Graphic Era HILL UNIVERSITY

Established by an Act of the State Legislature of Uttarakhand (Ajitesham Sanskrit 13 of 2011)
University under section 2(f) of UGC Act, 1956

End Term (Odd) Semester Examination December 2025

Roll no. 2.3.6.7.1.0.2.4

Name of the Course: B. Tech. CSE
Semester: III[rd]
Name of the Paper: Introduction to Cryptography
Paper Code: TCS-392

Time: 3 hours **Maximum Marks: 100**

Note:

(i) All 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. (2×10 = 20Marks)

a. With the help of a neat and clearly labelled diagram, illustrate the OSI Security Architecture and explain the role of each component in detail. [CO1]

b. Critically examine the strengths and weaknesses of Classical Ciphers against modern cryptanalysis techniques . [CO1]

c. Explain the principles of symmetric encryption with suitable block diagram. [CO1]

Q2. (2×10 = 20Marks)

a. Perform frequency analysis on the ciphertext "ZOLSSP" and attempt its decryption using a monoalphabetic substitution technique. Show all intermediate steps.[CO2]

b. Encrypt the plaintext "1101 0110" using a single round of simplified DES (S-DES). Show all steps. [CO2]

c. Discuss the necessity of Random Numbers and Pseudorandom Numbers in cryptographic systems. Provide suitable real-world applications for each. [CO2]

Q3. (2×10 = 20Marks)

a. Explain the importance of mathematical background in cryptography. Discuss with reference to prime numbers and modular arithmetic. [CO3]

b. A company aims to reduce the frequency of rekeying operations for secure communication channels. Recommend an appropriate key distribution mechanism and justify your selection [CO3]

c. Critically examine the role of message authentication codes (MACs) in ensuring integrity. [CO3]

Graphic Era
HILL UNIVERSITY

End Term (Odd) Semester Examination December 2025

Q4. (2×10 = 20Marks)

a. Given p=11, Choose a public exponent e=7,

(a) Compute the public key (n,e)and the private exponent d.

(b) Encrypt the message M=8.

(c) Decrypt the resulting ciphertext to recover M. [CO4]

b. Compare Symmetric Encryption, Asymmetric Encryption, and Hybrid Encryption. Recommend an optimal strategy for secure mobile banking communication and justify your choice. [CO4]

c. Discuss the challenges associated with Key Distribution in large-scale networks and suggest practical solutions to overcome these issues. [CO4]

Q5. (2×10 = 20Marks)

a. Discuss in detail the ethical and legal aspects of cybercrime, focusing on Intellectual Property Rights and Privacy. [CO5]

b. A company's network is under frequent intrusion attempts. Design a basic intrusion detection strategy for them. [CO5]

c. Propose a complete Network Plan for an organization facing frequent malware infections. Discuss measures at OS level, network level, application level, and user-training level. [CO5]

+++++++