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) Explain the operation of Remote Method Invocation (RMI) in Java. Your answer should cover both the method of operation and the semantics of the various actions and any support services that are required to allow an RMI call to complete. Illustrate your answer with examples. [20]

b) With what additional mechanisms would one need to enhance Java RMI to allow, say, monetary transfers from one remote bank account to another to be performed in the expectation that the results would be correct, even in the presence of failures. [13]

2) The US military are considering constructing a missile defence shield to protect themselves against attack from small numbers of nuclear missiles fired by 'rogue nations'. It is apparent that such a shield would require the interconnection of both satellite and ground-based early warning systems distributed across the globe and anti-missile launch sites. This requirement prescribes a wide-area real-time distributed system with strict consistency requirements, and continuous availability.

a) Describe in more detail the requirements of this distributed system.

b) What distributed systems issues do you believe that the US military will have to address in order to produce a workable system along the lines of the requirements you have specified in part (a)?

c) What mechanisms do you believe they should employ in addressing the issues you identified in part (b)? Comment on the practicability of implementing the system in this way and the likely level of confidence achievable in it performing as expected.

[33]

[TURN OVER]

3)

a) Explain the purpose of each of the steps in the following protocol that allows two processes in the same security domain to exchange encrypted data. Your answer should clearly indicate the meaning of any notation 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) Using any parts of the protocol in part (a) you feel to be appropriate, suggest a protocol for secret email communication among a group of 500 people. [8]

d) Access control to remote objects and their methods is needed. It has been decided that capabilities will be used, where each rights bit in the capability indicates whether the holder has access to the corresponding object function or not. For example, the capability for a particular user of a file object might permit access to the read method (read rights = 1) but not the write method (write rights = 0). It should be possible to pass capabilities as parameters in Remote Procedure Calls between clients and agents that access the object on their behalf and between clients and objects.

Discuss the security threats and suggest ways in which such capabilities can be structured and adequately protected. [13]

[CONTINUED]

4)

a) *'Message authentication codes were developed in order to satisfy the US export regulations of the time. Since these regulations have been modified to allow effectively free export, message authentication codes should be replaced by digital signatures.'*

i) Compare and contrast the concepts of a *message authentication code* and a *digital signature*.

ii) To what extent do you agree with the above statement? [6]

b) Poppleton University considers that it is failing to benefit fully from the discoveries made by its staff. As a consequence, it wishes to enforce a policy in which all information on university systems is held signed and encrypted at all times. Furthermore, it wishes to compel its staff to escrow both their encryption and signature keys so that it can replace staff and obtain access to information in the event that someone leaves or that they become ill.

i) How would you approach the implementation of such a scheme? [15]

ii) It is often said that management of secure systems is more difficult than the initial implementation. Discuss this with respect to the above scenario. [6]

iii) Answer all of the following in three or fewer sentences each:

(1) Do you believe that the invasion of privacy implied by the above scheme is justified?

(2) Would your answer change if the organisation concerned were a bank or a military installation? If so, why, if not why not?

(3) Are there any ethical principles that you believe should apply to such situations? [6]

[TURN OVER]

5)

a) Differentiate between *stream ciphers* and *block ciphers*. [4]

b) Show two different ways in which a block cipher can be used to produce a stream cipher and discuss their relative merits. [6]

c) What is *Cipher Block Chaining (CBC)*? Under what circumstances is it needed and why? [6]

d) Why are public key systems capable of general-purpose encryption normally used in conjunction with secret key systems rather than on their own? [4]

e) Explain the operation of the RSA algorithm and demonstrate that a message encrypted with an RSA public key can be decrypted with the corresponding secret key. State any assumptions you make. On what does the security of this process rely? [13]

[END OF PAPER]