Lab Report

Introduction and Objectives

In this lab, we implemented symmetric and asymmetric cryptographic operations using Python. The objective was to understand the inner workings of these cryptographic processes by coding them ourselves and measuring their execution times.

Description of Functionalities

1. **AES Encryption/Decryption**:
    - Two key lengths: 128 and 256 bits.
    - Two modes: ECB and CFB.
    - Data is encrypted and stored in a file, which is then decrypted and displayed.

2. **RSA Encryption/Decryption**:
    - Public and private keys are generated and used for encryption and decryption.
    - Data is encrypted and stored in a file, which is then decrypted and displayed.

3. **RSA Signature**:
    - A signature is generated for a given input and stored in a file.
    - The signature is verified using the corresponding public