VIT
Vellore Institute of Technology

REG.NO.:

SLOT: B1+TB1

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

Programme Name & Branch	: B.Tech Computer Science and Engineering
Course Code and Course Name	: BCSE309L Cryptography and Network Security
Faculty Name(s)	: MARY MEKALA A, RAMANI S, NARESH K, DEEPIKAA S, NAVAMANI T M, SELVI M, BHUVANESWARI M, SIVA SANKARI S, MOHANA SUNDARI L, UMAMAHESWARI M, S M FAROOQ, BALAJI N, THANGARAMYA K, MARIAPPAN R, SURESH A, ISLABUDEEN M, RAKHI MOL V
Class Number(s)	: VL2025260501934, 1936, 1938, 1923, 1928, 1941, 1948, 1932, 1935, 2478, 1943, 1946, 1950, 1931, 1982, 1954, 1959
Date of Examination	: 28-01-26 (FN)
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 (Type the CO statements covered in this question paper. Use the CO number as per the syllabus copy)
  CO1. To know the fundamental mathematical concepts related to security.
  CO2. To understand concept of various cryptographic techniques.

Q. No	Question	Module	Marks	CO	BL
1.	Use the Euclidean Algorithm to find GCD (32657, 8685) and find the multiplicative modulo inverse of given numbers using Extended Euclidean Algorithm (Show the steps).	1	10	CO1	BL3
2.	a. Find the integer value of x that satisfies the following system of congruence's: $x \equiv 3 \pmod 5$ $x \equiv 5 \pmod 7$ $x \equiv 7 \pmod{11}$	1	6	CO1	BL3
	b. Using Fermat's theorem, check whether 19 is prime or not?. Consider a is 7.	1	4	CO1	BL3
3.	Explain various Block Cipher modes of operation with neat diagrams.	2	10	CO2	BL2
4.	Let Alice wants to send a message "123456HELLO32536" to Bob through social	2	10	CO2	BL3

VIT
Vellore Institute of Technology

REG.NO.:

SLOT: B1+TB1

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

network. He uses Data Encryption Standard (DES) algorithm for session encryption during his communication and assume that he uses the key as "DABB 0918 2736 AADD". Show the key generated for the first two rounds. Refer the following tables.

Parity Drop Table

57	49	41	33	25	17	09	01
58	50	42	34	26	18	10	02
59	51	43	35	27	19	11	03
60	52	44	36	63	55	47	39
31	23	15	07	62	54	46	38
30	22	14	06	61	53	45	37
29	21	13	05	28	20	12	04

Compression Box Table

14	17	11	24	01	05	03	28
15	06	21	10	23	19	12	04
26	08	16	07	27	20	13	02
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

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 - I
WINTER SEMESTER 2025-2026

5.	Find the first round key of AES 128 using the following main key which is given in hexadecimal, S-Box table given below and the round constant is 01. Main Key K = 56 08 20 07 C7 1A B1 8F 76 43 55 69 A0 3A F7 FA	2 10		CO2	BI

X \ Y	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
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	C8	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	4D	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

S-Box for AES

CAT 1 - CNS - Bi Shot
Answer Key

1) GCD (32657, 8685)
There are coprime numbers.
Ans. 1

* Multiplicative Inverse using Extended Euclidean Algorithm
$t = t1 - q\,t2$

q	r1	r2	r	t1	t2	t
3	32657	8685	6602	0	1	-3
1	8685	6602	2083	1	-3	4
3	6602	2083	353	-3	4	-15
5	2083	353	318	4	-15	79
1	353	318	35	-15	79	-94
9	318	35	3	79	-94	925
11	35	3	2	-94	925	-10269
1	3	2	1	925	-10269	11194
2	2	1	0	-10269	11194	-32657
	1	0		11194	-32657	

M.I is 11194

2.

a.

$$x \equiv 3 \pmod 5$$
$$x \equiv 5 \pmod 7$$
$$x \equiv 7 \pmod{11}$$

Ans.

$$M = 5 \cdot 7 \cdot 11 = 385$$

$$M_1 = \frac{385}{5} = 77 \qquad m_1 = 5$$

$$M_2 = \frac{385}{7} = 55 \qquad m_2 = 7$$

$$M_3 = \frac{385}{11} = 35 \qquad m_3 = 11$$

Finding Modular inverse

$$77 \equiv 2 \pmod 5$$

$$y_1 = M_1^{-1} \pmod{m_1}$$

$$y_1 = 77^{-1} \pmod 5 \equiv 2^{-1} \bmod 5$$
$$\equiv 3 \pmod 5$$

$$y_2 = 55^{-1} \pmod 7 \equiv 6^{-1} \bmod 7$$
$$\equiv 6 \pmod 7$$

$$y_3 = 35^{-1} \pmod{11} \equiv 2^{-1} \pmod{11}$$
$$\equiv 6 \pmod{11}$$

Substituting in CRT formula

$$x \equiv 3(77)(3) + 5(55)(6) + 7(35)(6)$$
$$x \equiv 693 + 1650 + 1470 \bmod 385 \bmod 385$$
$$x \equiv 3813 \pmod{385} = \boxed{348}$$

2.b.

$7^2 \equiv 49 \equiv 11 \pmod{19}$

$7^4 \equiv 121 \equiv 7 \pmod{19}$

$7^9 \equiv 7^8 \cdot 7 \equiv 11 \cdot 7 = 77 \equiv 1 \pmod{19}$

$7^{18} = (7^9)^2 \equiv 1^2 \equiv 1 \pmod{19}$

$\therefore 7^{18} \equiv 1 \pmod{19}$ As per format's theorem

$\therefore$ 19 is prime number

3. Block Cipher Modes

ECB (Electronic Codebook) mode

CBC (Cipher Block chaining) mode

CFB (Cipher Feedback) mode

These have to be discussed with neat diagrams.

4. Round 1 key = 59C4D066DE8F

Round 2 key = C56838 1ABDCA

5. Round 1 key

D7 60 0D E7, 10 7A BC 68

66 39 E9 01, C6 03 1E FB