Vellore Institute

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

SLOT: D1+TD1

Programme Name & Branch	:BTECH-IT
Course Code and Course Name	:BITE401L-Network and Information Security
Faculty Name(s)	:Dr. R.Sivashankari, Dr. Shantharajah S P, Dr Rampriya R S
Class Number(s)	: VL2025260502222, 2224, 6712
Date of Examination	:30-01-2026
Exam Duration	: 90 minutes

Maximum Marks: 50

General instruction(s):

- Answer All Questions
- BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)
- Course Outcomes
  CO1. Understand the security principles and mechanisms.
  CO2. Analyze and evaluate cryptographic primitives

Q. No	Question	M	CO	BL
1a.	Describe different security attacks with short explanations.	5	1	1
1b.	"Computer and network security is both fascinating and complex." Justify this statement by explaining the various reasons that make computer and network security challenging.	5	1	
2a.	Find the encryption for the message "COMSEC means communications security" using Playfair cipher with key "GALOIS".	5	2	
2b.	Apply columnar transposition technique to encipher the plaintext PROGRAMMINGPRAXIS with the keyword COACH.	5	2	
3.	Use Simplified Data Encryption algorithm to convert the 8-bit plaintext = 1 0 0 1 0 1 1 1 into cipher text. The following parameters are necessary for the conversion IP=2,6, 3, 1, 4, 8, 5, 7 IP-1= 4, 1, 3, 5, 7, 2, 8, 6 EP= 4, 1,2, 3, 2, 3, 4, 1 P4=2, 4, 3, 1 Key-1 = 1 0 1 0 0 1 0 0 Key-2 = 0 1 0 0 0 0 1 1 S0 = [1,0,3,2 3,2,1,0 0,2,1,3 3,1,3,2] S1= [0,1,2,3 2,0,1,3 3,0,1,0 2,1,0,3]	10	2	
4a.	Calculate the round 1 key [w4, w5, w6, w7] using AES key expansion algorithm. The round 0 key - 0f1571c947d9e8590cb7add6af7f6798, Rcon (1)- 01 00 00 00 and the S-box is given below	5	2	3

Vellore Institute of Technology

SCHOOL OF COMPUTER SCIENCE ENGINEERING AND INFORMATION SYSTEMS

CONTINUOUS ASSESSMENT TEST - I

WINTER SEMESTER 2025-2026

SLOT: D1+TD1

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	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

S-box

4b.	**Given the plaintext {00010203040506070809 0A0B0C0D0E0F} and the key {01010101010101010101010101010101}, Find the following operations using AES.** i. **Show the original contents of State, displayed as a 4 x 4 matrix.** ii. **Show the key displayed as 4 x 4 matrix** iii. **Show the value of state matrix after initial round key.** iv. **Show the value of state matrix after Shift rows(use the initial round key output matrix)**	5	2	3
5.	Andrew and Ben has the following public key components **{p = 17, q = 13, e = 5}**. What would be the cipher text if Andrew attempts to send the message **M = {3}** in encrypted form to Ben using RSA approach. Compute the private key of Ben as well show that how he retrieve the plain text from the cipher.	10	2	3