CSCI 3104: Algorithms
Homework 2

Due at **11:00am on Wednesday, September 16, 2015**. Submit your solutions electronically at moodle (name file as **LastName_FirstName_HW2.pdf**) or submit in paper before class. Also, submit your python source code electronically at moodle (name your file as **LastName_FirstName_HW2.py**). Make sure to include your name and student ID. Digital submission should also include the Honor Code Pledge (`http://honorcode.colorado.edu/about-honor-code`), and paper submission should include your signature indicating adherence to the Honor Code Pledge .

1. In Aug 31's lecture (slide 5), we discussed a recursive multiplication algorithm. If the input is an m-bit number x and an n-bit number y, how long does it take to multiply x and y? Justify your answer.

2. Compute gcd(770, 546) in the following three different ways. Show your steps.

   (a) By finding the factorization of each number;

   (b) By using the Euclid algorithm;

   (c) By using the extended Euclid algorithm (also finds x and y).

3. What is the result of 7^{7293} (mod 342)? Show your steps.

4. Write a python program to

   (a) Generate a pair of public and private keys for the RSA scheme, where p and q each has n bits.

   (b) Given $x = 2015$, compute the encoded message y.

   (c) Given y computed above, compute the decoded message.

   Run your program for 3 different n values, report the results and the corresponding running time for each step (a), (b), and (c).