Assignment Two for ISEC 2000/5002

Total marks: **25 marks**.
Due Date: 17/05/2019 (12:00pm)

Requirement: You need to finish this assignment independently. Submit your e-copy of assignment and answer the following questions clearly. (Questions 1-3 are for both ISEC2000 and ISEC5002 students; Question 4 is for ISEC5002 students only and question 5 is for ISEC2000 students only). Also you need to show your demo in lab.

1. In the process of implementing RSA, you need to verify whether two integers are coprime via implementing the Euclidean Algorithm based on the following equation. **(5 marks)**

$$\gcd(a, b) = \gcd(b, a \ mod \ b) \quad \text{in case of } a>b \qquad (1)$$

Read paragraphs in page 108 in the textbook (6th edition) and make sure you fully understand the technical content and implement the Algorithm in equation (4.3) of page 110. You are required to do the following:

- You code this algorithm in one programming language and make sure it can be used to compute the greatest divisor for two positive integer numbers. Hand in the ecopy of your code with the demonstration of the following specific question.
- Use your code to compute the gcd(12543, 1682), and print out the final result.
- Prove the assertion in (1).

2. Implement RSA as described in the following steps. **(10 Marks)**

- 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 Euclid Algorithm in last question to select {e, n} satisfying gcd(e, ϕ(n))=1.
- Using the Extended Euclid Algorithm to solve a private key d.
- Covert each symbol on keyboard to its ASCII code for RSA encryption and decryption.
- Implement RSA encryption and decryption using the algorithm for exponential modular computation in page 289 of the text book (sixth version).
- When you finish all steps above, you are required to encrypt and decrypt a text file in the website and answer the following questions.
  1) **In your ecopy, state each step clearly with explanations of each function in your code.**
  2) The test file will be the same for SDES in Assignment One, which can be found in the unit website.

3) Hand in the one page of the original text, the ciphertext and decrypted text to validate the effectiveness of your code.

4) If your code is not working properly, address the difficulties you have.

3. Assuming that Alice signed a document **m** using RSA signature scheme. (You should describe RSA signature structure first with a diagram and explain the authentication principle). The signature is sent to Bob. Accidentally Bob found one message **m'** ($m \neq m'$) such that **H(m)=H(m')**, where **H()** is the hash function used in the signature scheme. Describe clearly how Bob can forge a signature of Alice's with such **m'. Justify your forgery with the knowledge you learned from this unit.** **(5 Marks)**

4. In page 36 of lecture 9, Please prove the verification stage for DSS. Make sure that you understand each step in your proof with detail comments for justification. For example, justify why $k^{-1} \bmod q$ exists. **(ISEC5002)** **(5 Marks)**

5. Based on lecture 8, please prove the following assertion. **(5 Marks)**

In a group of 23 randomly selected people, the probability that two of them share the same birthday is larger than 50%. **(ISEC2000)**