Graphic Era
HILL UNIVERSITY
Established by an Act of the State Legislature of Uttarakhand (Adhiniyam Sankhya 12 of 2011)
University under section 2(f) of UGC Act, 1956

End Term (Even) Semester Examination May-June 2025

Roll no.....

Name of the Program and semester: B. Tech CSE
Name of the Course: Network and System Security
Course Code: TCS 619

Time: 3hour Maximum Marks: 100

Note:

(i) All the questions are compulsory.
(ii) Answer any two sub questions from a, b and c in each main question.
(iii) Total marks for each question is 20 (twenty).
(iv) Each sub-question carries 10 marks.

Q1. (2X10=20 Marks)

a. Explain with a diagram model of network security. (CO1)
b. Perform encryption and decryption using Caesar cipher for the given plain text **"WELCOME TO HILL UNIVERSITY".** (CO1)
c. Explain why active attacks are generally considered more dangerous to network security than passive attacks, Describe each active attack with example. (CO1)

Q2. (2X10=20 Marks)

a. Given Alice private key=6, Bob private key = 15, primitive root = 5. Determine the shared secret for Bob and Alice using Diffie-Hellman key exchange. (CO4)
b. Explain the fundamental steps involved in a single round of the AES encryption process, detailing the transformations applied to the state matrix, including SubBytes, ShiftRows, MixColumns, and AddRoundKey, and how these steps contribute to the overall security and diffusion properties of the Algorithm. (CO2)
c. Describe CFB and Counter mode block operations with a diagram. (CO2)

Q3. (2X10=20 Marks)

a. Describe the Kerberos Version 4 authentication dialogue. (CO4)
b. Explain the SSL handshake protocol. (CO3)
c. Describe the X.509 certificate format with a diagram. (CO3)

Q4. (2X10=20 Marks)

a. Describe the primary techniques employed by PGP to achieve confidentiality (encryption), integrity (message authentication), and authenticity (digital signatures) of data. (CO5)
b. Explain the IEEE 802.11i Phases of Operation with a diagram. (CO5)
c. Differentiate between Transport mode and Tunnel mode in IP security. (CO5)

Q5. (2X10=20 Marks)

a. Describe the different types of firewalls with example for each. (CO6)
b. Explain the different password selection strategies used for password management. (CO6)
c. Differentiate between virus and worms. (CO6)