Premier University, Department of CSE
Spring 2025, 7th Semester,
Course Title: Network and Computer Security
Course Code: CSE 437
Course Outcome: CO3
Total Marks: 10
Assignment

You are tasked with designing an encryption system for the secure transfer of large sensitive files (such as medical data, financial records, or government documents) over untrusted networks. The system should use AES for fast encryption of the file data and RSA for secure exchange of the AES session key. The challenge is to provide confidentiality and integrity of the data while keeping the system efficient enough to handle large files across different network conditions.

Objectives:

1. Design an efficient encryption system using AES and RSA together
2. Ensure secure key exchange and data protection.
3. Improve performance and compatibility

Investigation:
In this task, students need to investigate how the symmetric encryption technique AES is much faster and better suited for encrypting large amounts of data, while asymmetric encryption RSA is mainly used for sending keys securely between sender and receiver. The investigation should also compare what happens if we rely only on AES or only on RSA, and why combining both gives a better result in practice

Evaluation:

- Explain why AES with RSA together is better than using only one method.
- Show how your design is secure against common attacks (man-in-the-middle, replay, brute force).
- Justify your design choices in terms of security, efficiency, and compatibility.

Design:
Draw the overall system architecture and show the steps:

- Generating a random AES key.
- Sender encrypts the file using AES.
- Sender encrypts the AES key using RSA and sends it.

Additionally, suggest how large files can be divided into smaller chunks for easier transfer, and a hash or checksum can be used to verify that the file was not changed during transmission.

Deliverables:
A handwritten assignment report should include clear system architecture diagrams of the encryption flow, graphical comparison charts, flowcharts with implementation details, a comparative analysis of hybrid AES-RSA versus symmetric-only and asymmetric-only

approaches, and an explanation of trade-offs in AES and RSA key sizes with respect to performance and security

Rubrics for Assignment marking:

Task	Criteria	Good (4-5)	Moderate (2-3)	Poor (1)
i.	Problem solution	Properly or near appropriately reasoned solution	Appropriate solution for some cases	Inappropriate or no solution
ii.	Problem analysis	In-depth analysis	Shallow analysis	Incomplete analysis

Complex Problem-Solving Questions

- How does your system ensure both confidentiality and authenticity during file transfer?
- What trade-offs did you face between security level (key size) and performance?
- How does your design handle very large files efficiently?
- How is your system secure against replay or tampering attacks?
- Does your design align with best practices and modern cryptographic standards?