



R22 Regulation

Subject code:4P6HA

# TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

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

**B.Tech VI Semester Supplementary Examinations, November 2025**

## INFORMATION SECURITY (CSE(DS))

Maximum Marks: 60

Date:13.11.2025

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	Bloom Tx
1.a)	Differentiate between Active attacks and Passive Attacks.	1M	1	II
b)	Compare plain text and cipher text.	1M	1	II
c)	Write the disadvantages of double DES.	1M	2	I
d)	How are the public and private keys in asymmetric key cryptography generated?	1M	2	I
e)	What properties must a hash function have to be useful for message authentication?	1M	3	II
f)	What role do cryptographic hash functions play in password storage?	1M	3	I
g)	Write the four SSL Protocols.	1M	4	I
h)	List the transfer encodings used by S/MIME.	1M	4	I
i)	State the benefits of IP security.	1M	5	I
j)	What are the limitations of firewalls?	1M	5	I

### Part-B

Answer All the following questions. (5X10M=50Marks)		Marks	CO	Bloom Tx
2	Give an account of the OSI Security Architecture as defined by ITU-T X.800. Illustrate how its components interrelate to provide comprehensive network security.	10M	1	IV
OR				
3	Compare and contrast the Caesar cipher, Playfair cipher, and Hill cipher in terms of their encryption methods, key structures, security levels and practical applications.	10M	1	IV
4	Explain which four tasks are performed in each round of AES Cipher? Also write a note on the Key Expansion process in AES.	10M	2	III
OR				
5	Discuss the Diffie Hellman Key Exchange algorithm with illustration.	10M	2	III
6	Illustrate the Secure Hash algorithm in detail.	10M	3	IV
OR				

7	Describe the HMAC algorithm and comment on the security of HMAC. Also write a note on the signing and verification in Digital Signature Algorithm.	10M	3	III
8	a) What is the need for security services at transport layer of Internet Protocol? b) Explain the four protocols defined by Secure Socket Layer.	5M 5M	4	III
	OR			
9	Present the two prominent standards used to address the confidentiality, integrity and authenticity of email.	10M	4	III
10	Explain IP Security protocols in detail.	10M	5	III
	OR			
11	a) Compare and contrast anomaly-based and signature-based intrusion detection methods. b) Write a note on the common password cracking techniques.	6M 4M	5	IV