R20 Regulation *Subject code: 3P4HB*

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

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

B.Tech IV Semester Supplementary Examinations, February 2024

Information Security

(CSE (DATA SCIENCE))

Maximum Marks: 70 Date: 21.02.2024 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 which carries 10M.
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)		CO	Bloom Tx
1	What is Cryptography and Cryptanalysis?	CO1	L1
2	What is steganography?	CO1	L1
3	What is the main difference between DES and AES?	CO2	L1
4	What are the disadvantages of ECC cryptography?	CO2	L1
5	What is the role of compression function in hash function?	CO3	L1
6	How is the security of a MAC function expressed?	CO3	L1
7	Identify the steps involved in SET Transactions.	CO4	L1
8	Point out the services provided by PGP.	CO4	L2
9	Discuss the protocols used to provide IP security.	CO5	L2
10	Give the advantages of intrusion detection system.	CO5	L1
	Part-B		
Answer All the following questions. (5X10M=50Marks)			
11	Discuss the model for network security along with secure access model with suitable diagrams. (10M)	CO1	L2
	OR		
12	Encrypt and decrypt the following messages using Play fair cipher. Use MONARCHY as keyword. Use X as the filler character for spaces if necessary. (10M) A. BALLOON B. CRYPTOGRAPHY C. SECURITY D. SWARAJ IS MY BIRTH RIGHT E. MEET ME TOMORROW	CO1	L3
13	List and explain various block cipher modes of operation with the help of diagrams. (10M)	CO2	L2

	OR		
14	State and explain the principles of public key cryptography. (10M)	CO2	L2
15	A. What is the purpose of digital signature? Explain its properties and requirements. (5M) B. Explain two different MACs based on block ciphers. (5M)	CO3	L2 L2
	OR		
16	A. Explain how authentication is performed in Kerberos. (5M) B. Enumerate the differences between Kerberos Version 4 and 5. (5M)	CO3	L2 L2
17	Elaborate how secure electronic transaction (SET) protocol enables e-transactions. Explain the components involved. (10M)	CO4	L2
	OR		
18	Explain the operational description of PGP. (10M)	CO4	L2
19	A. Draw and discuss the Architecture of IPSec. (5M) B. What is the need to combine Security Associations? Explain basic combinations of Security Associations. (5M)	CO5	L2 L2
	OR		
20	A. Explain the various measures that may be used for intrusion detection. (5M) B. Explain password management. (5M)	CO5	L2 L2