IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2015

BEng Honours Degree in Electronic and Information Engineering Part II
MEng Honours Degree in Electronic and Information Engineering Part II
BEng Honours Degree in Mathematics and Computer Science Part III
MEng 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

PAPER C527

COMPUTER NETWORKS AND DISTRIBUTED SYSTEMS

Friday 1 May 2015, 14:00
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions
Calculators required

1 a State three advantages of using the *Internet Message Access Protocol (IMAP)* over the *Post Office Protocol (POP3)*.

b Briefly list two advantages and two disadvantages of using *Packet Switching* vs. *Circuit Switching* in computer networks.

c Is the *Domain Name System (DNS)* really needed for the World Wide Web? Please explain your answer. Let's suppose two DNS queries are sent one after another to resolve *www.ststephens.edu*. The first query took 393ms, while it took 13ms the second time around. What is the reason for this difference?

d Why would you sometimes use UDP (User Datagram Protocol) instead of TCP (Transmission Control Protocol) as the transport-layer protocol? Is this also the case while transferring large files? Please explain.

e What is the fundamental problem associated with TCP when it operates in a lossy wireless environment? To what extent would adding reliability at the link layer help to solve the problem? Please explain.

The five parts carry, respectively, 15%, 20%, 20%, 20%, and 25% of the marks.

2a What is *Medium Access Control (MAC)* and why is it needed in computer networks?

b Explain the CSMA/CD and CSMA/CA protocols and outline one main difference between the two. When would you choose to use one over the other?

c Suppose you have an HTML page on a web-server that contains two images (each image can fit into one TCP packet) and some text (text can fit into one TCP packet). How many TCP packets are exchanged when using **HTTP/1.0** as opposed to using **HTTP/1.1** for transferring the web-page? Show your working clearly.

d Briefly explain each of the following terms and state which layer of the OSI reference model the term relates to:

i) HTTP

ii) Network switch

iii) Subnet

iv) ARP

The four parts carry, respectively, 15%, 20%, 25%, and 40% of the marks.

3 a Briefly explain the three terms, *Confidentiality*, *Integrity*, and *Availability* in relation to providing security for distributed systems. Describe what is required in order to be able to achieve them.

b Briefly describe each of the following terms and give one example of how they can be used:

i) Packet filtering router

ii) Circuit level gateway

iii) Application level gateway

c Assume that you have just been hired by *BestSecurity Inc.*, who specialise in bespoke security solutions. Your first task is to implement an authentication system whereby messages sent between any two users (say Alice and Charlie) in the company are legally binding and can be checked later for verification purposes. You are free to assume the presence of an Arbiter (called Jailor) within the company. The Arbiter holds a secret encryption key for each user, but users can share secret keys not known to the Arbiter. The Arbiter should only be able to verify/sign but not be able to read messages between users. Let's assume that Alice sends a message Msg to Charlie. List the sequence of steps that is used to validate that the message came from Alice and that it was not modified. Please state any assumptions used, and use the following notations:

- $K_{XY}(M)$ → Message M encrypted using the secret key K known only to X and Y.

- T_X → Timestamp of X.

- $H(M)$ → Hash of message M.

- $\{F, K_{XY}\{M\}\}$ → a message containing a field F sent as plain text and a message M encrypted with a secret key K known to X and Y.

The three parts carry, respectively, 30%, 30%, and 40% of the marks.

4a Do we need the security manager when using Remote Method Invocation (RMI) in Java? Please explain.

b List three advantages of using Remote Method Invocation (RMI) compared with using Remote Procedure Call (RPC).

c Consider the function for an RPC, *call (request, reply)*, that allows a client to send a call to the server. Using the primitives *send (request)* (which allows you to send a request to the server) and *receive (reply)* (which receives the reply from the server) show the implementation of the following call semantics for the function specified above. Strict syntax is not required. You may choose to extend the primitives given to include other parameters. Please state any additional assumptions you make.

i) Maybe (Best-Effort) call semantics

ii) At-least-once call semantics

d It is project season and students are looking to choose the best project. You are to build an RPC service that allows a student to rank projects as well as view their rank for a particular project later. Each student has a unique student identification number and each project a unique project identification number. Give a pseudo-code implementation of the server-side of this system which would permit the interface to be invoked using an RPC mechanism. The RPC implementation supports *at-least-once* call semantics, but students must only rank projects once and cannot change their ranking later. You are to use the interface provided as pseudo-code below:

```
interface projectrank {
  rank (studentid, projectid, myrank)
  listrank (studentid, projectid, myrank)
}
```

The four parts carry, respectively, 15%, 15%, 30%, and 40% of the marks.