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

REG.NO.:

SLOT: C1+TC1

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

Programme Name & Branch	: M. Tech (Int)
Course Code and Course Name	: CSI3022 and Cyber Security and Application
Faculty Name(s)	: Dr. Kovendan, Dr. Saranya, Dr. Parthiban, Dr. Gopinath
Class Number(s)	: Common
Date of Examination	: 7-10-2025
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

1. Know the fundamental mathematical concepts related to security
2. Know the basic concepts of information and network security
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.
6. Design suitable security policies and know about the industry practices

Q. No	Question	Module	Marks	CO	BL
1.	**Plaintext:** 00 04 12 14 12 04 12 00 0C 00 13 11 08 23 19 19 **Cipher Key:** 24 75 A2 B3 34 75 56 88 31 E2 12 00 13 AA 54 87 Determine the input state matrix of Mix Column in AES by clearly mentioning all the intermediate steps for the plain text shown.	3	10	3	3

SubBytes transformation table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8

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

REG.NO.:

SLOT:

429 - 37

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

	SubBytes transformation table (continued) 0 1 2 3 4 5 6 7 8 9 A B C D E F 7: 51 A3 40 8F 92 9D 38 F5 BC B6 DA 21 10 FF F3 D2 8: CD 0C 13 EC 5F 97 44 17 C4 A7 7E 3D 64 5D 19 73 9: 60 81 4F DC 22 2A 90 88 46 EE B8 14 DE 5E 0B DB A: E0 32 3A 0A 49 06 24 5C C2 D3 AC 62 91 95 E4 79 B: E7 CB 37 6D 8D D5 4E A9 6C 56 F4 EA 65 7A AE 08 C: BA 78 25 2E 1C A6 B4 C6 E8 DD 74 1F 4B BD 8B 8A D: 70 3E B5 66 48 03 F6 0E 61 35 57 B9 86 C1 1D 9E E: E1 F8 98 11 69 D9 8E 94 9B 1E 87 E9 CE 55 28 DF F: 8C A1 89 0D BF E6 42 68 41 99 2D 0F B0 54 BB 16				
2.	Evaluate the security of the Diffie-Hellman key exchange when using the prime q=83 and generator a=5. Alice's private key is x=7 and Bob's private key is y=11. Justify your assessment by demonstrating a brute-force attack an adversary could use to find one of the private keys. Then, discuss the necessary size of the prime number to ensure a secure exchange.	3	10	3	5
3.	Develop a new classification system for cybercrimes that addresses the shortcomings of existing models, such as the rise of cryptocurrency-based fraud and AI-driven attacks. Justify your new categories with a focus on improving law enforcement and risk management.	4	10	4	6
4.	Given a scenario where attackers use tailgating to enter a restricted area, analyse the weaknesses in the organization's security policies that allowed the attack, and suggest improvements to close those gaps.	4	10	4	4
5.	Evaluate the effectiveness of current government regulations and cyber-laws in deterring identity theft crimes. Discuss at least two strengths and shortcomings, and also suggest improvements.	5	10	5	5

****