CS557: CRYPTOGRAPHY
ASSIGNMENT-1

Deadline: 28th August 2024

1. Write program (in C language) for the followings. Write a doc file name manual.doc. In manual document write the algorithm, inputs and outputs for different cases. Zip your program-code along with the manual to the name as Ass1_yourRoll and subject as CS557 cs_557Ass1. Upload the zip file in the form to be circulated, before the deadline.

(a) We discussed about Enigma crypto machine, in class. Write a program to simulate Enigma machine.

(b) Write a program to find inverse mod N using Ext-Euclidean algorithm.
Test your code for at least 3 different inputs

(c) Write a program to find f(x) inverse mod p(x) using Ext-Euclidean algorithm.
Test your code for at least 3 inputs in GF(2^3) considering the irreducible polynomial
p(x) = x^3 + x +1