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

UNIVERSITY OF
LIVERPOOL

First Semester Examinations 2015/16 (Model Solution)

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

UNIVERSITY OF LIVERPOOL

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)

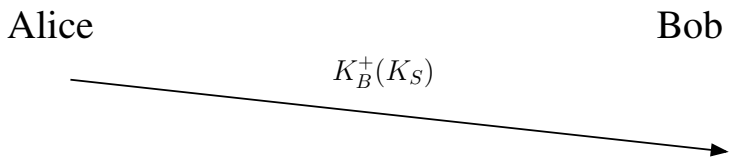
UNIVERSITY OF LIVERPOOL

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**

Model Solution:



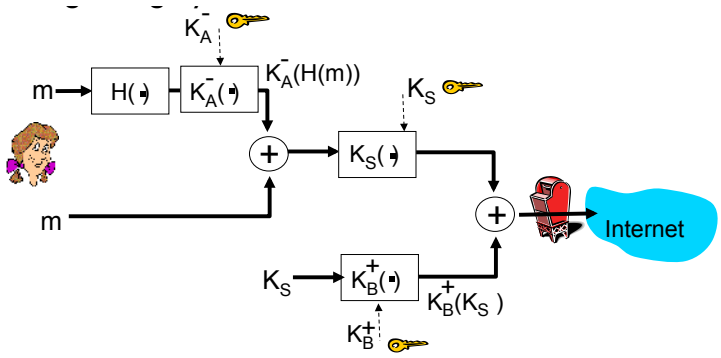
B. What is the main advantage of first distributing a session key and then using symmetric-key cryptography rather than using public-key cryptography techniques for the whole communication? **3 marks**

Model Solution:
Symmetric-key cryptography is more efficient than public-key cryptography. In particular DES is at least a factor 100 faster that RSA.

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**

Model Solution:



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

Model Solution:
Alice digitally signs a message digest $H(m)$ of the email using her private key K_A^-, verifying that she is the sender of the email, providing sender authentication and message integrity. She then generates a random symmetric key K_S and encrypts message and digest with K_S. Alice also encrypts the session key K_S with Bob's public key K_B^+. Encrypted key and message are send to Bob and only Bob can decrypt the session key $K_B^+(K_S)$ with his private key and then use K_S to retrieve the message m. This ensures secrecy.
The scheme is efficient since the computational intensive public key cryptography is only used for encoding/decoding the fixed size message digest and the session key K_S but not the whole email.

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**

Model Solution:

i. $n = p \cdot q = 55$
$z = (p - 1) \cdot (q - 1) = 40$

ii. $e = 3$ is less than n and has no common factors with z.

iii. $d = 27$

iv. $m = 8$, so
$c = (m^e \mod n) = (8^3 \mod 55) = (512 \mod 55) = 17$.

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**

Model Solution:

i. $d_{\text{prop}} = \frac{20{,}000km}{200{,}000\frac{km}{s}} = 0.1$ s. So $R \cdot d_{\text{prop}} = 200,000$ bits.

ii. $200,000$ bits.

iii. The bandwidth-delay product of a link is the maximum number of bits that can be in the link at any given time.

iv. The width of a bit $= \frac{\text{length of link}}{\text{number of bits on link}} = \frac{20{,}000 \text{ km}}{200{,}000} = 100$ m.

v. width of bit $= \frac{\ell}{R \cdot d_{\text{prop}}} = \frac{\ell}{R \cdot \frac{\ell}{s}} = \frac{s}{R}$

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

Model Solution:

TDMA: channel partitioning protocol; allocation of channel-use is by time-slots.

FDMA: channel partitioning protocol; allocation of channel-use is by frequencies.

CSMA/CD: random access protocol; if channel sensed busy defer transmission; if collision is detected abort transmission and wait random time.

Slotted ALOHA: random access protocol; time divided into slots, when node obtains fresh frame it transmits in next slot; if collision send frame in each subsequent slot with probability p.

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**

Model Solution:
If p is low, there is little chance to experience collisions. Thus, a random access protocol (CSMA/CD or

Slotted ALOHA) is desirable. If p is high, a channel partitioning protocol (TDMA or FDMA) is more efficient.

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**

Model Solution:
E.g.:
A: 98.22.82.0/23
B: 98.22.80.0/24
C: 98.22.81.0/24

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**

Model Solution:

i. Baud is defined as the number of symbols per second. Therefore if the system transmits at 1200 symbols per second then the data rate is also 1200 baud.

ii. A symbol is a voltage level that can have one of 8 possible values. Eight levels can be represented by 3 bits. Therefore one symbol represents 3 data bits. If each symbol represents 3 bits then the transmission rate in bits per second will be 1200 x 3 = 3600 bits per second.

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**

Model Solution:

(i) Shannon:

$$\text{max data rate} = B \cdot \log_2(1 + S/N) = 8000\mathrm{Hz} \cdot 10 = 80000\mathrm{bps}$$

(ii) Nyquist:

$$\text{max data rate} = 48000\mathrm{Hz} = 2 \cdot B \cdot \log_2(M) = 16000\mathrm{Hz} \cdot \log_2(M).$$

Thus $M = 8$ and each state must encode $\log_2(M) = 3$ bits.

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**

Model Solution:

(i) Yes. His first claim is possible, as long as there are enough peers staying in the swarm for a long enough time. Bob can always receive data through optimistic unchoking by other peers.

(ii) His second claim is also true. He can run a client on each host, let each client free-ride, and combine the collected chunks from the different hosts into a single file. He can even write a small scheduling program to make the different hosts ask for different chunks of the file. (This is actually a kind of Sybil attack in P2P networks.)

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

Model Solution:
Intra-AS routing creates routes for packets inside the same autonomous system, while Inter-AS routing is used to create routes between different autonomous systems. In Inter-AS routing the AS admin wants control about how its traffic is routed and who is routing through its network. This policy may dominate over performance. Inside an AS the focus is on performance, since no policy decisions are needed (single admin).

Hierarchical routing also saves table size and reduces update traffic.

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**

Model Solution:

(i) DNS to get the IP-address and HTTP for receiving the document.

(ii) DNS uses UDP in default mode, while HTTP uses TCP.

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**

Model Solution:

(i) 5 segments

(ii)
1100, 1999
2000, 2899
2900, 3799
3800, 4699
4700, 5399

(iii) 2000, 2900, 3800, 4700, 5400

(iv) all of them will have ACK number 922

(v) The MSC should show two vertical lines, one representing Alice and one Bob, with time running down the page. Between the two lines are diagonal arrows representing each message sent by either party, in sequence order, with each arrowhead pointed towards the receiver of the message. Each arrow should be annotated with the sequence numbers or ACK numbers corresponding to that message which the arrow represents.

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**

Model Solution:
If the receiver is waiting for packet 630, then it has received (and ACKed) packet 629 and the 3 packets before that. If none of those 4 ACKs have been yet received by the sender, then ACK messages with values of [626,629] may still be propagating back. Because the sender has sent packets [626, 629], it must be the case that the sender has already received an ACK for 625. Once the receiver has sent an ACK for 625 it will never send an ACK that is less than 625. Thus the range of in-flight ACK values can range from 625 to 629.

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

Model Solution:
00110101.00011001.00011111.10111101

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**

Model Solution:
The ratio is $10^{20/10} = 100$, and it is smaller than 1000 corresponding to the typical voice.

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**

Model Solution:
CRC stands for Cyclic Redundancy Check and is a checksum function. A checksum function is a means to assess whether data has been corrupted in transit.

Given the data bitstring $D = 111000$ and the generator $G = 1011$ we have to compute the CRC bits R such that $< D, R >$ is divisible (modulo-2) by G:

$$
\begin{array}{ll}
\overbrace{1011}^{G} & \overbrace{111000}^{D}000 \\
 & \underline{1011} \\
 & 1010 \\
 & \underline{1011} \\
 & 0010 \\
 & \underline{0000} \\
 & 0100 \\
 & \underline{0000} \\
 & 1000 \\
 & \underline{1011} \\
 & 0110 \\
 & \underline{0000} \\
 & \underbrace{110}_{R}
\end{array}
$$

The CRC bits are 110.