Subject Code	Subject Name	Credits
26CS010	CYBER SECURITY AND ETHICAL HACKING	4

Course Objectives:

1. The learner will gain knowledge about securing both clean and corrupted systems, protect personal data, and secure computer networks.
2. The learner will understand key terms and concepts in cyber law, intellectual property and cyber-crimes, trademarks and domain theft.
3. The learner will be able to examine secure software development practices.
4. The learner will understand principles of web security.
5. The learner will be able to incorporate approaches for incident analysis and response.

Learning Objectives:

On successful completion of the course, students will be able to:

1. After the completion of the course, the graduate will be able to:
2. Understand core cryptography concepts
3. Analyse cyber security frameworks and policies
4. Apply network security mechanisms
5. Develop digital forensics investigation skills

Unit 1 – Classical Cryptography (12 hrs.)

Convention Encryption Model, Steganography, Classical Encryption Techniques, Simplified DES, Block Cipher Principles, The Data Encryption Standard, The Strength Of DES, Differential and Linear Cryptanalysis, Block Cipher Modes of Operations, Public Key Encryption

Unit 2 – Cyber Security and Cyber Laws (12 hrs.)

Cyber Security and Cyber Laws: Overview of Cyber Security, Internet Governance – Challenges and Constraints, Cyber Threats: - Cyber Warfare-Cyber Crime-Cyber Terrorism-Cyber Espionage, need for a Comprehensive Cyber Security Policy, need for a Nodal Authority, Need for an International convention on Cyberspace. Introduction, Cyber Security Regulations, Roles of International Law, the state and Private Sector in cyberspace, Cyber Security Standards.

Unit 3 - Network Security (12 hrs.)

Introduction to The Concepts of Security, security Approaches, Principles of Security, Types of Attacks, Intruders, Intrusion Detection and Prevention System, Password Management, Viruses and Related Threats, MFA DOS and DDOS Distributed Denial of Service Attack, Firewall, Design Principles, Virtual Private Network.

Unit 4- Cyber Forensics (12 hrs.)

Cyber Forensics Overview of Cyber Forensics – Preparing digital investigation, private sector investigation, Data Acquisition and Incident Scenes – Understanding storage format for digital investigation, Examining NTFS disk, Network and Cloud Forensics – Developing procedure for network forensics, challenges in cloud forensics, acquisition in cloud forensics, Email and Social Media Forensics – exploring the role of email and server investigation, Forensics Report Writing and Ethics for Expert Witness - Understanding the importance of reports, guidelines for writing reports and generating report using forensic software.

Unit 5 - Cloud Computing and Vibe Coding (12 hrs.)

Introduction to Ethical Hacking - Classes of hacker, hacking methodology, Penetration testing, Scanning and Enumeration – Types of scanning, OS fingerprinting, vulnerability management, Sniffing and Social Engineering – MAC flooding, DHC Pattack, ARP poisoning, MCA spoofing, impact of social engineering, Dos and Session Hijacking– spoofing vs hijacking at the application level, session hi jacking defensive strategies, Web Server and applications–client server relationship, vulnerabilities of web server and applications, session management issues.

Reference Books:

1. Taha, H.A., Operations Research: An Introduction
2. Hillier, F.S. & Lieberman, G.J., Introduction to Operations Research
3. Rao, S.S., Engineering Optimization
4. Winston, W.L., Operations Research: Applications and Algorithms.