



Term Evaluation (ODD) Semester Examination Sep 2025

Roll no.....

Name of the Course and semester: MTech CSE , I st

Name of the Paper: **Cryptography and Network Security**

Paper Code: MCS 142

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. Using **Play Fair** cipher Encrypt the plaintext "**ATTACK AT TWO**" The keyword is "**PLAYFAIR**". Perform Decryption also

OR

- b. Encrypt and decrypt the following using the **Vigenère cipher (modulo 26 arithmetic)**:

Given Plaintext: ATTACK AT TWO Keyword: GRAPH

Q2. (10 Marks) : CO2

- a. Calculate the value of Private and public key pair using RSA algorithm, given that $p=13$; $q=17$. Also show the Encryption and decryption steps using the plain text value of $M=10$. Write all the steps involved.

OR

- b. Explain how plain text is converted into Cipher text in DES block symmetric algorithm. Explain how the round keys are calculated.

Q3. (10 Marks) : CO1, CO2

- a. Explain with suitable diagram the Key distribution scenario in Symmetric key distribution using symmetric encryption.

OR

- b. Explain the process of generating and verifying a digital signature. How does public key cryptography ensure authentication and integrity in this process?

Q4. (10 Marks) : CO2

- a. What do you mean by Block Cipher Mode of Operation in Cryptography? Explain about any two popular block cipher modes with suitable examples.

OR



Term Evaluation (ODD) Semester Examination Sep 2025

- b. What do you mean by Message Authentication? Explain how confidentiality and authentication is achieved in Message authentication using suitable block diagrams.

Q5.

(10 Marks) : CO2

- a. Illustrate with a diagram the lifecycle of certificate management in a Public Key Infrastructure (PKI), including certificate issuance, renewal, revocation, and trust establishment.

OR

- b. Calculate the values of sub key K1 and K2 using SDES algorithm , given the value of main key $K = 1111010101$, $P10 = \{3,5,2,7,4,10, 1,9,8,6\}$ and $P8 = \{6,3,7,4,8,5,10, 9\}$