R20 Regulation *Subject code: 3P4HB*

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

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

B.Tech IV Semester Supplementary Examinations, December 2025

INFORMATION SECURITY
(CSE(DS))

Maximum Marks: 70 Date: 20.12.2025 Duration: 3 hours

Note:
1. **This question paper contains two parts A and B.**
2. **Part A is compulsory which carries 20 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 (10X2M=20 Marks)		Marks	CO	BTL
1	Distinguish active and passive attacks?	2M	1	L1
2	Use Playfair cipher and secret key KEYWORD to encrypt plaintext SECRETMESSAGE.	2M	1	L1
3	List out the attacks to RSA.	2M	2	L1
4	Write uses of public key cryptography?	2M	2	L1
5	Write a note on Message Digest.	2M	3	L1
6	What is message authentication?	2M	3	L1
7	What are the roles of the Oakley key determination protocol and ISAKMP in IPSec?	2M	4	L1
8	Why does ESP include a padding field?	2M	4	L1
9	Differentiate SSL and TLS protocols.	2M	5	L1
10	List MIME content types.	2M	5	L1

Part-B

Answer All the following questions. (5X10M=50Marks)		Marks	CO	BTL
11	A) Consider the following: Plaintext: "PROTOCOL" Secret key: "NETWORK" What is the corresponding cipher text using play fair cipher method? B) What is the need for security?	5M 5M	1	L2
	OR			
12	A) Distinguish strong Symmetric and Asymmetric Cryptography? B) Explain about transposition techniques.	5M 5M	1	L2
13	With a neat diagram explain how encryption is done using Blowfish algorithm?	10M	2	L2
	OR			
14	Explain Eliptic Curve Cryptograpghy - Diffie Hellman key Exchange with both keys in detail with an example.	10M	2	L2

15	Discuss the different steps of SHA-512 to generate message digest.	10M	3	L2
	OR			
16	Describe the different approaches to message authentication.	10M	3	L2
17	Explain IP security architecture (a)Authentication Header (b)Encapsulation security payload	 5M 5M	4	L2
	OR			
18	Discriminate the process of combining security association is achieved?	10M	4	L2
19	A) Differentiate between TKIP and CCMP. B) Explain of MIME specification with an example.	5M 5M	5	L2
	OR			
20	Explain the general format of PGP message with an example.	10M	5	L2

4