PAPER CODE NO. **COMP211**	EXAMINER : Martin Gairing DEPARTMENT : Computer Science Tel. No. 0151 795 4264

UNIVERSITY OF LIVERPOOL

First Semester Examinations 2015/16

INTERNET PRINCIPLES

TIME ALLOWED : Two Hours

INSTRUCTIONS TO CANDIDATES

This examination consists of two sections. Section A is worth 25 marks and Section B is worth 75 marks. Answer **ALL** questions is Section A and **THREE** questions from Section B. If you attempt to answer more questions than the required number of questions (in any section), the marks awarded for the excess questions answered will be discarded (starting with your lowest mark).

THIS PAPER MUST NOT BE REMOVED FROM THE EXAMINATION ROOM

Section A

Each of the following questions comprises several statements, for which you should select ALL answers that apply. (2 marks each)

(10 MC questions)

The following TRUE/FALSE questions are worth 1 mark each.

(5 TRUE/FALSE questions)

Section B

1. **QUESTION ONE**

A. Alice wants to communicate with Bob using symmetric-key cryptography (e.g. DES) with a session-key K_S. In the lectures we learned how public-key cryptography (e.g. RSA) can be used to distribute a session key K_S from Alice to Bob. Suppose the private keys of Alice and Bob are K_A^- and K_B^-, while the public keys are K_A^+ and K_B^+. Draw a diagram that shows the message exchange between Alice and Bob which achieves this. **3 marks**

B. What is the main advantage of first distributing a session key and then using symmetric-key cryptography rather than using public-key cryptography techniques for the whole communication? **3 marks**

C. In the lectures we studied an efficient and secure e-mail scheme, which provides secrecy, sender authentication and message integrity.

i. Draw a diagram for the sender side of this scheme. **4 marks**

ii. Explain how the scheme ensures secrecy, sender authentication and message integrity and why it is efficient. **5 marks**

D. Consider RSA with $p = 5$ and $q = 11$.

i. What are n and z? Show all work. **3 marks**

ii. Let e be 3. Why is this an acceptable choice for e? **2 marks**

iii. Find d such that $(e \cdot d \mod z) = 1$. **2 marks**

iv. Encrypt the message $m = 8$ using the key (n, e). Let c denote the corresponding ciphertext. Show all work. **3 marks**

2. **QUESTION TWO**

A. Suppose two hosts, A and B, are separated by $20,000$ kilometers and are connected by a direct link of $R = 2,000,000$ Bps. Suppose the propagation speed over the link is $2 \cdot 10^8$ meters/sec.

i. Calculate the bandwidth-delay product, $R \cdot d_{\text{prop}}$. **3 marks**

ii. Consider sending a file of $800,000$ bits from host A to host B. Suppose the file is sent continuously as one large message. What is the maximum number of bits that will be in the link at any given time? **2 marks**

iii. Provide an interpretation of the bandwidth-delay product. **2 marks**

iv. What is the width (in meters) of a bit in the link? **2 marks**

v. Derive a general expression for the width of a bit in terms of the propagation speed s, the transmission rate R, and the length of the link ℓ. **2 marks**

B. Explain the difference between TDMA, FDMA, CSMA/CD and Slotted ALOHA. **5 marks**

C. Suppose 50 hosts are sharing a broadcast channel. Further suppose at any time each host has a frame to send with probability p. Which of the multiple access protocols from (2B) are desirable if p is low (say 1%)? Why? What about if p is high (say 90%)? **3 marks**

D. Consider a router that interconnects three subnets: A, B, and C. Suppose all of the interfaces in each of these subnets are required to have the prefix 98.22.80.0/22. Suppose subnet A is required to support 500 interfaces, and subnets B and C are each required to support 250 interfaces. Provide network addresses for A,B and C (in the form a.b.c.d/x) that satisfy these constraints. **6 marks**

3. **QUESTION THREE**

A. A digital transmission system uses a coding scheme that defines a symbol as a voltage that can have one of eight possible values. If the system operates at a transmission rate of 1,200 symbols per second, determine the data transmission rate measured in:

   i. Baud **2 marks**

   ii. Bits per second **3 marks**

B. Consider a communication channel with bandwidth $B = 8000\,\mathrm{Hz}$.

   i. Suppose the channel has a signal-to-noise ratio $S/N = 1023$. What is the *maximum data rate* of this channel? **3 marks**

   ii. What is the minimum number of signal states M needed to achieve a data rate of $48000\,\mathrm{bps}$? How many bits must each signal state encode? **3 marks**

C. Suppose Bob joins a BitTorrent torrent, but does not want to upload any data to any other peers (so called free-riding).

   i. Bob claims that he can receive a complete copy of the file that is shared by the swarm. Is Bob's claim possible? Why or why not? **3 marks**

   ii. Bob further claims that he can further make the free-riding more efficient by using a collection of multiple computers (with distinct IP addresses). How can he do that? **3 marks**

D. Why are there different protocols for Inter-AS and Intra-AS routing? **3 marks**

E. Consider an HTTP client that wants to retrieve a Web document at a given URL. The IP address of the HTTP server is initially unknown.

   i. Which application layer protocols are needed in this scenario and what are they used for? **3 marks**

   ii. Which transport layer protocols do these protocols use? **2 marks**

4. **QUESTION FOUR**

A. Alice sends a message to Bob which is 4300 bytes long, and is broken (by TCP) into segments of 900 bytes each. Alice chooses a random start value of 1100 for her sequence numbers.

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 922 for the sequence numbers (of his ACKs), and that he only sends headers (and no data) back to Alice. What will be the ACK numbers used by Alice in response to these ACKs? **2 marks**

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

B. Consider the Go-Back-N protocol with a sender window size of $N = 4$ and a sequence number range of 2048. Suppose that at time t the next in-order packet that the receiver is expecting has sequence number 630. Assume that the medium does not reorder messages. What are all possible values of the ACK field in all possible messages currently propagating back to the sender at time t? Justify your answer. **4 marks**

C. What is the 32-bit binary equivalent to the IP address 53.25.31.189 ? **3 marks**

D. What is the signal-to-noise ratio corresponding to 20dB? Is it smaller, equal or larger than the typical voice signal-to-noise ratio? **2 marks**

E. What is a CRC code? What purpose does it serve? Compute the CRC bits defined by the generator 1011 and the data bit string 111000. **6 marks**