INFA723 Homework 3

The homework assignment will be graded based on the following criteria:

- Accuracy: 1) the solution meets specific requirements in the problem description; 2) the solution produces correct results; 2) the procedures adopted in the solution are technically sound.
- Efficiency: efficiency will be one of the criteria when grading programing assignment. The solution should produce the desired results efficiently.
- Effort/neatness: the solution includes excellent effort, and all relate work is shown neatly and organized well.

Homework assignment feedback will be available through the DropBox folder on D2L.

1. (20 points) Determine gcd(12075, 4655).
   Don't forget to include answer for Question 1 in your solution.

2. Homework 3 includes 4 labs listed as below:

   (20 points) Lab5 Use OpenSSL to Generate Random Number and Test Primality

   (20 points) Lab6 Use OpenSSL to Create RSA Public/Private Key (512bits) without Password Protection

   (20 points) Lab 7 Use OpenSSL to Create RSA Public/Private Key (4096bits) with Password Protection

   (20 points) Lab8 A Combination of RSA and AES to Encrypt a File

The steps in each lab are documented for your learning purpose. You don't need to make screenshots for those steps.

There is a question section in the end of each lab. Please answer all the questions in each lab. The required data files for the labs have been enclosed in the labs5-7.zip file. Copy the data files to you OpenSSL testing environment to complete the labs.

Please create a single document to include all you answers to question 1 and the four labs and submit your work through D2L.