Information security(Theory)

Long Questions

2024 Paper

1. Explain different types of computer crimes in detail.

Computer crimes are illegal activities that involve computers, networks, or digital devices. Criminals use technology to steal, damage, or misuse data and systems. Major types are:

1. **Hacking** – Breaking into a computer system without permission.
2. **Phishing** – Sending fake emails/websites to steal user details like passwords.
3. **Identity Theft** – Stealing someone's personal information (bank details, Aadhaar, etc.) for fraud.
4. **Cyber Stalking** – Continuously harassing or threatening someone online.
5. **Virus/Worm Attacks** – Creating malicious programs to damage data or slow down systems.
6. **Denial of Service (DoS)** – Attacking servers to make them unavailable to users.
7. **Online Fraud** – Fake e-commerce websites, lottery scams, or online banking fraud.
8. **Intellectual Property Theft** – Copying or distributing software, music, movies illegally (piracy).

 In short, computer crimes misuse technology for financial gain, harassment, or destruction of data.

2. Describe computer forensics and ethics standards. OR Information Security Principles of Success in detail.

Computer Forensics:
Computer forensics is the process of collecting, analyzing, and preserving digital evidence so it can be presented in court for solving cybercrimes. It is a branch of forensic science that deals with crimes involving computers.

Steps in Computer Forensics:

1. **Identification:** Recognizing digital evidence like emails, files, logs.
2. **Collection:** Gathering data without damaging it.
3. **Preservation:** Ensuring evidence is safe and unaltered.
4. **Analysis:** Examining files, logs, deleted data to find proof.
5. **Presentation:** Preparing reports and presenting evidence legally.

Ethics Standards in Computing:
Computer ethics are moral guidelines for responsible computer use.

- Do not use other people's data without permission.
- Respect privacy of emails, files, and online activities.
- Avoid spreading viruses, malware, or fake information.
- Use technology for legal and positive purposes.
- Follow professional standards like ACM Code of Ethics and IEEE guidelines.

3. Discuss Patent and Trademark.

Patent:

- A patent is a legal right given to an inventor for a new invention, idea, or technology.
- It prevents others from making, selling, or copying the invention without permission.
- Valid usually for **20 years**.
- Example: A new processor design or a unique software algorithm.
- Types: Utility patents (machines, processes), Design patents (appearance), Plant patents (new plant species).

Trademark:

- A trademark is a symbol, logo, word, or phrase that represents a company or brand.
- It helps customers recognize genuine products.
- Example: Nike's ✔ logo, Apple's logo, Coca-Cola name.
- Protects brand reputation and prevents misuse by competitors

4. Explain the terms and concepts of Access Control System. OR Write a detail note on Intrusion Detection System.

Access control means deciding **who can access what resources** in a computer system.

- **Types of Access Control:**
    1. **Discretionary Access Control (DAC):** Owner of data decides who can access it.
    2. **Mandatory Access Control (MAC):** Access is given based on rules set by authority. Example: military data.
    3. **Role-Based Access Control (RBAC):** Access depends on the role of a person (Admin, User, Guest).
- **Concepts:**
    - **Authentication:** Verifying user identity (password, biometrics).
    - **Authorization:** Granting rights after authentication.

- **Accountability:** Keeping logs of user activities.

- **IDS** is a security system that monitors network or system activities to detect suspicious activities or policy violations.

- It acts like a **security camera** for networks.

- **Types of IDS:**

  1. **Network-based IDS (NIDS):** Monitors network traffic.
  2. **Host-based IDS (HIDS):** Monitors activities on a single computer.

- **Techniques:**

  - **Signature-based:** Detects attacks by comparing with known patterns.
  - **Anomaly-based:** Detects unusual behavior that differs from normal.

- **Advantages:** Detects attacks early, provides alerts.

- **Limitations:** Cannot stop the attack (only detects), may give false alarms

5. Explain Biometrics, Single Sign-on and Kerberos.

Biometrics

- **Meaning**: Biometrics means using physical or behavioral characteristics of a person to verify their identity.
- **Examples**: Fingerprint, face recognition, voice recognition, iris/eye scan, hand geometry.
- **Working**: A person's biometric data is captured, stored, and compared whenever they log in or need identification.
- **Advantages**:
  1. Hard to steal or forget (unlike passwords).
  2. Provides stronger security.
  3. Fast and convenient for users.
- **Limitations**:
  - Devices are costly.
  - If biometric data is stolen, it cannot be changed (like a password).

Single Sign-On (SSO)

- **Meaning**: Single Sign-On allows a user to log in once and get access to many related systems without entering their password again.
- **Example**:
    - If you log in to Google, you can use Gmail, YouTube, Google Drive, and other services without logging in again.
- **Advantages**:
    1. Saves time, no need to remember many passwords.
    2. Improves user experience.
    3. Reduces password fatigue and mistakes.
- **Limitations**:
    - If one login is hacked, all connected systems may be at risk.

Kerberos

- **Meaning**: Kerberos is a **network authentication protocol** that uses **secret-key cryptography**. It was developed at MIT.
- **How it works**:
    - It uses a trusted server called **Key Distribution Center (KDC)**.
    - KDC provides a "ticket" to a user after verifying their identity.
    - This ticket is used to access different services securely without sending passwords over the network.
- **Advantages**:
    1. Prevents password theft on networks.
    2. Provides mutual authentication (both user and server verify each other).
- **Limitations**:
    - Complex setup.
    - If KDC server fails, the system may not work.

6. Write a short note on Firewall and Antivirus.

Firewall:

- A firewall is a security system that filters network traffic.
- It decides which data packets are allowed and which are blocked.
- Types:
    - **Hardware Firewall:** A physical device placed between network and internet.
    - **Software Firewall:** Installed on computers (Windows Firewall).
- Example: Blocking malicious websites or preventing unauthorized access.

Antivirus:

- Antivirus is software that detects, prevents, and removes viruses, malware, worms, and spyware.
- It continuously scans files and downloads.
- Examples: Avast, Quick Heal, Windows Defender.
- Features: Auto-update, quarantine, real-time protection.

7. Discuss the OSI reference model.
OR What is Network? Explain different types of data networks.

The **OSI (Open Systems Interconnection) model** is a 7-layer framework developed by ISO to standardize how computers communicate over a network.

7 Layers of OSI Model:

1. **Physical Layer:** Deals with physical transmission (cables, signals, bits).
2. **Data Link Layer:** Provides error detection and correct data transfer (MAC address, Ethernet).
3. **Network Layer:** Handles routing and addressing (IP addresses, routers).
4. **Transport Layer:** Ensures reliable delivery of data (TCP, UDP).
5. **Session Layer:** Establishes, maintains, and terminates communication sessions.
6. **Presentation Layer:** Converts data into a format the application can understand. Handles encryption, compression.
7. **Application Layer:** Provides services to users (Email, HTTP, FTP, Browsers).

A **computer network** is a collection of interconnected computers and devices that communicate and share data, files, or resources.

Types of Data Networks:

1. **LAN (Local Area Network):** Small area like office, school, or home. Fast speed, limited area.
2. **MAN (Metropolitan Area Network):** Covers a city or large campus. Example: University campus network.
3. **WAN (Wide Area Network):** Covers large distances, even countries. Example: The Internet.
4. **PAN (Personal Area Network):** Very small range, such as Bluetooth, Hotspot, Wi-Fi Direct.
5. **VPN (Virtual Private Network):** A secure connection built over the internet for privacy and secure communication.

8. Explain SDLC.

The **Software Development Life Cycle (SDLC)** is a structured process used to plan, design, develop, test, and maintain software. It ensures software is reliable, cost-effective, and meets user needs.

Phases of SDLC:

1. **Requirement Analysis:** Collecting user needs and system requirements.
2. **System Design:** Creating architecture, data models, and technical designs.
3. **Implementation (Coding):** Developers write code using programming languages.
4. **Testing:** Software is tested for errors, bugs, and performance issues.
5. **Deployment:** Software is delivered and installed for real users.
6. **Maintenance:** Updating, fixing bugs, and upgrading features after release.

Advantages of SDLC:

- Provides a clear roadmap.
- Ensures quality and reliability.
- Reduces risks and costs.

Conclusion:
SDLC is important for systematic software development. It helps organizations deliver software that meets user requirements within time and budget.

2023 Paper

1. What is Information Security? Discuss Information Security principles of Success.

Information Security (InfoSec)

- **Meaning**: Information Security is the practice of protecting data and information systems from unauthorized access, misuse, modification, or destruction.
- It ensures that **data remains safe, accurate, and available** to only authorized people.

Principles of Success in Information Security

There are **three core principles** also called the **CIA Triad**:

1. **Confidentiality**
    - Data should only be accessible to authorized persons.
    - Example: Password-protected files, encryption.

2. **Integrity**
    - Information must remain correct, complete, and unchanged (unless updated by authorized users).
    - Example: Digital signatures, checksums.
3. **Availability**
    - Data and systems should be available to authorized users whenever they need it.
    - Example: Backup systems, reliable servers, disaster recovery plans.

2. Discuss: Intellectual Property Law, Patents Law and Trade Secrets. OR What are the different categories of Computer Crimes? How do cyber criminals commit cybercrime?

Intellectual Property Law (IP Law)

- Protects creations of the human mind such as inventions, art, music, software, and designs.
- Gives creators the right to control how their work is used.

Patent Law

- A **patent** gives inventors the exclusive right to use, make, or sell their invention for a specific period (usually 20 years).
- Protects new inventions and technologies.
- Example: A new mobile phone technology or medicine.

Trade Secrets

- A trade secret is confidential business information that gives a company an advantage.
- Example: Coca-Cola formula, Google's search algorithm.
- Trade secrets must be kept hidden; once exposed, protection may be lost.

OR Is repeted

3. Write a note on Computer Forensics.

Computer Forensics

- **Meaning**: Computer Forensics is the process of collecting, analyzing, and preserving digital evidence from computers, networks, and storage devices in a way that is acceptable in court.

- **Purpose**: To investigate crimes like hacking, fraud, identity theft, and cyber terrorism.

Steps in Computer Forensics

1. **Identification** – Detect potential sources of evidence.
2. **Preservation** – Ensure data is not altered or destroyed.
3. **Collection** – Copy data using secure methods.
4. **Analysis** – Examine files, emails, logs, and hidden data.
5. **Presentation** – Present evidence in reports and court.

Uses

- Solving cybercrime cases.
- Recovering deleted files.
- Tracking hackers and criminals.
- Providing digital proof in legal cases.

4. Explain the following technical controls of physical security: Smart cards, Intrusion detection.

Smart Cards

- A smart card is a plastic card with a microchip that stores and processes data.
- Used for secure identification and authentication.
- Examples: ATM cards, employee ID cards, SIM cards.
- **Advantages**:
    - Stronger than passwords.
    - Portable and easy to use.

Intrusion Detection

- Intrusion Detection System (IDS) is a security system that monitors networks or systems for suspicious activity.
- Types:
    1. **Network IDS (NIDS)** – Monitors network traffic.
    2. **Host IDS (HIDS)** – Monitors activities on a specific computer.
- **Purpose**: To detect hacking attempts, malware, or unauthorized access.
- **Limitations**: Cannot always prevent attacks; only detects them

5. Why is Physical Security important? What are the different types of physical security threats?

Importance of Physical Security

- Physical security is the **foundation of information security**.
- Even if you have the best antivirus, firewalls, or encryption, they are useless if someone can **physically damage, steal, or tamper with the computer systems**.
- Physical security protects **people, hardware, software, networks, and data** from harm.
- Example: If a hacker steals the server machine, they can bypass all passwords and security controls.

Types of Physical Security Threats

1. **Natural Threats**
    - Caused by nature and outside human control.
    - Examples: Earthquakes, floods, fire, storms, lightning.
2. **Human Threats (Intentional)**
    - Done purposely by attackers.
    - Examples: Theft, vandalism, terrorism, sabotage, insider threats (employees misusing access).
3. **Human Threats (Unintentional)**
    - Mistakes made by humans that cause harm.
    - Examples: Accidentally deleting data, spilling water on a laptop, leaving doors unlocked.
4. **Environmental Threats**
    - Issues caused by surroundings or infrastructure.
    - Examples: Power failures, overheating due to lack of cooling, humidity damaging devices.

6. What is the importance of Operations Security in information security? Also discuss the operations security principles.

What is Operations Security (OpSec)?

- Operations Security (OpSec) means **protecting day-to-day operations and processes** in an organization.
- It prevents attackers from collecting small bits of unclassified information that, when combined, reveal sensitive data.
- Example: A worker posting schedules online may unintentionally help attackers.

Importance

- Prevents information leaks during daily work.

- Protects against insider misuse.
- Helps in **identifying risks early** before attackers exploit them.
- Maintains confidentiality of business plans, passwords, and transactions.

Principles of OpSec

1. **Identify Critical Information**
    - Find out what information is sensitive and must be protected.
    - Example: Employee data, passwords, designs.
2. **Analyze Threats**
    - Find out who may attack.
    - Example: Hackers, competitors, disgruntled employees.
3. **Analyze Vulnerabilities**
    - Look for weaknesses in processes or systems.
    - Example: Weak passwords, unencrypted data, careless handling of documents.
4. **Assess Risks**
    - Study how much damage could happen if the information is leaked.
5. **Apply Countermeasures**
    - Implement steps to reduce risks.
    - Example: Encrypting files, using strong authentication, staff training.

7. What is the role of media control in Operations security?

Media Control

- "Media" means **data storage devices** such as hard disks, USB drives, CDs, DVDs, backup tapes, and even cloud storage.
- Media control means **managing, monitoring, and protecting these storage devices** to prevent unauthorized access or data loss.

Role of Media Control

1. **Access Restriction**
    - Only authorized people can use storage media.
    - Example: Locking USB drives in secure storage.
2. **Classification and Labeling**
    - Marking media as "Confidential," "Secret," or "Public" to handle accordingly.
3. **Data Backup and Recovery**
    - Ensures critical data stored on media can be recovered after damage or loss.
4. **Sanitization and Disposal**
    - Before reusing or throwing away old storage media, data should be properly wiped or destroyed.
    - Example: Degaussing or shredding hard disks.
5. **Tracking and Logging**

- Keeping a record of who accessed which media and when.

8. Write a detailed note on: Principles of Authentication.

What is Authentication?

- Authentication is the process of **verifying the identity** of a user, system, or device before giving access.
- It ensures that only **real, authorized people** can use the system.

Principles of Authentication

1. **Something You Know**
   - Information the user knows.
   - Example: Passwords, PINs, security questions.
2. **Something You Have**
   - Physical objects or devices the user owns.
   - Example: Smart cards, ID cards, mobile phones for OTPs.
3. **Something You Are**
   - Biological or behavioral characteristics of the user.
   - Example: Fingerprints, facial recognition, iris scans.
4. **Somewhere You Are**
   - Authentication based on location.
   - Example: Access allowed only if login is from the office network.
5. **Multi-Factor Authentication (MFA)**
   - Using more than one principle together for stronger security.
   - Example: ATM (Card = something you have, PIN = something you know).

9. Discuss: Kerberos and Federated Identities. OR Explain the role of symmetric keys and asymmetric keys in cryptosystems.

Kerberos

- Kerberos is a **network authentication protocol** that uses secret keys to prove identity.
- Developed at MIT.
- Works using a **trusted third party** called the Key Distribution Center (KDC).
- Prevents passwords from being sent over the network.
- Used in Windows Active Directory, enterprise logins.

Advantages: Secure, prevents password theft, supports Single Sign-On (SSO).

Federated Identities

- Federated Identity means **one user identity is shared across multiple organizations or services**.
- Example: Logging into many apps with your Google or Facebook account.
- Works using standards like **SAML, OAuth, OpenID Connect**.

Advantages:

- Fewer passwords to remember.
- Easier access across multiple systems.

Disadvantages:

- If the central account is hacked, all linked services are at risk.

Explain the role of symmetric keys and asymmetric keys in cryptosystems.

- **Symmetric Key Cryptography**
  - Same key used for both encryption and decryption.
  - Example: DES, AES.
  - **Fast** but the problem is securely sharing the key.
- **Asymmetric Key Cryptography**
  - Uses a **public key** for encryption and a **private key** for decryption.
  - Example: RSA.
  - **More secure**, but slower than symmetric.

10.Explain: Hashing functions and Block ciphers.

Hashing Functions

- A hashing function converts input data into a **fixed-length unique value** (called a hash or digest).
- Example: MD5, SHA-256.

Properties:

1. One-way function – cannot reverse the hash to original data.
2. Small change in input → big change in output.
3. Unique output for different inputs.

Uses: Password storage, digital signatures, verifying file integrity, blockchain.

Block Ciphers

- A method of encryption where data is divided into **fixed-size blocks** and then encrypted.
- Each block is processed separately using a key.
- Example: AES (128-bit), DES (56-bit).

Advantages: Secure, widely used, prevents data tampering.
Uses: Banking, VPNs, secure communication.

Hashing ensures **data integrity**, block ciphers ensure **confidentiality**.

11.Discuss the different types of Data Networks.

(Repeated – already answered)

12.Write a detailed note on Software Development Life Cycle (SDLC).

(Repeated – already answered)

OR What is a firewall? Explain application level gateway firewall with its benefits and limitations.

Firewall (Application Level Gateway Firewall):

- A firewall is a security device/software that filters network traffic.
- Application-level gateway firewall (proxy firewall) works at the application layer.
- It inspects data packets deeply (HTTP, FTP, DNS requests).

Benefits:

- Strong filtering (blocks malicious traffic).
- Hides internal network structure.
- Provides detailed logging.

Limitations:

- Slower because it checks all data.
- Complex to configure.
- Can become a bottleneck for traffic.

13.Discuss: Malware.

Meaning of Malware:
The term **Malware** comes from "Malicious Software." It is any software program that is specially designed to damage computers, steal data, disrupt services, or gain unauthorized access. Malware is harmful because it hides inside normal-looking files or programs and executes without the user's knowledge.

Characteristics of Malware:

1. Runs without user permission.
2. Can spread from one system to another.
3. Often stays hidden (stealth mode).
4. May damage data, slow down systems, or steal sensitive information.

Types of Malware:

1. **Virus** – Attaches itself to files or programs and spreads when those files are run. Example: File infector virus.
2. **Worms** – Self-replicating programs that spread over networks without needing a host file.
3. **Trojan Horse** – Looks like a useful program but contains harmful code. Example: Fake antivirus.
4. **Spyware** – Secretly monitors user activity (e.g., keystrokes, browsing habits).
5. **Adware** – Shows unwanted ads, often bundled with free software.
6. **Ransomware** – Locks or encrypts data and demands money to unlock it.
7. **Rootkits** – Hide other malware and give hackers remote access.
8. **Keyloggers** – Record everything typed on the keyboard to steal passwords and banking details.

Effects of Malware:

- Corrupts or deletes files.
- Slows down computer performance.

- Steals personal and financial data.
- Crashes systems and applications.
- Misuses system resources (like using your computer for spam or crypto-mining).

Prevention of Malware:

1. Install and regularly update antivirus/antimalware software.
2. Keep operating systems and applications updated with patches.
3. Avoid downloading files from unknown sources.
4. Do not click on suspicious email attachments or links.
5. Use firewalls to block unauthorized access.
6. Regularly back up important data.

2021 Paper

1. Explain Information Security principles of success.

Repeated (Already answered earlier – 2021 & 2023 papers).

2. Explain different types of computer crimes and how cyber criminals commit those crimes?

Repeated (Already answered earlier – 2021 & 2024 papers).

3. Write a note on Physical security domain and security threats.

Physical Security Domain:
Physical security is the protection of physical assets such as computers, servers, data centers, and people from physical threats like theft, fire, or unauthorized access. It is the **first line of defense** in information security because even the best digital protection is useless if the physical devices are not safe.

Components of Physical Security:

1. **Deterrence measures** – Security guards, warning signs, CCTV cameras to discourage attackers.
2. **Access control** – Locks, smart cards, biometrics to limit entry.
3. **Detection measures** – Motion sensors, intrusion alarms to detect unauthorized activities.
4. **Response measures** – Fire extinguishers, security teams, disaster recovery plans.

Physical Security Threats:

1. **Natural threats** – Earthquakes, floods, fire, storms.
2. **Human threats** – Theft, vandalism, terrorism, sabotage.
3. **Accidental threats** – Power failure, equipment malfunction, human error.
4. **Environmental threats** – Overheating of equipment, dust, humidity.

4. Explain principles of operation security.

Operation Security (OpSec):
Operation Security means protecting sensitive information about operations, systems, and procedures from being leaked to attackers. It ensures that day-to-day activities do not accidentally give away useful data to outsiders.

Principles of Operation Security:

1. **Identify Critical Information** – Know what information is sensitive (e.g., passwords, project plans).
2. **Analyze Threats** – Understand who might want to steal the information (hackers, competitors).
3. **Analyze Vulnerabilities** – Find weaknesses (like weak passwords, unsecured USB drives).
4. **Assess Risks** – Decide which vulnerabilities are most dangerous.
5. **Apply Countermeasures** – Take steps like encryption, strong authentication, employee awareness training.

5. Explain the terms and concepts of Access Control System.

Access Control System:
It is a method to decide **who is allowed to access what** in an information system. Its goal is to ensure that only authorized users can access resources like files, databases, or physical rooms.

Types of Access Control:

1. **Discretionary Access Control (DAC):**
    - The owner decides who can access resources.

    - Example: A file owner gives "read" or "write" permission to others.
2. **Mandatory Access Control (MAC):**
    - Access is based on strict rules and security labels (like Top Secret, Confidential).
    - Used in military and government systems.
3. **Role-Based Access Control (RBAC):**
    - Access depends on the user's role in the organization.
    - Example: HR manager can access employee records, but IT staff cannot.

Components:

- **Identification** – User provides username.
- **Authentication** – System checks identity (password, biometrics).
- **Authorization** – System decides what resources user can access.
- **Accountability** – System logs all user activities.

6. Write a note on examining digital cryptography.

Cryptography:
Cryptography is the science of protecting information by converting it into an unreadable form (encryption) and then converting it back to readable form (decryption) using keys.

Main Concepts of Digital Cryptography:

1. **Encryption and Decryption** – Converting plaintext to ciphertext and back.
2. **Keys** – Secret codes used in cryptography.
    - **Symmetric key** → same key for encryption & decryption.
    - **Asymmetric key** → public key for encryption, private key for decryption.
3. **Hashing** – One-way conversion of data to a fixed-size string (used for integrity check).
4. **Digital Signatures** – Used for authentication and integrity.
5. **Certificates** – Digital IDs issued by Certificate Authorities (CAs).

Uses:

- Protecting passwords, emails, and online banking.
- Digital certificates for secure websites (HTTPS).
- Ensuring integrity of files and software.

7. What is Network? Explain different types of data networks.

Repeated (Already answered in 2021 & 2024 papers).

8. Discuss the OSI reference model.

Repeated (Already answered in 2021 & 2024 papers).

? Short Questions

2024 Paper (Any Seven)

1. Define DoS.

DoS (Denial of Service) is an attack that makes a computer or network unavailable to users.

2. Define Encryption.

Encryption is the process of converting data into a secret code to protect it from unauthorized access.

3. What is TLS?

TLS (Transport Layer Security) is a protocol that secures communication over the internet.

4. Define Phishing.

Phishing is a cyber attack where attackers trick people to give sensitive information like passwords.

5. What is confidentiality?

Confidentiality ensures that information is kept secret and only accessible to authorized people.

6. What is vulnerability?

Vulnerability is a weakness in a system that can be exploited by attackers.

7. What is symmetric key?

Symmetric key is a type of encryption where the same key is used to encrypt and decrypt data.

8. Define Identity Theft.

Identity theft is when someone steals another person's personal information for fraud.

9. Define Software Ag.

Software AG is a company that provides software for business process management and integration.

10. What do you mean by one-time password?

A one-time password (OTP) is a temporary password used only once for secure login.

2023 Paper MCQs

1. **Which of the following terms is another name for a VPN?**

- (a) Tunnel □
- (b) By-pass
- (c) One-time password

2. **… arose from unwritten law that developed from judicial cases based on precedent and custom.**

- (a) Administrative law
- (b) Corporate law
- (c) Common law □
- (d) None of the above

3. **An antivirus software should**

- (a) Have a track record of successful implementation
- (b) Be self-updating
- (c) Protect a computer system without inhibiting normal processing
- (d) All of the above □

4. **Which of the following is not a risk with distributed system?**

- (a) Java applets
- (b) Firewall □
- (c) CORBA interfaces

- (d) ActiveX control

5. **Why does a digital signature contain a message digest?**

- (a) To detect any alteration of the message
- (b) To indicate the encryption algorithm
- (c) To confirm the identity of the sender
- (d) To enable transmission in a digital format

6. **Which of the following are considerations while selecting a site for a facility?**

- (a) Transportation system
- (b) Visibility
- (c) Locale considerations
- (d) All of the above

7. **What is an audit trail?**

- (a) An audit trail is a fitness path for quality inspectors
- (b) An audit trail is a sound recording of conversations taped through perimeter devices
- (c) An audit trail is a history of transactions indicating data that has been changed or modified
- (d) All of the above

8. **… is a method to destroy media by shredding or burning.**

- (a) Overwriting
- (b) Physical destruction
- (c) Degaussing
- (d) All of the above

9. **In … method of cryptosystem, letters are rearranged into a different order.**

- (a) Transposition
- (b) Substitution
- (c) Message digest
- (d) All of the above

10. **Which protocol of the TCP/IP suite addresses reliable data transport?**

- (a) IP
- (b) TCP
- (c) UDP
- (d) HTTP

11. **The CIA triad includes:**

- (a) Control, Information and Accountability
- (b) Control, Integrity and …
- (c) Confidentiality, Integrity and Availability □
- (d) Confidentiality, Information and Accountability

12. **Common Body of Knowledge (CBK) contains … domains.**

- (a) 8
- (b) 10 □
- (c) 12
- (d) 5

2021 Paper MCQs

1. **DoS stands for**

- (A) Denial-of-Service □
- (B) Digital-of-Service
- (C) Data-of-Service
- (D) Devices-of-Service

2. **A mechanism used to encrypt and decrypt data:**

- (A) Algorithm
- (B) Data flow
- (C) Cryptography □
- (D) None of these

3. **Using RSA cryptosystem with p=7 and q=9. What is n=?**

- (A) 7
- (B) 63 □
- (C) 9
- (D) 48

4. **TLS stands for**

- (A) Transport Layer Service
- (B) Transport Layer System
- (C) Transport Layer Structure
- (D) Transport Layer Security □

5. **In which of the following, a person is constantly followed/chased by another person or group?**

- (A) Phishing
- (B) Stalking □
- (C) Bullying
- (D) Identity theft

6. **VPN stands for**

- (A) Virtual Public Network
- (B) Virtual Private Network □
- (C) Network
- (D) Network

7. **CCTV stands for**

- (A) Closed-Circuit Transaction
- (B) Common-Circuit Television
- (C) Closed-Circuit Television □
- (D) Television Control-Circuit Television

8. **Which of the following is considered unsolicited commercial email?**

- (A) Virus
- (B) Spam □
- (C) Malware
- (D) All of the above

9. **Which of the following refers to the violation of the principle if a computer is not secure?**

- (A) Access control
- (B) Availability
- (C) Confidentiality
- (D) All of the above □

10. **Which of the following are the types of scanning?**

- (A) Network, vulnerability and port scanning □
- (B) Client, Server, and network
- (C) Port, network, and services