UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2000

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
BEng Honours Degree in Mathematics and Computer Science Part III
MEng 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
This paper is also taken for the relevant examinations for the
Associateship of the Royal College of Science*

PAPER C335=I3.14

DISTRIBUTED SYSTEMS

Friday 5 May 2000, 10:00
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions

Section A **(Use a separate answer book for this Section)**

1a Explain the following call semantics associated with Remote Procedure Call Mechanisms. For each one, outline the implementation issues and give an example of where it would be used.

i) Maybe

ii) At-least-once

iii) At-most-once

b Specify the RPC interface to an Election Service which allows a client to both query the current number of votes for a specified candidates and vote for one of the set of candidates. Each client has a voter number used for identification in requests and candidates are identified by a string name.

c Give a *pseudocode* implementation for the Election Service (server only) which would permit the interface to be invoked using an RPC mechanism which supports *at-least-once* calling semantics. Explain why your implementation deals with this calling semantics.

The three parts carry, respectively, 45%, 10%, 45% of the marks.

2a Define *binding*. Explain and compare *First-party* and *Third-party* binding, indicating how they work, where they would be used and how they cope with server failures.

b Assume the election service described in Question 1 is implemented using Java RMI. Give a *pseudocode* outline for the **client** showing how it binds to the vote server whose name is coded in the client. The client reads a candidate name from the terminal, invokes a vote operation for a candidate followed by a query operation and prints the current number of votes to the terminal.

c Assuming a system supports message passing primitives. Discuss how type-checking can be accomplished in the following. In both cases, comment on what compile type-checking can be performed.

i) at bind time.

ii) at run-time when message exchanges are taking place.

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

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

3a Give a diagram showing the structure of a simple X.500/LDAP Directory Service. Briefly describe the format of a hierarchical distinguished name and explain how to make sure a name is unique when assigning it.

b What is a *trading service?* Describe what information must be provided by both clients and servers when using a trading service.

c An international company frequently reorganises the company global file system to reflect current usage. This requires migrating subtrees of the file system to servers local to where the usage is greatest. Describe a suitable file identifier and how the system locates the current position of files.

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

4a Explain what a public-key (*asymmetric*) cryptographic system is and how it can be used to both authenticate the originator of a message and provide secrecy for the data in transit. Briefly describe the advantages and disadvantages of using public-key cryptography.

b An electronic cash system allows Alice to withdraw an electronic cash token for a requested amount (e.g., £50) from her account at BA Bank to her electronic wallet. She can then use this token to pay Bob for a £50 item. Assume the token cannot be split into smaller value tokens and that Alice and Bob have the same Bank. Bob sends the token to the bank to be credited to his account, and delivers the item once he receives positive confirmation that his account has been credited.

i) Draw a diagram of the various interactions between Alice, Bob and the BA Bank, indicting the order in which they occur.

ii) Assuming a *public-key* cryptographic system, describe and explain the message contents in the interactions between Alice, Bob and the BA Bank, assuming secrecy and authentication is required. Your solution must indicate how to prevent a token being used more than once. Use the following notation:

K_{sX} {M} denotes a message encrypted with the secret key of X
K_{pX} {M} denotes a message encrypted with the public key of X

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