REG.NO.:

VIT®

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

NAME OF THE SCHOOL
CONTINUOUS ASSESSMENT TEST - II
FALL SEMESTER 2024-2025

SLOT: E2

Programme Name & Branch : B.Tech ECE
Course Code and Course Name : BECE411L Cryptography & Network Security
Faculty Name(s) : Dr. Ravikumar CV ,Dr. Saranya KC
Class Number(s) : VL2024250103632, VL2024250107873
Date of Examination :17/10/24
Exam Duration : 90 minutes **Maximum Marks: 50**

General instruction(s):

- Answer All Questions

Q. No	Question	M	CO	BL
1.	From the given below specifications, compute public key, cipher text and private key. Comment on the outcomes and draw its block diagram for RSA Algorithm. P = 3 ; Q= 7 choose e such that second largest valid number (e = d) Plaintext = CDEF (Field entries to be assume it as A=0, B=1, C=2....in decimal form)	10	4	4
2.	Assume that two users are connected in point to point topology, compute the keys for user A and user B by enabling DHKE algorithm,for the given below specifications. Global parameter = $(D)_H$ Private key for user A and user B = 0110, 1000 Binary values	10	3	4
3.	Using simplified AES algorithm, generate the four different keys using key generation concept and draw its diagram. Key : $(2466)_H$ ----16 bit length Note: For RC-3 and RC-4 perform Caesar cipher for previous round constant	10	4	3
4.	The following plain text should be converted into encrypted text by means of the SNP cipher.Draw its diagram and comment on the outcomes. Plain text = $(1357)_H$ ----16 bit length Keys $K_0 = (0123)_H$ $K_1 = (4567)_H$ $K_2 = (AABB)_H$ $K_3 = (9900)_H$ Note: mapping with different s-boxes as Caesar cipher	10	4	3
5.	Generate the Codeword, PN sequence, and verify its properties using LCG. With unity as the seed value, set a = 3, c = 1, and m = 7.	10	3	4

****