E0254: Network and Distributed Systems Security

Assignment No. 1

Date given: September 04, 2017

Submission Due Date: September 24, 2017

1. Write a program in C++ to find a 1024-bit prime number. The program should output the prime number in both binary and decimal. You can use the Rabin-Miller or any other algorithm to find the prime number. The program should output the time required to find the number along with the number, and then wait for the instruction to either exit or produce the next prime number.
2. Using the 1024-bit prime number found in (1) above, say n, write a program to find the multiplicative inverse of a given number modulo n using the extended Euclid's algorithm. In this case, the program should first ask for the prime number (in decimal), and then for the number whose inverse (in decimal) is to be found. The program should then print out the multiplicative inverse (in both binary and decimal), and also give a check for its correctness.

Note: You may use the attached C++ program as a basis to develop your program. Do not use existing library to find the prime number or inverse. If you do so, you will automatically get zero marks for your assignment. A demo of the programs needs to be given sometime later.