CYBER SECURITY AND CYBER LAWS

Course Objectives:

1. Introduce cryptographic principles, methods, and algorithms for data protection.
2. Understand network vulnerabilities and apply security measures to counter threats.
3. Explore authentication techniques, key managementand digital signatures for communication.
4. Analyze security protocols, access controls, and securecommunication in networks.
5. Develop skills to assess risks, design secure systems, and ensure data integrity.

Module I (6 Hrs)

Introduction: Cyber Security Basics, Security Principles, Cyber Attacks and their Classification, Vulnerability Assessment, Intrusion Detection and Intrusion Prevention Systems, User Authentication Methods, Bio-metric Authentication Methods.

Module II (6 Hrs)

Standard Security Models: Information Security, Network Security, Operating System Security; Web Security: mail Security, Mobile Device Security, Cloud Security.

Module III (6 Hrs)

IoT Security: Cyber-Physical System Security, Social Media Security; Virtual Currency: Block Chain Technology, Security Auditing.

Module IV (6 Hrs)

Cyber Crimes: Types-Data Frauds, Analysis of Crimes-Human Behavior- Stylometry-Incident Handling, Investigation Methods-Criminal Profiling- Cyber Trails, Digital Forensics-HistoryChallenges-Branches of Digital Forensics, Digital Forensic Investigation Methods-Reporting Management of Evidence.

Module V (6 Hrs)

Cyber Law: Basics-Information Technology Act 2000-Amendments, Evidentiary value of Emails/SMS, Cybercrimes and Offences dealt with IPC-RBI Act-IPR in India, Jurisdiction of Cyber Crime, Creating awareness and Healthy practices.

Course Outcomes:

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

CO1. Analyze and resolve security issues in networks and computer systems to secure an IT infrastructure.
CO2. Design, develop, test, and evaluate secure software.
CO3. Develop policies and procedures to manage enterprise security risks.
CO4. Evaluate and communicate the human role in security systems with an emphasis on ethics, social engineering vulnerabilities and training.
CO5. Interpret and forensically investigate security incidents.

Essential Reading

1. Lester Evans, Cybersecurity: An Essential Guide to Computer and Cyber Security for Beginners, Including Ethical Hacking, Risk Assessment, Social Engineering, Attack and Defense Strategies, and Cyberwarfare, Kindle Edition
2. K. Jaishankar. Cyber Criminology: Exploring Internet Crimes and Criminal Behavior, CRC Press

Supplementary Reading

1. https://heimdalsecurity.com/pdf/cyber_security_for_beginners_ebook
2. http://docshare04.docshare.tips/files/21900/219006870.pdf
3. http://index-of.co.uk/Hacking-oleccion/Insider%20Attack%20&%20Cyber%20Security%20-%20Beyond%20the%20Hacker.pdf
4. http://www.uou.ac.in/sites/default/files/slm/FCS.pdf