VIT
Vellore Institute of Technology

Continuous Assessment Test – I

Programme Name & Branch: B. Tech (CSE)

Course Name & Code: Cyber Security (CSE4003)

Class Number:All **Slot:** A2/TA2

Faculty Name:All **Exam Duration:** 90 mins

Maximum Marks: 50

General instruction(s): **ANSWER ALL FIVE QUESTIONS.** **(5 x 10 = 50 marks)**

1. Prove that if p is prime, then ø $(P^i) = P^i P^{ii}$. Also, Show that if gcd $(m, n) = 1$ then ø (mn) = ø (m) ø (n). Using this property and the property developed using Euler totient function determine the value of ø (n) for 41, 27, 231 and 440.

2. Encrypt the message "meet me at the usual place at ten rather than eight oclock" using the Hill cipher with the key $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$. Show your calculations and the result. Also reveal the calculations for the corresponding decryption of the cipher text to recover the original plaintext.

3. Show the steps involved to derive the coefficient values $x_i = x_{i-2} - q_i x_{i-1}$ and $y_i = y_{i-2} - q_i y_{i-1}$ using extended Euclidean algorithm and find the integer coefficients x and y of gcd (210, 45) such that [ax + by = d], [d = gcd (a, b)].

4. Compare AES to DES and delineate the four transformation stages in AES round's with neat diagram and suitable illustration.

5. Compute the output of the Mix Columns transformation for the following sequence of input bytes "67 89 AB CD" based on Rijndael approach.

+126- x6

10 11 12 13
A B C D E
60x10=160
x