Where an algorithm is asked for, you may write in any suitable pseudocode. Correct syntax for any computer language is not expected.

Answer 3 questions.

1)

a) ACME RPC systems inc. have decided that they are going to expand their current business of producing RPC systems for fixed networks into producing RPC systems for mobile networks. However, there are people within the company who are arguing that RPC and mobile systems are mutually incompatible. You have been brought in as an independent consultant to write a short report outlining what the potential difficulties are in producing RPC systems for mobile environments. There are a number of questions which the company's board wish to have your opinion on:

i) What are the differences between wired RPC systems and mobile RPC systems?

ii) What sort of applications might one expect a mobile RPC system to support?

iii) To what extent would the RPC system need particular semantics of the underlying transport layer to operate efficiently? What might these requirements be, if any?

Your answer should address these points and any others that you feel the company should know about. [22]

b) The distributed shared memory model is one in which the programmer views the collection of machines on a network as a single virtual address space. References to local pages are made through local memory at full memory speed, and those to pages on other machines trap into the operating system, which then sends a message the appropriate machine to retrieve the appropriate page.

i) What are the potential advantages and disadvantages with this abstraction for use in standard LAN and WAN-based distributed systems?

ii) How well would the abstraction port to mobile systems? [11]

[TURN OVER]

2)

a) What are meant by the terms *schedule*, *serialisable*, and *two phase locking*? [6]

b) Are all correct schedules serialisable? Prove what you claim. [6]

c) Prove that if a schedule satisfies the constraints of two phase locking that it is also correct. [8]

d) 'Transactions are too heavyweight because they may give guarantees which are not always required.' Give a reasoned argument for or against this assertion, outlining the guarantees that are provided by transactions, and illustrating your answer with examples. [13]

3)

a) Explain what is meant by the term *hot standby replication*. Under what circumstances is it most useful and what assumptions must be made for it to work? Does it have any advantages over more complex mechanisms? [11]

b) A company is devising a hot standby system in which there is more than one standby object at any given point in time. If the currently active object fails, then a new active object must be chosen from among those currently passive. To do this, the company has chosen to use a leadership election algorithm. This is invoked whenever a standby notices that the active object has crashed and has the following properties:

- Each object executes the same algorithm
- The algorithm is decentralised: it cannot rely on any central point for its operation. It is possible for more than one object to initiate the algorithm simultaneously.
- The algorithm reaches a terminal configuration in which exactly one object is in the state 'leader' and all others are in the state 'standby'.

Devise and explain such an algorithm. You should assume that all objects are organised in a logical ring in such a way that each knows the identity of the next in the ring. Further you may (must) assume that each process has access to a routine call `int get_my_pid()` which returns an integer value representing the pid of the process. Argue that the algorithm that you have produced matches the above requirements and state any assumptions required in order to achieve this. [22]

[CONTINUED]

4)

The world's telephone companies have decided to get together to devise a global standard for holding telephone numbers online in a series of name servers. They have selected you to design their system.

a) What properties would the users and 'phone companies expect of such a system? [6]

b) What format would you recommend for the names, and why? [6]

c) For each of the properties you identified in a), say what protocols you would use to maintain them. [8]

d) How well would your system cope if it was used for:

   i) Migratable objects within a distributed object-based system.

   ii) Tracking the location of mobile 'phones. [8]

e) Do you believe that a single global standard is actually a desirable thing? Justify your answer. [5]

5)

a) Explain the purpose of each of the steps in the following protocol which allows two processes in the same security domain to exchange encrypted data. Your answer should clearly indicate the meaning of any notations used:

Step 1.	$A \rightarrow AS$:	A, B, I_a
Step 2.	$AS \rightarrow A$:	$\{B, I_a, K_S, \{A, K_S\}_{K_B}\}_{K_A}$
Step 3.	$A \rightarrow B$:	$\{A, K_S\}_{K_B}$
Step 4.	$B \rightarrow A$:	$\{I_b\}_{K_S}$
Step 5.	$A \rightarrow B$:	$\{f(I_b)\}_{K_S}$
Step 6.	data exchange:	$\{data\}_{K_S}$ [9]

b) Show how the protocol can be extended to deal with entities in different security domains. [3]

c) What considerations need to be taken into account in the data transfer phase between these processes? Where appropriate identify suitable solutions. [6]

[Question 5 continued over]

[TURN OVER]

[Question 5 continued]

d) Compare and contrast the way in which *Public Keys* might be managed in (i) a community only working with electronic mail and (ii) one only working with EDI (Electronic Data Interchange) for commercial transactions. In each case the community involves individuals in many organisations. Your answer should address issues of concern to governments, employers/companies and individuals. [15]

[END OF PAPER]