PANIMALAR ENGINEERING COLLEGE

(An Autonomous Institution, Affiliated to Anna University, Chennai)
Bangalore Trunk Road, Varadharajapuram,
Poonamallee, Chennai – 600123

Minor Degree

CYBER SECURITY

Curriculum & Syllabus

DEPARTMENT OF
COMPUTER SCIENCE AND ENGINEERING

REGULATION 2023

PANIMALAR ENGINEERING COLLEGE

Department of Computer Science Engineering

Minor Degree

on

Cyber Security

S. No	COURSE CODE	COURSE TITLE	Category	L/T/P	Contact Hours	Credit	Ext / Int Weightage
1.	23CS4001	Fundamentals of Data Structures	PE	3/0/0	3	3	60/40
2.	23CS4002	Foundations of Computer Networks	PE	3/0/0	3	3	60/40
3.	23CS4003	Ethical Hacking Essentials	PE	3/0/0	3	3	60/40
4.	23CS4004	Cyber Security	PE	3/0/0	3	3	60/40
5.	23CS4005	Cyber Forensics	PE	3/0/0	3	3	60/40
6.	23CS4006	Cryptography and Network Security	PE	3/0/0	3	3	60/40
7.	23CS4007	Principles of Digital and Mobile Forensics	PE	3/0/0	3	3	60/40
8.	23CS4008	Information Security	PE	3/0/0	3	3	60/40

23CS4001	FUNDAMENTALS OF DATA STRUCTURES	L	T	P	C
		3	0	0	3

COURSE OBJECTIVES:

- To familiarize with basic structures of arrays and lists
- To understand abstract data types
- To learn linear data structures
- To learn non– linear data structures
- To know about advanced data structures and applications

UNIT I BASIC STRUCTURES AND ADT 9

Data Structure – Algorithm – Data abstraction – ADT – Array – – List – Linked List – Singly linked list – Doubly linked list – Circular list – Elementary operations

UNIT II LINEAR DATA STRUCTURE 9

Stack – Operations – Array implementation – Linked list implementation – Expression evaluation – Queue – Elementary operations– Array implementation – Linked list implementation– Application– Priority queue

UNIT III NON– LINEAR DATA STRUCTURE– I 9

Tree– Terminologies– Binary tree – Properties– Representation– Traversal – Threaded Binary Tree – Heap – Min Heap – Max Heap –– Binary search tree – Elementary operations – Application

UNIT IV NON– LINEAR DATA STRUCTURE– II 9

Graph– Terminologies – Types– Representation – Elementary operations – Connected component – Spanning Tree – Application

UNIT V ADVANCED STRUCTURES 9

Balanced tree – AVL tree B Tree – Trie – Binomial heap – Hashing – Collision resolution techniques

Total: 45 Periods

TEXT BOOKS

1. Horowitz and Sartaj Sahni, Anderson Freed “Fundamentals of Data Structures in C”, University Press, 2008
2. Ellis Horowitz and Sartaj Sahni, Dinesh Mehta “Fundamentals of Data Structures in C++”, Silicon Press, 2007.
3. Yashavant Kanetkar, “Data Structures Through C”, BPB press, 4th edition, 2022

REFERENCES

1. Michael T. Goodrich, Roberto Tamassia “Data Structures and Algorithms in Python”, Wiley, 2021
2. Jean– Paul Tremblay and Paul G Sorenson, “An Introduction to Data Structures with Applications”, Second Edition, McGrawHill, 2017
3. Thomas H Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein, “Introduction to Algorithms”, Third Edition, Prentice Hall, 2010.
4. Ellis Horowitz and Sartaj Sahni, “Fundamental of Computer Algorithms”, Galgotia, 1985.

COURSE OUTCOMES:

Upon completion of the course, the students will be able to

- Select suitable data structure for an application
- Understand, design and implement linear data structures
- Understand, design and implement non– linear data structures
- Appreciate advanced data structures and applications
- Apply various data structures for solving problems

CO – PO MAPPING

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	3	3	3	2	–	–	–	–	–	–	2
CO2	3	3	3	1	–	–	–	–	–	–	–
CO3	2	3	3	1	–	–	–	–	–	–	–
CO4	3	2	2	2	–	–	–	–	–	–	2
CO5	2	2	2	3	–	–	–	–	–	–	3

Internal Assessment				**End Semester Examination**
Assessment I (100 Marks)		**Assessment II (100 Marks)**		
Individual Assignment / Case Study / Seminar / Mini Project	**Written Test**	**Individual Assignment / Case Study / Seminar / Mini Project**	**Written Test**	**Written Examination**
40	60	40	60	100
40%				**60 %**

23CS4002	FOUNDATIONS OF COMPUTER NETWORKS	L	T	P	C
		3	0	0	3

COURSE OBJECTIVES:

- To understand the division of network functionality into layers
- To familiarize the functions and protocols of each layer in the TCP/IP protocol suite
- To visualize end– to– end flow of information
- To understand the components required to build different types of networks
- To learn concepts related to the network addressing and routing

UNIT I INTRODUCTION/ APPLICATION LAYER 9

Building a network, Network edge and core – Layered Architecture, ISO/OSI Model, Internet Architecture (TCP/IP) –) Networking Devices: Hubs, Bridges, Switches, Routers, and Gateways – Performance Metrics – Application Layer protocols – HTTP – FTP – Email – DNS

UNIT II TRANSPORT LAYER 9

Introduction – Connectionless Transport: User Datagram Protocol – Principles of Reliable Data Transfer (GBN, SR) – Connection– Oriented Transport – TCP – Connection establishment and teardown – Triggering transmission – Flow Control – Congestion Control

UNIT III NETWORK LAYER 9

Inside a Router – Internet Protocols – IPV4, IPV6, IP Addressing and NAT – Subnetting – Variable Length Subnet Mask (VLSM) – Classless Inter– Domain Routing (CIDR)

UNIT IV ROUTING PROTOCOLS 9

Distance Vector Routing – Link State Routing – RIP – OSPF – BGP – ICMP – DHCP – Introduction to Quality of Services (QoS)

UNIT V LINK LAYER 9

Introduction – Link Layer Framing, Addressing – Error Detection/ Correction Techniques – Switched Local Area Networks (ARP, Ethernet, VLAN) – Wireless LAN (802.11)

Total: 45 Periods

TEXT BOOKS

1. James F. Kurose, Keith W. Ross, “Computer Networking: A Top– Down Approach”, Eighth Edition, Pearson Education, 2022.
2. Larry L. Peterson, Bruce S. Davie, “Computer Networks: A Systems Approach”, Sixth Edition, Morgan Kaufmann Publishers Inc., 2021.

REFERENCES

1. William Stallings, “Data and Computer Communications”, Tenth Edition, Pearson Education, 2017.

2. Ying– Dar Lin, Ren– Hung Hwang, Fred Baker, " Computer Networks: An Open Source Approach", 1st Edition, McGraw Hill, 2011

COURSE OUTCOMES:

Upon completion of the course, the students will be able to

- Highlight the significance of the functions of each layer in the network
- Identify the devices and protocols to design a network and implement it
- Build network applications using the right set of protocols and estimate their performance
- Apply addressing principles such as subnetting and VLSM for efficient routing
- Explain media access techniques

CO – PO MAPPING

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	3	3	3	2	1	1	–	–	–	–	–
CO2	3	3	3	3	2	1	–	3	–	–	2
CO3	3	3	3	3	2	1	–	3	–	–	2
CO4	3	3	3	2	1	1	–	–	–	–	2
CO5	3	3	3	2	1	1	–	1	–	–	1

Internal Assessment				**End Semester Examination**
Assessment I (100 Marks)		**Assessment II (100 Marks)**		
Individual Assignment / Case Study / Seminar / Mini Project	**Written Test**	**Individual Assignment / Case Study / Seminar / Mini Project**	**Written Test**	**Written Examination**
40	60	40	60	100
40%				**60 %**

23CS4003	ETHICAL HACKING ESSENTIALS	L	T	P	C
		3	0	0	3

COURSE OBJECTIVES:

- To understand the basics of computer based vulnerabilities.
- To explore different foot printing, reconnaissance and scanning methods.
- To expose the enumeration and vulnerability analysis methods.
- To understand hacking options available in Web and wireless applications.
- To explore the options for network protection.
- To practice tools to perform ethical hacking to expose the vulnerabilities.

UNIT I INTRODUCTION 9

Ethical Hacking Overview – Principles of Ethical hacking– Hacking Methodologies– Role of Ethical Hacker– Scope & limitations of hacking – Cyber Threats and Attacks Vectors– Policies and Controls

UNIT II MALWARE ANALYSIS 9

Malware Overviews– Viruses, Trojans, Malwares, and OS Level Attacks – Counter Measures– Malware Analysis Procedure – Malware Detection Method

UNIT III FOOTPRINTING AND SCANNING NETWORKS 9

Footprinting Concepts – Footprinting through Search Engines, Web Services, Social Networking Sites, Website, Email – Competitive Intelligence – Footprinting through Social Engineering – Footprinting Tools – Network Scanning Concepts – Port– Scanning Tools – Scanning Techniques – Scanning Beyond IDS and Firewall

Unit IV ENUMERATION AND VULNERABILITY ANALYSIS 9

Access control requirements for Cloud infrastructure – User Identification – Authentication and Enumeration Concepts – NetBIOS Enumeration – SNMP, LDAP, NTP, SMTP and DNS Enumeration – Vulnerability Assessment Concepts – Desktop and Server OS Vulnerabilities – Windows OS Vulnerabilities – Tools for Identifying Vulnerabilities in Windows– Linux OS Vulnerabilities– Vulnerabilities of Embedded Oss

UNIT V ATTACKS 9

SQL Injection – DOS Attacks – Session Hijacking– System Hacking– Web application security risks – Web server attacks

Total: 45 Periods

TEXT BOOKS

1. Stuart McClure, Joel Scambray and Goerge Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, Tata Mc Graw Hill Publishers, 2010.
2. Bensmith, and Brian Komer, Microsoft Windows Security Resource Kit, Prentice Hall of India, 2010.
3. Desai, Manthan M., “Hacking for Beginners: A beginners guide to learn ethical hacking”, Hacking Tech, 2013.
4. Michael T. Simpson, Kent Backman, and James E. Corley, Hands– On Ethical Hacking and Network Defense, Course Technology, Delmar Cengage Learning,

2010.
5. Patrick Engebretson, The Basics of Hacking and Penetration Testing, SYNGRESS, Elsevier, 2013.
6. Dafydd Stuttard and Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2011.

REFERENCES

1. Justin Seitz, Black Hat Python: Python Programming for Hackers and Pentesters, 2014.

COURSE OUTCOMES:

Upon completion of the course, the students will be able to

- Express knowledge on basics of computer based vulnerabilities.
- Gain understanding on different foot printing, reconnaissance and scanning methods.
- Demonstrate the enumeration and vulnerability analysis methods
- Gain knowledge on hacking options available in Web and wireless applications.
- Acquire knowledge on the options for network protection.

CO – PO MAPPING

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	2	2	3	2	1	1	1	1	2	2	1
CO2	1	2	1	2	1	1	1	2	2	1	1
CO3	2	2	3	3	1	1	1	1	2	1	2
CO4	2	1	1	2	1	1	1	1	3	3	3
CO5	2	3	1	1	2	1	1	2	1	1	1

Internal Assessment				**End Semester Examination**
Assessment I (100 Marks)		**Assessment II (100 Marks)**		
Individual Assignment / Case Study / Seminar / Mini Project	**Written Test**	**Individual Assignment / Case Study / Seminar / Mini Project**	**Written Test**	**Written Examination**
40	60	40	60	100
40%				**60 %**

23CS4004	CYBER SECURITY	L	T	P	C
		3	0	0	3

COURSE OBJECTIVES:

- To learn cybercrime and cyberlaw.
- To understand the cyber attacks and tools for mitigating them.
- To understand information gathering.
- To learn how to detect a cyber attack.
- To learn how to prevent a cyber attack.

UNIT I INTRODUCTION 9

Need for Cyber security – History of Cyber security – Defining Cyberspace and Cyber security– Standards – CIA Triad – Cyber security Framework

UNIT II ATTACKS AND COUNTERMEASURES 9

OSWAP; Malicious Attack Threats and Vulnerabilities: Scope of Cyber– Attacks – Security Breach – Types of Malicious Attacks – Malicious Software – Common Attack Vectors – Social engineering Attack – Wireless Network Attack – Web Application Attack –Cloud applications Attack– Attack Tools – Countermeasures – Counter Cyber Security Initiatives in India

UNIT III INFORMATION MANAGEMENT 9

Information Classification and Handling – Privacy – Document and Records Management – Sensitive Physical Information

UNIT IV NETWORKS AND COMMUNICATIONS 9

Network Management Concepts – Firewalls – Virtual Private Networks and IP Security – Security Considerations for Network Management – Electronic Communications

UNIT V THREAT AND INCIDENT MANAGEMENT 9

Technical Vulnerability Management – Security Event Logging – Security Event Management -Threat Intelligence – Cyber Attack Protection – Security Incident Management Framework -Security Incident Management Process.

Total: 45 Periods

TEXT BOOKS

1. Stallings, William, “Effective cybersecurity: a guide to using best practices and standards”, Addison– Wesley Professional, 2018.
2. AnandShinde, “Introduction to Cyber Security Guide to the World of Cyber Security”, Notion Press, 2021
3. Nina Godbole, SunitBelapure, “Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives”, Wiley Publishers, 2011

REFERENCES

1. David Kim, Michael G. Solomon, “Fundamentals of Information Systems Security”, Jones & Bartlett Learning Publishers, 2013
2. Patrick Engebretson, “The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made easy”, Elsevier, 2011
3. Kimberly Graves, “CEH Official Certified Ethical hacker Review Guide”, Wiley Publishers, 2007
4. William Stallings, Lawrie Brown, “Computer Security Principles and Practice”, Third Edition, Pearson Education, 2015
5. Georgia Weidman, “Penetration Testing: A Hands– On Introduction to Hacking”, No Starch Press, 2014

COURSE OUTCOMES:

Upon completion of the course, the students will be able to

- Explain the basics of cyber security, cyber crime and cyber law
- Classify various types of attacks and learn the tools to launch the attacks
- Apply various tools to perform information gathering
- Apply intrusion techniques to detect intrusion
- Apply intrusion prevention techniques to prevent intrusion

CO – PO MAPPING

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	1	1	1	1	–	1	–	–	–	1	–
CO2	1	3	1	3	2	1	–	–	–	–	–
CO3	2	1	1	1	–	1	–	–	–	1	–
CO4	3	3	2	2	2	1	–	–	–	–	–
CO5	3	2	1	1	1	1	1	–	–	1	–

Internal Assessment				**End Semester Examination**
Assessment I (100 Marks)		**Assessment II (100 Marks)**		
Individual Assignment / Case Study / Seminar / Mini Project	**Written Test**	**Individual Assignment / Case Study / Seminar / Mini Project**	**Written Test**	**Written Examination**
40	60	40	60	100
40%				**60 %**

23CS4005	CYBER FORENSICS	L	T	P	C
		3	0	0	3

COURSE OBJECTIVES:

- To understand the basic concepts and principles of computer forensics
- To identify the smart practices for carrying out forensic investigation
- To understand the legal frameworks in cyber forensics
- To understand the application of tools and techniques for recovering digital evidence
- To understand the future issues of computer forensics.

UNIT I INTRODUCTION 9

Computer Forensics Fundamentals – Types of Computer Forensics Technology – Types of Computer Forensics Systems – Vendor and Computer Forensics Services

UNIT II COMPUTER FORENSICS EVIDENCE AND CAPTURE 9

Data Recovery – Evidence Collection and Data Seizure– Duplication and Preservation of Digital Evidence– Computer Image Verification and Authentication.

UNIT III COMPUTER FORENSIC ANALYSIS 9

Discover of Electronic Evidence – Identification of Data – Reconstructing Past Events – Fighting against Macro Threats – Information Warfare Arsenal – Tactics of the Military – Tactics of Terrorist and Rogues – Tactics of Private Companies

UNIT IV INFORMATION WARFARE 9

Surveillance Tools – Hackers and Theft of Components – Contemporary Computer Crime– Identity Theft and Identity Fraud – Organized Crime &Terrorism – Avenues Prosecution and Government Efforts – Applying the First Amendment to Computer Related Crime– The Fourth Amendment and other Legal Issues.

UNIT V COMPUTER FORENSIC CASES 9

Developing Forensic Capabilities – Searching and Seizing Computer Related Evidence – Processing Evidence and Report Preparation – Future Issues

Total: 45 Periods

TEXT BOOKS

1. John R. Vacca, “Computer Forensics: Computer Crime Scene Investigation”, Cengage Learning, 2nd Edition, 2005.
2. Marjie T Britz, “Computer Forensics and Cyber Crime: An Introduction”, Pearson Education, 2nd Edition, 2008.
3. Michael Graves, "Digital Archaeology: The Art and Science of Digital Forensics”, Addison– Wesley Professional, 2014.
4. Darren R.Hayes, "Practical Guide to Computer Forensics Investigation”, Pearson, 2015.
5. Albert J. Marcella and Frederic Guillossou, "Cyber Forensics: From Data to Digital Evidence” , Wiley, 2015.

REFERENCES

1. Bill Nelson, Amelia Phillips and Christopher Steuart, —Guide to Computer Forensics and Investigations ‖, Fourth Edition, Cengage, 2013.
2. Marie–Helen Maras, "Computer Forensics: Cybercriminals, Laws, and Evidence", Jones & Bartlett Learning; 2nd Edition, 2014.
3. Majid Yar, "Cybercrime and Society", SAGE Publications Ltd, Hardcover, 2nd Edition, 2013.

COURSE OUTCOMES:

Upon completion of the course, the students will be able to

- Understand the fundamentals of computer forensics
- Identify and apply smart practices for investigation
- Recognize the legal underpinnings and critical was affecting forensics
- Apply tools and methods to uncover hidden information in digital systems
- Learn the issues of cyber forensics

CO – PO MAPPING

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	2	2	3	2	1	–	–	1	2	2	1
CO2	1	2	1	2	1	–	–	2	2	1	1
CO3	2	2	3	3	1	–	–	1	2	1	2
CO4	2	1	1	2	1	–	–	1	3	3	3
CO5	2	3	1	1	2	–	–	2	1	1	1

Internal Assessment				**End Semester Examination**
Assessment I (100 Marks)		**Assessment II (100 Marks)**		
Individual Assignment / Case Study / Seminar / Mini Project	**Written Test**	**Individual Assignment / Case Study / Seminar / Mini Project**	**Written Test**	**Written Examination**
40	60	40	60	100
40%				**60 %**

23CS4006	CRYPTOGRAPHY AND NETWORK SECURITY	L	T	P	C
		3	0	0	3

COURSE OBJECTIVES:

- To know the various state of the art security exploitation mechanisms.
- To understand the mathematics behind cryptography.
- To know the standard algorithms used to provide confidentiality, integrity, and authenticity.
- To understand the importance of authentication mechanism.
- To know the various security mechanisms related to networks.

UNIT I INTRODUCTION 9

Introduction to Cryptography – Discrete Logarithms – Security Levels – Basics of Number Theory – Fermat and Euler's Theory – Euclidian's Algorithm – Primality Testing – Chinese Remainder Theorem – Finite Fields of the form GF(P) – Modular Exponentiation

UNIT II SYMMETRIC CRYPTOGRAPHY 9

Block ciphers: Modes of operation, DES and its variants, finite fields, AES, linear and differential cryptanalysis

UNIT III PUBLIC KEY CRYPTOGRAPHY 9

RSA cryptosystem – Key distribution – Key management – Diffie Hellman key exchange – ElGamal cryptosystem – Elliptic curve arithmetic– Elliptic curve cryptography.

UNIT IV MESSAGE AUTHENTICATION AND INTEGRITY 9

Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC – SHA –Digital signature and authentication protocols – DSS– Entity Authentication: Biometrics, Passwords, Challenge Response protocols– Authentication applications – Kerberos, X.509

UNIT V NETWORK SECURITY 9

Firewalls – IP Security – VPN – Intrusion Detection – Web Security – SSL – TLS

Total: 45 Periods

TEXT BOOKS

1. Paar, Christof, and Jan Pelzl, "Understanding cryptography: a textbook for students and practitioners", Springer Science & Business Media, 2009.
2. William Stallings, "Cryptography and Network Security: Principles and Practices", Eighth Edition, Pearson Education, 2020.

3. Kahate, Atul. "Cryptography and Network Security", Tata McGraw– Hill, 4th reprint, 2005.
4. Jon Erickson, "Hacking: The Art of Exploitation", 2nd Edition, Starch Press, 2008.

REFERENCES

1. N. Ferguson, B. Schneier, and T. Kohno. "Cryptography Engineering: Design Principles and Practical Applications". Wiley, 2010.
2. Neil Daswani, Christoph Kern, and Anita Kesavan, "Foundations of Security: What Every Programmer Needs to Know", Frist Edition, Apress, 2007.
3. "The Shellcoder's Handbook: Discovering and Exploiting Security Holes", 2nd Edition by Chris Anley et al, 2007

COURSE OUTCOMES:

Upon completion of the course, the students will be able to

- Discuss various exploitations present in the security.
- Illustrate the basic concepts of encryption and decryption for secure data transmission.
- Develop solutions for security problems
- Analyze various cryptography techniques and their applications
- Learn the various network security techniques and their characteristics.

CO – PO MAPPING

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	3	3	2	1	1	2	1	1	–	–	2
CO2	3	3	2	2	2	3	1	1	–	–	2
CO3	3	2	2	1	1	2	–	1	–	–	2
CO4	3	3	3	1	2	3	1	1	–	–	2
CO5	3	3	3	1	2	3	1	1	–	–	2

Internal Assessment				**End Semester Examination**
Assessment I (100 Marks)		**Assessment II (100 Marks)**		
Individual Assignment / Case Study / Seminar / Mini Project	**Written Test**	**Individual Assignment / Case Study / Seminar / Mini Project**	**Written Test**	**Written Examination**
40	60	40	60	100
40%				**60 %**

23CS4007	PRINCIPLES OF DIGITAL AND MOBILE FORENSICS	L	T	P	C
		3	0	0	3

COURSE OBJECTIVES:

- To understand basic digital forensics and techniques.
- To understand digital crime and investigation.
- To understand how to be prepared for digital forensic readiness.
- To understand and use forensics tools for iOS devices.
- To understand and use forensics tools for Android devices

UNIT I INTRODUCTION TO DIGITAL FORENSICS 9

Digital Forensics – Digital Evidence – The Digital Forensics Process – Introduction – The Identification Phase – The Collection Phase – The Examination Phase – The Analysis Phase – The Presentation Phase

UNIT II DIGITAL CRIME AND INVESTIGATION 9

Digital Crime – Offenses – Investigation Methods for Collecting Digital Evidence – Use of Sleuthkit to analyze disk image and call logs.

UNIT III DIGITAL FORENSIC READINESS 9

Introduction – Rationale for Digital Forensic Readiness – Frameworks, Standards and Methodologies – Challenges in Digital Forensics

UNIT IV iOS FORENSICS 9

iOS Fundamentals – Jailbreaking – File System – Hardware – iPhone Security – iOS Forensics – Procedures and Processes – Use of Mobile Verification Toolkit (MVT) for decryption of ios backup

UNIT V ANDROID FORENSICS 9

Android basics – Key Codes – Android Debug Bridge (ADB) – Rooting Android – Boot Process – File Systems – Security – Use of Oxygen Forensics/MobilEdit for extraction of installed applications and diagnostic info

TOTAL: 45 PERIODS

TEXT BOOKS

1. Andre Arnes, “Digital Forensics”, Wiley, 2018.
2. Chuck Easttom, “An In– depth Guide to Mobile Device Forensics”, First Edition, CRC Press, 2022.

REFERENCES

1. Vacca, J, Computer Forensics, Computer Crime Scene Investigation, 2nd Ed, Charles River Media, 2005, ISBN: 1– 58450– 389.

COURSE OUTCOMES:

Upon completion of the course, the students will be able to

- Have knowledge on digital forensics.
- Know about digital crime and investigations.
- Being forensic ready.
- Investigate, identify and extract digital evidence from iOS devices.
- Investigate, identify and extract digital evidence from Android devices.

CO – PO MAPPING

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	3	1	3	2	1	–	–	1	1	3	3
CO2	3	3	3	3	3	–	–	2	2	1	2
CO3	3	3	2	3	1	–	–	3	2	1	1
CO4	3	1	2	2	3	–	–	1	3	3	2
CO5	1	3	2	3	2	–	–	2	3	2	3

Internal Assessment				**End Semester Examination**
Assessment I (100 Marks)		**Assessment II (100 Marks)**		
Individual Assignment / Case Study / Seminar / Mini Project	**Written Test**	**Individual Assignment / Case Study / Seminar / Mini Project**	**Written Test**	**Written Examination**
40	60	40	60	100
40%				**60 %**

23CS4008	INFORMATION SECURITY	L	T	P	C
		3	0	0	3

COURSE OBJECTIVES:

- To understand the software security development life cycle, list of attacks in Network, Host and Information and write the consequences of the attack
- To analyze risks in a given activity and write the impact of risk.
- To differentiate security models and suggest best model for the given institution
- To understand the functions of IDS and Firewall
- To document security policies and management activities for an organization.

UNIT I INFORMATION SYSTEMS AND SOFTWARE ATTACKS 9

Introduction to Information Systems – Trustworthiness of information systems – Security and Access – Security SDLC – Ethical and Professional Issues, CIA Triad, Types of Malware attacks

UNIT II RISK MANAGEMENT 9

Importance of risk Management – Integration of Risk Management in SDLC – Risk Assessment – System Characterization – Threat Identification – Vulnerability Identification – Control Analysis – Impact Analysis – Risk Determination – Risk Level Matrix – Control Recommendations.

UNIT III SECURITY MODELS 9

Bell– LaPadula model – Biba model – Clark– Wilson model – Information flow model – Noninterference model – Brewer and Nash model – Graham– Denning model – Harrison– Ruzzo– Ullman model

UNIT IV PHYSICAL SECURITY DESIGN AND NETWORK SECURITY 9

Security Technology – Digital certificate – Digital Signatures – Firewall– IDS. Cryptography and Network Security – Symmetric Key Encipherment – Asymmetric Key– Encipherment – Integrity, Authentication, and Key Management, Authentication and Authorization

UNIT V CERTIFICATION, ACCREDITATION, SECURITY ASSESSMENTS AND SECURITY PROTOCOLS 9

Certification, Accreditation, and Security Assessments Roles and Responsibilities – The Security Certification and Accreditation Process – Introduction to security protocols – SSH – SSL – IPSec –Kerberos – WEP

TOTAL: 45 PERIODS

TEXT BOOKS

1. Behrouz A. Forouzan, Cryptography and Network Security, McGraw– Hill Education, 2007.
   Behrouz A. Forouzan and Debdeep Mukhopadhyay , Cryptography and Network Security: Principles and Practice, McGraw– Hill Education, 2011

REFERENCES

1. Information Security Handbook: A Guide for Managers, National Institute of Standards and Technology, 2006.
2. Mark Stamp, “Information Security Principles and Practices”, John Wiley & Sons, 2011.

COURSE OUTCOMES:

Upon completion of the course, the students will be able to

- Explain software security development life cycle, list of attacks in Network, Host and Information and write the consequences of the attack
- Analyze risks in a given activity and write the impact of risk.
- Differentiate security models and suggest best model for the given institution
- Differentiate the functions of IDS and Firewall
- Document security policies and management activities for an organization.

CO – PO MAPPING

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11
CO1	3	3	3	2	2	2	2	1	–	–	2
CO2	3	2	3	2	2	3	1	1	–	2	3
CO3	3	3	3	2	1	2	1	1	–	1	2
CO4	3	3	2	2	1	2	–	2	–	1	2
CO5	3	2	2	1	1	2	–	1	–	1	1

Internal Assessment				**End Semester Examination**
Assessment I (100 Marks)		**Assessment II (100 Marks)**		
Individual Assignment / Case Study / Seminar / Mini Project	**Written Test**	**Individual Assignment / Case Study / Seminar / Mini Project**	**Written Test**	**Written Examination**
40	60	40	60	100
40%				**60 %**