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

Term Evaluation (Odd) Semester Examination September 2025

Roll no. 2294038

Name of the Course: B.Tech (CSE)
Semester: 7th
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) **CO1**

a. Explain about Digital Signature Standard with the help of a neat diagram. Also state how it is different than RSA approach?

OR

b. Compare and contrast the roles of confusion and diffusion in enhancing security in block ciphers.

Q2. (10 Marks) **CO2**

a. Calculate the value of Private and public key pair using RSA algorithm, given that p=7; q=11. Also show the Encryption and decryption steps using the plain text value of M=5. Write all the steps involved.

OR

b. What do you mean by Authentication? How it is different from Integrity. How Authentication works in Federated Identity Management.

Q3. (10 Marks) **CO2**

a. Compare the security of Single DES and Double DES. Why is Double DES not significantly more secure than DES?

OR

b. Define the Playfair Cipher and list the basic rules used for encrypting a pair of letters. Explain how the 5×5 key matrix is constructed in a Playfair Cipher using a given keyword.

Q4. (10 Marks) **CO1**

a. Design a simple symmetric encryption model using substitution and transposition techniques. Explain how your model can protect message confidentiality.

OR

b. Illustrate how security mechanisms such as encryption, authentication, and digital signatures can be used to enforce security policies.

Q5. (10 Marks) **CO2**

a. A multinational company needs to secure its communication between employees working in different countries. When employees within the same office share confidential files with each other daily, the company decides to use a fast encryption method that requires less computational power. However, when files are exchanged between offices across the world, the company is worried about securely sharing the secret key over the internet. Therefore, they decide to use a method where each employee has a public key and a private key.

- (a) Identify which scenario uses symmetric cryptography and which uses asymmetric cryptography.
- (b) Justify why each method is appropriate for its scenario.

OR

Term Evaluation (Odd) Semester Examination September 2025

b. Explain the following terms.

1. Intrusion detection system
2. Gateway
3. Distributed Denial of Service Attack
4. Rule based Firewall