Number Theory and Cryptography Lab

Note: At least any five from each section

Number Theory

- Implement Euclidean Algorithm.
- Implement Extended Euclidean Algorithm.
- Implement Modulo Inverse
- Implement modular exponentiation (square and multiply)
- Implement Miller-Rabin Algorithm for testing for primarily
- Write a simple four-function calculator in GF(2^4).
- Write a simple four-function calculator in GF(2^6).
- Implement Euclidean Algorithm to find gcd of polynomials (with coefficients in a field).
- Implement Extended Euclidean Algorithm to find gcd of polynomials (with coefficients in a field).
- Implement Chinese Remainder Theorem

Cryptography

- To implement a program for encrypting a plain text and decrypting a cipher text using Caesar Cipher (shift cipher) substitution technique
- To implement a program to encrypt a plain text and decrypt a cipher text using play fair Cipher substitution technique.
- To develop a program to encrypt and decrypt using the Hill cipher substitution technique
- To develop a program to implement encryption and decryption using vigenere cipher substitution technique
- To develop a program for implementing encryption and decryption using rail fence transposition technique.
- Develop a program to implement RSA algorithm for encryption and decryption.
- Develop a program to implement Diffie Hellman Key Exchange Algorithm for encryption and Decryption
- Develop a program to implement Secure Hash Algorithm (SHA-1)
- To write a program to implement the digital signature scheme in java