REG.NO.: 23BCE0717

SLOT: B2+TB2

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 2025-2026

Programme Name & Branch	: B. Tech CSE and All Specialization
Course Code and Course Name	: BCSE309L_ Cryptography and Network Security
Faculty Name(s)	: COMMON TO ALL
Class Number(s)	: COMMON TO ALL
Date of Examination	: 16 March 2026 [9:30 – 11:00 AM]
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	Module	Marks	CO	BL
1.	Construct an Elliptic Curve over the Finite Field Set of all Integers Mod 7. Consider the value for a and b in the equation to be 1. Perform the following a) List the points on the curve and demonstrate the point addition process by calculating the result of adding point P(0,6) to point Q(2,2) **[4 Marks]** b) Consider the Elliptic Curve $E(F_7)$ defined by $y^2 \equiv x^3+x+1 \pmod 7$. Given a Private Key n=2 and a Generator Point G=(2,2), calculate the resulting Public key Q. Encrypt the message point M(0,6) using the Public key and a chosen ephemeral key k=2 **[6 marks]**	3	10	2	3
2.	A research facility uses the Paillier cryptosystem to perform computations on encrypted data. Given the prime factors p=5 and q=7: a) Determine the Public Key (n, g) and the Private Key (λ, μ). (use the standard g=n+1)**[3 Marks]** b) Encrypt the message $m_1=2$ and $m_2=3$ using the random integers $r_1=1$ and $r_2=2$ and get C_1 and C_2 **[4 marks]** c) Verify the additive homomorphic property of the Paillier cryptosystem using C_1, C_2, m_1 and m_2. **[3 marks]**	3	10	2	3
3.	A security division at VIT Vellore uses the SHA-512 algorithm to authenticate the plaintext message "FLY". Given Parameters: • Plaintext ASCII: F (70), L (76), Y (121). • Register Snapshots (Binary):	4	10	3	4

REG.NO.:

SLOT: B2+TB2

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 2025-2026

	A=01100001 B=01100010 C=01100011 E=01100101 F=01100110 G=01100111 a) Calculate the total length of the padding required to format the message into a 1024-bit block. **[4 Marks]** b) Compute the result of the Majority function, Maj(A, B, C), using the provided register values for the first three buffers. **[3 Marks]** c) Compute the result of the function, Ch(E, F, G), using the provided register values for the last three buffers. **[3 Marks]**				
4.	a) Given an input message with a length of 1475 bits to be hashed using the MD5 algorithm, calculate the specific number of padding bits required to meet the necessary congruency requirement and determine the resulting total number of 512-bit blocks that will be generated for the compression function. **[5 Marks]** b) Within the MD5 compression function, a 512-bit message block is divided into sixteen 32-bit sub-blocks (M0 through M15). Explain how the algorithm determines which sub-block (M_g) is used during each of the four rounds. Specifically, calculate which message sub-block index (g) will be used in the first step of Round 2 (Step 16) and the first step of Round 3 (Step 32). **[5 Marks]**	4	10	3	4
5.	a) Consider the ElGamal Digital Signature algorithm with prime q=19 and primitive root g=2. Given that User A selects the private key X_A=5 and an ephemeral key k=7: Calculate User A's Public Key Y_A. Generate the digital signature (s_1, s_2) for a message with hash value H(M)=17. Demonstrate the verification process to prove the signature is authentic **[5 Marks]** b) A user transmits the unencrypted message along with the hash code of the message generated using SHA512 to another user. The hash code was generated using a secret key which only the sender and receiver know. The message is not confidential and hence it is unencrypted. Analyse the security of this message authentication scheme. Justify your analysis with examples. **[5 Marks]**	5	10	3	4