NIRMA UNIVERSITY

Institute:	Institute of Technology
Name of Programme:	BTech (CSE)
Course Code:	3CS209ME24
Course Title:	Network Security
Course Type:	Department Elective–II
Year of Introduction:	2024-25

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

Course Learning Outcomes (CLO):

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

1. demonstrate a clear understanding of fundamental network security concepts, terminologies, and principles (BL2)
2. analyse common network security threats, vulnerabilities, and attack vectors (BL4)
3. explain the principles of cryptography and apply cryptographic techniques to protect data and communications (BL5)
4. develop security policies and procedures to ensure compliance with relevant standards and regulations (BL6)

Unit	Contents	Teaching Hours (Total 45)
Unit-I	**Introduction to Network Security:** Introduction to network security concepts and terminology, The importance of network security in modern technology, Overview of security policies and procedures, introduction to Cryptography	05
Unit-II	**Information Security:** Fundamentals of cryptography, Symmetric and asymmetric encryption, Block Ciphers and DES, Advanced Encryption Standard (AES), Block Cipher Operations, Pseudo Random Number Generation and Stream Ciphers, Diffie Hellman Key Exchange, CRT Problem, RSA	10
Unit-III	**Network Threats and Defence:** Types of network threats: malware, phishing, DoS, etc., Attack vectors and methods, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), Understanding firewalls: types, technologies, and configurations, Access control and security policies.	10
Unit-IV	**Network Security:** 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-V	**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	10

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 contents

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 & Cryptography, Cengage Learning.

Suggested List of Experiments:

Sr. No.	Title	Hours
1	Implementation and crypt-analysis of shift-based ciphers- Caesar Cipher, ROT-13 cipher)	02
2	Implementation of Transposition ciphers (Single as well as Multilevel)	02
3	Exploration of various tools to perform encryption and decryption	02
4	Cryptography implementation using block-cipher DES	04
5	Asymmetric Cryptography- Creation of RSA key, RSA encryption and decryption	04
6	Simulating the Key Distribution Scenario for Symmetric Key Cryptography using the simulator of your choice	04
7	Use of Snort/Wireshark tool for Network Intrusion Detection Systems to monitor network traffic and analyze attack patterns	04
8	Configure and test VPN connections using technologies such as IPsec or OpenVPN	02
9	Perform vulnerability scans using tools like Nessus or OpenVAS to identify potential security weaknesses.	04
10	Set up network security monitoring tools to collect and analyze logs for signs of security incidents.	02