NIRMA UNIVERSITY

Institute:	Institute of Technology, School of Technology
Name of Programme:	MTech CSE
Course Code:	6CS469ME25
Course Title:	Information and Network Security
Course Type:	Department Elective-I
Year of Introduction:	2025-26

L	T	Practical Component				C
		LPW	PW	W	S	
3	0	2	-	-	-	4

Course Learning Outcomes (CLOs):

At the end of the course, the students will be able to –

1. represent the fundamental network security concepts, and principles (BL2)
2. apply cryptographic techniques to protect data and communications (BL3)
3. analyse common network security threats, vulnerabilities, and attack vectors (BL4)
4. design privacy-preserving models and techniques. (BL6)

Unit	Contents	Teaching Hours (Total 45)
Unit-I	**Security Concepts:** Significance of Information and Network Security, Security attacks, Security services, security mechanisms, Network Security Model	03
Unit-II	**Information Security:** Classic Encryption Techniques, Block Ciphers, Stream Ciphers, DES, Advanced Encryption Standard (AES), Symmetric-key Cryptography, Public Key Cryptography, Hashing, Digital Signature	12
Unit-III	**Network Security:** Firewalls, Secure Socket Layer (SSL) Architecture and working, Transport Level Security (TLS) including HTTPS, HTTPS Use, Secure Shell SSH Protocol, port forwarding, Electronic Mail Security: Email Security Enhancements, Pretty Good Privacy (PGP), S/MIME, IP Security, IPSec, IPSec key management	10
Unit-IV	**Network Threats and Intrusion Detection:** Types of network threats: malware, phishing, DoS, etc.; Attack vectors and methods; understanding firewalls: types, technologies, and configurations, Access control and security policies, Intrusion vs. Extrusion Detection, Categories of Intruders, Hacker Behaviour, Insider Behaviour, Intrusion Techniques, Password Guessing and Capture Notification Alarms, Types of IDS, Intrusion Detection and Prevention Systems (IDPS)	08
Unit-V	**Wireless Security:** Virtual Private Networks (VPNs) and Wireless Network Security, VPN principles and types, VPN protocols, and encryption, Wireless network security threats and solutions, Wireless encryption protocols, Wireless Network Security: IEEE 802.11 Architecture IEEE 802.11 Services Wired Equivalent Privacy (WEP)	06
Unit-VI	**Data privacy concepts**: Social and legal aspects of privacy and privacy regulations, Data localization issues, managing personally identifiable	06

or sensitive information, Data Consent, overview of anonymization models, and privacy-preserving techniques.

Self-Study:
The self-study contents will be declared at the commencement of the semester. Around 10% of the questions will be asked from self-study content.

Suggested Readings/ References:

1. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson
2. D. R. Stinson: Cryptography: Theory and Practice (Discrete Mathematics and Its Applications), CRC Press
3. B. Schneier: Applied cryptography: protocols, algorithms, and source code in C, John Wiley & Sons
4. Bernard Menezes: Network Security and Cryptography, 1st Edition, Cengage Learning
5. B. Forouzan, D. Mukhopadhyay, Cryptography and Network Security, Mc-Graw Hill.

Suggested List of Experiments:

Sr. No.	Name of Experiments/Exercises	Hours
1	Exploration of various tools to perform encryption and decryption	02
2	Implementation of Transposition ciphers (Single as well as Multilevel)	02
3	Cryptography implementation using block-cipher DES	02
4	Asymmetric Cryptography- Creation of RSA key, RSA encryption and decryption	04
5	Simulating the Key Distribution Scenario for Symmetric Key Cryptography using the simulator of your choice	04
6	Use of Snort/Wireshark tool for Network Intrusion Detection Systems to monitor network traffic and analyze attack patterns	04
7	Configure and test VPN connections using technologies such as IPsec or OpenVPN	02
8	Perform vulnerability scans using tools like Nessus or OpenVAS to identify potential security weaknesses	04
9	Set up network security monitoring tools to collect and analyze logs for signs of security incidents.	04
10	Implement machine learning algorithms with built-in privacy-preserving techniques like Differential Privacy (DP) or Federated Learning (FL).	02