



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

Page 1 of 2

Programme Name & Branch : M. Tech (Int)
Course Code and Course Name : CSI3022 and Cyber Security and Application Security
Faculty Name(s) : Dr. Saranya. P, Dr. Siva Shanmugam, Dr. Parthiban, Dr. Kovendan
Class Number(s) : Common to C2 slot
Date of Examination : 07-10-2025
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 - Analyse, 5 - Evaluate, 6 - Create)
- Course Outcomes
- 3. Understand and implement the cryptographic techniques and know the real time applications of various cryptographic techniques.
- 4. Know fundamentals of cybercrimes and the cyber offenses.
- 5. Understand the cyber threats, attacks, vulnerabilities and its defensive mechanisms

Q. No	Question	Module	Marks	CO	BL
1.	Explain the MixColumn transformation in AES and apply it to compute the transformed values of the third and fourth columns of the given ShiftRow matrix. $\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} 63 & 47 & a2 & f0 \\ 9c & 63 & c5 & f2 \\ 7b & 7c & f0 & ab \\ ca & af & 76 & 76 \end{bmatrix}$ Show all intermediate steps to support your answer	3	10	3	3
2.	Consider the elliptic curve defined over the finite field GF(37): E: $y^2 \equiv x^3 + 2x + 3 \pmod{37}$ Field: GF(37) 1. Find all the affine points (x, y) on the curve, i.e., all integer pairs with $x, y \in \{0, 1, \dots, 36\}$ that satisfy the curve equation. Also mention the point at infinity O. 2. For the point $P = (0, 15)$, compute the point doubling $2P = P + P$. Show step-by-step calculation of the slope λ and the resulting coordinates of 2P. Verify the result lies on the curve. 3. For the points $P = (0, 15)$ and $Q = (0, 22)$, compute the point addition $P + Q$. Show the slope calculation and the resulting point. Verify the result lies on the curve.	3	10	3	3



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

3.	Imagine you are part of a cybersecurity defence team for a smart city that relies on IoT devices for traffic control, healthcare monitoring, and public safety. Intelligence reports suggest that a group of attackers is planning a large-scale cyber-attack targeting these systems. As a defence analyst, break down how the attackers might plan such an attack (e.g., reconnaissance, identifying vulnerabilities, selecting attack vectors) and analyse how you would use this understanding to strengthen the city's cyber defences.	4	10	4	4
4.	In a small town, cybercrimes such as phishing and online harassment are frequently traced back to local cybercafés where computers are shared by many users daily. As a policy advisor, evaluate the effectiveness of current legal frameworks in holding cybercafés accountable. What improvements would you recommend ensuring both public access and digital safety?	4	10	4	5
5.	An employee of a company receives a friend request on social media from an account impersonating a senior manager. After accepting, they are tricked into clicking a link that captures their login credentials. Evaluate how phishing through social media can compromise organizational security. Recommend the strategies of both technical and behavioural that the company can implement to prevent such attacks in the future.	5	10	5	2

.....