Assignment Three for FCC 2000/IC5002

Total marks: 10 marks.
Due Date: 8/06/2016 (12:00pm)

Requirement: You need to finish this assignment independently.

1. Based on what you have learned in this unit, finish the following tasks.

- Summarize the encryption techniques (DES and RSA) with emphasis on their advantages and disadvantages. (you need to describe these algorithms briefly in order to make your statements logically smooth though not necessary to give implementation details).**(FCC2000 and IC5002)**
- List some main difficulties for key management of DES and RSA respectively and give your idea how to solve them. **(FCC 2000 only).**
- Summarize your understanding of digital signature with emphasis on aim, verification principle, and related mathematical problem. Based on your understanding, what does it mean by a secure digital signature? Give your own idea how to design a secure digital signature. **(IC5002 only).**

2. 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. **(FCC2000 and IC5002)**
3. Consider a Diffie-Hillman scheme with a common prime q=13 and a primitive root 7.
   - If Alice has a public X_A=9, what is Alice's private key ?
   - If Bob has a public key X_B=12, please compute the common secret key K shared with Alice.