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

Mid Term (Odd) Semester Examination October 2024

Roll no.....

Name of the Course and semester: B.Tech/7th Semester
Name of the Paper: Cryptography and Network Security
Paper Code: TIT 704
Time: 1.5 hour Maximum Marks: 50

Note:
(i) Answer all the questions by choosing any one of the sub questions
(ii) Each question carries 10 marks.

Q1. (10 Marks)

a. Explain the various types of security attacks. How do they differ from one another in terms of their objectives and techniques? CO-1

OR

b. Discuss the concept of security services. Illustrate with examples how confidentiality, integrity, and availability are maintained in a secure system. CO-1

Q2. (10 Marks)

a. Define and differentiate between security mechanisms and services. Provide examples to explain how security mechanisms support security services.? CO-1

OR

b. If a system uses a 128-bit block cipher, and you have a 512-bit message, how many blocks are needed to encrypt the entire message using block cipher encryption? Show the calculations. CO-2

Q3. (10 Marks)

a. For a stream cipher, the key length is 10 bits, and the plaintext is "HELLO" represented in binary. If the key stream is "0110100110", perform the XOR operation and show the resulting ciphertext. CO-2

OR

b. You are using a substitution cipher with a key that shifts each letter by 4 positions in the alphabet. If the ciphertext is "XLI PMR XLIEX", what is the original plaintext? Show the decryption process. CO- 1

Q4. (10 Marks)

a. Define and explain Shannon's theory of confusion and diffusion. How are these concepts applied in modern block cipher algorithms like AES?

OR

b. What is reinforcement learning, and how does it differ from supervised learning? Explain the concepts of reward, policy, and value function in reinforcement learning, and discuss how an agent can learn optimal behavior through interaction with its environment. CO-1

Q5. (10 Marks)

a. Explain the Advanced Encryption Standard (AES) algorithm, focusing on its structure and key operations (e.g., SubBytes, ShiftRows, MixColumns, and AddRoundKey). CO-2

OR

b. Define and differentiate between true random number generators (TRNGs) and pseudo-random number generators (PRNGs). What are the security implications of using PRNGs in cryptographic systems? CO-2