VIT

Vellore Institute of Technology

Continuous Assessment Test – I

Programme Name & Branch: B.Tech. ECE

Course Name & Code: Cryptography & Network Security BECE411L

Slot:E2 **Exam Duration: 90 mins** **Maximum Marks: 50**

General instruction(s):

a. Provide appropriate illustration, wherever necessary.
b. Assume relevant address, wherever necessary.

S.No.	Question	Marks
1.	Using the Affine cipher, convert plain text to cipher text and cypher text to plain text. Plaintext : Networking Keys : H, D Note : Inverse values to be computed using Extended Euclidian Algorithm	**10**
2.	Using Two square vertical and horizontal Play-fair cipher convert the following plain text into cipher text, comment on the results obtained. Plaintext : Technical Education Keys : "check "; "Tools" Note: Assuming that R/S as a single letter.	**10**
3.	Solve the system below using the Chinese Reminder theorem. $X \equiv 4 \bmod 11$; $X \equiv 5 \bmod 7$; $X \equiv 6 \bmod 13$ Note : Inverse values to be computed using Extended Euclidian Algorithm	**10**
4.	Encrypt the message "**Therecomesadayofthefinaljudgement**" using simple column transposition cipher technique with number of rounds is three, given that keyword is **ANALOG**. Note : Assume dummy letters as "X" ; Highest priority must be given to MSB bit for the key	**10**
5.	Two nodes are linked using point-to-point communication, utilizing physical addresses U and V, and running applications DNS (53) and Telnet (23). Suppose the client requests for a temporary port number and the server replies with a permanent port number. Suppose that a malicious user, S, is disrupted by active attacks.Draw an internetwork diagram and analyze the outcome by considering various types of attacks.	**10**