R22 Regulation Subject code: 4E7EB

# TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

(Autonomous, Accredited by NAAC with 'A+' Grade)

## B.Tech VII Semester Regular Examinations, November 2025

## NETWORK SECURITY AND CRYPTOGRAPHY

*(CSE)*

***Maximum Marks: 60*** Date: 26.11.2025 Duration: 3 hours

**Note:**
**1.This question paper contains two parts A and B.**
**2. Part A is compulsory which carries 10 marks. Answer all questions in Part A.**
**3. Part B consists of 5 Units. Answer any one full question from each unit.**
**4. Each question carries 10 marks and may have a, b, c, d as sub questions.**

Part-A

| All the following questions carry equal marks (10X1M=10 Marks) | | Marks | CO | BloomTx |
|---|---|---|---|---|
| 1.a) | Specify the four categories of security threats. | 1M | 1 | 2 |
| b) | What are active and passive attacks? | 1M | 1 | 1 |
| c) | Define Diffusion & Confusion. | 1M | 2 | 1 |
| d) | What are the criteria for design of block ciphers. | 1M | 2 | 1 |
| e) | List the schemes for the distribution of public keys. | 1M | 3 | 2 |
| f) | What is the difference between weak and strong collision resistance? | 1M | 3 | 2 |
| g) | What is the need of IP Security? | 1M | 4 | 1 |
| h) | What are the fields available in AH header? | 1M | 4 | 1 |
| i) | List the design goals of firewalls. | 1M | 5 | 3 |
| j) | What is dual signature? What it is purpose? | 1M | 5 | 1 |

Part-B

| Answer All the following questions. (5X10M=50Marks) | | Marks | CO | BloomTx |
|---|---|---|---|---|
| 2 | a) Discuss with neat sketch a network security model.<br>b) Explain in detail about various types of attacks. | 5M<br>5M | 1 | 3<br>2 |
| | OR | | | |
| 3 | a) Explain various transposition ciphers in detail.<br>b) Explain about play fair cipher algorithm and encrypt the message "MONARCHY" . | 5M<br>5M | 1 | 2<br>2 |
| 4 | a) Write short notes on block cipher modes of operation.<br>b) Explain the process of RSA algorithm with example. | 5M<br>5M | 2 | 2<br>3 |
| | OR | | | |
| 5 | a) Explain ECC - Diffie Hellman key Exchange method is used for key generation with the help of an example.<br>b) Explain about key management of public key encryption in detail. | 6M<br>4M | 2 | 3<br>3 |
| 6 | a) Explain the classification of authentication functions in detail.<br>b) Describe the MD5 message digest algorithm with necessary block diagrams. | 4M<br>6M | 3 | 3<br>2 |

| | | | | |
|---|---|---|---|---|
| | OR | | | |
| 7 | a) Explain in detail about properties of Hash Functions.<br>b) Discuss how Secure Hash Algorithm is used for message authentication. | 5M<br>5M | 3 | 2<br>3 |
| 8 | a) What is a security association? Explain its role in key exchange.<br>b) Explain in detail the operation of Internet Key Exchange with an example. | 4M<br>6M | 4 | 3<br>4 |
| | OR | | | |
| 9 | a) Explain the architecture of IP Security.<br>b) Write short notes on authentication header and ESP. | 5M<br>5M | 4 | 3<br>3 |
| 10 | a) Explain in detail the operation of Secure Socket Layer in detail.<br>b) Write brief note on E-mail Security. | 5M<br>5M | 5 | 2<br>2 |
| | OR | | | |
| 11 | a) Explain about operational details of PGP.<br>b) Write brief note on Web Security. | 5M<br>5M | 5 | 2<br>3 |