Name : Enrolment No. :	UPES UNIVERSITY OF TOMORROW

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, May 2025

Program Name : BTECH DATA-SCIENCE, AI & ML (H & NH), Full stack (H & NH) Semester : VI^{th}

Course Name : Cyber Security Time : 3 hours

Course Code : CSSF 3021 Max. Marks : 100

No. of Page(s) : 2

Instructions : Attempt all sections.

SECTION-A

S. No.	Questions	Marks	CO
Q.1	You are given a message and its corresponding digital signature. How would you verify its authenticity using public key cryptography? What role does a hash function play here?	4	CO 1
Q.2	A digital signature is 256 bits long. If a system processes 500 signed messages per second, how much bandwidth is used just for signatures in 1 minute?	4	CO 2
Q.3	Describe the role of key exchange protocols in symmetric key cryptography. Why is this a challenge over insecure channels?	4	CO 1
Q.4	A server logs 10 failed login attempts every minute. If the system flags an alert after 30 attempts, how long (in seconds) does it take to trigger the alert?	4	CO 3
Q.5	Find the multiplicative inverse of 7 modulo 26, i.e., find x such that $7x \equiv 1 \pmod{26}$.	4	CO 4

SECTION-B

Q.6	Suppose a message authentication code (MAC) changes after message transmission. What are the implications? How does this help detect tampering in communication systems?	10	CO 1
Q.7	A company uses the **mid-square method** to hash 4-digit employee IDs into a hash table of size 1000. The method involves: a) Squaring the key, b) Padding the result (if needed with 0's only) to at least 6 digits, c) Extracting the middle 3 digits, d) Using them directly as the hash index. Given the key: **Employee ID = 1234**, compute the hash value using this method. Show all intermediate steps and explain why the mid-square method may provide better dispersion than simple modulo-based hashing.	10	CO 2
Q.8	A company employee shared customer financial details via SMS without consent. Under which sections of the IT Act or IPC might the person be charged? Explain the legal consequences with reference to relevant acts.	10	CO 3

Q.9	Your organization's system has started to show pop-up ads, slow performance, and unknown installations. Identify the likely type(s) of malware involved and suggest which methods or protocols (e.g., anti-spyware, system tuning) can help mitigate the issue. OR You are given a 2-round small-scale Feistel Network with the following parameters: • Initial input block: $P = L_0 \Vert R_0 = 1010 \Vert 1101$ • Round function: $F(R, K) = R \oplus K$ • Round keys: $K_1 = 0110$, $K_2 = 0011$ Perform the encryption using the Feistel structure: $L_i = R_{i-1}, \quad R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$ Compute the final ciphertext after 2 rounds. Show all intermediate values.	10	CO 4
	SECTION-C		
Q.10	In 2023, a financial institution in India faced a cyberattack where customer data was leaked via a compromised email. The attack raised concerns about the evidentiary value of emails/SMS under the Information Technology Act 2000 and its amendments. Legal issues involving offenses under the IPC, RBI Act, and IPR Act also surfaced. Additionally, jurisdictional challenges arose as the attack originated from abroad. How should the institution address these legal and technical issues and enhance its cybersecurity awareness? OR A university's internal network was targeted by a ransomware attack that encrypted valuable research data, including student records and intellectual property. The attack came from an external threat actor exploiting a vulnerability in the university's outdated systems. The university had not recognized the growing need for cybersecurity in an increasingly connected cyber space. Following the attack, it was clear that the institution lacked an understanding of the types of cyberattacks it could face. What measures should the university implement to classify potential cyber threats and bolster its defenses against future attacks?	20	CO 1 & CO 2
Q.11	XYZ University implements an online exam system where students submit assignments and receive digitally signed feedback from faculty. To ensure authenticity and prevent tampering, the university uses SHA-256 for hashing, RSA for signing, and email-based communication for sharing the documents. Recently, a student claimed their assignment grade was altered after submission. The IT team investigates whether the signature on the feedback file matches the original submission. **Question:** a) Explain how digital signatures and hashing help in verifying the integrity and authenticity of feedback. b) If the feedback file hash doesn't match the signature, what could be the possible reasons? c) Suggest how message authentication codes (MAC) or timestamps can enhance this system.	20	CO 3 & CO 4