TRIAL EXAM QUESTIONS FOR THE e-COMMERCE TECHNOLOGIES COURSE

1. Consider the task of designing a Web server that will target specifically E-commerce, with the objective of accommodating a number of merchant sites, each consisting of a catalog, shopping cart, payment system interfacing with a credit card company, customer profiles repository based on previous transactions, and a recommender system. What specific architectural suggestions would you make to ensure

(a) efficiency
(b) security
(c) reliability?

2. Show how Diffie-Helmann key exchange over a non-secure channel will be achieved for the following values:
$\alpha = 3$, $q=47$. Assume $X_A=36$, $X_B=58$ are private keys. Compute the secret key.

3. Define an XML DTD which will be used to represent bids in an auction.

4. What security mechanisms can be used to ensure that mobile agents are secure for the site that receives them?

5. Your employer has tasked you with the design of a company-wide Certificate Authority (CA) for the procurement system (i.e. purchases on behalf of the company). What operations would you build for the CA administrator?

6. Discuss why, in the Electronic Election procedure, the Validator returns the signed ballot to the Voter, rather than sending it directly to the Tallier.

7. Describe how data mining (e.g. classification) could be used in an E-commerce setting to decide which customers should Chapters.ca contact by email with an offer to buy a new book.

8. Consider the following data being processed by the Associations algorithm:
3-ferequent itemsets: (1 3 5) (1 3 6) (1 5 6) (1 3 7) (3 5 6) (1 5 7)
Find the resulting candidate 4-frequent itemsets.

9. Which of the data mining functions mentioned in class (classification, clustering, associations) would be primarily used to generate recommendations in a recommender system (there are two answers, it is enough to give one, a 2 pt. Bonus for giving both).

10. Consider four layers of the Internet Protocol stack: physical, network, transport, and application. Describe BRIEFLY, in a bullet format, challenges to each of these layers if Internet is to move to wireless media, as postulated in the WAP proposed standard.

11. Simulate the RSA encryption and decryption in a very simplistic setting (in order to limit the computation). Assume $p=5$, $q=7$, $e=11$. Compute d, and show how a « message » $M=58$ is encrypted and its encrypted form is subsequently decrypted. Show how you avoid superfluous multiplications in exponentiation, eg do NOT do 11 multiplications in 58^{11} mod 24, but 5.

12. Consider the task of designing a Web server that will target specifically E-commerce, with the objective of accommodating a number of merchant sites, each consisting of a catalog, shopping cart, payment system interfacing with a credit card company, customer profiles repository based on previous transactions, and a recommender system. What specific architectural suggestions would you make to ensure

(a) efficiency
(b) security
(c) reliability?

13. Give an example of a double auction (e.g. shares in a stock exchange) in which there are six buying and six selling offers for shares of six different companies, four items are sold an bought. Show what is the share price determined in that auction.