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: Bachelor of Technology and 3rd Semester
Name of the Paper: Introduction to Cryptography
Paper Code: TCS-392
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.
(iii) Please specify COs against each question.

Q1. (10 Marks) **CO1**

a. Consider an automated cash deposit machine in which users provide a card or an account number to deposit cash. Give examples of confidentiality, integrity, and availability requirements associated with the system, and, in each case, indicate the degree of importance of the requirement.

List and briefly define categories of passive and active security attacks.

OR

b. Using Play Fair cipher encrypt the plaintext “Why, don’t you?” and “Come to the window.” The keyword to fill the diagraph is “KEYWORD”. Perform decryption also.

Q2. (10 Marks) **CO1, CO2**

a. Decrypt the following ciphertext, which was encrypted using a Caesar cipher with a shift of 5: "YMJVZNY."
Why is the Caesar cipher substitution technique vulnerable to a brute-force cryptanalysis?

OR

b. What is the purpose of the compression permutation (P8) in S-DES? How does it reduce the 10-bit shifted key to an 8-bit subkey?

Provide an example of applying the P8 permutation on a shifted key to obtain the first subkey (K1) in S-DES.

Q3. (10 Marks) **CO1, CO2**

a. Explain how a brute-force attack works. Why is key length an important factor in defending against brute-force attacks?
What is steganography? How does it differ from cryptography in terms of data protection?

OR

b. Explain the concept of diffusion and confusion in the context of block ciphers.
How many padding bits must be added to a message of 137 characters if 8-bit ASCII is used for encoding and the block cipher accepts blocks of 256 bits?

Mid Term (Odd) Semester Examination October 2024

Q4. (10 Marks) **CO2**

a. Explain, with the help of diagram, Feistel Cipher from first thought to final design. Explain the working of the RC4 stream cipher. What are its advantages and limitations?

OR

b. Explain the structure and working of the Data Encryption Standard (DES) algorithm. How does it use the Feistel structure and its function, to perform encryption and decryption?

Q5. (10 Marks) **CO2**

a. What is Double DES? How does it improve upon the security of standard DES, and what are the vulnerabilities it still faces?

OR

b. What is the difference between random and pseudorandom numbers in cryptography? Why are pseudorandom numbers important in cryptographic algorithms?