# Phase I Project Report

## RSA-OAEP (SHA-256) + AES-GCM Encryption System

## 1. Introduction and Problem Definition

In today's digital communication environment, data is often transferred through email, cloud storage, or file-sharing systems that may not be secure. Without proper encryption, sensitive files can be intercepted, altered, or accessed by unauthorized parties. Encryption ensures that only authorized users can read and modify data. PDF format was chosen because it is widely used, maintains document structure, and allows embedding encrypted attachments without affecting visible content. This system solves the problem of unsafe file sharing by combining AES-GCM for authenticated encryption and RSA-OAEP (SHA-256) for secure key transfer.

## 2. Objectives and Methodology

### Main Objective

To design a hybrid encryption system combining symmetric and asymmetric algorithms for secure data transfer through PDF files.

### Sub-Objectives

- Use AES-GCM for fast and secure encryption of data.

- Use RSA-OAEP (SHA-256) for securely encrypting the AES key.

- Embed encrypted data and key into PDF files.

- Ensure data integrity using GCM authentication tags.

- Test the system under different scenarios and file sizes.

## 3. Technical Approach

1. Generate a 256-bit AES key and a 12-byte nonce.

2. Encrypt plaintext using AES-GCM (produces ciphertext + tag).

3. Encrypt the AES key using RSA-OAEP (SHA-256).

4. Create a JSON object containing nonce, ciphertext, tag, and wrapped\_key.

5. Embed the JSON into the PDF as an attachment.

6. Receiver extracts data, unwraps AES key, and decrypts using AES-GCM.

## 4. Test Scenarios

|  |  |  |
| --- | --- | --- |
| ID | Scenario | Expected Result |
| T1 | Correct key pair | Decryption successful, identical plaintext. |
| T2 | Wrong private key | Decryption fails (RSA unwrap error). |
| T3 | Modified ciphertext | AES-GCM authentication fails. |
| T4 | Nonce reuse | Security warning (not allowed). |
| T5 | Different file sizes | System functions correctly. |

## 5. Conclusion

This hybrid encryption model provides both performance and strong security. AES-GCM ensures confidentiality and integrity with minimal overhead, while RSA-OAEP guarantees secure key exchange. The system demonstrates a practical and effective approach to secure file sharing via encrypted PDF attachments.