

**Question 1 (Compulsory)**

- (a) Can law of nature and mental process such as  $3+2=5$  be protected by patent? Why? [2]
- (b) Programs or applications which do not behave as their designer intended or users expected; are called *program flaws*. Unfortunately we do not have techniques to stop all program flaws, give **three** reasons why it is so? [3]
- (c) How do anti-virus products detect viruses? [3]
- (d) Explain the *three* steps involved in disaster planning process. [6]
- (e) When encrypting a document using public-key cryptography, what are the advantages of performing the encryption on a one-way hash of the document rather than on the document itself? [2]
- (f) In the context of Cryptography, what is a transposition? [1]
- (g) With a public key encryption, suppose A wants to send a message to B. Let  $A_{pub}$  and  $A_{priv}$  be A's public and private key, respectively; similarly for B. If A sends a message to B, what encryption should A use so that only B can decrypt the message? (This property is called secrecy.) Can A encrypt a message so that anyone receiving the message will be assured the message came only from A? (This property is called authenticity.) Can A achieve both secrecy and authenticity for one message? How or why not? [4]
- (h) The latest FBI and Computer Security Institute studies report that two-thirds of attacks on corporate networks originate from inside the company. What does this say about the effectiveness of security measures like firewalls and identity cards? [3]

*Please turn over*

- (i) The largest single source of flaws is I/O processing. There are several reasons why I/O is a weak spot, list five of them. [5]

*Please turn over*

## Question 2

- (a) In the context of distributed systems, one might need privilege passing to be restricted. Explain briefly the term privilege passing. [2]
- (b) Multiplication of large prime numbers is one trap-door function; name another. [2]
- (c) **RAID** can be used for backup and recovery purposes. What is **Raid** and explain how it does that? [3]
- (d) One means of gaining unauthorized knowledge of data over a computer network is known as *traffic analysis*.
  - (i) Explain the process involved in traffic analysis. [1]
  - (ii) What might a traffic analyst hope to learn by the process? [1]
  - (iii) What can be done to deter traffic analysis, what is it called, and what is the assumption on which it is based? [3]
- (e) In signing an electronic document one can use the Private Key Cryptography. **Describe** Private Key Cryptography. [3]

*Please turn over*

### Question 3

- (a) A virus can pass a malicious code or other non-malicious programs modifying them. A virus can either be transient or residents. How transient and resident virus works? [4]
- (b) Identify *three* ways in which unauthorized intruders can cause security problems, *and* give a concrete example of each. [6]
- (c) When do we say a system is *secure*? What are the *two* basic methods by which the computer system security provides protection? Provide at least *one* example in each case. [5]

### Question 4

- (a) What does the term TCSEC stand for? Explain what TCSEC is. [2]
- b) Based on the TCSEC standard, there is an access control policy, in which decisions are made beyond the control of the individual owner of an object. A central authority determines what information is to be accessible by whom, and the user cannot change access rights. What is the name of this type of access control policy? Give an example of this type of access control. [2]
- (c) Biometric devices are becoming ever more popular for identification purposes. Explain what is meant by the term *biometric device*. [3]
- (d) What advantages do biometric devices have over these other means? [2]
- (e) What disadvantages do biometric devices have? [4]
- (f) What is logic bomb? [2]

*Please turn over*

**Question 5**

- (a) Explain any *two* security concerns involved in wireless communication. [2]
- (b) What are the *two* advantages of conducting disaster simulation testing? [2]
- (c) Identify the *three* characteristics that make a “good” disaster plan. [3]
- (d) Explain any *two* benefits of preventing unauthorised users or the intruders from the computer systems, by identifying the type of attack it is associated with. [4]
- (e) Provide at least *four* points to compare and contrast between link and end-to-end encryption. [4]

**-END OF PAPER-**