WB Board Class 12 Cyber Security Question Paper with Solutions(Memory Based)

Time Allowed :3 Hour	**Maximum Marks :**60	**Total Questions :**24

General Instructions

Read the following instructions very carefully and strictly follow them:

- Answers to this Paper must be written on the paper provided separately.
- You will not be allowed to write during the first 15 minutes
- This time is to be spent in reading the question paper.
- The time given at the head of this Paper is the time allowed for writing the answers,
- The paper has four Sections.
- Section A is compulsory - All questions in Section A must be answered.
- You must attempt one question from each of the Sections B, C and D and one other question from any Section of your choice.

1. Define the three pillars of the CIA Triad.

Correct Answer: Confidentiality, Integrity, and Availability

Solution: Concept: The CIA Triad is a foundational model in information security that defines the three primary objectives of protecting information systems and data. It ensures that data is protected from unauthorized access, remains accurate, and is accessible when needed.

Step 1: Confidentiality

Confidentiality ensures that sensitive information is accessible only to authorized users and protected from unauthorized access. This is achieved through mechanisms such as:

- Encryption
- Access control (passwords, biometrics)
- Data classification

Step 2: Integrity

Integrity ensures that data remains accurate, consistent, and unaltered during storage or transmission. It protects against unauthorized modification or tampering. Common techniques include:

- Hashing and checksums
- Digital signatures

- Version control and audit logs

Step 3: Availability
Availability ensures that authorized users have reliable and timely access to data and systems when required. It focuses on maintaining system uptime and resilience using:

- Redundancy and backups
- Disaster recovery plans
- Protection against DoS/DDoS attacks

Quick Tip

Remember the CIA Triad as the core goals of cybersecurity: **Confidentiality** = Prevent unauthorized access,
Integrity = Prevent unauthorized changes,
Availability = Ensure reliable access.

---

2. What are the primary differences between a Computer Virus and a Worm?

Correct Answer: A virus requires a host file and user action to spread, whereas a worm is a standalone malware that self-replicates and spreads automatically over networks.

Solution: Concept: Both viruses and worms are types of malware that replicate and spread, but they differ significantly in how they infect systems and propagate. The key differences lie in dependency, propagation method, and impact.
Step 1: Dependency on Host
A **computer virus** attaches itself to a legitimate program or file and requires that host to execute. It spreads when the infected file is opened or shared.
A **worm**, on the other hand, is a standalone program and does not require a host file to spread.
Step 2: Method of Spread
Viruses typically spread through:

- Infected files (USB drives, downloads, email attachments)
- User actions such as running programs

Worms spread automatically through:

- Network vulnerabilities
- Internet connections and unsecured systems

Step 3: User Interaction Requirement
Viruses usually require **user intervention** (e.g., opening a file or running software).
Worms require **little or no user interaction** and propagate automatically once inside a network.
Step 4: Impact on Systems
Viruses often:

- Corrupt or modify files
- Damage software or data

Worms primarily:

- Consume network bandwidth
- Spread rapidly across multiple systems
- May install additional malicious payloads

Quick Tip

Virus = Needs a host + user action.
Worm = Self-contained + spreads automatically over networks.

---

3. Explain the process of Asymmetric Encryption using public and private keys.

Correct Answer: Asymmetric encryption uses a pair of keys — a public key for encryption and a private key for decryption — ensuring secure communication without sharing the secret key.

Solution: Concept: Asymmetric encryption, also known as public-key cryptography, is a method of secure communication that uses two mathematically related keys: a public key and a private key. Unlike symmetric encryption, the keys are not identical, which enhances security and enables secure data exchange over insecure networks.
Step 1: Key Pair Generation
A user generates two keys:

- **Public Key** — shared openly with others
- **Private Key** — kept secret by the owner

These keys are mathematically linked such that data encrypted with one can only be decrypted with the other.
Step 2: Encryption Using Public Key
When a sender wants to send a secure message:

- The sender obtains the receiver's public key
- The message is encrypted using this public key

Once encrypted, the message becomes unreadable to anyone without the corresponding private key.
Step 3: Transmission Over Insecure Channel
The encrypted data can be safely transmitted over insecure networks such as the internet because:

- The public key does not reveal the private key
- Even if intercepted, the message remains secure

Step 4: Decryption Using Private Key
Upon receiving the encrypted message:

- The receiver uses their private key
- The original plaintext message is recovered

Only the private key holder can decrypt the message, ensuring confidentiality.
Step 5: Additional Use — Digital Signatures
Asymmetric encryption can also provide authentication:

- A sender can encrypt a hash with their private key (digital signature)
- Anyone can verify it using the sender's public key

Quick Tip

Public Key = Lock (shared with everyone)
Private Key = Key (kept secret)
Encrypt with public key, decrypt with private key.

---

4. What is Phishing, and how can users identify a suspicious email?

Correct Answer: Phishing is a cyberattack where attackers impersonate trusted entities to steal sensitive information. Suspicious emails can be identified through signs like fake sender addresses, urgent language, suspicious links, and unexpected attachments.

Solution: Concept: Phishing is a type of social engineering attack where cybercriminals trick users into revealing sensitive information such as passwords, banking details, or personal data by pretending to be a legitimate organization (e.g., banks, companies, or government agencies).
Step 1: What is Phishing?
Phishing typically involves:

- Fraudulent emails, messages, or websites
- Impersonation of trusted entities
- Attempts to steal credentials or financial data

Attackers exploit fear, urgency, or curiosity to manipulate victims into taking action.
Step 2: Fake or Suspicious Sender Address
Users should carefully examine the sender's email:

- Slight spelling changes (e.g., `paypa1.com` instead of `paypal.com`)
- Random or unfamiliar domains

Step 3: Urgent or Threatening Language
Phishing emails often create panic:

- "Your account will be suspended immediately"

- "Act now to avoid penalties"

Legitimate organizations rarely demand immediate action.

Step 4: Suspicious Links or URLs

Before clicking links:

- Hover over links to preview the real URL
- Look for shortened or mismatched links

Phishing links often redirect to fake login pages.

Step 5: Unexpected Attachments or Requests

Warning signs include:

- Attachments you did not request
- Requests for passwords, OTPs, or bank details

Legitimate companies never ask for sensitive data via email.

Step 6: Poor Grammar and Formatting

Many phishing emails contain:

- Spelling errors
- Generic greetings (e.g., "Dear User")
- Unprofessional design

> Quick Tip
>
> **Think before you click:**
> Check the sender, verify links, avoid urgent demands, and never share sensitive information via email.

---

5. Describe the role of a Firewall in protecting a private network.

Correct Answer: A firewall acts as a security barrier that monitors and controls incoming and outgoing network traffic based on predefined rules, preventing unauthorized access to a private network.

Solution: Concept: A firewall is a network security device or software that acts as a protective boundary between a trusted private network and untrusted external networks such as the internet. It enforces security policies by filtering traffic and blocking malicious or unauthorized access.

Step 1: Traffic Monitoring and Filtering

A firewall continuously monitors data packets entering and leaving the network. It:

- Examines packet headers and contents
- Applies predefined security rules

Only trusted traffic is allowed, while suspicious traffic is blocked.
Step 2: Preventing Unauthorized Access
Firewalls restrict access by:

- Blocking unknown IP addresses
- Restricting specific ports or services
- Allowing access only to authorized users or devices

This prevents hackers from directly entering the private network.
Step 3: Protection Against Cyber Threats
Firewalls help defend against:

- Malware and intrusion attempts
- Port scanning attacks
- Unauthorized remote connections

Step 4: Traffic Control and Policy Enforcement
Organizations use firewalls to enforce security policies such as:

- Blocking access to unsafe websites
- Limiting employee internet usage
- Logging network activity

Step 5: Types of Firewalls
Common firewall types include:

- **Network firewalls** (hardware-based)
- **Host-based firewalls** (software on individual systems)
- **Next-generation firewalls (NGFW)** with deep packet inspection

Quick Tip

A firewall works like a **security gate** between a private network and the internet — it allows safe traffic in and blocks harmful traffic.

---

6. What is Digital Steganography, and how does it differ from encryption?

Correct Answer: Digital steganography is the practice of hiding secret data within ordinary media (like images or audio), whereas encryption scrambles data into unreadable form. Steganography conceals the existence of the message, while encryption protects its content.

Solution: Concept: Both steganography and encryption are techniques used to protect information, but they serve different purposes. Encryption transforms data to make it unreadable, while steganography hides the presence of the data itself.
Step 1: What is Digital Steganography?
Digital steganography is a method of concealing secret information inside ordinary digital files so that the existence of the hidden data is not noticeable. Common carriers include:

- Images (e.g., hiding data in pixel values)
- Audio or video files
- Text documents

The goal is secrecy through invisibility.
Step 2: What is Encryption?
Encryption converts plaintext into ciphertext using an algorithm and a key. Even if intercepted:

- The data appears scrambled and unreadable
- Only someone with the correct key can decrypt it

The goal is secrecy through mathematical protection.
Step 3: Key Difference — Visibility

- In **steganography**, the message is hidden and appears non-existent.
- In **encryption**, the message is visible but unreadable.

Step 4: Security Approach

- Steganography relies on **concealment** (security by obscurity).
- Encryption relies on **cryptographic algorithms and keys**.

Step 5: Usage in Practice

- Steganography is used in covert communication and watermarking.
- Encryption is widely used in secure messaging, banking, and HTTPS.

In many systems, both techniques are combined for enhanced security.

Quick Tip

Steganography hides the message.
Encryption hides the meaning of the message.

---

7. Explain the concept of Two-Factor Authentication (2FA) and its importance.

Correct Answer: Two-Factor Authentication (2FA) is a security method that requires two different types of verification (such as a password and a one-time code) to confirm a user's identity, significantly improving account security.

Solution: Concept: Two-Factor Authentication (2FA) is an additional layer of security used to verify a user's identity by requiring two independent authentication factors. It reduces the risk of unauthorized access even if one credential (like a password) is compromised.
Step 1: What is Two-Factor Authentication?
2FA requires users to provide two different forms of identification during login. These factors typically belong to different categories:

- Something you know (password or PIN)
- Something you have (OTP, mobile device, hardware token)
- Something you are (biometrics like fingerprint or face scan)

Step 2: How 2FA Works
A typical 2FA login process:

1. User enters username and password
2. System sends a second verification (e.g., OTP or app prompt)
3. Access is granted only after successful second verification

Step 3: Common Types of 2FA

- SMS or email-based one-time passwords (OTP)
- Authenticator apps (Google Authenticator, Microsoft Authenticator)
- Biometric verification
- Hardware security keys

Step 4: Importance of 2FA
2FA enhances security by:

- Protecting accounts even if passwords are stolen
- Reducing risks from phishing and brute-force attacks
- Adding an extra barrier for attackers

Step 5: Real-World Applications
2FA is widely used in:

- Online banking and payment apps
- Email and social media accounts
- Corporate systems and cloud services

Quick Tip

Password alone is not enough.
2FA adds a second layer of verification, making unauthorized access much harder.

---

8. What are the key provisions of the Indian IT Act 2000 regarding cyber crimes?

Correct Answer: The IT Act 2000 defines cyber offences, prescribes penalties for hacking, identity theft, and online fraud, provides legal recognition to electronic records and digital signatures, and establishes authorities for cyber regulation and adjudication.

Solution: Concept: The Information Technology Act, 2000 (IT Act 2000) is India's primary legislation dealing with cyber law. It provides a legal framework for electronic governance, recognizes digital transactions, and defines offences and penalties related to cyber crimes.

Step 1: Legal Recognition of Electronic Records

The Act grants legal validity to:

- Electronic documents and records
- Online contracts and digital communication

This enabled the growth of e-commerce and e-governance in India.

Step 2: Recognition of Digital Signatures

The Act recognizes digital signatures as legally valid for authentication. It:

- Enables secure electronic transactions
- Establishes Certifying Authorities (CAs)

Step 3: Definition of Cyber Offences

The IT Act defines several cyber crimes, including:

- Hacking and unauthorized access (Section 66)
- Identity theft and impersonation (Section 66C, 66D)
- Publishing obscene content online (Section 67)
- Data theft and system damage

Step 4: Penalties and Punishments

The Act prescribes penalties such as:

- Fines for unauthorized access or data damage
- Imprisonment for serious cyber offences
- Compensation to victims

Step 5: Adjudication and Cyber Authorities

To enforce cyber laws, the Act provides:

- Adjudicating Officers for cyber disputes
- Cyber Appellate Tribunal (now merged into TDSAT)
- Role of CERT-In for incident response

Step 6: Amendments and Strengthening (2008)

The IT Amendment Act 2008 introduced:

- Stronger data protection provisions
- Cyber terrorism (Section 66F)
- Enhanced penalties for identity theft and fraud

Quick Tip

The IT Act 2000 is India's foundation for cyber law — it legalizes digital transactions and punishes cyber crimes like hacking, identity theft, and online fraud.

---

9. Define Ransomware and suggest two methods to prevent such attacks.

Correct Answer: Ransomware is a type of malware that encrypts or locks a victim's data and demands payment for its release. It can be prevented through regular data backups and strong cybersecurity practices such as updated software and cautious email handling.

Solution: Concept: Ransomware is a form of malicious software designed to deny users access to their systems or data until a ransom is paid, typically in cryptocurrency. It is one of the most damaging cyber threats affecting individuals, businesses, and governments.
Step 1: What is Ransomware?
Ransomware works by:

- Encrypting files or locking the system
- Displaying a ransom note demanding payment
- Threatening permanent data loss if payment is not made

Attackers often spread ransomware through phishing emails, malicious downloads, or software vulnerabilities.
Step 2: Prevention Method 1 — Regular Data Backups
Maintaining frequent backups helps:

- Restore data without paying ransom
- Reduce business downtime

Backups should be stored offline or in secure cloud storage to avoid infection.
Step 3: Prevention Method 2 — Safe Cyber Practices
Users can minimize risk by:

- Avoiding suspicious email attachments and links
- Keeping operating systems and software updated
- Using antivirus and firewall protection

Quick Tip

Best defense against ransomware:
Keep secure backups and avoid clicking unknown links or attachments.

---

10. What is the difference between a Denial of Service (DoS) and a Distributed Denial of Service (DDoS) attack?

Correct Answer: A DoS attack is launched from a single system to overwhelm a target, while a DDoS attack uses multiple distributed systems (often a botnet) to flood and disrupt a service, making it more powerful and harder to stop.

Solution: Concept: Both DoS and DDoS attacks aim to make a website, server, or network unavailable by overwhelming it with excessive traffic or requests. The main difference lies in the number of sources and the scale of the attack.

Step 1: Denial of Service (DoS) Attack

A DoS attack:

- Originates from a single machine or IP address
- Floods the target with traffic or requests
- Exhausts system resources (CPU, memory, bandwidth)

It is relatively easier to detect and block since the source is limited.

Step 2: Distributed Denial of Service (DDoS) Attack

A DDoS attack:

- Comes from multiple compromised systems
- Often uses a botnet (network of infected devices)
- Generates massive, distributed traffic

This makes it highly difficult to mitigate or trace.

Step 3: Key Differences

- **Source:** DoS = single source, DDoS = multiple distributed sources
- **Scale:** DDoS is larger and more destructive
- **Detection:** DoS is easier to block; DDoS requires advanced mitigation tools

Step 4: Impact

Both attacks can:

- Disrupt online services
- Cause financial loss
- Damage reputation

However, DDoS attacks are generally more severe due to their distributed nature.

Quick Tip

DoS = One attacker.
DDoS = Many attackers working together (botnet).

---

11. Define SQL Injection and how it affects database security.

Correct Answer: SQL Injection is a cyberattack where malicious SQL queries are inserted into input fields to manipulate a database. It can lead to unauthorized data access, modification, or deletion, compromising database security.

Solution: Concept: SQL Injection (SQLi) is a type of injection attack that targets databases by exploiting vulnerabilities in applications that accept user input. Attackers insert malicious SQL code into queries, allowing them to interact with the database in unintended ways.
Step 1: What is SQL Injection?
SQL Injection occurs when:

- User input is not properly validated or sanitized
- Malicious SQL statements are injected into queries

For example, attackers may manipulate login forms to bypass authentication.
Step 2: How SQL Injection Works
A vulnerable application may construct queries like:

- Concatenating user input directly into SQL statements

Attackers exploit this by inserting:

- Always-true conditions (e.g., bypass login)
- Commands to extract or modify data

Step 3: Impact on Database Security
SQL Injection can severely compromise databases by:

- Unauthorized data access (customer records, passwords)
- Data modification or deletion
- Exposure of sensitive information
- Complete database takeover in severe cases

Step 4: Real-World Consequences
Successful SQLi attacks may lead to:

- Financial loss and legal issues
- Data breaches and privacy violations
- Loss of user trust and reputation damage

Step 5: Prevention Measures
To prevent SQL Injection:

- Use parameterized queries (prepared statements)
- Validate and sanitize user inputs
- Apply least-privilege database access

Quick Tip

Never trust user input directly in SQL queries — use parameterized queries to prevent SQL Injection.

---

12. What is Social Engineering, and why is it considered a non-technical threat?

Correct Answer: Social engineering is a manipulation technique where attackers exploit human psychology to gain confidential information or access. It is considered a non-technical threat because it targets human behavior rather than system vulnerabilities.

Solution: Concept: Social engineering is a cyberattack method that relies on psychological manipulation instead of technical hacking. Attackers trick individuals into revealing sensitive information such as passwords, financial data, or access credentials.
Step 1: What is Social Engineering?
It involves deceiving users by:

- Impersonating trusted individuals or organizations
- Creating fake scenarios to gain trust
- Manipulating emotions like fear, urgency, or curiosity

Common examples include phishing, pretexting, and baiting.
Step 2: How It Works
Attackers typically:

1. Build trust with the victim
2. Create a believable story (pretext)
3. Convince the victim to share confidential data

Step 3: Why It is a Non-Technical Threat
Unlike malware or hacking tools:

- It does not exploit software vulnerabilities
- It targets human weaknesses
- Even highly secure systems can be compromised if users are tricked

Step 4: Impact on Security
Social engineering can result in:

- Credential theft
- Unauthorized access to systems
- Financial fraud and data breaches

Step 5: Prevention
The best defense includes:

- User awareness and training
- Verifying identities before sharing information
- Strong authentication methods (e.g., 2FA)

Quick Tip

Social engineering hacks **people**, not computers — awareness is the strongest defense.
