REG.NO.:

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

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

SLOT: E2 + TE2

Programme Name & Branch	: B.Tech. & Computer Science and Engineering
Course Code and Course Name	: BCSE309L & Cryptography and Network Security
Faculty Name(s)	: Applicable to all
Class Number(s)	: Applicable to all
Date of Examination	: 20-March-2025
Exam Duration	: 90 minutes **Maximum Marks:** 50

General instruction(s):

- Answer All Questions
- M - Max mark; CO – Course Outcome; BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyze, 5 – Evaluate, 6 – Create)
- **Course Outcomes**
  CO2 - To understand concept of various cryptographic techniques.
  CO3 - To apprehend the authentication and integrity process of data for various applications.

Q. No.	Question	M	CO	BL
1.	Emma, a security consultant, wants to securely send a confidential message, "INTELLIGENT," to her colleague Liam using RSA encryption. She decides to use a public-key cryptosystem where the modulus is n=17680 and the encryption exponent is e=3. To ensure that only Liam can decrypt the message, Emma encrypts it using the 00-26 encoding scheme. Meanwhile, Liam, who holds the secret decryption key, must compute the private exponent, d to retrieve the original message. Show the ciphertext of the message sent to Liam and compute d, the private exponent required to decrypt the ciphertext.	10	2	3
2.	Given a prime number p=233 and a primitive root g=5, Alice chooses a secret key a=191 and Bob chooses a secret key b=211. However, an attacker Eve performs a Man-in-the-Middle (MITM) attack by intercepting and replacing the public keys exchanged between Alice and Bob. Instead of forwarding the correct values, Eve sends her own public keys to both parties. Eve selects her secret key as e_1=181 and e_2=157 for Alice and Bob respectively. a. Compute the public keys that Eve sends to Alice and Bob. [4] b. Compute shared secret keys between Alice and Eve, and between Bob and Eve. [4] c. Show that Alice and Bob end up with different secret keys due to the attack. [2]	10	2	3
3.	a. David, a cybersecurity researcher, is analysing the security of a hashing algorithm used in digital forensics. As part of his research, he needs to compute a specific word in the SHA-512 message schedule expansion for a given set of 16-bit hexadecimal words. He has been provided with the following words: W_0=0x1234, W_1=0xFEDC, W_2=0x0011, W_3=0x8899, W_9=0x5555, W_{14}=0x1111 Using SHA-512's word expansion and addition modulo 2^{16}, David must compute the value of W_{16}.	8	3	4

REG.NO.:

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

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

SLOT: E2 + TE2

	b. Compute and show the result of the function which is used in SHA-512 round operations and acts on the first three buffers (64bits each). a = 510E527FADE682D1 e = 6A09E667F3BCC908 b = 9B05688C2B3E6C1F f = BB67AE8584CAA73B c = 1F83D9ABFB41BD6B g = 3C6EF372FE94F82B d= 5BE0CD19137E2179 h = A54FF53A5F1D36F1	2	3	4
4.	a. HMAC is used for message authentication in a banking system. If an attacker can observe the HMAC output but not the key: i. Can they forge a valid message? Justify. [2] ii. How does HMAC resist preimage attacks? [3]	5	3	2
	b. Alice wants to sign a message using the ElGamal signature scheme with small values for easy computation. She chooses a prime modulus q=23, a generator α=5, and her secret key X_a=6. She needs to sign a message with hash value h(M)=9 using a randomly chosen integer k=7. Illustrate the steps involved in signing process and the verification process.	5	3	2
5.	Bob wants to generate a digital signature using DSA with the prime modulus p=67, subgroup order q=11, and h=3. i. Compute the value of g and check whether it is prime or not. [4] ii. Assume if Bob selects the per message secret integer as 7, the pseudo random integer, k as 5 and the hash of the message as 13, what would be the signer digital signature component. [4] iii. How does the receiver verify the signature component sent by Bob? [2]	10	3	3

****