M.TECH (CYBER FORENSICS & INFORMATION SECURITY)
Department of CSE, JNTUHCEH

COURSE STRUCTURE

(Applicable for the Batch admitted from the Academic Year 2021-22 onwards)

I SEMESTER

S.No	Course Code	Subject	L	T	P	Credits
1	PC 1	Advanced Data Structures & Algorithms	3	0	0	3
2	PC 2	Mathematical Foundations of Cryptography	3	0	0	3
3	PE I	Program Elective – I	3	0	0	3
4	PE II	Program Elective - II	3	0	0	3
5	Laboratory 1	Advanced Data Structures& Algorithms Lab	0	0	4	2
6	Laboratory 2	Based on Program Elective I	0	0	4	2
7	MLC	Research Methodology & IPR	2	0	0	2
8	Audit I	Audit Course - I	2	0	0	0
		TOTAL	**16**	**0**	**8**	**18**

Program Elective I
1. Database Security
2. Cloud Computing Security
3. Blockchain Technologies

Program Elective II
1. Social Media Security
2. Mobile Application Security
3. Lightweight Cryptography

II SEMESTER

S.No	Course Code	Subject	L	T	P	Credits
1	PC 3	Vulnerability Assessment and Penetration Testing	3	0	0	3
2	PC 4	Systems and Network Security	3	0	0	3
3	PE III	Program Elective - III	3	0	0	3
4	PE IV	Program Elective - IV	3	0	0	3
5	Laboratory 3	Systems and Network Security Lab	0	0	4	2
6	Laboratory 4	Based on Program Elective - IV	0	0	4	2
7	MLC	Technical Seminar	2	0	0	2
8	Audit II	Audit Course - II	2	0	0	0
		TOTAL	**16**	**0**	**8**	**18**

Program Elective III
1. Cryptanalysis
2. Privacy PreservingData Publishing
3. Security Incident and Response Management

Program Elective IV
1. Cyber Crime Investigation & Digital Forensics
2. Data Analytics for Fraud Detection
3. Digital Watermarking and Steganography

III SEMESTER

Group Code	Group	Subject	L	T	P	Credits
	PE V	Program Elective - V	3	0	0	3
	OEC	Open Elective	3	0	0	3
	PW	Project/ Dissertation Phase–I	0	0	20	10
		TOTAL	**6**	**0**	**20**	**16**

Program Elective V

1. Authentication Techniques
2. Quantum Cryptography
3. Security in 5G Technologies

IV SEMESTER

Group Code	Group	Subject	L	T	P	Credits
	PW	Project/ dissertation Phase–II	-	-	32	16
		TOTAL	**0**	**0**	**32**	**16**

Open Elective

1. Digital Forensics
2. Ethical Hacking
3. Vulnerability Assessment and Penetration Testing

Audit Course I & II

1. EnglishforResearchPaperWriting.
2. DisasterManagement.
3. SanskritforTechnicalKnowledge.
4. ValueEducation.
5. IndianConstitution.
6. PedagogyStudies.
7. StressManagementbyyoga.
8. PersonalityDevelopmentThrough LifeEnlightenmentSkills.
9. ResearchMethodology&IPR

M.Tech CFIS I Semester **L T P C**
3 0 0 3

ADVANCED DATA STRUCTURES AND ALGORITHMS

Prerequisites

1.A course on " Data Structures"

Objectives

1. Introduces the heap data structures such as leftist heaps, binomial heaps, fibonacci and min-max heaps
2. Introduces a variety of data structures such as disjoint sets, hash tables, search structures and digital search structures

Outcomes

1. Ability to select the data structures that efficiently model the information in a problem
2. Ability to understand how the choice of data structures impact the performance of programs
3. Can Design programs using a variety of data structures, including hash tables, search structures and digital search structures

UNIT - I

Heap Structures

Introduction, Min-Max Heaps, Leftist trees, Binomial Heaps, Fibonacci heaps.

UNIT - II

Hashing and Collisions

Introduction, Hash Tables, Hash Functions, different Hash Functions:- Division Method, Multiplication Method, Mid-Square Method, Folding Method, Collisions

UNIT - III

Search Structures

OBST, AVL trees, Red-Black trees, Splay trees,

Multiway Search Trees

B-trees., 2-3 trees

UNIT - IV

Digital Search Structures

Digital Search trees, Binary tries and Patricia, Multiway Tries, Suffix trees, Standard Tries, Compressed Tries

Pattern matching

Introduction, Brute force, the Boyer –Moore algorithm, Knuth-Morris-Pratt algorithm, Naïve String, Harspool, Rabin Karp

UNIT - V

Dynamic programming, graph algorithms: DFS, BFS, topological sorting, shortest path algorithms, network flow problems. String algorithms, suffix trees, geometric algorithms.

Textbooks:

1. Fundamentals of data structures in C++ Sahni, Horowitz, Mehatha, Universities Press.
2. Introduction to Algorithms, TH Cormen, PHI

References:

1. Design methods and analysis of Algorithms, SK Basu, PHI.
2. Data Structures & Algorithm Analysis in C++, Mark Allen Weiss, Pearson Education.
3. Fundamentals of Computer Algorithms, Ellis Horowitz, SartajSahni, SanguthevarRajasekaran, 2nd Edition, Universities Press.

M.Tech CFIS I Semester **L T P C**

3 0 0 3

MATHEMATICAL FOUNDATIONS OF CRYPTOGRAPHY

Objectives

1.Build a solid mathematical basis to understand foundations of cryptography
2. Formally understand the notions related to security authentication and privacy.
3.Provide a rigorous treatment of the emerging and key subject subarea of CSE - security.

Outcomes

1.Students will gain an understanding of cryptosystems widely used to protect data security on the internet, and be able to apply the ideas in new situations as needed.

UNIT- I

Basic functions of cryptography - Encryption Schemes, Digital Signatures ,Fault Tolerant Protocols and Zero-Knowledge Proofs

The Computational Model: P , NP , and NP- Completeness, Probabilistic Polynomial Time, Non-Uniform Polynomial Time

UNIT- II

Computational Difficulty

One-Way Functions Definitions, Strong One- Way Functions, Weak One-Way Functions, Universal One-Way Function, Trapdoor One-Way Permutations Computational Indistinguishability: Definition, Relation to Statistical Closeness, Indistinguishability by Repeated Experiments, Indistinguishability by Circuits

UNIT - III

Zero-Knowledge Proof Systems

Zero-Knowledge Proofs, Perfect and Computational Zero-Knowledge, An Example (Graph Isomorphism in PZK) Zero-Knowledge with Respect to Auxiliary Inputs

UNIT - IV

Encryption Schemes

Private-Key versus Public-Key Schemes, The Syntax of Encryption Schemes, Semantic Security, Indistinguishability of Encryptions, Stream--Ciphers, Preliminaries: Block

--Ciphers

UNIT- V

Digital Signatures and Message Authentication: Attacks and security, Variants

Constructions of Message Authentication Schemes: Applying a pseudorandom function to the document

Textbook:

1. Foundations of Cryptography (two volumes), OdedGoldreich, Cambridge university Press, 2004. (Indian print available).

References:

1. Introduction to Modern Cryptography, J.Katz, Y.Lindell, Chapman Hall, USA 2007.
2. Modern cryptography - Theory and practice, Wen Bo Mao, Prentice Hall, USA, 2003 (Indian edition available)

M.Tech CFIS I Semester **L T P C**
3 0 0 3

DATABASE SECURITY
(Program Elective - I)

Prerequisites

1. A Course on "Databases"

Objectives

To study the different models involved in database security and their applications in real time world to protect the database and information associated with them.

Outcomes

- Avoid unauthorized data observation, modification.
- Ensure the data confidentiality.
- Prove that the data integrity is preserved, only authorized user has access to the data.
- Identify security threats in database systems.
- Design and Implement secure database systems.

UNIT I

Introduction (Databases and Information Systems, An example usage context, Database system concepts and architecture), Overview of Information Security,
Database design using the relational model: -Functional dependencies: Keys in a relational model, Concept of functional dependencies,Normal forms based on primary keys, BCNF Further Dependencies: Multi-valuesdependencies and fourth normal form, Join dependencies and fifth normal form, Inclusiondependencies, Other dependencies and normal forms

UNIT II

Database security lifecycle, data risk assessment, Analyze data threats, risks and vulnerabilities, Understand the need for a database security architecture, database security architecture, Implement a feedback mechanisms, Understand how to adjust policies and practices based on feedback mechanisms using different security models.

UNIT III

Database Vulnerabilities, Threats and Physical Security: distinction between data and database security from network and perimeter security, external and internal database threats, flaws in perimeter security, risks of not securing an organization's data, typical database security hierarchy, analysis general security landscape, evaluation of security fundamentals, Understand the importance for staying current with database releases, fixes and security patches , Managing USB ports and USB enabled devices, Understand the implications of the physical placement of database files and their copies

UNIT IV

Access control of relational databases, Temporal role-based access control in database management, Access control models for XML databases. Managing and Querying Encrypted Data, Security in Data Warehouses and OLAP Systems

UNIT V

Secure Semantic Web Services, Geospatial Database Security, Damage Quarantine and Recovery in Data Processing Systems, Privacy-enhanced Location-based Access Control, Efficiently Enforcing the Security and Privacy Policies in a Mobile Environment

Textbook

1. Handbook of Database Security: Applications and Trends by Michael Gertz and Sushil Jajodia
2. Database Security and Auditing, Hassan A. Afyouni, India Edition, CENGAGE Learning, 2009.
3. Database Security, Castano, Second edition, Pearson Education
4. Database security by alfred basta, melissa zgola, CENGAGE learning

M.Tech CFIS I Semester

L	T	P	C
3	0	0	3

CLOUD COMPUTING SECURITY
(Program Elective - I)

Objectives

1. Guiding Security design principles for Cloud Computing
2. Be able to understand the legal, security, forensics, personal & data privacy issues within Cloud environment
3. Understand the concepts and guiding principles for designing and implementing appropriate safeguards and countermeasures for Cloud based IT services

Outcomes

1. Approaches to designing cloud services that meets essential Cloud infrastructure characteristics on demand computing, shared resources, elasticity and measuring usage.
2. Design security architectures that assures secure isolation of physical and logical infrastructures
3. Understand the industry security standards, regulatory mandates, audit policies and compliance requirements for Cloud based infrastructures.

UNIT - I

Introduction to cloud – Basic Concepts and Terminology – Concepts and Models of cloud computing – Cloud delivery and deployment models.

UNIT - II

Cloud enablers and security – Internet, Broadband, Data centre and virtualization technologies

UNIT - III

Web and Multitenant services – Cloud security,

UNIT - IV

Agent threats: Cloud infrastructure mechanisms, Specialized cloud mechanisms,

UNIT - V

Cloud Management and Cloud Security. AWS, Azure and Google case study

Text Books

1. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, T. Mather, S. Kumaraswamy, S. Latif, O'Reilly Series, 2009.
2. Cloud Computing: Concepts, Technology & Architecture, T. Erl, R. Puttini, Z. Mahmood Prentice Hall, 2013.

References

1. The Google file system. In Proceedings of the nineteenth ACM symposium on Operating systems principles (SOSP '03). ACM, New York, NY, USA, 29-43.
2. MapReduce: simplified data processing on large clusters. Commun. ACM 51, 1, 107113, 2008.
3. Controlling data in the cloud: outsourcing computation without outsourcing control. In Proceedings of the 2009 ACM workshop on Cloud computing security (CCSW '09). ACM, New York, NY, USA, 85-90, 2009.

M.Tech CFIS I Semester **L T P C**

3 0 0 3

BLOCKCHAIN TECHNOLOGIES
(Program Elective - I)

Prerequisites

1. Knowledge in information security and applied cryptography.
2. Knowledge in distributed databases.

Objectives

1. To learn the fundamentals of Block Chain and various types of block chain and consensus mechanism.
2. To understand public block chain system, Private block chain system and consortium block chain.
3. Able to know the security issues of blockchain technology.

Outcomes

1. Able to work in the field of block chain technologies.

UNIT-I

Fundamentals of Blockchain: Introduction, Origin of Blockchain, Blockchain Solution, Components of Blockchain, Block in a Blockchain,The Technology and the Future. **Blockchain Types and Consensus Mechanism**: Introduction, Decentralization and Distribution, Types of Blockchain, Consensus Protocol.

Cryptocurrency – Bitcoin, Altcoin and Token: Introduction, Bitcoin and the Cryptocurrency, Cryptocurrency Basics, Types of Cryptocurrencies, Cryptocurrency Usage.

UNIT-II

Public Blockchain System: Introduction, Public Blockchain, Popular Public Blockchains, The Bitcoin Blockchain, Ethereum Blockchain.

Smart Contracts: Introduction, Smart Contract, Characteristics of a Smart Contract, Types of Smart Contracts, Types of Oracles, Smart Contracts in Ethereum, Smart Contracts in Industry.

UNIT-III

Private Blockchain System: Introduction, Key Characteristics of Private Blockchain, Why We Need Private Blockchain, Private Blockchain Examples, Private Blockchain and Open Source, E-commerce Site Example, Various Commands (Instructions) in E-commerce Blockchain, Smart Contract in Private Environment, State Machine, Different Algorithms of Permissioned Blockchain, ByzantineFault, Multichain.

Consortium Blockchain: Introduction, Key Characteristics of Consortium Blockchain, Why We Need Consortium Blockchain, Hyperledger Platform, Overview of Ripple, Overview of Corda.

Initial Coin Offering: Introduction, Blockchain Fundraising Methods, Launching an ICO, Investing in an ICO, Pros and Cons of Initial Coin Offering, Successful Initial Coin Offerings, Evolution of ICO,
ICO Platforms.

UNIT-IV

Security in Blockchain: Introduction, Security Aspects in Bitcoin, Security and Privacy Challenges of Blockchain in General, Performance and Scalability, Identity Management and Authentication, Regulatory Compliance and Assurance, Safeguarding Blockchain Smart Contract (DApp), Security Aspects in Hyperledger Fabric.

Applications of Blockchain: Introduction, Blockchain in Banking and Finance, Blockchain in Education, Blockchain in Energy, Blockchain in Healthcare, Blockchain in Real-estate, Blockchain in Supply Chain, The Blockchain and IoT.Limitations and Challenges of Blockchain.

UNIT-V

Blockchain Case Studies: Case Study 1 – Retail, Case Study 2 – Banking and Financial Services, Case Study 3 – Healthcare, Case Study 4 – Energy and Utilities.

Blockchain Platform using Python: Introduction, Learn How to Use Python Online Editor, Basic Programming Using Python, Python Packages for Blockchain.

Blockchain platform using Hyperledger Fabric: Introduction, Components of Hyperledger Fabric Network, Chain codes from Developer.ibm.com, Blockchain Application Using Fabric Java SDK.

Text book:

1. "Block chain Technology", Chandramouli Subramanian, Asha A.George, Abhilasj K A and Meena Karthikeyan , Universities Press.

References:

1. Blockchain Blue print for Economy, Melanie Swan, SPD Oreilly.
2. Blockchain for Business, Jai Singh Arun, Jerry Cuomo, Nitin Gauar, Pearson Addition Wesley.

M.Tech CFIS I Semester **L T P C**
3 0 0 3

SOCIAL MEDIA SECURITY
(Program Elective – II)

Objectives

1.Give introduction about the networks, its use, the need of security

Outcomes

1. Learn about browser's risks
2. Learn about Social Networking, Understands the risks while using social media. Guidelines for social networking
3. Understand how to secure different web browsers.
4. Understand how an e-mail works does; learn threats involved using an email communication, safety measures while using e-mail.

UNIT - I

Introduction to Social Media, Understanding Social Media,Different Types and Classifications,The Value of Social Media, Cutting Edge Versus Bleeding Edge,The Problems That Come With Social Media, Is Security Really an Issue? Taking the Good With the Bad

UNIT - II

Dark side

Cyber crime ,Social Engineering ,Hacked accounts , cyberstalking, cyberbullying, predators, phishing, hackers

UNIT - III

Being bold versus being overlooked

Good social media campaigns , Bad social media campaigns, Sometimes it's better to be overlooked ,Social media hoaxes, The human factor ,Content management, Promotion of social media

UNIT - IV

Risks of Social media

Introduction Public embarrassment, Once it's out there, it's out thereFalse information, Information leakage, Retention and archiving, Loss of data and equipment

UNIT - V

Policies and Privacy

Blocking users controlling app privacy ,Location awareness, Security Fake accounts passwords ,privacy and information sharing

Textbooks:

1.Interdisciplinary Impact Analysis of Privacy in Social Networks,Recognizing Your Digital Friends, Encryption for Peer-to-Peer Social NetworksCrowdsourcing and Ethics ,Authors: Altshuler Y, EloviciY, Cremers A.B, Aharony N, Pentland A. (Eds.) .
2. Social media security
https://www.sciencedirect.com/science/article/pii/B97815974998660000

M.Tech CFIS I Semester

L	T	P	C
3	0	0	3

MOBILE APPLICATION SECURITY
(Program Elective – II)

Prerequisites

1. Undergraduate level knowledge of Network Security

Objectives

1. Gain in-depth knowledge on mobile security and its relation to the new security based protocols.
2. Apply proactive and defensive measures to counter potential threats, attacks and intrusions.

Outcomes

1. By the end of this course students will be able to learn security based protocols, attacks and intrusions

UNIT-I

Top Mobile Issues and Development Strategies:

Top Issues Facing Mobile Devices, Physical Security , Secure Data Storage (on Disk), Strong Authentication with Poor Keyboards , Multiple-User Support with Security, Safe Browsing Environment , Secure Operating Systems, Application Isolation, Information Disclosure, Virus, Worms, Trojans, Spyware, and Malware , Difficult Patching/Update Process, Strict Use and Enforcement of SSL, Phishing , Cross-Site Request Forgery (CSRF), Location Privacy/Security, Insecure Device Drivers, Multifactor Authentication, Tips for Secure Mobile Application Development .

UNIT-II

WAP and Mobile HTML Security

WAP and Mobile HTML Basics , Authentication on WAP/Mobile HTML Sites , Encryption, Application Attacks on Mobile HTML Sites ,Cross-Site Scripting , SQL Injection , Cross-Site Request Forgery , HTTP Redirects , Phishing , Session Fixation , Non-SSL Login , WAP and Mobile Browser Weaknesses , Lack of HTTPOnly Flag Support , Lack of SECURE Flag Support , Handling Browser Cache , WAP Limitations.

UNIT-III

Bluetooth Security

Overview of the Technology , History and Standards , Common Uses , Alternatives , Future, Bluetooth Technical Architecture , Radio Operation and Frequency, Bluetooth Network Topology , Device Identification , Modes of Operation , Bluetooth Stack ,Bluetooth Profiles, Bluetooth Security Features , Pairing , Traditional Security Services in Bluetooth, Security "Non-Features" , Threats to Bluetooth Devices and Networks, Bluetooth Vulnerabilities, Bluetooth Versions Prior to v1.2, Bluetooth Versions Prior to v2.1.

UNIT-IV

SMS Security

Overview of Short Message Service, Overview of Multimedia Messaging Service, Wireless Application Protocol (WAP), Protocol Attacks, Abusing Legitimate Functionality, Attacking Protocol Implementations, Application Attacks, iPhone Safari, Windows Mobile MMS, Motorola RAZR JPG Overflow, Walkthroughs, Sending PDUs,Converting XML to WBXML.

UNIT-V

Enterprise Security on the Mobile OS

Device Security Options, PIN, Remote, 346 Secure Local Storage, Apple iPhone and Keychain, Security Policy Enforcement, Encryption, Full Disk Encryption, E-mail Encryption, File Encryption, Application Sandboxing, Signing, and Permissions, Application Sandboxing, Application Signing, Permissions, Buffer Overflow Protection,Windows Mobile, iPhone, Android,BlackBerry, Security Feature Summary.

Textbook:

1. Mobile Application Security, HimanshuDwivedi, Chris Clark, David Thiel, TATA McGRAW-Hill.

References:

1. Mobile and Wireless Network Security and Privacy, Kami S.Makki,et al, Springer.
2. Android Security Attacks Defenses, Abhishek Dubey, CRC Press

M.Tech CFIS I Semester

L	T	P	C
3	0	0	3

LIGHTWEIGHT CRYPTOGRAPHY
(Program Elective - II)

Prerequisites

1. Undergraduate level knowledge of Network Security

Objectives

1. Gain in-depth knowledge on Lightweight Cryptography and its relation to the new security in RFID tags
2. Apply proactive and defensive measures to counter potential threats, attacks and intrusions.

Outcomes

1. Ability to learn Cryptographic based solutions, attacks and intrusions.
2. Understand security and privacy issues in radio frequency identification (RFID) systems.
3. Understanding multiple ways to attack and defend in industrial systems.

UNIT – I

Anti-counterfeiting and RFID - Anti-Counterfeiting and Supply Chain Security, Networked RFID Systems, PC Network Architecture, A Security Primer .

UNIT –II

Security and Privacy Current Status - Addressing Insecurities and Violations of Privacy, RFID Tag Vulnerabilities in RFID Systems, From Identification to Authentication – A Review of RFID Product Authentication Techniques.

UNIT – III

Network Based Solutions - EPC System for a Safe & Secure Supply Chain and How it is Applied , The Potential of RFID and NFC in Anti-Counterfeiting , Improving the Safety and Security of the Pharmaceutical Supply Chain .

UNIT- IV

Cryptographic Solutions - Product Specific Security Based on RFID Technology, Strengthening the Security of Machine-Readable Documents, Enhancing Security of Class I Generation 2 RFID against Traceability and Cloning .

UNIT –V

Low-cost Cryptraphicsolutions : A Random Number Generator for Application in RFID Tags , A Low Cost Solution to Cloning and Authentication Based on a Lightweight Primitive, Lightweight Cryptography for Low Cost RFID .

Text book

1. Networked RFID Systems and Lightweight Cryptography by Peter H. Cole · Damith C. Ranasinghe First edition ,Springer publication 2008.

References

1. RFID Security and Privacy by YingjiuLi , Robert H. Deng
2. RFID HANDBOOK by Klaus Finkenzeller, Third edition Wiley Publications

M.Tech CFIS I Semester **L T P C**
0 0 4 2

ADVANCED DATA STRUCTURES AND ALGORITHMS LAB

Prerequisites

1. A course on "Computer Programming & Data Structures"

Objectives

1. Introduces the basic concepts of Abstract Data Types.
2. Reviews basic data structures such as stacks and queues.
3. Introduces a variety of data structures such as hash tables, search trees, tries, heaps, graphs, and B-trees.
4. Introduces sorting and pattern matching algorithms

Outcomes

1. Ability to select the data structures that effeciently model the information in a problem.
2. Ability to assess efficiency trade-offs among different data structure implementations or combinations.
3. Implement and know the application of algorithms for sorting and pattern matching.
4. Design programs using a variety of data structures, including hash tables, binary and general tree structures, search trees, tries, heaps, graphs, and B-trees.

List of Programs

1.Write a program to perform the following operations:
   a) Insert an element into a binary search tree.
   b) Delete an element from a binary search tree.
   c) Search for a key element in a binary search tree.

2.Write a program for implementing the following sorting methods:
   a) Merge sort b) Heap sort c) Quick sort

3.Write a program to perform the following operations:
   a) Insert an element into a B- tree.
   b) Delete an element from a B- tree.
   c) Search for a key element in a B- tree.

4.Write a program to perform the following operations:
   a) Insert an element into a Min-Max heap
   b) Delete an element from a Min-Max heap
   c) Search for a key element in a Min-Max heap

5. Write a program to perform the following operations:
   a) Insert an element into a Leftist tree
   b) Delete an element from a Leftist tree
   c) Search for a key element in a Leftist tree

6. Write a program to perform the following operations:
   a) Insert an element into a binomial heap
   b) Delete an element from a binomial heap.
   c) Search for a key element in a binomial heap

7. Write a program to perform the following operations:
    a) Insert an element into a AVL tree.
    b) Delete an element from a AVL search tree.
    c) Search for a key element in a AVL search tree.
8. Write a program to perform the following operations:
    a) Insert an element into a Red-Black tree.
    b) Delete an element from a Red-Black tree.
    c) Search for a key element in a Red-Black tree.
9. Write a program to implement all the functions of a dictionary using hashing.
10. Write a program for implementing Knuth-Morris-Pratt pattern matching algorithm.
11. Write a program for implementing Brute Force pattern matching algorithm.
12. Write a program for implementing Boyer pattern matching algorithm.

Textbooks:

1. Fundamentals of Data structures in C, E.Horowitz, S.Sahni and Susan Anderson Freed, 2nd Edition ,Universities Press
2. Data Structures Using C – A.S.Tanenbaum, Y. Langsam, and M.J. Augenstein, PHI/Pearson education.
3. Introduction to Data Structures in C, AshokKamthane

References:

1. The C Programming Language, B.W. Kernighan, Dennis M.Ritchie, PHI/Pearson Education
2. C Programming with problem solving, J.A. Jones & K. Harrow, DreaM.Tech Press
3. Data structures: A Pseudocode Approach with C, R.F.Gilberg And B.A.Forouzan, ,2nd Edition , Cengage Learning.

M.Tech CFIS I Semester

L	T	P	C
0	0	4	2

BLOCKCHAIN TECHNOLGIES LAB

Prerequisites:

1. Knowledge in Basics of JavaScript /Java for Hyperledger Fabric.
2. Basics of Solidity for ETH.

Objectives:

1. To learn the basic blockchain applications.
2. To be familiar with the blockchain lab setup.

Outcomes:

1.Able to work in the field of block chain technologies.

List of Experiments

1) Setup Metamask in the System and Create a wallet in the Metamask with Test Network.
2) Create multiple accounts in Metamask and perform the balance transfer between the accounts and describe the transaction specifications.
3) Setup the Ganache Tool in the system.
4) Create a custom RPC network in Metamask and connect it with Ganache tool and transfer the ether between ganache accounts.
5) Write a smart contract using a solidity program to perform the balance transfer from contract to other accounts.
6) Write a solidity program to perform the exception handling.
7) Setup the Hyperledger Fabric Network with 2 Organizations 1 Peer Each in the system.
8) Create a channel called mychannel, carchannel in the deployed network.
9) Take the existing Fabcar smart contract and add a new function to query the car on the basis of person name and deploy the smart contract on the Hyperledger Fabric Network.
10) Write an SDK program to query the person details from the deployed smart.

M.Tech CFIS I Semester

L	T	P	C
2	0	0	2

RESEARCH METHODOLOGIES & IPR

Objectives

1. Introduce research paper writing and induce paper publication skills.
2. Give the introduction to Intellectual Property Rights

Outcomes

1. Ability to distinguish research methods
2. Ability to write and publish a technical research paper
3. Ability to review papers effectively
4. IPR and Patent filing

UNIT – I

Introduction

Objective of Research; Definition and Motivation; Types of Research; Research Approaches; Steps in Research Process; Criteria of Good Research; Ethics in Research.

Research Formulation and Literature Review

Problem Definition and Formulation; Literature Review; Characteristics of Good Research Question; Literature Review Process.

UNIT – II

Data Collection

Primary and Secondary Data; Primary and Secondary Data Sources; Data Collection Methods; Data Processing; Classification of Data.

Data Analysis

Statistical Analysis; Multivariate Analysis; Correlation Analysis; Regression Analysis; Principle Component Analysis; Samplings;

UNIT – III

Research Design

Need for Research Design; Features of a Good Design; Types of Research Designs; Induction and Deduction.

Hypothesis Formulation and Testing

Hypothesis; Important Terms; Types of Research Hypothesis; Hypothesis Testing; Z-Test; tTest; f-Test; Making a Decision; Types of Errors; ROC Graphics.

UNIT – IV

Test Procedures

Parametric and Non Parametric Tests; ANOVA; Mann-Whitney Test; Kruskal-Wallis Test; Chi-Square Test; Multi-Variate Analysis.

Presentation of the Research Work

Business Report; Technical Report; Research Report; General Tips for Writing Report; Presentation of Data; Oral Presentation; Bibliography and References; Intellectual Property Rights; Open-Access Initiatives; Plagiarism.

UNIT – V

Law of Patents, Patent Searches, Ownership, Transfer

Patentability – Design Patents – Double Patenting – Patent Searching – Patent Application Process – Prosecuting the Application, Post-issuance Actions, Term and Maintenance of Patents. Ownership Rights – Sole and Joint Inventors – Inventions Made by Employees and Independent Contractors – Assignment of Patent Rights – Licensing of Patent Rights – Invention Developers and Promoters.

Patent Infringement, New Developments and International Patent Law

Direct Infringement – Inducement to Infringe – Contributory Infringement – First Sale Doctrine – Claims Interpretation – Defenses to Infringement – Remedies for Infringement – Resolving an Infringement Dispute – Patent Infringement Litigation. New Developments in Patent Law

Textbooks

1. Research Methodology. Methods &Technique , Kothari. C.R.
2. Research Methodology, S.S Vinod Chandra, S AnandHareendran, Pearson
3. Intellectual Property – Copyrights, Trademarks, and Patents by Richard Stim, Cengage Learning

References

1. Practical Research : planning and Design,Paul D. Leedy and Jeanne E. Ormrod, (8th Edition)
2. A Hand Book of Education Research , NCTE
3. Methodology of Education Research , K.S. Sidhu.
4. Tests, Measurements and Research methods in Behavioural Sciences, A.K. Singh.
5. Statistical Methods, Y.P. Agarwal.
6. Methods of Statistical Ananlysis, P.S Grewal.
7. Fundamentals of Statistics ,S.C. Gupta, V.K. Kapoor.
8. Intellectual Property Rights by Deborah E. Bouchoux, Cengage Learning.
9. Managing Intellectual Property The Strategic Imperative, Vinod V.Sople, 2nd edition, PHI Learning Private Limited.

M.Tech CFIS II Semester **L T P C**

3 0 0 3

VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Prerequisites

1. Knowledge in information security.
2. Knowledge on Web Application.

Objectives

1. Give an introduction to Vulnerability Assessment and Penetration Testing.
2. To be familiar with the Penetration Testing and Tools.
3. To get an exposure to Metasploit exploitation tool, Linux exploit and Windows exploit.
4. To gain knowledge on Web Application Security Vulnerabilities, Vulnerability analysis and Malware analysis.

Outcomes

1. Learn to handle the vulnerabilities of a Web application.

UNIT-I

Introduction

Ethics of Ethical Hacking: Why you need to understand your enemy's tactics, recognizing the gray areas in security, Vulnerability Assessment and Penetration Testing.

Penetration Testing and Tools:

Social Engineering Attacks: How a social engineering attack works, conducting a social engineering attack, common attacks used in penetration testing, preparing yourself for face-to-face attacks, defending against social engineering attacks.

UNIT-II

PhysicalPenetrationAttacks: Why a physical penetration is important, conducting a physical penetration, Common ways into a building,Defending against physical penetrations.

InsiderAttacks: Conducting an insider attack,Defending against insider attacks.

Metasploit: The Big Picture,Getting Metasploit,Using the Metasploit Console to Launch Exploits, Exploiting Client-Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit's Meterpreter, Automating and Scripting Metasploit, Going Further with Metasploit.

UNIT-III

Managing a Penetration Test: planning a penetration test, structuring a penetration test, execution of a penetration test,information sharing during a penetration test, reporting the results of a Penetration Test.

Basic Linux Exploits: Stack Operations, Buffer Overflows, Local Buffer Overflow Exploits, Exploit Development Process.

Windows Exploits: Compiling and Debugging Windows Programs, Writing Windows Exploits, Understanding Structured Exception Handling (SEH), Understanding Windows Memory Protections(XPSP3,Vista,7 and Server2008), Bypassing Windows Memory Protections.

UNIT-IV

Web Application Security Vulnerabilities:

Overview of top web application security vulnerabilities, Injection vulnerabilities, cross-Site scripting vulnerabilities, the rest of the OWASP Top Ten SQL Injection vulnerabilities, Cross-site scripting vulnerabilities.

VulnerabilityAnalysis:

Passive Analysis, Source Code Analysis, Binary Analysis.

UNIT-V

Client-Side Browser Exploits:

Why client-side vulnerabilities are interesting, Internet explorer security concepts, history of client-side exploits and latest trends, finding new browser-based vulnerabilities heap spray to exploit, protecting yourself from client-side exploit.

Malware Analysis: Collecting Malware and Initial Analysis: Malware, Latest Trends in Honeynet Technology, Catching Malware: Setting the Trap, Initial Analysis of Malware.

Text books:

1." Gray Hat Hacking-The Ethical Hackers Handbook", Allen Harper, Stephen Sims, Michael Baucom, 3rd Edition, Tata Mc Graw-Hill.

2." The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws", Dafydd Suttard, Marcus pinto, 1st Edition, Wiley Publishing.

Reference Books:

1. "Penetration Testing: Hands-on Introduction to Hacking", Georgia Weidman, 1st Edition, No Starch Press.

2." The Pen Tester Blueprint-Starting a Career as an Ethical Hacker ", L. Wylie, Kim Crawly, 1st Edition, Wiley Publications.

M.Tech CFIS II Semester **L T P C**

3 0 0 3

SYSTEMS AND NETWORK SECURITY

Prerequisites

1. A Course on "Computer Networks"
2. A Course on "Network Security"

Objectives

1.A brief explanation of the objective is to provide knowledge on different types of Intrusions occur at various Network levels , and level of security provisions required when the systems are used at different networks in LAN,WAN

Outcomes

1. Students will get the knowledge in detection, protection of Intrusions.
2. It gives an opportunity to students to get awareness on the level of security required for a system in Intranet ,Internet ,cellular networks

UNIT - I

Detecting System Intrusions

Monitoring Key Files in the System, Zero Day attacks, Fullpacket capture devices ,Data correlation ,SEIM, Network-Based Detection of System Intrusions

Preventing System Intrusions

Symptoms of Intrusions ,Security policies , Risk Analysis ,Controlling user Access, Intrusion Prevention capabilities

UNIT - II

Guarding Against Network Intrusions

Traditional Reconnaissance and Attacks, Malicious Software, Defense in Depth, Preventive Measures, Intrusion Monitoring and Detection, Reactive Measures, Network-Based Intrusion Protection

Internet Security - Internet Protocol Architecture,. Internet Threat Model, Defending against Attacks on the Internet, Internet Security Checklist

UNIT - III

Intranet Security

Smartphones and Tablets in the Intranet ,SecurityConsiderationsPlugging the Gaps: NAC and AccessControl, Measuring Risk: Audits,. Guardian at the Gate: Authentication,and Encryption ,Wireless Network Security , Shielding the Wire: NetworkProtection,Weakest Link in Security: User Training , Documenting the Network: Change Management **UNIT - IV**

Local Area Network Security

Identify Network Threats, Establish Network Access Controls, Risk Assessment, Listing Network Resources, Threats, Security Policies, The Incident-Handling Process, Secure Design Through Network, Access Controls , IDS Defined NIDS: Scope and Limitations, Firewalls , Dynamic NAT Configuration Packet Filtering: IP Filtering Routers, ApplicationLayer Firewalls: Proxy Servers

UNIT - V

Cellular Network Security - The State of the Art of Cellular Network Security, Cellular Network Attack Taxonomy, Cellular Network Vulnerability Analysis

RFID Security - RFID challenges ,RFID protections

Text Books

1. Network and System Security ,John R Vacca , 2nd edition , Syngress publications

M.Tech CFIS II Semester **L T P C**

3 0 0 3

CRYPTANALYSIS
(Program Elective - III)

Prerequisites

A Course on Network Security, Mathematics"

Objectives

To understand the importance of cryptanalysis in our increasingly computer-driven world.
To understand the fundamentals of Cryptography
To understand the Lattice- based cryptanalysis and elliptic curves and pairings
To understand birthday- based algorithms for functions and attacks on stream ciphers # To apply the techniques for secure transactions in real world applications

Outcomes

Ability to apply cryptanalysis in system design to protect it from various attacks.
Ability to identify and investigate vulnerabilities and security threats and the mechanisms to counter them.
Ability to analyze security of cryptographic algorithm against brute force attacks, birthday attacks.

UNIT-I

A bird's – eye view of modern Cryptography: Preliminaries, Defining Security in Cryptography Mono alphabetic Ciphers: Using Direct Standard Alphabets, The Caesar Cipher, Modular arithmetic, Direct Standard alphabets, Solution of direct standard alphabets by completing the plain component, Solving direct standard alphabets by frequency considerations, Alphabets based on decimations of the normal sequence, Solution of decimated standard alphabets, Mono alphabets based on linear transformation.

Poly alphabetic Substitution: Poly alphabetic ciphers, Recognition of poly alphabetic ciphers, Determination of number of alphabets, Solution of individual alphabets if standard, Poly alphabetic ciphers with a mixed plain sequences, Matching alphabets , Reduction of a poly alphabetic cipher to a mono alphabetic ciphers with mixed cipher sequences

UNIT- II

Transposition : Columnar transposition, Solution of transpositions with Completely filled rectangles, Incompletely filled rectangles, Solution of incompletely filled rectangles – Probable word method, Incompletely filled rectangles general case, Repetitions between messages ; identical length messages.

Sieve algorithms: Introductory example: Eratosthenes's sieve, Sieving for smooth composites

UNIT- III

Brute force Cryptanalysis: Introductory example: Dictionary attacks , Brute force and the DES Algorithm, Brute force as a security mechanism, Brute force steps in advanced cryptanalysis, Brute force and parallel computers.

The birthday paradox: Sorting or not?: Introductory example: Birthday attacks on modes of operation, Analysis of birthday paradox bounds, Finding collisions, Application to discrete logarithms in generic groups.

UNIT- IV

Birthday- based algorithms for functions: Algorithmic aspects, Analysis of random functions, Numbertheoretic applications, A direct cryptographic application in the context of blockwise Security, Collisions in hash functions.

Attacks on stream ciphers: LFSR- based key stream generators, Correlation attacks, Noisy LFSR model, Algebraic attacks, Extension to some non- linear shift registers, The cube attack.

UNIT-V

Lattice- based cryptanalysis: Direct attacks using lattice reduction, Coppersmith's small roots attacks. Elliptic curves and pairings: Introduction to elliptic curves, The Weil pairing, the elliptic curve factoring method.

Text Books:

1. "Elementary Cryptanalysis A Mathematical Approach" by Abraham Sinkov, The mathematical Association of America (lnc).
2. "Algorithmic Cryptanalysis" by Antoine joux, CRC Press'

References:

1. Algebraic Cryptanalysis, Bard Gregory, Springer, 2009
2. Cryptanalysis of Number Theoretic Ciphers, Sameul S. Wag staff, Champan & Hall/CRC
3. Cryptanalysis: A Study of Cipher and Their Solution, Helen F. Gaines,1989

M.Tech CFIS II Semester **L T P C**
3 0 0 3

PRIVACYPRESERVINGDATAPUBLISHING
(Program Elective - III)

Prerequisites

A Course on Network Security, Mathematics"

Objectives

1. To understand the importance of cryptanalysis in our increasingly computer-driven world.
2. To understand the fundamentals of Cryptography
3. To understand the Lattice- based cryptanalysis and elliptic curves and pairings
4. To understand birthday- based algorithms for functions and attacks on stream ciphers
5. To apply the techniques for secure transactions in real world applications

Outcomes

1. Ability to apply cryptanalysis in system design to protect it from various attacks.
2. Ability to identify and investigate vulnerabilities and security threats and the mechanisms to counter them.
3. Ability to analyze security of cryptographic algorithm against brute force attacks, birthday attacks.

UNIT-I

A bird's – eye view of modern Cryptography: Preliminaries, Defining Security in Cryptography
Mono alphabetic Ciphers: Using Direct Standard Alphabets, The Caesar Cipher, Modular arithmetic, Direct Standard alphabets, Solution of direct standard alphabets by completing the plain component, Solving direct standard alphabets by frequency considerations, Alphabets based on decimations of the normal sequence, Solution of decimated standard alphabets, Mono alphabets based on linear transformation.
Poly alphabetic Substitution: Poly alphabetic ciphers, Recognition of poly alphabetic ciphers, Determination of number of alphabets, Solution of individual alphabets if standard, Poly alphabetic ciphers with a mixed plain sequences, Matching alphabets , Reduction of a poly alphabetic cipher to a mono alphabetic ciphers with mixed cipher sequences

UNIT- II

Transposition: Columnar transposition, Solution of transpositions with Completely filled rectangles, Incompletely filled rectangles, Solution of incompletely filled rectangles – Probable word method, Incompletely filled rectangles general case, Repetitions between messages ; identical length messages.
Sieve algorithms: Introductory example: Eratosthenes's sieve, Sieving for smooth composites

UNIT- III

Brute force Cryptanalysis: Introductory example: Dictionary attacks , Brute force and the DES Algorithm, Brute force as a security mechanism, Brute force steps in advanced cryptanalysis, Brute force and parallel computers.
The birthday paradox: Sorting or not?: Introductory example: Birthday attacks on modes of operation, Analysis of birthday paradox bounds, Finding collisions, Application to discrete logarithms in generic groups.

UNIT- IV

Birthday- based algorithms for functions: Algorithmic aspects, Analysis of random functions, Number theoretic applications, A direct cryptographic application in the context of blockwise Security, Collisions in hash functions.
Attacks on stream ciphers: LFSR- based key stream generators, Correlation attacks, Noisy LFSR model, Algebraic attacks, Extension to some non- linear shift registers, The cube attack.

UNIT-V

Lattice- based cryptanalysis: Direct attacks using lattice reduction, Coppersmith's small roots attacks. Elliptic curves and pairings: Introduction to elliptic curves, The Weil pairing, the elliptic curve factoring method.

Text Books:

1. "Elementary Cryptanalysis A Mathematical Approach" by Abraham Sinkov, The mathematical Association of America (lnc).
2. "Algorithmic Cryptanalysis" by Antoine joux, CRC Press'

References:

1. Algebraic Cryptanalysis, Bard Gregory, Springer, 2009
2. Cryptanalysis of Number Theoretic Ciphers, Sameul S. Wag staff, Champan & Hall/CRC
3. Cryptanalysis: A Study of Cipher and Their Solution, Helen F. Gaines,1989

M.Tech CFIS II Semester

L	T	P	C
3	0	0	3

SECURITY INCIDENT AND RESPONSE MANAGEMENT
(Program Elective - III)

Prerequisites

1. Knowledge in information security and applied cryptography.
2. Knowledge in Operating Systems.

Objectives

1. Give an introduction to preparation of inevitable incident and incident detection and characterization.
2. To get an exposure to live data collection, Forensic duplication.
3. To gain knowledge on data analysis including Windows and Mac OS Systems.

Outcomes

1. Learn how to handle the incident response management.

UNIT-I

Introduction: Preparing for the Inevitable incident: Real world incident, IR management incident handbook, Pre-incident preparation, Preparing the Organization for Incident Response, Preparing the IR team, PreparingtheInfrastructureforIncidentResponse.

Incident Detection and Characterization: Getting the investigationstarted on the right foot, collecting initial facts, Maintenance of Case Notes,Understanding Investigative Priorities. Discovering the scope of incident: Examining initial data, Gathering and reviewing preliminary evidence, determining a course of action, Customer data loss scenario, Automated clearing fraud scenario.

UNIT-II

Data Collection: Live Data Collection: When to perform live response, Selecting a live response tool, what to collect, collection best practices, Live data collection on Microsoft Windows Systems, Live Data Collection on Unix-Based Systems.

Forensic Duplication: Forensic Image Formats, Traditional duplication, Live system duplication, Duplication of Enterprise Assets.

UNIT-III

Network Evidence: The case for network monitoring, Types for network monitoring, Setting Up a Network Monitoring System,Network Data, Analysis,Collect Logs Generated from Network Events.

Enterprise Services: Network Infrastructure Services, Enterprise Management Applications, Web servers, Database Servers,

UNIT-IV

Data Analysis: Analysis Methodology: Define Objectives, Know your data, Access your data, Analyse your data, Evaluate Results.

Investigating Windows Systems: NTFS and File System analysis, Prefetch, Event logs, Scheduled Tasks, The Windows Registry, OtherArtifactsofInteractiveSessions, Memory Forensics, Alternative Persistence Mechanisms.

UNIT-V

Investigating Mac OS X Systems: HFS+andFileSystemAnalysis, Core Operating systems data.
Investigating Applications: What is Application Data?, Where is application data stored?, General Investigation methods, Web Browser, Email Clients, Instant Message Clients.

Text books:

1. “Incident Response and Computer Forensics”, Jason T.Luttgens, Mathew Pepe and Kevin Mandia, 3rd Edition, Tata McGraw-Hill Education.
2. “Cyber Security Incident Response-How to Contain, Eradicate, and Recover from Incidents”, Eric.C.Thompson,Apress.

Reference Books:

1. “The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk”, N.K. McCarthy,Tata McGraw-Hill.

M.Tech CFIS II Semester **L T P C**

3 0 0 3

CYBER CRIME INVESTIGATION & DIGITAL FORENSICS
(Program Elective - IV)

Prerequisites

1.Knowledge of information technology fundamentals (computer hardware, operating systems, applications and networking) is required.

Objectives

1.An introduction to the methodology and procedures associated with digital forensic analysis in a network environment

Outcomes

1. Obtain and analyze digital information for possible use as evidence in civil, criminal or administrative cases.
2. They will learn about the importance of digital forensic principles and procedures, legal considerations, digital evidence controls

UNIT – I

Foundations of Digital Forensics : Digital Evidence ,Principles of Digital Forensics,
Challenging aspects of Digital Evidence
The Role of computers in crime, Cyber Crime Law

UNIT – II

Digital Investigations : Digital Investigation process models, Applying Scientific method in Digital Investigations ,Handling A digital Crime scene:Fundamental Principles, Surveying and Preserving Digital Investigation

UNIT - III

Voilent Crime and Digital Investigation : The role of Computers in violent crime , Processing Digital crime scene , Investigative Reconstruction ,Digital Evidence as Alibi

UNIT - IV

Cyberstalking , Computer basics for Digital Forensics , Applying Forensics science to computers, Digital Evidence on windows systems, Digital Evidence on unix systems

UNIT - V

Network Forensics : Networks basics for Digital Investigators, Applying Forensics science to networks, Digital Evidence on physical and datalink layers, Digital Evidence on Network and Transport layers.

Text Books

1. Digital Evidence and computer Crime by EoghanCasey Academic Press Third Edition
2. Real Digital Forensics for Handheld Devices , E. P. Dorothy, Auerback Publications, 2013.
2. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012.
3. Handbook of Digital Forensics and Investigation, E. Casey, Academic Press, 2010

M.Tech CFIS II Semester **L T P C**

3 0 0 3

DATA ANALYTICS FOR FRAUD DETECTION
(Program Elective - IV)

Objectives

1. Discuss the overall process of how data analytics is applied
2. Discuss how data analytics can be used to better address and identify risks
3. Help mitigate risks from fraud and waste for our clients and organizations

Outcomes

1. Formulate reasons for using data analysis to detect fraud.
2. Explain characteristics and components of the data and assess its completeness.
3. Identify known fraud symptoms and use digital analysis to identify unknown fraud symptoms.
4. Automate the detection process.
5. Verify results and understand how to prosecute fraud

UNIT - I

Introduction: Defining Fraud, Anomalies versus,Fraud, Types of Fraud, Assess the Risk of Fraud, Fraud Detection, Recognizing Fraud, Data Mining versus Data Analysis and Analytics, Data Analytical Software, Anomalies versus Fraud within Data, Fraudulent Data Inclusions and Deletions

UNIT - II

The Data Analysis Cycle, Evaluation and Analysis, Obtaining Data Files, Performing the Audit, File Format Types, Preparation for Data Analysis, Arranging and Organizing Data, Statistics and Sampling, Descriptive Statistics, Inferential Statistics

UNIT - III

Data Analytical Tests,Benford's Law, Number Duplication Test , Z-Score, Relative Size Factor Test, Same-Same-Same Test , Same-Same-Different Test

UNIT - IV

Advanced Data Analytical Tests

Correlation, Trend Analysis, , GEL-1 and GEL-2 , Skimming and Cash Larceny, Billing schemes : and Data Familiarization, , Benford's Law Tests, Relative Size Factor Test , Match Employee Address to Supplier data

UNIT - V

Payroll Fraud , Expense Reimbursement Schemes , Register disbursement schemes

Textbook:

1. Fraud and Fraud Detection: A Data Analytics Approach by Sunder Gee , Wiley

M.Tech CFIS II Semester **L T P C**

3 0 0 3

DIGITAL WATERMARKING AND STEGANOGRAPHY
(Program Elective - IV)

Objectives

1. To learn about the watermarking models and message coding
2. To learn about watermark security and authentication.
3. To learn about steganography Perceptual models

Outcomes

1. Know the History and importance of watermarking and steganography
2. Analyze Applications and properties of watermarking and steganography
3. Demonstrate Models and algorithms of watermarking
4. Possess the passion for acquiring knowledge and skill in preserving authentication of Information
5. Identify theoretic foundations of steganography andsteganalysis

UNIT - I

Introduction

Information Hiding, Steganography and Watermarking – History of watermarking – Importance of digital watermarking – Applications – Properties – Evaluating watermarking systems.

Watermarking models & message coding

Notation – Communications – Communication based models – Geometric models – Mapping messages into message vectors – Error correction coding – Detecting multi-symbol watermarks.

UNIT - II

Watermarking with side information &analyzing errors

Informed Embedding – Informed Coding – Structured dirty-paper codes - Message errors – False positive errors – False negative errors – ROC curves – Effect of whitening on error rates.

UNIT - III

Perceptual models

Evaluating perceptual impact – General form of a perceptual model –
Examples of perceptual models – Robust watermarking approaches - Redundant Embedding, Spread Spectrum Coding, Embedding in Perceptually significant coefficients

UNIT - IV

Watermark security & authentication

Security requirements – Watermark security and cryptography – Attacks – Exact authentication – Selective authentication – Localization – Restoration.

UNIT - V

Steganography

Steganography communication – Notation and terminology – Information-theoretic foundations of steganography – Practical steganographic methods – Minimizing the embedding impact – Steganalysis

Text Books

1. Digital Watermarking and Steganography, Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, Margan Kaufmann Publishers, New York, 2008.
2. Digital Watermarking, Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Margan Kaufmann Publishers, New York, 2003.
3. Techniques and Applications of Digital Watermarking and Contest Protection, Michael Arnold, Martin Schmucker, Stephen D. Wolthusen ,Artech House, London, 2003.
4. Digital Watermarking for Digital Media, JuergenSeits, IDEA Group Publisher, New York, 2005.
5. Disappearing Cryptography – Information Hiding: Steganography & Watermarking, Peter Wayner, Morgan Kaufmann Publishers, New York, 2002.

M.Tech CFIS II Semester **L T P C**

0 0 4 2

SYSTEMS AND NETWORK SECURITY LAB

Objectives

1.The main objective is to get knowledge in Configuring DNS Server,Detecting malicious codes and analysing networks through tools ,implementing various Encryption algorithms

Outcomes

1. Get the knowledge in detection,protection of Intrusions,malicious codes
2. To get awareness on DNS server, webcrawler, encryption the level of security required for a system in Intranet, Internet,cellular networks

List of Experiments

1. Write a procedure to Logon and Logoff to linux in both Text mode and graphical mode.
2. Configure a DNS Server with a domain name of your choice.
3. Configure FTP on Linux Server. Transfer files to demonstrate the working of the same. 4.Detection of Malicious Code in Registry and Task Manager
5. Checking for rootkits existence in windows.
6. Extracting website map using sam spade (any web crawler)
7. Techniques to stop web crawler
8. Sniff the network traffic while performing port scanning using Nmap.
9. Perform port scanning on Metasploitable 2 vulnerable VM
10. Install JCrypt tool (or any other equivalent) and demonstrate Asymmetric, Symmetric crypto algorithm, Hash and Digital/PKI signatures studied in theory Network Security and Management.

11.Write a client-server program where client sends a text message to server and server sends the text message to client by changing the case (uppercase and lowercase) of each character in the message.

12. Write a client-server program to implement following classical encryption techniques:

(I) Ceaser cipher (II) Transposition cipher
(III) Row substitution cipher (IV)Hill cipher

Text Books

1.Network and System Security ,John R Vacca , 2nd edition , Syngress publications

M.Tech CFIS II Semester **L T P C**

0 0 4 2

CYBER CRIME INVESTIGATION & DIGITAL FORENSICS LAB

Objectives

1. To provide students with a comprehensive overview of collecting, investigating, preserving, and presenting evidence of cyber crime left in digital storage devices, emails, browsers, mobile devices using different Forensics tools
2. To Understand file system basics and where hidden files may lie on the disk, as well as how to extract the data and preserve it for analysis.
3. Understand some of the tools of e-discovery.
4. To understand the network analysis ,Registry analysis and analyse attacks using different forensics tools

Outcomes

1. Learn the importance of a systematic procedure for investigation of data found on digital storage media that might provide evidence of wrong-doing
2. To Learn the file system storage mechanisms and retrieve files in hidden format
3. Learn the use of computer forensics tools used in data analysis.
4. Learn how to find data that may be clear or hidden on a computer disk, find our the open ports for the attackers through network analysis , Registry analysis.

Experiments

1. **Perform email analysis** using the tools like Exchange EDB viewer , MBOX viewer and View user mailboxes and public folders , Filter the mailbox data based on various criteria, Search for particular items in user mailboxes and public folders
2. **Perform Browser history analysis** and get the downloaded content , history ,saved logins,searches ,websites visited etc using Foxton Forensics tool,Dumpzilla .
3. **Perform mobile analysis** in the form of retrieving call logs ,SMS log ,all contacts list using the forensics tool like SAFT
4. **Perfrom Registry analysis** and get boottime logging using process monitor tool
5. **Perform Disk imaging and cloning the** using the X-way Forensics tools
6. **Perform Data Analysis i.e**History about open file and folder, and view folder actionsusing Lastview activity tool
7. **Perform Network analysis** using theNetwork Miner tool **.**
8. **Perform information for incident response** using the crowd Response tool
9. **Perform File type detection using** Autospy tool
10. **Perform Memory capture and analysis** using the Live RAM capture or any forensic tool

Textbooks

1. Real Digital Forensics for Handheld Devices , E. P. Dorothy, Auerback Publications, 2013.
2. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012.
3. Handbook of Digital Forensics and Investigation, E. Casey, Academic Press, 2010
4. Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, C. H. Malin, E. Casey and J. M. Aquilina, Syngress, 2012
5. The Best Damn Cybercrime and Digital Forensics Book Period, J. Wiles and A.Reyes, Syngress, 2007.

M.Tech CFIS II Semester **L T P C**
0 0 4 2

DATA ANALYTICS FOR FRAUD DETECTION LAB

Objective

1.The main objective is to perform data analysis and detect fraud activities

Outcome

1.Gain knowledge in performing fraud detection by data analysis using different tools

List Of Experiments

1. Perform data analysis i.e history about open file and folder, and view folder actions using last view activity tool
2. Perform file type detection using auto spy tool
3. Perform network analysis using the network miner tool
4. Create a social networking website login page using phishing techniques
5. Analyse ddos attacks and write code to prevent ddos attacks
6. Analyse sql injection attacks and write code to prevent ddosattacks
7. Analyse buffer overflow attacks and write code to prevent ddos attacks .
8. Perform memory capture and analysis using the live ram capture or any forensic tool

Text Books

1.Fraud and Fraud Detection: A Data Analytics Approach by Sunder Gee, Wiley

M.Tech CFIS II Semester **L T P C**
0 0 4 2

DIGITAL WATERMARKING AND STEGANOGRAPHY LAB

Objective

1.To provide knowledge in implementing watermarking and stegnography lab

Outcomes

1.To implement watermarking techniques and Stegnography techniques using code

List of Experiments

1. Write a code to implement watermarking in the document.
2. Write a code to remove watermarking from the document
3. Write a code to hide the data in image
4. Write a code to hide the photo in plain sight
5. Write a code to hide to implement Information hiding
6. Implement the Hiding the text in image using stegnography S-Tool
7. Write a code to retrieve the hidden image from data
8. Write a code to retrieve the hidden text from image
9. Write a code to extract photo from plainsight
10. Write a code to implement encryption using stegnography

Textbooks:

1. Digital Watermarking and Steganography, Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker,"Margan Kaufmann Publishers, New York, 2008.
2. Digital Watermarking, Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Margan Kaufmann Publishers, New York, 2003.
3. Techniques and Applications of Digital Watermarking and Contest Protection, Michael Arnold, Martin Schmucker, Stephen D. Wolthusen ,Artech House, London, 2003.
4. Digital Watermarking for Digital Media, JuergenSeits, IDEA Group Publisher, New York, 2005.
5. Disappearing Cryptography – Information Hiding: Steganography & Watermarking, Peter Wayner, Morgan Kaufmann Publishers, New York, 2002.

M.Tech CFIS II Semester **L T P C**
3 0 0 3

AUTHENTICATION TECHNIQUES
(Program Elective - V)

Unit-1: Definition of Authentication, Identification/verification, Stages and steps of authentication, Authentication Entity : User, Device and Application; Authentication attributes: Source, Location, Path, Time duration etc.; Authentication Types : Direct / Indirect, One Way / Mutual, On demand/ Periodic/ Dynamic/Continuous authentication, Assisted/Automatic; 3 Factors of authentication; Passwords, Generation of passwords of varied length and of mixed type, OTP, passwords generation using entity identity credentials; Secure capture, processing, storage, verification and retrieval of passwords;

Unit-2: Physical identification using smart cards, remote control device, proximity sensors, surveillance camera, authentication in Card present / Card Not Present transactions as ATM/ PoS Device, mobile phone, wearable deviceand IoT device based authentication; single sign-on; Symmetric Key Generation, Key Establishment, Key Agreement Protocols;

Unit-3: Biometrics – photo, face, iris, retinal, handwriting, signature, fingerprint, palm print, hand geometry, voice – Text based and text independent voice authentication, style of talking, walking, writing, keystrokes, gait etc. multi-modal biometrics.

Unit-4: Matching algorithms, Patterns analysis,errors, performance measures, ROC Curve; Authentication Standards – International, UIDAI Standard. Kerberos, X.509 Authentication Service, Public Key Infrastructure, Scanners and Software; Web Authentication Methods: Http based, Token Based, OAuthand API.

Unit-5: User authentication protocols in multi-server environment, BAN Logic, Representation of authentication protocols using BAN Logic, Random Oracle Model, Scyther Tools, Proverif tool, Chebyshev Chaotic Map, Fuzzy Extractor, Fuzzy Extractor Map, Bloom Filter, LU Decomposition based User Authentication, Blockchain based authentication.

Text Books:

1. Protocols for Authentication and Key Establishment, Colin Boyd and Anish Mathuria, springer, 2021
2. Guide to Biometrics,Ruud M.Bolle,SharathPankanti, Nalini K. Ratha,Andrew W. Senior, Jonathan H. Connell,Springer 2009.

References:

1.Digital Image Processing using MATLAB, Rafael C. Gonzalez, Richard Eugene Woods, 2nd Edition, Tata McGraw-Hill Education 2010.
2.Biometric System and Data Analysis: Design, Evaluation, and data Mining,TedDunstone and Neil Yager, Springer.
3. Biometrics Technologies and verification Systems, John Vacca, , Elsevier Inc. , 2007.
4.Pattern Classification, Richard O. Duda, David G.Stork,Peter E. Hart, Wiley 2007.

M.Tech CFIS II Semester **L T P C**
3 0 0 3

QUANTUM CRYPTOGRAPHY
(Program Elective - V)

Course objectives:
The course is designed to train the graduates in:
1. In depth understanding of quantum cryptography.
2. Understanding of the cryptographic techniques.
3. To understand quantum cryptography encryption and decryption schemes.

Course Outcomes:
Graduates after completing the course shall gain:
1. Ability to understand concepts of quantum cryptography and cryptographic techniques.
2. To work in research institutions / Industry in the field of quantum cryptography.
3. To design new or modify existing quantum cryptographic techniques.

UNIT I
Quantum Information Theory, Unconditional Secure Authentication, Entropy, Quantum Key Distribution, Quantum Channel, Public Channel, QKD Gain, Finite Resources

UNIT II
Adaptive Cascade
Introduction, Error Correction and the Cascade Protocol, Adaptive Initial Block-Size Selection, Fixed Initial Block-Size, Dynamic Initial Block-Size, Examples

UNIT III
Attack Strategies on QKD Protocols:Introduction, Attack Strategies in an Ideal Environment, Individual Attacks in an Realistic Environment
QKD Systems: Introduction, QKD Systems

UNIT IV
Statistical Analysis of QKD Networks in Real-Life Environment: Statistical Methods, Statistical Analysis
QKD Networks Based on Q3P: QKD Networks, PPP, Q3P, Routing, Transport

UNIT V
Quantum-Cryptographic Networks from a Prototype to the Citizen: The SECOQC Project, How to Bring QKD into the “Real” Life
The Ring of Trust Model: Introduction, Model of the Point of Trust, Communication in the Point of Trust Model, Exemplified Communications, A Medical Information System Based on the Ring of Trust

Textbooks:
1. Kollmitzer C., Pivk M. (Eds.), Applied Quantum Cryptography, Lect. Notes Phys. 797 (Springer, Berlin Heidelberg 2010)

M.Tech CFIS II Semester **L T P C**
3 0 0 3

SECURITY IN 5G TECHNOLOGIES
(Program Elective - V)

Pre-requisite: Nil

Outcomes

1. Able to understand the security of 5G
2. Able to realize the evolution of technologies in Mobile Devices

Unit I

Evolution of Cellular Systems: Introduction, First Generation Cellular Systems, Second Generation Cellular Systems, Third Generation Cellular Systems, Cellular Systems beyond 3G, Fourth Generation Cellular Systems, 5G Mobile Networks: Requirements, Enabling Technologies and Research Activities, Mobile Networks Security Landscape,

Unit II

Design Principles for 5G Security, Cyber Security Business Models in 5G, Physical Layer Security, 5G- WLAN Security, Safety of 5G Network Physical Infrastructures, Customer Edge Switching: A Security Framework, Evaluation of CES Security, Deployment in 5G Networks

Unit III

Software Defined Security Monitoring in 5G Networks: 5G Device and User Security, IoT Security, User Privacy, Identity and Trust in 5G, 5G Positioning: Security and Privacy Aspects, Outdoor versus Indoor Positioning Technologies, Passive versus Active Positioning, Brief Overview of 5G Positioning Mechanisms, Survey of Security Threats and Privacy Issues in 5G Positioning , Main Privacy Concerns, Passive versus Active Positioning Concepts, Physical- Layer Based Security Enhancements, Mechanisms for Positioning in 5G, Enhancing Trustworthiness

Unit IV

Cryptographic Techniques for Security and Privacy of Positioning, Legislation on User Location Privacy in 5G

5G Cloud and Virtual Network Security: Mobile Virtual Network Operators (MVNO) Security, NFV and NFV- based Security Services, A Brief Introduction to NFV, NFV, SDN, and a Telco Cloud Common NFV Drivers, NFV Security: Challenges and Opportunities, NFV- based Security Services

Unit V

Cloud and MEC Security: Cloud Computing in 5G Networks, MEC in 5G Networks, Security Challenges in 5G Cloud, Security Challenges in 5G MEC, Security Architectures for 5G Cloud and MEC Regulatory Impact on 5G Security and Privacy: Regulatory Objectives for Security and Privacy, Legal Framework for Security and Privacy, Security and Privacy Issues in New 5G Technologies, Relevance Assessment of Security and Privacy Issues for Regulation, Analysis of Potential Regulatory Approaches

Text Book:

1. A Comprehensive Guide to 5G Security by Madhusanka LiyanageIjaz Ahmad, Ahmed Bux Abro,Andrei Gurtov, Mika Ylianttila

M.Tech CFIS III Semester

L	T	P	C
3	0	0	3

DIGITAL FORENSICS
(Open Elective)

Objectives
1. Know the history and evaluation of digital forensics
2. Describe various types of cyber crime
3. Understand benefits of forensics
4. Implement forensics readiness plan

Outcomes
1. Interpret and appropriately apply the laws and procedures associated with identifying, acquiring, examining and presenting digital evidence.
2. Create a method for gathering, assessing and applying new and existing legislation and industry trends specific to the practice of digital forensics

UNIT - I
Computer Forensics Fundamentals

Introduction to Computer Forensics, Use of Computer Forensics in Law Enforcement, Computer Forensics Assistance to Human Resources/Employment Proceedings, Computer Forensics Services, Benefits of Professional Forensics Methodology, Steps taken by Computer Forensics Specialists, Types of Computer Forensics Technology: Types of Military Computer Forensic Technology, Types of Law Enforcement — Computer Forensic Technology — Types of Business Computer Forensic Technology Computer Forensics Evidence and Capture: Data Recovery Defined — Data Back-up and Recovery — The Role of Back-up in Data Recovery — The Data-Recovery Solution.

UNIT - II
Evidence Collection and Data Seizure

Why Collect Evidence? Collection Options — Obstacles — Types of Evidence — The Rules of Evidence — Volatile Evidence — General Procedure — Collection and Archiving — Methods of Collection — Artifacts — Collection Steps — Controlling Contamination: The Chain of Custody Duplication and Preservation of Digital Evidence: Preserving the Digital Crime Scene — Computer Evidence Processing Steps — Legal Aspects of Collecting and Preserving Computer Forensic Evidence Computer Image Verification and Authentication: Special Needs of Evidential Authentication — Practical Consideration —Practical Implementation.

UNIT - III
Computer Forensics analysis and validation
Determining what data to collect and analyze, validating forensic data, addressing data-hiding techniques, performing remote acquisitions
Network Forensics
Network forensics overview, performing live acquisitions, developing standard procedures for network forensics, using network tools, examining the honeynet project.
Processing Crime and Incident Scenes
Identifying digital evidence, collecting evidence in private-sector incident scenes, processing law enforcement crime scenes, preparing for a search, securing a computer

incident or crime scene, seizing digital evidence at the scene, storing digital evidence, obtaining a digital hash, reviewing a case

UNIT - IV

Current Computer Forensic tools

Evaluating computer forensic tool needs, computer forensics software tools, computer forensics hardware tools, validating and testing forensics software E-Mail Investigations: Exploring the role of e-mail in investigation, exploring the roles of the client and server in email, investigating e-mail crimes and violations, understanding e-mail servers, using specialized e-mail forensic tools.

Cell phone and mobile device forensics

Understanding mobile device forensics, understanding acquisition procedures for cell phones and mobile devices.

UNIT - V

Working with Windows and DOS Systems

Understanding file systems, exploring Microsoft File Structures, Examining NTFS disks, Understanding whole disk encryption, windows registry, Microsoft startup tasks, MS-DOS startup tasks, virtual machines.

Textbooks:

1. Computer Forensics, Computer Crime Investigation by John R. Vacca, Firewall Media, New Delhi.
2. Computer Forensics and Investigations by Nelson, Phillips Enfinger, Steuart, CENGAGE Learning

References:

1. Real Digital Forensics by Keith J. Jones, Richard Bejtiich, Curtis W. Rose, AddisonWesley Pearson Education
2. Forensic Compiling, A Tractitioneris Guide by Tony Sammes and Brian Jenkinson, Springer International edition.
3. Computer Evidence Collection & Presentation by Christopher L.T. Brown, Firewall Media.
4. Homeland Security, Techniques & Technologies by Jesus Mena, Firewall Media.
5. Software Forensics Collecting Evidence from the Scene of a Digital Crime by Robert M. Slade, TMH 2005
6. Windows Forensics by Chad Steel, Wiley India Edition.

M.Tech CFIS III Semester

L	T	P	C
3	0	0	3

ETHICAL HACKING
(Open Elective)

Prerequisites

1. A course on "Operating Systems"
2. A course on "Computer Networks"
3. A course on "Network Security and Cryptography"

Objectives

1. The aim of the course is to introduce the methodologies and framework of ethical hacking for enhancing the security.
2. The course includes-Impacts of Hacking; Types of Hackers; Information Security Models; Information Security Program; Business Perspective; Planning a Controlled Attack; Framework of Steps (Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Deliverable and Integration)

Outcomes

1. Gain the knowledge of the use and availability of tools to support an ethical hack
2. Gain the knowledge of interpreting the results of a controlled attack
3. Understand the role of politics, inherent and imposed limitations and metrics for planning of a test
4. Comprehend the dangers associated with penetration testing

UNIT- I

Introduction

Hacking Impacts, The Hacker

Framework

Planning the test, Sound Operations, Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Final Analysis, Deliverable, Integration

Information Security Models

Computer Security, Network Security, Service Security, Application Security, Security Architecture

Information Security Program

The Process of Information Security, Component Parts of Information Security Program, Risk Analysis and Ethical Hacking

UNIT - II

The Business Perspective

Business Objectives, Security Policy, Previous Test Results, Business Challenges

Planning for a Controlled Attack

Inherent Limitations, Imposed Limitations, Timing is Everything, Attack Type, Source Point, Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Intermediates, Law Enforcement

UNIT - III

Preparing for a Hack

Technical Preparation, Managing the Engagement

Reconnaissance

Social Engineering, Physical Security, Internet Reconnaissance

UNIT - IV

Enumeration

Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase

Exploitation

Intutive Testing, Evasion, Threads and Groups, Operating Systems, Password Crackers, RootKits, applications, Wardialing, Network, Services and Areas of Concern

UNIT - V

Deliverable

The Deliverable, The Document, Overal Structure, Aligning Findings, Presentation

Integration

Integrating the Results, Integration Summary, Mitigation, Defense Planning, Incident Management, Security Policy, Conclusion

Textbook:

1.The Ethical Hack: A Framework for Business Value Penetration Testing, Auerbach Publications, James S. Tiller, CRC Press

References:

1. Ethical Hacking and Countermeasures Attack Phases, EC-Council, Cengage Learning
2. Hands-On Ethical Hacking and Network Defense, Michael Simpson, Kent Backman, James Corley, Cengage Learning

M.Tech CFIS III Semester **L T P C**
3 0 0 3

VULNERABILITY ASSESSMENT AND PENETRATION TESTING
(Open Elective)

Prerequisites

1. Knowledge in information security.
2. Knowledge on Web Application.

Objectives

5. Give an introduction to Vulnerability Assessment and Penetration Testing.
6. To be familiar with the Penetration Testing and Tools.
7. To get an exposure to Metasploit exploitation tool, Linux exploit and Windows exploit.
8. To gain knowledge on Web Application Security Vulnerabilities, Vulnerability analysis and Malware analysis.

Outcomes

1. Learn to handle the vulnerabilities of a Web application.

UNIT-I

Introduction

Ethics of Ethical Hacking: Why you need to understand your enemy's tactics, recognizing the gray areas in security, Vulnerability Assessment and Penetration Testing.

Penetration Testing and Tools:

Social Engineering Attacks: How a social engineering attack works, conducting a social engineering attack, common attacks used in penetration testing, preparing yourself for face-to-face attacks, defending against social engineering attacks.

UNIT-II

PhysicalPenetrationAttacks: Why a physical penetration is important, conducting a physical penetration, Common ways into a building,Defending against physical penetrations.

InsiderAttacks: Conducting an insider attack,Defending against insider attacks.

Metasploit: The Big Picture,Getting Metasploit,Using the Metasploit Console to Launch Exploits, Exploiting Client-Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit's Meterpreter, Automating and Scripting Metasploit, Going Further with Metasploit.

UNIT-III

Managing a Penetration Test: planning a penetration test, structuring a penetration test, execution of a penetration test,information sharing during a penetration test, reporting the results of a Penetration Test.

Basic Linux Exploits: Stack Operations, Buffer Overflows, Local Buffer Overflow Exploits, Exploit Development Process.

Windows Exploits: Compiling and Debugging Windows Programs, Writing Windows Exploits, Understanding Structured Exception Handling (SEH), Understanding Windows Memory Protections(XPSP3,Vista,7 and Server2008), Bypassing Windows Memory Protections.

UNIT-IV

Web Application Security Vulnerabilities:

Overview of top web application security vulnerabilities, Injection vulnerabilities, cross-Site scripting vulnerabilities, the rest of the OWASP Top Ten SQL Injection vulnerabilities, Cross-site scripting vulnerabilities.

VulnerabilityAnalysis:

Passive Analysis, Source Code Analysis, Binary Analysis.

UNIT-V

Client-Side Browser Exploits:

Why client-side vulnerabilities are interesting, Internet explorer security concepts, history of client-side exploits and latest trends, finding new browser-based vulnerabilities heap spray to exploit, protecting yourself from client-side exploit.

Malware Analysis: Collecting Malware and Initial Analysis: Malware, Latest Trends in Honeynet Technology, Catching Malware: Setting the Trap, Initial Analysis of Malware.

Text books:

1." Gray Hat Hacking-The Ethical Hackers Handbook", Allen Harper, Stephen Sims, Michael Baucom, 3rd Edition, Tata Mc Graw-Hill.

2." The Web Application Hacker's Handbook-Discovering and Exploiting Security flaws", Dafydd Suttard, Marcus pinto, 1st Edition, Wiley Publishing.

Reference Books:

1. "Penetration Testing: Hands-on Introduction to Hacking", Georgia Weidman, 1st Edition, No Starch Press.

2." The Pen Tester Blueprint-Starting a Career as an Ethical Hacker ", L. Wylie, Kim Crawly, 1st Edition, Wiley Publications.

M.Tech CFIS III Semester

L	T	P	C
2	0	0	0

ENGLISH FOR RESEARCH PAPER WRITING
(AUDIT COURSE-II)

Course Objectives: To help students:

1. Understand the essentials of writing skills and their level of readability
2. Learn about what to write in each section
3. Ensure qualitative presentation with linguistic accuracy.

Course Outcomes: Students will be able to:

1. Understand writing skills and level of readability
2. Write title, abstract, different sections in research paper
3. Develop the skills needed while writing a research paper

Syllabus

Unit 1 Overview of a Research Paper- Planning and Preparation- Word Order- Useful Phrases - Breaking up Long Sentences-Structuring Paragraphs and Sentences- Being Concise and Removing Redundancy -Avoiding Ambiguity

Unit 2 Essential Components of a Research Paper- Abstracts- Building Hypothesis- Research Problem - Highlight Findings- Hedging and Criticizing, Paraphrasing and Plagiarism, Chapterisation

Unit 3 Introducing Review of the Literature – Methodology - Analysis of the Data- Findings - Discussion- Conclusions-Recommendations.

Unit 4 Key skills needed for writing a Title, Abstract, and Introduction

Unit 5 Appropriate language to formulate Methodology, incorporate Results, put forth Arguments and draw Conclusions

Suggested Reading:

1. Goldbort R (2006) Writing for Science, Yale University Press (available on Google Books)
Model Curriculum of Engineering & Technology PG Courses [Volume-I]
2. Day R (2006) How to Write and Publish a Scientific Paper, Cambridge University Press
3. Highman N (1998), Handbook of Writing for the Mathematical Sciences, SIAM. Highman'sbook .
4. Adrian Wallwork , English for Writing Research Papers, Springer New York Dordrecht
Heidelberg London, 2011

****

M.Tech CFIS III Semester

L	T	P	C
2	0	0	0

VALUE EDUCATION
(AUDIT COURSE-I)

Course Objectives: To help the students:
1. Understand value of education and self- development
2. Imbibe good values
3. Know about the importance of character

Course outcomes: Students will be able to:
1. Acquire knowledge about self-development
2. Learn the importance of Human values
3. Develop the overall personality

Syllabus

Unit1 Values and Self-development –Social Values and Individual Attitudes. Work Ethics, Indian Vision of Humanism. Ethical Standards and Principles. Value Judgments

Unit2 Importance of Cultivating Values. Sense of Duty. Devotion, Self-reliance, Confidence, Concentration. Truthfulness, Cleanliness. Honesty, Humanity. National Unity. Patriotism. Love for Nature, Discipline

Unit3 Personalityand Behavior Development - Soul and Scientific Attitude- Integrity and Discipline. Punctuality- Compassion and Benevolence -Positive Thinking- Composure and Equipoise- Dignity of Labour.

Unit4 Universal Brotherhood and Religious Tolerance. True Friendship. Happiness Vs Suffering- Aware of Self-destructive Habits. Association and Cooperation. Eco-friendly Consciousness

Unit5 Character and Competence – Values of Scriptures- Self-management and Good health. Science of Reincarnation. Equality, Nonviolence, Humility, Role of Women-Secular Thinking- Mind your Mind, Self-control- Non Ethnocentric Behavior

Suggested Readings

1. Chakroborty, S.K. "*Values and Ethics for organizations Theory and practice*", Oxford University Press, New Delhi. 1998.
2. Dostoyevsky, Fyodor, Constance Garnett, and Ernest J. Simmons. *Crime and Punishment*. New York: Modern Library, 1950. Print.
3. Galsworthy, John. *Justice.* Czechia, Good Press, 2019.
4. TED Talks

****