Lab 9 – Implementation of RSA Cryptosystem

AI331: Information Security and Cryptography
SVNIT, Surat

Learning Objectives

- Understand the mathematical foundation of the RSA cryptosystem.
- Implement RSA key generation, encryption, and decryption in C++.
- Practice modular exponentiation, greatest common divisor, and modular inverse computation.
- Verify correctness using small, known test parameters.

Background Theory

RSA is a public-key cryptosystem based on the hardness of integer factorization. Its working steps are as follows:

1. Choose two large prime numbers p and q.
2. Compute $n = pq$ and $\varphi(n) = (p-1)(q-1)$.
3. Choose an integer e such that $\gcd(e, \varphi(n)) = 1$.
4. Compute the private exponent d such that:
$$d \equiv e^{-1} \pmod{\varphi(n)}$$
5. Encryption:
$$c \equiv m^e \pmod{n}$$
6. Decryption:
$$m \equiv c^d \pmod{n}$$

Note: In practice, RSA uses padding schemes such as OAEP for security. In this lab, we implement textbook RSA for conceptual understanding.

Lab Tasks

Task 1: Implement the **Extended Euclidean Algorithm** to find $d = e^{-1} \bmod \varphi(n)$.

Task 2: Implement **Modular Exponentiation** to compute $a^b \bmod n$ efficiently.

Task 3: Generate RSA keys using small primes (e.g., $p = 61, q = 53$).

Task 4: Perform encryption and decryption on an integer message $m < n$.

Task 5: Verify that decrypted message equals original plaintext.

Example Output

```
RSA Implementation (Toy Example)
p = 61
q = 53
n = 3233
phi(n) = 3120
e = 17
d = 2753

Message m = 65
Ciphertext c = 2790
Decrypted m = 65

[OK] Decryption successful!
```

Lab Discussion Questions

1. What is the purpose of choosing e coprime with $\varphi(n)$?
2. Why is the modular inverse necessary in key generation?
3. What happens if $m \geq n$?
4. Explain why this "textbook RSA" is not secure in practice.

Additional Tasks (Optional)

- Generate random small primes using a simple Miller–Rabin test.
- Implement Chinese Remainder Theorem (CRT) optimization for decryption.
- Encode ASCII messages as integers for multi-block RSA.
- Research: Why is padding (OAEP) essential for secure RSA encryption?

References

1. Stinson, D. R., *Cryptography: Theory and Practice*, CRC Press.
2. Menezes, van Oorschot, and Vanstone, *Handbook of Applied Cryptography.*
3. FIPS 186-4, *Digital Signature Standard (DSS)*, NIST.