# M.Tech. Degree

# PROGRAMME

# in

# COMPUTER SCIENCE AND ENGINEERING

# (CYBER SECURITY)

# CURRICULUM

# (w. e. f. Session 2025-26)




## DEPARTMENT OF COMPUTER ENGINEERING
## NATIONAL INSTITUTE OF TECHNOLOGY
## KURUKSHETRA - 136119

# VISION AND MISSION OF THE INSTITUTE

**VISION**

To be a role-model in technical education and research, responsive to global challenges.

**MISSION**

To impart technical education that develops innovative professionals and entrepreneurs and to undertake research that generates cutting-edge technologies and futuristic knowledge, focusing on the socio-economic needs.

# VISION AND MISSION OF THE DEPARTMENT

**VISION**

To address societal needs and global industry challenges in the field of Computer & IT with state-of-art education & research.

**MISSION**

M-1: To create a platform for education, research and development by providing sound theoretical knowledge and practical skills in Computer Engineering and Information Technology.

M-2: To produce motivated professional technocrats capable of generating solutions for industry and society.

M-3: To develop the ability to work ethically at individual and team level and be responsive towards socio-economic needs.

# VISION AND MISSION OF THE PROGRAM

## VISION

To disseminate state-of-the-art education to develop competent professionals in Computer Engineering with capability to serve the global society**.**

## MISSION

To educate and train manpower engaged in cutting-edge research by offering latest in the field of Computer Engineering for sustainable development of society.

## PROGRAMME EDUCATIONAL OBJECTIVES (PEOs)

The PG programme in Computer Engineering (Cyber Security) will produce post graduates that, within a few years of graduation:

| PEOs | Description |
|---|---|
| **PEO 1** | Graduates of the institute will have adequate knowledge of Computer Science and Engineering to excel in professional career and/or higher education. |
| **PEO 2** | Graduates of the institute will be skilled enough to analyze real life problems, design cyber security systems that delivers appropriate solutions that are technically sound, economically feasible and socially acceptable. |
| **PEO 3** | Graduates of the institute will have attitude towards continuous learning and will exhibit professional ethics, communication skills, team work in all walks of life. |

## PROGRAM OUTCOMES (POs)

**Graduates of the Programme:**

| PO | Description |
|---|---|
| **PO 1** | An ability to independently carry out research /investigation and development work to solve practical problems. |
| **PO 2** | An ability to write and present a substantial technical report/document. |
| **PO 3** | Students should be able to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program. |
| **PO 4** | Students should be able to analyse, design and develop solutions or models with understanding of their limitations for complex engineering problems through appropriate literature, techniques, resources and tools. |

**Proposed Scheme for the**

**Master of Technology in Computer Science and Engineering (Cyber Security)**

**Curriculum w.e.f AY 2025-26**

| Sr. No. | Code | Course Title | Teaching Schedule | | | | Credit |
|---|---|---|---|---|---|---|---|
| | | | L | T | P | Total | |
| **First Semester** | | | | | | | |
| 1. | MCS2C01 | Advanced Data Structures and Algorithms | 3 | 0 | 0 | 3 | 3 |
| 2. | MCS2C03 | System and Network Security | 3 | 0 | 0 | 3 | 3 |
| 3. | MCS2C05 | Cyber Security and Data Privacy | 3 | 0 | 0 | 3 | 3 |
| 4. | | Elective-1 | 3 | 0 | 0 | 3 | 3 |
| 5. | | Elective -2 | 3 | 0 | 0 | 3 | 3 |
| 6. | MCS2L01 | Algorithms Laboratory | 0 | 0 | 2 | 2 | 1 |
| 7. | MCS2L03 | System and Network Security Lab | 0 | 0 | 2 | 2 | 1 |
| 8. | MCS2S01 | Seminar | 0 | 0 | 2 | 2 | 1 |
| Total | | | | | | **21** | **18** |
| **Second Semester** | | | | | | | |
| 1. | MCS2C02 | Number Theory and Cryptography | 3 | 0 | 0 | 3 | 3 |
| 2. | MCS2C04 | Cloud and IoT Security | 3 | 0 | 0 | 3 | 3 |
| 3. | | Elective-3 | 3 | 0 | 0 | 3 | 3 |
| 4. | | Elective-4 | 3 | 0 | 0 | 3 | 3 |
| 5. | | Elective-5 | 3 | 0 | 0 | 3 | 3 |
| 6. | MCS2L02 | Number Theory and Cryptography Lab | 0 | 0 | 2 | 2 | 1 |
| 7. | MCS2LXX | Elective-3 Laboratory | 0 | 0 | 2 | 2 | 1 |
| 8. | MCS2P02 | Project | 0 | 2 | 0 | 2 | 1 |
| Total | | | | | | **21** | **18** |
| **Third Semester** | | | | | | | |
| 1. | MCS2D01 | Dissertation Part - I | **14** | | | | |
| **Fourth Semester** | | | | | | | |
| 1. | MCS2D02 | Dissertation Part - II | **14** | | | | |

*Course code in accordance with Elective-3 being run in the current semester

**Note:**

- Elective can be opted from the list of electives/ core subjects of various specializations of Computer Engineering Department.
- Electives-5 can be opted from the list of electives of other departments as well.
- List of Electives, being offered by the Department along with the number of slots and pre-requisites, if any, will be notified by the concerned department well before the registration.

# Annexure

**List of Elective Courses**

| Odd Semester (Electives 1 & 2) | | Even Semester (Elective 3 with Lab) | | | Even Semester (Electives 4 & 5) | |
|---|---|---|---|---|---|---|
| **Code** | **Course Title** | **Code** | **Course Title** | **Lab Code** | **Code** | **Course Title** |
| MCS2E01 | Advanced Computer Networks | MCS2E04 | Soft Computing | MCS2L04 | MCS2E12 | Big Data and Analytics |
| MCS2E03 | Intrusion Detection Systems | MCS2E06 | Secure Coding | MCS2L06 | MCS2E14 | Information Security Management |
| MCS2E05 | Distributed Computing | MCS2E08 | Network Forensics | MCS2L08 | MCS2E16 | Advances in Cloud and Mobile Computing |
| MCS2E07 | Biometric Security | MCS2E10 | Network Security Tools and Techniques | MCS2L10 | MCS2E18 | Information Warfare |
| MCS2E09 | Social Network Analysis | | | | MCS2E20 | Cyberspace Operations and Design |
| MCS2E11 | Vulnerability Discovery and Exploit Development | | | | MCS2E22 | Ethics and Laws of Cyber Security |

## Advanced Data Structures and Algorithms (MCS2C01)

| L | T | P/D | Total | Credit | | |
|---|---|---|---|---|---|---|
| 3 | - | - | 3 | 3 | Max. Marks: | 100 |
| | | | | | Theory: | 50 Marks |

Mid-Sem: 50 Marks

**Course Objectives:**

To develop the understanding of advanced algorithms.

1. To study complexity of advanced algorithms.
2. Design new algorithms or modify existing ones for new applications and able to analyze the space & time efficiency of most algorithms.

**Course Outcomes:**

The participants must at the end of the course be able to:

1. Apply basic concepts of approximation, randomization and distributed computing in algorithmic context.
2. Designs randomized parallel algorithms, approximation and distributed algorithms that run fast or that return the correct output with high probability.
3. Derives good upper bounds for the expected running time of advanced algorithms.
4. Can apply the probabilistic method to show the existence of certain combinatorial objects design and analyse.

**Syllabus:**

Data Structures: AVL trees**,** Red black trees, Balanced Multi-way trees, Splay trees, tries, Segment trees, Binomial heap and Fibonacci heap.

Approximation Algorithms: Coping with NP-Hardness, Greedy Approximation Algorithms, Dynamic Programming and Weakly Polynomial-Time Algorithms, Linear Programming Relaxations, Randomized Rounding, Vertex Cover, set cover, TSP, knapsack, bin packing, subset-sum problem, Load balancing, Analysis of the expected time complexity of the algorithms.

Randomized and Probabilistic Algorithms: Game-theoretic techniques, Moments and Deviations, Numerical Probabilistic algorithms, Lovasz local lemma, Markov Chains and Random Walks, Algebraic Techniques, Geometric Algorithms, Randomized Quick sort, Las Vegas and Monte Carlo algorithms, Applications problems like load balancing, packet routing etc.

**References:**

1. Introduction to Algorithms by Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein. Third Edition. MIT Press and PHI, 2010.
2. Algorithm Design and Applications by Michael T. Goodrich and Roberto Tamassia, John wiley publication.
3. Randomized Algorithms by Rajeev Motwani, Prabhakar Raghavan, published by Cambridge University Press, 2014.
4. Probability and Computing: Randomized Algorithms and Probabilistic Analysis, by Mitzenmacher and Upfal, Cambridge University Press, 2nd edition, 2017
5. The Design of Approximation Algorithms by David P. Williamson and David B. Shmoys, Cambridge University Press.
6. Algorithm Design by Jon Kleinberg, Eva Tardos by Pearson publications.

## System and Network Security (MCS2C03)

| L | T | P/D | Total | Credit |
|---|---|---|---|---|
| 3 | - | - | 3 | 3 |

Max. Marks: 100
Theory: 50 Marks
Mid-Sem: 50 Marks

**Course Objectives:**

The purpose of this course is to provide understanding of the main issues related to security in modern networked computer systems. This covers underlying concepts and foundations of computer security, basic knowledge about security-relevant decisions in designing IT infrastructures, techniques to secure complex systems and practical skills in managing a range of systems, from personal laptop to large-scale infrastructures.

**Course Outcomes:**

On completion of this course, students should be able to:

1. Understand the concepts and foundations of computer security, and identify vulnerabilities of IT systems.
2. Make use of basic security tools to enhance system security
3. Develop basic security enhancements in stand-alone applications.

**Syllabus:**

Computer Security Concepts- Introduction to Information Security, Introduction to Data and Network Security, Integrity, and Availability, NIST FIPS 199 Standard, Assets and Threat Models, Examples

Least privilege, access control, operating system security- The principle of least privilege, Access control concepts, Operating system mechanisms, Unix, Windows, and Android examples.

Web Application Security- SQL injection, Cross-site request forgery, Cross-site scripting, Click-Jacking, Attacks and Defenses, Generating and storing session tokens, Authenticating users, The SSL protocol, Pretty Good Privacy, Web Tracking, Browser content, Document object model (DOM), Same-origin policy.

Network Defenses- Network concepts, Threats in Networks, Threats in Transit, TCP/IP security issues, Impersonation, DNS security issues and defenses, Network defense tools, Secure protocols, Firewalls, VPNs, Tor, I2P, Intrusion Detection and filters, Host-Based IDS vs Network-Based IDS, Dealing with unwanted traffic: Denial of service attacks.

Malicious Software and Software Security- Malicious Web, Internet Security Issues, Types of Internet Security Issues, Viruses, Trojans, rootkits, worms, botnets, Spyware, Key-Loggers, Ransomware, Honeypot, Security policies, penetration testing, Sandboxing, buffer overflow vulnerability and attack, control hijacking attacks, mobile security, Repackaging attacks, Attacks on mobile apps, Whole-disk encryption.

Android platform security models- Android, iOS Mobile platform security models, Detecting Android malware in Android markets, Whole-disk encryption.

The Trusted Computing Architecture- Introduction to Trusted Computing, TPM Provisioning, Exact Mechanics of TPM.

**References:**

1. William Stallings, Network Security Essentials: Applications and Standards, Prentice Hall, 4th edition, 2010.
2. Michael T. Goodrich and Roberto Tamassia, Introduction to Computer Security, Addison Wesley, 2011.
3. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 2001
4. Gupta, B., Dharma P. Agrawal, and Shingo Yamaguchi, eds. Handbook of research on modern cryptographic solutions for computer and cyber security. IGI Global, 2016.
5. Rhodes-Ousley, Mark. Information security: the complete reference. McGraw Hill Education, 2013.
6. Charlie Kaufman, Radia Perlman and Mike Spencer, "Network Security: Private Communication in a Public World", Prentice Hall.
7. Marshall D. Adams, Sushil Jajodia and Harold J. Podell, eds., "Information Security: An Integrated Collection of Essays". IEEE Computer Society Press.
8. Peter J. Denning, "Computers under Attack", Addison-Wesley.
9. White, Gregory B., et al. "Principles of Computer Security. Security+ and Beyond." (2004).

## Cyber Security and Data Privacy (MCS2C05)

| L | T | P/D | Total | Credit |
|---|---|---|---|---|
| 3 | - | - | 3 | 3 |

Max. Marks: 100
Theory: 50 Marks
Mid-Sem: 50 Marks

**Course Objectives:**

The objective of this course is to create architectural, algorithmic and technological foundations for ensuring cyber security, maintenance of the privacy of individuals, the confidentiality of organizations, and the protection of sensitive information, despite the requirement that information be released publicly or semi-publicly.

**Course Outcomes:**

After successful completion of this course, students will be able to:

1. Understand the concepts of cyber security and data privacy in today's environment.
2. Obtain the understanding of how automation is changing the concepts and expectations concerning privacy and the increasingly interconnected issue of security.
3. Obtain the knowledge of the role of private regulatory and self-help efforts.
4. Have an understanding of how emerging issues are affecting society and business, with a concentration on how information security must shape corporate practices.

**Syllabus:**

Basic Cyber Security Concepts: Introduction to Cyber Security, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Spectrum of attacks, Taxonomy of various attacks, IP spoofing, Methods of defense, Security Models, risk management, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc., Comprehensive Cyber Security Policy, Nodal Authority, International convention on Cyberspace.

Basic Data Privacy Concepts: Fundamental Concepts, Definitions, Statistics, Data Privacy Attacks, Data linking and profiling, access control models, role based access control, Discretionary and mandatory access control, privacy policies and their specifications, privacy policy languages, privacy in different domains- medical, financial, etc.

Cyber Security Vulnerabilities and Cyber Security Safeguards: Cyber Security Vulnerabilities – Overview, vulnerabilities in software, System administration, Complex Network Architectures, Open Access to Organizational Data, Weak Authentication, Poor Cyber Security Awareness. Cyber Security Safeguards – Overview, Access control, Audit, Authentication, Biometrics, Cryptography, Deception, Denial of Service Filters, Ethical Hacking, Firewalls, Intrusion Detection Systems, Response, Scanning, Security policy, Threat Management.

Data explosion: Statistics and Lack of barriers in Collection and Distribution of Person-specific information, Mathematical model for characterizing and comparing real-world data sharing practices and policies and for computing privacy and risk measurements.

Survey of techniques: Protection models, Disclosure control, inferring entity identities, Strength and weaknesses of techniques, entry specific databases, computation systems for protecting delimited data, protecting textual documents, Scrub.

Cyber Forensics: Introduction to Cyber Forensics, Handling Preliminary Investigations, controlling an Investigation, conducting disk-based analysis, Investigating Information-hiding, Scrutinizing E-mail, Validating E-mail header information, Tracing Internet access, Tracing memory in real-time.

Legal and Ethical Issues: Cybercrime and computer crime, Cyber Warfare, Cyber terrorism, Cyber Espionage, Intellectual property, copyright, patent, trade secret, Hacking and intrusion, Cyber laws, Roles of International Law, Privacy, identity theft, National Cyber Security Policy.

**References:**

1. B. Raghunathan, The Complete Book of Data Anonymization: From Planning to Implementation, Auerbach Pub, 2013.
2. L. Sweeney, Computational Disclosure Control: A Primer on Data Privacy Protection, MIT Computer Science, 2002.
3. B. B. Gupta, D. P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and Perspectives, CRC Press, ISBN 9780815371335, 2018.
4. Raef Meeuwisse, Cyber Security for Beginners, Cyber Simplicity Ltd., 2017.
5. William Stallings, "Cryptography and Network Security: Principles and Practice.", Prentice-Hall.
6. William R. Cheswick and Steven M. Bellovin, "Firewalls and Internet Security: Repelling the Wily Hacker", Addison-Wesley.
7. Charles P. Pfleeger, "Security in Computing", Pearson Education.
8. Edward Amoroso, "Fundamentals of Computer Security Technology", Prentice-Hall.

# First Semester
# Electives

## Advanced Computer Networks (MCS2E31)

| L | T | P/D | Total | Credit | | |
|---|---|---|---|---|---|---|
| 3 | - | - | 3 | 3 | Max. Marks: | 100 |
| | | | | | Theory: | 50 Marks |
| | | | | | Mid-Sem: | 50 Marks |

**Course Objectives:** To give the students an understanding of the principles behind the latest advances in computer network technology, from IPv6 extending to pervasive and ubiquitous computing

**Course Outcomes:**
1. To understand the concepts behind Opportunistic, IoT and Software Defined Networking.
2. To identify different issues in Opportunistic, Social, IoT and SDN Networks.
3. To analyze various protocols proposed to handle issues related to Opportunistic, Social, IoT and SDN Networks.

**Syllabus:**
Opportunistic and Social Networks: Handling Spectrum Scarcity and Disruption, Architecture of Cognitive Radio Network (CRN) and Delay Tolerant Networks (DTN), Routing in Opportunistic Mobile and Social Networks, Multicasting, Single-node, Multiple-copy, and Single-copy model, Interest-based Data Dissemination, User Interest Profile, Multi-party data transmission, System Implementation, Quality-of-Service (QoS), QoS parameters, Metrics and classification, Network QoS parameters (bandwidth, delay, etc.), System QoS parameters (reliability, capacity, etc.), Task QoS parameters (memory, CPU usage, response time, etc.), Extension QoS parameters (reputation, security, etc.).

IoT Networks: Convergence of domains, Key technologies for IoT and its components, Multi-homing, Sensing, Actuation, Data Aggregation, IoT communication patterns, IoT data and its impact on communication, Characteristics of IoT networks, Protocols for IoT, NFC (Near field communication), Tactile Internet, Caching, Edge computing, Inter-dependencies, SoA, Gateways, Comparison between IoT and Web, Complexity of IoT networks, Scalability, Protocol classification, MQTT, SMQTT, CoAP, XMPP, AMQP, Wireless HART protocol and layered architecture, HART network manager, HART vs ZigBee, Cross layer QoS parameters

Software Defined Networks (SDN):Network Function Virtualization (NFV), Unicast and multicast routing, Fundamental graph algorithms, Modern protocols for content delivery, Video delivery using HTTP, HTTP Live Streaming, DASH, Content Delivery Networks (CDN), TVOD and SVOD, Architecting a content distribution system over IP-based networks, CDN topologies, Edge-Caching, Streaming-Splitting, Pure-Play, Operator, Satellite, Hybrid, Computer hosting and orchestration for dedicated appliances and virtualization, Robust synchronization of absolute and difference clocks, Precision time protocol, Clock synchronization in SDN, ReversePTP scheme

**References:**

1. Jie Wu and Yunsheng Wang, Opportunistic Mobile Social Networks, CRC Press, 2015.
2. James F. Kurose and Keith W. Ross, Computer Networking: A Top-down Approach Featuring the Internet, Addison-Wesley, 2001.
3. Huitema, C., Routing in the Internet, 2nd ed., Prentice-Hall, 2000.
4. Peterson and Davie, Computer Networks: A Systems Approach, 5 th ed., Morgan Kaufmann, 2011.
5. Rajiv Ramaswami, Kumar N. Sivarajan, Galen H. Sasaki, Optical Networks: A Practical Perspective, Morgan Kaufmann.
6. Vijay Madisetti and Arshdeep Bahga, Internet of Things: A Hands-On- Approach, 2014, ISBN: 978 0996025515
7. Francis daCosta, Rethinking the Internet of Things: A Scalable Approach to Connecting Everything, 1 st Edition, Apress Publications, 2013.

## Intrusion Detection Systems (MCS2E33)

| L | T | P/D | Total | Credit | | |
|---|---|---|---|---|---|---|
| 3 | - | - | 3 | 3 | Max. Marks: | 100 |
| | | | | | Theory: | 50 Marks |
| | | | | | Mid-Sem: | 50 Marks |

**Course Objectives:** The objective of this course is to provide an in depth introduction to the science and art of intrusion detection. The course covers methodologies, techniques, and tools for monitoring events in computer system or network, with the objective of preventing and detecting unwanted process activity and recovering from malicious behavior.

**Course Outcomes:**

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

1. Obtain comprehensive knowledge on the subject of intrusion detection
2. Understand the state of the art of intrusion detection research
3. Get a hands-on exposure to the principles and techniques used in intrusion detection, as well as the technical challenges and fundamental limitations of intrusion detection become either a capable practitioner or independent researcher in intrusion detection.

**Syllabus:**

Overview of intrusions, system intrusion process, dangers of system intrusions, history and state of the art of intrusion detection systems (IDSs): anomaly detection, misuse detection, types of IDS: Network-Based IDS. Host-Based IDS, Hybrid IDS, Intrusion Prevention Systems (IPS): Network-Based IPS, Host-Based IPS, Intrusion Detection Tools, the limitations and open problems of intrusion detection systems, advanced persistent threats, case studies of intrusion detection systems against real-world threats and malware.

Statistical and machine approaches to detection of attacks on computers - Techniques for studying the Internet and estimating the number and severity of attacks, network based attacks, host based attacks. Statistical pattern recognition for detection and classification of attacks, and techniques for visualizing network data, etc.

**References:**

1. Roberto Di Pietro, Luigi V. Mancini, Intrusion Detection System, Springer, 2008.
2. Anderson, Ross (2001). Security Engineering: A Guide to Building Dependable Distributed Systems. New York: John Wiley & Sons. pp. 387–388. ISBN 978-0-471-38922-4.
3. Anderson, James P., "Computer Security Threat Monitoring and Surveillance," Washing, PA, James P. Anderson Co., 1980.

## Distributed Computing (MCS2E35)

| L | T | P/D | Total | Credit | | |
|---|---|---|---|---|---|---|
| 3 | - | - | 3 | 3 | Max. Marks: | 100 |
| | | | | | Theory: | 50 Marks |
| | | | | | Mid-Sem: | 50 Marks |

**Course Objectives:** To understand fundamental concepts of distributed computing and to acquire knowledge about development of fault tolerant protocols for middleware design.

**Course Outcomes:**

After completion of this course, student should be able to apply these course concepts to:

1. Study software components of distributed computing systems. Know about the communication and interconnection architecture of multiple computer systems.
2. Recognize the inherent difficulties that arise due to distributed-ness of computing sources.
3. Understanding of networks & protocols, mobile & wireless computing and their applications to real world problems.
4. At the end students will be familiar with the design, implementation and issues of distributed system.

**Syllabus:**

Unit 1: Design issues and challenges, Models and Architectures, Synchronous Vs Asynchronous, Classification of Failures in Distributed Systems, Basic Techniques for Handling Time in Distributed Systems, Physical Clocks, Physical Clock Synchronization, NTP, Inter-process Communication, Logical Clocks, Scalar, Vector, and Matrix Clock, Global State, Consistent Snapshot Algorithms for FIFO, Non-FIFO and Causal Delivery Systems,, Monitoring, Consistency, Necessary and Sufficient Condition for Consistent Snapshot, Z-path and Z-cycles, Synchronous Vs. Asynchronous Checkpointing and Recovery.

Unit 2: Message Ordering and Group Communication Protocols, Naming in Distributed Systems, Quiescence Detection, Termination and Deadlock, Weight-throwing, MST-based, and Message-optimal Protocols, Mutual Exclusion, Shared Memory Vs. Message Passing Model, 2-P and n-P Algorithms, Contention-based and Token-based algorithms, Leader Election, Election in Ring Networks, Distributed Graph Algorithms for MST, MIS, CDS, and other Virtual Structures.

Unit 3: Agreement Protocols, Coordinated Attack, Distributed Consensus with Process Failures, Synchronous Systems with Crash and Byzantine Failures, Lower Bound, EIG, Phase-king Algorithm, Concept of Valance, FLP impossibility, Wait-free and 1-failure Termination, BGP, Weak Byzantine Agreement, k-agreement, Approximate Agreement, Distributed Commit, 2-PC and 3-PC protocols, Distributed Scheduling and Load Balancing. Distributed File Systems, and Distributed Shared Memory,Security.

**References:**

1. Distributed Systems: Concepts and Design; G Colouris, J Dollimore, T Kindberg 3/e Pearson Ed. 2002.
2. Distributed Systems: Principles and Paradigm; Andrew S Tanenbaum, Maarten van Steen 3/e Pearson Ed.2002.
3. Principles of Distributed Systems, VK Garg, Kluwer Academic Publishers, 1996.
4. Distributed Systems and Algorithmic Approach by Su Kumar Boss, Chamal &Hall.
5. Principles of Distributed Computing by V K Garg, IEEE Press.
6. Distributed Computing by A D Kshem Kalyani & Mukesh Singha.
7. Distributed Algorithms by Nancy Lynch, Morgan Kaufmann Press.
8. Introduction to Distributed Algorithms by G Tel, Cambridge University.

## Biometric Security (MCS2E37)

| L | T | P/D | Total | Credit |
|---|---|---|---|---|
| 3 | - | - | 3 | 3 |

Max. Marks: 100
Theory: 50 Marks
Mid-Sem: 50 Marks

**Course Objectives:**

To provide students with understanding of biometrics, biometric equipment and standards applied to security.

**Course Outcomes:**

Successful completion of this course will prepare the students to:

1. Explain different biometrics parameters
2. Evaluate and design security systems incorporating biometrics
3. Perform R&D on biometrics methods and systems
4. Understand the privacy challenges of Biometrics
5. Explain the errors generated in biometric measurements
6. Understand the technology of biometrics for public policy matters involving security and privacy.

**Syllabus:**

Overview of Biometrics: Definitions, biometric modalities, basic applications, access control, security

Biometric System Architecture: Scanning/digitizing, enhancement, feature extraction, classification, matching, searching and verification.

Algorithms Face recognition Voice Recognition Fingerprint Recognition Iris Recognition Other biometric modalities: Retina, signature, hand geometry, gait, keystroke

Quantitative analysis on the biometrics, Performance evaluation in Biometrics – false acceptance rate; false rejection rate.

Multimodal Biometric Systems Biometric system integration, multimodal biometric systems: theory and applications, performance evaluation of multimodal biometric systems.

Biometric System Security: Biometric attacks/tampering; solutions, biometric encryption.

**References:**

1. Benjamin Muller, Security, Risk and the Biometric State: Governing Borders and Bodies, 1st Edition, Routledge, 2010.
2. Anil K Jain, Patrick Flynn, Arun A. (Eds.), Handbook of Biometrics, Springer, 2008.
3. Julian D. M. Ashbourn, Biometrics: Advanced Identify Verification: The Complete Guide, Springer-Verlag, 2000.
4. Davide Maltoni, Handbook of Fingerprint Recognition.
5. Biometric Systems: Technology, Design and Performance Evaluation, Editors: J. Wayman, A. Jain, D. Maltoni and D. Maio, Springer, 2005.

## Social Network Analysis (MCS2E39)

| L | T | P/D | Total | Credit |
|---|---|---|---|---|
| 3 | - | - | 3 | 3 |

Max. Marks: 100
Theory: 50 Marks
Mid-Sem: 50 Marks

**Course Objectives:** To learn about structure and evolution of networks, to build a framework of network analysis that covers measures such as density, centrality, clustering, centralization, and specialization.

**Course Outcomes:**

On completion of this course, students will be able to:

1. Understand various concepts in networks, dynamics and development of social structures
2. Analyze framework of network analysis and compare various random network models
3. Apply network centrality using various concepts like betweenness, closeness, page ranks etc.
4. Know about various community concepts like: clustering, community structure, modularity.
5. Understand how various social media networks are working and using SNA in their infrastructure.

**Syllabus:**

Networks- Concepts: nodes, edges, adjacency matrix, one and two-mode networks, node degree Random network models: Erdos-Renyi and Barabasi-Albert- Concepts: connected components, giant component, average shortest path, diameter, breadth-first search, preferential attachment

Network centrality- Concepts: Betweenness, closeness, eigenvector centrality (+ PageRank), network centralization

Community- Concepts: clustering, community structure, modularity, overlapping communities

Small world network models, optimization, strategic network formation and search-Concepts: small worlds, geographic networks, decentralized search

Contagion, opinion formation, coordination and cooperation- Concepts: simple contagion, threshold models, opinion formation, unusual applications of SNA

SNA and online social networks- Concepts: how services such as Facebook, LinkedIn, Twitter, Couch Surfing, etc. are using SNA to understand their users and improve their functionality

**References:**

1. John Scott, Social Network Analysis, 3rd Edition, SAGE, 2012.
2. Wouter de Nooy, Andrej Mrvar, Vladimir Batagelj, Exploratory Social Network Analysis with Pajek, 2nd Revised Edition, Cambridge University Press, 2011.
3. Patrick Doreian, Frans Stokman, Evolution of Social Networks, Routledge, 2013.
4. David Easley and Jon Kleinberg, Networks, Crowds, and Markets: Reasoning About a Highly Connected World, Cambridge University Press, 2010.

## Vulnerability Discovery & Exploit Development (MCS2E41)

| L | T | P/D | Total | Credit |
|---|---|---|---|---|
| 3 | - | - | 3 | 3 |

Max. Marks: 100
Theory: 50 Marks
Mid-Sem: 50 Marks

**Course Objectives:** Objective of this course is to focus on a comprehensive coverage of software exploitation. In addition, this course will present different domains of code exploitation and how they can be used together to test the security of an application.

**Course Outcomes:**

Upon completion of this course, students will be able to:

1. Understand how to exploit a program and different types of software exploitation techniques
2. Understand the exploit development process
3. Search for vulnerabilities in closed-source applications
4. Write their own exploits for vulnerable applications

**Syllabus:**

Background- Vulnerability Discovery Methodologies, What is Fuzzing, Fuzzing Methods and Fuzzer Types, Data Representation and Analysis, Requirements for Effective Fuzzing

Targets and Automation- Automation and Data Generation, Environment Variable and Argument Fuzzing, Environment Variable and Argument Fuzzing: Automation, Web Application and Server Fuzzing, Web Application and Server Fuzzing: Automation, File Format Fuzzing, File Format Fuzzing: Automation on UNIX, File Format Fuzzing: Automation on Windows, Network Protocol Fuzzing, Network Protocol Fuzzing: Automation on UNIX, Network Protocol Fuzzing: Automation on Windows, Web Browser Fuzzing, Web Browser Fuzzing: Automation, In-Memory Fuzzing, In-Memory Fuzzing: Automation

Advanced Fuzzy Technologies- Fuzzing Frameworks, Automated Protocol Dissection, Fuzzer Tracking, Intelligent Fault Detection.

Advanced Linux Exploitation-Linux heap management, constructs, and environment, Navigating the heap, Abusing macros such as unlink() and frontlink(), Function pointer overwrites, Format string exploitation, Abusing custom doubly-linked lists, Defeating Linux exploit mitigation controls, Using IDA for Linux application exploitation, Patch Diffing, one day Exploits and Return Oriented Shellcode, The Microsoft patch management process and Patch Tuesday, Obtaining patches and patch extraction, Binary diffing with BinDiff, patchdiff2, turbodiff, and darungrim, Visualizing code changes and identifying fixes, Reversing 32-bit and 64-bit applications and modules, Triggering patched vulnerabilities, Writing one-day exploits, Handling modern exploit mitigation controls.

Windows Kernel Debugging and Exploitation- Understanding the Windows Kernel, Navigating the Windows Kernel, Modern Kernel protections, Debugging the Windows Kernel, WinDbg, Analysing Kernel vulnerabilities and Kernel vulnerability types, Kernel exploitation techniques.

Windows Heap Overflows and Client-Side Exploitation- Windows heap management, constructs, and environment, Browser-based and client-side exploitation, Remedial heap spraying, Understanding C++, vftable/vtable behavior, Modern heap spraying to determine address predictability, Use-After-Free attacks and dangling pointers, Determining exploitability, Defeating ASLR, DEP, and other common exploit mitigation controls

Android Exploitation- Android Basics, Android Security Model, Introduction to ARM, Android Development Tools, Engage with Application Security, Android Security Assessment Tools, Exploiting Applications, Protecting Applications, Secure Networking, Native Exploitation and Analysis.

iOS exploitation-Introduction to iOS hacking, iOS User Space Exploitation, iOS Kernel Debugging and Exploitation

**References:**

1. Hack I.T. - Security Through Penetration Testing, T. J. Klevinsky, Scott Laliberte and Ajay Gupta, Addison-Wesley, ISBN: 0-201-71956-8
2. Metasploit: The Penetration Tester's Guide, David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni
3. Professional Penetration Testing: Creating and Operating a Formal Hacking Lab, Thomas Wilhelm

# Second Semester
# Core Courses

## Number Theory and Cryptography (MCS2C02)

| L | T | P/D | Total | Credit |
|---|---|---|---|---|
| 3 | - | - | 3 | 3 |

Max. Marks: 100
Theory: 50 Marks
Mid-Sem: 50 Marks

**Course Objectives:**

1. To emphasize the application of the number theory in the design of cryptographic algorithms.
2. To understand the strength and weakness of cryptosystems.
3. To introduce the elliptic curve cryptography.

**Course Outcomes:**

On successful completion of this course, students will be able to:

1. Understand the significance of cryptography to the modern world
2. Able to learn basic elements of number theory and its applications in cryptography
3. Understand the mathematical foundations of Cryptographic algorithms
4. Understand Public Key Cryptography, Discrete Logarithm problem, RSA Cryptosystem, ECC and various attacks
5. Solve elementary problems in number theory relating to cryptography.
6. Build on number theoretic basics to further their knowledge of advanced methods of cryptography.

**Syllabus:**

Elementary Number Theory: Divisibility, Division Algorithm, Euclidean Algorithm; Congruences, Complete Residue systems, Reduced Residue systems; Fermat's little theorem, Euler's Generalization, Wilson's Theorem; Chinese Remainder Theorem, Generalized Chinese Remainder Theorem-Euler Phi-function, multiplicative property; Finite Fields, Primitive Roots; Quadratic Residues, Legendre Symbol, Jacobi Symbol; Gauss's lemma, Quadratic Reciprocity Law.

Primality Testing and Factorization: Primality Tests; Pseudoprimes, Carmichael Numbers; Fermat's pseudoprimes, Euler pseudoprimes; Factorization by Pollard’s Rho method; Simple Continued Fraction, simple infinite continued fractions; Approximation to irrational numbers using continued fractions; Continued Fraction method for factorization.

Public Key Cryptosystems: Traditional Cryptosystem, limitations; Public Key Cryptography; Diffie-Hellmann key exchange; Discrete Logarithm problem; One-way functions, Trapdoor functions; RSA cryptosystem; Digital signature schemes; Digital signature standards; RSA signature schemes; Knapsack problem; ElGamal Public Key Cryptosystem; Attacks on RSA cryptosystem: Common modulus attack; Homomorphism attack, timing attack; Forging of digital signatures; Strong primes, Safe primes, Gordon's algorithm for generating strong primes; Strong pseudoprimes to the base $a$.

Elliptic Curve Cryptography: Cubic Curves, Singular points, Discriminant; Introduction to Elliptic Curves, Geometry of elliptic curves over reals; Weierstrass normal form, point at infinity; Addition of two points; Bezout's theorem, associativity; Group structure, Points of finite order; Elliptic Curves over finite fields, Discrete Log problem for Elliptic curves; Elliptic Curve Cryptography; Factorization using Elliptic Curve; Lenstra's algorithm; ElGamal Public Key Cryptosystem for elliptic curves.

Mini Project (Implementation of any Cryptographic Algorithm from above related topics, as an assignment)

**References:**

1. A Course in Number Theory and Cryptography, Neal Koblitz, (Springer 2006)
2. An Introduction to Mathematical Cryptography, Jill Pipher, Jeffrey Hoffstein, Joseph H. Silverman (Springer, 2008)
3. An Introduction to theory of numbers, Niven, Zuckerman and Montgomery, (Wiley 2006)
4. Elliptic curves: Number theory and cryptography, Lawrence C. Washington, (Chapman & Hall/CRC 2003)
5. An Introduction to Cryptography, R.A. Mollin (Chapman & Hall, 2001)
6. Rational Points on Elliptic Curves, Silverman and Tate (Springer 2005)
7. Guide to elliptic curve cryptography Hankerson, Menezes, Vanstone (Springer, 2004)
8. Elementary Number Theory, Jones and Jones (Springer, 1998)

## Cloud and IoT Security (MCS2C04)

| L | T | P/D | Total | Credit |
|---|---|---|---|---|
| 3 | - | - | 3 | 3 |

Max. Marks: 100
Theory: 50 Marks
Mid-Sem: 50 Marks

**Course Objectives:**

1. To understand the fundamentals of Internet of Things (IoT) and Cloud Computing.
2. Understand various protocols used at different layers for IoT.
3. Ability to understand the Security requirements in IoT and cloud computing.
4. To apply the concept of Internet of Things in the real world scenario

**Course Outcomes:**

1. To analyze various protocols and reference architectures developed for IoT.
2. Identify different issues in IoT security.
3. To analyze various security issues of IoT based cloud systems
4. To identify the various real life applications of IoT based cloud systems.

**Syllabus:**

Fundamentals of IoT and Cloud Computing: Evolution of Internet of Things, Enabling Technologies, IoT Architectures: oneM2M, IoT World Forum (IoTWF) and Alternative IoT models, Simplified IoT Architecture and Core IoT Functional Stack, Fog, Edge and Cloud in IoT, Functional blocks of an IoT ecosystem, Sensors, Actuators, Smart Objects and Connecting Smart Objects.

IoT Architectures and Protocols: M2M high-level ETSI architecture, IETF architecture for IoT, OGC architecture. IoT reference model: Domain model, information model, functional model, communication model. IoT reference architecture. Protocol Standardization for IoT: Efforts, M2M and WSN Protocols, SCADA and RFID Protocols. IoT Access Technologies: Physical and MAC layers, topology and Security of IEEE 802.15.4, LoRaWAN, Network Layer: IP versions, Constrained Nodes and Constrained Networks. Optimizing IP for IoT: From 6LoWPAN to 6Lo, Routing over Low Power and Lossy Networks, Application Layer Protocols: CoAP and MQTT.

Securing the IoT: Security Requirements in IoT Architecture, Security in Enabling Technologies, Security Concerns in IoT Applications. Security Architecture in the Internet of Things, Security Requirements in IoT, Insufficient Authentication/Authorization, Insecure Access Control, Threats to Access Control, Privacy, and Availability, Attacks Specific to IoT. Vulnerabilities. Secrecy and Secret-Key Capacity, Authentication/Authorization for Smart Devices, Transport Encryption, Attack & Fault trees.

Cloud Security for IoT: Cloud services and IoT: offerings related to IoT from cloud service providers, Cloud IoT security controls, and an enterprise IoT cloud security architecture. New directions in cloud enabled IoT computing.

Applications & Case Study: Real world design constraints, Applications, Asset management, Industrial automation, smart grid, Commercial building automation, Smart cities, participatory sensing. Data Analytics for IoT. Software & Management Tools for IoT Cloud Storage Models & Communication APIs. Cloud for IoT: Amazon Web Services for IoT.

**References:**

1. Xu, L. D., & Li, S. (2017). Securing the Internet of Things. Elsevier.
2. Weippl, E. (2018). Internet of Things Security: Fundamentals, Techniques and Applications. River Publishers.
3. Russell, B., & Van Duren, D. (2016). Practical internet of things security. Packt Publishing Ltd.
4. Hu, F. (2016). Security and privacy in Internet of things (IoTs): Models, Algorithms, and Implementations. CRC Press.
5. Zhou, H. (2012). The internet of things in the cloud: a middleware perspective. CRC press.
6. Hersent, O., Boswarthick, D., & Elloumi, O. (2011). The internet of things: Key applications and protocols. John Wiley & Sons.
7. Gupta, B., Agrawal, D., Handbook of Research on Cloud Computing and Big Data Applications in IoT, IGI Global, USA, ISBN13: 9781522584070, 2019.
8. Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294-1312.

# Second Semester
# Electives with Lab

## Soft Computing (MCS2E32)

| L | T | P/D | Total | Credit | | |
|---|---|---|---|---|---|---|
| 3 | - | - | 3 | 3 | Max. Marks: | 100 |
| | | | | | Theory: | 50 Marks |
| | | | | | Mid-Sem: | 50 Marks |

**Course Objective:**
The objective of the course is to understand and apply different domains of soft computing techniques like neural networks, fuzzy logic, genetic algorithm and swarm optimization.

**Course Outcomes:**
1. Understand different soft computing techniques.
2. Understand applications of soft computing techniques to solve real world problems.
3. Design robust and low-cost intelligent machines.

**Syllabus:**
Soft Computing and Artificial Intelligence: Introduction of Soft Computing, Soft Computing vs. Hard Computing, Various Types of Soft Computing Techniques, Applications of Soft Computing, AI Search Algorithm, Predicate Calculus, Rules of Interference, Semantic Networks, Frames, Objects, Hybrid Models.
Artificial Neural Networks and Paradigms: Introduction, Neuron Model, Neural Network Architecture, Learning Rules, Perceptrons, Single Layer Perceptrons, Multilayer Perceptrons, Back propagation Networks: Kohnen'sself organizing networks, Hopfield network, Applications of NN.

Fuzzy Logic: Introduction, Fuzzy sets and Fuzzy reasoning, Basic functions on fuzzy sets, relations, rule based models and linguistic variables, fuzzy controls, Fuzzy decision making, applications of fuzzy logic.

Neuro - Fuzzy Modeling: Adaptive Networks Based Fuzzy Interface Systems, Classification and Regression Trees, Data Clustering Algorithms, Rule Based Structure Identification, Neuro-Fuzzy Controls, Simulated Annealing, Evolutionary Computation.

Genetic Algorithms and Swarm Optimizations: Introduction, Genetic Algorithm, Fitness Computations, Cross Over, Mutation, Evolutionary Programming, Classifier Systems, Genetic Programming Parse Trees, Variants of GA, Applications, Ant Colony Optimization, Particle Swarm Optimization, Artificial Bee Colony Optimization.

**References:**
1. Srikanta Patnaik, Baojiang Zhong, Soft Computing Techniques in Engineering Applications,Springer, 2014.
2. Anupam Shukla, Real Life Applications of Soft Computing, CRC Press, 2010.
3. Saroj Kaushik, Artificial Intelligence, Cengage Learning, 2007.

4. Zimmermann, “Fuzzy Set Theory and its Application”, 3rd Edition, 2001.
5. Jang J.S.R., Sun C.T. and Mizutani E, "Neuro-Fuzzy and Soft computing", Prentice Hall, 1998.
6. Timothy J. Ross, "Fuzzy Logic with Engineering Applications", McGraw Hill, 1997.
7. Gupta, B., Sheng, Quan Z., Machine Learning for Computer and Cyber Security: Principles, Algorithms, and Practices, CRC Press, Taylor & Francis, ISBN 9781138587304, 2019.
8. D.E. Goldberg, "Genetic Algorithms: Search, Optimization and Machine Learning", Addison Wesley, N.Y, 1989.

## Secure Coding (MCS2E34)

| L | T | P/D | Total | Credit | | |
|---|---|---|---|---|---|---|
| 3 | - | - | 3 | 3 | Max. Marks: | 100 |
| | | | | | Theory: | 50 Marks |
| | | | | | Mid-Sem: | 50 Marks |

**Course Objectives:**

This course aims to provide an understanding of the various security attacks and knowledge to recognize and remove common coding errors that lead to vulnerabilities. It gives an outline of the techniques for developing a secure application.

**Course Outcomes:**

On successful completion of this course, students will be able to:

1. To implement security as a culture and show mistakes that make applications vulnerable to attacks.
2. To understand various attacks like DoS, buffer overflow, web specific, database specific, web-spoofing attacks.
3. To demonstrate skills needed to deal with common programming errors that lead to most security problems and to learn how to develop secure applications.
4. To identify the nature of the threats to software and incorporate secure coding practices throughout the planning and development of the product.
5. Able to properly handle application faults, implement secure authentication, authorization and data validation controls used to prevent common vulnerabilities.

**Syllabus:**

Introduction: Security, CIA Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts- exploit, threat, vulnerability, risk, attack. Malware Terminology: Rootkits, Trapdoors, Botnets, Key loggers, Honeypots. Active and Passive Security Attacks. IP Spoofing, Tear drop, DoS, DDoS, XSS, SQL injection, Smurf, Man in middle, Format String attack. Types of Security Vulnerabilities- buffer overflows, Invalidated input, race conditions, access-control problems, weaknesses in authentication, authorization, or cryptographic practices. Access Control Problems.

Need for secure systems: Proactive Security development process, Secure Software Development Cycle (S-SDLC), Security issues while writing SRS, Design phase security, Development Phase, Test Phase, Maintenance Phase, Writing Secure Code – Best Practices SD3 (Secure by design, default and deployment), Security principles and Secure Product Development Timeline.

Threat modelling process and its benefits: Identifying the Threats by Using Attack Trees and rating threats using DREAD, Risk Mitigation Techniques and Security Best Practices. Security techniques, authentication, authorization. Defence in Depth and Principle of Least Privilege.

Secure Coding Techniques: Protection against DoS attacks, Application Failure Attacks, CPU Starvation Attacks, Insecure Coding Practices In Java Technology. ARP Spoofing and its countermeasures. Buffer Overrun- Stack overrun, Heap Overrun, Array Indexing Errors, Format String Bugs. Security Issues in C Language: String Handling, Avoiding Integer Overflows and

Underflows and Type Conversion Issues- Memory Management Issues, Code Injection Attacks,Canary based countermeasures using StackGuard and Propolice. Socket Security, Avoiding Server Hijacking, Securing RPC, ActiveX and DCOM

Database and Web-specific issues: SQL Injection Techniques and Remedies,Race conditions, Time of Check Versus Time of Use and its protection mechanisms. Validating Input and

Interprocess Communication, Securing Signal Handlers and File Operations. XSS scripting attack and its types – Persistent and Non persistent attack XSS Countermeasures and Bypassing the XSS Filters.

Testing Secure Applications: Security code overview, secure software installation. The Role of the Security Tester, Building the Security Test Plan. Testing HTTP-Based Applications, Testing File-Based Applications, Testing Clients with Rogue Servers

**References:**

1. Writing Secure Code, Michael Howard and David LeBlanc,Microsoft Press, 2nd Edition, 2004
2. Buffer Overflow Attacks: Detect, Exploit, Prevent by Jason Deckar,Syngress,1st Edition, 2005
3. Threat Modeling, Frank Swiderski and Window Snyder,Microsoft Professional, 1st Edition, 2004.

## Network Forensics (MCS2E36)

| L | T | P/D | Total | Credit |
|---|---|---|---|---|
| 3 | - | - | 3 | 3 |

Max. Marks: 100
Theory: 50 Marks
Mid-Sem: 50 Marks

**Course Objectives:**

Aim of this course is to teach deep understanding of security issues and digital forensics & incident response. In addition, this course also provides the students with specialist knowledge and experience of various digital forensics techniques and incident response.

**Course Outcomes:**

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

1. Understanding of various digital forensics techniques and its usage for the potential countermeasures or incident response.
2. Demonstrate a critical evaluation and use of digital forensics technique to do incident response with an independent project.

**Syllabus:**

Forensics Overview: Computer Forensics Fundamentals, Benefits of Computer Forensics, Computer Crimes, Computer Forensics Evidence and the Courts, Legal Concerns and Privacy Issues

Forensics Process: Forensics Investigation Process, Securing the Evidence and Crime Scene,

Chain of Custody, Law Enforcement Methodologies, Forensics Evidence, Evidence Sources. Evidence Duplication, Preservation, Handling, and Security, Forensics Soundness, Order of Volatility of Evidence, Collection of Evidence on a Live System, Court Admissibility of Volatile Evidence

Acquisition and Duplication: Sterilizing Evidence Media, Acquiring Forensics Images, Acquiring Live Volatile Data, Data Analysis, Metadata Extraction, File System Analysis, Performing Searches, Recovering Deleted, Encrypted, and Hidden files, Internet Forensics, Reconstructing Past Internet Activities and Events, E-mail Analysis, Messenger Analysis: AOL, Yahoo, MSN, and Chats

Mobile Device Forensics: Evidence in Cell Phone, PDA, Blackberry, iPhone, iPod, and MP3.

Evidence in CD, DVD, Tape Drive, USB, Flash Memory, Digital Camera, Court Testimony, Testifying in Court, Expert Witness Testimony, Evidence Admissibility

**References:**

1. Jason Luttgens, Matthew Pepe, Kevin Mandia, Incident Response & Computer Forensics, McGraw-Hill Osborne Media, 3/e, 2014.
2. Keith J. Jones, Richard Bejtlich, Curtis W. Rose, Real Digital Forensics: Computer Security and Incident Response, Paperback – Import, 2005.
3. John Sammons, The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics Paperback, February 24, 2012.
4. Hacking Exposed: Network Security Secrets & Solutions, Stuart McClure, Joel Scambray and George Kurtz, McGraw-Hill, 2005.

## Network Security Tools and Techniques (MCS2E38)

| L | T | P/D | Total | Credit |
|---|---|---|---|---|
| 3 | - | - | 3 | 3 |

Max. Marks: 100
Theory: 50 Marks
Mid-Sem: 50 Marks

**Course Objectives:**

The objective of this course is the use and application of security tools and techniques on real life scenarios such as cyber security consultancy and forensics. In addition to this, students will be able to improve their technical skill-sets and enhance their learning experiences through the use of various cyber tools.

**Course Outcomes:**

After completion of this course, students will be able to:

1. Understand how important security principles must be adhered to when securing the infrastructures
2. Understand the importance of balancing security, operational effectiveness and cost
3. Analyze and to aptly secure the cyber perimeter of the infrastructures against cyber attacks

**Syllabus:**

Network Security tool taxonomy: Reconnaissance tools, attack and penetration tools, defensive tools.

High, Medium, Low and Virtual honeypots, NMAP, TCPDUMP, Wireshark, Reverse firewalling, securing honeypots, sebek, Argos, Honeywall.

Hybrid systems, client honeypots, Botnets, tracking botnets, analysing malware.

Capturing malware using honeypots, implementing honeypots, medium interaction and high interaction honeypots.

Security metrics: What is a security metric? Metric and measurement, Designing effective security metrics, Data sources for security metrics, Analysis of security metrics data, Designing the security measurement project, Measuring security cost and value, Different context for security process management.

**References:**

1. Gary M. Jackson, Predicting Malicious Behavior, John Wiley & Sons, 2012.
2. Niels Provos, Thorsten Holz, Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Addison Wesley, 2007.
3. IT Security Metrics, Lance Hayden, Tata McGraw Hill.
4. Lance Spitzner, Know Your Enemy: Learning about Security Threats (2nd Edition), 2004.
5. Building Open Source Network Security Tools: Components and Techniques, Mike Schiffman.

# Second Semester
# Electives 4 and 5

## Big Data and Analytics (MCS2E40)

| L | T | P/D | Total | Credit |
|---|---|---|---|---|
| 3 | - | - | 3 | 3 |

Max. Marks: 100
Theory: 50 Marks
Mid-Sem: 50 Marks

**Course Objectives:** The objectives of this subject are:

1. To know the fundamental concepts of big data and analytics.
2. To explore tools and practices for working with big data
3. To learn about stream computing.
4. To know about the research that requires the integration of large amounts of data and practice with C, python and R.

**Course Outcomes:**

1. Work with big data tools and its analysis techniques.
2. Analyze data by utilizing clustering and classification algorithms.
3. Learn and apply different mining algorithms and recommendation systems for large volumes of data.
4. Perform analytics on data streams.
5. Learn NoSQL databases and management.

**Syllabus:**

Introduction to Big Data: Evolution of Big data – Best Practices for Big data Analytics, Big data characteristics, Validating, The Promotion of the Value of Big Data, Big Data Use Cases, Characteristics of Big Data Applications, Perception and Quantification of Value, Understanding Big Data Storage, A General Overview of High-Performance Architecture – HDFS – Map Reduce and YARN – Map Reduce Programming Model. Feature engineering and visualization.

Clustering and Classification: Advanced Analytical Theory and Methods: Overview of Clustering, K-means, Use Cases, Overview of the Method – Determining the Number of Clusters, Diagnostics – Reasons to Choose and Cautions. Classification: Decision Trees, Overview of a Decision Tree, The General Algorithm – Decision Tree Algorithms, Evaluating a Decision Tree, Decision Trees in R, Naïve Bayes, Baye's Theorem, Naive Bayes Classifier.

Association and Recommendation System: Advanced Analytical Theory and Methods: Association Rules, Overview – Apriori Algorithm, Evaluation of Candidate Rules, Applications of Association Rules, Finding Association & finding similarity. Recommendation System: Collaborative Recommendation, Content Based Recommendation, Knowledge Based Recommendation, Hybrid Recommendation Approaches.

Stream Memory: Introduction to Streams Concepts – Stream Data Model and Architecture, Stream Computing, Sampling Data in a Stream, Filtering Streams, Counting Distinct Elements in a Stream, Estimating moments, Counting oneness in a Window, Decaying Window, Real time Analytics Platform (RTAP) applications, Case Studies – Real Time Sentiment Analysis, Stock Market Predictions. Using Graph Analytics for Big Data: Graph Analytics.

Nosql Data Management for Big Data and Virtualization:NoSQL Databases: Schema-less Models‖: Increasing Flexibility for Data Manipulation-Key Value Stores, Document Stores, Tabular Stores, Object Data Stores, Graph Databases Hive, Sharding, Hbase, Analyzing big data with twitter, Big data for E-Commerce Big data for blogs. Review of Basic Data Analytic Methods using R.

**References:**

1. Anand Rajaraman and Jeffrey David Ullman, "Mining of Massive Datasets", Cambridge University Press, 2012.
2. David Loshin, "Big Data Analytics: From Strategic Planning to Enterprise Integration with Tools, Techniques, NoSQL, and Graph", Morgan Kaufmann/El sevier Publishers, 2013.
3. EMC Education Services, "Data Science and Big Data Analytics: Discovering, Analyzing, Visualizing and Presenting Data", Wiley publishers, 2015.
4. Bart Baesens, "Analytics in a Big Data World: The Essential Guide to Data Science and its Applications", Wiley Publishers, 2015.
5. Dietmar Jannach and Markus Zanker, "Recommender Systems: An Introduction", Cambridge University Press, 2010.

## Information Security Management (MCS2E42)

| L | T | P/D | Total | Credit |
|---|---|---|---|---|
| 3 | - | - | 3 | 3 |

Max. Marks: 100
Theory: 50 Marks
Mid-Sem: 50 Marks

**Course Objectives:**

The main objective of this course is to study and understand the principles of information security management that are widely used in organizations and businesses that deal with data and are connected to the Internet. It will introduce the students to commonly used methods and frameworks for addressing organizational and business security needs, and will help to understand risks involvement in managing and storing information assets.

**Course Outcomes:**

Upon successful completion of this course, students should be able to:

1. Understand basics of information security management including principles, themes and design solutions
2. Understand how to apply principles of information security management based on different contexts
3. Study various possible cyber-attacks and their adverse effects on information assets in an organization
4. Understand inter-relationship between various elements of information security management and its role in protecting enterprises and organizations.

**Syllabus:**

Fundamentals of Information Security: Key Elements of Networks, Logical Elements of Network, Critical Information Characteristics, Information States etc.

Information Security Management Concerns: Threats and Attack Vectors, Types of Attacks, Common Vulnerabilities, and Exposures (CVE), Security Attacks, Computer Security Concerns, Information Security Measures etc., threat and vulnerability management, incident management, risk management, information leakage, crisis management and business continuity, legal and compliance, security awareness and security implementation considerations,

Information Security Management – Methodologies and Frameworks: ISO 27000 series and the Plan-Do-Check-Act model, assessment of threats and vulnerabilities, incident response, forensics and investigations, risk assessment and risk management frameworks, dealing with classified/ sensitive data, contingency planning, legal and regulatory drivers and issues, certification, common criteria, security awareness, education and training, and practical considerations when implementing the frameworks to address current and future threats.

Information Security Policies, Procedures, and Audits: Information Security Policies necessity-key elements & characteristics, Governance, Security Policy Implementation, Configuration, Security Standards-Guidelines & Frameworks etc.

Information Security Management – Roles and Responsibilities: Security Roles & Responsibilities, Accountability, Roles, and Responsibilities of Information Security Management, team-responding to emergency situation-risk analysis process etc.

**References:**

1. Harold F. Tipton, Micki Krause, Information Security Management Handbook, CRC Press, 2007.
2. Jake Kouns, Daniel Minoli, Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practical Guide to Risk Management Teams, John Wiley & Sons, 2011
3. Dave Tyson, Security Convergence: Managing Enterprise Security Risk, Butterworth-Heinemann, 2011
4. Malcolm Harkins, Managing Risk and Information Security: Protect to Enable, Apress, 2012
5. Greg Witte, Melanie Cook, Matt Kerr, Shane Shaffer, Security Automation Essentials: Streamlined Enterprise Security Management & Monitoring with SCAP, McGraw Hill Professional, 2012.

## Advances in Cloud and Mobile Computing (MCS2E44)

| L | T | P/D | Total | Credit | | |
|---|---|---|---|---|---|---|
| 3 | - | - | 3 | 3 | Max. Marks: | 100 |
| | | | | | Theory: | 50 Marks |
| | | | | | Mid-Sem: | 50 Marks |

**Course Objectives:** To understand issues and research challenges Cloud and Mobile Computing**.**

**Course Outcomes:**

1. After completion of the course, the student will be able to:
2. Understand the basics the of Cloud and Mobile computing paradigms.
3. Understand different architectures of Cloud Computing.
4. Design Cloud and Mobile Computing based applications.

**Syllabus:**

Cloud Computing: Cloud Stability, and Scalability, Robustness of Data Centers, Dynamic Failure Detection and Recovery, Arbitrary and Non-arbitrary Failures, Membership Management, Group Communication, Gossip Protocols, Energy efficiency in Clouds, Mobile Cloud Computing, State of Art, Applications, Challenges, Cloud Gaming System, Correlation, Modelling, Architecture and Integration, Service Components, Routing, QoS, Cloud Computing for Mobile Services, Fusion, Event-driven Systems and Mobile Applications, Communication, Big Data, Value and Development, IoT and Big data, Generation and Acquisition, Storage, Analysis, Tools, Applications

Mobile Computing: Challenges in Mobile Computing, Coping with Uncertainty, Cooperative and Temporal Spectrum Sensing, Emerging Sensing Paradigms and Intelligence, Spectrum Management, Resource Scarcity, Bandwidth, Mobility, Localization, Synchronization, Handling Fundamental Challenges in Faulty Environments, Mitigating Coexistence and Interference, Reliable Message Delivery, Publish/Subscribe, Advanced Graph Theoretic Approaches in Mobile Computing Systems, Algorithms for Construction of Virtual Structures, Fault Tolerance, Blocking and Non-blocking Protocols

**References:**

1. Kenneth P. Birman, Guide to Reliable Distributed Systems, Springer, 2012.
2. Zaigham Mahmood, Ricardo Puttini, and Thomas Erl, Cloud Computing: Concepts, Technology & Architecture. Prentice Hall. ISBN: 9780133387568
3. S. Thamarai Selvi, Christian Vecchiola, and Rajkumar Buyya, Mastering Cloud Computing, Morgan Kaufmann. ISBN: 9780124114548
4. F. Richard Yu and Victor Leung, Advances in Mobile Cloud Computing Systems, CRC Press.
5. Advances on Cloud Computing and Context-Aware Systems, vol. 19, no. 2, April 2014, Mobile Networks and Applications, Springer.
6. Ivan Stojmenovic, Handbook of Wireless Networks and Mobile Computing, John Wiley & Sons.
7. Sudip Misra, Barun Kumar Saha, and Sujata Pal, Opportunistic Mobile Networks: Advances and Applications, Springer International Publishing, 2016.

## Information Warfare (MCS2E46)

| L | T | P/D | Total | Credit |
|---|---|---|---|---|
| 3 | - | - | 3 | 3 |

Max. Marks: 100
Theory: 50 Marks
Mid-Sem: 50 Marks

**Course Objectives:**

This course addresses some of the unique and emerging policy, doctrine, strategy, and operational requirements of conducting cyber warfare at the nation-state level. It provides students with a unified battle-space perspective and enhances their ability to manage and develop operational systems and concepts in a manner that results in the integrated, controlled, and effective use of cyber assets in warfare.

**Course Outcomes:**

On completion of this course, students should be able to:

1. Explain the theory of data, information and knowledge as they pertain to information warfare
2. Apply strategies of using information as a weapon and a target
3. Apply the principles of offensive and defensive information warfare for a given context
4. Discuss the social, legal and ethical implications of information warfare
5. Evaluate contemporary information warfare concepts for their application in a corporate environment

**Syllabus:**

Introduction and Models of Information Warfare- Information Resources, The Value of Resources, Players, The Offense, The Defense, A Dual Role, Offensive Information Warfare, Increased Availability to Offensive Player, Decreased Availability to Defensive Player, Decreased Integrity, Other Classification Schemes, Defensive Information Warfare, Types of Defense, Information Security and Information Assurance, The CIA Model and Authorization, Playgrounds to Battlegrounds, Play, Motivation, Culture, More than Child's Play, Intellectual Property Crimes, Fraud, Computer Fraud and Abuse. Fighting Crime, Individual Rights, National Security, Foreign Intelligence, War and Military Conflict, Terrorism, Netwars, Protecting National Infrastructures.

Open Sources- Open Source and Competitive Intelligence, Privacy, Snooping on People Through Open Sources, Web Browsing, Privacy Regulations, Piracy, Copyright Infringement, Trademark Infringement, Dark Sides.

Psyops and Perception Management- Lies and Distortions, Distortion, Fabrication, Hoaxes, Social Engineering, Denouncement, Conspiracy Theories, Defamation, Harassment, Advertising, Scams, Spam Wars, Censorship, United States Restrictions.

Inside the Fence- Traitors and Moles, State and Military Espionage, Economic Espionage, Corporate Espionage, Privacy Compromises, Business Relationships, Visits and Requests, Fraud and Embezzlement, Bogus Transactions, Data Diddling, Inside Sabotage, Physical Attacks, Software Attacks, Penetrating the Perimeter, Physical Break-ins and Burglaries, Search and Seizure, Dumpster Diving, Bombs.

Computer Break-Ins and Hacking- Accounts, Getting Access, Tools and Techniques, A Demonstration, Network Scanners, Packet Sniffers, Password Crackers, Buffer Overþows and Other Exploits, Social Engineering, Covering up Tracks, Information Theft, Gathering Trophies, More than Trophies, Tampering, Web Hacks, Domain Name Service Hacks, Takedown, Remote Shutdown Extent.

**References:**

1. Daniel Ventre, Cyberwar and Information Warfare, John Wiley & Sons.2012
2. Daniel Ventre, Information Warfare, Wiley - ISTE (2009) (ISBN 9781848210943).
3. Information Warfare and Security, Dorothy E. Denning, Denning Edition 1, 1998 Addison-Wesley.
4. Dorothy Denning, Information Warfare and Security, Addison-Wesley (1998.)

## Cyberspace Operations and Design (MCS2E48)

| L | T | P/D | Total | Credit |
|---|---|---|---|---|
| 3 | - | - | 3 | 3 |

Max. Marks: 100
Theory: 50 Marks
Mid-Sem: 50 Marks

**Course Objectives:**

This course provides a basic understanding of full-spectrum cyberspace operations, the complexities of the cyberspace environment, as well as planning, organizing, and integrating cyberspace operations. The course will consist of presentations and exercises that will teach students how to develop a cyber-operations design and bring it to fruition. At the conclusion of the course, students will have a fundamental understanding of how to analyze, plan for, and execute cyberspace operations.

**Course Outcomes:**

In this course, students will gain a better understanding of cyber operations (CO) for the deployment of computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE), against an adversary to achieve objectives and cause effects in support of a mission set.

This course, founded on concept operations and real cyber capabilities, provides students with the understanding, tools, and processes needed to conduct malware analysis with real-world malicious code samples to dissect. Students will be able to prepare and plan an effective offensive and defensive strategy, as well as evaluate covert protocols. Analysis of system specific, non-descript tools will be introduced to aid in attack and defense. After attending this course students will have the knowledge of following topics

1. Understanding of Cyberspace Environment and Design
2. Cyberspace Operational Approaches
3. Cyberspace Operations
4. Cyberspace Integration
5. Building Cyber Warriors and Warrior Corps
6. Designing Cyber Related Command
7. Training and Readiness for Cyber Related Commands

**Syllabus:**

Understanding the Cyberspace Environment and Design- Cyberspace environment and its characteristics, Developing a design approach, Planning for cyberspace operation

Cyberspace Operational Approaches- Foundational approaches that utilize cyberspace capabilities to support organizational missions, The pros and cons of the different approaches

Cyberspace Operations- Network Operations (NETOPS), Defensive Cyberspace Operations (DCO), Offensive Cyberspace Operations (OCO), Defense and Diversity of Depth network design, Operational methodologies to conduct cyberspace operations

Cyberspace Integration- Design a cyberspace operation and integrate it with a Joint Operations plan, Practice the presented methodologies in a practical application exercise.

Building Cyber Warriors and Warrior Corps- The warrior and warrior corps concept as applied to cyber organizations, The challenges of training and developing a cyber-workforce from senior leadership to the technical workforce

Designing Cyber Related Commands- Mission statements, Essential tasks, Organizational structures, Tables of organizations

Training and Readiness for Cyber Related Commands- Mission Essential Tasks (METs), Developing the cyber workforce, Plan your own training programs within your organization.

**References:**

1. Paulo Shakarian et al. "Introduction of Cyber Warfare: A Multidisciplinary Approach," syngress, Elsevier 2013.
2. Jeffery carr et al, "Inside Cyber Warfare: Mapping the Cyber Underworld," O'ReillyPublication December 2012.
3. Jason Andress et al. "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners" Syngress, Elsevier 2013.
4. R. A. Clarke, Robert Knake "Cyber War: The Next Threat to National Security and What to Do About It" Haper Collins Publisher 2010.

## Ethics and Laws of Cyber Security (MCS2E50)

| L | T | P/D | Total | Credit |
|---|---|---|---|---|
| 3 | - | - | 3 | 3 |

Max. Marks: 100
Theory: 50 Marks
Mid-Sem: 50 Marks

**Course Objectives:**

To understand the basics of cyber law, its related issues and ethical laws of computer for different countries.

**Course Outcomes:**

The students of this course will be able to:

1. Understand key terms and concepts in cyber law, intellectual property and cyber-crimes, trademarks and domain theft.
2. Determine computer technologies, digital evidence collection, and evidentiary reporting in forensic acquisition.
3. Secure both clean and corrupted systems, protecting personal data, securing simple computer networks, and safe Internet usage.
4. Incorporate approaches for incident analysis and response.

**Syllabus:**

Introduction-Cyber Security and its Problem-Intervention Strategies: Redundancy, Diversity and Autarchy.

Introduction to the Legal Perspectives of Cybercrimes and Cyber security, Cybercrime and the Legal Landscape around the World, Why Do We Need Cyber laws, The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India, Consequences of Not Addressing the Weakness in Information Technology Act, Digital Signatures and the Indian IT Act, Cybercrime and Punishment, Cyber law, Technology and Students: Indian Scenario.

Private ordering solutions, Regulation and Jurisdiction for global Cyber security, Copy Right-source of risks, Pirates, Internet Infringement, Fair Use, postings, criminal liability, First Amendments, Data Losing.

Ethics, Legal Developments, Cyber security in Society, Security in cyber laws case studies, General lawand Cyber Law-a Swift Analysis.

**References:**

1. Sunit Belapure and Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley India Pvt. Ltd, 2011.
2. Mark F Grady, Fransesco Parisi, “The Law and Economics of Cyber Security”, Cambridge University Press, 2006.
3. Jonathan Rosenoer, “Cyber Law: The law of the Internet”, Springer-Verla.