UNIT I: Introduction to Cyber Crime

Q.No	Pattern – 1 (Original Set)	Bloom's	Pattern – 2 (Revised Set)	Bloom's
1	Define cybercrime and explain its core characteristics, highlighting why it is considered a global threat.	K2	Explain cybercrime and discuss its key characteristics with suitable examples.	K2
2	Provide a detailed overview of Social Engineering, describing its life cycle from investigation to exit.	K2	Describe the nature and scope of cybercrime in the modern digital era.	K2
3	Discuss the Nature and Scope of Cyber Crime in the modern era, explaining why it is an "uncontrollable evil".	K2	Explain social engineering and analyze its life cycle stages.	K4
4	Describe the different types of Phishing attacks, including spear phishing, whaling, and angler phishing.	K2	Discuss various types of phishing attacks and their impact on users.	K2
5	Explain the three major categories of cybercrime: crimes against people, property, and government.	K2	Explain crimes against people with reference to hacking and cyberstalking.	K2
6	Compare and contrast Hacking and Cracking as defined under crimes against people.	K4	Compare crimes against property and crimes against government with examples.	K4
7	Detail Cryptocurrency Crime and explain Cyber Terrorism as defined by I4C.	K2	Analyze malware as a cybercrime tool and explain its common variants.	K4
8	Analyze Malware as a cybercrime tool, describing common types.	K4	Examine why cybercrime is considered an uncontrollable global threat.	K5

2 Marks Questions

Q.No	Pattern – 1	Pattern – 2
1	What is the definition of Cybercrime Investigation?	Define cybercrime.
2	Briefly explain DDoS attacks.	What is social engineering?
3	What is Cyber Stalking?	Define phishing.
4	Define Identity Theft.	What is cyberstalking?
5	What are Botnets?	Define malware.
6	Explain Honey Trap in social engineering.	What are botnets?
7	What is Cyber Squatting?	Define identity theft.
8	Define Cryptojacking.	What is cryptojacking?

UNIT II: Cyber Crime Issues

10 Marks Questions – Comparison Table

Q.No	Pattern – 1	Bloom's	Pattern – 2	Bloom's
1	Examine risks of unauthorized access and long-term company damage.	K5	Explain unauthorized access and discuss its risks.	K2
2	Discuss tips to detect and prevent unauthorized access.	K3	Analyze long-term damage caused by unauthorized access.	K4
3	Explain Computer Intrusions and misuse techniques.	K4	Explain computer intrusions and intrusion techniques.	K3
4	Define white-collar crime with examples.	K2	Describe white-collar crimes with cyber examples.	K2
5	Discuss viruses and malicious code.	K2	Discuss viruses and malicious code propagation.	K2
6	Compare Hacker vs Cracker traits.	K4	Compare hacking and cracking.	K4
7	Detail impact of Software Piracy.	K5	Examine impact of software piracy.	K5
8	Identify law enforcement roles in cybercrime.	K2	Discuss law enforcement agencies' role.	K2

2 Marks Questions

Q.No	Pattern – 1	Pattern – 2
1	What is Unauthorized Access?	What is unauthorized access?
2	Define Snooping.	Define snooping.
3	What is Bribery in cyber context?	What is a Trojan horse?
4	Explain Eavesdropping.	Define software piracy.
5	What is a Trojan Horse?	What is mail bombing?
6	Define Software Piracy.	Define eavesdropping.
7	What is a Mail Bomb?	What is cyber obscenity?
8	Define Cyberstalking as obscenity.	Define white-collar crime.

UNIT III: Investigation

10 Marks Questions

Q.No	Pattern – 1	Bloom's	Pattern – 2	Bloom's
1	Define Cybercrime Investigation and process.	K2	Explain concept and objectives of cybercrime investigation.	K2
2	Describe Digital Forensics tools.	K2	Describe digital evidence collection and preservation.	K3
3	Explain eDiscovery process.	K2	Explain eDiscovery process.	K2
4	Discuss rules of Evidence Collection.	K4	Analyze importance of chain of custody.	K4
5	Detail E-Mail Investigation techniques.	K3	Discuss email investigation techniques.	K3
6	Explain IP Tracking.	K3	Explain IP tracking methods.	K3
7	Discuss Encryption and Decryption.	K2	Discuss encryption and decryption techniques.	K2
8	Explain Search and Seizure of computers.	K4	Analyze legal and technical aspects of search and seizure.	K4

2 Marks Questions

Q.No	Pattern – 1	Pattern – 2
1	What is Digital Evidence?	What is digital evidence?
2	Name two Network Analysis tools.	Define hash value.
3	What is Drive Imaging?	What is email tracking?
4	Define Hash Value.	Define drive imaging.
5	What is Chain of Custody?	What is password cracking?
6	What is Email Tracking?	What is file carving?
7	Define Password Cracking.	Define chain of custody.
8	What is File Carving?	What is IP tracking?

UNIT IV: Digital Forensics

10 Marks Questions

Q.No	Pattern – 1	Bloom's	Pattern – 2	Bloom's
1	Introduction to Digital Forensics and process.	K2	Explain digital forensics and its importance.	K2
2	Challenges in digital forensics.	K4	Describe digital forensics investigation process.	K2
3	Forensic Software and Hardware tools.	K2	Discuss forensic software and hardware tools.	K2
4	Forensic Ballistics & Photography.	K2	Analyze challenges in modern digital forensics.	K4
5	Biometric recognition technologies.	K2	Explain forensic ballistics and photography.	K2
6	Audio and Video Analysis.	K3	Discuss biometric technologies.	K3
7	Linux directory layout.	K4	Analyze Linux file system.	K4
8	Network Forensics & DiD.	K4	Explain network forensics & defense-in-depth.	K4

2 Marks Questions

Q.No	Pattern – 1	Pattern – 2
1	Define Mobile Device Forensics.	What is digital forensics?
2	What is a Write Blocker?	Define write blocker.
3	Explain Data Carving.	What is live acquisition?
4	Purpose of Hash Analysis.	Define data carving.
5	Define Cloud Forensics.	What is hash analysis?
6	What is a Resident Virus?	Define cloud forensics.
7	What is Live Acquisition?	What is mobile device forensics?
8	Define Order of Volatility.	Define order of volatility.

UNIT V: Laws and Acts

10 Marks Questions – Comparison Table

Q.No	Pattern – 1	Bloom’s	Pattern – 2	Bloom’s
1	Explain CFAA and its significance.	K2	Explain cyber laws and ethics.	K2
2	Detail ECPA titles.	K2	Discuss digital evidence controls.	K3
3	Discuss Digital Evidence Controls.	K3	Explain evidence handling procedures.	K2
4	Evidence Handling Procedures stages.	K2	Role of Indian Evidence Act.	K2
5	Overview of Indian Cyber Laws.	K2	Explain IPC and CrPC provisions.	K2
6	Ethical considerations in cybersecurity.	K5	Discuss ECPA.	K2
7	Legal policies in organizations.	K3	Analyze ethical challenges.	K5
8	Incident Response Policies.	K3	Explain AUP and data retention policy.	K3

2 Marks Questions

Q.No	**Pattern – 1**	**Pattern – 2**
1	What is the Wiretap Act?	What is IPC?
2	Define SCA.	Define CrPC.
3	What are ACLs?	What is AUP?
4	Define IPC.	Define data retention policy.
5	What is CrPC?	What is digital evidence control?
6	Define AUP.	Define cyber law.
7	Define Intellectual Property Policy.	What is intellectual property policy?
8	Define Data Retention Policies.	Define ECPA.