VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

REG.NO.:

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2024-2025

SLOT: A1

Programme Name & Branch	: 5 Year Integrated M.Tech (MIC, MID)
Course Code and Course Name	: CSI 3002 and Applied Cryptography and Network Security
Faculty Name(s)	: Dr. Nivitha K, Dr. Sunil Kumar, Dr. Thangaramya K, Dr. S M Farooq
Class Number(s)	: VL2024250101930, 1934, 1937 and 1940
Date of Examination	: 13-10-2024
Exam Duration	: 90 minutes

Maximum Marks: 50

Answer All Questions

Course Outcomes:

- CO3. Identify the authentication schemes for membership authorization
- CO4. Identify computer and network security threats, classify the threats and develop a security model for detect and mitigate the attacks.
- CO5. Identify the requirements for secure communication and challenges related to the secure web services
- CO6. Identify the need of ethical and professional practices, risk management using emerging security solutions.

Q. No	Question	M	CO	BL
1.	Consider the elliptic curve point E_{11} (1,6) to encode the plaintext message on the curve (10,9) using generator point G (2,7) with private key of 4 and the random k value is 3. Perform the encryption and decryption operations.	10	CO3	BL3
2.	Using the digital signature standard, Alice chooses prime number p = 11, q = 5 and private key X = 3. Alice wants to sign a message M=54 with hash value h = 2. i) Find the public key Y (2 Marks) ii) How Alice does the signing process to compute (r, s)? (4 Marks) iii) How Bob does the verification process? (4 Marks)	10	CO5	BL3
3.	a) Compute the value of the padding field, length field and number of blocks in MD5 for the following given message lengths i. 2000 bits ii. 4000 bits	4	CO5	BL3
	b) How will you select a good hash function? Give the criteria for selection.	6		

VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

REG.NO.:

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2024-2025

SLOT: A1

4.	a) How multi-factor authentication is used for identification and authentication. Provide an example of how a student can access the system.	4	CO4	BL2
	b) A application needs both message authentication and confidentiality properties. But authentication is needed with respect to plaintext. Hence, which model of message authentication code is suitable for this application. Draw a respective model.	3		
	c) Examine the approaches used by attackers to exploit identification and authentication flaws.	3		
5.	Imagine you are a security analysist. How do you employ X.509 certificate to ensure efficient authentication of data in your network. Provide an explanation and illustrate the scenario.	10	CO6	BL4

****