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

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

SLOT: E1 + TE1

CONTINUOUS ASSESSMENT TEST - I
WINTER SEMESTER 2024-2025

| | |
|---|---|
| Programme Name & Branch | : B.Tech & Computer Science and Engineering |
| Course Code and Course Name | : BCSE309L & Cryptography and Network Security |
| Faculty Name(s) | : Applicable to all |
| Class Number(s) | : Applicable to all |
| Date of Examination | : 31.01.25 |
| 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)
- CO1: To know the fundamental mathematical concepts related to security.
- CO2: To understand concept of various cryptographic techniques.

| Q. No | Question | M | CO | BL |
|---|---|---|---|---|
| 1. | a) Find 15^276 mod 97 using the method of fast modular exponentiation. Also, determine the result step-by-step and explain how the exponentiation and modular operations are applied iteratively. | 7 | CO1 | BL3 |
| | b) Compute ϕ (8820) using the property of Euler's Totient Function. Describe your steps clearly. | 3 | CO1 | BL3 |
| 2. | a) Solve the following congruent equations and find the X value using Chinese Remainder Theorem.<br>$X \equiv 5 \pmod{18}$<br>$X \equiv 3 \pmod{11}$<br>$X \equiv 0 \pmod{5}$ | 7 | CO2 | BL3 |
| | b) Write the algorithm steps of Miller-Robin algorithm. | 3 | CO2 | BL3 |
| 3. | Explain in detail the state and key initialization, initial state permutation, key stream generation and encryption process of RC4 algorithm with diagram and algorithm steps. | 10 | CO2 | BL2 |
| 4. | Construct the shift row matrix from the given sub byte matrix (given in Hex) in AES algorithm. Also, find X and Y values in the given output of mix column matrix using the given fixed matrix and determined shift row matrix (Hint: when finding X & Y values, consider fixed matrix as first matrix and shift row matrix as second matrix)<br>$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$ Fixed matrix<br>$\begin{bmatrix} 63 & 09 & cd & ba \\ 53 & d0 & 30 & 20 \\ 72 & ca & 94 & 6d \\ 04 & 84 & 85 & 25 \end{bmatrix}$ Sub byte matrix<br>$\begin{bmatrix} X & - & - & - \\ Y & - & - & - \\ - & - & - & - \\ - & - & - & - \end{bmatrix}$ Mix column matrix | 10 | CO2 | BL3 |
| 5. | Describe the operation of S-Box group and S-Box rule. Also, Find the output of S box group from the output of the whitener (XOR) operation of DES function using given S-Box tables. The output of the whitener is 48-bit values, which serves as the input to the S-boxes. The 48-bit values are given as follows:<br>110011101010011001110110000011111000101011011110 | 10 | CO2 | BL4 |