VEER SURENDRA SAI UNIVERSITY OF TECHNOLOGY (VSSUT), ODISHA

Odd Mid Semester Examination for Academic Session 2025-26

COURSE NAME: B.Tech SEMESTER: 5th

BRANCH NAME: Computer Science and Engineering

SUBJECT NAME: Cryptographic Foundation and Network Security

FULL MARKS: **30** TIME: **90 Minutes**

Answer **All** Questions.

The figures in the right hand margin indicate Marks. *Symbols carry usual meaning.*

Q1. Answer all Questions. **[2 × 3]**

a) Differentiate between "Confidentiality'' and "Non-repudiation''? - CO1

b) Distinguish between Stream Ciphers and Block Ciphers? - CO2

c) What are the criteria for Cryptographic Hash Function? - CO3

Q2. **[8]**

(a) What is the difference between Substitution Cipher and Transposition Cipher? - CO1

Discuss Multiplicative and Playfair Ciphers?

(b Write the process to find Multiplicative Inverse of a number using Extended Euclidean Algorithm (EEA). Find all the additive and multiplicative inverse pairs in $\mathbf{Z_{10}}$? Find GCD of 161 and 28 using EEA?

OR

(a)Use the Affine cipher to decrypt the message "ZEBBW" with key pair (7,2) in modulo 26. - CO1

(b) What is OSI security architecture? What are the three different components of Information Security? Discuss in detail?

Q3. **[8]**

(a)Discuss in detail DES structure and working? Discuss the analysis of DES? - CO2

(b) What are the different Data Units used in AES? Explain the architecture of AES? Explain the Key Expansion algorithm used in AES?

OR

(a)Find the particular and general solutions to the equation $21x + 14y = 35$? - CO2

(b) Describe the idea of the Merkle-Damgard scheme and why this idea is so important for the design of a cryptographic hash function.

Q4. **[8]**

Define the RSA digital signature scheme and compare it to the RSA cryptosystem. - CO3

Distinguish between message integrity and message authentication.

Compare and contrast attacks on digital signatures with attacks on cryptosystems.

OR

What is SHA-512? Discuss the process of Message Digest Creation? What is the number of padding bits if the length of the original message is 2590 bits? We apply the Majority function on buffers A, B, and C in SHA-512. If the leftmost hexadecimal digits of these buffers are 0x7, 0xA, and 0xE, respectively, what is the leftmost digit of the result? - CO3

****Best of Luck****