Lab sheet for CSIT 5th Semester

Cryptography

Lab 1

1. Write a program that takes an integer value K (i.e. shift value between +/- 26) and a plaintext message and returns the corresponding Ceasar cipher. The program should also implement a decryption routine that reconstructs the original plaintext from the ciphertext.
2. Write a program that asks user for key and plain text and displays the corresponding Vigenere cipher.

Lab 2

3. Using the Rail Fence algorithm with depth 3, write a program to encrypt the message “I love my college”.
4. Write a program to demonstrate the calculation of initial permutation of a plain text in DES algorithm.

Lab 3

5. Write a program for simple RSA algorithm to encrypt and decrypt the data.
6. Write a program to calculate the Key for two persons using the Diffie Hellman Key exchange algorithm.

Lab 4

7. Write a program to print Multiplicative Inverse of a Number.
8. Write a program that asks for two numbers and check whether they are co-prime or not?
9. Write a program to find GCD of two numbers using Euclidian algorithm.

Format for the Report

1. Title
2. Algorithm
3. Source Code
4. Sample Output / Screenshot