# Network Fundamentals

## Key Terms

| Term | Definition |
|---|---|
| **Bit** | A binary digit (0 or 1), the smallest unit of information in computing. |
| **Byte** | A group of 8 bits treated as a single unit, used to represent data. |
| **Software** | Computer programs and data that can be changed or modified by the user. |
| **Network** | A system of connected devices like routers, hubs, and cables that communicate. |
| **Defense-in-Depth** | A security approach that uses multiple layers of defense, including people, technology, and operations. |
| **Authentication** | Verifying the identity of a user or device to ensure access is granted to the correct entity. |
| **Authorization** | Confirming that a user or system has permission to access specific resources or perform certain actions. |
| **Identification** | The process of confirming and asserting a user's or system’s identity. |
| **Confidentiality** | Keeping sensitive information private and ensuring it's accessible only to authorized users. |
| **Integrity** | Protecting information from being changed, corrupted, or destroyed. |
| **Availability** | Ensuring that data and systems are available and accessible when needed. |
| **Non-Repudiation** | Preventing someone from denying their actions, such as sending a message or performing a task. |
| **Vulnerability** | A weakness in a system or network that can be exploited by an attacker. |
| **Threat** | A potential source of harm that exploits vulnerabilities to cause damage. |
| **Risk** | The chance that a threat will exploit a vulnerability and cause harm. |
| **Threat Actor** | An individual or group that uses threats to exploit system weaknesses and cause damage. |

## Summary of the CIA Triad

The **CIA Triad** is a core concept in information security, representing three key principles that help secure data and systems:

### 1. Confidentiality

- Ensures that sensitive information is only accessed by those who are authorized.

- **Techniques Used**:
    - Encryption (protects data by converting it into a secure format)
    - Access controls (limits access to authorized users)
    - Authentication (verifies the identity of users)
    - Data classification (organizes data based on its sensitivity)

### 2. Integrity

- Ensures that data is accurate, complete, and not altered by unauthorized users.
- **Techniques Used**:
    - Checksums (used to detect errors in data)
    - Hashing (ensures data has not been tampered with)
    - Digital signatures (verifies the authenticity of the data)
    - Version control (keeps track of changes to data)

### 3. Availability

- Ensures that data and resources are accessible when needed by authorized users.
- **Techniques Used**:
    - Redundancy (having backups or alternatives available if something fails)
    - Backups (copying data so it can be restored if lost or corrupted)
    - Failover systems (systems that automatically switch to backup resources in case of failure)
    - Disaster recovery plans (strategies for recovering from major failures)

---

## Key Takeaways

- The **CIA Triad** (Confidentiality, Integrity, and Availability) is the foundation of information security.
- **Confidentiality** ensures data is kept private.
- **Integrity** ensures that data is accurate and not tampered with.
- **Availability** ensures that data and systems are accessible when needed.
- Understanding these principles helps in designing and evaluating security measures and policies.