R22 Regulation *Subject code:4E7EB*

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

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

B.Tech VII Semester Regular/Supplementary Examinations, October 2026

NETWORK SECURITY AND CRYPTOGRAPHY

(CSE)

Maximum Marks: 60 Date: 28.10.2026 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	BTL
1.a)	Define a security mechanism.	1M	1	L1
b)	Distinguish between plaintext and ciphertext.	1M	1	L2
c)	What is a block cipher?	1M	2	L1
d)	State the purpose of Diffie-Hellman key exchange.	1M	2	L1
e)	What is Birthday attack? Explain.	1M	3	L1
f)	Write about the technical deficiencies of Kerberos v4.	1M	3	L2
g)	Discuss the benefits of IP security.	1M	4	L2
h)	Differentiate between Transport Mode and Tunnel Mode in IPsec.	1M	4	L2
i)	What are the key web security threats at the Network/Transport vs. Application layers?	1M	5	L2
j)	What is Secure Electronic Transaction?	1M	5	L1

Part-B

Answer All the following questions. (5X10M=50Marks)		Marks	CO	BTL
2	a) Explain the principles of security and different types of security attacks. b) Describe the model for network security and identify its major elements	5M 5M	1	L2
	OR			
3	a) Explain encryption and decryption using a suitable cryptographic model. b) Compare symmetric and asymmetric key cryptography.	5M 5M	1	L3
4	a) Explain the principles of public key cryptosystems with suitable representation. b) Describe public key distribution and Public Key Infrastructure.	5M 5M	2	L3
	OR			
5	a) Explain the structure of the Feistel Cipher network. b) Demonstrate encryption and decryption for the RSA algorithm parameters: $p = 3, q = 11, e = 7, d = ?, M = 5$.	5M 5M	2	L3

6	a) Differentiate the authentication tied to plain text and cipher text with message authentication codes. b) Explain message digest generation and round function of SHA-512	5M 5M	3	L3
	OR			
7	a) Explain digital signature with ElGamal public key cryptosystem. b) Explain HMAC and its role in message authentication.	5M 5M	3	L3
8	a) Explain the working of the Internet Key Exchange (IKE) protocol. b) Why is it necessary to combine Security Associations? Explain the two main approaches.	5M 5M	4	L2
	OR			
9	a) Explain the architecture of IP security and its major components. b) With a neat diagram, Explain in detail about the IPSec Authentication header.	5M 5M	4	L2
10	Write a short notes on a) Web Security b) SSL	5M 5M	5	L2
	OR			
11	a) Explain pretty Good Privacy in detail. b) Compare S/MIME and Secure Electronic Transaction with respect to their applications.	5M 5M	5	L2