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

REG.NO.:

SLOT: B1+TB1

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - II
WINTER SEMESTER 2025-2026

Programme Name & Branch	: B.Tech (All Branches)
Course Code and Course Name	: BCSE309L- Cryptography & Network Security
Faculty Name(s)	: All
Class Number(s)	: All
Date of Examination	: 16-03-2026 (AN)
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 – Analyse, 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.	Prove ***RSA's multiplicative homomorphism***, showing all the steps for the given message "VIT" (*ASCII-decimal: 86 73 84*) with *modulus* $n = 143$ and *private key* $d = 7$.	3	10	2	3
2.	The research division at VIT Vellore uses ***ECC-based encryption*** to secure sensitive data. A ciphertext {C1(7,4), C2(0,6)} has been intercepted, and your task is to recover the original data. Given that Elliptic curve: $y^2 \equiv x^3 + 10x + 6 (\text{mod } 13)$,with base point: $G = (5,5)$ and public key point (7,9).	3	10	2	3
3.	A research lab uses ***SHA-512*** for the message authentication. Generate the first block of message pattern, including message, padding, etc for the given message "VIT"(ASCII: 56 49 54); Round const K_0: $x428a2f98d728ae22$ Also, calculate its round-0 functions: *Maj()*, *Ch()* and updated *buffer 'E'*. $a = 0x6a09e667f3bcc908$ $b = 0xbb67ae8584caa73b$ $c = x3c6ef372fe94f82b$ $d = 0xa54ff53a5f1d36f1$ $e = 0x510e527fade682d1$ $f = x9b05688c2b3e6c1f$ $g = 0x1f83d9abfb41bd6b$ $h = 0x5be0cd19137e2179$.	4	10	3	5
4.	A) A University uses **MD5** for the message authentication. Calculate Round-1 function and updated buffers, after round-1,operation-0 for the given message, "VIT" (ASCII: 56 49 54) Round const, K1: $0xd76aa478$ *Buffers: A:* $0x67452301$ *B:* $0xEFCDAB89$ *C:* $0x98BADCFE$ *D:* $0x10325476$.	4	7	3	5
	B) Given a *64-bit hash function*, calculate required number of trials/samples for **Birthday attack** with collision probability of ½.		3		
5.	A) The finance department at VIT University uses **ElGamal digital signature** to authenticate confidential reports. A signed report is signed by secret key, *x=7*, and you need to verify whether the *signature(r,s): (4,13)* is valid or not for the received *hash: 79*. Given that $(p, g) = (47, 3)$.	5	3	3	4
	B) The examination office at VIT University uses the **DSA** to authenticate grade reports. Your task is to verify whether the *signature(r,s): (22,16)* is valid for the received hash: 80. Given *(p, q, g): (107,53,3) & public key: 36.*		7		4

***