R22 Regulation *Subject code:4P6HA*

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

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

B.Tech VI Semester Regular/Supplementary Examinations, April 2026

INFORMATION SECURITY

(CSE(DS))

Maximum Marks: 60 Date:21.04.2026 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)	Define threat and attack.	1M	CO1	L1
b)	Define Substitution Cipher	1M	CO1	L1
c)	What is Cipher Block Chaining Mode.	1M	CO2	L1
d)	What is meant by the Diffie-Hellman key exchange?	1M	CO2	L2
e)	What is data authentication code?	1M	CO3	L1
f)	List the properties of hashing functions?	1M	CO3	L1
g)	What is e-mail security?	1M	CO4	L2
h)	What are the requirements of web security?	1M	CO4	L2
i)	Illustrate the services provided by IPSec.	1M	CO5	L2
j)	What is meant by intrusion detection system?	1M	CO5	L1

Part-B

Answer All the following questions. (5X10M=50Marks)		Marks	CO	Bloom Tx
2	a) Explain the operations, requirements, components of Network security model. b) Briefly explain the security services and mechanisms defined under X800 standard.	5M 5M	CO1 CO1	L2 L2
	OR			
3	a) Discuss any four Substitution Technique and list their merits and demerits. b) Use Caesar cipher with key =15 to encrypt the message "Hello".	5M 5M	CO1 CO1	L4 L3
4	a) Explain the Modes of Operations of Block Cipher. b) Write about the round functions and key expansion of DES algorithm.	5M 5M	CO2 CO2	L2 L4
	OR			
5	a) Discuss about the Principles of public key cryptosystems. b) Find the secret key shared between user A and user B using Diffie - Hellman algorithm for the variables Q=353, α (primitive root)=3, XA=45, XB=50.	5M 5M	CO2 CO2	L2 L3

6	a) Explain message digest generation and round function of SHA-512. b) What is digital signature? Explain the approaches for digital signature based on public key encryption.	5M 5M	CO3 CO3	L4 L2
	OR			
7	a) Formulate what are the requirements of Kerberos? Explain about Kerberos version. b) Give a brief note on X.509 authentication services.	5M 5M	CO3 CO3	L2 L2
8	a) Explain about SSL Handshake protocol. b) Explain Secure Electronic Transaction with neat diagram.	5M 5M	CO4 CO4	L4 L2
	OR			
9	a) What is PGP? Examine how authentication and confidentiality is maintained in PGP. b) Explain in detail S/MIME certification processing.	5M 5M	CO4 CO4	L4 L2
10	a) Draw IPSec Authentication Header and write short notes on each element of the Header. b) Discuss about Encapsulating Security Payload.	5M 5M	CO5 CO5	L2 L2
	OR			
11	a) What is IDS? Explain the profile-based IDS? b) Write about manual and automated key management of IP Security.	5M 5M	CO5 CO5	L2 L2