Walchand College of Engineering, Sangli *(Government Aided Autonomous Institute)*	
AY 2025-26	
Course Information	
Programme	B.Tech. (Computer Science and Engineering)
Class, Semester	Final Year B. Tech., Sem VII
Course Code	6CS451
Course Name	Cryptography and Network Security Lab

Experiment No. 07

Title - Implementation of RSA Algorithm.

Objectives:

1. **To understand the theoretical foundation of the RSA algorithm**
   - Explore the mathematical principles behind RSA, including prime numbers, Euler's theorem, and modular exponentiation.
2. **To implement the RSA algorithm from scratch using a programming language (e.g., Python, Java, C++)**
   - Develop modules for key generation, encryption, and decryption.
3. **To ensure secure key generation**
   - Implement a method to generate large, random prime numbers and compute public and private key pairs.
4. **To demonstrate the encryption and decryption process**
   - Encrypt a plaintext message using the public key and decrypt it using the private key.
5. **To validate the correctness and performance of the implementation**
   - Test the algorithm with different input sizes and ensure accurate decryption of encrypted messages.
6. **To explore the limitations and possible optimizations of RSA**
   - Analyze time complexity, key size limitations, and potential vulnerabilities in naive implementations.

Problem Statement:

In the current era of digital communication and data exchange, ensuring the confidentiality, integrity, and authenticity of information is critically important. Traditional symmetric encryption methods face challenges in secure key distribution and scalability. To address these issues, public key cryptography provides a robust solution where encryption and decryption are performed using separate keys. The **RSA algorithm** is one of the most widely used public key cryptosystems that enables secure data transmission over insecure networks.

However, understanding and implementing RSA from scratch requires a deep understanding of number theory, modular arithmetic, and key generation processes. There is a need for a clear, educational, and functional implementation of the RSA algorithm that demonstrates its core principles and operations, including key generation, encryption, and decryption.

Equipment/Tools:

Theory:

Procedure:

Steps:

Observations and Conclusion: