IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2012

BEng Honours Degree in Information Systems Engineering Part III
MEng Honours Degree in Information Systems Engineering Part III
BSc Honours Degree in Mathematics and Computer Science Part III
MSci Honours Degree in Mathematics and Computer Science Part III
MSc in Computing Science
for Internal Students of the Imperial College of Science, Technology and Medicine

This paper is also taken for the relevant examinations for the Associateship of the City and Guilds of London Institute
This paper is also taken for the relevant examinations for the Associateship of the Royal College of Science

PAPER C527

COMPUTER NETWORKS AND DISTRIBUTED SYSTEMS

Wednesday 2 May 2012, 10:00
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions
Calculators required

Section A (Use a separate answer book for this section.)

1 a Briefly explain each of the following terms and state which layer of the OSI reference model it relates to:

i) SYN flag

ii) Signal attenuation

iii) Differential Manchester encoding

iv) Distance vector

v) Start frame delimiter

vi) ICMP echo response packet

b An application on host A sends data to another application on host B over a network using the *Transmission Control Protocol* (TCP). The application on host A generates 512 KBytes of data every second. The application receiving the data on host B can accept at most 128 KBytes of data every second.

Host B has a *receive buffer* of 2048 KBytes. The round-trip time of the network between hosts A and B is 2 seconds. You may assume that only a single TCP packet can be in-flight at any given time and that any processing time is negligible.

i) Briefly explain what *flow control* means in the context of networks.

ii) Describe how TCP implements flow control, mentioning relevant fields from the TCP header.

iii) For the first **10** seconds after the TCP connection has been established in the above example, list all TCP packets that are exchanged between the hosts, including relevant header fields. At each time step, also state the receive buffer space currently in use at host B.

iv) TCP also provides a *congestion control* mechanism based on packet loss. As an alternative solution to this, describe how TCP and Internet routers would have to be modified so that TCP's flow control mechanism could be used to handle network congestion instead.

The two parts carry, respectively, 30% and 70% of the marks.

2a i) Give a definition of *multiplexing* in networks.

ii) Briefly explain the following four multiplexing schemes, stating their respective advantages and disadvantages.

A) TDM

B) Statistical TDM

C) FDM

D) CDMA

iii) Give an example, together with an explanation, of multiplexing at the transport layer.

b A host that is connected to the Internet has the following two addresses associated with it:

Address 1: `140.247.60.123`
Address 2: `c4:2c:03:01:03:17`

i) Explain the purpose of the two addresses above.

ii) Describe **three** pieces of information that can be inferred from the two addresses.

iii) How can a relationship between the two addresses be established?

iv) In addition to the two addresses above, the host has the following pieces of information in its network configuration:

Netmask: `255.255.253.0`
Default router: `140.225.0.1`
DNS server 1: `192.168.0.240`
DNS server 2: `140.247.1.2`

State **three** mistakes that are part of this network configuration.

The two parts carry, respectively, 55% and 45% of the marks.

Section B (Use a separate answer book for this Section)

3 Conventional *symmetric key* protocols assume that the Key Distribution Centre (KDC) maintains the list of keys it shares with the communicating parties. A typical protocol for communication between Alice (A) and Bob (B), where the KDC is denoted as T (Tom) would look as follows:

Message 1. $B \longrightarrow A: \quad \{A, msg\}_{K_{BT}}$

Message 2. $A \longrightarrow T: \quad B, \{A, msg\}_{K_{BT}}$

Message 3. $A \longrightarrow B: \quad \{B, msg\}_{K_{AT}}$

where K_{XY} represents a secret key shared by X and Y and msg a message.

Note that the KDC Tom is effectively a translator i.e., he decrypts and re-encrypts the message and is trusted to access the message plain text.

However, it is not always practical that the KDC (Tom) remembers the shared keys. It can instead issue *secret key certificates*, encrypted with its own secret key K_T which can be distributed to any party (e.g., through a web-site) and presented back to it. For example:

$T \longrightarrow B: \quad \{B, K_{BT}, L_B\}_{K_T}$ where L_B denotes a validity period

a Specify a 3 message protocol ($B \longrightarrow A$, $A \longrightarrow T$, $T \longrightarrow A$) in which secret key certificates are used by Bob to send a message to Alice.

b Specify a 2 message protocol ($B \longrightarrow T$, $T \longrightarrow B$) for Bob to renew its certificate under its old key.

c Specify a 3 message protocol ($B \longrightarrow T$, $T \longrightarrow B$, $B \longrightarrow A$) showing how a symmetric key for communication between Alice and Bob can be generated by Tom and conveyed to both parties.

d Alice and Bob are distant pen-pals. While Tom remains Bob's KDC, Alice has a different KDC called Sally (S). Assume a higher level KDC named Charlie (C) issues secret key certificates to Tom and Sally. Specify a protocol showing how Bob can obtain a symmetric key with Alice in this case. Identify clearly who generates this key.

Note: In each of the cases above you **must** explain clearly what each message achieves and you must state clearly **all** assumptions that you make. The answer must use the same notation as used above.

The four parts carry equal marks.

4a Briefly explain the functionality of the following Java RMI services: (i) Registry, (ii) Security Manager, (iii) Remote object garbage collection - explain how it works.

b A hospital ward monitoring system has a computer for each bed which monitors temperature and pulse of the patient in the bed. Every 60 seconds it reads these values and reports them to the nurse station. The nurse station updates a display showing readings for each patient. If the readings are out of range, the nurse station invokes an alarm on the nurses mobile device indicating the bed number, and current readings for temperature and pulse, as the nurse may not be at the nurse station. Assume a single nurse per ward.

A Java RMI object invocation system is used for implementation. Use the following interface specification:

```
public interface iNurse extends Remote {
   // report interface to nurse station
   public void report(int bed, int temp, int pulse)
        throws RemoteException;  }

public interface iMobile extends Remote {
   // generate alarm for nurse mobile
   public void alarm(int bed, int temp, int pulse)
        throws RemoteException;  }
```

Assume the following device control functions are available:

```
public static int deviceRead(String devName)
// used by bed monitor to read sensors  e.g. temp, pulse

public static void update(int bed, int temp, int pulse)
// used by nurse station to update its display with each bed's status
```

i) Give the Java class for the `bedMonitor` as a **client**, which is created with a parameter indicating the bed number.

ii) Give the Java class for the `nurseStation` as a **remote object** i.e. a server which is also a client of the `nurseMobile` remote object. Implementation for `nurseMobile` is not needed. Assume constants `mintemp, maxtemp, minpulse, maxpulse` for out of range detections.

Strict Java syntax is not required but your solution should indicate what is needed for instantiating remote objects, remote reference registration, binding, security and appropriate exception handling.

The two parts carry, respectively, 30%, and 70% of the marks.