System & Network Security Lab Assignment 3

(R1 and R2 batch)

Total Marks: 15 Submission Date:-12/10/2018

Time: 2.00 PM

Question 1:-Write a program to find QR and QNR for any Z_P^*.

[5 M]

Question 2:- Write a program to find all primitive roots for the set Z_P^*.

[5 M]

Question 3:-Write a computer program that implements the Miller-Rabin algorithm for a user-specified n. The program should allow the user two choices:

a) specify a possible witness a to test using the witness procedure or
b) specify a number s of random witness for the Miller-Rabin test to check

[5 M]