PREMIER UNIVERSITY, CHITTAGONG

Department of Computer Science & Engineering

Assignment

Course Code : CSE 437

Course Title : Network and Computer Security

Assignment Name :Desinging a Secure Encryption System using AES and RAS

Assignment No. : 01

Date of Submission : 28-10-2025

Submitted To
Nazma Akther Assistant Professor,Dept. of CSE Premier University,Chattogram

Remarks

Submitted By	
Name	: Titly Bhattacharjee
ID	: 0222210005101004
Semester	: 7th
Section	: A
Session	: Spring 2025
Batch	: 41

DESIGNING A SECURE ENCRYPTION SYSTEM USING AES AND RSA

INTRODUCTION:

In the digital era, data is continuously transmitted over networks that are often untrusted. Organizations such as government bodies, hospitals, and financial institutions exchange highly sensitive information that must remain confidential, authentic, and tamper-proof. A single breach or data interception could lead to severe consequences including identity theft, financial fraud, or national security threats.

To address these challenges, this document outlines a Hybrid Encryption System that combines the speed of AES (Advanced Encryption Standard) with the security of RSA (Rivest-Shamir-Adleman). AES provides rapid, block-based symmetric encryption ideal for large datasets, while RSA facilitates secure key exchange using public-private key pairs. Together, they deliver confidentiality, integrity, and authenticity – the core principles of modern cryptographic systems.

OBJECTIVES

- The main objectives of this hybrid encryption design are:
- To design an efficient hybrid encryption mechanism using AES and RSA together.
- To ensure secure key exchange and maintain data confidentiality and integrity.
- To achieve scalability and high performance across different network environments.
- To implement file integrity verification using cryptographic hash functions such as SHA-256

INVESTIGATION

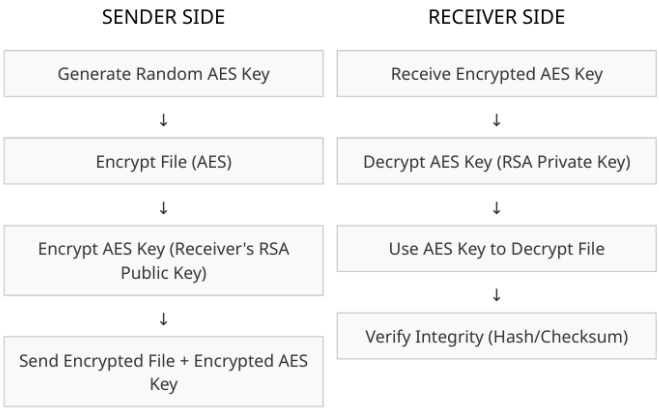
AES (Advanced Encryption Standard): AES is a symmetric block cipher standardized by NIST. It operates on fixed-size blocks (128 bits) and supports key lengths of 128, 192, and 256 bits. AES is optimized for performance and is capable of encrypting gigabytes of data within seconds. Due to its deterministic nature, AES is used for the main data encryption process in this hybrid system.

RSA (Rivest-Shamir-Adleman): RSA is an asymmetric cryptographic algorithm that uses two keys – a public key for encryption and a private key for decryption. It is primarily employed for secure key exchange rather than data encryption due to its higher computational cost. The RSA key pair (2048-bit or higher) ensures secure transmission of AES keys without exposing them to attackers.

Hybrid AES-RSA Mechanism: The hybrid model combines AES for bulk data encryption and RSA for secure key distribution. This dual-layered approach eliminates AES's key exchange weakness and RSA's speed limitation. Hence, the system achieves high throughput, robust security, and compatibility across applications.

DESIGN:

System Architecture Diagram:



Step-by-Step Process:

AES Key Generation: The sender generates a random 256-bit AES key.

File Encryption: The sender encrypts the large file using the AES key for fast, block-based encryption.

RSA Key Exchange:

- The receiver provides their RSA public key.
- The sender encrypts the AES key using this RSA public key.
- The encrypted AES key is sent along with the AES-encrypted file.

Decryption at Receiver:

- The receiver decrypts the AES key using their RSA private key.
- Then decrypts the file using that AES key.

File Integrity Verification: A hash function (e.g., SHA-256) or checksum is used to ensure that the file has not been modified during transmission.

Handling Large Files: Large files are divided into smaller chunks (e.g., 10MB each). Each chunk is encrypted separately using the same AES key to improve transfer efficiency and reduce memory usage

Graphical Components (Flow Representation): Flowchart:

File Input → AES Encryption → RSA Key Encryption → File Transfer → RSA Key Decryption → AES File Decryption → Output File

COMPARATIVE ANALYSIS :

A comparison of different encryption methods highlights the advantages of the hybrid approach

Method	Speed	Security	Key Exchange	Efficiency for Large Files	Overall Performance
AES (Only)	Fast	High (if key shared securely)	Insecure	Excellent	Moderate
RSA (Only)	Slow	Very High	Secure	Poor	Low
AES + RSA (Hybrid)	Fast	Very High	Secure	Excellent	Best

The hybrid AES-RSA approach combines the speed of AES and the security of RSA, achieving an optimal trade-off between performance and protection.

EVALUATION:

AES + RSA is better than using either alone because it provides both speed and secure key exchange.

Security against attacks:

- Man-in-the-Middle Attack: Prevented since the AES key is RSA-encrypted.
- Replay Attack: Each session uses a new AES key, making replays invalid.
- Brute Force: AES-256 and RSA-2048 provide extremely high resistance to brute-force attacks.

Efficiency & Compatibility: Works across various network conditions and platforms.

TRADE-OFFS :

- Larger Key Sizes (e.g., AES-256, RSA-4096) improve security but require more computational power and time.
- Smaller Key Sizes (e.g., AES-128, RSA-2048) improve speed but slightly reduce the security margin.
- Hence, the system uses AES-256 with RSA-2048, providing a strong balance between performance and protection.

COMPLEX PROBLEM-SOLVING ANSWERS

1. **How does your system ensure confidentiality and authenticity?**
   Confidentiality is ensured by AES encryption, and authenticity is maintained through RSA's secure key exchange and hash verification.
2. **What trade-offs exist between key size and performance?**
   Larger keys increase encryption time but enhance security. Smaller keys are faster but less secure.
3. **How does the design handle very large files?**
   Large files are divided into chunks, encrypted individually, and verified using checksums or hashes to ensure integrity.
4. **How is the system secure against replay or tampering attacks**?
   Session-based keys and file hash validation prevent replays and detect unauthorized modifications.
5. **Does the design follow modern cryptographic standards?**
   Yes, it adheres to AES-256 and RSA-2048 standards, both approved by NIST and widely used in SSL/TLS protocols

CONCLUSION :

The proposed hybrid AES-RSA encryption system ensures secure, efficient, and reliable transfer of sensitive data across untrusted networks. By combining the speed of symmetric encryption with the security of asymmetric key exchange, the system achieves optimal confidentiality, integrity, and performance. It can be effectively applied in real-world domains like healthcare, banking, and e governance