

DCS-1-01T: Data Communication and Networks

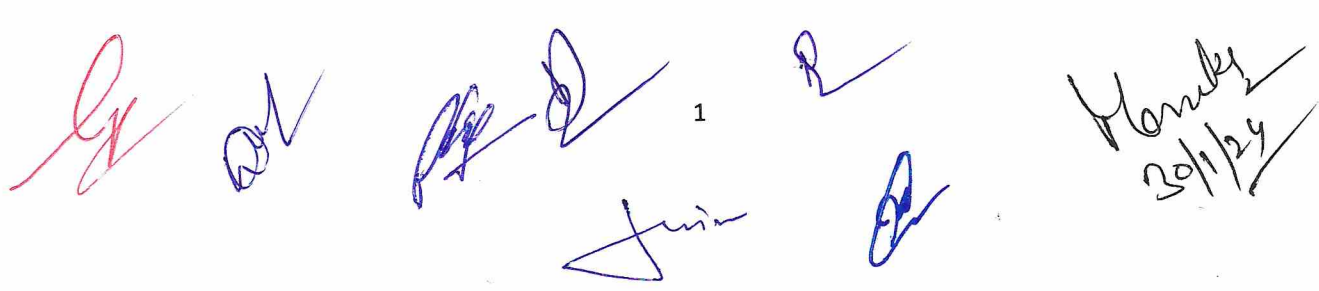
Total Marks: 100
 External Marks: 70
 Internal Marks: 30
 Credits: 4
 Pass Percentage: 40%

Course: Data Communication and Networks	
Course Code: DCS-1-01T	
Course Outcomes (COs)	
After the completion of this course, the students will be able to:	
CO1	Understand the fundamental concepts in data communication and networking
CO2	Explore real-world applications of principles of network design, topology, and the OSI/TCP/IP model
CO3	Develop the ability to identify and formulate problems related to computer network
CO4	Apply networking knowledge to design and configure basic computer networks, addressing schemes and Routing Protocols
CO5	Describe the basic concepts, principles, and techniques for the development of networks and trouble shooting

Section A

Module	Module Name	Module Content
Module I	Basic concepts	Basic Concepts: Components of data communication, modes of communication, standards and organizations, Network Classification, Network Topologies; Transmission media, network protocol; layered network architecture.
Module II	Models	Models: Overview of OSI reference model; TCP/IP protocol suite. Physical Layer: Cabling, Network Interface Card, Transmission Media Devices- Repeater, Hub, Bridge, Switch, Router, Gateway; Transmission impairments.
Module III	Data Link Layer, Network Layer and Transport Layer	Framing techniques; Error Control; Flow Control Protocols; Shared media protocols - CSMA/CD and CSMA/CA. Virtual Circuits and Datagram approach, IP addressing methods – Sub netting; Routing Algorithms (adaptive and non-adaptive) Elements of transport protocols - Addressing, Connection establishment and release, Flow control and buffering, Transport services, Transport Layer protocol of TCP and UDP.

1

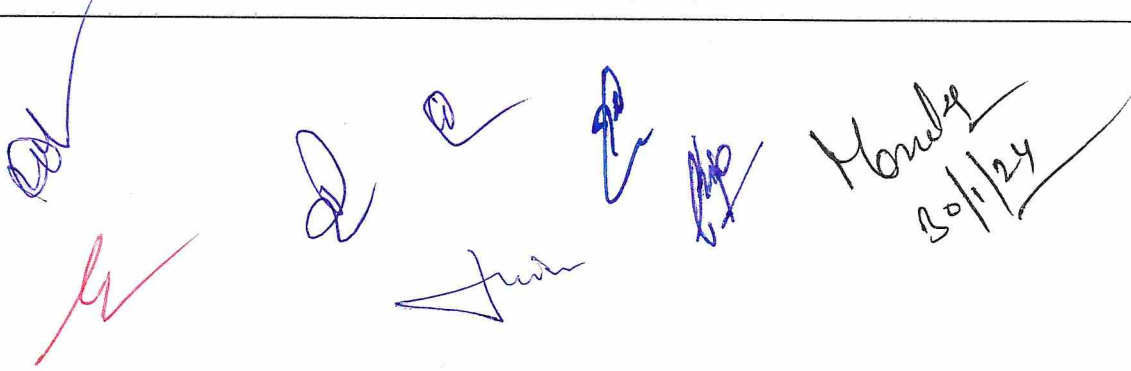


 Monday
 30/1/24

Module VI	Session Layer, Presentation Layer, Application Layer and Network Security	Session Layer: Design issues, remote procedure call. Presentation Layer: Design issues, Data compression techniques, Cryptography Common Terms, Firewalls, Virtual Private Networks
------------------	--	---

Books

<ol style="list-style-type: none"> 1. B.A. Forouzan, "Data Communication and Networking", 4th Ed., Tata McGraw Hill, 2017. 2. A. S. Tanenbaum, "Computer Networks", 5th Ed., Pearson, 2011 3. D.E. Comer, "Internetworking with TCP/IP", vol. I, PHI, 2015 4. W. Stalling, "Data & Computer Communication", 8th Ed., PHI, 2013 5. D. Bertsekas, R. Gallager, "Data Networks", 2nd Ed., PHI, 1992


 A collection of handwritten signatures and initials in blue and red ink, located below the bibliography table. The signatures are scattered and include a prominent red signature on the left, several blue initials and signatures in the center, and a blue signature with the date '30/1/24' on the right.

DCS-1-02T: Operating Systems

Total Marks: 100
 External Marks: 70
 Internal Marks: 30
 Credits: 6
 Pass Percentage: 40%

Course: Operating Systems	
Course Code: DCS-1-02T	
Course Outcomes (COs)	
After the completion of this course, the students will be able to:	
CO1	Understand the structure of computing systems, from the hardware level through the operating system level and onto the applications level.
CO2	Understand basics of operating system viz. system programs, system calls, user mode and kernel mode.
CO3	Learn the working with CPU scheduling algorithms for specific situation, and analyze the environment leading to deadlock and its rectification.
CO4	Explore the memory management techniques viz. caching, paging, segmentation, virtual memory, and thrashing.
CO5	Apply Methods for Handling Deadlocks, Deadlock Prevention, and Recovery from Deadlock.

Detailed Contents:

Module	Module Name	Module Contents
Module 1	Introduction and System Structures	Computer-System Organization, Computer-System Architecture, Operating-System Structure, Operating-System Operations, Process Management, Memory Management, Storage Management, Protection and Security, Computing Environments, Operating-System Services, User and Operating-System Interface, System Calls, Types of System Calls, System Programs.
Module II	Process Management	Process Concept, Process Scheduling, Operations on Processes, Multi-threaded programming: Multithreading Models, Process Scheduling: Basic Concepts, Scheduling Criteria, and Scheduling Algorithms.
Module III	Deadlock	Deadlock: System Model, Deadlock Characterization, Methods for Handling Deadlocks, Deadlock Prevention, Deadlock Avoidance, Deadlock Detection, Recovery from

		Deadlock.
Module IV	Memory Management	Basic Hardware, Address Binding, Logical and Physical Address, Dynamic linking and loading, Swapping, Contiguous Memory Allocation, Segmentation, Paging, Demand Paging, Page Replacement algorithms.
Module V	File Systems	File Systems: File Concept, Access Methods, Directory and Disk Structure, File-System Structure, File-System Implementation, Directory Implementation, Allocation Methods, Free-Space Management.
Module VI	Introduction to Linux and Linux Commands	Linux's shell, Kernel, Features of Linux, File System: Filenames, Introduction to different types of directories: Parent, Subdirectory, Home directory; rules to name a directory, Important directories in Linux File System, Linux Commands: cal, date, echo, bc, who, cd, mkdir, rmdir, ls, cat cp, rm, mv, more, gzip, tar, File ownership, file permissions, chmod, Directory permission, change file ownership.

Books

<ol style="list-style-type: none"> 1. A Silberschatz, P.B. Galvin, G. Gagne, "Operating Systems Concepts", 8th Ed., John Wiley Publications, 2009 2. A.S. Tanenbaum, "Modern Operating Systems", 3rd Ed., Pearson Education, 2014 3. G. Nutt, "Operating Systems: A Modern Perspective", 2nd Ed., Pearson Education, 2000 4. S. Das, "Unix Concepts and Applications", 4th Ed., McGraw Hill Education, 2017

Handwritten signatures in blue ink, including names like 'Srinivas', 'Ravi', 'Hemant', and 'Srinivas'.

DCS-1-02P: Operating Systems Lab

Total Marks: 50
External Marks: 35
Internal Marks: 15
Credits: 2
Pass Percentage: 40%

Course: Operating Systems Lab	
Course Code: DCS-1-02P	
Course Outcomes (COs)	
After the completion of this course, the students will be able to:	
CO1	Understand Basics of UNIX/LINUX
CO2	Demonstrate the installation process of various operating systems.
CO3	Apply UNIX/LINUX operating system commands.
CO4	Understand different UNIX/LINUX shell scripts
CO5	Implement and execute various shell programs.

Detailed List of Programs:

Programme No.	Name of Program
P1	Install UNIX/LINUX – Complete Step by Step
P2	Study of Basic UNIX Commands and various UNIX editors such as vi, ed, ex and EMACS
P3	Write a shell script that deletes all lines containing the specified word in one or more files Supplied as arguments to it.
P4	Write a shell script that displays a list of all files in the current directory to which the user has read, write and execute permissions
P5	Write a shell script that receives any number of file names as arguments checks if every argument supplied is a file or directory and reports accordingly. Whenever the argument is a file it reports no of lines present in it
P6	Write a shell script that accepts a list of file names as its arguments, counts and reports the occurrence of each word that is present in the first argument file on other argument files.
P7	Write a shell script to list all of the directory files in a directory

Monika
20/1/24

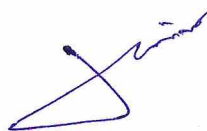
P8	Write a shell script to find factorial of a given number
P9	Write an awk script to count number of lines in a file that does not contain vowels
P10	Write an awk script to find the no of characters ,words and lines in a file
P11	Implement in C language, the following Unix commands using system calls a) cat b) ls c) mv
P12	Write a C program that takes one or more file/directory names as command line input and reports following information
P13	Write a C program to list every file in directory, its inode number and file name
P14	Write a C program to create zombie process
P15	Write a C program to illustrate how an orphan process is created
P16	Write client server programs using c for interaction between server and client process using Unix Domain sockets











Monday
20/1/24

		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.

Edy

[Red signature]

[Blue signature]

[Blue signature]

[Blue signature]

[Blue signature]

*Howdy
20/1/24*

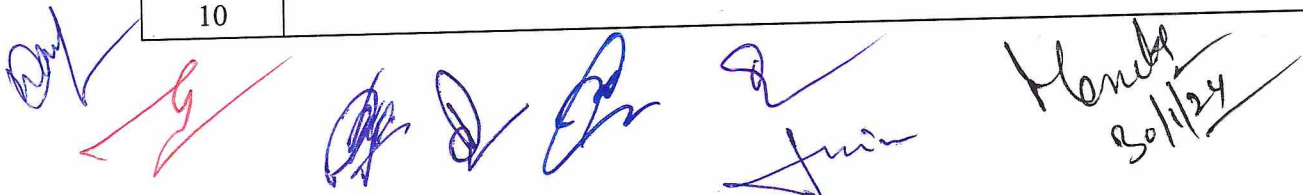
ICS-1-02P: Introduction to Cyber Security Lab

Total Marks: 50
External Marks: 35
Internal Marks: 15
Credits: 2
Pass Percentage:
40%

Course Name: Introduction to Cyber Security Lab	
Course Code: ICS-1-02P	
Course Outcomes (COs)	
After the completion of this course, the students will be able to:	
CO 1	Identify and analyze common cyber threats, including malware, phishing attacks, and network vulnerabilities.
CO 2	Apply techniques to detect, mitigate, and respond to various types of cyber threats.
CO 3	Implement security configurations for operating systems, network devices, and applications.
CO 4	Apply ethical hacking techniques to identify and exploit vulnerabilities in controlled environments, emphasizing responsible and legal practices.
CO5	Implement cryptographic techniques for security purpose

Detailed Contents:

S. No.	Name of Experiments
1	How to identify open ports, services, and potential vulnerabilities on target systems.
2	How to scan and enumerate devices on a network using Nmap tool.
3	How to analyse the malware in a controlled environment.
4	Conduct an experiment for phishing simulation to demonstrate common phishing tactics.
5	How to configure a firewall to control incoming and outgoing network traffic.
6	Design and implement the rules to permit or deny specific types of traffic.
7	Design and implement the secure communication using tools like OpenSSL or GPG.
8	Simulate various common password cracking techniques.
9	Study of Computer Forensics and different tools used for forensic investigation
10	How to encrypt and decrypt messages using the chosen algorithm and analyze the



	security properties.
--	----------------------

[Handwritten signatures and notes in blue and red ink]

Handwritten signatures in blue ink include: a stylized signature on the left, a signature resembling 'd', a signature resembling 'e', a signature resembling 'a', and a signature resembling 'J'. To the right, the text 'Handwritten' is written above 'solipsy'.

A signature in red ink is located below the blue signatures, resembling the letter 'u'.

DCS-2-01T: Digital Forensics

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits: 6
Pass Percentage: 40%

Course Name: Digital Forensics	
Course Code: DCS-2-01T	
Course Outcomes (COs)	
After the completion of this course, the students will be able to:	
CO 1	Understand the principles and concepts of digital forensics.
CO 2	Understand various types of cyber crimes
CO 3	Analyze computer architectures, file systems, and operating systems relevant to digital forensics investigations.
CO 4	Understand the legal and ethical considerations associated with digital forensics, including the admissibility of digital evidence in court.
CO 5	Utilize popular forensic tools and software for digital investigations.

Detailed Contents:

Module No.	Module Name	Module Contents
Module I	Introduction to Digital Forensics	<ul style="list-style-type: none"> Introduction to digital forensics, definition and scope of digital forensics Different Branches of Digital Forensics Importance and applications of digital forensics in law enforcement and cybersecurity.
Module II	Cyber Crime and Computer Crime	<ul style="list-style-type: none"> Definition and types of cybercrimes Electronic evidence and handling, electronic media, collection, searching and storage of electronic media, Introduction to internet crimes Hacking and cracking, credit card and ATM frauds, web technology, cryptography, emerging digital crimes and modules
Module III	Computer Fundamentals for Digital Forensics	<ul style="list-style-type: none"> Basic Computer Organization Analysis of File systems and Data Structures Memory organization concept Data storage concepts Basics of operating systems and their role in digital forensics. Investigating network-based attacks. Analysing network traffic and logs. Understanding volatile memory. Windows Systems and Artifacts Linux Systems and Artifacts
Module IV	Legal aspects of	<ul style="list-style-type: none"> Understanding of legal aspects and their

Handwritten signature in blue ink

Handwritten signature in blue ink

Handwritten signature in blue ink with date 30/1/24

	Digital Forensics	<p>impact on digital forensics, Electronics discovery</p> <ul style="list-style-type: none"> • Overview of legal and ethical issues in digital forensics. • Types of digital evidence (e.g., documents, emails, logs). • Collection, preservation, and documentation of digital evidence. • Preparing forensic reports. • Providing expert testimony in court. • Admissibility of digital evidence in court.
Module V	Forensic Tools	<ul style="list-style-type: none"> • Introduction to Forensic Tools • Usage of Slack space • Tools for Disk Imaging, Data Recovery, Vulnerability • Assessment Tools, Encase and FTK tools • Anti-Forensics and probable counters • Retrieving information
Module VI	Processing of Electronic Evidence	<ul style="list-style-type: none"> • Process of computer forensics and digital investigations • Processing of digital evidence, digital images, damaged SIM and data recovery, multimedia evidence • Retrieving deleted data: desktops, laptops and mobiles • Retrieving data from slack space, renamed file, ghosting, compressed files • Techniques for analysing and extracting information from computer memory • Forensic analysis of smartphones and tablets.

Books

1. C. Altheide & H. Carvey, "Digital Forensics with Open Source Tools", Syngress
2. John Sammons "The Basics of Digital Forensics", Syngress
3. Brain Carrier "File System Forensic Analysis", Addison-Wesley
4. Harlan Carvey "Advanced Digital Forensic Analysis of the Windows Registry", Syngress
5. Diane Barrett "Virtualization and Forensics - A Digital Forensic Investigator's Guide to Virtual Environments", Syngress
6. B. Nelson, A. Phillips, and C. Steuart "Guide to Computer Forensics and Investigations", Cengage

A collection of handwritten signatures and initials in blue and red ink, including a prominent signature that reads "Monika 30/1/24".

DCS-2-02T: Cyber Attacks and Counter Measures

Total Marks: 100
 External Marks: 70
 Internal Marks: 30
 Credits: 6
 Pass Percentage:
 40%

Course Name: Cyber Attacks and Counter Measures	
Course Code: DCS-2-02T	
Course Outcomes (COs)	
After the completion of this course, the students will be able to:	
CO 1	Understand the importance of a network basics and brief introduction on security of network protocols
CO 2	Demonstrate a solid understanding of foundational cybersecurity concepts, principles, and best practices.
CO 3	Apply risk assessment methodologies to evaluate and prioritize potential vulnerabilities within a given system or network.
CO 4	Design and develop security plans and strategies to ensure the integrity of information in compliance with best practices, relevant policies, standards, and regulations.
CO 5	Evaluate the impact of cybersecurity decisions on privacy, compliance, and organizational reputation, and adhere to ethical standards in the field.

Detailed Contents:

Module No.	Module Name	Module Contents
Module 1	Introduction to Cybersecurity and Threat Landscape	<ul style="list-style-type: none"> Overview of Cybersecurity: Fundamental concepts, objectives, and importance. Cyber Threat Landscape: Types of cyber threats, attack vectors, and motivations. Current Trends: Analysis of recent cyber threats and emerging trends in the cybersecurity landscape.
Module II	Security Fundamentals	<ul style="list-style-type: none"> Overview of Security Fundamentals. Security Foundations: Principles, protocols, and standards in cybersecurity.
Module III	Risk Assessment	<ul style="list-style-type: none"> Vulnerability Assessment: Techniques for identifying and assessing vulnerabilities. Risk Management: Understanding risk, assessing potential impacts, and prioritizing security measures.
Module IV	Implementing Security Measures and Incident Response	<ul style="list-style-type: none"> Security Controls: Designing and implementing security measures, including firewalls, antivirus, encryption, and access controls. Incident Response Planning: Developing and implementing an incident response

		<p>plan.</p> <ul style="list-style-type: none"> • Security Monitoring: Using tools and techniques to monitor for potential security incidents.
Module V	Ethical Hacking, Penetration Testing	<ul style="list-style-type: none"> • Ethical Hacking: Introduction to ethical hacking principles and practices. • Penetration Testing: Conducting controlled attacks to identify and address vulnerabilities.
Module VI	Legal Considerations	<ul style="list-style-type: none"> • Legal and Ethical Considerations: Understanding the legal and ethical aspects of cybersecurity, including compliance, privacy, and responsible disclosure.

Books

1. Sammons, John, and Michael Cross, "The basics of cyber safety: computer and mobile device safety made easy", Syngress
2. Charles P. Pfleeger, Shari Lawrence, Pfleeger Jonathan Margulies, "Security in Computing", Pearson
3. Brooks, Charles J., Christopher Grow, Philip Craig, and Donald Short, "Cybersecurity essentials", Sybex
4. William Stallings "Network Security Essentials", Pearson
5. Ross J. Anderson "Security Engineering: A Guide to Building Dependable Distributed Systems", 2nd Ed., John Wiley & Sons

Handwritten signatures in blue ink, including names like 'Monks' and 'D'.

DCS-2-02P: Cyber Attacks and Counter Measures Lab

Total Marks: 50
External Marks: 35
Internal Marks: 15
Credits: 2
Pass Percentage:
40%

Course Name: Cyber Attacks and Counter Measures	
Course Code: DCS-2-02P	
Course Outcomes (COs) After the completion of this course, the students will be able to:	
CO 1	Develop skills in configuring security settings for operating systems, networks, and applications.
CO 2	Analyse network traffic using tools like Wireshark.
CO 3	Conduct vulnerability assessments to identify potential weaknesses and recommend appropriate countermeasures.
CO 4	Apply tools to analyze network traffic and system logs in real-time.
CO 5	Understand and apply secure coding practices to develop resilient software.

Detailed Contents:

S. No.	Name of Experiment
1	How to create signatures to detect and block the malware using antivirus or intrusion detection systems.
2	How to capture and analyse network traffic using tools like Wireshark.
3	How to configure and test an intrusion detection system to identify and respond to malicious activities.
4	Implement the firewall rules by simulating different attack scenarios and assessing the effectiveness of the configured rules.
5	Conduct a phishing simulation to test user awareness and susceptibility.
6	Evaluate the effectiveness of implemented countermeasures and educate users on recognizing phishing attempts.
7	Develop and implement a patch management plan to address identified vulnerabilities.
8	Simulate a cybersecurity incident and implement an incident response plan.
9	Perform security testing on a web application to identify and remediate common vulnerabilities.
10	How to implement countermeasures to mitigate the impact of the attack and

(Handwritten signatures and notes)
Monika
30/1/24

ensure service availability.

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten date]

[Handwritten signature]

[Handwritten signature]

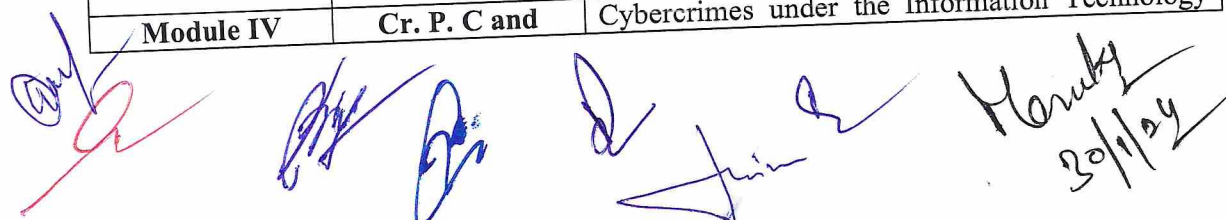
CL-2-03T: Cyber Laws

Total Marks: 100
External Marks: 70
Internal Marks: 30
Credits: 6
Pass Percentage: 40%

Course Name: Cyber Laws	
Course Code: CL-2-03T	
Course Outcomes (COs)	
After the completion of this course, the students will be able to:	
CO 1	Understand various types of cyber crimes
CO 2	Understand Indian Laws to deal with Cyber Crimes and its critical analysis
CO 3	Understand Legal Recognition of Electronic Records and Electronic Evidence
CO 4	Examine and interpret laws related to cybercrimes, including hacking, identity theft, and online fraud.
CO 5	Explore the legal aspects of intellectual property rights, including copyright, patents, and trademarks, in the digital environment.

Detailed Contents:

Module No.	Module Name	Module Contents
Module I	Introduction to Cyber Crimes	Cybercrimes and related offences and penalties: Introduction to Cybercrimes, Classification of cybercrimes, Distinction between cybercrime and conventional crimes, Reasons for commission of cybercrime, Kinds of cybercrimes – cyber stalking; cyber pornography; forgery and fraud; crime related to IPRs; Cyber terrorism; Spamming, Phishing, Privacy and National Security in Cyberspace, Cyber Defamation and hate speech, computer vandalism etc.
Module II	Indian Cyber Laws	Provisions in Indian Laws in dealing with Cyber Crimes and its critical analysis, Information Technology Act, 2000, Penalties under IT Act, Offences under IT Act, Offences and Analysis related with Digital Signature and Electronic Signature under IT Act, Statutory Provisions, Establishment of Authorities under IT Act and their functions, powers. Cybercrimes under IPC
Module III	Electronic Governance	Legal Recognition of Electronic Records and Electronic Evidence -Digital Signature Certificates - Securing Electronic records and secure digital signatures - Duties of Subscribers - Role of Certifying Authorities - Regulators under the IT Act -The Cyber Regulations Appellate Tribunal - Internet Service Providers and their Liability- Powers of Police under the IT Act – Impact of the IT Act on other Laws.
Module IV	Cr. P. C and	Cybercrimes under the Information Technology



 30/1/22

	Indian Evidence Act	Act, 2000 - Cybercrimes under International Law - Hacking Child Pornography, Cyber Stalking, Denial of service Attack, Virus Dissemination, Software Piracy, Internet Relay Chat (IRC) Crime, Credit Card Fraud, Net Extortion, Phishing etc - Cyber Terrorism Violation of Privacy on Internet - Data Protection and Privacy – Indian Court cases
Module V	Intellectual Property Rights	Copyrights – Software – Copyrights vs Patents debate - Authorship and Assignment Issues - Copyright in Internet - Multimedia and Copyright issues - Software Piracy - Trademarks - Trademarks in Internet – Copyright and Trademark cases
Module VI	International Cooperation and Emerging Legal Issues	Examination of international frameworks and agreements related to cybersecurity. Analysis of the challenges and legal considerations associated with cross-border cyber threats. Exploration of emerging legal issues in cybersecurity, including artificial intelligence, blockchain, and the Internet of Things (IoT).

Books

1. "The Information Technology Act, 2000 Bare Act with Short Notes", Universal Law Publishing Co., New Delhi
2. Justice Yatindra Singh, "Cyber Laws", Universal Law Publishing Co., New Delhi
3. Farouq Ahmed, "Cyber Law in India", New Era publications, New Delhi
4. S. R. Myneni, "Information Technology Law (Cyber Laws)", Asia Law House, Hyderabad.
5. Chris Reed, "Internet Law-Text and Materials", Cambridge University Press.
6. Pawan Duggal, "Cyber Law- the Indian Perspective", Universal Law Publishing Co., New Delhi.
7. Elias. M. Awad, "Electronic Commerce", Prentice-Hall of India Pvt. Ltd

Handwritten signature

Handwritten signature

Handwritten signature

Handwritten signature

Handwritten signature

Handwritten signature
30/1/24

Handwritten signature

Handwritten signature