MGMUNIVERSITY

MGM UNIVERSITY, CHHATRAPATI SAMBHAJINAGAR

ACADEMIC SECTION

NOTIFICATION

No. 95/2023 17th August 2023

Enclosed Format of Curriculum Booklet

Registrar 17/8/23

Registrar
MGM University
Aurangabad

To,

All Deans and Principals / Directors / HoD's

Copy to :

1. PS of Hon'ble Chancellor - For kind information please.
2. PS of Hon'ble Vice-Chancellor
3. The Controller of Examinations
4. The ERP section
5. The Website Team
6. The Deputy Registrar (Academics)

MGM University

Chhatrapati Sambhajinagar

Name of Faculty – Engineering & Technology

Name of Institute – Institute of Information and Communication Technology (IICT)

Name of Programme – Diploma in Cyber Security and Digital Forensics

CURRICULUM BOOKLET

(With effect from Academic year 2025-26)

MGM University

Chhatrapati Sambhajinagar

Published by –

Academic Section,

Registrar Office,

MGM University

Contents

MGM University

Vision

- To ensure sustainable human development which encourages self-reliant and self-content society.
- To promote activities related to community services, social welfare and also Indian heritage and culture.
- To inculcate the culture of non-violence and truthfulness through vipassanna meditation and Gandhian Philosophy.
- To develop the culture of simple living and high thinking

Mission

- To impart state of art education and technical expertise to students and give necessary training to teachers to create a self-reliant society for future.
- To encourage students to participate in Indian and International activities in sports, literature, etc. so that future generation becomes base for free and liberal society
- To educate students in areas like Management, Finance, Human relations to inculcate philosophy of simple living and high thinking value of simple economic society.
- To inculcate a culture of non-violence and truthfulness through Vipassana.
- To sustain activities of Indian culture (viz. classical dance, music and fine arts) through establishing institutes like Mahagami, Naturopathy, etc.

विद्यापीठ गीत

अत्त दिप भव भव प्रदिप भव,
स्वरूप रूप भव हो
ज्ञान सब्ब विज्ञान सब्ब भव,
सब्ब दिप भव हो
अत्ताहि अत्त नो नाथो,
अत्ताहि अत्त नो गति
अत्त मार्गपर अप्रमादसे है तुझे चलना
सब्ब का कल्याण हो,
वो कार्यकुशल करना
सब्ब का उत्तम मंगल, पथप्रदर्शक हो
अत्त दिप भव भव प्रदिप भव,
स्वरूप रूप भव हो
ज्ञान सब्ब विज्ञान सब्ब भव,
सब्ब दिप भव हो
बुद्धमं शरनं गच्छामि :
धम्मं शरनं गच्छामि :
संघं शरनं गच्छामि :

Institute of Information and Communication Technology (IICT) at a Glance

The Institute of Information and Communication Technology (IICT) offers emerging courses in Information Technology, with a focus on Internet of Things (IoT), Blockchain, and Big Data Analytics (BDA). Additionally, it provides Diploma in Cyber Security and Digital Forensics, undergraduate degrees in Artificial Intelligence & Machine Learning (B.Tech. AI and ML) and Data Science (B.Tech. Data Science). Furthermore, the Institute offers Master of Technology Degrees in Data Science (M.Tech. Data Science) and AI & ML (M.Tech. AI and ML). Moreover, IICT offers a PhD program in IT.

Vision

IICT shall be a center of excellence fostering innovation, entrepreneurship, and technological advancement with social and global perspectives. It will develop skilled professionals and contribute to industry, research, and interdisciplinary growth.

Mission

The IICT will:

- Empower students with human values, ethical conduct, and environmental responsibility.
- Foster interdisciplinary technocrats contributing to sustainable industrial growth.
- Promote expertise in emergent technologies through research, innovation, and industry collaboration to solve real-world challenges.
- Encourage entrepreneurship and leadership, preparing students for future challenges.

Programs offered at IICT

Undergraduate Programmes	Postgraduate Programmes	UG Diploma	PhD Programmes
B.Tech. in Information Technology	M.Tech. Data Science	Cyber Security and Digital Forensics	PhD in IT
B.Tech. in Artificial Intelligence and Machine Learning	M.Tech. AI and ML		
B.Tech. in Data Science			
B. Tech CSE(AI)			

Name of Programme – Diploma

Duration – Two Years

Eligibility –Passed HSC or its equivalent examination from science stream and obtained at least 45% marks (at least 40% marks, in case of Backward class categories belonging to Maharashtra State only)

1. Maharashtra State Candidate

(i) The Candidate should be an Indian National and having domicile of Maharashtra state and/or born in Maharashtra state.

(ii) Passed HSC or its equivalent examination with Physics and Mathematics as compulsory subjects along with one of the Chemistry or Biotechnology or Biology or Technical Vocational subject or Computer Science or Information Technology or Informatics Practices or Agriculture or Engineering Graphics or Business Studies, and obtained at least 45% marks (at least 40% marks, in case of Backward class categories and Persons with Disability candidates belonging to Maharashtra State only) in the above subjects taken together and the candidate should have appeared in MGMU-CET 2024/ MHT-CET 2024/ PERA CET 2024/ JEE (Main) Paper-I 2024 and should obtain non zero score in MGMU-CET 2024/ MHT-CET 2024/ PERA CET 2024/ JEE (Main) Paper-I 2024.. However, preference shall be given to the candidate obtaining non-zero positive score in MGMU-CET 2024 over the candidates who obtained non-zero score in MHT-CET 2024/ PERA CET 2024.

OR

(ii)Passed Diploma in Engineering and Technology and obtained at least 45% marks (at least 40% marks, in case of Backward class categories and Persons with Disability candidates belonging to Maharashtra State only).

2. All India Candidates

(i) The Candidate should be an Indian National.

(ii) Passed HSC or its equivalent examination with Physics and Mathematics as compulsory subjects along with one of the Chemistry or Biotechnology or Biology or Technical Vocational subject or Computer Science or Information Technology or Informatics Practices or Agriculture or Engineering Graphics or Business Studies , and obtained at least 45% marks (at least 40% marks, in case of Backward class categories and Persons with Disability candidates belonging to Maharashtra State only) in the above subjects taken together and candidate should have appeared in MGMU-CET 2024/ MHT-CET 2024/ PERA CET 2024/ JEE (Main) Paper-I 2024 and should obtain non-zero score in MGMU-CET 2024/ MHT-CET 2024/ PERA CET 2024/ JEE (Main) Paper-I 2024. However, preference shall be given to the candidate obtaining non-zero positive score in JEE Mains Paper-I over the candidates who obtained non-zero score in MGMU-CET 2024/ MHT-CET 2024/ PERA CET 2024.

OR

(ii) Passed Diploma in Engineering and Technology and obtained at least 45% marks (at least 40% marks, in case of Backward class categories and Persons with Disability candidates belonging to Maharashtra State only)

Name of Faculty: Faculty of Engineering and Technology
Name of the Institute : Institute of Information and Communication Technology (IICT)
Name of the Programme:Diploma in Cyber Security and Digital Forensics
Programme Type : Diploma
Duration: 2 Years

First Year - Semester I												
Course Category	Course Code	Course Title	Nature of Course	No of Credits	Teaching (Contact hrs/ week)		Evaluation Scheme (Marks)			Minimum Passing (Marks)		
					L	P	Internal	External	Total	Internal	External	Total
PCC	DCS23PCL101	Fundamentals of Networking	Lecture	3	3	-	60	40	100	-	16	40
PCC	DCS23PCL102	Information Security and Cryptography	Lecture	3	3	-	60	40	100	-	16	40
PCC	DCS23PCL103	Operating Systems	Lecture	3	3	-	60	40	100	-	16	40
PCC	DCS23PCL104	Database Management Systems	Lecture	3	3	-	60	40	100	-	16	40
PCC	DCS23PCL105	Introduction to Cyber Security	Lecture	2	2	-	60	40	100	-	16	40
PCC	DCS23PCP101	Fundamentals of Networking Lab	Practical	1		2	30	20	50	-	8	20
PCC	DCS23PCP102	Information Security and Cryptography Lab using C	Practical	2		4	30	20	50	-	8	20
PCC	DCS23PCP103	Operating Systems Lab	Practical	1		2	30	20	50	-	8	20
PCC	DCS23PCP104	Database Management Systems Lab	Practical	2		4	30	20	50	-	8	20
		Total		20	14	12	420	280	700			

First Year - Semester II												
Course Category	Course Code	Course Title	Nature of Course	No of Credits	Teaching (Contact hrs/ week)		Evaluation Scheme (Marks)			Minimum Passing (Marks)		
					L	P	Internal	External	Total	Internal	External	Total
PCC	DCS23PCL151	Network Security and Firewalls	Lecture	3	3	-	60	40	100	-	16	40
PCC	DCS23PCL152	Advanced Cryptography	Lecture	3	3	-	60	40	100	-	16	40
PCC	DCS23PCL153	Software Engineering & Security Testing	Lecture	3	3	-	60	40	100	-	16	40
PCC	DCS23PCL154	Digital Forensics	Lecture	3	3	-	60	40	100	-	16	40
PCC	DCS23PCL155	Ethical Hacking	Lecture	2	2	-	60	40	100	-	16	40
PCC	DCS23PCP151	Network Security and Firewalls Lab	Practical	1		2	30	20	50	-	8	20
PCC	DCS23PCP152	Advanced Cryptography using C Lab	Practical	1		2	30	20	50	-	8	20
PCC	DCS23PCP153	Software Engineering and Security Testing Lab	Practical	1		2	30	20	50	-	8	20
PCC	DCS23PCP154	Digital Forensics Lab	Practical	1		2	30	20	50	-	8	20
SEC	DCS23SEC151	Basics of Python	Practical	2		4	30	20	50	-	8	20
		Total		20	14	12	450	300	750			

Second Year - Semester III												
Course Category	Course Code	Course Title	Nature of Course	No of Credits	Teaching (Contact hrs/ week)		Evaluation Scheme (Marks)			Minimum Passing (Marks)		
					L	P	Internal	External	Total	Internal	External	Total
PCC	DCS23PCL201	Network Threat Management Techniques	Lecture	3	3	-	60	40	100		16	40
PCC	DCS23PCL202	Computer and Mobile Forensics	Lecture	3	3	-	60	40	100		16	40
PCC	DCS23PCL203	Dark Web OSINT Investigation	Lecture	3	3	-	60	40	100		16	40
PCC	DCS23PCL204	Cyber Laws and Ethics	Lecture	2	2	-	60	40	100		16	40
PEC	1. DCS23PEL201 2. DCS23PEL202	Elective - 1. Blockchain and Cryptocurrency Forensics 2. Cloud and IOT Security	Lecture	3	3	-	60	40	100	-	16	40
PCC	DCS23PCP201	Network Threat Management Techniques Lab	Practical	2		4	30	20	50	-	8	20
PCC	DCS23PCP202	Computer and Mobile Forensics Lab	Practical	2		4	30	20	50	-	8	20
PEC	1. DCS23PEP201 2. DCS23PEP202	Elective 1.Blockchain and Cryptocurrency Forensics Lab 2.Cloud and IOT Security	Practical	1		2	30	20	50	-	8	20
SEM	DCS23SEM201	Seminar	Practical	1		2	50		50			20
		Total		20	14	12	440	260	700			

Second Year - Semester IV												
					L	P	Internal	External	Total	Internal	External	Total
PCC	DCS23PCL 251	Cyber Risk Management & Compliance	Lecture	2	2	-	60	40	100		16	40
PCC	DCS23PCL 252	Security Operations Center	Lecture	2	2	-	60	40	100		16	40
OJT	DCS23OJT 251	Project /Internship	Practical	12		24	100	200	300		80	120
		Total		16	4	24	220	280	500			

Semester –I

Course Code: DCS23PCL101 **Course Name:** Fundamentals of Networking **Course Category:** PCC
Credits:3 Teaching Scheme: L- 3 Hrs/week **Evaluation Scheme:** CA–40, MSE–20, ESE–40
Duration of Theory Exam: 2 Hrs
Pre-requisites: Basic computer literacy and familiarity with operating systems
Course Objectives: This course will enable students to
1. Understand Network Concepts
2. Understand Network Protocols and standards
3. Describe the components of network architecture, including routers, switches, firewalls, and access points.
4. Understand the structure of IP addresses and the difference between IPv4 and IPv6
Course Outcomes: At the end of the course, the students will be able to -
CO1: Demonstrate knowledge of basic networking concepts, including types of networks.
CO2: Describe and differentiate between the OSI and TCP/IP networking models, including the functions of each layer.
CO3: Identify key network protocols (e.g., TCP, UDP, IP, HTTP) and analyze their roles in data communication.
CO4: Perform IP addressing and subnetting calculations, understanding the significance of subnet masks

Contents–

Unit	Content	Teaching Hours
1	**Basics of Computer Network-** Computer Network: Definition, Goals; Broadcast and Point-ToPoint Networks; Connectionless and Connection-Oriented Services; Network Devices; Network Topologies; Types of Network: LAN, MAN, WAN; Server Based LANs and Peer-to-Peer LANs; Transmission Types; Modes of Communication; Switching Techniques	9

2	**Network Models-** Design Issues of the Layer, Protocol Hierarchy, ISO-OSI Reference Model: Functions of each Layer; Various Terminology used in Computer Network; Connection-Oriented and Connectionless Services, Internet (TCP/IP) Reference Model, Comparison of ISO OSI and TCP/IP Model	**9**
3	**Network Interface Devices-** Network Adaptor Cards (both wired and wireless), Hubs, Switches, Routers, Access Points (Wireless), Repeaters. Their basic architecture, working and use/application, understanding their technical specifications	**9**
4	**Transmission Media -** Transmission Medium, Guided Media: Coaxial Cable, Twisted Pair, Fiber Optics Cable; Unguided Media: Radio Waves, Infrared, Micro-wave, Satellite. Introduction to UTP CAT series cables, RJ-45 connectors, color coding scheme, crimping a UTP cable to RJ-45 connector, physically connecting individual nodes to the switch	**9**
5	**Internet Basics -** Internet: Architecture, Accessing, Internet Service Providers (ISP), Organization of Internet Protocol suite, IP Address, DNS, URL; World Wide Web (WWW): Web Page, Web Servers, Web Browsers	**9**

Text Books:

1. Fourauzan B., "Data Communications and Networking , 5thEdition, Tata McGraw-Hill,Publications, ISBN: 0 –07 –058408 –7
2. Andrew S. Tenenbaum,"Computer Networks"‖,PHI, ISBN 81-203-2175-8 5 TH Edition,Pearson publication

Reference Books:

1. Networking Fundamentals by Crystal Panek Published by John Wiley & Sons, Inc. 111 River Street ISBN: 978-1-119-65074-4
2. Fundamentals of Computer Networks by Matthew N. O. Sadiku 1st ed. 2022 , Springer International Publishing AG , ISBN-10 , 3031094166

Online Resources:

1.NPTEL course of Networking Fundamentals

Semester –I

Course Code: DCS23PCL102 **Course Name:** Information Security and Cryptography **Course Category:** PCC
Credits: 3 Teaching Scheme: L- 3 Hrs/week **Evaluation Scheme:** CA–40, MSE–20, ESE–40
Duration of Theory Exam: 2 Hrs
Pre-requisites: Basic Mathematics and Probability
Course Objectives: This course will enable students to
1. Understand fundamental principles of Information theory.
2. Explore entropy, mutual information, and data compression.
3. Study coding techniques for secure communication.
4. Analyze how Information Theory applies to Cryptography and Cybersecurity
Course Outcomes: At the end of the course, the students will be able to -
CO1 Understand Fundamental Concepts of Information Theory
CO2 Apply Information Theory to Secure Communication.
CO3 Analyze Cryptographic Algorithms Using Information Theory
CO4 Implement Secure Data Encoding and Compression.

Contents–

Unit	Content	Teaching Hours
1	**Introduction to Information Theory:** Characteristics of Information, Shannon's theorems on Information theory, entropy, Noisy Channel Model, Channel Capacity Theorem, finding information content and calculating source capacity and Channel capacity using entropy, Mutual information, Binary Symmetric Channel and calculation of priori and posteriori entropy. Use of Information theory in Cybersecurity	9
2	**Source Coding and Compression-** Fixed length and variable length coding, Huffman Coding, Arithmetic Coding, Shannon-Fano Coding, Lossy and lossless compression, their advantages and disadvantages, Block Codes and its Application, Secure Data Storage and its uses.	9

3	**Error Detection Error Correction-** Techniques used for designing Error detection and Correction Codes, Hamming Codes, Reed-Solomon Codes	**9**
4	**Cryptography and Information Theory-** Perfect Secrecy (Shannon's Theorem) Entropy in Cryptographic Protocols, One-Time Pad Security, Key Distribution and Entropy Source Analysis	**9**
5	**Advanced Topics in Information Security-** Differential Privacy, Data Leakage Prevention, Secure Multiparty Computation, Information-Theoretic Secure Encryption, Side Channel Attacks and Countermeasures, Information-Theoretic Secure Authentication	**9**

Text Books:

1. Elements of Information Theory" – Thomas M. Cover & Joy A. Thomas. 2nd Edition Wiley publication(2006)
2. Cryptography and Network Security: Principles and Practice" – William Stallings, 7th edition Pearson Publication 2017

Reference Books:

1. Mark Nelson, Jean loup Gailly ,"The Data Compression Book" , Second Edition, Wiley & Sons, Publication
2. "Information Theory and Network Coding" – Raymond W. Yeung, Springer publication

Online Resources:

1. MIT OpenCourseWare – Information Theory
2. Stanford University – Cryptography Course

Semester –I

Course Code: DCS23PCL103 **Course Name:** Operating Systems **Course Category:** PCC
Credits:3 Teaching **Scheme:** L- 3 Hrs./week **Evaluation Scheme:** CA–40, MSE–20, ESE–40
Duration of Theory Exam: 2 Hrs.
Pre-requisites: Basic Knowledge of computer fundamentals and operating system.
Course Objectives: This course will enable students to
1. Understand OS functions and process management.
2. Understand file system, memory management and device management in OS.
Course Outcomes: At the end of the course, the students will be able to -
CO1: Explain the importance of an operating system in terms of its functions.
CO2: Analyze process management techniques in operating systems.
CO3: Demonstrate concepts of process synchronization and deadlock
CO4: Illustrate the structure and functionality of file systems in an operating system.
CO5: Evaluate memory management and device management techniques in an operating system.

Contents–

Unit	Content	Teaching Hours
1	**OS Introduction -** Objectives and Functions, Evolution of Operating system, The OS as a User/Computer Interface, OS as a resource manager, Operating System Structure, System Calls and Shell.	9
2	**Process Management:** Process concept, Process Description Process states, PCB, CPU scheduling, scheduling criteria, scheduling Algorithms, Thread: Process and Threads, Thread functionality, User level and Kernel.	9
3	**Process Synchronization and Deadlock -** Process Synchronization Principle of concurrency, Race condition, Critical Sections/Regions, Mutual Exclusion, Sleep and wakeup, Producer consumer problem, Semaphore, Monitors, Message Passing, Dining Philosopher Problem, Readers and writer's problem System model, Characterization, Deadlock Prevention Deadlock avoidance, Bankers Algorithm for single and multiple resources, Deadlock detection and recovery.	9

4	**File Systems -** Overview: File, File Management System, File System Architecture, File Management Functions, File Organization and access, File System Layout File Directories, File Sharing. Secondary Storage Management, File Allocation, Disk space management, File System Consistency and Performance.	9
5	**Memory Management & Device Management -** Memory Management Requirements: Relocation, Protection, Sharing, Logical & Physical Organization. Memory Partitioning, Fixed, Dynamic Partitioning, Buddy Systems, Relocation Fragmentation, Swapping, Managing, Page replacement Algorithms, Allocation of Frames, Managing free Memory, Paging, Segmentation, Thrashing, Principles of I/O Hardware, Principle of I/O software, Disk Scheduling Algorithms, Clocks	9

Text Books:

1. Abraham Silberschatz, Peter Galvin, "Operating System Concepts", 6th edition, Addison Wesley.
2. Andrew S. Tanenbaum, "Modern Operating Systems", Prentice Hall 3rd Edition.
3. Andrew S. Tanenbaum, "Operating System Design & Implementation", Second edition, Pearson Education.
4. William Stallings, "Operating systems", Prentice Hall, 4th Edition.

Reference Books:

1. Deital H.M., "Operating Systems", Addison Wesley, Addison Wesley.
2. William Stallings, "Operating systems internals and Design Principles", Pearson Education. 6th Edition.
3. Milan Milenkovic, “Operating System: Concepts & design” - TMH publication.
4. Dhamdhere, “Operating System -A Concept based approach” Third edition, Mc Graw Hill Publication.

Online Resources:

1.NPTEL course on Operating Systems .

Semester –I

Course Code: DCS23PCL104 **Course Name:** Database Management Systems **Course Category:** PCC
Credits:3 Teaching Scheme: L- 3 Hrs/week **Evaluation Scheme:** CA-40, MSE-20, ESE 40
Duration of Theory Exam: 2 Hrs
Pre-requisites: Basic Mathematics
Course Objectives: This course will enable students to
1. Understand architecture and functioning of database management systems
2. Acquaint with various normalization forms and query processing.
3. Use structured query language (SQL) and its syntax, transactions, database recovery and techniques for query optimization.
Course Outcomes: At the end of the course, the students will be able to -
CO1: Explain and justify the underlying concepts of database technologies.
CO2: Design and normalize a database schema for a given problem domain.
CO3: Implement database operations to populate, query, and enforce integrity constraints using commands.
CO4: Analyze the basics of transaction management and its significance.

Contents–

Unit	Content	Teaching Hours
1	**ER Model -**Entity Types, Entity sets, Attributes, Keys, Relationship Types, S Relationship Sets, Roles, Structural Constraints, Strong and Weak entity types, E-R diagram: o Naming Conventions and Design Issues, Relationship Types of Degree higher than two, The Enhanced ER Model: Subclasses, Super classes and Inheritance ,Specialization and Generalization, Data Abstraction	9
2	**Structured Query Language-** Introduction, Characteristics and advantages, Data types and literals, DDL, Tables: creating, modifying, deleting, Views: creating, dropping, Updation using views, DML, Operators, SQL DML queries, SELECT	9

	query and clauses. Set operations, Predicates and joins, Set membership, Tuple variables, Set comparison, Ordering of tuples, Aggregate functions, Nested queries	
3	**Set Theory & Function-** Relational Algebra, Unary Relational Operations, Relational Algebra Operations from set theory, Binary Relational Operations, Examples of Queries in Relational Algebra	**9**
4	**Normalization-** Normalization, Functional Dependencies, Normal Forms based on Primary Keys, General Definitions of Second and Third Normal Forms, Boyce-Codd Normal Form, Multi-valued Dependencies and 4NF	**9**
5	**Transaction Management** - Introduction to Transaction Processing ACID Properties of Transactions, Characterizing Schedules Based on Recoverability, Characterizing Schedules Based on Serializability, Concurrency Control, Concurrency Control Based on Lock Based Protocol, Deadlock Handling, Multiple Granularity, Timestamp Based Protocol, Validation Based Protocol	**9**

Text Books:

1. Abraham Silberschatz, Henry F. Korth, and S. Sudarshan, "Database System Concepts", McGraw Hill Education, 6th Edition, 2011.
2. Ramez Elmasri and Shamkant B. Navathe, "Fundamental Database Systems", Pearson Education, 7th Edition, 2015.

Reference Books:

1. Carlos Coronel, Steven Morris "Database systems: Design Implementation and Management", Cengage Learning Press, 11th Edition, 2014.
2. J. Murach, "Murach's MySQL", Shroff Publication, 2nd Edition, 2016.

Semester –I

Course Code: DCS23PCL105 **Course Name:** Introduction to Cyber Security **Course Category:** PCC
Credits:2 Teaching Scheme: L- 2 Hrs/week **Evaluation Scheme:** CA-40, MSE-20, ESE: 40
Duration of Theory Exam: 2 Hrs
Pre-requisites: Familiarity with Computers, Operating Systems, Basic Networking
Course Objectives: This course will enable students to
1. Introduce the core principles of cybersecurity, including the **CIA triad** (Confidentiality, Integrity, and Availability).
2. Help students recognize different types of cyber threats and attacks.
3. Introduce the concept of cryptography and its role in securing information and communication.
4. Explain the importance of network security and the concept of ethical hacking
Course Outcomes: At the end of the course, the students will be able to -
CO1: **Explain** key cybersecurity concepts, including the CIA Triad, cyber threats, and security frameworks.
CO2: **Describe** fundamental cybersecurity principles, threats, and attack methodologies.
CO3: **Demonstrate** cryptographic techniques, such as encryption and hashing, and **analyze** their role in data protection.
CO4: **Apply** network security practices and **evaluate** the role of cybersecurity professionals in ensuring system and network integrity through ethical hacking and incident response strategies.

Contents–

Unit	Content	Teaching Hours
1	**Introduction to Cybersecurity and Core Concepts -** Overview of Cybersecurity, The CIA Triad: Confidentiality, Integrity, and Availability, Key Cybersecurity Terms and Concepts, Types of Cybersecurity, Cybersecurity Governance, Importance of Cybersecurity in Today's World	6

2	**Cybersecurity Threats, Attacks, and Vulnerabilities-** Types of Cybersecurity Threats, Common Vulnerabilities, Attack Techniques, Case Studies of Real-World Cyberattacks-WannaCry Ransomware, Equifax Breach, Stuxnet..	**8**
3	**Basic Cryptography and Data Protection -** Introduction to Cryptography,Types of Cryptographic Techniques, Cryptographic Algorithms, AES, SHA, RSA, ECC, Public Key Infrastructure (PKI), Data Protection Techniques, Role of Cryptography in Cybersecurity.	**8**
4	**Network Security, Ethical Hacking, and Incident Response-** Introduction to Network Security**,** Network Security Protocols, Introduction to Ethical Hacking, Incident Response and Crisis Management, Security in Business Continuity, The Role of Cybersecurity in Protecting Organizational Assets	**8**

Text Books:

1. Michael E. Whitman and Herbert J. Mattord, "Principles of Information Security, Sixth Edition, Cengage Learning publication
2. Charles J. Brooks, Christopher Grow, Philip Craig, and Donald Short, "Cybersecurity Essentials". Wiley Publication,2017

Reference Books:

1. William Stallings, "Network Security Essentials: Applications and Standards",Sixth edition , Prentice Hall, 2007
2. P.W. Singer and Allan Friedman, "Cybersecurity and Cyberwar: What Everyone Needs to Know",Oxford University Press

Online Resources:

1.NPTEL course on Cyber Security and Privacy

Semester –I

Course Code: DCS23PCP101 Course Name: Fundamentals of Networking Lab **Course Category: PCC**
Credits: 1 **Teaching Scheme:** P- 2 Hrs/Week **Evaluation Scheme:** TW: 30, PR: 20
Pre-requisites: Fundamentals of programming logic
Lab Objectives: This course will enable students to
1.Identify and compare different network topologies
2.Demonstrate the setup and configuration of basic network devices, including routers, switches, and access points.
3.Explore and analyze various network protocols (e.g., TCP/IP, UDP, HTTP, FTP) and their roles in data transmission.
4. Differentiate between various types of network cables
Lab Outcomes: At the end of the course, the students will be able to -
LO1. Identify and assess different network topologies and select appropriate designs for specific scenarios.
LO2. Demonstrate the ability to configure routers, switches, and access points, ensuring proper connectivity and functionality.
LO3. Accurately design subnets and assign IP addresses according to best practices,
LO4. Effectively explain and apply various network protocols in practical situations,
LO5. Set up and configure a basic LAN, demonstrating proper device interconnectivity and functionality.

List of Experiments:

Sr. No.	List of Experiments
1	Introduction to Computer components.
2.	To study networking device: repeater, hub, switch, router and gateway.
3.	Write a c program to determine the IP address is in class A, B, C, D and E.
4.	Configuring a Basic Web Server to understand the concepts of subnetting and supernetting.
5.	Study of basic network commands: ipconfig, hostname, ping<ip_address>, tracert <ip_address>, netstat<ip_address>

6	To establish a straight over and a cross over cable in LAN
7.	Write a c program to translate dotted decimal IP address into 32 bit address.
8.	Creating workgroup of computers and resource sharing (file & printer)
9.	Study of client-server architecture.

Semester –I

Course Code: DCS23PCP102 **Course Name:** Information Security and Cryptography **Lab Course Category: PCC**
Credits: 2 **Teaching Scheme:** P- 4 Hrs/Week **Evaluation Scheme:** TW: 30, PR: 20
Pre-requisites: Fundamentals of programming logic
Lab Objectives: This course will enable students to
1. Build foundation in Information Theory fundamental concepts
2. Develop programming skills
3. Apply programming constructs to implement different Compression methods .
Lab Outcomes: At the end of the course, the students will be able to -
LO1. Apply knowledge of basic programming constructs to analyze entropy and information in digital transmission.
LO2. Implement and understand various encryption and compression methods
LO3. Write neat code for generating codewords for the message of size k bits
LO4. Analyze performance and efficiency of the Block code.
LO5. Analyze the password entropy based on character combination
LO6. Measure information leakage using entropy based methods and K-L Divergence

List of Experiments:

1. (a) Compute Shannon's entropy for the source which emits characters with certain probabilities (b) Compute information bits and entropy of the string message given the probabilities of the characters
2. (a) Write a program to generate Hamming Code (7,4) (b) Write a program using hamming code to detect and correct error in received codeword .
3. (a) Implement Simple Encryption & Decryption using Caesar cipher (b) Implement Simple Encryption & Decryption using XOR cipher
4. Develop a simple Huffman coding algorithm for text compression
5. Compress a text using Run-Length Encoding (RLE).

6. Implementing Lempel-Ziv-Welch (LZW) Compression for text
7. Create a program to encrypt and decrypt text using a One time pad (OTP)
8. Write a program to analyze password entropy based on character combinations
9. Write a program to Measure Redundancy in given Text
10. Implement Arithmetic Coding for compression
11. Measure information leakage using Kullback- Leibler divergence
12. Write a program to calculate Entropy-Based Data Leakage Detection
13. Write a program to Measure Kolmogorov complexity of a string to detect anomalies.
14. Use entropy analysis to detect phishing links URLs

Semester –I

Course Code: DCS23PCP103 **Course Name:** Operating Systems Lab **Course Category: PCC**
Credits: 1 **Teaching Scheme:** P- 2 Hrs./Week **Evaluation Scheme:** TW: 30, PR: 20
Pre-requisites: Fundamentals of operating systems
Lab Objectives: This course will enable students to
1.Understand various concepts of operating system related to process management and file systems
Lab Outcomes: At the end of the course, the students will be able to -
LO1. Apply knowledge of basic programming to implement UNIX system calls and file management.
LO2. Apply knowledge of basic programming to demonstrate various process related concepts.
LO3.Apply knowledge of programming to demonstrate various thread related concepts.
LO4. Apply knowledge of programming to simulate CPU scheduling algorithms: FCFS, SJF, and Round Robin.
LO5. Apply knowledge of programming to simulate Bankers Algorithm for Deadlock Avoidance.
LO6. Apply knowledge of programming to simulate implementation of Disk Scheduling Algorithms: FCFS, SSTF.

List of Experiments:

1. Write a C program to implement UNIX system calls and file management.
2. Write C programs to demonstrate various process related concepts.
3. Write C programs to demonstrate various thread related concepts.
4. Write C programs to simulate CPU scheduling algorithm: FCFS.
5. Write C programs to simulate CPU scheduling algorithm: SJF.
6. Write C programs to simulate CPU scheduling algorithms: Round Robin.
7. Write a C program to simulate Bankers Algorithm for Deadlock Avoidance.
8. Write C programs to simulate implementation of Disk Scheduling Algorithm: FCFS.
9. Write C programs to simulate implementation of Disk Scheduling Algorithm: SSTF.

Semester –I

Course Code: DCS23PCP104 **Course Name: D**atabase Management Systems Lab **Course Category: PCC**
Credits: 2 **Teaching Scheme:** P- 4 Hrs/Week **Evaluation Scheme:** TW: 30, PR: 20
Pre-requisites: Fundamentals of programming logic
Lab Objectives: This course will enable students to
1. Work on existing database systems, designing of database
2. Create relational databases, analysis of table design.
3. Apply programming constructs to implement different operations on tables .
Lab Outcomes: At the end of the course, the students will be able to -
LO1. Design a database schema for a given problem domain.
LO2. Practice and master DDL and DML through SQL
LO3. Demonstrate the use of constraints and relational algebra operations.

List of Experiments:

1. Design a Database and create required tables. For e.g. Bank, College Database
2. Apply the constraints like Primary Key , Foreign key, NOT NULL to the tables.
3. Write a sql statement for implementing ALTER,UPDATE and DELETE
4. Write the query for implementing the following functions: MAX(),MIN(),AVG(),COUNT()
5. Write the query to implement the concept of Integrity constraints.
6. Write the query to create the views
7. Perform the queries for triggers
8. Perform the following operation for demonstrating the insertion , updation and deletion using the referential integrity constraints
9. Write the queries to implement the joins
10. Implementation of PL/SQL

Semester –II

Course Code: DCS23PCL151 **Course Name:** Network Security and Firewalls **Course Category:** PCC
Credits: 3 Teaching Scheme: L- 3 Hrs/week **Evaluation Scheme:** CA-40, MSE-20, ESE: 40
Duration of Theory Exam: 2 Hrs
Pre-requisites: Basic Networking and Linux/Windows Operating Systems understanding
Course Objectives: This course will enable students to
1. Introduce students to network security threats and defenses.
2. Explain firewalls, VPNs, and intrusion detection systems.
3. Provide hands-on experience in configuring firewalls and security tools..
4. Teach basic penetration testing and network traffic analysis
Course Outcomes: At the end of the course, the students will be able to -
CO1 Understand network threats, its types and defenses
CO2 Understand Cryptographic Techniques for Network Security
CO3 Configure and Manage Firewalls
CO4 Implement and Analyze Intrusion Detection & Prevention Systems (IDS/IPS)

Contents–

Unit	Content	Teaching Hours
1	**Introduction to Network Security:** Definition and importance of network security, Key security principles: Confidentiality, Integrity, Availability (CIA Triad), Security challenges in modern networks, Malware (Viruses, Worms, Trojans, Ransomware, Spyware, Adware), Phishing and Social Engineering Attacks, Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks, Man-in-the-Middle (MITM) Attacks, Zero-Day Exploits and Advanced Persistent Threats (APT)	9
2	**Basics of Firewalls :** What is a Firewall? , Definition and importance of firewalls in cybersecurity, Firewall placement in network security architecture, Evolution of firewalls: From packet filtering to Next-Gen Firewalls (NGFWs) Types of Firewalls: Packet Filtering Firewalls (Stateless vs Stateful Inspection), Circuit-Level Gateways, Application	9

	Layer Firewalls (Proxy Firewalls), Stateful Firewalls, Next-Generation Firewalls (NGFWs), Cloud-based Firewalls (Firewall as a Service - FWaaS), Firewall Architectures & Deployment Strategies, Firewall Rules and Policies, Firewall Bypass Techniques & Countermeasures	
3	**Virtual Private Networks (VPNs):** Introduction to Virtual Private Networks (VPNs), Definition, protocols and tunnelling technologies , Types of VPNs : Remote Access VPN (SSL VPN, PPTP, L2TP), Site-to-Site VPN (IPSec VPN, GRE Tunnel), Hybrid VPNs (MPLS VPN, Cloud-based VPNs),	**9**
4	**Intrusion Detection & Prevention Systems (IDS/IPS)-** Role of IDS/IPS in cybersecurity, between IDS and IPS, IDS/IPS placement in network topology, Network-based IDS (NIDS) vs Host-based IDS (HIDS), Signature-based IDS vs Anomaly-based IDS, Inline vs Passive IDS/IPS, Introduction to Snort, Writing and Implementing Snort Rules, Traffic Analysis and Intrusion Detection using Wireshark, Machine Learning in Intrusion Detection ,Combining Firewalls, VPNs, and IDS/IPS for layered security**.**	**9**
5	**Network Security Tools & Penetration Testing-** importance of security tools in cybersecurity, Overview of penetration testing (Ethical Hacking vs Malicious Hacking), Penetration Testing Methodologies (OSSTMM, PTES, NIST), Legal and Ethical considerations in penetration testing, Whois & Nslookup for domain information gathering, theHarvester: Email & subdomain enumeration, Types of scans (TCP SYN Scan, UDP Scan, OS Detection) ,Detecting open ports, services, and vulnerabilities	**9**

Text Books:

1. William Stallings, “Network Security Essentials: Applications and Standards” , Pearson publication , sixth edition (2017)
2. Michael Stewart, “Network Security, Firewalls, and VPNs” , Jones & Bartlett Learning, second edition (2020)

Reference Books:

1. "Hacking Exposed: Network Security Secrets & Solutions" – Stuart McClure, Joel Scambray, & George Kurtz
2. "The Web Application Hacker’s Handbook: Finding and Exploiting Security Flaws" – Dafydd Stuttard & Marcus Pinto

Online Resources:

1. Cisco Certified Network Associate (CCNA) – Security
2. Certified Information Systems Security Professional (CISSP)

Semester –II

Course Code: DCS23PCL152 **Course Name:** Advanced Cryptography **Course Category:** PCC
Credits: 3 Teaching Scheme: L- 3 Hrs/week **Evaluation Scheme:** CA-40, MSE-20, ESE: 40
Duration of Theory Exam: 2 Hrs
Pre-requisites: Basic Maths, probability and statistics
Course Objectives: This course will enable students to
1. Explore advanced cryptographic algorithms.
2. Understand public-key cryptography, digital signatures, and hash functions.
3. Learn about real-world cryptographic applications in cybersecurity
Course Outcomes: At the end of the course, the students will be able -
CO1 To Understand modern cryptographic algorithm designs
CO2 To implement various hash functions
CO3 To implement coding for secure communication
CO4 To apply cryptography techniques for handling security issues in digital communication

Contents–

Unit	Content	Teaching Hours
1	**Introduction to Advanced Cryptography:** Overview of Modern Cryptography Types of Cryptographic Algorithms: Symmetric & Asymmetric, Operations used by Encryption Algorithms , RSA algorithm ,PGP, one-way hashing , advantages and disadvantages of these methods	9
2	**Public Key Cryptography:** Elliptic Curve Cryptography (ECC) Basics, Key Exchange Protocols (Diffie-Hellman), Secure communication using Chaos Functions , Biometric Encryption , Cryptanalysis	9
3	**Cryptographic Hash Functions:** Properties of Hash Functions (MD5, SHA-256, SHA-3), Implementing Message Authentication Codes (HMAC).	9

4	**Digital Signatures & Certificates-** How Digital Signatures Ensure Authenticity, RSA & DSA Signature Schemes, PKI (Public Key Infrastructure) and SSL/TLS	**9**
5	**Quantum Cryptography & Future Trends -** Introduction to Quantum Cryptography (QKD), Post-Quantum Cryptography Techniques, Future Trends in Encryption & Security	**9**

Text Books:

1. William Stallings – Cryptography and Network Security: Principles and Practice, 8th Edition, Pearson, 2022.
2. Behrouz A. Forouzan, Debdeep Mukhopadhyay – Cryptography and Network Security, 3rd Edition, McGraw-Hill, 2019.

Reference Books:

1. Delfs, Knebl – Introduction to Cryptography: Principles and Applications, 3rd Edition, Springer, 2015.
2. Jonathan Katz, Yehuda Lindell – Introduction to Modern Cryptography, 3rd Edition, CRC Press, 2020.
3. Nigel Smart – Cryptography Made Simple, 1st Edition, Springer, 2016.

Online Resources:

1. Introduction to Cryptography by NPTEL (IIT Kharagpur) – Prof. Debdeep Mukhopadhyay
2. Applied Cryptography by University of Washington (Coursera)
3. Cryptography by Stanford University (Coursera) – Dan Boneh

Semester –II

Course Code: DCS23PCL153 **Course Name:** Software Engineering & Security Testing Course **Category:** PCC
Credits:3 Teaching **Scheme:** L- 3 Hrs./week Evaluation **Scheme:** CA–40,MSE: 20, ESE–40
Duration of Theory Exam: 2 Hrs.
Pre-requisites: Knowledge of computer fundamentals and software types
Course Objectives: This course will enable students
1. To understand software lifecycle development models.
2.To understand and apply software requirements engineering techniques, software design principles, modeling.
3. To understand the use of metrics in software engineering.
4. To understand software project management.
Course Outcomes: At the end of the course, the students will be able to -
CO1: Explain basic computer engineering concepts through the Software Development Life Cycle (SDLC) and software engineering models.
CO2: Apply design concepts to develop software systems.
CO3: Implement and analyze basic software testing strategies.
CO4: Identify and evaluate security risks in software applications.
CO5: Recommend remediation strategies to enhance the overall security of software applications.

Contents–

Unit	Content	Teaching Hours
1	**Software Development Process:** Software crisis and myths, Software process and development: Generic view of process, Software life cycle and models, Analysis and comparison of various models, an agile view of process.	9

2	**Requirement Engineering:** Requirements engineering tasks, initiating requirement engineering process, eliciting requirement, Building the analysis model, Negotiating and validating requirement, Building the analysis model.	9
3	**System Design Overview:** Design process and design quality, Design concepts, Design model, Pattern based software design, Architectural design, User interface design. UML: Different methods: Rumbaugh / Booch / Jakobsons, Need for standardization. Developing diagrams in UML (Use CASE, Class, Interaction, and State Diagrams) CASE TOOLS.	9
4	**Validation and Testing:** Strategic approach to Software testing, Strategic issues, Test strategies for conventional software, Validation testing, System testing, Debugging. White box testing and Black box testing.	9
5	**Security Testing –** Introduction to security testing, security testing importance, security testing types, goals of security testing, security testing principles, security testing tools, Best Practices for Effective Security Testing, advantages and disadvantages of security testing.	9

Text Books:

1. Roger S. Pressman, “Software Engineering”, Tata McGraw-Hill
2. G. Booch, J. Rumbaugh, and I. Jacobson, “The Unified Modeling Language User Guide”, Addison Wesley
3. K.K.Aggarwal , Yogesh Singh , “Software Engineering” , New Age International Publishers
4. Bruce Maxim, Roger Pressman, “Software Engineering: A Practitioner's Approach”

Reference Books:

1.Shari Pfleeger, “Software Engineering”, Pearson Education

2.Ian Sommerville, “Software Engineering”, Pearson Higher Education

3.Pankaj Jalote, “An Integrated Approach to Software Engineering”, Springer New York

4.Mall Rajib,” Fundamentals of Software Engineering”, PHI Learning

5.**"Software Testing Series - Security Testing"** by Michael Pasono.

Online Resources:

1.NPTEL course on Software Engg and Software Testing

Semester –II

Course code: DCS23PCL154 **Course name:** Digital Forensics **Course category:** PCC
Credits: 3 **Teaching scheme:** L-3 hrs per **Evaluation scheme:** CA–40, MSE–20, ESE–40
Pre-requisites: Basic understanding of computer systems, including operating systems, file structures, and data storage.
Course Objectives:
1. Students will develop skills in digital evidence handling and forensic analysis.
2. Students will gain knowledge of computer crime investigation techniques and forensic tools.
Course Outcomes: At the end of the course, the students will be able to –
CO1: Students will acquire the skills to identify, preserve, analyze, and present digital evidence, understand the forensics process, and apply computer forensics in legal and cybersecurity contexts.
CO2: Students will learn to assess, acquire, analyze, and report on digital evidence in computer crime investigations.
CO3: Students will understand digital evidence, the first responder toolkit, forensic challenges, investigation types, and forensic techniques.
CO4: Students will understand the internal structure of hard disk drives, the booting process, and file systems.

Contents –

Unit	Content	Teaching hours
1	**Unit 1: COMPUTER FORENSICS** Introduction, Evolution Of Computer Forensics, Stages Of Computer Forensics Process, Benefits Of Computer Forensics, Uses Of Computer Forensics, Objectives Of Computer Forensics, Role Of Forensics Investigator, Forensics Readiness	9
2	**Unit 2: COMPUTER FORENSICS INVESTIGATION PROCESS:** Introduction To Computer Crime Investigation, Assess The Situation, Acquire The Data, Analyze The Data, Report The Investigation	9
3	**UNIT 3: DIGITAL EVIDENCE AND FIRST RESPONDER PROCEDURE:** Digital Evidence, First Responder Toolkit, Issues Facing Computer Forensics, Types Of Investigation, Techniques Of Digital Forensics	9
4	**UNIT 4: UNDERSTANDING STORAGE MEDIA** Introduction to Storage Media in Cybersecurity, Hard Disk Drive (HDD) Structure and working principle of HDD: Internal Architecture of HDD, Data Storage Mechanism, Storage-Related Security Threats,Emerging Storage Technologies; Security,Digital Forensics and HDD	9
5	**Unit 5: UNDERSTANDING FILE SYSTEM** Booting Process in Cybersecurity Context, BIOS and UEFI Security, Boot-Level Attacks,Boot Security Mechanisms,Introduction to File Systems,Types of File Systems and Security Features,File System Security Concepts, File Allocation & Vulnerabilities,Disk Partitioning and Security,Incident Response, Forensics	9

Text Books: 1. Warren G. Kruse II and Jay G. Heiser, "Computer Forensics: Incident Response Essentials", Addison Wesley, 2002.
2. Dr. Jeetendra Pande, Dr. Ajay Prasad, "DIGITAL FORENSICS "
Reference Books: 1. Vacca, J, Computer Forensics, Computer Crime Scene Investigation, 2nd Ed, Charles River Media, 2005, ISBN: 1-58450-389.
Online Resources: 1. NPTEL / SWAYAM lectures.

Semester –II

Course Code: DCS23PCL155	**Course Name:** Ethical Hacking	**Course Category:** PCC
Credits: 2 Teaching Scheme: L- 2 Hrs/week **Evaluation Scheme:** CA-40, MSE: 20, ESE-40		
Duration of Theory Exam: 2 Hrs		
Pre-requisites: Basic Computer Knowledge, Networking Fundamentals, Cybersecurity Basics		
Course Objectives: This course will enable students		
1. To understand the fundamentals of ethical hacking		
2. To understand exploitation methodologies.		
3.To identify and understand vulnerabilities of web applications and wireless networks.		
4. To understand legal and career aspects of ethical hacking		
Course Outcomes: At the end of the course, the students will be able to -		
CO1 Assess and explain network security fundamentals, identify vulnerabilities, and understand the ethical and legal considerations involved in hacking..		
CO2 Use common ethical hacking tools and techniques to perform security assessments and exploit vulnerabilities.		
CO3 Secure web applications and wireless networks, identifying vulnerabilities, and applying practical measures to mitigate security risks.		
CO4 Conduct ethical hacking assessments in a structured manner, adhere to legal and ethical standards, and explore career opportunities in the cybersecurity field.		

Contents–

Unit	Content	Teaching Hours
1	**Introduction to Ethical Hacking and Network Security -** Introduction to Ethical Hacking - Definition and scope, Key principles of ethical hacking, Five phases of hacking, Understanding Network Security - Basics of networking, Network protocols, Network devices, Common network vulnerabilities and security measures, Types of Cybersecurity Attacks, Network Defense Mechanisms - IDS, IPS, Network security tools and devices, Ethical and Legal Considerations - Laws and regulations governing	8

	ethical hacking(Computer Fraud and Abuse Act, GDPR, etc.)	
2	**Hacking Techniques and Tools -** Overview of penetration testing: The process, methodology, and objectives, Phases of penetration testing: Information gathering, vulnerability scanning, exploitation, post-exploitation, and reporting, Differences between black box, white box, and gray box penetration testing, Methods for gathering information on targets (WHOIS, DNS records, public information), Tools for information gathering: Nmap, Maltego, Netcat, OSINT (Open-Source Intelligence) gathering techniques, Network scanning techniques: port scanning, IP scanning, and identifying open ports and services Tools for scanning, Introduction to exploitation, Exploiting vulnerabilities, common Ethical Hacking Tools, Vulnerability Assessment and Reporting	**10**
3	**Web Application and Wireless Network Security -** Introduction to web application security, Common web application vulnerabilities, Techniques for exploiting and preventing the top 10 vulnerabilities, Web Application Penetration Testing, Basics of wireless networking, Wireless network attacks, Aircrack-ng, Wireless Network Defense-How to secure Wi-Fi networks from common attacks, Use of VPNs and firewalls to protect wireless communication.	**6**
4	**Ethical Hacking Lifecycle, Legal Aspects, and Career Pathways-** Ethical Hacking Lifecycle, Incident Response and Post-Breach Activities: Incident response process: Identification, containment, eradication, and recovery, Introduction to digital forensics: Gathering and analyzing evidence from security incidents, Post-breach analysis: Identifying root causes and strengthening defenses to prevent future attacks, Legal Aspects of Ethical Hacking, Career Pathways in Ethical Hacking Ethical Responsibilities and Professional Conduct.	**6**

Text Books:

1. Dafydd Stuttard, Marcus Pinto, "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" Wiley (3rd Edition, 2021).
2. Jon Erickson, "Hacking: The Art of Exploitation"

Reference Books:

1. Peter Kim,"The Hacker Playbook 3: Practical Guide To Penetration Testing"CreateSpace Independent Publishing (2018)
2. Rohit Tamma, Ankit Fadia, ."Ethical Hacking and Penetration Testing Guide"McGraw-Hill Education (1st Edition, 2017)

Online Resources:

1.NPTEL course on Ethical Hacking

Semester –II

Course Code: DCS23PCP151 **Course Name:** Network Security and Firewalls Lab **Course Category: PCC**
Credits: 1 **Teaching Scheme:** P- 2 Hrs/Week **Evaluation Scheme:** TW: 30, PR: 20
Pre-requisites: Fundamentals of networking and Operating Systems
Lab Objectives: This course will enable students to
1. Understand basic network security concepts
2. Install and configure Wireshark, Nmap
3. Understand firewall rules and policies
Lab Outcomes: At the end of the course, the students will be able to -
LO1. Capture, analyze, and interpret network traffic and security threats.
LO2. Configure Windows/Linux firewalls and apply basic access control rules.
LO3. Enable Deep Packet Inspection (DPI) to analyze and filter malicious traffic
LO4. Write and apply custom Snort rules to detect attacks such as DoS, brute force, and malware infections
LO5. Conduct network scanning and vulnerability assessment using Nmap, Nessus, and OpenVAS
LO6. Analyze and test firewall evasion techniques such as fragmentation and tunneling

List of Experiments:

1. Perform deep network scanning to identify open ports, running services, and vulnerabilities using nmap
2. Detecting Live Hosts in a Network by Identifying active devices in a subnet using ARP and ICMP scanning.
3. Firewalls and Packet Filtering with Configuring Linux Firewall with iptables
4. Configure a secure VPN tunnel using OpenVPN.
5. Deploying Snort for Network Intrusion Detection
6. Performing SQL Injection Testing

7. Analyzing HTTPS Traffic Using Wireshark
8. Simulating a Secure Network in Cisco Packet Tracer
9. Advanced password recovery & cracking
10. Web security testing & vulnerability analysis

Semester –II

Course Code: DCS23PCP152 **Course Name:**Advanced Cryptography Using C Lab **Course Category: PCC**
Credits: 1 **Teaching Scheme:** P- 2 Hrs/Week **Evaluation Scheme:** TW: 30, PR: 20
Pre-requisites: Fundamentals of Basic Programming logic
Lab Objectives: This course will enable students to
1. Explore the fundamentals of symmetric and asymmetric encryption
2. Understand cryptographic hashing, digital signatures, and key exchange mechanisms.
3. Demonstrate Elliptic Curve Cryptography (ECC) for encryption.
Lab Outcomes: At the end of the course, the students will be able to -
LO1. Understanding and Implementing Cryptographic Algorithms.
LO2. Apply TLS/SSL encryption for securing online communications..
LO3. Evaluate the vulnerabilities of cryptographic algorithms through cryptanalysis techniques.
LO4. Perform attacks on weak encryption methods and analyze the effectiveness of security countermeasures.
LO5. Develop custom encryption techniques for specific use cases.
LO6.Understand and implement next-generation cryptographic methods (Post-Quantum Cryptography, Zero-Knowledge Proofs, etc.).

List of Experiments:

1. **Implementation of Classical Ciphers** Implement Caesar Cipher, Vigenère Cipher, and Playfair Cipher for encryption and decryption.
2. **Implementation of ElGamal Cryptosystem** Develop a program for secure key exchange and encryption using the ElGamal algorithm.
3. **Implementation of Elliptic Curve Cryptography (ECC)** Implement ECC for secure communication and key exchange.
4. **Password Hashing and Secure Storage** Implement salting, peppering, and PBKDF2 password hashing to store passwords securely.

5. **Implementation of Digital Signature Algorithm (DSA)** Develop a digital signature system using DSA for message verification.
6. **Implementation of ECDSA (Elliptic Curve Digital Signature Algorithm)** Implement ECDSA for secure signing and verification of messages.
7. **Implementation of Diffie-Hellman Key Exchange** Develop a secure key exchange system using Diffie-Hellman.
8. **Implementation of SSL/TLS Encryption** Simulate TLS encryption for a secure client-server chat application.
9. **Implementation of PGP Encryption for Email Security** Write a program to encrypt and decrypt emails using PGP (Pretty Good Privacy).
10. **Implementation of Homomorphic Encryption** Develop a basic homomorphic encryption system (Paillier cryptosystem) for performing
11. Implementation of Zero-Knowledge Proofs (ZKP) Simulate a ZKP authentication system using a mathematical proof without revealing the secret.
12. Implementation of Post-Quantum Cryptography (Lattice-based Cryptosystem) Implement a simple lattice-based cryptosystem for quantum-safe encryption.
13. Cryptanalysis of Classical Ciphers Perform brute-force attacks and frequency analysis on Caesar and Vigenère ciphers.
14.Side-Channel Attack Simulation Demonstrate timing attacks or power analysis on RSA encryption.

Semester –II

Course Code: DCS23PCP153 **Course Name:** Software Engineering and Security Testing Lab **Course Category:** PCC
Credits: 1 **Teaching Scheme:** P- 2 Hrs./Week **Evaluation Scheme:** TW: 30, PR: 20
Pre-requisites: Computer awareness
Lab Objectives: This course will enable students to
1.Build foundation in software development
2. Understanding software testing importance.
3. Applying software testing tools for security testing.
Lab Outcomes: At the end of the course, the students will be able to -
LO1. Students will understand the importance of SRS.
LO2. Students will understand Matrix multiplication and introspect the causes for its failure.
LO3. Students will understand ATM system and study its specifications using various UML diagram
LO4. Students will understand Database Security Testing
LO5. Students will understand Cloud Data Testing.
LO6. Students will understand Static Application Security Testing (SAST).

List of Experiments:

1. Study of Security Requirement Service
2. Write a program in C for Matrix multiplication and check its failure, also introspect the causes for its failure and write down the possible reasons for its failure.
3. Take the system ATM system and study its system specifications and draw the various UML diagrams.
4. Apply security testing tools for Database Security Testing.
5. Apply security testing tools and cloud data testing.
6. Apply security testing tools for static application security testing.
7. Apply security testing tools for Network Vulnerability Assessment and Penetration Testing.

8. Perform Web Application Security Testing using security testing tools.

Semester –II

Course code: DCS23PCP154 Course name: Digital Forensics Lab **Course category:** PCC
Credits: 1 **Teaching scheme:** P-2 hrs/week **Evaluation scheme:** TW–30, PR–20
Pre-requisites: Basic understanding of computer systems, including operating systems, file structures, and data storage.
Lab Objectives:
1. To apply forensic investigation techniques for email, internet history, and smartphone data analysis.
2. To demonstrate proper digital evidence collection and preservation methods.
3. To compare and evaluate forensic tools for data recovery and analysis.
Lab Outcomes: On the successful completion of this course Students will be able to:
LO1: Investigate and analyze digital forensic cases using appropriate tools.
LO2:Collect and preserve digital evidence while maintaining integrity.
LO3: Perform forensic imaging, file system analysis, and data recovery effectively.

List of Experiments:

1	**Types of Digital Investigations** Investigate and analyze different types of digital forensics cases such as email analysis, internet history recovery, and smartphone data extraction.
2	**Digital Evidence Collection and Preservation** Experiment on how to properly collect and preserve digital evidence from a computer system while maintaining chain of custody
3	**Digital Forensics Tools Comparison** Compare and evaluate different digital forensics tools (e.g., Autopsy, Sleuth Kit, X1) for their effectiveness in recovering and analyzing digital evidence.
4	**Data Recovery from Deleted Files**Conduct a practical experiment to recover deleted files from a formatted or damaged hard drive using recovery tools
5	**HDD Internal Structure Exploration** Examine the internal structure of a hard disk drive, including sectors, clusters, and partitions, using forensic tools like FTK Imager or EnCase.
6	**Incident Response Simulation**

	Perform a simulation of a computer crime scenario, assessing the situation, acquiring data, analyzing it, and reporting findings.
7	**First Responder Toolkit Setup and Use** Set up and utilize a first responder toolkit for collecting digital evidence from a live system, including identifying volatile data.
8	**Boot Process Analysis** Study the boot process of a computer and how it can be used for forensic investigation, including examining boot logs and BIOS configurations.
9	**File System Analysis** Analyze different file systems (e.g., FAT, NTFS, EXT) to understand their structures, data storage methods, and how files are stored and retrieved.
10	**Forensic Imaging of a Hard Disk Drive (HDD)** Conduct an experiment to create a forensic image of a hard disk drive using write-blockers to ensure data integrity.

Semester –II

Course Code: DCS23SEC151 **Course Name:** Basics of Python Programming **Course Category: SEC**
Credits: 2 **Teaching Scheme:** P- 4 Hrs/Week **Evaluation Scheme:** TW: 30, PR: 20
Pre-requisites: Fundamentals of programming logic
Lab Objectives: This course will enable students to
1. Build foundation in python programming.
2. Develop programming skills.
3. Apply python programming constructs to solve real world problems.
Lab Outcomes: At the end of the course, the students will be able to -
LO1: Write and execute basic Python programs using input/output functions and fundamental syntax.
LO2: Demonstrate proficiency in using Python data types, type conversion, and different operators for arithmetic, logical, and relational operations.
LO3: Apply conditional statements (if-else, if-elif-else) and loop constructs (for, while) to solve problems effectively.
LO4: Apply the concept of functions, function parameters, return values, and recursion in Python.
LO5: Perform hands-on experience in performing various string and list operations, such as slicing, searching, and modifying elements.
LO6: Create and manipulate dictionaries, store key-value pairs, and apply them in real-world scenarios such as a phonebook application.

List of Experiments:

1. Write a Python program to print "Hello, World!" and display the Python version being used.
2. Write a Python program to take input from the user (name and age) and print a greeting message.
3. Write a Python program to swap two numbers without using a temporary variable.
4. Write a Python program to demonstrate different data types (int, float, string, list, tuple, dictionary, set) and print their types.

5. Write a Python program to perform arithmetic operations (+, -, *, /, //, %,) on two numbers entered by the user.
6. Write a Python program to compare two numbers using relational operators and display appropriate messages.
7. Write a Python program to check whether a given number is even or odd using an if-else statement.
8. Write a Python program to check if a number is positive, negative, or zero using an if-elif-else statement.
9. Write a Python program to find the largest among three numbers entered by the user.
10. Write a Python program to print the first N natural numbers using a for loop.
11. Write a Python program to print the multiplication table of a given number using a while loop.
12. Write a Python program to check whether a given number is prime or not.
13. Write a Python program to define a function that takes two numbers as parameters and returns their sum, difference, product, and quotient.
14. Write a Python program to define a recursive function to calculate the factorial of a number.
15. Write a Python program to perform string operations like concatenation, slicing, length, and reversing a string.
16. Write a Python program to check whether a given string is a palindrome or not.
17. Write a Python program to find the maximum and minimum elements in a list of numbers.
18. Write a Python program to remove duplicates from a list and display the modified list.
19. Write a Python program to demonstrate the use of a dictionary by creating a phonebook that stores names and phone numbers. Allow users to search for a contact.
20. Write a Python program to demonstrate tuple operations like indexing, slicing, and concatenation.

Semester –III

Course Code: DCS23PCL201 Course Name: Network Threat Management Techniques **Course Category:** PCC
Credits:3 Teaching Scheme: L- 3 Hrs/week **Evaluation Scheme:** CA–40, MSE–20, ESE–40
Duration of Theory Exam: 2 Hrs
Pre-requisites: Basic knowledge of computer fundamentals, computer networks, network devices, Awareness of cybersecurity fundamentals
Course Objectives: This course will enable students to
1. Understand common network threats and attack vectors.
2. Identify vulnerabilities in wired and wireless networks.
3. Use tools for detecting and analyzing network threats.
4. Implement network security controls and countermeasures.
5. Respond to and manage network security incidents.
6. Apply best practices for continuous network threat management.
Course Outcomes: At the end of the course, the students will be able to -
CO1: Identify and classify different types of network threats and attacks.
CO2: Analyze network traffic to detect suspicious or malicious activities.
CO3: Apply network security tools and techniques to prevent and mitigate threats.
CO4: Manage network security incidents using standard incident response practices.

Contents–

Unit	Content	Teaching Hours
1	Overview of computer networks, Basics of network security, Security principles: CIA Triad, Concepts of threat, vulnerability, and risk, Introduction to cyber threat landscape, Importance of network security in organizations.	**9**
2	Types of network threats: Internal and external threats, Active and passive attacks, Common attack vectors, Malware-based attacks: Virus, worm, trojan, ransomware, Overview of modern attack scenarios.	**9**

3	Network attacks: DoS and DDoS, Man-in-the-Middle attack, ARP spoofing, IP spoofing, DNS spoofing, Packet sniffing concepts, Basics of intrusion detection, Network traffic monitoring concepts.	**9**
4	Firewalls and firewall types, Intrusion Prevention Systems (IPS), Network segmentation and VLANs, Secure communication protocols: HTTPS, SSH, VPN, Access control mechanisms, Patch management and updates, Best practices in network hardening.	**9**
5	Incident response lifecycle, Network security incident handling, Log analysis basics, Network forensics overview, Documentation and reporting, Legal and ethical considerations, Emerging threats (APT, Zero-day - overview)	**9**

Text Books:

3. Stallings, W. . Network security essentials: Applications and standards.
2. Stallings, W. . Cryptography and network security: Principles and practice

Reference Books:

1. Menezes, B. Network security and cryptography.
2.Kaufman, C., Perlman, R., & Speciner, M. Network security: Private communication in a public world.
3. Whitman, M. E., & Mattord, H. J. Principles of information security

Online Resources:

1. NPTEL / SWAYAM lectures.

Semester –III

Course Code: DCS23PCL202 **Course Name:** Computer and Mobile Forensics **Course Category:** PCC
Credits: 3 Teaching Scheme: L- 3 Hrs/week **Evaluation Scheme:** CA–40, MSE–20, ESE–40
Duration of Theory Exam: 2 Hrs
Pre-requisites: Basics of programming concepts and file systems Awareness of cyber security concepts and cyber laws
Course Objectives: This course will enable students to
5. To introduce students to the principles and processes of computer and mobile forensics, including cybercrimes, digital evidence, and standard investigation methodologies
6. To develop practical skills in acquiring, analyzing, and reporting digital evidence from computer systems and mobile devices using forensic tools while following legal and ethical practices.
Course Outcomes: At the end of the course, the students will be able to -
CO1 Understand and explain the fundamentals of computer forensics, types of cybercrimes, digital evidence characteristics, and standard forensic investigation procedures
CO2 Apply appropriate computer forensic techniques and tools for evidence acquisition, analysis, documentation, and reporting in cybercrime investigations.
CO3 Analyze mobile devices and associate evidence by following standard mobile forensic processes including seizure, preservation, and data acquisition techniques
CO4 Evaluate and interpret mobile forensic artifacts such as calls, messages, application data, and multimedia evidence to prepare professional forensic reports.

Contents–

Unit	Content	Teaching Hours
1	**Introduction to Computer Forensics:** Definition, objectives, and scope of computer forensics; Types of cybercrimes and digital evidence; Digital evidence characteristics and challenges; Principles of computer forensics: integrity, authenticity, chain of custody; Computer forensic investigation overview.	7
2	**Computer Crime Scene Investigation & Evidence Handling:** Computer crime scene investigation process, Roles of forensic investigator and incident response team: Evidence identification, collection, and preservation; Chain of custody documentation; Legal and ethical issues in computer forensics.	8

3	**Computer Forensic Tools, Analysis and Reporting:** Types of computer forensic tools (software and hardware), Disk imaging and data acquisition techniques, File system basics and deleted file recovery, Log analysis and timeline reconstruction, Forensic documentation and report writing.	**7**
4	**Fundamentals of Mobile Forensics:** Introduction, scope, and challenges of mobile forensics; Mobile device architecture and evidence types, Mobile operating systems overview (Android, iOS), Mobile forensic process and investigation phases, Legal considerations in mobile forensics.	**8**
5	**Mobile Evidence Acquisition Techniques:** Mobile device seizure and preservation techniques, SIM card and memory card forensics: Logical, physical, and file system acquisition, Live and post-mortem acquisition, Data integrity and validation.	**7**
6	**Mobile Forensic Analysis, Tools and Reporting:** Extraction and analysis of calls, SMS, contacts, and media; Application and social media artifact analysis, Overview of mobile forensic tools, Cloud and backup basics, Mobile forensic reporting and expert testimony	**8**

Text Books:

3. Jones, J. (2013). Computer forensics: Computer crime scene investigation (3rd ed.). Jones & Bartlett Learning.
4. Tamma, R., Mahalik, H., & Skulkin, O. (2022). Mobile forensics. Packt Publishing.

Reference Books:

3. Nelson, B., Phillips, A., & Steuart, C. (2018). Guide to computer forensics and investigations (6th ed.). Cengage Learning
4. Newman, R. C. (2007). Computer forensics: Evidence collection and management. Auerbach Publications.
5. Tamma, R., Skulkin, O., Mahalik, H., & Bommisetty, S. (2019). Practical mobile forensics (3rd ed.). Packt Publishing.
6. Easttom, C. (2020). An in-depth guide to mobile device forensics (2nd ed.). Cengage Learning.

Online Resources:

3. MIT OpenCourseWare – Information Theory
4. Stanford University – Cryptography Course

Semester –III

Course Code: DCS23PCL203 **Course Name:**Dark Web OSINT Investigation **Course Category:** PCC
Credits: 3 Teaching **Scheme:** L- 3 Hrs./week **Evaluation Scheme:** CA–40, MSE–20, ESE–40
Duration of Theory Exam: 2 Hrs.
Pre-requisites: Basic Understanding of Operating System , Computer Hardware and Internet usage
Course Objectives: This course will enable students to
1. Introduce students to the concepts of Open Source Intelligence (OSINT) and its role in cybercrime and digital investigations.
2. Familiarize students with the structure of the Internet, including the Surface Web, Deep Web, and Dark Web.
3. Train students to use legal and ethical OSINT techniques for collecting intelligence from open and dark web sources
4. Develop the ability to evaluate the credibility and authenticity of OSINT data sources, including anonymous and dark web platforms, using established credibility indicators
5. Prepare basic OSINT investigation reports and comply with legal and ethical guidelines during dark web investigations.
Course Outcomes: At the end of the course, the students will be able to -
CO1: Explain the fundamentals of OSINT, cybercrime, and dark web environments
CO2: Differentiate between the Surface Web, Deep Web, and Dark Web, and describe their uses and risks.
CO3: Apply ethical and legal OSINT methods to collect publicly available information related to dark web investigations**.**
CO4: Analyze and validate the credibility of information obtained from dark web and open sources using OSINT verification indicators.
CO5: Prepare basic investigation reports and comply with legal and ethical guidelines while performing OSINT-based dark web investigations.

Contents–

Unit	Content	Teaching Hours
1	**Introduction to OSINT and Cybercrime**: Intelligence, Types of Intelligence, Historical evolution of OSINT , OSINT Lifecycle (Planning, Collection, Processing, Analysis, Reporting), opensource v/s classified information, OSINT principles, Overview of cybercrime and cybercriminal behavior, Role of OSINT in cybercrime investigation and law enforcement, OSINT data sources	9
2	**Internet Architecture and Dark Web Ecosystem:** Logical and physical structure of the Internet, Role of ISPs, servers, clients, and routing, Domain Name System (DNS) , functional overview, Centralized vs decentralized web architecture, Layered Web Architecture, Working Principle of TOR network , Purpose of the Tor network, Onion routing concept, Multi-layer encryption (conceptual explanation), Entry, relay, and exit nodes (overview only), Limitations and risks of Tor usage, Comparative overview of Surface Web, Deep Web and Dark Web, Need for Dark Web OSINT Investigation	9
3	**Building OSINT Skills and Workflow Process**: Role of an OSINT investigator, understanding investigation objectives, defining scope and constraints, OSINT workflow stages: Requirement identification, Information collection, Data validation, Analysis and correlation, Reporting and review, Ethics Legal skills and knowledge for OSINT investigation , planning an OSINT investigation and Information Collection Techniques	9
4	**Data Organization, Documentation and Evidence Handling**: Importance of structured data handling, Types of OSINT data, File naming conventions and folder structures, Importance of documentation in investigations, maintaining investigation logs, Manual vs digital logs, avoiding bias in documentation, Primary vs secondary sources, evaluating source authenticity, Credibility indicators (Consistency, Reputation, Corroboration), Handling anonymous and dark web sources	9
5	**OSINT Analysis, Correlation and Reporting**: Pattern recognition in OSINT data, Behavioral patterns, Repeated identifiers (usernames, emails, wallets),Temporal and spatial relationships, Need for verification in OSINT, Multiple-source validation, Triangulation of information, Avoiding confirmation bias, Meaning of correlation in OSINT, Purpose of correlation in investigations, Classification of correlation techniques: Temporal correlation (time-based events), Entity-based correlation (people, usernames, accounts),Content-based correlation (text, images, keywords),Platform-based correlation (cross-platform presence), advantages and disadvantages of Manual vs automated correlation (conceptual) ,	9

	Structure of an OSINT analytical report, Presenting correlated findings, Ethical and legal considerations in reporting	

Text Books:

5. Bazzell, M. (2023). Open source intelligence techniques: Resources for searching and analyzing online information (10th ed.). IntelTechniques.
6. Bhardwaj, A. (2021). A practical approach to open source intelligence (OSINT) (Vol. 1). BPB Publications.

Reference Books:

5. Belapure, Godbole, N. (2017). Cyber security: Understanding cybercrimes, computer forensics and legal perspectives. Wiley India.
6. Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers and the internet (3rd ed.). Academic Press

Online Resources: NPTEL/SWAYAM E-learning resources

1. Digital Forensics : https://onlinecourses.swayam2.ac.in/nou25_cs19/preview
2. Computer Fraud : https://onlinecourses.swayam2.ac.in/ini26_cm08/preview
3. https://inteltechniques.com/services.html

Semester –III

Course Code: DCS23PCL204 **Course Name: Cyber Laws and Cyber Ethics Course Category:** PCC
Credits:2 Teaching Scheme: L- 2 Hrs/week **Evaluation Scheme:** CA-40, MSE-20, ESE 40
Duration of Theory Exam: 2 Hrs
Pre-requisites: Basic Knowledge of Internet
Course Objectives: This course will enable students to
2. Understand Cyber Space, Cyber Crime, Cyber Laws, Information Technology, Internet, Internet Services
2. Know Legal Aspects of Regulation concerned with Cyber Space, Technology and Forms of Cyber Crimes
3. Understand Computer Crimes and Cyber Crimes, Cyber Crime in Global and Indian Response
4. Understand Criminal Liability, Cyber Crime implications and challenges
5. Learn Precaution & Prevention of Cyber Crimes, Human Rights perspective of Cyber Crime
Course Outcomes: At the end of the course, the students will be able to -
CO1: Understand Cyber Space, Cyber Crime, Information Technology, Internet & Services.
CO2: List and discuss various forms of Cyber Crimes
CO3: Understand Computer Crimes and Cyber Crimes
CO4: Understand Criminal Liability, Cyber Crime implications and challenges

Contents–

Unit	Content	Teaching Hours
1	**UNIT–I: Foundations of Cyber Crimes & Regulation** : Introduction to Information Technology and Cyber Crimes,Glimpses, Definition and Scope of Cyber Crimes,Nature and Extent of Cyber Crimes,Rapid Transmission and Accuracy, Diversity and Span of Victimization,Cyber World and Inadequacy of Law,Influence of Teenagers on Cyber Space,Regulatory Perspective on Technology,Impact of Information Technology,Regulation of Cyber Space,Legal Aspects of Regulation	8

2	**UNIT–II: Technology, Forms & Criminal Aspects of Cyber Crimes:** Influence of Technology on Criminality,Forms of Cyber Crimes,Computer Crimes vs. Cyber Crimes,Opportunities to Cyber Criminals & Motives of Offenders,Problems Affecting Prosecution,Challenges of Prevention and Control of Cyber Crimes,Mens Rea and Criminal Liability,Mens Rea in Indian Criminal Law,Mens Rea in English Criminal Law,Abetment of Offence,Criminal Liability and Role of Mens Rea under the Information Technology Act, 2000	**8**
3	**UNIT–III: Cyber Legal Framework & Global Response**:Cyber Crimes and Global Response,Global Perspective,Country-wise Legal Response,Country-wise Analysis,Cyber Crimes and Indian Response,**Information Technology Act, 2000:** Preamble & Coverage,Nature of Offences and Penalties,Miscellaneous and Subsidiary,Provisions,Shortcomings,Future Prospects and Needs	**8**
4	**UNIT–IV: Investigation, Human Rights, Prevention & Control**:Investigation in Cyber Crimes: Implications and Challenges,Introduction,Procedural Aspects,Issues, Complications and Challenges,Precautionary Measures for Investigation,Human Rights Perspectives on Cyber Crimes,Ideological Aspects,Fundamental Rights and Civil Liberties,Issues and Challenges,Precaution and Prevention of Cyber Crimes,Awareness and Law Reforms,Improving Criminal Justice Administration, Increasing International Cooperation,Curricular Endeavours,Checking Kids' Net Addiction,Role of Guardians,Mobile Pornography: No Nearer Solution in Sight, Self-regulation in Cyber Space	**6**

Text Books:

3. Singh, P. K. (n.d.). Lawson cyber crimes: Along with IT Act and relevant rules. Book Enclave.

Reference Books:

1. Craig, B. (n.d.). Cyber law: The law of the Internet and information technology. Pearson Education.
2. Duggal, P. (n.d.). Cyber laws. Universal Law Publishing.
3. Kumar, K. (2011). Cyber laws: Intellectual property & e-commerce security (1st ed.). Dominant Publishers.

Semester –III

Course Code: DCS23PEL201 **Course Name:** Blockchain and Cryptocurrency Forensics **Course Category:** PEC
Credits: 3 Teaching Scheme: L- 3 Hrs/week **Evaluation Scheme:** CA-40, MSE-20, ESE: 40
Duration of Theory Exam: 2 Hrs
Pre-requisites: 1. Data Structure and Files
2. Expertise in Programming
3. Database Management Systems, Cryptography
Course Objectives: This course will enable students to
2. To explain what blockchain is and how it works.
2. To Analyze cryptocurrency transaction flows using blockchain explorers and forensic tools
3. To Identify and classify various cryptocurrency-related cybercrimes
4. To perform basic cryptocurrency forensic investigations and reporting
Course Outcomes: At the end of the course, the students will be able to -
CO1:Understand the fundamentals of blockchain technology and cryptocurrency systems.
CO2: Learn the working of cryptocurrency transactions, wallets, and exchanges.
CO3: Identify cybercrimes involving blockchain and cryptocurrencies
CO4:Understand various digital forensic techniques to trace and analyze cryptocurrency transactions

Contents–

Unit	Content	Teaching Hours
1	**Introduction** - Evolution of blockchain and distributed ledger technology, Types of blockchain: Public, Private, Consortium, Blockchain architecture: Blocks, hashes, Merkle trees, Cryptographic concepts: Hashing, digital signatures, Consensus mechanisms: PoW, PoS, PoA, Use cases of blockchain in cybersecurity	9

2	**Cryptocurrency Fundamentals** - Introduction to cryptocurrencies and digital assets, Bitcoin architecture and transaction lifecycle, Ethereum and smart contracts, Cryptocurrency wallets: Hot, cold, hardware wallets, Cryptocurrency exchanges: Centralized vs decentralized, Mining, staking, and transaction fees	**9**
3	**Cryptocurrency Crimes and threats** - Types of crypto crimes: Fraud, ransomware, scams,Dark web and cryptocurrency usage, Tracking transactions on hidden networks, Money laundering and terrorism financing through crypto, Ponzi schemes, rug pulls, and phishing attacks, Case studies of major cryptocurrency crimes, Challenges in cryptocurrency investigations	**9**
4	**Cryptocurrency Investigation Methodology** - Reporting and documentation of forensic findings, Forensic Process: Identification, preservation, analysis, and reporting of crypto evidence, Introduction to forensic tools (Chainalysis, CipherTrace – concepts only), Evidence collection and preservation in crypto cases, On-chain vs. Off-chain Data: Extracting data from blockchain explorers (mempool.space, blockchain.com), De-anonymizing users, identifying entities	**10**
5.	**Legal, Regulatory, and Ethical Aspects** - Global and Indian regulations on cryptocurrency, AML (Anti-Money Laundering) and KYC norms, Legal admissibility of digital evidence, Ethical challenges in crypto investigations	**8**

Text Books:

3. Shukla, S., Dhawan, M., Sharma, S., & Venkatesan, S. (2019). Blockchain technology: Cryptocurrency and applications (Draft version). Oxford University Press.
4. Thompson, J. (2017). Blockchain: The blockchain for beginnings, guide to blockchain technology and blockchain programming. CreateSpace Independent Publishing Platform.
5. Prasad, K. (n.d.). Cryptocurrency forensics and investigation using open source intelligence techniques (OSINT) (Vol. 1). CRC Press.

Reference Books:

1. Bashir, I. (2017). Mastering blockchain: Deeper insights into decentralization, cryptography, Bitcoin, and popular blockchain frameworks.
2. Mukherjee, M. (2023). Crypto crimes: Inside India's best-kept secret. HarperCollins India.

Online Resources:NPTEL

1. Free Digital Forensics Tutorial – Intro to Cryptocurrency Forensics & Investigation
2. https://ocw.mit.edu/courses/15-s12-blockchain-and-money-fall-2018 /
3. https://www.youtube.com/watch?v=EH6vE97qIP

Semester –III

Course Code: DCS23PEL202 **Course Name:** Cloud and IOT Security **Course Category: PEC**
Credits: 3 **Teaching Scheme:** L-3 Hrs/Week **Evaluation Scheme:** CA–40, MSE–20, ESE–40
Pre-requisites: Basic programming and fundamental networking concepts
Course Objectives: This course will enable students to
1.To understand security challenges in Cloud and IoT environments
2.To understand basic security mechanisms for data, devices, and networks
3.To develop awareness of threats, attacks, and mitigation techniques
Course Outcomes: At the end of the course, the students will be able to -
CO1: Explain basic concepts of cloud computing and its models.
CO2: Describe IoT Fundamentals and data communication in IoT.
CO3: Identify threats and vulnerabilities in Cloud and IoT systems
CO4: Identify the techniques for secure communication in Cloud & IoT
CO5: Explain the Security Solutions & Best Practices in Cloud & IoT

Content-

Unit	Content	Teaching Hours
1	**Cloud Computing Basics**: Definitions, Key Characteristics, Benefits, Risks & Challenges, service models (IaaS, PaaS, SaaS) and deployment models (Public, Private, Hybrid), Virtualization (hypervisors, VMs) and data centers, Cloud infrastructure, storage, and management.	9
2	**Iot Fundamentals:** Introduction to IoT, Functional characteristics, architecture (layers), M2M communication, Sensors, actuators, embedded systems (Arduino, Raspberry Pi), IoT protocols (MQTT, AMQP) and standards, Benefits of IoT: Healthcare, Smart Transportation, Smart Cities.	9
3	**Security Threats & Challenges**: IoT Device Security: Hardware/Software vulnerabilities, firmware updates, Network Security: DDoS attacks, Man-in-the-Middle, Reply Attacks, Physical Attacks, Cloud Security: Data breaches, Account Hijacking, Insure APIs, compliance, identity management.	9

4	**Cryptography & Access Control:** Symmetric/Asymmetric Encryption, Hashing, Digital Signatures, Identity & Access Management (IAM), Multi-Factor Authentication (MFA), Privacy & Data Security in the Cloud, Secure Communication: SSL/TLS, VPNs**.**	**9**
5	**Security Solutions & Best Practices:** Data Security in Cloud: Data at Rest, Data in Transit, Network Monitoring & Intrusion Detection, Secure Coding Practices for IoT, Cloud Security as a Service (SecaaS), Secure Monitoring & Incident Response	**9**

Text Books:

1. Mather, T., Kumaraswamy, S., & Latif, S. (n.d.). Cloud security and privacy. O'Reilly.
2. Buyya, R., Vahid, D., & Vasilakos, A. (n.d.). Internet of things: Principles and paradigms. Elsevier.

Reference Books:

1. Kamal, R. (2022). Internet of things: Architecture and design (2nd ed.). McGraw Hill.
2. Rittinghouse, J. W. (n.d.). Cloud computing security. CRC Press.
3. Hu, F. (n.d.). Security and privacy in Internet of Things. CRC Press.

Semester –III

Course Code: DCS23PCP201 **Course Name:** Network Threat Management Techniques Lab **Course Category: PCC**
Credits: 2 **Teaching Scheme:** P- 4 Hrs/Week **Evaluation Scheme:** TW: 30, PR: 20
Pre-requisites: Basic knowledge of computer fundamentals, computer networks, network devices, IP addressing and subnetting, Awareness of cyber security fundamentals
Lab Objectives: This course will enable students to
1. Understand network threats and vulnerabilities.
2. Learn threat detection and mitigation techniques.
3. Gain hands-on experience with security tools
4. Analyze real-world cyber attack scenarios.
Lab Outcomes: At the end of the course, the students will be able to -
LO1: Identify and analyze network threats and vulnerabilities.
LO2: Use security tools to monitor and analyze network traffic.
LO3: Implement security controls such as firewalls and IDS.
LO4: Apply cryptographic techniques for secure communication.
LO5: Analyze cyber incidents and recommend mitigation strategies.

List of Experiments:

1. Study different types of network threats and attacks.
2. Perform network reconnaissance using Nmap.
3. Capture and analyze network packets.
4. Understand password vulnerabilities and cracking techniques.
5. Configure and test firewall rules.
6. Detect intrusions using Snort IDS.
7. Simulate Denial of Service attack in a controlled environment.
8. Encrypt and decrypt data using cryptographic techniques.

9. Identify phishing attacks and prevention methods.
10. Analyze real-world network security breaches.
11. Set up Snort and basic rule configuration.
12. Monitor alerts and analyze intrusion logs.
13. Perform DoS testing in an isolated lab environment.
14. Use symmetric and asymmetric encryption tools.
15. Generate and verify hashes (MD5/SHA)
16. Identify phishing emails and analyze case studies of network attacks

Semester –III

Course Code: DCS23PCP202 **Course Name:** Computer & Mobile Forensics Lab **Course Category: PCC**
Credits: 2 **Teaching Scheme:** P- 4 Hrs./Week **Evaluation Scheme:** TW: 30, PR: 20
Pre-requisites: Basics of programming concepts and file systems
Awareness of cyber security concepts and cyber laws
Lab Objectives: This course will enable students to
1.To introduce students to the principles and processes of computer and mobile forensics, including cybercrimes, digital evidence, and standard investigation methodologies.
2. To develop practical skills in acquiring, analyzing, and reporting digital evidence from computer systems and mobile devices using forensic tools while following legal and ethical practices.
Lab Outcomes: At the end of the course, the students will be able to -
LO1: Perform forensic disk imaging and evidence acquisition using open-source tools while preserving data integrity and maintaining proper forensic procedures.
LO2: Verify the integrity of digital evidence using cryptographic hash functions such as MD5 and SHA to ensure evidence authenticity.
LO3: Recover and analyze deleted files and system artifacts including browser history and Internet activity from digital storage media

List of Experiments:

10. Forensic Disk Imaging and Evidence Acquisition Using Open-Source Tools
11. Integrity Verification of Digital Evidence Using Cryptographic Hash Functions (MD5/SHA)
12. Recovery and Analysis of Deleted Files from Digital Storage Media
13. Forensic Analysis of Web Browser History and Internet Artifacts
14. Timeline Reconstruction and Event Correlation of a Compromised Computer System
15. Mobile Forensics Practicals (Any 5)
16. Logical Acquisition of Android Mobile Device Data

17. SIM Card Data Extraction and Forensic Analysis
18. Forensic Examination of Call Logs and SMS Records
19. Extraction and Analysis of Multimedia Files from Mobile Devices

Semester –III

Course Code: DCS23PEP201 **Course Name:** Blockchain and Cryptocurrency Forensics Lab **Course Category:** PEC
Credits: 1 **Teaching Scheme:** P- 2 Hrs/Week **Evaluation Scheme:** TW: 30, PR: 20
Pre-requisites: Data Structure and Files Expertise in Programming Database Management Systems, Cryptography
Lab Objectives: This course will enable students to
1. Introduce students to the practical working of blockchain and cryptocurrency systems.
2. Enable students to use public blockchain explorers for transaction and address analysis
3. Develop basic skills in analyzing cryptocurrency wallets and transaction lifecycles.
4. Familiarize students with common cryptocurrency-related cybercrime patterns
5. Provide hands-on experience in basic blockchain forensic investigation techniques.
Lab Outcomes: At the end of the course, the students will be able to -
LO1: Interpret blockchain structure, blocks, hashes, and transactions using real-time blockchain data.
LO2. Identify and analyze cryptocurrency wallets, address formats, and transaction histories
LO3. Examine the lifecycle of cryptocurrency transactions including confirmations and fees.
LO4. Detect suspicious transaction patterns associated with cryptocurrency-based cybercrimes.

List of Experiments:

1. Hands-on use of public blockchain explorers like bitcoin and ethereum
2. To create a demo software wallet (testnet), Identify public/private keys, Analyze wallet addresses (BTC vs ETH formats), Study transaction history of a given address
3. To analyze how crypto transactions are created and confirmed, Observe transaction creation to confirmation, Study transaction hash, inputs, outputs, gas fee, Compare confirmed vs pending transactions, Identify transaction timestamps and block confirmations

4. To identify suspicious patterns in crypto transactions: Analyze sample scam or ransomware wallet addresses, Identify red flags: high-frequency transfers, mixers, multiple hops, Study real case reports of crypto fraud, Classify crime type based on transaction behavior
5. To perform basic forensic tracing of transactions: Trace fund movement from a suspect wallet, Identify linked addresses using transaction flow, Create a simple transaction graph
6. To understand address clustering techniques: Identify possible wallet clusters, Analyze exchange-linked addresses
7. To learn forensic documentation and reporting: Capture screenshots of blockchain evidence, Record transaction details systematically, Prepare a basic forensic report
8. To understand legal and ethical considerations: Study a real cryptocurrency investigation case, Identify legal violations (AML/KYC, fraud), Discuss admissibility of blockchain evidence

Semester –III

Course Code: DCS23PEP202 **Course Name:** Cloud and IOT Security Lab **Course Category:** PEC
Credits: 1 **Teaching Scheme:** P- 2 Hrs/Week **Evaluation Scheme:** TW: 30, PR: 20
Pre-requisites: Basics of Computer Networks
Lab Objectives: This course will enable students to
1. ITo design secure Cloud and IoT architecture
2. To implement basic security mechanisms for data, devices, and networks
Lab Outcomes: At the end of the course, the students will be able to -
LO1: To demonstrate cloud storage with security measures.
LO2: To implement Secure IoT systems.
LO3:Identify and critically evaluate threats, risks, and vulnerabilities associated with IoT and cloud solutions.

List of Experiments:

1. To study IoT Devices and Security Risks.
2. To study Cloud service models and Cloud deployment models.
3. Implement a simple IoT System using a Simulator.
4. Implement basic authentication with password for IoT device access
5. Demonstrate basic data decryption in IoT Communication.
6. To study Different Cloud services (AWS Free Tier / Google Cloud)
7. Implement Cloud user access Management.
8. Demonstrate data storage on the cloud with encryption.
9. Configure simple Firewall settings for secure data communication.
10. Case study based on Cloud and IoT Security Breaches.

Semester –III

Course Code:DCS23SEM201 Course Name: Seminar **Course Category:** SEM
Credits: 1 **Teaching Scheme:** P- 2 Hrs/Week **Evaluation Scheme:** Internal TW-50
Pre-requisites: Basics of Computer Networks
Course Objectives: This course will enable students to
To familiarize students with recent developments in the discipline and to enhance their skills in literature survey, technical writing, and oral presentation.
Course Outcomes: At the end of the course, the students will be able to -
CO1: Students will be able to identify and review relevant literature on a contemporary topic in their discipline.
CO2: Students will be able to analyze and organize technical information and present it effectively using appropriate communication tools..
CO3: Students will be able to demonstrate improved oral presentation skills, professional ethics, and confidence in responding to questions.

Instructions —

- The 3rd semester seminar is for 50 marks and should balance technical depth, clarity, and professional presentation.
- Begin with a title section that includes the topic, your name, roll number, course, department, guide's name, institution, and year.
- Start the seminar with an introduction that gives background about the topic, explains its importance, and shows real-world relevance or motivation.
- For academic or research-oriented seminars, include a short problem statement to identify the issue or gap the topic addresses.
- Clearly state the objectives to describe what the seminar intends to achieve.
- Include a brief literature review or existing-work section to show how earlier technologies, research, or solutions relate to the topic.
- Present the main technical content in the methodology or system section, covering architecture, workflow, modules, algorithms, tools, or technology as needed.
- Use diagrams, flowcharts, tables, or block diagrams to improve clarity and structure.

- If suitable, add a case study, simulation, experiment, or comparative analysis to strengthen technical content.
- Present results or outcomes to show key findings, achievements, comparisons, or performance details.
- Marks are typically based on technical content, presentation quality, seminar report or documentation, viva-voce performance, and attendance/discipline.
- Many institutions require a printed seminar report of about 40–60 pages, including introduction, theoretical background, methodology, results, conclusion, and references.
- Use clear diagrams, clean and uncluttered slides, relevant and current topics, and be prepared to answer questions during viva.

Semester –IV

Course Code: DCS23PCL251 **Course Name:** Cyber Risk Management & Compliance **Course Category:** PCC
Credits: 2 Teaching Scheme: L- 2 Hrs/week **Evaluation Scheme:** CA-40, MSE-20, ESE: 40
Duration of Theory Exam: 2 Hrs
Pre-requisites: Basic Networking and Linux/Windows Operating Systems understanding Networking, operating systems, cyber security fundamentals, and introductory digital forensics. cyber risk concepts, risk assessment, legal/regulatory compliance, security policies, and practical exposure to risk analysis and compliance documentation
Course Objectives: This course will enable students to
1. Analyze major cybersecurity regulations and standards
2. Apply risk management models
3. Design and implement Governance, Risk, and Compliance (GRC) frameworks
4. Evaluate auditing, monitoring, and incident reporting processes
Course Outcomes: At the end of the course, the students will be able to -
CO1 Identify and assess cyber risks
CO2 Demonstrate compliance knowledge by mapping organizational controls to regulations such as ISO 27001, NIST CSF, PCI-DSS, GDPR, HIPAA, and SOX
CO3 Develop and document GRC strategies, including policies, governance structures, and compliance programs.
CO4 Conduct security audits and compliance assessments and interpret audit findings to recommend corrective actions.

Contents–

Unit	Content	Teaching Hours
1	**Fundamentals of Cyber Risk Management** Covers cyber risk identification, classification, and assessment methodologies. Introduces risk management models, including quantitative vs. qualitative risk analysis and risk treatment options.	7
2	**Regulatory and Compliance Frameworks** Explores major cybersecurity regulations and compliance requirements. Discusses ISO 27001, NIST CSF, PCI-DSS, GDPR, HIPAA, SOX, and other global security standards.	7

3	**Governance, Risk, and Compliance (GRC) Implementation**: Introduces GRC models and strategies for integrating risk management with business objectives. Covers compliance program development, policy creation, and security governance structures.	**8**
4	**Auditing, Incident Reporting, and Compliance Monitoring** Focuses on cyber risk assessment tools, security audits, continuous monitoring strategies, and incident reporting procedures. Discusses third-party risk management and compliance automation..	**8**

Text Books:

3. Brumfield, C. (n.d.). Cybersecurity risk management.
4. National Institute of Standards and Technology. (n.d.). NIST cybersecurity framework: A guide for policy makers.

Reference Books:

3. Landoll, D. (n.d.). The security risk assessment handbook.
4. Lukings, M., & Jochelson, R. (n.d.). Cybersecurity and privacy law handbook.
5. International Organization for Standardization. (n.d.). ISO 27001 and NIST CSF compliance guides.

Semester –IV

Course Code: DCS23PCL252 **Course Name:** Security Operations Center **Course Category:** PCC
Credits: 2 Teaching Scheme: L- 2 Hrs/week **Evaluation Scheme:** CA-40, MSE-20, ESE: 40
Duration of Theory Exam: 2 Hrs
Pre-requisites: Basic knowledge of computer systems, networking and Internet, and operating system
Course Objectives: This course will enable students to
1. To introduce core SOC concepts, including cybersecurity challenges, incident response, SOC evolution, and maturity models
2. To develop understanding of SOC technologies, infrastructure, and capability assessment, covering data analysis, threat and vulnerability management, cloud and network monitoring, SOC strategy, and operating models
Course Outcomes: At the end of the course, the students will be able -
CO1: explain core SOC concepts, including cybersecurity challenges, incident response, SOC evolution, and maturity models
CO2: explain SOC technologies and architecture, including data analysis, threat management, compliance, and case handling.
CO3: assess SOC capabilities by understanding assessment methods, IT processes, SOC strategy, operating models, services, and capability roadmaps.
CO4: explain SOC infrastructure and security operations, including event generation and collection, network and cloud monitoring, vulnerability management, and threat intelligence.

Contents–

Unit	Content	Teaching Hours
1	Introduction to Security Operations and the SOC: Cybersecurity Challenges, Introduction to Information Assurance , Introduction to Risk Management , Information Security Incident Response , SOC Generations , Characteristics of an Effective SOC , Introduction to Maturity Models , Applying Maturity Models to SOC , Phases of Building a SOC, Challenges and Obstacles	**4**

2	Overview of SOC Technologies : Data Collection and Analysis, Vulnerability Management, Threat Intelligence, Compliance, Ticketing and Case Management , Collaboration , SOC Conceptual Architecture.	**8**
3	Assessing Security Operations Capabilities: Assessment Methodology, Assessing IT Processes , SOC Strategy: Strategy Elements, SOC Model of Operation, SOC Services, SOC Capabilities Roadmap.	**4**
4	The SOC Infrastructure: Model of Operation, Facilities, Active Infrastructure. Security Event Generation and Collection: Data Collection, Cloud Security, Intrusion Detection and Prevention Systems, Breach Detection, DNS Servers, Network Telemetry with Network Flow Monitoring. Vulnerability Management: Identifying Vulnerabilities, Security Services, Vulnerability Tools, Handling Vulnerabilities, Automating Vulnerability Management, Threat Intelligence**.**	**8**

Text Books:

1. Security Operations Center, Joseph Muniz, Gary McIntyre, Nadhem AlFardan
Copyright© 2016 Cisco Systems, Inc., Published by: Cisco Press, 800 East 96th Street , Indianapolis, IN 46240 USA

Reference Books:

1. The Modern Security Operation Center by Joseph Muniz, Aamir Lakhani, Omar Santos, Moses Frost
2. Security Operation Center Guidebook: A Practical Guide for a successful SOC, Gregory Jarpey

Semester –IV

Course Code:DCS23OJT251 Course Name: Project/Internship **Course Category:** OJT
Credits: 12 **Teaching Scheme:** P- 24 Hrs/Week **Evaluation Scheme:** Internal TW-100 External 200
Pre-requisites: Basics of Computer Networks
Course Objectives: This course will enable students to
1. Apply theoretical and technical skills in cybersecurity and digital forensics to solve real-life problems
2. Acquire exposure to workplace environments, security operations, and forensic procedure
3. Develop project planning, documentation, research, and analytical skills.
4. Demonstrate knowledge of security tools, investigation methods, and forensic techniques
Course Outcomes: At the end of the course, the students will be able to -
CO1: Identify and define a cybersecurity or forensic problem relevant to industry or society.
CO2: Analyze security threats, vulnerabilities, incidents, or forensic requirements.
CO3: Apply suitable tools, frameworks, and techniques for security or forensic investigation.
CO4: Interpret results, logs, artifacts, or digital evidence with accuracy and clarity.
CO5: Document technical findings and prepare structured project/internship reports.
CO6: Demonstrate professional ethics, legal awareness, and safe handling of cybersecurity tools.

Instructions —

- Students must undertake a technical project or industry internship in the domain of cybersecurity and/or digital forensics.
- Topics should be relevant, current, and aligned with practical industry needs or real-world problems.
- Projects may involve security tools, penetration testing, incident response, malware analysis, forensic investigation, secure system design, or reporting techniques.
- Students should demonstrate application of technical knowledge gained during coursework.
- Internship may be completed in IT companies, cybersecurity firms, forensic labs, government agencies, or relevant organizations.

- Students are expected to maintain work logs, documentation, and reflective records during the internship period.
- A project report or internship report must be submitted at the end of the term, following institutional formatting guidelines.
- Evaluation will include project quality, implementation depth, documentation, presentation, viva, and industry feedback (if applicable).
- Students are encouraged to use standard tools and platforms such as Kali Linux, Wireshark, Autopsy, FTK Imager, Volatility, OSINT tools, etc., depending on project suitability.
- Ethical conduct, legal compliance, and responsible use of cybersecurity tools must be strictly followed