
INFS3202/INFS7202 – Web Information Systems

Assignment 1

This is an individual assignment. You have to answer all of the questions. The answers should be concise descriptions of your understanding. Greater marks will be awarded for answers that are simple, short and concrete than for answers that are sketchy and cumbersome. Marks will be lost for giving irrelevant information.

If, by and chance, you think the assumptions are not sufficient to solve the problem, then you can add the assumptions that you think are necessary. State explicitly what assumptions that you have made.

This assignment accounts for 10% of the course assessment. There are totally 2 questions. **The due date of this assignment is 21st May 2009.** No late submission is allowed unless in exceptional circumstance. The submission method will be announced on the web.

Question 1 (10 marks)

Assume that John wants to buy some CD from an online shop called MusicPlus. Please describe step by step (with figures and words):

- (a) How John should encrypt the information and send via the Internet so that the information will be sent securely to MusicPlus.
- (b) How MusicPlus can ensure the information received is not being altered during the transmission process.

Question 2 (10 marks)

What are the differences between key distribution centre and certification authority? Briefly describe their mechanisms step by step.