Assignment Two for FCC 220/520

Total marks: 20 marks.
Due Date: 16/05/2013 (4:00pm)

Requirement: You need to finish this assignment independently.

1. In the process of implementing RSA, exponentiation in modular arithmetic is an important issue in computing

   $$M^{e} \bmod n .$$

   Read paragraphs in page 271-272 in the textbook (4th edition) and make sure you fully understand the technical content and implement the Algorithm in Figure 9.7. You are required to do the following:

   - You code this algorithm in C/C++ and make sure it can be used to compute $a^{b} \bmod n$ for positive integer numbers a, b n with length less than 10 digits . Hand in the hard copy of your code.
   - Use your code to compute $12^{23} \bmod 64$ and print out the final result.

2. In RSA algorithm, if two users are using two public keys **(n, e1)** and **(n, e2)** with same modular **n**, where **e1 and e2** are co-prime. If they encrypt the same message **m** as following

   c1=m^{e1} **mod n**
   c2=m^{e2} **mod n**

   and a cryptanalyst knows the information **{e1,e2,c1,c2,n}**, can he/she recover the information **m** from **{e1,e2,c1,c2,n}** ? With any possible answer you give, explain your justification.

3. Implement the following steps.

   - Select two prime numbers p and q using the algorithm in Question 3 of lab 2. The range of p and q is required to be between 1000 and 10000.
   - Using the Extended Euclidean Algorithm (question 5 in lab 3) to select {e, n} with constraint gcd(e, □(n))=1.
   - Using the Extended Euclidean Algorithm (question 5 in lab 3) to solve d.
   - Covert each symbol on keyboard to its ASCII code for RSA encryption and decryption.
   - Implement RSA encryption and decryption using the algorithm in Question 1 of this assignment.

- When you finish all steps above, you are required to encrypt and decrypt a text file. In your hard copy, state each step clearly with explanations in your code. The test file will be the same for SDES on the website.