M.Tech. Degree
PROGRAMME

in

COMPUTER ENGINEERING (CYBER SECURITY)

CURRICULUM
(w. e. f. Session 2019-2020)

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 will produce post graduates that, within a few years of graduation:

<table>
<thead>
<tr>
<th>PEOs</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEO 1</td>
<td>Graduates of the institute will have adequate knowledge of computer science and engineering to excel in professional career and/or higher education.</td>
</tr>
<tr>
<td>PEO 2</td>
<td>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.</td>
</tr>
<tr>
<td>PEO 3</td>
<td>Graduates of the institute will have attitude towards continuous learning and will exhibit professional ethics, communication skills, team work in all walks of life.</td>
</tr>
</tbody>
</table>

PROGRAM OUTCOMES (POs)

Graduates of the Programme:

<table>
<thead>
<tr>
<th>PO</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO 1</td>
<td>Apply the knowledge of science, mathematics, engineering and computing fundamentals appropriate to the discipline.</td>
</tr>
<tr>
<td>PO 2</td>
<td>Identify, formulate, review research literature, and analyse complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.</td>
</tr>
<tr>
<td>PO 3</td>
<td>Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.</td>
</tr>
<tr>
<td>PO 4</td>
<td>Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.</td>
</tr>
<tr>
<td>PO 5</td>
<td>Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.</td>
</tr>
<tr>
<td>PO 6</td>
<td>Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal, environmental impact, sustainable development, cultural issues and the consequent responsibilities relevant to the professional engineering practice.</td>
</tr>
<tr>
<td>PO 7</td>
<td>Recognize the need for, and have the preparation and ability, through knowledge of contemporary issues, to engage in independent and life-long learning in the broadest context of technological change.</td>
</tr>
<tr>
<td>PO 8</td>
<td>Apply ethical principles and commit to social issues, professional ethics, and responsibilities and norms of the engineering practice.</td>
</tr>
<tr>
<td>PO 9</td>
<td>Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.</td>
</tr>
<tr>
<td>PO 10</td>
<td>Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.</td>
</tr>
<tr>
<td>PO 11</td>
<td>Demonstrate knowledge and understanding of the engineering and management principles and apply these to one’s own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.</td>
</tr>
</tbody>
</table>
SCHEME
Department of Computer Engineering, NIT Kurukshetra

Proposed Scheme for the
Master of Technology in Computer Engineering (Cyber Security)
Curriculum w.e.f July 2019

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>Code</th>
<th>Course Title</th>
<th>Teaching Schedule</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>L</td>
<td>T</td>
</tr>
<tr>
<td>First Semester</td>
<td></td>
<td></td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>1.</td>
<td>MCO2C01</td>
<td>Advanced Data Structures and Algorithms</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>2.</td>
<td>MCO2C03</td>
<td>System and Network Security</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>3.</td>
<td>MCO2C05</td>
<td>Cyber Security and Data Privacy</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>4.</td>
<td></td>
<td>Elective-1</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>5.</td>
<td></td>
<td>Elective-2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>6.</td>
<td>MCO2L01</td>
<td>Algorithms Laboratory</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7.</td>
<td>MCO2L03</td>
<td>System and Network Security Lab</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8.</td>
<td>MCO2S01</td>
<td>Seminar</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total</td>
<td>21</td>
<td>18</td>
</tr>
</tbody>
</table>

Second Semester

|        |         |                                                  | 3  | 0  | 0  | 3    | 3    |
|        |         |                                                  | 3  | 0  | 0  | 3    | 3    |
|        |         |                                                  | 3  | 0  | 0  | 3    | 3    |
|        |         |                                                  | 3  | 0  | 0  | 3    | 3    |
|        |         |                                                  | 3  | 0  | 0  | 3    | 3    |
|        |         |                                                  | 0  | 0  | 2  | 2    | 1    |
|        |         |                                                  | 0  | 0  | 2  | 2    | 1    |
|        |         |                                                  | 0  | 2  | 0  | 2    | 1    |
|        |         | Total                                             | 21 | 18 |     |       |

Third Semester

|        |         |                                                  | 14  |     |     |     |
|        |         |                                                  |     |     |     |     |
| Fourth Semester | |                                                  | 14  |     |     |     |

Note:
- Elective can be opted from the list of electives/ core subjects of various specializations of Computer Engineering Department.
- Electives-V 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

<table>
<thead>
<tr>
<th>Code</th>
<th>Course Title</th>
<th>Code</th>
<th>Course Title</th>
<th>Code</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCO2E31</td>
<td>Advanced Computer Networks</td>
<td>MCO2E32</td>
<td>Soft Computing</td>
<td>MCO2E40</td>
<td>Big Data and Analytics</td>
</tr>
<tr>
<td>MCO2E33</td>
<td>Intrusion Detection Systems</td>
<td>MCO2E34</td>
<td>Secure Coding</td>
<td>MCO2E42</td>
<td>Information Security Management</td>
</tr>
<tr>
<td>MCO2E35</td>
<td>Distributed Computing</td>
<td>MCO2E36</td>
<td>Network Forensics</td>
<td>MCO2E44</td>
<td>Advances in Cloud and Mobile Computing</td>
</tr>
<tr>
<td>MCO2E37</td>
<td>Biometric Security</td>
<td>MCO2E38</td>
<td>Network Security Tools and Techniques</td>
<td>MCO2E46</td>
<td>Information Warfare</td>
</tr>
<tr>
<td>MCO2E39</td>
<td>Social Network Analysis</td>
<td></td>
<td></td>
<td>MCO2E48</td>
<td>Cyberspace Operations and Design</td>
</tr>
<tr>
<td>MCO2E41</td>
<td>Vulnerability Discovery and Exploit Development</td>
<td></td>
<td></td>
<td>MCO2E50</td>
<td>Ethics and Laws of Cyber Security</td>
</tr>
<tr>
<td>MCO2E32</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MCO2E34</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MCO2E40</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MCO2E42</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MCO2E44</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MCO2E46</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MCO2E48</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MCO2E50</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Advanced Data Algorithms and Algorithms (MCO2C01)

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

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.

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


References:
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.

System and Network Security (MCO2C03)

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
<th>Max. Marks: 100</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>3</td>
<td>Theory: 50 Marks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mid-Sem: 50 Marks</td>
</tr>
</tbody>
</table>

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.

Syllabus:
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.

Android platform security models- Android, iOSMobile 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.

Textbooks and References:

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.

Cyber Security and Data Privacy (MCO2C05)

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Max. Marks: 100</td>
</tr>
</tbody>
</table>

8 | P a g e
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.

Syllabus:
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.
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.

Textbooks and References:

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.

First Semester
Electives
Advanced Computer Networks (MCO2E31)

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

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.

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:
5. Rajiv Ramaswami, Kumar N. Sivarajan, Galen H. Sasaki, Optical Networks: A Practical Perspective, Morgan Kaufmann.

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.

Intrusion Detection Systems (MCO2E33)

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
<th>Max. Marks: 100</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td></td>
<td>-</td>
<td>3</td>
<td>3</td>
<td>Theory: 50 Marks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mid-Sem: 50 Marks</td>
</tr>
</tbody>
</table>

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.

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.

Text books:

Reference books:

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.

Distributed Computing (MCO2E35)

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

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.

Syllabus:


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.
Text books:
4. Distributed Systems and Algorithmic Approach by Su Kumar Boss, Chamal & Hall.
8. Introduction to Distributed Algorithms by G Tel, Cambridge University.

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.

Biometric Security (MCO2E37)

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
<th>Max. Marks: 100</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>3</td>
<td>Theory: 50 Marks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mid-Sem: 50 Marks</td>
</tr>
</tbody>
</table>

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

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.

**Text books:**

**Reference books:**

**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.

**Social Network Analysis (MCO2E39)**

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
<th>Max. Marks:</th>
<th>100</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>3</td>
<td>Theory:</td>
<td>50 Marks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mid-Sem:</td>
<td>50 Marks</td>
</tr>
</tbody>
</table>

**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.

**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

Text books and References:

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.

Vulnerability Discovery & Exploit Development (MCO2E41)

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
<th>Max. Marks: 100</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>3</td>
<td>Theory:  50 Marks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mid-Sem:  50 Marks</td>
</tr>
</tbody>
</table>

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.

Syllabus:


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 differencing 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 Heap Overflows and Client-Side Exploitation- Windows heap management, constructs, and environment, Browser-based and client-side exploitation, Remedial heap spraying, Understanding C++, vtable/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


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

Text books and References:
3. Professional Penetration Testing: Creating and Operating a Formal Hacking Lab, Thomas Wilhelm

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

Second Semester
Core Courses

Number Theory and Cryptography (MCO2C02)

<table>
<thead>
<tr>
<th></th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>T</td>
<td></td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

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.

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:
3. An Introduction to theory of numbers, Niven, Zuckerman and Montgomery, (Wiley 2006)

Reference books:
1. An Introduction to Cryptography, R.A. Mollin (Chapman & Hall, 2001)
2. Rational Points on Elliptic Curves, Silverman and Tate (Springer 2005)
4. Elementary Number Theory, Jones and Jones (Springer, 1998)

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.
Cloud and IoT Security (MCO2C04)

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

Course Objectives:
1. To understand the fundamentals of Internet of Things (IoT) and Cloud Computing.
2. Explore the cryptographic fundamentals for IoT.
3. Ability to understand the Security requirements in IoT.
4. To apply the concept of Internet of Things in the real world scenario.

Syllabus:


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

Books and References:

Course Outcomes:
1. Identify different issues in IoT security.
2. To analyze protocols and reference architectures developed for IoT.
3. To identify and understand various applications of IoT.

Second Semester
Electives with Lab

Soft Computing (MCO2E32)

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
<th>Max. Marks: 100</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>3</td>
<td>Theory: 50 Marks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mid-Sem: 50 Marks</td>
</tr>
</tbody>
</table>
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.

Syllabus:
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.

Text books:

Reference books:

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.

Secure Coding (MCO2E34)

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

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.

Syllabus:


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.


**Text books and References:**

**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.

**Network Forensics (MCO2E36)**

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
<th>Max. Marks:</th>
<th>100</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>-</td>
<td>3</td>
<td>3</td>
<td>Theory:</td>
<td>50 Marks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>-</td>
<td></td>
<td></td>
<td>Mid-Sem:</td>
<td>50 Marks</td>
</tr>
</tbody>
</table>

**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.

**Syllabus:**
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

**Text books:**

**Reference books:**

**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.

**Network Security Tools and Techniques (MCO2E38)**

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
<th>Max. Marks: 100</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>3</td>
<td>Theory: 50 Marks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mid-Sem: 50 Marks</td>
</tr>
</tbody>
</table>

**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.

**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.

**Text books:**

**Reference books:**

**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

**Second Semester**
**Electives 4 and 5**

**Big Data and Analytics (MCO2E40)**

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Max. Marks: 100

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Theory</td>
<td>50 Marks</td>
<td></td>
</tr>
<tr>
<td>Mid-Sem</td>
<td>50 Marks</td>
<td></td>
</tr>
</tbody>
</table>

**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.

**Syllabus:**


Association and Recommendation System: Advanced Analytical Theory and Methods:


References:

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.

Information Security Management (MCO2E42)

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
<th>Max. Marks: 100</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>3</td>
<td>Theory: 50 Marks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mid-Sem: 50 Marks</td>
</tr>
</tbody>
</table>

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.

**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,


**Text books and References:**

**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.

---

**Advances in Cloud and Mobile Computing (MCO2E44)**

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
<th>Max. Marks: 100</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>3</td>
<td>Theory: 50 Marks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mid-Sem: 50 Marks</td>
</tr>
</tbody>
</table>

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

**Syllabus:**

References:

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.
4. Design Cloud and Mobile Computing based applications.

Information Warfare (MCO2E46)

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

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.

Syllabus:
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.


Text books:

Reference books:
2. Dorothy Denning, Information Warfare and Security, Addison-Wesley (1998.)

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

Cyberspace Operations and Design (MCO2E48)
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.

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.

Text books and References:

**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

**Ethics and Laws of Cyber Security (MCO2E50)**

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P/D</th>
<th>Total</th>
<th>Credit</th>
<th>Max. Marks:</th>
<th>100</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>3</td>
<td>Theory:</td>
<td>50 Marks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Mid-Sem:</td>
<td>50 Marks</td>
</tr>
</tbody>
</table>

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

**Syllabus:**
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.


Text book:

Reference books:

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.