Unit 1: Introduction to Cyber Crime & Cyber Security

1.1 Introduction

- **Cyber Security** → The practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
- It is also known as *information technology security* or *electronic information security*.
- Cyber Security applies in different contexts:
    - Business
    - Mobile computing
    - Government
    - Personal data protection

1.2 Cybercrime: Definition & Significance

- **Cybercrime** = Any illegal activity carried out using computers, networks, or digital devices.
- Examples: Hacking, Identity Theft, Cyberstalking, Phishing, Online Fraud.
- **Significance**:
    - Leads to **financial losses** (bank frauds, ransomware).
    - Causes **reputational damage** to organizations.
    - Impacts **national security** (cyber terrorism, espionage).
    - Affects **individuals** (identity theft, harassment).

Evolution & Historical Context

- 1960s → First hacking incidents on mainframe systems.
- 1980s → Introduction of computer viruses.
- 1990s → Rise of internet-based frauds & hacking.
- 2000s → Cyber terrorism & large-scale corporate breaches.
- Today → Advanced persistent threats, ransomware, AI-powered attacks.

1.3 Cybercrime and Information Security

- **Information Security (InfoSec):** Protects information from unauthorized access, disclosure, alteration, or destruction.
- **Cybercrime:** Exploits weaknesses in InfoSec.

- Example:
    - If a company does not update its firewall → hacker (cybercrime) can launch a **DDoS attack** exploiting the weakness (InfoSec failure).

1.4 Who are Cybercriminals?

- Individuals or groups involved in illegal digital activities.
  Types:

1. **Hackers** (ethical or malicious)
2. **Insiders** (employees misusing access)
3. **Organized crime groups** (cyber gangs, mafia)
4. **Terrorists** (cyber terrorism)
5. **Nation-state attackers** (government-backed espionage)

1.5 Hackers & Types of Hackers

- **White Hat Hackers** → Ethical, test systems for vulnerabilities.
- **Black Hat Hackers** → Malicious, steal data, damage systems.
- **Grey Hat Hackers** → Work in between (sometimes ethical, sometimes illegal).
- **Hacktivists** → Use hacking for political/social causes.
- **Script Kiddies** → Amateur hackers using pre-made tools.
- **Nation-Sponsored Hackers** → Backed by governments for espionage.

1.6 Types of Cybercrimes

1. **Email Spoofing & Spamming** – Fake identity emails, mass messages.
2. **Cyber Defamation** – Damaging someone's reputation online.
3. **Internet Time Theft** – Using internet services without authorization.
4. **Salami Attack / Data Diddling** – Small changes in systems, hard to detect.
5. **Forgery & Web Jacking** – Fake documents/websites to cheat people.
6. **Cyber Espionage** – Spying using internet & hacking.
7. **Hacking & Unauthorized Access**
8. **Online Frauds (Phishing, Scams, Fake Sites)**
9. **Computer Sabotage (Viruses, Worms, Malware)**
10. **Email Bombing, Mail Bombs**
11. **Identity Theft, Credit Card Fraud, Password Sniffing**

1.7 Vulnerability, Threats & Harmful Acts

- **Vulnerability** = Weakness (e.g., weak password).
- **Threat** = Potential danger (e.g., hacker trying brute force).
- **Attack** = Execution of threat exploiting vulnerability (e.g., account hacked).

1.8 CIA Triad

The **foundation of Cyber Security** is built on **CIA Triad**:

1. **Confidentiality** → Data is private & accessible only to authorized users.
    - Methods: Encryption, Access Control, Authentication.
2. **Integrity** → Data remains accurate & unchanged unless authorized.
    - Methods: Hashing, Digital Signatures, Checksums.
3. **Availability** → Systems & data are available when needed.
    - Methods: Redundancy, Backups, Disaster Recovery.

Unit 1 – PYQs (with Answers)

Q1. Define Cybercrime. Explain its significance in today's world.
Ans: Cybercrime is any illegal activity conducted via computer or digital device. It is significant because it causes financial losses, damages reputations, threatens national security, and impacts individuals through fraud and identity theft.

Q2. Differentiate between Cybercrime and Information Security.
Ans:

- Cybercrime → Illegal act (e.g., phishing attack).
- Information Security → Defense mechanism to prevent it (e.g., firewall, encryption).

Q3. Explain the CIA Triad with examples.
Ans:

- Confidentiality (encryption of emails).
- Integrity (hashing files to prevent tampering).
- Availability (backup servers to ensure uptime).

Q4. Who are Cybercriminals? Explain with examples.
Ans: Cybercriminals include hackers (black hats), insiders, organized groups, terrorists, and nation-sponsored attackers. Example: Anonymous (hacktivist group).

Q5. List and explain different types of Hackers.
Ans: White Hat, Black Hat, Grey Hat, Hacktivists, Script Kiddies, Nation-Sponsored.

Unit 2: Cybercrime Tools, Techniques & Cyber Laws

2.1 Introduction

- Cybercriminals use **various tools & techniques** to exploit vulnerabilities in systems and networks.
- Understanding these is critical to design preventive security mechanisms.

2.2 Proxy Servers & Anonymizers

- **Proxy Server** → Acts as an intermediary between user and internet.
  - Used to hide identity or bypass restrictions.
- **Anonymizer** → Special proxy that hides user's IP address to maintain privacy.
- **Misuse**: Criminals use proxies to launch attacks anonymously.

2.3 Phishing

- A **social engineering attack** where fake emails or websites trick users into sharing sensitive data (passwords, banking details).
- Example: A fake bank email asking user to "update account".

2.4 Password Cracking

- Methods attackers use to discover passwords.
- Techniques:
  1. Brute Force Attack (trying all possibilities).
  2. Dictionary Attack (using common words).
  3. Rainbow Tables (pre-computed hashes).
  4. Social Engineering (guessing based on personal info).

2.5 Keyloggers & Spyware

- **Keylogger** → Records keystrokes to steal sensitive info (e.g., passwords).
- **Spyware** → Malicious software that secretly monitors user activity.

2.6 Viruses & Worms

- **Virus** → Attaches itself to files/programs, spreads when executed.
- **Worm** → Self-replicates and spreads through networks without user action.

2.7 Trojan Horses & Backdoors

- **Trojan Horse** → Malicious program disguised as legitimate software.
- **Backdoor** → Hidden entry point bypassing normal authentication.

2.8 Steganography

- Technique of hiding secret information inside images, audio, or text.
- Example: Embedding confidential data in an image file.

2.9 DoS & DDoS Attacks

- **DoS (Denial of Service)** → Flooding a server to crash it.
- **DDoS (Distributed DoS)** → Multiple systems attack a single server simultaneously.
- Example: Botnets used to shut down websites.

2.10 SQL Injection

- Attack where malicious SQL queries are inserted into input fields.
- Example: `OR '1'='1'` → bypasses login page.

2.11 Introduction to Cyber Laws

- Cyber laws provide **legal framework** to prevent and punish cybercrimes.
- Covers issues like hacking, privacy, data protection, e-commerce frauds.

2.12 Cybercrime and Legal Landscape (World)

- Different countries have their own cyber laws (e.g., USA → Computer Fraud and Abuse Act).
- International treaties like **Budapest Convention on Cybercrime** provide cooperation.

2.13 Why Do We Need Cyber Laws (Indian Context)

- India has a growing digital economy (UPI, Aadhaar, E-commerce).
- Need for laws to protect citizens from fraud, identity theft, and cyber terrorism.

2.14 The Indian IT Act, 2000

- Primary law governing cybercrimes in India.
- Key Provisions:
  - **Section 43** → Unauthorized access, data theft.
  - **Section 65** → Tampering with computer source code.
  - **Section 66** → Hacking, identity theft, phishing.
  - **Section 67** → Publishing obscene material online.
  - **Section 69** → Power of government to intercept communication.
- Amended in 2008 to include cyber terrorism, data privacy, digital signatures.

2.15 Cybercrime & Punishment

- Cybercrimes in India are punishable by **fines, imprisonment, or both** depending on severity.
- Example: Identity theft (Sec 66C) → up to 3 years jail + fine.

2.16 Cyberlaw, Technology & Students (Indian Scenario)

- Students are increasingly exposed to cyber threats (social media scams, gaming frauds, exam paper leaks).
- Awareness of **cyber ethics** and **safe practices** is crucial.

Unit 2 – PYQs (with Answers)

Q1. What is Phishing? Give examples.
Ans: Phishing is a social engineering technique where fake websites or emails trick users into revealing sensitive information. Example: Fake bank login page.

Q2. Differentiate between Virus, Worm, and Trojan Horse.
Ans:

- Virus → needs host file to spread.
- Worm → self-replicating over networks.
- Trojan Horse → disguised as legitimate software.

Q3. What is SQL Injection? Explain with an example.
Ans: In SQL Injection, attackers insert malicious queries into input fields to manipulate databases. Example: Using `' OR '1'='1` in login forms.

Q4. Explain the importance of the Indian IT Act, 2000.
Ans: Provides legal recognition for e-commerce, digital signatures, and sets penalties for hacking, identity theft, data tampering, and publishing obscene content.

Q5. What are DoS and DDoS attacks? How can they be prevented?
Ans:

- DoS → Single attacker floods a server.
- DDoS → Multiple attackers.
- Prevention: Firewalls, IDS/IPS, Load Balancers.

Unit 3 – Security Mechanisms

📌 Theory Topics

1. **Cryptography** – definition, types (symmetric & asymmetric), applications.
2. **Encryption & Decryption** – working, examples.
3. **Hash Functions** – purpose, SHA, MD5.
4. **Digital Signature** – process, advantages.
5. **Public Key Infrastructure (PKI)** – components and working.
6. **Authentication Mechanisms** – passwords, OTP, biometrics, multi-factor.
7. **Access Control Models** – DAC, MAC, RBAC.
8. **Intrusion Detection Systems (IDS) & Prevention (IPS)**.
9. **Firewalls** – types, packet filtering, proxy.
10. **Virtual Private Network (VPN)** – working, advantages.

Important PYQs (with Answers)

1. Define cryptography.

Ans: Cryptography is the science of securing information by converting it into unreadable format (cipher text) using encryption algorithms, so only authorized users can read it.

---

2. Differentiate between symmetric and asymmetric encryption.

Ans:

- **Symmetric** → Same key for encryption & decryption (e.g., AES, DES).
- **Asymmetric** → Different public & private keys (e.g., RSA, ECC).

---

3. What is a digital signature?

Ans: A digital signature is an electronic equivalent of a handwritten signature used to ensure message authenticity, integrity, and non-repudiation.

---

4. Explain hash function with example.

Ans: Hashing converts input data into fixed-size value. Example: SHA-256 produces a 256-bit hash. Used in passwords & digital signatures.

---

5. What is Public Key Infrastructure (PKI)?

Ans: PKI is a framework that manages digital certificates and public-key encryption. It includes Certificate Authority (CA), Registration Authority (RA), and Key Management.

---

6. Explain firewall and its types.

Ans: A firewall is a security device that filters traffic between trusted and untrusted networks.

- Packet Filtering Firewall
- Proxy Firewall
- Stateful Inspection Firewall
- Next-Generation Firewall (NGFW)

---

7. Differentiate between IDS and IPS.

Ans:

- **IDS (Intrusion Detection System):** Detects malicious activities and alerts admin.
- **IPS (Intrusion Prevention System):** Detects and automatically blocks malicious activities.

---

8. Define authentication. List different mechanisms.

Ans: Authentication is verifying user identity before granting access. Mechanisms: Passwords, PINs, OTP, Biometrics, Multi-Factor Authentication.

---

9. Explain access control models.

Ans:

- **DAC (Discretionary Access Control):** Owner decides access.
- **MAC (Mandatory Access Control):** Based on security labels.
- **RBAC (Role-Based Access Control):** Based on user roles.

---

10. What is a VPN?

Ans: A Virtual Private Network (VPN) provides secure communication over the internet by encrypting data and hiding the user's IP address.

Alright 👍 let's **retry properly** — I'll now create a **FULL 100 Questions + Answers set** based exactly on the **Cyber Security syllabus (Unit 1 & Unit 2)**.
I'll make it structured, syllabus-based, and exam-ready.

📘 Cyber Security – Unit 1 & 2 (100 Questions & Answers)

UNIT 1 – Introduction to Cyber Crime & Cyber Security (50 Q&A)

Section A – Basics (Q1–Q10)

Q1. Define Cyber Security.
Ans: Cyber Security is the practice of protecting computers, networks, and data from unauthorized access, attacks, and damage.

Q2. Why is Cyber Security important?
Ans: It ensures confidentiality, integrity, and availability (CIA triad) of information and prevents financial & reputational loss.

Q3. Define Cybercrime.
Ans: Cybercrime is any illegal activity using computers or digital networks (e.g., hacking, phishing).

Q4. Differentiate between Cybercrime and Information Security.
Ans: Cybercrime = act of committing digital crime; Information Security = protecting data against such acts.

Q5. Who are Cybercriminals?
Ans: Hackers, insiders, cyber terrorists, organized crime groups, nation-state attackers.

Q6. List the main motives of Cybercriminals.
Ans: Financial gain, revenge, curiosity, political or social agenda, espionage.

Q7. Differentiate between Traditional Crime and Cybercrime.
Ans: Traditional crime occurs physically, while cybercrime occurs digitally with global reach and anonymity.

Q8. What is Cyber Espionage?
Ans: Unauthorized spying on confidential data, usually for political or economic advantage.

Q9. Define Cyber Terrorism.
Ans: Use of cyberspace to spread fear, disrupt systems, or attack national security.

Q10. What is Cyber Defamation?
Ans: Publishing defamatory content about a person or organization online.

Section B – Hackers & Attacks (Q11–Q25)

Q11. Who is a Hacker?
Ans: A person skilled in exploiting system vulnerabilities.

Q12. Types of Hackers?
Ans: White Hat (ethical), Black Hat (malicious), Grey Hat (mixed), Script Kiddies, Hacktivists, Nation-sponsored.

Q13. Differentiate between White Hat and Black Hat Hackers.
Ans: White Hat = ethical testing; Black Hat = malicious exploitation.

Q14. What is Hacking?
Ans: Unauthorized access to computer systems or networks.

Q15. What is a Script Kiddie?
Ans: Amateur hacker using pre-made tools without deep knowledge.

Q16. Define Hacktivism.
Ans: Hacking for social or political activism.

Q17. Explain Insider Threat.
Ans: Cybercrime committed by employees/insiders misusing access.

Q18. What is Social Engineering?
Ans: Manipulating people to reveal confidential information.

Q19. Define Internet Time Theft.
Ans: Unauthorized use of internet services without payment.

Q20. What is Salami Attack?
Ans: Minor data manipulations accumulating into a large fraud (e.g., rounding off transactions).

Q21. Define Data Diddling.
Ans: Altering data before or during entry into a computer.

Q22. What is Web Jacking?
Ans: Taking control of a website illegally.

Q23. What is Cyberstalking?
Ans: Repeated harassment or threats using electronic means.

Q24. Explain Email Spoofing.
Ans: Sending emails with forged sender addresses.

Q25. What is Spamming?
Ans: Sending unsolicited bulk messages via email or messaging platforms.

Section C – Security Concepts (Q26–Q40)

Q26. What is Vulnerability?
Ans: Weakness in a system that can be exploited.

Q27. Define Threat.
Ans: Potential cause of damage exploiting vulnerabilities.

Q28. Define Attack.
Ans: Actual exploitation of a system's vulnerability.

Q29. Explain the CIA Triad.
Ans: Confidentiality, Integrity, and Availability of information.

Q30. What is Confidentiality?
Ans: Ensuring data is accessible only to authorized users.

Q31. What is Integrity?
Ans: Ensuring data is accurate and unaltered.

Q32. What is Availability?
Ans: Ensuring systems and data are accessible when needed.

Q33. Define Non-Repudiation.
Ans: Assurance that the sender cannot deny sending a message.

Q34. What is Authentication?
Ans: Verifying identity of a user/system before access.

Q35. What is Authorization?
Ans: Granting permissions to authenticated users.

Q36. What is Cyber Forensics?
Ans: Application of investigation techniques to collect digital evidence.

Q37. Define Malware.
Ans: Malicious software designed to disrupt systems.

Q38. What is Ransomware?
Ans: Malware that encrypts files and demands ransom.

Q39. What is Botnet?
Ans: A network of infected devices controlled remotely.

Q40. Define Phishing Attack.
Ans: Tricking users into revealing sensitive info via fake websites/emails.

Section D – PYQs / Case Based (Q41–Q50)

Q41. Explain difference between Cybercrime & Traditional Crime with examples.
Q42. List types of Cybercriminals with examples.
Q43. Why is Cyber Security important for organizations?
Q44. Explain Email Bombing.
Q45. Define Cyber Vandalism.
Q46. What is Identity Theft? Give example.
Q47. Explain Credit Card Fraud.
Q48. Define Online Gambling Fraud.
Q49. Explain Cyber Espionage in national security.
Q50. Explain CIA Triad with real-world examples.

UNIT 2 – Cybercrime Tools, Techniques & Cyber Laws (50 Q&A)

Section A – Tools & Techniques (Q51–Q70)

Q51. What is a Proxy Server?
Ans: Intermediary server used to hide user identity.

Q52. Define Anonymizer.
Ans: Service that hides IP address for anonymous browsing.

Q53. Define Phishing.
Ans: Fake emails/websites tricking users into revealing info.

Q54. What is Password Cracking?
Ans: Recovering passwords using brute force, dictionary, rainbow tables.

Q55. Differentiate between Brute Force & Dictionary Attack.
Ans: Brute force = all combinations, Dictionary = list of common words.

Q56. What is a Keylogger?
Ans: Tool recording user keystrokes secretly.

Q57. Define Spyware.
Ans: Software that secretly monitors user activity.

Q58. What is a Virus?
Ans: Malware that attaches to files/programs and spreads.

Q59. Define Worm.
Ans: Self-replicating malware spreading via networks.

Q60. What is a Trojan Horse?
Ans: Malware disguised as legitimate software.

Q61. Define Backdoor.
Ans: Hidden entry point into a system bypassing authentication.

Q62. What is Steganography?
Ans: Hiding information inside media files.

Q63. Define DoS Attack.
Ans: Flooding system to make it unavailable.

Q64. Define DDoS Attack.
Ans: Distributed DoS using multiple machines (botnets).

Q65. What is SQL Injection?
Ans: Injecting malicious queries to manipulate database.

Q66. What is Cross-Site Scripting (XSS)?
Ans: Inserting malicious scripts into trusted websites.

Q67. Define Cyber Sabotage.
Ans: Deliberately damaging systems or networks.

Q68. What is Adware?
Ans: Software that displays unwanted ads.

Q69. Define Ransomware.
Ans: Malware locking data until ransom is paid.

Q70. Explain Email Spoofing with example.

Section B – Cyber Laws (Q71–Q90)

Q71. What are Cyber Laws?
Ans: Laws regulating online behavior, crimes, and e-commerce.

Q72. Why are Cyber Laws needed in India?
Ans: Protects individuals, ensures digital trust, regulates e-commerce.

Q73. What is the IT Act, 2000?
Ans: Primary Indian cyber law covering e-signatures, hacking, online fraud.

Q74. What are objectives of IT Act, 2000?
Ans: Legal recognition for e-documents, prevent cybercrime, promote e-commerce.

Q75. What is Section 43 of IT Act?
Ans: Covers unauthorized access, data theft.

Q76. What is Section 65 of IT Act?
Ans: Covers tampering with computer source code.

Q77. What is Section 66 of IT Act?
Ans: Covers hacking, identity theft, phishing.

Q78. What is Section 67 of IT Act?
Ans: Covers publishing obscene material online.

Q79. What is Section 69 of IT Act?
Ans: Grants govt power to intercept communication.

Q80. What is IT Act 2008 amendment?
Ans: Introduced cyber terrorism, stronger data protection, stricter penalties.

Q81. Define Digital Signature under IT Act.
Ans: Electronic method to authenticate messages, certified by CA.

Q82. What is Cyber Terrorism under IT Act?
Ans: Use of cyberspace to attack sovereignty, security of India.

Q83. What are punishments under IT Act?
Ans: Jail + fine, depending on severity (e.g., hacking = 3 years + fine).

Q84. Explain Cyber Defamation under IT Act.

Q85. What is E-Governance under IT Act?

Q86. What is E-commerce regulation under IT Act?

Q87. Define Cyber Ethics.

Q88. What is Cyber Law landscape globally?

Q89. What is Budapest Convention on Cybercrime?

Q90. How does Cyber Law affect students in India?

Section C – PYQs / Case Based (Q91–Q100)

Q91. Differentiate between Virus, Worm, and Trojan.
Q92. Explain SQL Injection with example.
Q93. Define DoS and DDoS with prevention methods.
Q94. Explain role of Proxy Servers in cybercrime.
Q95. Define Cyber Forensics with applications.
Q96. Explain role of IT Act in securing E-commerce.
Q97. Discuss impact of Cybercrime on Indian economy.
Q98. Explain case study of Identity Theft.
Q99. What are challenges in enforcing Cyber Laws in India?
Q100. Suggest preventive measures for Cybercrime.
