PAPER CODE NO.	EXAMINERS : Peter McBurney and Darek Kowalski
COMP211	DEPARTMENT : Computer Science TEL. NO. 795 4245

THE UNIVERSITY
of LIVERPOOL

JANUARY 2007 EXAMINATIONS

Bachelor of Arts : Year 2
Bachelor of Science : Year 2
No qualification aimed for : Year 1

INTERNET PRINCIPLES

TIME ALLOWED: Two 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 neither necessary nor permitted.

THE UNIVERSITY
of LIVERPOOL

QUESTION 1

(a) Draw a diagram to show the standard 5-layer (*"North American"*) model of distributed communication. **3 marks**

(b) Briefly describe the function of each layer in the 5-layer model. **1 mark each**

(c) What are the primary differences between the Internet and traditional telecommunications networks? How can both types of network operate on the same physical infrastructure? **4 marks**

(d) In Peer-to-Peer (P2P) networks a key issue is the location of the catalogue of content. What is this problem? Explain why this is a problem in P2P networks, but not in client-server architectures. Give two examples of how the catalogue may be located in a P2P architecture. **6 marks**

(e) Why are there different protocols on the Internet? Illustrate your answer with examples. **7 marks**

QUESTION 2

(a) What information is contained in an Internet socket? **2 marks**

(b) 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**

(c) What does an Application-Layer protocol provide to protocols in the layer beneath? **3 marks**

(d) What is the difference between a "push" and a "pull" protocol? **2 marks**

(e)

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

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

(iii) Is HTTP a "push" or a "pull" protocol? Why? **2 marks**

(f)

(i) The Simple Mail Transfer Protocol (SMTP) is an Application-Layer protocol for mail transfer between hosts. Is SMTP a "push" or a "pull" protocol? Why? **2 marks**

(ii) Why is SMTP not always used for the final leg of mail transfer, between the receiver host machine and the receiver mail software program? **3 marks**

(g) Suppose you were tasked with designing a new Internet application. Which Transport Layer protocols would you use for this application? Why? **7 marks**

THE UNIVERSITY
of LIVERPOOL

QUESTION 3

(a) Alice sends a message to Bob which is 4500 bytes long, and is broken into segments of 800 bytes each. Alice chooses a random start value of 3200.

(i) How many segments will the message be broken into? **1 mark**

(ii) Give the start and end bytes of each segment. **2 marks**

(iii) Give the ACK numbers which Bob will use to indicate that each segment was received uncorrupted. **2 marks**

(iv) Suppose Bob chooses a random start of 118 for his ACK numbers, and that he only sends headers (and no data) back to Alice. What will be the sequence numbers used by Alice in response to these ACKs? **2 marks**

(v) Draw a brief Message Sequence Chart for the interaction. **3 marks**

(b) What characteristics of the Internet lead it to being described as an *"unreliable"* communications medium? **3 marks**

(c) How does TCP differ from UDP? **2 marks**

(d) What is the problem of *buffer overflow*? Which nodes in the Internet first know about this problem? Do they communicate their knowledge to other nodes when using TCP? If so, how? What happens when the sender of a message using TCP learns of the problem? **5 marks**

(e) What is the problem of *network congestion*? Which nodes in the Internet first know about this problem? Do they communicate their knowledge to other nodes when using TCP? If so, how? What happens when the sender of a message using TCP learns of the problem? **5 marks**

THE UNIVERSITY
of LIVERPOOL

QUESTION 4

(a) Using an example, explain the difference between authentication and integrity in network security. **3 marks**

(b) Compare and contrast symmetric and asymmetric (public-key) cryptography techniques. Explain the advantages and disadvantages of using each approach. **5 marks**

(c) The Caesar cipher, discussed in lectures, is a simple symmetric-key encryption method that, for every letter in a message, substitutes that letter with a letter that is K letters ahead of it in the alphabet, where K is the key.

(i) Assuming a key of 5 (that is, to **encrypt** a message, each occurrence of the letter is replaced with a letter 5 places ahead of it in the alphabet, so 'a' is replaced with an 'f'), **decrypt** the following message and write the decoded plaintext: `snhj btwp` **2 marks**

(ii) There are only 25 possible keys for the Caeser cipher, yet it was used to much success by Julius Caesar. Such a small key space is easily searchable and messages easily decoded by hand. If this is the case, explain why this method was so successful for Caesar (assume that the people trying to decode the messages would understand the plaintext when they see it – that is, they share the same language as Caesar). **3 marks**

(d) Alice wants to send Bob a confidential (encrypted), authenticated message. Both Alice and Bob know each other's public key, but the message is so large that encrypting it with Bob's public key, and then having Bob decrypt it with his private key would take far too long. Therefore, Alice and Bob would like to use a symmetric key for encryption and decryption, which is much faster. However, they have not been in contact previously to agree on such a key.

Using methods discussed in lectures, describe a method allowing Alice to send the message to Bob using only one transaction (that is, only one message is sent in its entirety, similar to an email or text message) in a confidential, authenticated manner if Alice and Bob have had no prior contact. Explain how this protocol achieves confidentiality and authentication. NOTE: integrity of the message is not an issue. **7 marks**

(e)

(i) What is a digital signature and what is one used for in network security? **1 marks**

(ii) Digitally signing messages is computationally expensive, so instead, message digests are often digitally signed and sent with the unsigned message. What is a message digest and why are they beneficial? **2 marks**

(iii) Why are Internet checksums considered to be poor for creating message digests? **2 marks**

THE UNIVERSITY
of LIVERPOOL

QUESTION 5

(a) In which layers do error detection and correction take place? Give examples. **2 marks**

(b) What are the main services in the Network Layer? **4 marks**

(c) What is an exponential backoff protocol? In which protocols and in what layer is it used? **3 marks**

(d) Suppose you have seven host machines and one router all connected together, with the following IPv4 addresses:

- Two hosts have addresses in the network 221.1.1.0/24.
- Two hosts have addresses in the network 221.2.0.0/16.
- Three hosts have addresses in the network 221.1.3.0/30.
- The router has addresses 221.1.1.40, 221.2.0.9 and 221.1.3.85.

(i) Draw a diagram to represent this configuration. **5 marks**

(ii) Draw a forwarding table for the host machine with IP number 221.1.1.1 **3 marks**

(iii) Draw a forwarding table for the router. **3 marks**

(iv) Show the steps involved when a datagram is sent from host machine 221.2.0.1 to host machine 221.1.1.1. **5 marks**

QUESTION 6

(a) Give three examples of multiple access channel protocols, with at least one used in wire and one in wireless technologies. Must a datagram use the same link protocol while transported through many links? **4 marks**

(b) Imagine that during link transmission one bit per 16 may be faulty.

(i) How do you design the mechanism to detect and correct errors? **3 marks**

(ii) Give an example and analyse the mechanism in the case when the fifth bit was faulty. **2 marks**

(c) What is a CSMA? What kinds of CSMA do you know? Describe them, point out similarities and differences. Give examples of technologies where each of these kinds is used. **7 marks**

(d) Imagine you design a wireless LAN which is assumed to serve between 500 and 1000 users in any time (each user is assumed to generate heavy traffic). What kind of multiple access protocol would you choose to assure small latency (choose one from TDMA, CSMA/CA using backoff protocol, FDMA and ALOHA)? Compare its expected behaviour with some other protocol which you'd rather avoid. **9 marks**

THE UNIVERSITY
of LIVERPOOL

QUESTION 7

(a) What kind of data can be transmitted in the Physical Layer and what does such data represent? Give examples of such data. **2 marks**

(b) What is the signal-to-noise ratio corresponding to 20dB? Is it bigger or smaller than the typical voice signal-to-noise ratio? **3 marks**

(c) Give three examples of different kinds of wireless communication. Indicate the kind of electromagnetic spectrum they each use and order them accordingly. **5 marks**

(d) What is a virtual circuit in the Internet? How do virtual Internet circuits differ from voice circuits in telecommunications networks? **5 marks**

(e) What are the advantages and disadvantages of digital transmission. **10 marks**