QUESTION 1
Sensors are used to monitor seismic activity. At the end of each day, all the data are transmitted to a central computer. This is hundreds of kilometres away. Describe one way of ensuring that the integrity of the data is retained during the transmission stage.

ANSWER 1
Parity Check
- uses even or odd parity which is decided before data sent
- each byte has a parity bit
- parity bit is set to 0 or 1 to make parity for byte correct
- after transmission, parity of each byte re-checked
- if it is different, then an error is flagged
- any reference to use of parity blocks/parity byte to (identify position of incorrect bit)

Checksum
- a calculation is carried out on the data to be sent (checksum)
- the result is sent, along with data to recipient
- checksum is re-calculated at receiving end
- if both sums are the same, no error has occurred
- if the sums are different, the data has been corrupted during transmission
- request is sent to re-send data

QUESTION 2
Description of input/output uses:
- Input of credit card number into an online form
- Selection of an option at an airport information kiosk
- Output of a single high-quality photograph
- Output of several hundred high-quality leaflets
- Input of a hard copy image into a computer

All of the above uses involve the input or output of data.

(a) Describe two methods of preventing accidental loss of data.
(b) Describe one way of ensuring the security of the data against malicious damage.

ANSWER 2
(a) frequent (or equivalent) backup EITHER to secondary media/to 3rd party server/cloud/removable devices/continuous backup OR stored remotely
- disk-mirroring strategy/RAID
- UPS (uninterruptable power supply)/backup generator

(b) protection of data (or equivalent) with passwords/using password and username for logging on include e.g. fingerprint scanning
- encryption
• installation and use of up to date anti-malware/anti-virus
• give different access rights to different users
• use a firewall,
• physical methods/lock doors and use secure entry devices/CCTV

QUESTION 3
(a) Give the definition of the terms firewall and authentication. Explain how they can help with the security of data.

(b) Describe two differences between data integrity and data security.

ANSWER 3
(a) Firewall
• sits between the computer or LAN and the Internet/WAN and permits or blocks traffic to/from the network
• can be software and/or hardware
• software firewall can make precise decisions about what to allow or block as it can detect illegal attempts by specific software to connect to Internet
• can help to block hacking or viruses reaching a computer

Authentication
• process of determining whether somebody/something is who/what they claim to be
• frequently done through log on passwords/biometrics
• because passwords can be stolen/cracked, digital certification is used
• helps to prevent unauthorised access to data

(b) • integrity deals with validity of data/freedom from errors/data is reasonable
• security deals with protection of data
• security protects data from illegal access/loss
• integrity deals with making sure data is not corrupted after, for example, being transmitted

QUESTION 4
What we mean by the term ‘IT Security’?

ANSWER 4
IT Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction.

QUESTION 5
What we mean by the term ‘Confidentiality’?

ANSWER 5
Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems.
For example, a credit card transaction on the Internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in databases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored. If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.
QUESTION 6
What we mean by the term ‘Integrity’?

ANSWER 6
In information security, Integrity means that data cannot be modified without permission. Integrity is violated when
• an employee accidentally or with malicious intent deletes important data files
• a computer virus infects a computer
• an employee is able to modify his own salary in a payroll database
• an unauthorized user vandalizes a web site
• someone is able to cast a very large number of votes in an online poll.

QUESTION 7
What are the security measures designed to protect computer systems?

ANSWER 7
• Authentication and Authorization
• Firewall
• Password Protection
• Digital Signatures

QUESTION 8
Briefly explain Authentication and Authorization.

ANSWER 8
• Remove or disable accounts upon loss of eligibility: Accounts which are no longer needed must be disabled in a timely fashion using an automated or documented procedure.

• Separate user and administrator accounts: Administrator accounts must not be used for non-administrative purposes. System administrators must be provisioned with non-administrator accounts for end-user activities, and a separate administrator account that is used only for system-administration purposes.

• Use unique passwords for administrator accounts: Privileged accounts must use unique passwords that are not shared among multiple systems.

• Throttle repeated unsuccessful login-attempts: A maximum rate for unsuccessful login attempts must be enforced. Account lockout is not required, but the rate of unsuccessful logins must be limited.

• Enable session timeout: Sessions must be locked or closed after some reasonable period.

• Enforce least privilege: Non-administrative accounts must be used whenever possible. User accounts and server processes must be granted the least-possible level of privilege that allows them to perform their function.

QUESTION 9
Briefly explain Firewall.

ANSWER 9
• Systems must be protected by a firewall that allows only those incoming connections necessary to fulfill the business needs of that system.
• Client systems which have no business need to provide network services must deny all incoming connections. Systems that provide network services must limit access to those services to the smallest reasonably manageable group of hosts that need to reach them.
QUESTION 10
Briefly explain **Password Protection**.

ANSWER 10
All accounts and resources must be protected by passwords which meet the following requirements, which must be automatically enforced by the system:
- Must be at least 8 characters long.
- Must NOT be dictionary or common slang words in any language, or be relatively easy to guess.
- Must include at least 3 of the following 4 characteristics, in any order: upper case letters, lower case letters, numbers, and special characters: !@#$%^&*
- Must be changed at least once per year.

QUESTION 11
Briefly explain **Digital Signature**.

ANSWER 11
- It is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is **authentic**.
- Authentic means that you know who created the document and you know that it has not been altered in any way since that person created it.
- Digital signatures rely on certain types of **encryption** to ensure authentication.
- Encryption is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode.
- Authentication is the process of verifying that information is coming from a trusted source.
- These two processes work hand in hand for digital signatures.

QUESTION 12
What are the **security measures** designed to protect the **security of data**?

ANSWER 12
- Data Backup
- Encryption
- Access Rights
- Disk mirroring strategy

QUESTION 13
Briefly explain **Data Backup**.

ANSWER 13
Data protection is crucial for protecting your business’s continuity. If you only data backup is on a computer and the hard disk is damaged, your business’s data is gone.
For adequate data protection, you need to establish a data backup system that follows these 3 steps:
- Archive the business data regularly
- Create data backups on reliable media
- Keep updated data backups in a secure, off-site location

QUESTION 14
Briefly explain **Encryption**.
1.6 SECURITY, PRIVACY AND DATA INTEGRITY

**ANSWER 14**
- The translation of data into a secret code.
- **Encryption** is the most effective way to achieve data security.
- To read an encrypted file, you must have access to a secret key or password that enables you to **decrypt** it.
- Unencrypted data is called **plain text**; encrypted data is referred to as **cipher text**.
- There are 2 main types of encryption: **asymmetric encryption** and **symmetric encryption**.

**QUESTION 15**
Briefly explain **Symmetric Encryption**.

**ANSWER 15**
- **Symmetric encryption** is where the **same key** is used to **encrypt** and **decrypt** the message.

**QUESTION 16**
Briefly explain **Asymmetric Encryption**.

**ANSWER 16**
- **Asymmetric encryption** uses **one key** to **encrypt** a message and **another key** to **decrypt** the message.

**QUESTION 17**
Briefly explain **Access Rights**.

**ANSWER 17**
- **Access rights** is a mechanism by which a system gives the right to access some data, or perform some action.
- Normally a user must first **Login** to a system.
- Next the **Access Control** mechanism will control what operations the user may or may not make by comparing the **User ID** to an **Access Control database**.
- **Access Control** systems include:
  - **File permission**, such as create, read, edit or delete on a file server.
  - **Program permissions**, such as the right to execute a program on an application server.
  - **Data rights**, such as the right to retrieve or update information in a database.

**QUESTION 18**
Briefly explain **Disk mirroring strategy**.

**ANSWER 18**
- **Disk mirroring** is a real-time strategy that writes data to two or more disks at the same time.
- If one disk fails, the other continues to operate and provide access for users.
- Server mirroring provides the same functionality, except that an entire server is duplicated.
- This strategy allows users to continue accessing data if one of the servers fails.

**QUESTION 19**
Briefly explain **Replication**.

**ANSWER 19**
- **Replication** copies information to alternate servers on distributed networks to make that information more readily available to people in other locations.
- While replication is not necessarily a backup technique, replicated data on remote servers can be made available to local users should the server close to them go down.
DATA INTEGRITY

QUESTION 1
Data integrity is required at the input stage and also during transfer of the data.
(i) State two ways of maintaining data integrity at the input stage. Use examples to help explain your answer.
(ii) State two ways of maintaining data integrity during data transmission. Use examples to help explain your answer.

ANSWER 1
(i) **Validation** (to ensure data is reasonable)
   • examples include range checks, type checks, length checks, ...

   **Verification** (checks if data input matches original/if transmitted data matches original)
   • can use double data entry or visual check/other methods such as parity checks
   • doesn’t check whether or not data is reasonable

(ii) **Parity Checking**
   • one of the bits is reserved as parity bit
   • e.g. 1 0 1 1 0 1 1 0 uses odd parity
   • number of 1s must be odd
   • parity is checked at receiver’s end
   • a change in parity indicates data corruption

   **Check Sum**
   • adds up bytes in data being sent and sends check sum with the data
   • calculation is re-done at receiver’s end
   • if not the same sum then the data has been corrupted during transmission

QUESTION 2
(a) Give a brief description of each of the following terms: **Validation** and **Verification**.

(b) Data are to be transferred between two devices. **Parity checks** are carried out on the data. Explain what is meant by a **parity check**. Give an example to illustrate your answer

ANSWER 2
(a) **Validation**
   – check whether data is reasonable / meets given criteria

   **Verification**
   – method to ensure data which is copied / transferred is the same as the original
   – entering data twice and computer checks both sets of data
   – check entered data against original document / source

(b) – parity can be even or odd
    – parity check uses the number of 1s in a binary pattern
    – if there is an even / odd number of 1s, then the parity is even / odd
    – following transmission ...
    – parity of each byte checked
– a parity bit is used to make sure binary pattern has correct parity
– example: 1 0 0 1 0 1 1 1 has parity bit set to 1 in MSB since system uses odd parity (original data: 0 0 1 0 1 1 1 which has four 1 bits)

**QUESTION 3**

Verification and validation can be applied during data entry. Describe what is meant by these terms. For each method, explain why it is needed.

**ANSWER 3**

**Verification**

- needed to ensure that the data entered exactly matches the original source/data is consistent
- comparison of two versions of the data
- examples include double entry, visual checking, proof reading etc...
- does not check data is sensible/acceptable

**Validation**

- needed to check that the data entered is sensible/reasonable/acceptable/matches required criteria
- automatic check by computer
- examples include range, type, length, etc.
- does not check data is correct

**QUESTION 4**

When data is transmitted, it may become corrupted.

(a) Explain how a parity check can be used to detect a possible error in a transmitted byte.

(b) Describe how parity can be used to identify and correct the single error in this transmitted data block.

\[
\begin{array}{cccccccccc}
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
\end{array}
\]

**Parity byte**

\[
\begin{array}{cccccccccc}
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{array}
\]

**ANSWER 4**

(a) - type of parity (odd or even) is agreed by both devices concerned with the communication
- transmitting device counts number of 1 bits in the byte
- one bit is reserved for parity bit
- this parity bit is set to 1 or 0 in order to make the number of 1s in the byte an odd or even number dependent on what type of parity is used
- receiving device on receipt of byte counts number of 1s
- ...odd number of 1s in even parity gives an error/even number of 1s in odd parity gives error
QUESTION 5

The following bytes of data are sent to a second device using even parity:

01001101
10001000
10101011
00011011
00011011

An automatic checking technique is used to check that the data has been transmitted without error.

(a) State which byte has been received incorrectly, explaining how you arrived at your answer.

(b) Explain why it is possible that a byte of data could still be incorrect despite passing the test that you used in part (a).

(c) If the parity byte 11110101 had been transmitted with the data block, explain how the error could be self checked and corrected.

ANSWER 5

(a) - The third byte, 10101011, is in error.
- Bytes should pass a parity check.
- The other bytes have an even number of ones while this one has an odd number of ones.

(b) If two bits in the same byte are in error, they will cancel out each other.

(c) - All columns should have an even number of ones in order to be of even parity.
- The first column has an odd number of ones . . .
- . . . therefore the error is in the first column and the third row.
- The correct data byte in the third row is 00101011.