CYBER SECURITY

OPEN ELECTIVE

SEMESTER – FIFTH

These important questions have been prepared using your previous exam papers (PYQs), verified concepts, and additional reference from trusted online academic sources.
For deeper understanding, please refer   your class notes as well.

🟦 *For more study materials, notes, important questions, and updates, visit –*
[DiplomaWallah.in](#)
🟦 *join our official WhatsApp group for free updates, contact [CLICK HERE JOIN](#)*

1️⃣ HIGH & LONG IMPORTANT QUESTIONS (90–95% Guaranteed)

(These are the "Master Questions". If you study these 10, you cover almost 60% of the paper. Long Answer Section usually comes from here.)

Q1. Define **Cyber Security**. Explain the core principles of security using the **CIA Triad** (Confidentiality, Integrity, Availability) and **AAA** (Authentication, Authorization, Accounting).

Q2. What is **Malware**? Classify and explain the following with symptoms:

- Virus vs. Worms
- Trojan Horse
- Ransomware
- Spyware & Rootkits

Q3. Explain the concept of **Defense in Depth**. Describe its various layers (Physical, Network, Host, Application, Data) with a neat diagram. Why is a single layer of security not enough?

Q4. What is **Cryptography**? Differentiate between **Symmetric (Private Key)** and **Asymmetric (Public Key)** Encryption. Briefly explain how the **RSA Algorithm** works.

Q5. Explain **Network Security Devices**:

- Function of a **Firewall** (Packet filtering vs. Stateful).
- Difference between **IDS** (Intrusion Detection System) and **IPS** (Intrusion Prevention System).

Q6. Describe **Windows Security Architecture**. Write short notes on:

- Windows Active Directory
- Group Policy Objects (GPO)
- User Account Control (UAC)

Q7. What is **Secure SDLC** (Software Development Life Cycle)? Explain how security is handled in the *Design, Development, and Testing* phases.

Q8. Explain **Threat Modeling**. Describe the **STRIDE** methodology (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) in detail.

Q9. Explain **Linux Security** basics:

- File Permissions (r-w-x)
- User Accounts & Root Privileges
- What is "System Hardening"?

Q10. What are **Web Application Attacks**? Explain the mechanism of **SQL Injection** and **Cross-Site Scripting (XSS)** with a simple example of how they happen.

2️⃣ IMPORTANT & SHORT QUESTIONS (50–70% Chance)

Q11. Differentiate between **Vulnerability, Threat, and Risk**. Give one example of each.

Q12. What is **Social Engineering**? Briefly explain **Phishing, Pretexting, and Tailgating**.

Q13. Write a short note on **Digital Signatures**. How do they ensure non-repudiation?

Q14. Explain **Data Classification**. What is the difference between *Restricted, Confidential, and Top Secret* data?

Q15. What is a **VPN** (Virtual Private Network)? How does **IPSec** help in securing data?

Q16. Explain **DoS (Denial of Service)** vs. **DDoS (Distributed Denial of Service)** attacks.

Q17. What is **Hashing**? How is SHA-256 different from Encryption? (Hint: One-way vs Two-way).

Q18. Write short notes on **Password Attacks**:

- Brute Force Attack
- Dictionary Attack
- Rainbow Table Attack

Q19. What is the **OWASP Top 10**? Briefly explain why it is important for developers.

Q20. Explain the concept of **Two-Factor Authentication (2FA)** and **Multi-Factor Authentication (MFA)**.

3️⃣ "AA BHI SAKTA HAI" (20–30% - The Tricky Ones)

Q21. What is the **McCumbers Cube**? (Focus on the 3 dimensions: Security Goals, Information States, Safeguards).

Q22. What are **Hardware Vulnerabilities**? Briefly explain **Meltdown and Spectre**.

Q23. What is **Steganography**? (Hiding data within data).

Q24. Explain **Version Control Systems**. Why is **Git** used in software development?

Q25. What is a **WAF** (Web Application Firewall)? How is it different from a Network Firewall?

📝 **Exam Strategy for JUT 2025 For Diploma Wallah Students :**

1. **Diagrams are King:** Even if the question doesn't ask, draw the **CIA Triad**, **OSI Model layers**, or **Encryption Keys** diagram.
2. **Point-wise Answers:** Never write paragraphs. Use headings like "1. Definition", "2. Working Principle", "3. Types".
3. **Real Examples:** When explaining attacks (like Ransomware), mention "WannaCry" or similar famous examples if you remember them.

.

DIPLOMA WALLAH (SWANGAM 💓)