UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 1997

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 / I3.14

DISTRIBUTED SYSTEMS

Monday, April 28th 1997, 10.00 - 12.00

Answer THREE questions

For admin. only: paper contains 5 questions

1 A building security system has a microcomputer for every room with keypad, motion detector and display. The keypad can be used to enable or disable the local motion detector. The display indicates disabled, enabled or alarm condition. Each room controller communicates with a centralised operator via a network. The current state of every room is indicated on the operator's display. The operator has a keyboard to enter room numbers and commands to enable, disable or clear an alarm for a particular room. Assume the room controller sends state information every 5 seconds to the operator.

a Assuming a Corba like object invocation system for implementation, produce a diagram indicating all the objects needed to model this security system and the operation invocations between objects (only a single room system need be shown). Using the following data types, specify in and out parameters for each operation.

```
enum keypad_data ( nochange, enable, disable);
enum opsettings ( nochange, enable, disable, clear); //operator settings
enum status ( enabled, disabled, alarm);  //alarm status to operator & to display
```

b Give a *pseudocode* outline for the room controller (strict Corba syntax is not required).

The two parts carry, respectively, 50%, 50% of the marks.

2a Describe the underlying protocol needed to cater for timeouts for the synchronous message interaction primitives:

Send (port, t, message) - sends message to port and blocks, up to t seconds waiting for it to be received.
Receive (port, msg) - blocks the receiver until a message is available on port, then it is received into variable msg.

b Briefly explain the differences between **first** and **third party binding** using Corba and Darwin as examples of each.

c Explain the function of a dispatcher for Remote procedure call implementation. Why are threads needed for implementing servers.

The three parts carry, respectively, 30%, 50%, 20% of the marks.

3a Explain the difference between **recursive** and **iterative** lookup at a name server. Explain which you would you choose for implementing a name server in a system with no support for server threads.

b Describe the function of a trader. A processing service consists of a pool of workstations which register with the trader when they are available for use. Suggest suitable properties for specifying and selecting processing servers and indicate how to deal with both **static** and **dynamic** properties.

The two parts carry, respectively, 40%, 60% of the marks.

4a Briefly discuss why global time is needed and why it is difficult to achieve.

b A clock is reading 15:00:05 (hours:min:secs) and is 5 seconds fast. Explain why it should not be reset to 15:00:00 and how it can be adjusted over a period of 10 seconds. Assume a timer interrupt is generated every 50ms to update the clock.

c Using the Network Timing Protocol, computer X sends a message to synchronise computer Y over the internet. The message is sent at 20:35:03.570 with a timestamp and is received by Y at 20:35:03.650. Y sends a response at 20:35:04.130, containing a timestamp, which is received at 20:35:04.230.

Assuming both messages have equivalent delays, show how you can calculate the delay and the clock offset of Y with respect to X.

The three parts carry, respectively, 35%, 25%, 40% of the marks.

5 The NUXI operating system encrypts passwords for storage in the filing system using a well known, one-way hash function of the password. A company has offices in Boston and London each with a NUXI system and with internet connection. Users at each site need to login to the other site. Joe Dumb, suggests that a simple solution is to exchange the password files over the internet between the two sites; as the passwords are encrypted, they cannot be read by anyone else.

a Discuss the security risks involved in sending password files across the internet. When a user in London wishes to login to Boston her password is encrypted locally using the hash function and the hashed password is sent with her identity over the internet to Boston. Explain why this is not secure.

b Assume the company actually has offices in 20 cities. Describe a suitable centralised authentication service (A) that would permit a user (U) to login to any remote company office server (S). Describe the messages between U, A and S and explain how the protocol works. Use the notation Kus{m} to indicate a message m is encrypted by a session key Kus known to U and S.

The two parts carry, respectively, 25%, 75% of the marks.

End of paper