



Name:

Enrolment No:

UPES

End Semester Examination, December 2023

Course: Cyber Crimes
 Program: BA.LLB
 Course Code: CLCL 5002

Semester: IX
 Time: 03 hrs.
 Max. Marks: 100

Instructions:

SECTION A
(5Qx2M=10Marks)

S. No.		Marks	CO
Q1.	What are the different types of cybercrime that were perpetrated in the <i>Jamtara</i> cyber fraud case?	2	CO1
Q2	Distinguish between users, subscribers, and consumers.	2	CO1
Q 3	What do you understand by Decryption?	2	CO1
Q4	Define the term “Cyber Pornography.”	2	CO1
Q 5	What is Phishing?	2	CO1

SECTION B
(4Qx5M= 20 Marks)

Q 6	“Cyber criminals are everywhere” Explain and discuss the various techniques to commit cybercrimes.	5	CO2
Q 7	“Objectives for implementing the IT Act 2000 were well described” Discuss. What are the exclusions from the Act?	5	CO2
Q 8	Cryptography is used in a wide variety of applications, including e-commerce, online banking, and secure communication. What are some of the challenges of implementing cryptography in these applications?	5	CO2
Q 9	Specify the benefits of using EDI over traditional paper-based methods of exchanging data.	5	CO2

SECTION-C
(2Qx10M=20 Marks)

Q 10	Analyse the potential violations mentioned under the IT Act, 2000 for the stealing/tampering of data and highlight the penalties that he/she may face.	10	CO3
Q 11	A cybercrime investigation reveals that the crime was committed by a person living in another country. Determine the challenges faced by	10	CO3

	Indian law enforcement agencies in investigating and prosecuting cybercrimes committed by individuals or groups located outside of India.		
SECTION-D (2Qx25M=50 Marks)			
Q 12	A renowned Indian film production company has encountered a cyber-attack aimed at leaking unreleased movies online, leading to significant financial losses. Examine the measures that the company should take to investigate the attack, prevent further leaks, and collaborate with law enforcement agencies to apprehend the perpetrators and protect their intellectual property.	25	CO4
Q 13	<p>In 2012, two girls, Arfiya Siddique, and Reka Srinivasan, were arrested in Mumbai, India, for posting comments on Facebook that were critical of a bandh called in the wake of a famous Political Party chief's death. The girls were charged under Section 66A of the Information Technology Act of 2000, which criminalized the sending of "grossly offensive" or "annoying" messages through a computer resource or communication device. The arrests sparked widespread public outcry, and many people argued that Section 66A was unconstitutional and violated the right to freedom of speech and expression. In 2015, the Supreme Court of India struck down Section 66A in its entirety, ruling that it was vague and overbroad. The Court also found that the law violated the freedom of speech and expression guaranteed by Article 19(1)(a) of the Indian Constitution.</p> <p>In light of the above landmark judgment, discuss the potential legal and ethical implications of this policy.</p> <ol style="list-style-type: none"> a) Appraise the meaning of Section 66A, Information Technology Act of 2000, and why was it challenged in the above case. b) Analyse the interpretation of the 'Right to freedom of expression' under Article 19(1)(a) of the Constitution of India as held by the Supreme Court of India. c) Examine the factors that the Supreme Court of India considered in determining whether Section 66A was a reasonable restriction on the right to freedom of expression. d) Compare and contrast between "offensive" speech and speech that "incites violence or public disorder." e) Point out the implications of the above judgment for the regulation of online speech in India. 	5 x 5= 25	CO4