B. TECH. (MINOR) CBCS-2023

B. TECH. (MINOR) Semester-II (Sem-IV Level) CYBER SECURITY : SUMMER : 2025

SUBJECT: NETWORK SECURITY

Day : Friday
Date : 06/06/2025

S-29443-2025

Time : 10:00 AM-01:00 PM
Max. Marks : 60

NB :
1. Assume suitable data, if necessary.
2. Draw neat labelled diagrams WHEREVER necessary.
3. Figures to the right indicate FULL marks for the question.
4. All Questions carry EQUAL marks.
5. All questions are COMPULSORY.

Q. 1	Analyze the importance of network security in protecting against financial fraud and cybercrimes, providing real-world examples of cyber-attacks and their consequences.	(10)
	OR	
Q. 1	Evaluate the strengths and weaknesses of various network security models and how they apply to different types of networks.	(10)
Q. 2	Apply your understanding of the DES encryption algorithm to identify its security vulnerabilities and propose mitigation strategies.	(10)
	OR	
Q. 2	Discuss the RC4 algorithm and illustrate how stream cipher operation differs from block cipher with examples.	(10)
Q. 3	Elaborate the primary challenges in key distribution for public key cryptosystems and explain how these challenges are addressed in large organizations.	(10)
	OR	
Q. 3	Design an RSA key generation process using two prime numbers and compute the corresponding public and private keys.	(10)
Q. 4	Define SSL and TLS, analyze their roles in securing web communications, and discuss their differences in terms of encryption, session management, and performance.	(10)
	OR	
Q. 4	Summarize the security features of IPsec, its role in secure inter-network communication, and analyze the challenges and strategies for its deployment in large-scale enterprises.	(10)
Q. 5	Describe the primary components of a firewall configuration and explain the role of access control lists (ACLs) and filtering rules in securing a network.	(10)
	OR	
Q. 5	Compare and contrast Network-based IDS (NIDS) and Host-based IDS (HIDS) in terms of architecture, detection capabilities, and use cases.	(10)
Q. 6	Assess how the Role-Based Access Control (RBAC) model interacts with password, certificate-based, and biometric authentication methods to enhance network security.	(10)
	OR	
Q. 6	Explain the architecture of the Kerberos authentication protocol and how it prevents replay attacks and ensures secure communication between clients and servers in a network.	(10)

* * * * * *