VIT

Vellore Institute of Technology

School of Computer Science and Engineering

Fall Semester 2024-25

CAT-I

SLOT:C1+TC1

Programme Name & Branch: M.Tech (Integrated), Computer Science and Engineering

Course Name & Code: Cyber Security and Application Security & CSI3022

Class Number (s):VL2024250101961 & VL2024250101962

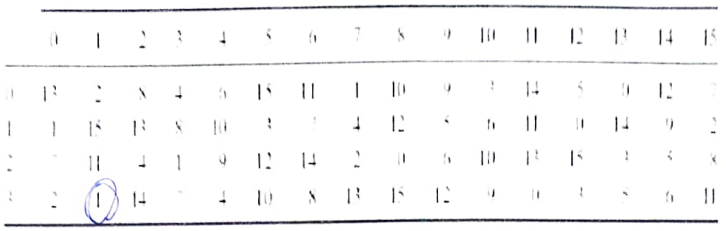
Faculty Name (s): Prof. K. Parthiban & Prof. S. Siva Sankari

Exam Duration: 90 Min. **Maximum Marks: 50**

General instruction(s):

Answer All the Questions and calculator is allowed

Q. No.	Question	Max Marks
1.	a) Determine the greatest common divisor of 1160718174 and 316258250 using Euclidian algorithm. (5 Marks) b) Elucidate the steps followed in Euler's theorem to find the modulus of the positive number. Apply Euler's theorem to find a number 'a' between 0 and 9 such that 'a' is congruent to 9^{101} modulo 14. (5 Marks)	10
2.	a) Compute the following by applying Fermat's Little theorem (5 Marks) (i)29^{25} mod 11 (ii)2^{35} mod 7 b) Consider P=13 and Q=23 then calculate and verify Euler's theorem. (5 Marks)	10
3.	a) Given the ciphertext and key below, find the plaintext if the Playfair cipher was used. (6 Marks) Ciphertext = morzcdwxprkygo Key = network b) Given Plaintext=Cryptography and Network Security, Key=VELLORE. Compute the ciphertext using Vigenere cipher technique where the set of characters are the alphabets. (4 Marks)	10

4.	a) Compute the output. If the the input of the S-box of DES is 100011. (4 Marks)  b) To compute encrypted data in S-DES the 10-bit key is given as 1010000010, find the sub keys (k1 andk2) to complete encryption? Here the permutations are P10= {3,5,2,7,4,10,1,9,8,6} and P8= {6,3,7,4,8,5,10,9} (6 Marks)	10
5.	A hacker obtained the password of an employee in your organization. The hacker accomplished this by claiming to be a support desk executive. How would you classify this attack? Describe the different types of attacks that come under within this category, with examples.	10