

**JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD**

**M. Tech. (CYBER FORENSICS & INFORMATION SECURITY)**

**EFFECTIVE FROM ACADEMIC YEAR 2022 - 23 ADMITTED BATCH**

**R22 COURSE STRUCTURE AND SYLLABUS**

**I YEAR 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** | **Program Elective II** |
| 1. Database Security | 1. Social Media Security |
| 2. Cloud Computing Security | 2. Mobile Application Security |
| 1. Blockchain Technologies | 1. Lightweight Cryptography |

**I YEAR 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 | 0 | 0 | 4 | 2 |
| 8 | Audit II | Audit Course - II | 2 | 0 | 0 | 0 |
|  |  | **TOTAL** | **14** | **0** | 12 | **18** |

|  |  |
| --- | --- |
| **Program Elective III** | **Program Elective IV** |
| 1. Cryptanalysis | 1. Cyber Crime Investigation & Digital Forensics |
| 2. Privacy PreservingData Publishing | 2. Data Analytics for Fraud Detection |
| 1. Security Incident and Response Management | 1. Digital Watermarking and Steganography |

**II YEAR I – 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 | 12 | 6 |
|  |  | **TOTAL** | **6** | **0** | **12** | **12** |

**Program Elective V**

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

**II YEAR II – SEMESTER**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Course Code** | **Subject** | **L** | **T** | **P** | **Credits** |
| Dissertation | Dissertation Work Review–II | 0 | 0 | 12 | 16 |
| Dissertation | Dissertation Viva-Voce | 0 | 0 | 28 | 14 |
|  | **TOTAL** | **0** | **0** | **40** | **20** |

**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 & 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, SocialEngineering, Hackedaccounts,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>

**References:**

1. Social media security by Michael Cross, Syngress.

**M.Tech CFIS I Semester**

**MOBILE APPLICATION SECURITY**

**(Program Elective – II)**

**Prerequisites**

1. Undergraduate level knowledge of Network Security

**Objectives**

**L T P C 3 0 0 3**

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& 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.

1. Implement and know the application of algorithms for sorting and pattern matching.
2. 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 AVL tree.   
b) Delete an element from a AVL search tree.   
c) Search for a key element in a AVL search tree.

6. 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.

7. Write a program to implement all the functions of a dictionary using hashing.   
  
8. Write a program for implementing Knuth-Morris-Pratt pattern matching algorithm.   
  
9. Write a program for implementing Brute Force pattern matching algorithm.   
  
10. Write a program for implementing Boyer pattern matching algorithm

11. Write a program for implementing Shortest path algorithm

12. Write a program for implementing graph traversal DFS and BFS

13. Write a program for implementing String algorithms

14. Write a program for implementing geometric algorithms.

**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 METHODOLOGY& IPR**

**Course Objectives:**

* To understand the research problem
* To know the literature studies, plagiarism and ethics
* To get the knowledge about technical writing
* To analyze the nature of intellectual property rights and new developments
* To know the patent rights

**Course Outcomes:** At the end of this course, students will be able to

* Understand research problem formulation.
* Analyze research related information
* Follow research ethics
* Understand that today’s world is controlled by Computer, Information Technology, but tomorrow world will be ruled by ideas, concept, and creativity.
* Understanding that when IPR would take such important place in growth of individuals & nation, it is needless to emphasis the need of information about Intellectual Property Right to be promoted among students in general & engineering in particular.
* Understand that IPR protection provides an incentive to inventors for further research work and investment in R & D, which leads to creation of new and better products, and in turn brings about, economic growth and social benefits.

**UNIT-I:**

Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem.

Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations

**UNIT-II:**

Effective literature studies approaches, analysis, Plagiarism, Research ethics

**UNIT-III:**

Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee

**UNIT-IV:**

Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Copyleft and Creative Commons Licensing. Process of Patenting and Development: technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT.

**UNIT-V:**

Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information

and databases. Geographical Indications. New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.

**TEXT BOOKS:**

1. Stuart Melville and Wayne Goddard, “Research methodology: an introduction for science &

engineering students’”

1. Wayne Goddard and Stuart Melville, “Research Methodology: An Introduction”

**REFERENCES:**

1. Ranjit Kumar, 2nd Edition , “Research Methodology: A Step by Step Guide for beginners”
2. Halbert, “Resisting Intellectual Property”, Taylor & Francis Ltd ,2007.
3. Mayall , “Industrial Design”, McGraw Hill, 1992.
4. Niebel , “Product Design”, McGraw Hill, 1974.
5. Asimov , “Introduction to Design”, Prentice Hall, 1962.
6. Robert P. Merges, Peter S. Menell, Mark A. Lemley, “ Intellectual Property in New

Technological Age”, 2016.

7. T. Ramappa, “Intellectual Property Rights Under WTO”, S. Chand, 2008

**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, Defence 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

**References:**

1. Network and System Security by Zheng Yan, Springer

**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

**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.

**UNIT- II**

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- III**

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.

**UNIT- IV**

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.

**UNIT-V**

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.

**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**

# **PRIVACY PRESERVING DATA PUBLISHING**

**(Program Elective - III)**

**Pre requisites:** Probability Mathematics, Design and Analysis of Algorithms.

**Course Outcomes:** By the end of the course students will  
CO1: Apply anonymization methods for sensitive data protection.  
CO2: Apply state-of art techniques for data privacy protection.  
CO3: Design privacy preserving algorithms for real-world applications.  
CO4: Identify security and privacy issues in OLAP systems.  
CO5: Apply information metrics for Maximizing the preservation of information in the anonymization process.

**UNIT I**

Data Collection and Data Publishing, What Is Privacy-Preserving Data Publishing, Attack Models and Privacy Models: Record Linkage Model, Attribute Linkage Model, Probabilistic Model, Modeling Adversary’s Background Knowledge

**UNIT II**

Anonymization Operations, Generalization and Suppression, Anatomization and Permutation, Random Perturbation, Information Metrics, General Purpose Metrics, Special Purpose Metrics, Trade-Off Metrics, Anonymization Algorithms: Algorithms for the Record Linkage Model, Algorithms for the Attribute Linkage Model, Algorithms for the Table Linkage Model, Algorithms for the Probabilistic Attack Model, Attacks on Anonymous Data,

**UNIT III**

Anonymization for Classification Analysis: Introduction, Anonymization Problems for Red Cross BTS, High-Dimensional Top-Down Specialization (HDTDS), Workload-Aware Mondrian, Bottom-Up Generalization, Genetic Algorithm, Evaluation Methodology, Anonymization for Cluster Analysis: Introduction, Anonymization Framework for Cluster Analysis, Dimensionality Reduction-Based Transformation

**UNIT IV**

Multiple Views Publishing: Introduction, Checking Violations of *k*-Anonymity on Multiple Views, Checking Violations with Marginals, Anonymizing Sequential Releases with New Attributes: Introduction, Monotonicity of Privacy, Anonymization Algorithm for Sequential Releases, Anonymizing Incrementally Updated Data Records: Introduction, Continuous Data Publishing, Dynamic Data Republishing

**{{{**

**UNIT V**

Collaborative Anonymization for Vertically Partitioned Data: Introduction, Privacy-Preserving Data Mashup, Cryptographic Approach, Collaborative Anonymization for Horizontally Partitioned Data: Introduction, Privacy Model, Overview of the Solution, Anonymizing Transaction Data: Introduction, Cohesion Approach, Band Matrix Method, *km*-Anonymization, Transactional *k*-Anonymity, Anonymizing Query Logs

**Text Books:**

1. Benjamin C.M. Fung, Ke Wang, Ada Wai-Chee Fu and Philip S. Yu, Introduction to Privacy-Preserving Data Publishing: Concepts and Techniques, 1st Edition, Chapman & Hall/CRC, 2010.  
2. Charu C. Aggarwal, Privacy-Preserving Data Mining: Models and Algorithms, 1st Edition, Springer, 2008.

**References:**

1. Privacy Preserving Data Mining - Issues & Techniques by Sanjay Garg, Scholars Press

**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.

**References:**

1. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, J. Sammons, Syngress Publishing, 2012.

2. 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**
4. Formulate reasons for using data analysis to detect fraud.
5. Explain characteristics and components of the data and assess its completeness.
6. Identify known fraud symptoms and use digital analysis to identify unknown fraud symptoms.
7. Automate the detection process.
8. 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

**References:**

1. Data Analysis Techniques for Fraud Detection by Gerard Blokdyk

**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.

**References:**

1. Techniques and Applications of Digital Watermarking and Contest Protection, Michael Arnold, Martin Schmucker, Stephen D. Wolthusen ,Artech House, London, 2003.
2. Digital Watermarking for Digital Media, JuergenSeits, IDEA Group Publisher, New York, 2005.
3. 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. Using Snort to create log file to record the packet data
2. Using GnuPGcreate public and private keys
3. Detection of Malicious Code in Registry and Task Manager
4. Checking for rootkits existence in windows.
5. Extracting website map using sam spade (any web crawler)
6. Using N-Stalker, analyze a web session for vulnerabilities.
7. Sniff the network traffic while performing port scanning using Nmap.
8. 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.
9. 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.
10. Write a client-server program to implement following classical encryption techniques:

(I) Ceaser cipher (II) Rail fence cipher

(III) Row substitution cipher (IV)Play fair 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 Autopsy and View deleted items.
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 or UFED.
4. **Perfrom Registry analysis** and get boottime logging using process monitor tool
5. **Perform Disk imaging and cloning the** using the Falcon - Hard Drive Forensics Tool
6. **Perform Data Analysis i.e**History about open file and folder, and view folder actionsusing Lastview activity tool
7. **Perform Read-only access to** any data storage device to provide integrity to the data**.**
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 FTK Imager.

**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 steganography 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 steganography

**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 III Semester** **L T P C**

**3 0 0 3**

**AUTHENTICATION TECHNIQUES**

**(Program Elective - V)**

**Course Objectives:**

1. Students can explain what it means to verify someone’s identity and compare how verification works in different situations.
2. Students can express why authentication is important in cybersecurity.

**Course Outcomes:**

1. On completion of the course, student will be able to–
2. describe how and why a username and password combination is used for authentication.
3. summarize some high-level weaknesses to using shared secrets to authenticate to a website or computer.
4. identify good password practices on the user side and the system side, and discuss the costs of implementing them.

**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 III 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)

**References:**

1. Quantum Cryptography by Donald J. Barrett.

**M.Tech CFIS III 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 beyond3G, Fourth Generation Cellular Systems, 5G Mobile Networks: Requirements. Enabling Technologies and Research Activities.

**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.

**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.

**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.

**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 5G Technologies.

**Text Book:**

1. A Comprehensive Guide to 5G Security by Madhusanka Livanageljaz Ahmad, Ahmed Bux

Abro,Andrei Gurtov, Mika Ylianttila.

# **IPR (Open Elective)**

**M.Tech CFIS II Year I Sem. L T P C**

**3 0 0 3**

**Course Objectives:**

1. To explain the art of interpretation and documentation of research work
2. To explain various forms of intellectual property rights
3. To discuss leading International regulations regarding Intellectual Property Rights

**Course Outcomes:** Upon the Successful Completion of the Course, the Students would be able to:

1. Understand types of Intellectual Property
2. Analyze trademarks and its functionality
3. Illustrate law of copy rights and law of patents

**UNIT- I**

**Introduction to Intellectual property:** Introduction, types of intellectual property, international organizations, agencies and treaties, importance of intellectual property rights.

**UNIT - II**

**Trade Marks:** Purpose and function of trademarks, acquisition of trade mark rights, protectable matter, selecting, and evaluating trade mark, trade mark registration processes.

**UNIT - III**

**Law of copy rights:** Fundamental of copy right law, originality of material, rights of reproduction, rights to perform the work publicly, copy right ownership issues, copy right registration, notice of copy right, international copy right law.

**Law of patents:** Foundation of patent law, patent searching process, ownership rights and transfer

**UNIT - IV**

**Trade Secrets:** Trade secret law, determination of trade secrete status, liability for misappropriations of trade secrets, protection for submission, trade secrete litigation.

**Unfair competition:** Misappropriation right of publicity, false advertising.

**UNIT - V**

**New development of intellectual property:** new developments in trade mark law; copy right law, patent law, intellectual property audits.

International overview on intellectual property, international – trade mark law, copy right law, international patent law, and international development in trade secrets law.

**TEXT BOOKS & REFERENCES:**

1. Intellectual property right, Deborah. E. Bouchoux, Cengage learning.
2. Intellectual property right – Unleashing the knowledge economy, prabuddha ganguli, Tata McGraw Hill Publishing company ltd.

# **FAULT TOLERANCE SYSTEMS (Open Elective)**

**M.Tech CFIS II Year I Sem.**

**Course Objectives:**

1. To know the different advantages and limits of fault avoidance and fault tolerance techniques.
2. To impart the knowledge about different types of redundancy and its application for the design of computer system being able to function correctly even under presence of faults and data errors.
3. To understand the relevant factors in evaluating alternative system designs for a specific set of requirements.
4. To understand the subtle failure modes of "fault-tolerant" distributed systems.

**Course Outcomes:** Upon the Successful Completion of the Course, the Students would be able to:

1. Become familiar with general and state of the art techniques used in design and analysis of fault tolerant digital systems.
2. Be familiar with making system fault tolerant, modeling and testing, and benchmarking to evaluate and compare systems.

**UNIT - I**

**Introduction to Fault Tolerant Computing:** Basic concepts and overview of the course; Faults and their manifestations, Fault/error modeling, Reliability, availability and maintainability analysis, System evaluation, performance reliability tradeoffs.

**UNIT - II**

**System level fault diagnosis:** Hardware and software redundancy techniques. Fault tolerant system design methods, Mobile computing and Mobile communication environment, Fault injection methods.

**UNIT - III**

**Software fault tolerance:** Design and test of defect free integrated circuits, fault modeling, built in selftest, data compression, error correcting codes, simulation software/hardware, fault tolerant system design, CAD tools for design for testability.

**UNIT - IV**

**Information Redundancy and Error Correcting Codes:** Software Problem. Software Reliability Models and Robust Coding Techniques, Reliability in Computer Networks Time redundancy. Re execution in SMT, CMP Architectures, Fault Tolerant Distributed Systems, Data replication.

**UNIT - V**

**Case Studies in FTC:** ROC, HP Non-Stop Server. Case studies of fault tolerant systems and current research issues.

**TEXT BOOK:**

1. Fault Tolerant Computer System Design by D. K. Pradhan, Prentice Hall.

**REFERENCES:**

1. Fault Tolerant Systems by I. Koren, Morgan Kauffman.
2. Software Fault Tolerance Techniques and Implementation by L. L. Pullum, Artech House Computer Security Series.
3. Reliability of Computer Systems and Networks: Fault Tolerance Analysis and Design by M. L. Shooman, Wiley.

# **INTRUSION DETECTION SYSTEMS (Open Elective)**

**M.Tech CFIS II Year I Sem. L T P C**

**3 0 0 3**

**Prerequisites:**Computer Networks, Computer Programming

**Course Objectives:**

1. Compare alternative tools and approaches for Intrusion Detection through quantitative analysis to determine the best tool or approach to reduce risk from intrusion.
2. Identify and describe the parts of all intrusion detection systems and characterize new and emerging IDS technologies according to the basic capabilities all intrusion detection systems share.

**Course Outcomes:** After completion of the course, students will be able to:

1. Possess a fundamental knowledge of Cyber Security.
2. Understand what vulnerability is and how to address most common vulnerabilities.
3. Know basic and fundamental risk management principles as it relates to Cyber Security and Mobile Computing.
4. Have the knowledge needed to practice safer computing and safeguard your information using Digital Forensics.
5. Understand basic technical controls in use today, such as firewalls and Intrusion Detection systems.
6. Understand legal perspectives of Cyber Crimes and Cyber Security.

**UNIT - I**

The state of threats against computers, and networked systems-Overview of computer security solutions and why they fail-Vulnerability assessment, firewalls, VPN’s -Overview of Intrusion Detection and Intrusion Prevention, Network and Host-based IDS

**UNIT - II**

Classes of attacks - Network layer: scans, denial of service, penetration Application layer: software exploits, code injection-Human layer: identity theft, root access-Classes of attackers-Kids/hackers/sop Hesitated groups-Automated: Drones, Worms, Viruses

**UNIT - III**

A General IDS model and taxonomy, Signature-based Solutions, Snort, Snort rules, Evaluation of IDS, Cost sensitive IDS

**UNIT - IV**

Anomaly Detection Systems and Algorithms-Network Behavior Based Anomaly Detectors (rate based)Host-based Anomaly Detectors-Software Vulnerabilities-State transition, Immunology, Payload Anomaly Detection

**UNIT - V**

Attack trees and Correlation of alerts- Autopsy of Worms and Botnets-Malware detection -Obfuscation, polymorphism- Document vectors.

Email/IM security issues-Viruses/Spam-From signatures to thumbprints to zero-day detection-Insider Threat issues-Taxonomy-Masquerade and Impersonation Traitors, Decoys and Deception-Future: Collaborative Security

**TEXT BOOKS:**

1. Peter Szor, The Art of Computer Virus Research and Defense, Symantec Press ISBN 0-321- 30545-3.
2. Markus Jakobsson and Zulfikar Ramzan, Crimeware, Understanding New Attacks and Defenses.

**REFERENCE BOOKS:**

1. Saiful Hasan, Intrusion Detection System, Kindle Edition.
2. Ankit Fadia, Intrusion Alert: An Ethical Hacking Guide to Intrusion Detection.

**Online Websites/Materials:**

1. <https://www.intechopen.com/books/intrusion-detection-systems/>

**Online Courses:**

1. <https://www.sans.org/course/intrusion-detection-in-depth>
2. <https://www.cybrary.it/skill-certification-course/ids-ips-certification-training-course>

# **DIGITAL FORENSICS (Open Elective)**

**M.Tech CFIS II Year I Sem. L T P C**

**3 0 0 3**

Objectives1. 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

Outcomes1. 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, Addison Wesley 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.

# **OPTIMIZATION TECHNIQUES (Open Elective)**

**M.Tech CFIS II Year I Sem. L T P C**

**3 0 0 3**

**Prerequisite:** Mathematics –I, Mathematics –II **Course Objectives:**

1. To introduce various optimization techniques i.e classical, linear programming, transportation problem, simplex algorithm, dynamic programming
2. Constrained and unconstrained optimization techniques for solving and optimizing electrical and electronic engineering circuits design problems in real world situations.
3. To explain the concept of Dynamic programming and its applications to project implementation.

**Course Outcomes:** After completion of this course, the student will be able to:

1. explain the need of optimization of engineering systems.
2. understand optimization of electrical and electronics engineering problems.
3. apply classical optimization techniques, linear programming, simplex algorithm, transportation problem.
4. apply unconstrained optimization and constrained non-linear programming and dynamic programming.
5. Formulate optimization problems.

**UNIT - I**

**Introduction and Classical Optimization Techniques:** Statement of an Optimization problem – design vector – design constraints – constraint surface – objective function – objective function surface - classification of Optimization problems.

**Linear Programming:** Standard form of a linear programming problem – geometry of linear programming problems – definitions and theorems – solution of a system of linear simultaneous equations – pivotal reduction of a general system of equations – motivation to the simplex method – simplex algorithm.

**UNIT - II**

**Transportation Problem:** Finding initial basic feasible solution by north – west corner rule, least cost method and Vogel’s approximation method – testing for optimality of balanced transportation problems. Degeneracy.

**Assignment problem** – Formulation – Optimal solution - Variants of Assignment Problem; Traveling Salesman problem.

**UNIT - III**

**Classical Optimization Techniques:** Single variable Optimization – multi variable Optimization without constraints – necessary and sufficient conditions for minimum/maximum – multivariable Optimization with equality constraints: Solution by method of Lagrange multipliers – Multivariable Optimization with inequality constraints: Kuhn – Tucker conditions.

Single Variable Nonlinear Unconstrained Optimization: Elimination methods: Uni Model function-its importance, Fibonacci method & Golden section method.

**UNIT - IV**

Multi variable nonlinear unconstrained optimization: Direct search methods – Univariant method, Pattern search methods – Powell’s, Hooke - Jeeves, Rosenbrock’s search methods. Gradient methods: Gradient of function & its importance, Steepest descent method, Conjugate direction methods: FletcherReeves method & variable metric method.

**UNIT - V**

**Dynamic Programming:** Dynamic programming multistage decision processes – types – concept of sub optimization and the principle of optimality – computational procedure in dynamic programming – examples illustrating the calculus method of solution - examples illustrating the tabular method of solution.

**TEXT BOOKS:**

1. Optimization Techniques & Applications by S.S.Rao, New Age International.

2. Optimization for Engineering Design by Kalyanmoy Deb, PHI

**REFERENCES:**

1. George Bernard Dantzig, Mukund Narain Thapa, “Linear programming”, Springer series in Operations Research 3rd edition, 2003.
2. H. A. Taha, “Operations Research: An Introduction”, 8th Edition, Pearson/Prentice Hall, 2007.
3. Optimization Techniques by Belegundu & Chandrupatla, Pearson Asia.
4. Optimization Techniques Theory and Practice by M.C. Joshi, K.M. Moudgalya, Narosa Publications

# **CYBER PHYSICAL SYSTEMS (Open Elective)**

**M.Tech CFIS II Year I Sem. L T P C**

**3 0 0 3**

**Course Objective:** To learn about design of cyber-physical systems

**Course Outcomes:** Upon the Successful Completion of the Course, the Students would be able to:

1. Understand the core principles behind CPS
2. Identify Security mechanisms of Cyber physical systems
3. Understand Synchronization in Distributed Cyber-Physical Systems

**UNIT - I**

**Symbolic Synthesis for Cyber-Physical Systems**

Introduction and Motivation, Basic Techniques - Preliminaries, Problem Definition, Solving the Synthesis Problem, Construction of Symbolic Models, Advanced Techniques: Construction of Symbolic Models, Continuous-Time Controllers, Software Tools

**UNIT - II**

**Security of Cyber-Physical Systems**

Introduction and Motivation, Basic Techniques - Cyber Security Requirements, Attack Model, Countermeasures, Advanced Techniques: System Theoretic Approaches

**UNIT - III**

**Synchronization in Distributed Cyber-Physical Systems:** Challenges in Cyber-Physical Systems, A Complexity-Reducing Technique for Synchronization, Formal Software Engineering, Distributed Consensus Algorithms, Synchronous Lockstep Executions, Time-Triggered Architecture, Related Technology, Advanced Techniques

**UNIT - IV**

**Real-Time Scheduling for Cyber-Physical Systems**

Introduction and Motivation, Basic Techniques - Scheduling with Fixed Timing Parameters, Memory Effects, Multiprocessor/Multicore Scheduling, Accommodating Variability and Uncertainty

**UNIT - V**

**Model Integration in Cyber-Physical Systems**

Introduction and Motivation, Causality, Semantic Domains for Time, Interaction Models for Computational Processes, Semantics of CPS DSMLs, Advanced Techniques, ForSpec, The Syntax of CyPhyML, Formalization of Semantics, Formalization of Language Integration.

**TEXT BOOKS:**

1. Raj Rajkumar, Dionisio De Niz, and Mark Klein, Cyber-Physical Systems, Addison-Wesley Professional.
2. Rajeev Alur, Principles of Cyber-Physical Systems, MIT Press, 2015

# **GRAPH ANALYTICS (Open Elective)**

**M.Tech CFIS II Year I Sem. L T P C**

**3 0 0 3**

**Course Objectives:**

1. To explore the concept of Graphs and related algorithms.
2. To learn new ways to model, store, retrieve and analyze graph-structured data.
3. To be aware of advanced concepts in graph analytic techniques and its applications.

**Course Outcomes:** Upon Successful Completion of the Course, the Students would be able to:

1. Understand Large-scale Graph and its Characteristics
2. Analyze Breadth-First Search Algorithm
3. Illustrate Recent Advances in Scalable Network Generation

**UNIT - I**

**Introduction and Application of Large-scale Graph:** Characteristics, Complex Data Sources - Social Networks, Simulations, Bioinformatics; Categories- Social, Endorsement, Location, Co-occurrence graphs; Graph Data structures, Parallel, Multicore and Graph Algorithms

**UNIT - II Algorithms: Search and Paths**

A Work-Efficient Parallel Breadth-First Search Algorithm (or How To Cope With the Nondeterminism of Reducers), Multi-Objective Shortest Paths

**UNIT - III Algorithms: Structure**

Multicore Algorithms for Graph Connectivity Problems, Distributed Memory Parallel Algorithms for Massive Graphs, Massive-Scale Distributed Triangle Computation and Applications

**UNIT - IV Models**

Recent Advances in Scalable Network Generation, Computational Models for Cascades in Massive Graphs, Executing Dynamic Data-Graph Computations Deterministically Using Chromatic Scheduling.

**UNIT - V Frameworks and Software**

Graph Data Science Using Neo4j, A Cloud-Based Approach to Big Graphs, Interactive Graph Analytics at Scale in Arkouda

**TEXT BOOKS:**

1. David A. Bader, Massive Graph Analytics, CRC Press

**REFERENCES:**

1. Stanley Wasserman, Katherine Faust, "Social Network Analysis: Methods and Applications”, (Structural Analysis in the Social Sciences), Cambridge University Press, 1995.
2. Matthew O. Jackson, “Social and Economic Networks”, Princeton University Press, 2010.
3. Tanja Falkowski, "Community Analysis in Dynamic Social Networks", (Dissertation), University Magdeburg, 2009.