THE UNIVERSITY
of LIVERPOOL

MAY 2003 EXAMINATIONS

Master of Science : Year 1
Master of Science : Year 2

TECHNOLOGIES FOR E-COMMERCE

TIME ALLOWED: Two and a half Hours

INSTRUCTIONS TO CANDIDATES

Answer any four questions.

Each question is worth 25 marks.

If you attempt to answer more than the required number of questions, the marks awarded for the excess questions will be discarded (starting with your lowest mark).

Electronic calculators are not permitted.

THE UNIVERSITY *of* LIVERPOOL

QUESTION 1

(a) What do the letters "HTTP" stand for? **1 mark**

(b) What is the purpose of this protocol? **2 marks**

(c) List the four main commands of this protocol. **4 marks**

(d) HTTP lacks state. What does this mean? **3 marks**

(e) List two advantages and two disadvantages of HTTP's being stateless. **4 marks**

(f) Briefly describe three methods for overcoming HTTP's lack of state. **6 marks**

(g) When would you advise an e-commerce programmer to use session variables? Why? **5 marks**

QUESTION 2

(a) What is the name of a model of distributed computing in which one computer requests something from a second computer, and the second computer seeks to fulfill this request? **1 mark**

(b) Draw diagrams for the following distributed system architectures, showing the different layers:

    (i) 2-tier architecture **1 mark**

    (ii) 3-tier architecture. **1 mark**

(c)

    (i) What is the difference between applets and servlets? **2 marks**

    (ii) When would you prefer to program with applets rather than servlets? **2 marks**

    (iii) When would it be better to program with servlets rather than applets? **2 marks**

(d)

    (i) What is the function of a stub in a CORBA architecture? **2 marks**

    (ii) What is the function of the Object Request Broker in a CORBA architecture? **2 marks**

    (iii) Draw a diagram to show how a CORBA client and server are connected through an Object Request Broker, showing stubs and skeletons.

3 marks

(e) You are commissioned by a company to develop a distributed electronic commerce application for them, incorporating all their current business activities and systems. About which aspects of the distributed system would you need to make design decisions? What criteria would you use to assess the resulting system?

9 marks

QUESTION 3

(a) What are each of the following auction protocols called?

(i) Bidders place a single bid in a sealed envelope. The winner is the bidder with the highest bid. The amount paid is the amount of the second-highest bid.

(ii) Bidders place a single bid in a sealed envelope. The winner is the bidder with the highest bid. The amount paid is the amount of the highest bid.

(iii) Bidders call out their bids in successive rounds, each bidding higher than any previous price called. The winner is the bidder who bids the highest amount. The amount paid is the amount of the highest bid.

(iv) The auctioneer starts by calling out a high price. When a bidder hears a price he or she is willing to pay, he/she calls out *"Accept"*. The winner is the first bidder to call out *"Accept"*. The amount paid is the price at which this call is made.

4 marks

(b)

(i) What does FIPA ACL stand for? **1 mark**

(ii) Briefly describe the purpose of the following FIPA performatives:

inform   cfp   query-if. **6 marks**

(c) Draw a diagram to show the sequence of FIPA ACL performatives for a Dutch Auction protocol.

6 marks

(d) A brewing company called *Global Beers* approaches you to build them an extranet to manage their relationships with their suppliers. Their suppliers fall into three categories: agricultural producers of hops, bottle and keg manufacturers, and manufacturers of brewing machinery. Global Beers wants to have on-line auctions, so that suppliers in each category have to compete with each other to sell their products or services to Global Beers. What objectives should Global Beers have for such auctions, and why? Given these objectives, what type of auction(s) would you recommend, and why?

8 marks

QUESTION 4

For this question, assume throughout that two participants are engaged in an interaction using the mono-tonic concession protocol (MCP), which proceeds through a number of rounds.

(a) What is the purpose of the MCP?   **1 mark**

(b) How does an interaction using the MCP begin?   **1 mark**

(c) What utterances can each participant make at each round of this protocol?   **4 marks**

(d) Under what circumstances does the interaction end?   **4 marks**

(e) Describe with a diagram how you could represent this interaction using Javaspaces (or Tuple spaces)? What Javaspace (or Tuplespace or Linda) commands would correspond to each possible utterance?

7 marks

(f) Suppose one participant asked you to advise him or her on what to do at each round of the interaction. What general rule would you give the participant to enable him or her to make this decision themselves at each round? Why? What assumptions does your advice depend on? How practical is this general rule?   **8 marks**

QUESTION 5

(a)

    (i) Explain the difference between symmetric and asymmetric key algorithms for encryption.

2 marks

    (ii) What is the main weakness of symmetric key algorithms?   **1 mark**

    (iii) List three types of attacks which symmetric key encryption algorithms are subject to. **3 marks**

(b)

    (i) List two types of attacks which public key encryption algorithms are subject to.   **2 marks**

    (ii) Explain the steps involved in public key encryption methods.   **4 marks**

(c)

    (i) Briefly describe three methods of secure payment of goods purchased over the internet.

6 marks

    (ii) How would you determine which method was most appropriate in a particular application?

7 marks

QUESTION 6

(a) A company called *Global Beers* approaches you to design and develop an e-commerce application for them, to enable their customers to make purchases of beer and wines over the Internet. The company wants all visitors to its web-site to fill in a form with their name, postal address and other details, with this form submitted to the company's server. From there, Global Beers will then store this information in a company database, which they can analyze for marketing purposes.

    (i) What law governs the keeping of such databases in Great Britain?   **1 mark**

    (ii) Is it legal to keep such a database *on a computer* in Great Britain?   **1 mark**

    (iii) Global Beers also wants to sell their database of customer names and addresses to other companies. What must Global Beers do first for this to be legal in Britain?

    2 marks

    (iv) Further, Global Beers asks you to develop a cookie which will track all the other web-sites visited subsequently by each client who browses their site. Is this possible with HTTP? Why or why not?   **3 marks**

(b) (i) What is a firewall?   **2 marks**

    (ii) What is a screened subnet?   **2 marks**

    (iii) Draw a diagram to show a screened subnet architecture.   **2 marks**

(c) Following your successful project with Global Beers, you win a project with the British Government to design an electronic voting system for local and national elections.

    (i) Provide an outline specification of the security, confidentiality and authentication requirements of the proposed system.

    6 marks

    (ii) Do you believe such a specification is achievable using current Internet technologies? Why or why not?   **6 marks**