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

UNIVERSITY OF LIVERPOOL

First Semester Examinations 2017/18

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 MCQ questions)

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

(5 True/False questions)

Section B

Reminder: You have to answer **THREE** questions from Section B.

1. **QUESTION ONE**

A. If you intercepted a message that was encrypted using a Monoalphabetic cipher, but you did not know the key, what type of attack could you use to decrypt the message? Outline how this attack would be performed. **3 marks**

B. 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. **6 marks**

C. Alice wants to communicate with Bob using symmetric-key cryptography (e.g. DES) with a session-key K_S.

i. 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. **4 marks**

ii. Now we want to distribute the session key without public-key cryptography using a Key Distribution Centre (KDC). The KDC is a server that shares a secret symmetric key with each registered user. For Alice and Bob denote those keys by K_{A-K} and K_{B-K}. Upon request the KDC issues a session key K_S. Design a scheme that uses the KDC to distribute K_S to Alice and Bob. Your scheme should use three messages:

- a message from Alice to the KDC requesting a session key K_S with Bob,
- a message from the KDC to Alice,
- a message from Alice to Bob.

Draw a diagram showing the exchanged messages. **5 marks**

iii. 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**

2. **QUESTION TWO**

A. Alice sends a message to Bob which is 4500 bytes long, and is broken into segments of 1200 bytes each. Alice chooses a random start value of 2400 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 852 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 1024. Suppose that at time t the next in-order packet that the receiver is expecting has sequence number 650. Assume that the medium does not reorder messages. What are the possible sets of sequence numbers inside the sender's window at time t? Justify your answer. **4 marks**

C. 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 71.5.88.0/22. 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**

D. 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? How does the sender of a message using this protocol respond to such communications? **5 marks**

3. **QUESTION THREE**

A. Suppose 6 host machines and 1 router are connected by a company network consisting of 3 subnets. The configuration is given in the following table:

Subnets	**Host IP-addresses**	**Router IP-Addresses**
66.25.48.0/22	66.25.48.1	66.25.48.44
66.25.52.0/23	66.25.52.1	66.25.52.22
66.25.56.0/23	66.25.52.2	66.25.56.11
	66.25.53.1	
	66.25.56.1	
	66.25.56.3	

i. Draw a diagram to represent this configuration. **4 marks**

ii. Draw the forwarding table for the host machine with IP address 66.25.52.2 **3 marks**

iii. Draw the forwarding table for the router. **3 marks**

iv. Suppose an additional host machine is connected to the company network. For each of the following IP addresses, either give the subnet to which this IP address belongs, or state that it is not a valid IP address for any of the subnets.

- 66.25.50.1 **2 marks**
- 66.25.58.1 **2 marks**

B. Suppose two network interface cards (NIC) A and B are attached to the same broadcast LAN and that A wants to send a datagram to B but doesn't know B's MAC address. Which protocol can be use to resolve this? Explain step by step how A retrieves B's MAC address using this protocol. **5 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**

4. **QUESTION FOUR**

A. Consider a communication channel with bandwidth $B = 6000\,\mathrm{Hz}$.

i. Suppose the channel has a signal-to-noise ratio $S/N = 511$. 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**

B. What is a CRC code? What purpose does it serve? Compute the CRC bits defined by the generator 1001 and the data bit string 101110. **6 marks**

C. For a communication session between a pair of processes, which process is the client and which is the server? **2 marks**

D. What is the difference between *persistent* and *non-persistent* HTTP? Which version of HTTP supports both? **3 marks**

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

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