ICS-1-02T: Introduction to Cyber Security

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits: 4
Pass Percentage: 40%

Course: Introduction to Cyber Security	
Course Code: ICS-1-02T	
Course Outcomes (COs) After the completion of this course, the students will be able to:	
CO1	Understand network security threats, security services, and countermeasures.
CO2	Understand principles of network security by monitoring and analyzing the nature of attacks through cyber/computer forensics software/tools.
CO3	Develop cyber security strategies and policies
CO4	Measure the performance and troubleshoot cyber security systems.
CO5	Understand various Cryptographic Techniques

Detailed Contents:

Module No.	Module Name	Module Contents
Module I	**Cyber Attacks and Security**	**Cyber Attacks:** Introduction, Types. Assets: Identification, Accountability. Vulnerability and Threats, Risk Management, Qualitative Risk Assessment, Information Security Framework: Introduction, Policies, Standards, Baselines, Guidelines and Procedures. **Security:** Basics, User Access Controls, Authentication, Access Control: Framework, Techniques and Technologies, Training and Awareness and Its types, Technical Security Controls: Preventive, Detective, Corrective. Protection form malicious attacks.
Module II	**Networks and Communication & Software Engineering Life Cycle::**	**Networks and Communication:** Data Communication, Characteristics and components, Data flow. Computer Network, Categories, Protocol, External Services, Cloud Computing: Introduction, Models, Benefits, Challenges, Private, Public Clouds. **Software Engineering Life Cycle:** Stages, Models: Waterfall, Iterative, Spiral, V Model, Big Bang, Agile, RAD, Prototype.
Module III	**Authentication**	**Authentication:** Authentication Vs Authorization, Methods and Protocols: Kerberos, SSL, Protocol, Password Authentication, Challenge-Handshake Authentication (CHAP), MSCHAP, Extensible Authentication, Remote Authentication.

		Service Set Identification (SSID), Encryption Methods: Wire Equivalent Privacy, WPA, WPA2, MAC Filtering, Wireless Routers, Creating Wireless Network, WLAN.
Module IV	**Investigation Techniques & Cyber Forensics and Cryptography**:	**Investigation Techniques and Cyber Forensics**: Types of Investigation, Evidence and Analysis, Steps for Forensics Investigation, Forensics Tools, Investigation, Common Types of Email Abuse, Tracking Location of Email Sender, Scam or Hoax Emails and Websites, Fake Social Media Profile. **Cryptography:** Objectives, Type, OS Encryption, Public key Cryptography.

Books

1. Mayank Bhushan, Rajkumar Singh Rathore, Aatif Jamshed, "Fundamentals of Cyber Security", BPB Publications.
2. Nina Godbole, SModule Belapure, "Cyber Security", Wiley.
3. Sanil Nadkarni, "Fundamentals of Information Security", pbp.
4. Mike Chapple, James Michael Stewart, Darril Gibson, "CISSP Certified Information Systems Security Professional Official Study Guide" 9th Ed., SYBEX, A Wiley Brand.
5. William Chuck Eastton, "Computer Security Fundamentals", 4th Edition, Pearson.