VERY SHORT ANS QNS ISS

---

1. Why is information system security required for an organization?

Information system security is needed to protect an organization's data, systems, and networks from unauthorized access, cyber threats, and data breaches. It ensures **confidentiality, integrity, and availability (CIA)** of information, preventing financial loss, reputation damage, and legal consequences.

---

2. What is a threat in an information system?

A **threat** in an information system is any potential danger that can exploit vulnerabilities to cause harm. It can be **internal (e.g., insider misuse)** or **external (e.g., hacking, malware, phishing, DDoS attacks)** and may lead to data loss, system damage, or unauthorized access.

---

3. Define Digital Signature and PKI with components.

✓ **Digital Signature:** A cryptographic technique used to verify the authenticity and integrity of a digital message or document. It ensures **authentication, integrity, and non-repudiation** using a private key for signing and a public key for verification.

✓ **PKI (Public Key Infrastructure):** A security framework that manages **digital certificates and encryption keys** for secure communication.

🔹 **Components of PKI:**

1. **Certificate Authority (CA):** Issues and manages digital certificates.
2. **Registration Authority (RA):** Verifies user identities before certificate issuance.
3. **Public and Private Keys:** Used for encryption and decryption.

---

4. Differentiate symmetric cryptography with asymmetric cryptography.

Feature	Symmetric Cryptography	Asymmetric Cryptography
Definition	Uses a **single secret key** for both encryption and decryption.	Uses a **public key for encryption** and a **private key for decryption**.
Security	Less secure as the same key is used.	More secure due to separate key pairs.

Feature	Symmetric Cryptography	Asymmetric Cryptography
Speed	Faster	Slower
Examples	AES, DES	RSA, ECC

---

5. Define Honeypots, Port Scanner, Packet Sniffers, and VPN.

✓ **Honeypots:** A **decoy system** designed to attract cyber attackers and analyze their activities without exposing real network assets.

✓ **Port Scanner:** A tool that scans network ports to detect **open, closed, or filtered ports**, helping in security assessments and identifying vulnerabilities.

✓ **Packet Sniffers:** A network monitoring tool that captures and analyzes data packets transmitted over a network, used for **troubleshooting or detecting cyber threats**.

✓ **VPN (Virtual Private Network):** A secure network connection that **encrypts data traffic** and masks IP addresses, ensuring **privacy and security** over public or untrusted networks.

---

6. Define NIST Security Model.

The **NIST Security Model**, developed by the **National Institute of Standards and Technology (NIST)**, provides a framework for securing information systems. It includes **five key functions:**

✓ **Identify** – Recognize assets, risks, and vulnerabilities.
✓ **Protect** – Implement security measures like access control and encryption.
✓ **Detect** – Monitor networks for threats and anomalies.
✓ **Respond** – Take action to mitigate security incidents.
✓ **Recover** – Restore systems and operations after a security breach.

---

7. What is the role of risk assessment?

Risk assessment helps identify, evaluate, and prioritize potential security risks in an organization. Its main roles include:

✓ **Identifying threats and vulnerabilities** in IT systems.
✓ **Determining the impact** of security breaches.

✓ **Developing risk mitigation strategies** to minimize damage.
✓ **Ensuring compliance** with legal and industry standards (e.g., ISO 27001, GDPR).

---

8. In which situation is Disaster Recovery Planning useful?

Disaster Recovery Planning (DRP) is useful in scenarios where an organization faces **unexpected disruptions** such as:

✓ **Natural disasters** – Earthquakes, floods, or fires affecting data centers.
✓ **Cyberattacks** – Ransomware, DDoS attacks, or data breaches.
✓ **Hardware failures** – Server crashes or power outages.
✓ **Human errors** – Accidental data deletion or misconfigurations.

DRP ensures **business continuity** by restoring critical systems and data after an incident.

---

9. What kinds of digital forensic facilities are available in Nepal?

In Nepal, digital forensic facilities are still developing but include:

✓ **Nepal Police Cyber Bureau** – Investigates cybercrimes and digital fraud.
✓ **Nepal Rastra Bank (NRB) IT Department** – Handles forensic analysis for financial frauds.
✓ **Private Cybersecurity Firms** – Provide forensic investigation services.
✓ **University Research Labs** – Conduct studies on digital forensics.
✓ **Computer Emergency Response Teams (CERT-NP)** – Help in handling cybersecurity incidents.

These facilities focus on **data recovery, cybercrime investigation, and fraud detection**.

---

10. Why are Ethical Concepts important for IT Professionals?

Ethical concepts are crucial for IT professionals because they:

✓ **Ensure data privacy and security** – Protect user and organizational data.
✓ **Prevent cybercrimes** – Discourage hacking, fraud, and misuse of technology.
✓ **Promote trust and professionalism** – Maintain integrity in IT work.

✓ **Ensure compliance with laws** – Follow regulations like GDPR and cybersecurity laws.
✓ **Prevent misuse of power** – Avoid unethical activities like insider threats.

Ethics help IT professionals act responsibly and **protect users and organizations**.

---

11. Define Information System and write its types.

✓ **Definition:** An **Information System (IS)** is a combination of **hardware, software, people, and processes** used to collect, store, and manage data for decision-making.

✓ **Types of Information Systems:**

1. **Transaction Processing System (TPS)** – Processes business transactions (e.g., ATM systems).
2. **Management Information System (MIS)** – Helps managers with reports and analytics.
3. **Decision Support System (DSS)** – Aids in complex decision-making (e.g., forecasting tools).
4. **Enterprise Resource Planning (ERP)** – Integrates business processes (e.g., SAP, Oracle).
5. **Customer Relationship Management (CRM)** – Manages customer data (e.g., Salesforce).

---

12. Compare Public Key and Private Key.

Feature	Public Key	Private Key
Definition	A key used for encryption, shared openly.	A secret key used for decryption.
Usage	Encrypts data or verifies digital signatures.	Decrypts data or creates digital signatures.
Security	Can be shared publicly without risk.	Must be kept confidential.
Example Algorithms	RSA, ECC	RSA, ECC

Example:
✓ **Public Key:** Used to encrypt a message before sending it securely.
✓ **Private Key:** Used by the receiver to decrypt the message.

---

13. What are the types of firewalls used in information security?

Firewalls are categorized based on their functionality and filtering methods:

1. **Packet Filtering Firewall** – Inspects packets and allows or blocks them based on rules.
2. **Stateful Inspection Firewall** – Tracks active connections and decides traffic flow based on the session state.
3. **Proxy Firewall** – Acts as an intermediary between users and the internet for security.
4. **Next-Generation Firewall (NGFW)** – Combines traditional firewall features with **intrusion detection/prevention and deep packet inspection**.
5. **Circuit-Level Gateway** – Verifies the security of a connection before data transmission.

---

14. What do you mean by IoT? Write its uses.

✓ **IoT (Internet of Things):** A network of **interconnected smart devices** that communicate and exchange data over the internet without human intervention.

✓ **Uses of IoT:**

1. **Smart Homes** – Home automation systems (e.g., Alexa, smart thermostats).
2. **Healthcare** – Remote patient monitoring and wearable devices.
3. **Industrial Automation** – Smart factories with automated machines.
4. **Transportation** – GPS tracking, smart traffic management.
5. **Agriculture** – Smart irrigation and weather monitoring.

---

15. What are the information security risks?

✓ **Information security risks** refer to threats that can compromise data **confidentiality, integrity, or availability (CIA Triad)**. Common risks include:

1. **Cyberattacks** – Hacking, phishing, ransomware.
2. **Insider Threats** – Employees misusing access.
3. **Data Breaches** – Unauthorized access to sensitive data.
4. **Malware Infections** – Viruses, trojans, spyware.
5. **Weak Passwords** – Easily guessable credentials leading to unauthorized access.

---

16. Why do firms need an information security plan?

Firms need an **information security plan** to:

✓ **Protect sensitive data** from unauthorized access or cyberattacks.
✓ **Ensure business continuity** by preventing disruptions.
✓ **Comply with legal and industry regulations** (e.g., ISO 27001, GDPR).
✓ **Maintain customer trust and reputation** by preventing data breaches.
✓ **Reduce financial losses** from cyber incidents and fraud.

An effective security plan includes **risk assessments, security policies, incident response strategies, and employee training**.

---

17. What are Affidavits and Warrants?

- **Affidavit**: A written statement made under oath, used as evidence in court. It confirms facts but is not the same as testimony in a trial.
- **Warrant**: A legal document issued by a judge that allows authorities to take specific actions, such as arresting someone (arrest warrant) or searching a location (search warrant).

---

18. What is Professional Ethics?

Professional ethics refers to the moral principles and rules that guide behavior in a specific profession. It ensures honesty, fairness, responsibility, and respect while performing job duties. Examples include medical ethics for doctors and cybersecurity ethics for IT professionals.

---

19. What are the Critical Characteristics of Information?

Information should have these key qualities to be valuable and secure:

- **Confidentiality** – Only authorized people can access it.
- **Integrity** – The information must be accurate and unchanged.
- **Availability** – It should be accessible when needed.
- **Authenticity** – The source of information must be trustworthy.
- **Non-repudiation** – The sender cannot deny sending the information.

---

20. What do you mean by Deviations in QoS in the Context of Threats and Attacks?

QoS (Quality of Service) refers to the performance of a network, like speed, reliability, and availability. Deviations in QoS occur when threats or attacks disrupt normal operations. Examples include:

- **DoS (Denial of Service) attacks** – Overloading a network to slow it down or shut it down.
- **Latency issues** – Delays in data transmission due to cyberattacks.
- **Packet loss** – When data packets are lost due to network attacks.
- **Jitter** – Inconsistent data flow causing disruptions in services like video calls.

---

21. Briefly introduce about SET.

✓ **SET (Secure Electronic Transaction)** is a security protocol designed to secure **online credit card transactions**. It was developed by **Visa and MasterCard** to ensure **confidentiality, integrity, and authentication** in e-commerce transactions.

✓ **Key Features:**

- Uses **encryption** for secure data transmission.
- Requires **digital certificates** for user authentication.
- Protects both **customers and merchants** from fraud.

---

22. Define Information System Audit.

✓ **Information System Audit (IS Audit)** is a process of evaluating an organization's **IT systems, security policies, and controls** to ensure **data accuracy, reliability, and security**.

✓ **Purpose:**

- Detect and prevent **security vulnerabilities**.
- Ensure **compliance** with regulations (e.g., ISO 27001, GDPR).
- Improve **IT governance and risk management**.

---

23. For what purposes is Digital Forensic done?

✓ **Digital Forensics** is conducted to investigate and analyze **digital evidence** for:

1. **Cybercrime Investigations** – Identifying hackers, fraud, and online threats.
2. **Legal Proceedings** – Collecting evidence for court cases.
3. **Data Recovery** – Retrieving lost or deleted data.
4. **Insider Threat Detection** – Investigating employees' unauthorized activities.
5. **Network Security Breaches** – Analyzing cyberattacks and preventing future incidents.

---

24. What are the three main characteristics of a Hash Function?

✓ **A hash function must have:**

1. **Deterministic** – The same input always produces the same output.
2. **Irreversible** – It should be computationally impossible to **reverse-engineer** the original input from the hash value.
3. **Collision-Resistant** – No two different inputs should generate the same hash value.

🔻 **Example:** SHA-256, MD5, and SHA-1 are commonly used cryptographic hash functions.

---

25. What are the Ethical Concepts in Information Security?

Ethical concepts in **Information Security** ensure that data is protected while maintaining fairness and responsibility. Key principles include:

- **Confidentiality** – Keeping sensitive data private.
- **Integrity** – Ensuring information is not altered by unauthorized people.
- **Availability** – Ensuring data is accessible when needed.
- **Accountability** – Users must take responsibility for their actions.
- **Honesty** – Avoiding deceptive or fraudulent activities.
- **Compliance** – Following laws, policies, and best practices.
- **Respect for Privacy** – Not misusing personal or confidential data.

---

26. What is Business Resumption Planning?

Business Resumption Planning (BRP) is a **strategy to restore business operations** after a disruption (like cyberattacks, natural disasters, or system failures). It focuses on:

- **Recovering IT systems** and essential data.
- **Restoring business functions** quickly to reduce downtime.
- **Ensuring employees know their roles** during a crisis.
- **Minimizing financial losses** and protecting customers.
  It is a part of **Business Continuity Planning (BCP)** but mainly focuses on getting back to normal operations.

---

27. What is an IPsec Tunnel? Where is it used?

IPsec (Internet Protocol Security) Tunnel is a method used to securely transfer data between two networks over the internet. It encrypts the entire IP packet, ensuring **privacy, integrity, and authentication**.

Where is it used?

- **VPNs (Virtual Private Networks)** – To secure remote access for employees.
- **Site-to-Site Connections** – To connect branch offices securely.
- **Cloud Services** – To protect data while transferring it to cloud servers.
- **Government & Military Networks** – To safeguard confidential communications.

---

28. Why is it important to strike a balance between providing adequate security measures and allowing appropriate access to information systems?

✓ **Definition:** Balancing security and access ensures that information systems remain **protected from threats** while allowing **authorized users** to perform their tasks efficiently.

✓ **Importance:**

- **Too much security** can make it difficult for users to access needed resources, **reducing productivity**.
- **Too little security** increases the risk of **data breaches, cyberattacks, and unauthorized access**.
- A **balanced approach** ensures **data protection, operational efficiency, and compliance** with security policies.

---

29. Define Malware with Examples.

✓ **Definition: Malware (Malicious Software)** is any **harmful program** designed to **damage, steal, or disrupt** computer systems and networks.

✓ **Examples:**

- **Virus** – Attaches to files and spreads when executed.
- **Worm** – Self-replicates and spreads across networks.
- **Trojan Horse** – Disguised as legitimate software but contains harmful code.
- **Ransomware** – Encrypts data and demands ransom for decryption.
- **Spyware** – Secretly monitors and collects user information.

---

30. What are Hash Functions and When Are They Used?

✓ **Definition:** A **hash function** is a mathematical algorithm that converts input data into a **fixed-length unique string (hash value)**, ensuring **data integrity and security**.

✓ **Uses of Hash Functions:**

- **Data Integrity** – Checks whether data has been altered (e.g., file verification).
- **Password Storage** – Stores encrypted passwords securely.
- **Digital Signatures** – Ensures document authenticity.
- **Blockchain Technology** – Links transactions securely.

🔹 **Example Algorithms:** SHA-256, MD5, SHA-1.

---

31. What is Penetration Testing?

✓ **Definition: Penetration Testing (Pen Testing)** is a **simulated cyberattack** performed to identify and fix **security vulnerabilities** in an information system before real attackers exploit them.

✓ **Purpose:**

- Detect weaknesses in **networks, applications, and devices**.
- Improve **security defenses** by fixing vulnerabilities.
- Ensure compliance with **security standards** (e.g., ISO 27001, PCI-DSS).

---

32. What do you mean by Packet Filtering?

✓ **Definition: Packet Filtering** is a **network security technique** that controls incoming and outgoing data packets based on **predefined security rules**.

✓ **How It Works:**

- Examines packet **headers** (IP address, port number, protocol).
- **Allows or blocks** packets based on **firewall rules**.
- Used in **firewalls** to filter unauthorized network traffic.

🔻 **Example:** A firewall rule allowing only HTTP (port 80) traffic but blocking FTP (port 21).

---

33. What is IDPS?

✓ **Definition: IDPS (Intrusion Detection and Prevention System)** is a security tool that **monitors network traffic** for suspicious activities and can **prevent attacks** in real time.

✓ **Types:**

- **IDS (Intrusion Detection System)** – **Detects** threats and alerts administrators.
- **IPS (Intrusion Prevention System)** – **Detects and blocks** threats automatically.

✓ **Purpose:**

- Protects against **hacking, malware, and DoS attacks**.
- Ensures **network and system security**.

---

34. What are the two major objectives of Digital Forensics?

✓ **Definition: Digital Forensics** is the process of **collecting, analyzing, and preserving digital evidence** for investigation.

✓ **Two Major Objectives:**

1. **Investigate Cybercrimes** – Identify and analyze evidence in **hacking, fraud, identity theft, and cyberattacks**.

2. **Ensure Legal Admissibility** – Collect digital evidence in a **secure and legally acceptable** way for use in **court cases**.

---

35. In risk management strategies, why must periodic review be a part of the process?

✓ **Definition: Periodic review** in risk management ensures that **security measures remain effective**, and new risks are identified and mitigated over time.

✓ **Importance:**

- **New threats** emerge due to evolving technology and attack methods.
- **Existing controls** may become outdated or ineffective.
- **Compliance requirements** may change.
- Helps in **continuous improvement** of security measures.

---

36. What is Business Resumption Planning?

✓ **Definition: Business Resumption Planning (BRP)** is a strategy for **restoring business operations** after a disruption, such as a cyberattack, natural disaster, or system failure.

✓ **Key Aspects:**

- Focuses on **critical business functions** recovery.
- Includes plans for **IT systems, communication, and staff coordination**.
- Ensures **minimum downtime** and business continuity.

---

37. What is Evidentiary Material?

✓ **Definition: Evidentiary material** refers to any **digital or physical evidence** that can be used in an **investigation or legal proceedings** to support a claim or case.

✓ **Examples:**

- **Digital Evidence:** Emails, log files, encrypted messages.
- **Physical Evidence:** Hard drives, mobile devices, printed documents.

- Used in **cybercrime investigations, fraud cases, and forensic analysis**.

---

38. What is the difference between Policy and Law?

✓ **Policy:** A **set of guidelines** established by an **organization** to **regulate internal actions** and decision-making.
✓ **Law:** A **legally binding rule** created by a **government or legal authority**, enforceable by courts.

✓ **Key Differences:**

Aspect	Policy	Law
Authority	Set by organizations	Set by government
Enforceability	Internal enforcement	Legally enforced
Purpose	Guides decision-making	Regulates societal behavior
Examples	Company security policy	Cybercrime law

---

39. What is a Digital Certificate?

✓ **Definition:** A **Digital Certificate** is an **electronic document** issued by a **Certificate Authority (CA)** that verifies the identity of a user, website, or organization. It ensures **secure communication** over the internet.

✓ **Components:**

- **Public Key** – Used for encryption.
- **Certificate Authority (CA) Signature** – Confirms authenticity.
- **Owner's Information** – Name, organization, and validity period.
- **Serial Number** – Unique identifier.

✓ **Uses:**

- Secure websites (**SSL/TLS encryption**).
- Digital signatures for document authentication.

- Secure email communication.

---

40. What are Different Tools and Techniques of Digital Forensics?

✓ **Definition: Digital forensics tools and techniques** help in **collecting, analyzing, and preserving digital evidence** for investigations.

✓ **Tools:**

- **Autopsy & Sleuth Kit** – File system analysis.
- **FTK (Forensic Toolkit)** – Data recovery and analysis.
- **Wireshark** – Network packet analysis.
- **EnCase** – Advanced digital investigation.
- **Volatility** – Memory forensics.

✓ **Techniques:**

- **Disk Imaging** – Creates an exact copy of a digital device.
- **Live Forensics** – Examines running systems without shutting them down.
- **Log Analysis** – Reviews system logs for suspicious activities.
- **Data Recovery** – Retrieves deleted or lost data.

---

41. Write a Brief Note on DES (Data Encryption Standard).

✓ **Definition: DES (Data Encryption Standard)** is a **symmetric-key encryption algorithm** used to encrypt and decrypt data. It was developed by **IBM** and adopted as a standard by **NIST** in **1977**.

✓ **Key Features:**

- **Key Size:** 56-bit encryption key.
- **Block Cipher:** Encrypts data in **64-bit blocks**.
- **Rounds:** Uses **16 rounds** of encryption.
- **Weakness:** Vulnerable to **brute-force attacks** due to short key length.

✓ **Use Case:**

- Previously used in **banking and government encryption** but replaced by **AES** due to security concerns.

---

42. What are the Different Processing Modes of Firewall?

✓ **Definition:** A **firewall processing mode** determines how the firewall analyzes and filters network traffic to enforce security policies.

✓ **Types of Firewall Processing Modes:**

1. **Packet Filtering Firewall** – Inspects packets based on **IP addresses, ports, and protocols** before allowing or blocking them.
2. **Stateful Inspection Firewall** – Tracks active connections and makes filtering decisions based on **connection state and context**.
3. **Proxy Firewall** – Acts as an **intermediary** between users and the internet, filtering requests before forwarding them.
4. **Circuit-Level Gateway** – Verifies **handshaking protocols** between trusted and untrusted hosts without inspecting individual packets.
5. **Next-Generation Firewall (NGFW)** – Integrates **deep packet inspection, intrusion prevention, and advanced security features**.

---

43. Write a Brief Note on Vulnerability Scanning

✓ **Definition: Vulnerability Scanning** is an automated process of **identifying security weaknesses** in systems, networks, and applications.

✓ **Purpose:**

- Detect **misconfigurations, outdated software, and security flaws**.
- Helps organizations **fix vulnerabilities before attackers exploit them**.

✓ **Types of Vulnerability Scanning:**

1. **Network Scanning** – Checks for open ports and insecure network services.
2. **Application Scanning** – Detects flaws in **web applications** (e.g., SQL Injection, XSS).
3. **Host-Based Scanning** – Analyzes **individual devices** for vulnerabilities.

✓ Tools Used:

- **Nessus**, **OpenVAS**, **Qualys**, **Nmap**.
