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 (Odd) Semester Examination November 2025

Roll no............................

Name of the Course and semester: M.Tech. and III
Name of the Paper: Cryptography and Network Security
Paper Code: MCS 142
Time: 3 hour 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. Analyze how the CIA Triad helps in designing a robust cybersecurity framework. Illustrate its role in preventing attacks such as data tampering, unauthorized access, and denial of service.
(CO I)

b. Compare and contrast symmetric and asymmetric key cryptography in terms of security, computational efficiency, and key distribution. Discuss with examples of real-world applications for each type. (CO I)

c. (i) Eva have received a message "FRGHGDPQ" from Bob. Eva knows that Bob have encrypted the message using the Caeser cipher with key = 3 help Eva to retrieve the original message. (CO I)

(ii) Encrypt the message "Secure network" with Caeser cipher using key value 5.

Q2. (2X10=20 Marks)

a. (i) Use Playfair cipher to encrypt the message "Computer", with the key "Direct".
(CO II)

(ii) Compare substitution cipher and transposition cipher.

b. Discuss the following in context of AES. Add key, shift row and mix column. (CO II)

c. Discuss various block cipher modes of operations along with pros and cons associated with them. (CO II)

Q3. (2X10=20 Marks)

a. Discuss the cryptographic hash function MD-5 in detail. (CO III)

b. Discuss the components of public key cryptosystem. Also explain RSA cryptosystem in detail. (CO III)

c. Analyze how firewalls and Intrusion Detection Systems (IDS) complement each other in protecting an enterprise network. Discuss their placement, working principles, and limitations. (CO III)

Q4. (2X10=20 Marks)

a. Discuss the services provided by the firewall along with its type and limitations. (CO III)

b. Discuss the services provided by IPsec along with its architecture in detail. (CO IV)

c. Categorize the web security attacks along with their countermeasures. (CO IV)

Q5. (2X10=20 Marks)

a. A user initiates a TLS handshake with a web server. Illustrate the complete sequence of messages exchanged with a labeled diagram. (CO IV)

b. Describe the phases of ethical hacking. For each phase, mention one tool or technique used and its purpose. (CO IV)

c. Compare black-box, white-box, and gray-box approaches in ethical hacking. Analyze their advantages, limitations, and suitability for different penetration testing environments. (CO IV)