UNIVERSITY OF PROFESSIONAL STUDIES, ACCRA


NAME: OSAFO PAUL PARRY

PROGRAMME: BSc INFORMATION TECHNOLOGY

COURSE: INFORMATION SYSTEMS SECURITY

COURSE CODE: BSIT309

INDEX NUMBER: 10309590

DATE: 14th September 2025

# QUESTIONS

1. Give five (5) examples or scenarios each, that define: Confidentiality, Integrity & Availability (CIA)

Look for concepts that help define:

2. Confidentiality Mechanism

3. Integrity Mechanism

4. Availability Mechanism

5. Find case study/scenario examples for: Zombies, Botnets, Honeypots

6. Find out the various System Security Technologies and explain how a layered security approach could be designed.

Examples: Antivirus, Firewalls, ACLs, etc.

# ANSWERS

## Question 1

**Confidentiality**

It is about protecting sensitive data from being seen or stolen by unauthorized users. This is usually done through passwords, encryption, and access controls.

Examples of confidentiality:

- A hospital allowing only doctors and nurses to view a patient's medical records.
- Logging into your email with a password so strangers can't read your messages.
- A company encrypting files before storing them in the cloud.
- A bank worker not giving out customer details to someone without permission.
- A social media account set to "private" so only friends can see your posts.

**Integrity**

Integrity means keeping information accurate, correct, and trustworthy. It ensures that data is not changed, corrupted, or tampered with, whether by accident or on purpose

Examples of integrity:

- An online banking system always showing the correct account balance.
- A student's assignment submitted online arriving exactly as uploaded, not corrupted.
- Software updates being digitally signed to prove they haven't been altered.
- A voting system making sure votes are counted correctly without being changed.
- A database backup restoring records exactly as they were.

**Availability**

Availability means making sure information and systems are accessible whenever they are needed. This is ensured with reliable systems, backups, and good maintenance.

Examples of availability:

- An online shopping site staying up during Black Friday sales.
- Students being able to access the school's portal during exam registration.
- A hospital's emergency system always being accessible to doctors.
- Cloud storage services like Google Drive being available at all times.
- Bank ATMs working so customers can withdraw money any time.

## Question 2

**Encryption**

Encryption is the process of converting data into a coded form that can only be read by someone who has the correct decryption key.

Example: When you send a WhatsApp message, it is encrypted so that only the person you are chatting with can read it.

**Access Controls**

Access controls determine who is allowed to use certain resources or data. This could be role-based (like an admin vs. a normal user) or rule-based.

Example: A company might restrict access to financial records so only the finance department can view them.

**Authentication**

Authentication is the process of verifying the identity of a user before giving them access. This usually involves passwords, biometrics, or multi-factor authentication.

Example: Logging into your Gmail account using both your password and a code sent to your phone.

**Physical Security**

Confidentiality is not only digital but also physical. This includes protecting devices, servers, and files from being stolen or accessed by unauthorized people.

Example: Locking server rooms and restricting who can enter with ID badges.

## QUESTION 3

**Hash Functions**

A hash function generates a unique fixed-length value (hash) for data. If the data changes even slightly, the hash value changes completely, helping detect tampering.

Example: A file download is checked against its original hash value to confirm it hasn't been modified.

**Digital Signatures**

Digital signatures combine hashing and encryption to verify the authenticity of data and confirm it hasn't been altered. They also prove who sent the data.

Example: An email with a digital signature assures the receiver that it truly came from the sender and wasn't changed in transit.

**Checksums**

A checksum is a simple calculation performed on data to detect errors during transmission or storage. If the checksum doesn't match, the data has been corrupted.

Example: When downloading software, a checksum ensures the file is complete and unaltered.

**Version Control Systems**

These systems track changes made to files or code over time, allowing rollback to a correct version if errors or tampering occur.

Example: Developers using Git to keep track of changes in source code.

**Audit Trails and Logging**

Logging records of who accessed or changed data helps detect unauthorized modifications and provides evidence in case of a breach.

Example: A hospital keeping logs of which doctor viewed or edited a patient's medical record.

**Input Validation**

This ensures that only correct and expected data can be entered into a system, preventing corruption or malicious input (like SQL injections).

Example: A web form checking that a phone number field contains only numbers.

## QUESTION 4

**Redundancy**

Redundancy means having backup components (servers, power supplies, network links) so if one fails, another takes over immediately.

Example: A data center using multiple internet connections so that if one goes down, traffic switches to the other.

**Disaster Recovery (DR) & Business Continuity Planning (BCP)**

DR focuses on restoring IT systems after a disaster, while BCP ensures the business can still operate during and after disruptions.

Example: A company using backup data centers in another region to quickly recover if the main one fails.

**High Availability (HA) Clustering**

This involves linking multiple servers together so if one fails, another takes over without downtime.

Example: An online banking system using clustered servers so customers can always access their accounts.

**Load Balancing**

Load balancing spreads workloads across multiple servers to prevent overload and keep services running smoothly.

Example: A popular e-commerce site using load balancers during Black Friday sales to handle high traffic.

**Regular Maintenance & Updates**

Keeping systems updated, patched, and maintained reduces the risk of crashes or vulnerabilities that can affect availability.

Example: IT staff updating a server's software at scheduled times to prevent failures.

**DDoS Protection**

Distributed Denial of Service (DDoS) attacks flood a system with traffic to make it unavailable. DDoS protection tools help absorb or block this traffic.

Example: A gaming platform using DDoS protection to keep servers online during cyberattacks.

# QUESTION 5

**Zombies**

Explanation: In cybersecurity, a zombie computer is one that has been secretly taken over by a hacker, usually through malware, and is controlled remotely without the owner knowing.

Case Study Example:

In 2016, many home users unknowingly had their personal computers infected with malware that turned them into zombies. These infected machines were later used as part of the Mirai botnet to launch attacks on large websites. The owners didn't realize their devices were being controlled in the background.

**Botnets**

Explanation: A botnet is a network of zombie computers or devices controlled by hackers to carry out coordinated attacks, like spreading spam or launching Distributed Denial of Service (DDoS) attacks.

Case Study Example:

The Mirai Botnet attack (2016) is one of the most famous cases. Hackers infected thousands of IoT devices (like cameras and routers) and used them to flood Dyn, a major DNS provider. This caused huge platforms like Twitter, Netflix, and Reddit to go offline for hours.

**Honeypots**

Explanation: A honeypot is a decoy system set up to attract hackers and study their behavior. It looks like a real target but is actually a trap.

Case Study Example:

Researchers at Kippo Honeypot Project created a fake SSH server to observe how hackers break into systems. They discovered that hackers often used automated tools to guess weak passwords like "123456"

or “password.” The honeypot allowed researchers to collect attack data without putting real systems at risk.

# QUESTION 6

**System Security Technologies**

- Antivirus: Detects and removes malware on computers.
- IPS/IDS: IDS detects suspicious activity; IPS blocks it in real time.
- Firewalls: Filter traffic between internal and external networks.
- VPNs: Secure and encrypt online connections, especially for remote access.
- Encryption: Makes data unreadable without the right key.
- ACLs (Access Control Lists): Restrict which users or systems can access certain resources.

**How a Layered Security Approach Could Be Designed**

At the perimeter layer, firewalls would be set up to filter traffic entering the network, while intrusion detection and prevention systems (IDS/IPS) would be responsible for monitoring and blocking suspicious activities.

Moving to the network layer, secure communication can be achieved through Virtual Private Networks (VPNs), particularly for remote users, and Access Control Lists (ACLs) would be applied to regulate which users or devices are permitted to access specific areas of the network.

At the host layer, security measures such as antivirus software would be deployed to protect endpoints from malware, alongside regular system updates and patches to address vulnerabilities and reduce risks of exploitation.

In the data layer, encryption would be used to ensure that sensitive information remains unreadable even if stolen, while routine backups would guarantee that data remains available in the event of loss or corruption.

Finally, at the user layer, strong authentication methods such as multi-factor authentication would help prevent unauthorized access, while policies and training programs would guide users on safe practices, including how to identify phishing attempts, use strong passwords, and browse securely.