces RSA public and private keys.

Hashing and Signing Module

Purpose: Ensure message integrity and authenticate the sender.

Process: The email content is hashed using SHA-512. The resulting hash is then signed with the sender's private RSA key, creating a digital signature.

AES Encryption Module

Purpose: Securely encrypt the email content.

Process: A random AES key is generated to encrypt the email message. This AES key is then encrypted using the recipient's public RSA key to ensure that only the intended recipient can recover it.

Decryption and Verification Module

Purpose: Allow the recipient to retrieve and verify the original email content.

Process: The recipient decrypts the AES key using their private RSA key. With the recovered AES key, the encrypted email content is decrypted. Finally, the system verifies the digital signature by comparing the SHA-512 hash of the decrypted message with the signed hash.

3.3 Algorithms

RSA Key Generation Algorithm

Where Used: Key Generation Module

What It Achieves: Generates a consistent pair of RSA keys (public and private) for each user based on their password.

Outline:

1. User inputs password.

2. Use password-based key derivation (PBKDF2) to derive a secure seed.

3. Generate RSA key pair (Public Key, Private Key) from the seed.

4. Store Public Key for encryption, keep Private Key secure for decryption/signing.

Real-Life Analogy: Similar to issuing a personal, unchangeable ID card at login, this algorithm ensures that only you can unlock your secured messages.

SHA-512 Hashing Algorithm

Where Used: Hashing and Signing Module

What It Achieves: Produces a unique, fixed-size fingerprint of the email content to detect any tampering.

Outline:

1. Take email content as input.

2. Apply SHA-512 hashing algorithm.

3. Generate a fixed 512-bit hash value.

4. Use hash for digital signature and verification.

Real-Life Analogy: Like a tamper-evident seal on a package, it assures both sender and receiver that the content remains unchanged during transit.

RSA Digital Signature Algorithm

Where Used: Hashing and Signing Module / Decryption and Verification Module

What It Achieves: Signs the SHA-512 hash with the sender's private key and verifies it with the sender's public key, confirming sender authenticity and message integrity.

Outline:

1. Compute SHA-512 hash of the email content.

2. Encrypt hash using the sender's Private RSA Key (Digital Signature).

3. Send signature along with the encrypted email.

4. At receiver's end:

   a. Decrypt signature using sender's Public RSA Key.

   b. Compute SHA-512 hash of the decrypted email.

   c. If hashes match, the email is authentic.

Real-Life Analogy: Functions like a handwritten signature on a document, ensuring the message comes from the stated sender and hasn't been altered.

AES Encryption Algorithm

Where Used: AES Encryption Module

What It Achieves: Encrypts the email body and attachments using a randomly generated AES key, ensuring fast and secure data encryption.

Outline:

1. Generate a random AES key.

2. Encrypt email content using AES algorithm with the AES key.

3. Encrypt the AES key using recipient's Public RSA Key.

4. Send encrypted email and encrypted AES key.

Real-Life Analogy: Similar to locking your valuables in a safe, this algorithm protects your email content from unauthorized access.

RSA Key Decryption Algorithm

Where Used: Decryption and Verification Module

What It Achieves: Decrypts the AES key using the recipient's private RSA key, allowing only the intended recipient to access the original message.

Outline:

1. Extract encrypted AES key from the received email package.

2. Decrypt AES key using recipient's Private RSA Key.

3. Use decrypted AES key to decrypt email content.

Real-Life Analogy: Comparable to using a unique key to open a personal safe deposit box, ensuring that only the rightful owner can unlock the contents.

3.4 RESULT AND ANALYSIS

Key outcomes include:

Enhanced Data Security:

The dual-layer encryption (AES for the message and RSA for key encapsulation) effectively protected the email content from unauthorized access. The SHA-512 hash and digital signature mechanism reliably detected any tampering.

Efficient Performance:

Both encryption and decryption processes were executed with minimal latency, preserving the prompt delivery of emails even when attachments were included.

User-Friendly Experience:

The automated RSA key generation based on user passwords simplified the process, making secure email communication accessible to non-technical users.

Scalability:

The system maintained robust performance during simulations of multiple concurrent communications, proving its scalability for practical use.

In summary, the Secure Email System demonstrates a robust, user-friendly approach to achieving secure email communication. The detailed diagrams and step-by-step flowcharts provide a comprehensive understanding of the system's operation, highlighting both its security features and practical efficiency.