CS 773C Cryptography and Biometrics

Spring 2000

Homework 1 - Dr. George Bebis and Dr. Peter Li

Due date: 2/8/00

1. Implement the fast probabilistic algorithm for testing primality. The description of the algorithm is attached. Also, you will have to implement your own *large integer* abstract data type. Some notes on this issues have also been attached. Use the algorithm to find some very large primes (let's say, 100-200 digits). Report running times.

2. Implement the *substitution cipher* method. Chose 1-2 plaintexts and encrypt them using this method. Report your results.