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. 22 92104

Name of the Course: BCA semester: V
Name of the Paper: Cryptography
Paper Code: TBC - 504
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. Define Cryptography. List the several principles of Security. [C01]

OR

b. Explain CIA Triad. [C01]

Q2. (10 Marks)

a. Differentiate between Active attacks and Passive attacks. [C02]

OR

b. Explain how the Caesar cipher works. Provide a step-by-step example by encrypting the plaintext "HELLO WORLD" with a shift of 3. Then, decrypt the resulting cipher text back to plaintext. [C03]

Q3. (10 Marks)

a. what is Block cipher and how it is Different from Stream Cipher. [C03]

OR

b. Discuss Feistel Design and it's Features. [C03]

Q4. (10 Marks)

a. Explain Symmetric Key Ciphers and some of the Categories of it. [C03]

OR

b. Given the keyword "SECURITY", perform the following tasks:

1. Construct the 5x5 Playfair grid.
2. Encrypt the plaintext message "MEET ME AT DAWN" using the constructed grid. Make sure to handle repeated letters and padding appropriately. [C03]

Q5. (10 Marks)

a. Differentiate Between AES and DES. [C03]

OR

b. Explain the Mechanism of DES. [C03]