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) Briefly explain what is meant by a *Cryptographic Hash Function* (sometimes called *a Cryptographic Sumcheck*) and state its main properties. [5]

b) Outline two protocols for *non-repudiation* of messages in distributed systems. One of these will directly involve the use of a third party or *notary* and the other one will not. Discuss the advantages and disadvantages of each. [10]

You work as a systems administrator for a company with 500 employees that plans to install a *Public Key Infrastructure (PKI)*, i.e. be able to provide employees with secret and public keys for signing and encrypting material. At this stage the company plans to sign its employees' certificates (which will not be used for communication with other companies.)

c) Briefly describe the main functions of each of the software and hardware components that will be needed to support the appropriate use of Public Keys in the company. (Hint: you may find it easiest to draw a diagram representing the production of key-related entities and then identify and describe the major components.) [7]

d) Your operating system vendor claims to provide a Public Key Infrastructure with their latest release. Indicate any steps you would take in assuring yourself and your employer that this software is sound. [4]

e) Discuss any personnel-related issues and appropriate solutions that you would advise senior management to consider before they introduce the PKI. [7]

[TURN OVER]

2)

a) What is the role of a naming service and what properties do we require of it? [5]

b) Briefly explain the operation of the DNS system and say whether or how it meets the requirements you identified in part (a). [13]

c) ACME is a growing company that has just taken over three other companies in different parts of the world. They wish to create a distributed systems infrastructure that will allow all three companies to interwork seamlessly. Of the companies they have bought, one uses CORBA, one uses a proprietary system, and one uses a system based on DNS for object location. However, they wish to harmonise on a single approach and they are minded to make that CORBA, because the term seems to be very widely used. In you answer, explain to ACME

   i) The basics of how the CORBA naming system works and what advantages it has

   ii) Any potential problems that they may face by adopting it

   iii) Any potential advantages of adopting a different technology

   iv) Your conclusion saying whether CORBA is a good choice or not. [15]

3)

a) Explain what a *transaction* is, what its major properties are, and how it is useful. [8]

b) The *two phase commit protocol* is used for realising atomicity in a distributed system.

   i) Using pseudocode, explain its operation.

   ii) Explain what happens when messages are corrupted or nodes fail. [18]

c) *Because an approach to concurrency control based on timestamping cannot lead to deadlock, it is inherently superior to an approach based on locking, which can.*

   i) Explain why timestamping cannot lead to deadlock and why locking can.

   ii) Produce a reasoned argument either for or against the above assertion. [7]

[CONTINUED]

4)

a) Explain why a measure of reliability based on a simple percentage of the time that a node is up may be inadequate in general. [4]

b) *Voting* is a scheme for managing replicated information.

i) Explain what parameters must be selected for a replicated object when the replication scheme employs *voting*. Say which of these parameters you believe could be selected automatically and which would require human intervention.

ii) Explain, using pseudocode, how an object replicated using a voting scheme may be read and written.

iii) Does the scheme you have described maintain replication transparency in the case of node failure, message loss and partition? [22]

c) Under what circumstances or for what applications do you believe that the complexity of selecting the parameters for a voting scheme would be outweighed by its positive properties? [7]

5) The Bluetooth chip is a short range radio chip that is (or will become) sufficiently cheap to incorporate into all manner of devices, from laptops, PDAs and mobile 'phones through to VCRs, fridges and heating controllers. These devices will be connected to the Internet through cable modems, 'phone lines etc.

The consequences of this include the following two points:

- There will be a massive increase in the heterogeneity of devices connected to the Internet.

- There will be a need to develop a wide range of new applications to exploit this market.

What, in your opinion, are the implications of the development of Bluetooth (or similar technologies) for the construction of future distributed applications. Are the technologies we currently have available to us adequate? If not, what deficiencies must be addressed to allow this market to be exploited? [33]

[END OF PAPER]