

**Do not award half marks.**

**In all cases give credit for appropriate alternative answers.**

**Question 1 (Compulsory)**

- (a) What is Trojan horse? Give one example how the Trojan horse works. [4]

**Answer:**

**Trojan horse is a piece of malicious code that, (1) in addition to its primary effect, has a second nonobvious malicious effect. (1)**

**An example of a Trojan horse is a login script that solicits a user's identification password, (1) passes the information on the login processing, but also retains a copy of the information for later, malicious use (1).**

**Give mark for any other alternative correct answer.**

- (b) What is logic bomb? [2]

**Answer:**

**Logic bomb is a class of malicious code (1) that “detonates” or goes off when a specified condition occurs. (1)**

- (c) A virus is a program that can pass on malicious code to other non-malicious programs by modifying them. A virus can either be a *transient* or *resident*. How transient and resident virus works? [4]

**Answer:**

**Transient virus runs when its attached program executes (1) and terminates when its attached program ends. (1)**

**Resident virus locates itself in memory so that it can remain active, (1) or be activated, even after its attached program ends. (1)**

- (d) Can virus infect hardware? Explain your answer. [2]

**Answer:**

**Viruses cannot infect hardware (1).**

**However, if hardware contains writable storage that can be accessed under program control, the storage can be attacked by virus (1).**

**Or**

**It might seem as if hardware device has been infected by virus, but the real thing is the software driver that driving the hardware has been infected (1 mark).**

- (e) Distinguish between the legal devices: copyright and Trade Secret, give examples of area where these things could be applied. [4]

**Copyrights:**

**-Are designed to protect the expression of ideas [1]**

**-Applies to a creative work, such as a program, song or story [1]**

**Trade Secret (maximum 2markss):**

**-Are designed to protect the information that gives one company a competitive edge over other (1 mark)**

**-Applies to information that has a value only as a secret [1]**

**example: formula of a soft drink or any suitable example [1]**

- (f) The RSA public key algorithm can be used for digital signature; briefly describe any two important characteristic of a signature. [4]

**Any two of the following:**

**-Unforgeable [1]: nobody else can produce the signature (1 mark)**

**-Authentic / verifiable [1]: it is possible to tell who signed (1 mark)**

**-Unalterable] 1]: any change can be detected (1 mark)**

**-Cannot be reused [1]: the signature is tied to the signed document, it cannot be transferred [1]**

(g) What are four types of protection applicable to PC files? [4]

- Access controls
- User-invoked encryption
- Copy right protection
- No protection

(h) Security functions may be isolated in a security kernel for several reasons, explain six such reasons. [6]

1. **Separation:** By isolating security mechanisms from the rest of the operating system and from the user space, it is easier to protect them from penetration by the operating system or users. [1]
2. **Unity:** All security functions are performed by a single set of code. [1]
3. **Modification:** Changes to the security mechanism are easier to make and easier to test. [1]
4. **Compactness:** Because it performs only security functions, the kernel is likely to be relatively small. [1]
5. **Verifiability:** Being relatively small, the security kernel may be proven correct in a rigorous, formal sense. [1]
6. **Coverage:** Every access to protected object must pass through the security kernel. This makes it possible to ensure that every access is checked. [1]

**If no explanation for each reason, give maximum 3 marks only.**

**Do not award half marks.**

**In all cases give credit for appropriate alternative answers.**

## **QUESTION 2**

Organisation must make regular backups and store them off site. A contingency plan should be available for the employees to continue working.

- (a) What are the differences between Full and Differential backup? [6]

### **Full Backup**

- **In a full backup, all network data is backed up.**
- **If you have to do a restore after a crash, you have only one set of tapes to restore from.**
- **Normally, full backups take several hours**

### **Differential Backup**

- **In a differential backup strategy, a single, full backup is done typically once a week. Every night for the next six nights, the backup utility backs up all files that have changed since the last full backup (the actual differential backup).**
- **After a week's worth of differential backups, another full backup is done, starting the cycle all over again.**
- **With differential backups, you use a maximum of two backup sessions to restore a file or group of files.**
- **The backup utility keeps track by using archive bit, which is simply an attribute that indicates a file's status of the current backup type. The archive bit is cleared for each file backed up during the full backup**

**(Any 3)**

- (b) System documentation is also part of backup. Why documentation is important and what is required in system documentation? [3]

- **This information is important to rebuild the network after disaster and also recover from network crash.**
- **System documentation required that you keep a full and timely record of LAN configuration.**
- **You should make sure the instruction is clear and easy to understand.**

- (c) Describe a cold site and discuss the advantages and disadvantages of a cold site. [6]

**A cold site cannot guarantee server uptime. [1]**

**It has little or no fault tolerance and relies completely on efficient disaster recovery methods to ensure data integrity. [1]**

**If a server fails, the IT personnel do their best to recover and fix the problem. [1]**

**If a major component needs to be replaced, the server stays down until the component is replaced. [1] Apart from regular system backups, no fault tolerance or disaster recovery methods are implemented. [1]**

**(Max 4 marks)**

**This type of site has one major advantage: it is the cheapest way to deal with errors and system failures. [1] No extra hardware is required (except hardware required for backing up). [1]**

**Do not award half marks.**

**In all cases give credit for appropriate alternative answers.**

### **QUESTION 3**

- (a) Some vulnerability in PC security is low awareness level and few hardware controls.

Discuss **five** other vulnerabilities. [5]

- **No audit trail**
- **No unique responsibility**
- **Environment attack**
- **Physical access**
- **Care of media, components**
- **No backup**
- **Questionable documentation**
- **Amateur quality software**
- **High portability**
- **Magnetic retention**
- **Combination of duties**

**(Any 5 of the above)**

- (b) In Operating system, there are possibilities of three known flaws. List and explain all of them. [6]

**The three known flaws:**

- **I/O Processing [1]: Most of I/O processing is outside the operating system [1] or Many I/O activities bypass the operating systems function [1]**
- **Ambiguity in access policy ;[1] Distinction between isolation and sharing is not always clear at the policy level.[1]**
- **Customise installations [1] provides opportunities to allow users to penetrate the operating system. [1]**

- (c) In data access control, there are two controls that can be used by the system, list the **two** control and explain each of them. [4]

**a) Discretionary access control (DAC): [1]**

**is an access policy that restricts access to files based on the identity of users. [1]**

**b) Mandatory access control (MAC): [1]**

**is an access policy supported for systems that process especially sensitive data.[1]**

**Do not award half marks.**

**In all cases give credit for appropriate alternative answers.**

## **QUESTION 4**

- (a) Explain **four** issues to be considered in the physical security regarding disaster recovery.

[4]

**Four issues to be considered in the physical security (1 mark each)**

- **The cost of replacing the equipment**
- **The speed with which equipment can be replaced**
- **The need for available computing power**
- **The cost of replacing data and program**

- (b) Using RSA encryption, given  $p = 7$ ,  $q = 11$ ,  $e=37$ , describe the properties that the variable  $d$  should have. In addition, find a suitable value for  $d$ . [3]

$$m = (p-1)(q-1) = 60 \quad [1]$$

$$d \text{ should be such that } d \cdot e \bmod m = 1 \quad [1]$$

$$d \cdot 37 \bmod 60 = 1$$

$$d = ((60 \cdot ?) + 1) / 37 = 13 \quad [1]$$

- (c) Cascading authentication is a prevalent issue in the context of distributed systems. What is cascading authentication? [2]

**Cascading authentication is the user or process acting on behalf of user, to be able to pass its authentication information to multiple nodes and process in network [2]**

- (d) In computer security, what is the meaning of the term biometrics? [2]

**Biometrics is the use of unique physiological, behavioural or morphological characteristics [1] to provide positive personal identification. [1]**

- (e) In physical security issues, list four ways to keep intruders out of organization [4]

**Any four of the following:**

**Dropped ceilings: Be sure the walls extend above the dropped ceiling so intruders can't climb over the walls. [1]**

**Raised floors: Be sure the walls extend down beyond the raised floor so intruders can't crawl under the raised floor. [1]**

**Air ducts: Be sure the air ducts are small enough, so intruders can't crawl through them. [1]**

**Do not use glass walls. [1]**

**Hidden Network connections. [1]**

**Do not award half marks.**

**In all cases give credit for appropriate alternative answers.**

## **QUESTION 5**

- (a) How would you estimate the likelihood or probability of a security failure occurring?

[4]

**To estimate the likelihood or probability of a security failure occurring:**

**consider past history or observed data, [1]**

**either for the general class of systems/general population or for specific system under consideration. [1]**

**estimate number of occurrences for a given time period. [1]**

**ask a number of informed individuals for their opinions. [1]**

**[max 4]**

- (b) Explain how virtual machines, such as the one defined for Java, can help to make a system more secure. [3]

**Virtual machines can help to make a system more secure as the user interacts with the virtual machine [1]**

**not the underlying operating system; [1]**

**a security failure in the virtual machine need not result in a security failure for the operating system; [1]**

**security controls can be imposed at a logical or user level if the virtual machine is more abstract. [1]**

**one mark for each of the points made above to a maximum of 2 marks; this is intended to be difficult. [max 3]**

- (c) Explain the possible disadvantages of a security kernel. [4]

**The possible disadvantages of a security kernel:**

**degradation in system performance, [1]**

**increased overhead on all operations. [1]**

**lack of modularity; [1]**

**in a large, distributed or modular system, the kernel will become too large and unwieldy. [1]**

**one mark for each of the points made above, or equally persuasive account of a disadvantage, to a maximum of 2 marks; this is intended to be difficult.**

**[max 2]**



- (d) There are several types of security modems that protect computers from unauthorised access. Explain **two** of them. [4]

**Any two of the following:**

- Call-back or dial-back modems [1]:** The modem at the computer's end figures out the telephone number of the authorised owner, and calls that number. [1]
- Password modems [1]** you must enter a password before the modem will connect you to the computer. [1]
- Encryption modems:** All information sent is encrypted. [1]
- Silent modems:** The modem won't signal that the connection has been made until the login process is begun. [1]