UNIVERSITY OF LONDON

IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 1999

BEng Honours Degree in Computing Part III
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
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
Associateship of the Royal College of Science

PAPER 3.35 / I 3.14

DISTRIBUTED SYSTEMS

Thursday, May 6th 1999, 2.00 – 4.00

Answer THREE questions

For admin. only:
paper contains 4 questions

1a Outline in a few sentences the main differences between the static and the dynamic invocation interfaces in CORBA. Show the circumstances in which each one would be used and their respective advantages.

b A trading system consists of several trading stations which share the service of the same stock-broker. For simplicity, assume that each trading station monitors the shares of a single company and is initialised with the share name, the number of shares held and a 'stop-loss' value for each share. If the share price falls below the 'stop-loss' value, the shares should be sold. The trading station must then display an alarm on the trader's screen, request keyboard confirmation to sell the shares and sell them through the stock-broker. The value at which the shares have been sold is then displayed on the trader's screen. Every five seconds the trading station polls a quote server to find the latest quote for the monitored share and displays the returned values on the trader's screen. The quotes obtained from the quote server contain the opening value, the current value and the change since the beginning of the trading day.

i) Assuming a CORBA like invocation system for implementation, produce a diagram indicating all the objects needed and the operation invocations between objects (only a single trading station need be shown).

ii) The interface for the trader screen is given below. Give an interface specification for each of those remaining objects which require an interface specification. (Strict IDL syntax is not required.)

```
interface Display {
    display(in string shareName, in float open, in float current, in float change);
    alarm(in string shareName);
    sold(in string shareName, in float value);
}
```

iii) Give a *pseudocode* outline for the trading station (strict CORBA syntax is not required).

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

2 A large international company wishes to provide a distributed service for looking up company services, employee phone numbers, email and postal addresses. The service should be accessible from every workstation connected to the company network. Suggest an outline design for the system with respect to the following:

a What directory structure would you suggest for storing entries? How should the information be partitioned and replicated? Justify whether a *strong* or *weak* consistency strategy should be used for updating information.

b Explain the difference between **recursive** and **iterative** lookup at a name server. Explain which you would choose for implementing a name server in a system with no support for server threads.

c Describe the functions implemented by the name service component which is needed in every workstation.

The three parts carry, respectively, 45%, 30% and 25% of the marks.

Turn over ...

3a Outline Cristian's algorithm for clock synchronisation and discuss its disadvantages and assumptions.

b An airline traffic control system has a dedicated time server receiving the Universal Coordinated Time (UTC) from Geostationary Satellites with an accuracy of ± 5 milliseconds (ms) and a set of operator workstations. The workstations and the server are interconnected by a LAN.

i) Assume a clock drift of the operator workstations with respect to the server of 2 ms/1000 seconds. How often must the workstations synchronise with the time server to ensure a time difference of less than 5 ms ?

ii) A private jet has a cruising speed of 720 Km/h. It receives UTC directly from the satellites with an accuracy of ± 5ms. The plane communicates its precise position to the operator workstation via radio-waves which incur a 10ms propagation delay. Assume the workstation is synchronised to within 5ms with the time server. What is the inaccuracy of the position of the plane as given by an air traffic control workstation due to propagation delay and time synchronisation ?

c A workstation uses Cristian's algorithm in order to synchronise with a time server. The times at which the messages are sent (T0) and received (T1) are outlined below.

T0	T1
16:32:04.220	16:32.04.234
16:32:04:250	16:32:04.262
16:32:04:275	16:32:04.307

i) Assuming the server takes less than 2 ms to reply to any time synchronisation message, calculate in each case the clock offset of the workstation with respect to the server.

ii) Explain what correction should be applied to the clock justifying which of the pairs (T0, T1) you take into account.

The three parts carry, respectively, 35%, 30% and 35% of the marks.

4a Briefly explain the differences between single secret key (symmetric) cryptography and public key (asymmetric) cryptography.

b In an electronic auction a client C wants to make an offer by sending message M to the auctioneer A. While the message can remain public it should be associated with an encrypted digital signature obtained by C from the trusted authentication server S. On receipt of the message, A asks S to decrypt the digital signature and must be able to check that the message is recent and has not been modified in transit. C, A and S each have their individual secret key and S knows all the secret keys.
Using the following notation:

$X, K_Z\{Y\}$ A message contains a field X sent as plain text and a field Y encrypted with a secret key K known to Z

i) Show how C can make the offer and how A can satisfy itself that the signature is genuine and that the message has not been tampered with. Indicate the contents of messages and explain how your system works.

ii) Can C claim that the signature was forged ?

NB. The notarisation service is **NOT** the correct protocol.

The two parts carry, respectively, 20% and 80% of the marks.

End of paper