Name:

Enrolment No:

UPES

End Semester Examination, December 2024

Course: Cyber Crimes & Electronic Evidence **Semester: IX**
Program: B. Tech. LL.B (Hons. 4) **Time : 03 hrs.**
Course Code: CLCB 5015 **Max. Marks: 100**

Instructions: All the questions are compulsory.

SECTION A
(5Qx2M=10Marks)

S. No.		**Marks**	**CO**
Q 1	How can the rise of digital payment platforms contribute to an increase in online financial crimes?	**2**	**CO1**
Q 2	What do you mean by Social Engineering Crimes in cyberspace?	**2**	**CO1**
Q 3	Ms. Yogita discovered that her personal information was used without her consent to open a new account on facebook. From her fake account many requests were sent for seeking money, resulting in significant reputation losses. What is the punishment of this act under the IT Act, 2000?	**2**	**CO1**
Q 4	Ms Shahin gained unauthorized access to a hospital’s database and threatened to release patient data unless a ransom was paid. Discuss the legal consequences of this act under the IT Act, 2000.	**2**	**CO1**
Q 5	In a scenario a teenager was tricked into sharing personal information of her friend on Instagram through a fake social media profile. What is the role of law enforcement agencies in handling such cybercrimes?	**2**	**CO1**

SECTION B
(4Qx5M= 20 Marks)

Q 6	How do social engineering techniques like phishing, pretexting, and baiting exploit human psychology to facilitate cybercrimes?	**5**	**CO2**
Q 7	Explain the role of Investigating Agencies in solving complex cybercrime cases.	**5**	**CO2**
Q 8	Elaborate the latest judgement on ‘Fundamental Right to Privacy’ in India.	**5**	**CO2**
Q 9	Evaluate the impact of the Information Technology Act, 2000 in regulating cybercrimes in India. What are its [5] strengths and [5] weaknesses?	**5**	**CO2**

SECTION-C
(2Qx10M=20 Marks)

Q 10	Critically analyze the salient features of the Information Technology Act, 2000 as amended in 2008.	**10**	**CO3**
Q 11	Examine & evaluate the validity of electronic evidences in Indian Judicial system with relevant & landmark case laws. Or Analyze the key challenges in determining jurisdiction in cybercrime cases, and how do legal theories address the cross-border nature of online offenses	**10**	**CO3**
SECTION-D **(2Qx25M=50 Marks)**			
Q 12	A leading e-commerce platform, ShopEasy, has become the target of a cyber attack. Hackers deployed hacking & malware that encrypts all company data, including customer records, payment information, and operational databases, rendering the platform inoperable. The attackers demanded $10 million in cryptocurrency as ransom, threatening to leak sensitive customer data on the dark web if the payment is not made within seven days. ShopEasy initially attempted to negotiate with the attackers but ultimately refused to pay the ransom, citing concerns about funding criminal activities. The hackers followed through on their threat, releasing partial data to prove their claims and putting millions of users' personal information at risk. The attack exposed ShopEasy's inadequate cybersecurity measures, including outdated firewalls and unpatched vulnerabilities in its system. Several affected users file lawsuits claiming damages due to identity theft and financial fraud. Meanwhile, law enforcement agencies face challenges in identifying and apprehending the attackers, who operate anonymously and across multiple jurisdictions. Answer the following questions based on the above scenario: 1. Name the cybercrimes occurred against ShopEasy? [5] 2. What do you mean by 'Ransomware Attack'? [5] 3. To what extent can **ShopEasy** be held legally liable for failing to implement adequate cybersecurity measures to protect customer data? [5] 4. What are the legal remedies available with ShopEasy? Advise. [10]	**25**	**CO4**
Q 13	Mr. Nitin, with a malicious intent to threaten the unity, integrity, and national security of the country Sindia, carried out a sophisticated hacking operation. He unlawfully infiltrated the military website of Sindia, gaining unauthorized access to the nation's highly sensitive and classified information. During the breach, he managed to extract critical data related to the country's defense infrastructure, which is part of	**25**	**CO4**

	Sindia's Critical Information Infrastructure (CII). Using this stolen data, Mr. Nitin executed a series of cyberattacks aimed at causing extensive harm. This cyberattack not only endangered public safety but also highlighted severe vulnerabilities in the nation's digital infrastructure. Answer the following questions based on the above scenario: (a) Describe the offence committed by Mr. Nitin, if any according to the IT Act, 2000 (2008)? [10] (b) Explain the modes of committing an offence under the above mentioned provision. Mention relevant case laws to support your answer. [10] (c) What is the punishment prescribed for the commission of the offence and for conspiring to commit the offence? [5]		