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. 22941038

Name of the Course and semester: B.Tech CSE VII CORE, AI/ML
Name of the Paper: Cryptography and Network Security
Paper Code: TIT 704
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. Define Steganography? Describe various techniques used in Steganography. CO1
b. Illustrate the rules to perform encryption using play fair cipher and encrypt 'snowshooos' using 'monarchy' I and J count as one letter and x is the filler letter. CO1
c. Compare transposition cipher and substitution cipher. Apply two stage transpositions Cipher on the "treat diagrams as single units" using the keyword "sequence". CO1

Q2. (2X10=20 Marks)

d. How do you convert a block cipher into a stream cipher by using the Cipher Feedback (CFB) mode? Explain. CO2
e. Discuss the Structure of Simplified DES (S-DES) and Cipher and Reverse Cipher. CO2
f. What do you mean by AES? Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process. CO2

Q3. (2X10=20 Marks)

a. Describe the steps in finding the message digest using SHA-512 algorithm. What is the order of finding two messages having the same message digest? CO4
b. How is GCD calculated with Euclid's algorithm? Calculate the GCD of (270,192) CO3
c. In a public-key system using RSA, you intercept the cipher text C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M? CO3

Q4. (2X10=20 Marks)

a. What is Digital Signature? Explain how it is created at the sender end and retrieved at receiver end .differentiate digital signature from digital certificate. CO5
b. Write about PGP cryptographic functions for authentication only, confidentiality only and both confidentiality and authentication. CO5
c. Explain briefly about the architecture and certification mechanisms in Kerberos and X.509. CO4

Q5. (2X10=20 Marks)

a. Discuss transport mode and tunnel mode authentication in IP? Describe how ESP is applied to both these modes.CO5
b. Explain the role of encryption in wireless network security. How do different encryption standards impact the security of a WLAN? CO6
c. Explain how firewalls help in the establishing a security framework for an organization.CO6