# CURRICULUM

## I SEMESTER

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Name of the Subject</th>
<th>Category</th>
<th>Periods</th>
<th>Marks*</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS162</td>
<td>Mathematical Foundations of Information Security</td>
<td>TY</td>
<td>3 1 -</td>
<td>40 60 100</td>
<td>4</td>
</tr>
<tr>
<td>CS163</td>
<td>Advanced Data Structure and Algorithms</td>
<td>TY</td>
<td>3 1 -</td>
<td>40 60 100</td>
<td>4</td>
</tr>
<tr>
<td>CS164</td>
<td>Security Threats and Trusted Computing</td>
<td>TY</td>
<td>3 1 -</td>
<td>40 60 100</td>
<td>4</td>
</tr>
<tr>
<td>CS165</td>
<td>Secure Software Engineering</td>
<td>TY</td>
<td>3 1 -</td>
<td>40 60 100</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Elective-I</td>
<td>TY</td>
<td>3 1 -</td>
<td>40 60 100</td>
<td>4</td>
</tr>
<tr>
<td>CS166</td>
<td>Information Security Laboratory-I</td>
<td>LB</td>
<td>- - 3</td>
<td>60 40 100</td>
<td>2</td>
</tr>
</tbody>
</table>

**Total Credits** 26

## II SEMESTER

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Category</th>
<th>Periods</th>
<th>Marks*</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS167</td>
<td>Security Standards and Information Security Management</td>
<td>TY</td>
<td>3 1 -</td>
<td>40 60 100</td>
<td>4</td>
</tr>
<tr>
<td>CS168</td>
<td>Applied Cryptography</td>
<td>TCM</td>
<td>3 - 2</td>
<td>50 50 100</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Elective-III</td>
<td>TY</td>
<td>3 1 -</td>
<td>40 60 100</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Elective-IV</td>
<td>TY</td>
<td>3 1 -</td>
<td>40 60 100</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Elective-V</td>
<td>TY</td>
<td>3 1 -</td>
<td>40 60 100</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>Elective-VI</td>
<td>TY</td>
<td>3 1 -</td>
<td>40 60 100</td>
<td>4</td>
</tr>
<tr>
<td>CS169</td>
<td>Information Security Laboratory-II</td>
<td>LB</td>
<td>- - 3</td>
<td>60 40 100</td>
<td>2</td>
</tr>
<tr>
<td>CS159</td>
<td>Research Methodology</td>
<td>PR</td>
<td>- - 3</td>
<td>100 - 100</td>
<td>2</td>
</tr>
</tbody>
</table>

**Total Credits** 27
### III SEMESTER

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Category</th>
<th>Periods</th>
<th>Marks*</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS170</td>
<td>Project Work (Phase I)</td>
<td>PR</td>
<td>-</td>
<td>150</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>150</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>300</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>9</strong></td>
</tr>
</tbody>
</table>

### IV SEMESTER

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Category</th>
<th>Periods</th>
<th>MARKS*</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS171</td>
<td>Project Work (Phase II)</td>
<td>PR</td>
<td>-</td>
<td>200</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>200</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>400</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td>Professional Development Courses</td>
<td>PR</td>
<td>-</td>
<td>200</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>(2 one credit courses)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Total Credits</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>16</strong></td>
</tr>
</tbody>
</table>

A representative list of Professional Development Courses is given below *(Limited to one credit)*:

- a) Industrial Training
- b) Specific Field Knowledge Training
- c) Seminar related with directed study
- d) Paper Publication in SCI Journals

# CA – Continuous Assessment, SE – Semester Examination, TM – Total Marks  
* TY – Theory, LB – Laboratory, TCM – Theory with a Mini Project, PR – Practice
<table>
<thead>
<tr>
<th>Sl.No.</th>
<th>Subject Code</th>
<th>Subject</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>CSE67</td>
<td>Internals of Operating System</td>
<td>TY</td>
</tr>
<tr>
<td>2.</td>
<td>CSE68</td>
<td>Distributed System Security</td>
<td>TY</td>
</tr>
<tr>
<td>3.</td>
<td>CSE69</td>
<td>Ethical Hacking</td>
<td>TY</td>
</tr>
<tr>
<td>4.</td>
<td>CSE70</td>
<td>Embedded Systems</td>
<td>TY</td>
</tr>
<tr>
<td>5.</td>
<td>CSE71</td>
<td>Information Theory and Coding</td>
<td>TY</td>
</tr>
<tr>
<td>6.</td>
<td>CSE72</td>
<td>Digital and Cyber Forensics</td>
<td>TY</td>
</tr>
<tr>
<td>7.</td>
<td>CSE73</td>
<td>Mobile Wireless Security</td>
<td>TY</td>
</tr>
<tr>
<td>8.</td>
<td>CSE74</td>
<td>Security Assessment and Verification</td>
<td>TY</td>
</tr>
<tr>
<td>9.</td>
<td>CSE75</td>
<td>Internet Security Protocols</td>
<td>TY</td>
</tr>
<tr>
<td>10.</td>
<td>CSE76</td>
<td>Network Security Essentials</td>
<td>TY</td>
</tr>
<tr>
<td>11.</td>
<td>CSE77</td>
<td>Human Aspects in Information Security</td>
<td>TY</td>
</tr>
<tr>
<td>12.</td>
<td>CSE78</td>
<td>Game Theory</td>
<td>TY</td>
</tr>
<tr>
<td>13.</td>
<td>CSE79</td>
<td>Database Security and Auditing</td>
<td>TY</td>
</tr>
<tr>
<td>14.</td>
<td>CSE80</td>
<td>Intelligent Systems</td>
<td>TY</td>
</tr>
<tr>
<td>15.</td>
<td>CSE81</td>
<td>Cloud and Big Data Security</td>
<td>TY</td>
</tr>
<tr>
<td>16.</td>
<td>CSE82</td>
<td>Data Hiding and Biometric Security</td>
<td>TY</td>
</tr>
<tr>
<td>17.</td>
<td>CSE83</td>
<td>Intellectual Property Rights</td>
<td>TY</td>
</tr>
<tr>
<td>18.</td>
<td>CSE84</td>
<td>Information Security Policies</td>
<td>TY</td>
</tr>
<tr>
<td>19.</td>
<td>CSE85</td>
<td>Secure Coding</td>
<td>TY</td>
</tr>
<tr>
<td>20.</td>
<td>CSE86</td>
<td>Web Application Security</td>
<td>TY</td>
</tr>
</tbody>
</table>
SYLLABUS (Core Subjects)
<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS162</td>
<td>Mathematical Foundations of Information Security</td>
<td>3 1 - 4</td>
<td>40 60 100</td>
<td></td>
</tr>
</tbody>
</table>

**Prerequisite**
- -

**Objectives**
- To provide concepts of security and mechanisms
- To learn mathematical background foundation insight of information security

**Outcomes**
On successful completion of the course, the students will be able to:
- apply the concepts in the implementation of security issues
- mathematically prove the efficiency of the cryptography algorithms
- perform crypt analysis

**UNIT – I**


**UNIT – II**


**UNIT – III**


**UNIT – IV**

Primality and Factoring: Pseudoprimes – the rho (γ) method – Format factorization and factor bases – the continued fraction method – the Quadratic Seieve method.

**UNIT – V**


(*Theorem Proofs are excluded from all the units in this course of study*)

**Text Books:**

**Reference Books:**

**Websites:** -
### Subject Code: CS163

**Subject:** Advanced Data Structure and Algorithms

<table>
<thead>
<tr>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>T</td>
<td>P</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
</tbody>
</table>

**Prerequisite:** -

**Objectives:**
- To learn techniques for designing algorithms using appropriate data structures
- To develop the data structures for implementing the algorithms
- To identify a problem and analyze it in terms of its significant parts and the information needed to solve it

**Outcomes:**
On successful completion of the course, the students will be able to:
- Familiarize the student with good programming design methods, particularly Top-Down design
- Develop skills of design and analysis of algorithms in program development and organization
- Solve problems using different data structures and design techniques, and compare their performance and tradeoffs
- Prove correctness and analyze run time complexity of algorithms

**UNIT – I**

<table>
<thead>
<tr>
<th>Hours: 09</th>
</tr>
</thead>
</table>

**UNIT – II**

<table>
<thead>
<tr>
<th>Hours: 09</th>
</tr>
</thead>
</table>

**UNIT – III**

<table>
<thead>
<tr>
<th>Hours: 09</th>
</tr>
</thead>
</table>

**UNIT – IV**

<table>
<thead>
<tr>
<th>Hours: 09</th>
</tr>
</thead>
</table>

**UNIT – V**

<table>
<thead>
<tr>
<th>Hours: 09</th>
</tr>
</thead>
</table>

**Total contact Hours:** 45

**Total Tutorials:** 15

**Total Practical Classes:** -

**Total Hours:** 60

**Text Books:**

**Reference Books:**

**Websites:**
1. http://nptel.ac.in/courses/106102064/
<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS164</td>
<td>Security Threats and Trusted Computing</td>
<td>3 1 - 4 40 60 100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Prerequisite**
- To introduce the various types of threats to security, approaches for threat modeling and threat containment.
- To familiarize the vulnerability scanning process and the tools available.
- To introduce the concept of Trusted Computing.

**Objectives**

**Outcomes**

On successful completion of the course, the students will be able to:
- Understand the various threats to security and their relation to vulnerabilities.
- Perform threat modeling to identify, prioritize and mitigate threats.
- Understand the operation of Trusted Computing.

**UNIT – I** **Introduction**

Hours: 09


**UNIT – II** **Network Security Threats**

Hours: 09


**UNIT – III** **Threat Modeling**

Hours: 09


**UNIT – IV** **Trusted Computing**

Hours: 09


**UNIT – V** **Design Goals and Implementation**

Hours: 09


Total contact Hours: 45 Total Tutorials: 15 Total Practical Classes: - Total Hours: 60

**Text Books:**


**Reference Books:**


**Websites:**

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS165</td>
<td>Secure Software Engineering</td>
<td>3 1 - 4</td>
<td>40 60 100</td>
<td></td>
</tr>
</tbody>
</table>

**Prerequisite**

-  

**Objectives**

- To understand the security concerns that need to be taken care in every phase of the software development
- To understand how the security requirements are incorporated into software systems

**Outcomes**

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

- appreciate the importance of security considerations in software engineering
- design and develop secure software systems

**UNIT – I**

**Introduction to Secure Software Engineering**

Hours: 09


**UNIT – II**

**Requirements Gathering for Secure Software**

Hours: 09


**UNIT – III**

**Secure Software Architecture and Design**

Hours: 09


**UNIT – IV**

**Secure Coding and Testing**

Hours: 09


**UNIT – V**

**Security – Complexity and Management for Secure Software**

Hours: 09


**Text Books**:  

**Reference Books**:  

**Websites**:

1. www.sis.pitt.edu/jjoshi/Devsec/secureSoftware.pdf
Department: Computer Science and Engineering
Programme: M.Tech. (Information Security)

Semester: One
Category: LB

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS166</td>
<td>Information Security Laboratory – I</td>
<td>-</td>
<td>3</td>
<td>60</td>
</tr>
</tbody>
</table>

Prerequisite:
- To gain a hands on experience of cryptographic algorithms
- To inculcate logical and practical thinking towards security problem solving
- To learn a hands on experience of threats and attacks

Objectives:

Outcomes:
On successful completion of the course, students will be able to:
- Implement cryptographic algorithms to solve specified problems
- Solve Security Problem for the industry
- Have the programming skills in the aspects of security

Cycle – I

Any Ten of the following exercises have to be implemented:
1. Understanding of cryptographic algorithms and implementation of the same in C or C++
2. Performance evaluation of various cryptographic algorithms
3. Illustrate Intrusion Detection and IPS
4. Program to implement AVL tree
5. Program to implement Dynamic Programming.
6. To verify the integrity of the message using Digital signature.
7. Penetration Testing and justification of penetration testing through risk analysis
8. Password guessing and Password Cracking
9. Configuring S/MIME for e-mail communication
10. Implementation of Access Control List
11. Develop an application which should include authentication, authorization and access control mechanism.
12. Implement Elliptic Curve Cryptosystems
13. Implement RSA Cryptosystem
14. Implement the Diffie–Hellman Key Agreement Protocol
15. Implement Zero-Knowledge Protocol
16. Implement Oblivious Transfer

Cycle – II

17. Any Five programs related to concern electives offered in this semester need to be implemented.

Total contact Hours: 45 Total Tutorials: 45 Total Practical Classes: 45 Total Hours: 45
### Course Overview

**Department:** Computer Science and Engineering  
**Programme:** M.Tech. (Information Security)

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS167</td>
<td>Security Standards and Information Security Management</td>
<td>L: 3  T: 1  P: -</td>
<td>C: 3  CA: 40  SE: 60  TM: 100</td>
<td></td>
</tr>
</tbody>
</table>

**Prerequisite:** -

**Objectives**
- To compile, analyze, and assess the applicability of best practices in addressing information security issues
- To integrate principles and techniques of risk analysis, project planning and ethics in the development of information security strategies
- To understand the security standards, laws and policies and practice in information security

**Outcomes**
On successful completion of the course students will be able to:
- Design information system with high level of security by planning and risk assessment
- Have knowledge on security standards, laws and policies and practice in information security
- Design information security by developing the Security Program using Management Models

**UNIT – I**  
**Introduction**


**UNIT – II**  
**Security Policy and Standards**


**UNIT – III**  
**Risk Management and Auditing for Security**


**UNIT – IV**  
**Information Security Management in Organizations**


**UNIT – V**  
**Law, Ethics and Maintenance**


**Total contact Hours:** 45  
**Total Tutorials:** 15  
**Total Practical Classes:** -  
**Total Hours:** 60  

**Text Books:**

**Reference Books:**


**Websites:**

Department: Computer Science and Engineering  
Programme: M.Tech. (Information Security)

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS168</td>
<td>Applied Cryptography</td>
<td>3</td>
<td>2</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>

Prerequisite: -

Objectives:
- To understand the various cryptographic concepts, algorithms and various methods of analysis of the cryptographic algorithms
- To understand the underlying mathematical structures of cryptographic algorithm
- To get an overview of the various applications of the cryptographic algorithms and implement them in mini project

Outcomes:
On successful completion of the course, the students will be able to:
- Understand the theories and concepts of Cryptographic
- Understand the Cryptographic Techniques
- Design the Cryptographic Algorithms
- Apply Cryptographic Algorithms in real world problems

UNIT – I  
Cryptographic Protocols


UNIT – II  
Cryptographic Techniques


UNIT – III  
Cryptographic Algorithms


UNIT – IV  
Cryptographic Algorithms Design


UNIT – V  
Cryptographic Algorithms Application


Mini Project

The students need to form in teams with maximum 3 students and carry out the mini project. Each team has to take a real world security issues or problem. They have to analyze, design and solve the problem using the suitable cryptographic protocols and algorithms.

Total contact Hours: 45  
Total Tutorials: -  
Total Practical Classes: 30  
Total Hours: 75

Text Books:

Reference Books:

**Websites:**

1. http://cacr.uwaterloo.ca/hac/l
**Department:** Computer Science and Engineering  
**Programme:** M.Tech. (Information Security)  
**Semester:** Two  
**Category:** LB

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS169</td>
<td>Information Security Laboratory – II</td>
<td>-</td>
<td>-</td>
<td>60</td>
</tr>
</tbody>
</table>

**Prerequisite:**

- To gain a hands on experience of security design, analysis and testing tools
- To assess and implement web application with Information security

**Objectives**

- On successful completion of the course, students will be able to:
  - Design solution for to solve specified problems
  - Analyze and Design security solutions to problems in applications and network layers
  - Calculate the strength of the generated password
  - Assess and implement web application with Information security

**Outcomes**

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

- Design solution for to solve specified problems
- Analyze and Design security solutions to problems in applications and network layers
- Calculate the strength of the generated password
- Assess and implement web application with Information security

**Cycle – I**

- Any Four programs related to concern electives offered in this semester need to be implemented.
- The following exercises have to be implemented using various software tools/utilities.
  - Passive Information Gathering
    - IP Address and Domain Identification of log entries
    - Information Gathering of a web site
    - Banner Grabbing
  - Detecting Live Systems
    - Port Scanning
    - Passive Fingerprinting
    - Active Fingerprinting
  - Enumerating Systems
    - SNMP Enumeration
    - Enumerating Routing Protocols
  - Automated Attack and Penetration Tools
    - Vulnerability Assessment Tool
  - Defeating Malware
    - Building Trojans, Rootkit Hunter
    - Finding malware
  - Securing Wireless Systems
    - Scan WAPs
  - Network analysis
    - Analyze your network using any tool
    - Find the Vulnerabilities present in your Network
    - Perform Penetration Testing on your network
    - Implement Pro-active and Reactive measures to secure your network

**Cycle – II**

- Setting up the local security policy
- Develop a web application with secure database using any hashing algorithm
- Program to generate Password automatically which is easy to remember and calculate the strength the generated password
- Develop a web application and perform penetration testing to detect the vulnerabilities present in it.
- Suggest and implement measures to overcome the vulnerabilities identified in exercise 4

**Total contact Hours:** -  
**Total Tutorials:** -  
**Total Practical Classes:** 45  
**Total Hours:** 45
<table>
<thead>
<tr>
<th>Subject code</th>
<th>Subject</th>
<th>Hours/week</th>
<th>Credit</th>
<th>Maximum marks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>L</td>
<td>T</td>
<td>P</td>
</tr>
<tr>
<td>CS159</td>
<td>Research Methodology</td>
<td>-</td>
<td>-</td>
<td>3</td>
</tr>
</tbody>
</table>

**Prerequisite**: -

**Objectives**
- To educate students to methods of selection of research problems
- To expose students to different research methods

**Outcomes**
- Students will be capable to identify and narrow down to the area of research on the basis the requirements of industrial and global requirements
- Students will exhibit the domain skill to choose suitable research methods to execute research effectively
- Students will possess knowledge to further their academic program, namely, Ph.D program.

- **Characteristics of research**: Various functions that describe characteristics of research such as systematic, valid, verifiable, empirical and critical approach.
- **Types of research**: Pure and applied research. Descriptive and explanatory research. Qualitative and quantitative approaches.
- **Research procedure**: Formulating the Research Problem, Literature Review, Developing the objectives, Preparing the research design including sample. Design, Sample size.
- **Considerations in selecting research problem**: Relevance, interest, available data, choice of data, Analysis of data, Generalization and interpretation of analysis.

**Total contact hours**: -  
**Total tutorials**: -  
**Total practical classes**: 15  
**Total hours**: 15

**Reference books**:
1. Dawson, Catherine, Practical Research Methods, UBS Publishers and Distributors, New Delhi, 2002
<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS170</td>
<td>Project Work (Phase I)</td>
<td>-</td>
<td>9</td>
<td>150</td>
</tr>
</tbody>
</table>

**Prerequisite**
- 

**Objectives**
- To expose students with project-product development cycle using state-of-art technologies
- To understand the Product Development Cycle through Project
- To plan for various activities of the project

**Outcome**
On successful completion of the course, the students will be able to:
- Able to State problem definition clearly
- Prepare SRS for projects and develop design
- Exposure to Learning and knowledge access techniques using Conferences, Journal papers and participation in research activities

**PHASE – I**
The student is required to do the following:
1. Select a Research Problem.
2. Conduct a Survey in the chosen area.
3. Perform a feasibility study.
4. Study the limitations of the Existing System.
5. Define the Problem Statement and Objectives.
6. Choose the Research Methodology.
7. Finalize the Experimental Environment.
8. Choose the evaluation parameters.
9. Implement the Existing System.
10. Document the outcome of Phase I.

**Total contact Hours:** -  
**Total Tutorials:** -  
**Total Practical Classes:** -  
**Total Hours:** -
<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>L  T  P   C</td>
<td>CA</td>
<td>SE  TM</td>
</tr>
<tr>
<td>CS171</td>
<td>Project Work (Phase II)</td>
<td>-  -  -   14</td>
<td>200</td>
<td>200 400</td>
</tr>
</tbody>
</table>

**Prerequisite**
- 

**Objectives**
- To encourage and expose students for participation in National/ International paper presentation activities
- Acquire in depth working knowledge in the chosen area of problem

**Outcomes**
On successful completion of the course, the students will be able to:
- Acquire knowledge and skills needed for the construction of highly software project
- Enhance the technical presentation skills
- Inculcate the practice of publishing in Conferences and Journal

**PHASE – II**
The student is required to do the following:
1. High level Design of the Proposed Solution.
2. Detailed Design of the Proposed Solution.
3. Implementation of the Proposed Solution.
4. Comparison of the performance with the existing system

Total contact Hours: -
Total Tutorials: -
Total Practical Classes: -
Total Hours: -
SYLLABUS (Elective Subjects)
# CSE67: Internals of Operating System

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSE67</td>
<td>Internals of Operating System</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
</tbody>
</table>

**Prerequisite:**
- No prerequisites specified.

**Objectives:**
- To identify the necessity of various sub-systems in UNIX operating system.
- To analyze the mechanism of process communication and the differences in the organization of Unix and Windows operating systems.
- To design various data structures needed to develop an operating system.

**Outcomes:**
On successful completion of the course, the students will be able to:
- Explain the components in Unix and Windows operating system
- Use the system calls whenever they are necessary
- Know the storage of information of system usage and other information in Windows system and develop the algorithms to perform kernel functions

## UNIT – I
**Buffer cache and File sub-system**

- **Hours:** 09
- **Introduction to Kernel:** Architecture of the UNIX operating system, System concepts, Data structures. Buffer Cache: Buffer header, Structure of Buffer pool, Reading and writing disk blocks. Files INODES, Structure of a regular file, Directories, Super block, Inode assignment.

## UNIT – II
**System Calls and Process sub-system**

- **Hours:** 09
- **System calls:** OPEN, Read, Close, Write, Create, CHMOD, CHOWN, Pipes, Mounting and Unmounting. Process - Layout the system memory, Context, Process control, process creation, signals, Process scheduling, time, clock.

## UNIT – III
**Inter-Process Communications**

- **Hours:** 09

## UNIT – IV
**Windows System Components**

- **Hours:** 09
- **Windows Operating system:** versions, Concepts and tools, Windows internals, System Architecture, Requirements and design goals, Operating system model, Architecture overview, Key system components. System mechanisms - Trap dispatching, object manager, Synchronization, System worker threads, Windows global flags, Local procedural calls, Kernel event tracing.

## UNIT – V
**Registry and Process Management**

- **Hours:** 09
- **Windows Management Mechanisms:** The registry, Registry usage, Registry data types, Local structure, Trouble shooting Registry problems, Registry Internals, Services, Applications, Accounts, Service control Manager, Windows Management Instrumentation, Processes, Threads, and Jobs: Process Internals, Flow of create process, Thread Internals, Examining Thread creation, Thread Scheduling, Job Objects.

**Total contact Hours:** 45  
**Total Tutorials:** 15  
**Total Practical Classes:** -  
**Total Hours:** 60

**Text Books:**

**Reference Books:**

**Websites:**
### Objectives
- To understand the various threats, vulnerabilities, solutions and security standards for each layers of distributed systems
- To understand the secure software development lifecycle process for distributed systems

### Outcomes
On successful completion of the course students will be able to:
- Structure and design the distributed systems using multiple levels of security
- Have knowledge on the threats, vulnerabilities and solution at various level of distributed systems

#### UNIT – I

**Introduction:**
- Distributed Systems, Distributed Systems Security
- Security in Engineering: Secure Development Lifecycle Processes
- A Typical Security Engineering Process
- Security Engineering Guidelines and Resources

**Hours:** 09

#### UNIT – II

**Host-level Threats and Vulnerabilities:**
- Transient code Vulnerabilities
- Resident Code Vulnerabilities
- Trojan Horse
- Spyware
- Worms/Viruses
- Eavesdropping
- Job Faults
- Resource Starvation
- Overflow
- Privilege Escalation
- Injection Attacks
- Infrastructure-Level Threats and Vulnerabilities:
- Network-Level Threats and Vulnerabilities:
- Grid Computing Threats and Vulnerabilities: Storage Threats and Vulnerabilities
- Overview of Infrastructure Threats and Vulnerabilities

**Hours:** 09

#### UNIT – III

**Application-Level Threats and Vulnerabilities:**
- Application-Layer Vulnerabilities
- Injection Vulnerabilities
- Cross-Site Scripting (XSS)
- Improper Session Management
- Improper Error Handling
- Improper Use of Cryptography
- Insecure Configuration Issues
- Denial of Service
- Canonical Representation Flaws
- Overflow Issues
- Service-Level Threats and Vulnerabilities: SOA and Role of Standards
- Service-Level Security Requirements
- Service-Level Threats and Vulnerabilities
- Service-Level Attacks
- Services Threat Profile

**Hours:** 09

#### UNIT – IV

**Host-Level Solutions:**
- Sandboxing
- Virtualization
- Resource Management
- Proof-Carrying Code
- Memory Firewall
- Antimalware
- Infrastructure-Level Solutions:
- Network-Level Solutions
- Grid-Level Solutions
- Storage-Level Solutions
- Application-Level Solutions: Application-Level Security Solutions

**Hours:** 09

#### UNIT – V

**Service-Level Solutions:**
- Services Security Policy
- SOA Security Standards Stack
- Standards in Dept - Deployment Architectures for SOA Security
- Managing Service-Level Threats
- Compliance in Financial Services
- SOX Compliance
- SOX Security Solutions
- Multilevel Policy-Driven Solution Architecture
- Case Study: Grid - The Financial Application – Security Requirements Analysis
- Future Directions
- Cloud Computing Security
- Security Appliances
- User-centric Identity Management
- Identity-Based Encryption (IBE)
- Virtualization in Host Security

**Total contact Hours:** 45
**Total Tutorials:** 15
**Total Practical Classes:** -
**Total Hours:** 60

### Text Books:

### Reference Books:

### Websites:
<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSE69</td>
<td>Ethical Hacking</td>
<td>3 1 - 4</td>
<td>40</td>
<td>60 100</td>
</tr>
</tbody>
</table>

**Prerequisite**
- To immerse the students into an interactive environment where they will be shown how to scan, test, hack and secure their own systems
- To give students in-depth knowledge and practical experience with the current essential security systems
- To learn how intruders escalate privileges and what steps can be taken to secure a system

**Objectives**
On successful completion of the course, the students will be able to:
- Defend a computer against a variety of different types of security attacks using a number of hands-on techniques
- Defend a LAN against a variety of different types of security attacks using a number of hands-on techniques Practice and use safe techniques on the World Wide Web

**Outcomes**

**UNIT – I**  
**Introduction to Ethical Hacking**  
Hours: 12  

**UNIT – II**  
**Footprints**  
Hours: 12  
Introduction—Information gathering methodology—Footprinting tools—WHOIS Tool—DNS Information tool—Locating the network range—E-mail spiders—Locating network activity—Meta Search Engines.

**UNIT – III**  
**Scanning and Enumeration**  
Hours: 12  

**UNIT – IV**  
**Social Engineering**  
Hours: 12  

**UNIT – V**  
**System Hacking**  
Hours: 12  

**Text Books:**

**Reference Books:**

**Websites:**
<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSE70</td>
<td>Embedded Systems</td>
<td>L:3 T:1 P:-</td>
<td>C:4</td>
<td>CA:40 SE:60</td>
</tr>
</tbody>
</table>

**Prerequisite**
- 

**Objectives**
- To provide a clear understanding on the basic concepts, ARM processor and Architecture
- To introduce on Embedded Process development Environment
- To study on Basic of Processes and Operating systems

**Outcomes**
On successful completion of the course, the students will be able to:
- Have skills in the Embedded C Programming
- Design Embedded System with real time constraints

**UNIT – I**

**UNIT – II**

**UNIT – III**

**UNIT – IV**

**UNIT – V**

**Total contact Hours: 45**
**Total Tutorials: 15**
**Total Practical Classes: -**
**Total Hours: 60**

**Text Books:**

**Reference Books:**

**Websites:**
Department: Computer Science and Engineering  
Programme: M.Tech. (Information Security)

Semester:  
Category: TY

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSE71</td>
<td>Information Theory and Coding</td>
<td>3 L 1 T - P 4</td>
<td>CA 40</td>
<td>SE 60 TM 100</td>
</tr>
</tbody>
</table>

Prerequisite:
- To support the analysis and research on information and information system systematically and comprehensively.
- To strengthen the fundamental concepts of information theory and error control coding.

Objectives:
- On successful completion of the course, the students will be able to:
  - understand how error control coding techniques are applied in communication systems
  - analyze the information and information system

Outcomes:
- Introduction to Information theory- Uncertainty and information – average mutual information, Average self information, Average conditional self information, Measures of information-Information content of a message-
- Average information content of symbols in long independent sequences – Average information content of symbols in long dependent sequences – Markoff statistical model for information sources, Entropy and information rate of Markoff sources, Information measure for continuous random variables.

UNIT – I  
Information Theory  
Hours: 09

UNIT – II  
Channels and Channel Capacity  
Hours: 09

UNIT – III  
Source Coding  
Hours: 09

UNIT – IV  
Channel Coding - Convolution Codes  
Hours: 09

UNIT – V  
Channel Coding - Convolution Codes  
Hours: 09

Text Books:

Reference Books:

Websites:
1. http://www.nptel.ac.in
### Course Information

**Department:** Computer Science and Engineering  
**Programme:** M.Tech. (Information Security)  
**Semester:**  
**Category:** TY

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSE72</td>
<td>Digital and Cyber Forensics</td>
<td>3</td>
<td>1</td>
<td>40</td>
</tr>
</tbody>
</table>

| Prerequisite | -                                 |

| Objectives     | To introduce the fundamental concepts of computer fraud and threat concepts  
|                | To familiarize with Cyber forensics and Computer Forensics Technology  
|                | To know the concepts of Evidence Collection and Data Seizure |

| Outcomes | On successful completion of the course, students will be able to:  
|          | • Analyze digital forensics and use them to inference for security based problems  
|          | • Design the new ideas of detecting the key fraud selection process  
|          | • Design applications related to Computer Forensics techniques |

### Unit I

**Hours:** 09  

### Unit II

**Hours:** 09  
**Topics:** Key Fraud Indicator selection process customized taxonomies – Key fraud signature selection process – Accounting Forensics – Computer Forensics – Journaling and it requirements – Standardized logging criteria – Journal risk and control matrix – Neural networks – Misuse detection and Novelty detection.

### Unit III

**Hours:** 09  
**Topics:** Introduction to Cyber forensics: Computer Forensics fundamentals, Types of Computer Forensics Technology: Types of Military Computer Forensic Technology, Types of Law Enforcement: Computer Forensic Technology, Types of Business Computer Forensic Technology, Specialized Forensics Techniques, Hidden Data and How to Find It, Spyware and Adware, Encryption Methods and Vulnerabilities, Protecting Data from Being Compromised.

### Unit IV

**Hours:** 09  

### Unit V

**Hours:** 09  

**Total contact Hours:** 45  
**Total Tutorials:** 15  
**Total Practical Classes:** -  
**Total Hours:** 60

### Text Books:


### Reference Books:


### Websites:

<table>
<thead>
<tr>
<th>Department</th>
<th>Computer Science and Engineering</th>
<th>Programme</th>
<th>M.Tech. (Information Security)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Semester</td>
<td></td>
<td>Category</td>
<td>TY</td>
</tr>
<tr>
<td>Subject Code</td>
<td>Subject</td>
<td>Hours / Week</td>
<td>Credit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L</td>
<td>T</td>
</tr>
<tr>
<td>CSE73</td>
<td>Mobile Wireless Security</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

**Prerequisite**

-  

**Objectives**

- To focus security issues in the wireless networks
- To differentiate between the issues in wired and wireless networks
- To educate the students about the security vulnerabilities and counter measures.

**Outcomes**

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

- Map the mathematical models of security algorithms onto wireless and mobile environment
- Understand the specific vulnerabilities in a wide range of wireless systems
- Design robust systems against state-of-the-art security attacks

**UNIT – I**

<table>
<thead>
<tr>
<th>Hours: 09</th>
</tr>
</thead>
</table>


**UNIT – II**

<table>
<thead>
<tr>
<th>Hours: 09</th>
</tr>
</thead>
</table>


**UNIT – III**

<table>
<thead>
<tr>
<th>Hours: 09</th>
</tr>
</thead>
</table>


**UNIT – IV**

<table>
<thead>
<tr>
<th>Hours: 09</th>
</tr>
</thead>
</table>


**UNIT – V**

<table>
<thead>
<tr>
<th>Hours: 09</th>
</tr>
</thead>
</table>


**Total contact Hours: 45**  
**Total Tutorials: 15**  
**Total Practical Classes: -**  
**Total Hours: 60**

**Text Books:**


**Reference Books:**


**Websites:**

2. [http://www.netsec.ethz.ch/Publication](http://www.netsec.ethz.ch/Publication)
### Subject: Security Assessment and Verification

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSE74</td>
<td>Security Assessment and Verification</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>40</td>
<td>60</td>
</tr>
</tbody>
</table>

#### Prerequisite
- To understand the core business processes and the critical technologies that support core business processes
- To introduce the methods available to perform risk analysis to identify process-related risks and controls to mitigate those risks
- To introduce the key standards and legislations that is relevant for information security

#### Objectives
- To understand the core business processes and the critical technologies that support core business processes
- To introduce the methods available to perform risk analysis to identify process-related risks and controls to mitigate those risks
- To introduce the key standards and legislations that is relevant for information security

#### Outcomes
- On successful completion of the course, the students will be able to:
  - Gain an in-depth understanding of the process, components, skills, and experience required and other factors required for a security risk assessment process
  - Positioned to commission a security risk assessment for any organization that requires security service and address their risks in a cost-effective manner

#### UNIT – I

*Hours: 09*


#### UNIT – II

*Hours: 09*


#### UNIT – III

*Hours: 09*


#### UNIT – IV

*Hours: 09*


#### UNIT – V

*Hours: 09*


#### Text Books:

#### Reference Books:

#### Websites:
<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSE75</td>
<td>Internet Security Protocols</td>
<td>3 1 -</td>
<td>4 40</td>
<td>60 100</td>
</tr>
</tbody>
</table>

**Prerequisite**
- To introduce some of the known security problems related to the protocols and applications of the Internet
- To overview the contemporary security solutions on architectures and protocols.
- To understand concepts and terminology associated System level security.

**Objectives**
On successful completion of the course, the students will be able to:
- Develop a clear understanding of Internet security protocols
- Understand clearly MAC, IP and Transport level protocols
- Understand the general system level security

**Outcomes**

### UNIT – I  Introduction
Hours: 09
Overview of ISO OSI model and TCP/IP model, Key Management, X.509 certificates, Public-Key Infrastructure (PKI), Remote user authentication using symmetric key encryption, Kerberos, Remote user authentication using asymmetric key encryption Federated Identity management, Biometrics. Intruders, Intrusion detection, Password management, malicious software, Viruses and related threats, Virus countermeasures, Distributed denial of service attacks, Firewalls: Firewall design principles, trusted systems.

### UNIT – II  Wireless Network Security
Hours: 09

### UNIT – III  WAP Security
Hours: 09

### UNIT – IV  Electronic Mail Security
Hours: 09

### UNIT – V  Web and IP Security
Hours: 09

**Text Books:**

**Reference Books:**

**Websites:**
<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSE76</td>
<td>Network Security Essentials</td>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>60</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>

**Prerequisite**

- 

**Objectives**

- To introduce the security problems associated with malicious software and intruders
- To familiarize the network security controls that help to protect the usability, integrity, reliability and safety of the network infrastructure and the data that travels through it

**Outcomes**

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

- Identify the attacks against network infrastructure and the sources of attacks
- Identify the various types of security controls available to protect the network infrastructure
- Implement appropriate security controls to safeguard the network infrastructure

**UNIT – I Introduction**


**UNIT – II Cryptography and Key Distribution**


**UNIT – III Message Authentication and Digital Signatures**

- Requirement of Authentication Functions, Message Authentication Codes, Hash and MAC Algorithms, MD2, MD4, MD5, SHA, HMAC, CMAC, Whirlpool, Address bases authentication, password based authentication, trusted intermediaries, digital Signatures, Digital Signature Standard.

**UNIT – IV IP Security, Transport Layer Security**


**UNIT – V Network Security Applications**


**Text Books:**


**Reference Books:**


**Websites:**

### Subject Code: CSE77

**Subject:** Human Aspects in Information Security

<table>
<thead>
<tr>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>T</td>
<td>P</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>-</td>
</tr>
</tbody>
</table>

**Prerequisites:**
- To learn and understand the human aspects and socio cultural aspects of security
- To understand usable security and privacy
- To understand security from the perspective of an organization

**Objectives:**
- To learn and understand the human aspects and socio cultural aspects of security
- To understand usable security and privacy
- To understand security from the perspective of an organization

**Outcomes:**
- On successful completion of the course, the students will be able to:
  - Understand the motivations for misuse
  - Recognize the importance of user acceptance of security policies and technologies
  - Realize the need for Non-intrusive security and organizational governance for information security

#### UNIT – I Human and Psychological Aspects


#### UNIT – II Social and Cultural Aspects


#### UNIT – III Usability Issues


#### UNIT – IV Organizational Aspects


#### UNIT – V Organizational Security

- Responsibilities and Liabilities with respect to catastrophes-The complex new world of information security-Employee Surveillance based on Free Text Detection of Keystroke Dynamics-E-risk insurance product design: A Copula based Bayesian Belief Network-E-commerce Security and Honesty-credit-Towards a Scalable Role and Organization Based Access Control Model with Decentralized Security Administration-Enterprise Information System Security ; A Life-Cycle Approach.

**Total contact Hours:** 45  
**Total Tutorials:** 15  
**Total Practical Classes:** -  
**Total Hours:** 60

**Text Books:**

**Reference Books:**

**Websites:** -
<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSE78</td>
<td>Game Theory</td>
<td>3 1 - 4</td>
<td>40 60 100</td>
<td></td>
</tr>
</tbody>
</table>

Prerequisite -

Objectives
- To train students in the logic and strategic decision making involved in the theory of games.
- To learn the classification of games the course will move onto important definitions and concepts of game theory and teach students to solve strategic games between two and more agents in non-cooperative scenario.
- To analyze and solve both simultaneous-moves and sequential-moves games and will be familiarized with different solution concepts like minimax, Nash equilibrium, dominant strategy equilibrium, Subgame perfect equilibrium, etc.

Outcomes
On successful completion of the course, the students will be able to:
- Have knowledge to mixed strategy equilibria, and to repeated games
- Apply game theory in voting and bargaining
- Recognize and understand game theory in the world around them
- Apply the concepts, ideas that constitute these various game types and their solutions, and apply them to the problems at hand

UNIT – I Introduction on Game theory  
Hours: 09

UNIT – II Dynamic games of complete information  
Extensive form games – Commitment and perfection in multistage games – Strategies and Equilibria in extensive form – Backward induction and Subgame perfection – Critics of backward induction and Subgame perfection- Application of Multistage games with observed Actions – Open and closed Loop Horizons – Repeated Games.  
Hours: 09

UNIT – III Static games of Incomplete information  
Incomplete Information- The notations of Type and Strategy – Bayesian Equilibrium – Deletion of Strictly dominated strategies – Distributed Approach – Bayesian game and mechanism design: Revelation Principle – Single Agent – feasible allocation – Optimization  
Hours: 09

UNIT – IV Dynamic games of incomplete information  
Hours: 09

UNIT – V Application of game theory in Networking  
Routing game basics – Cooperation enforcement and learning using repeated games – Hierarchal routing using network function game – Auction theory – Basics of cooperation transmission – Non cooperative game for relay selection – Auction theory for resource allocation - Cooperative games for transmission  
Hours: 09

Text Books:

Reference Books:
1. Martin J. Osborne and Ariel Rubinstein, A Course in game theory, 1994

Websites:
1. https://www.coursera.org/course/gametheory
Subject Code | Subject                                | Hours / Week | Credit | Maximum Marks |
------------|----------------------------------------|--------------|--------|---------------|
            |                                        | L  T  P  C  CA  SE  TM |        |               |
CSE79       | Database Security and Auditing         | 3  1  -  4  40  60  100 |        |               |

Prerequisite:
- To understand the need to secure and audit the Databases
- To get the knowledge of different methods of securing Databases
- To know how to do auditing with Database

Objectives:
- To understand the need to secure and audit the Databases
- To get the knowledge of different methods of securing Databases
- To know how to do auditing with Database

Outcomes:
- On successful completion of the course, the students will be able to:
  - Develop the applications with secured Databases
  - Auditing the Databases

UNIT – I
Security Architecture and Operating System Security Fundamentals


UNIT – II
Administration of Users, Profiles, Password Policies, Privileges and Roles


UNIT – III
Database Application Security Models and Security Within the General Security Landscape


UNIT – IV
Auditing Categories and Auditing Database Activity


UNIT – V
Security and Auditing Case Studies


Total contact Hours: 45  Total Tutorials: 15  Total Practical Classes: -  Total Hours: 60

Text Books:

Reference Books:

Websites:
### Course Information

**Department:** Computer Science and Engineering  
**Programme:** M.Tech. (Information Security)  
**Semester:**  
**Category:** TY  
**Subject Code:** CSE80  
**Subject:** Intelligent Systems  
**Hours / Week:** 3  
**Credit:** 1  
**Maximum Marks:** 40  
**L:** 3  
**T:** 1  
**P:** -  
**C:** 4  
**CA:** 40  
**SE:** 60  
**TM:** 100

### Prerequisite
-  

### Objectives
- To provide the ideas of fuzzy sets, fuzzy logic and use of heuristics based on human experience  
- To understand different Knowledge representation schemes for typical AI problems  
- To introduce soft computing techniques and intelligent control

### Outcomes
- On successful completion of the course, students will be able to:  
  - Construct intelligent and use them for inferencing solution to real world problems  
  - Design fuzzy logic and implement the fuzzy sets and operations in fuzzy systems  
  - Analyze uses of intelligent control problems  
  - Design applications related to optimization techniques

### Unit I: Artificial Intelligence

**Hours:** 09  
Introduction, Intelligent Agents, Problem-solving: Solving Problems by Searching, Informed Search and Exploration, Constraint Satisfaction Problems, Adversarial Search

### Unit II: Knowledge and reasoning

**Hours:** 09  
Logical Agents, First-Order Logic, Inference in First-Order Logic, Knowledge Representation, Planning: Planning and Acting in the Real World, Uncertain knowledge and reasoning

### Unit III: Intelligent Modeling

**Hours:** 09  
Introduction of soft computing techniques, Fuzzy logic systems; fuzzy sets, inferencing, fuzzy relation models, Tagaki-Sugeno models, Neural networks, Neuro-fuzzy systems, Modeling of dynamical systems

### Unit IV: Optimization

**Hours:** 09  
Model building, Fuzzy inverse model development, Model-based forward optimization, Application of model-based optimization to numerical examples, Application of model-based optimization scheme to practical problems

### Unit V: Intelligent Control

**Hours:** 09  
Neural control, Rule-based fuzzy control, Model-based fuzzy control, Stability analysis, Fuzzy control for SISO nonlinear systems, Fuzzy control application to practical problems

### Total Hours
- **Total contact Hours:** 45  
- **Total Tutorials:** 15  
- **Total Practical Classes:** -  
- **Total Hours:** 60

### Text Books:

### Reference Books:

### Websites:
2. [www.ics.uci.edu/~smyth/courses/cs271/topic0_introduction.ppt](www.ics.uci.edu/~smyth/courses/cs271/topic0_introduction.ppt)  
3. [www.cs.utexas.edu/users/novak/cs381kcontents.html](www.cs.utexas.edu/users/novak/cs381kcontents.html)
<table>
<thead>
<tr>
<th>Department</th>
<th>Programme</th>
<th>Semester</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Science and Engineering</td>
<td>M.Tech. (Information Security)</td>
<td></td>
<td>TY</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSE81</td>
<td>Cloud and Big Data Security</td>
<td>3 L 1 T 4 P</td>
<td>40 CA 60 SE 100 TM</td>
<td></td>
</tr>
</tbody>
</table>

**Prerequisite**

- 

**Objectives**

- To introduce the basics of Cloud and Big data
- To explore the fundamental concepts of big data analytics
- To learn to analyze the big data using intelligent techniques

**Outcomes**

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

- Understand the basics concepts of cloud computing and its related techniques.
- Analyze the big data analytic techniques for useful business applications.
- Design efficient algorithms for mining the data from large volumes.
- Analyze the HADOOP and Map Reduce technologies associated with big data analytics

**UNIT – I**

**Security Concepts**


**UNIT – II**

**Multi-Tenancy Issues**


**UNIT – III**

**Introduction to BigData**


**UNIT – IV**

**HADOOP**


**UNIT – V**

**HADOOP Environment**


**Text Books:**


**Reference Books:**


**Websites:**
<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSE82</td>
<td>Data Hiding and Biometric Security</td>
<td>3 1 -</td>
<td>4</td>
<td>40 60 100</td>
</tr>
</tbody>
</table>

**Prerequisite**


**Objectives**

- To understand existing security methods
- To understand how biometric systems are implemented
- To understand the intricacies involved

**Outcomes**

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

- design new/existing security methods
- compare and appreciate new/existing biometric systems, hiding techniques

**UNIT – I**

**Introduction to Information hiding**


**UNIT – II**

**Steganography and Steganalysis**


**UNIT – III**

**Watermarking techniques**


**UNIT – IV**

**Biometric Security**

Introduction to Biometrics – benefits of biometrics over traditional authentication systems – benefits of biometrics in identification systems – selecting a biometric for a system – Applications – Key biometric terms and processes - biometric matching methods – Accuracy in biometric systems.

**UNIT – V**

**Physiological and Behavioral Technologies**


**Text Books:**


**Reference Books:**


**Websites:** -
<table>
<thead>
<tr>
<th>Department: Computer Science and Engineering</th>
<th>Programme: M.Tech. (Information Security)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Semester:</td>
<td>Category: TY</td>
</tr>
<tr>
<td>Subject Code</td>
<td>Subject</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>CSE83</td>
<td>Intellectual Property Rights</td>
</tr>
<tr>
<td>Prerequisite</td>
<td></td>
</tr>
<tr>
<td>Objectives</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• To understand the difference between intellectual and conventional property</td>
</tr>
<tr>
<td></td>
<td>• To learn how to value intangible assets, taking into account their commercial potential and legal status.</td>
</tr>
<tr>
<td></td>
<td>• To explore the legal and business issues surrounding marketing of new products related to technology</td>
</tr>
<tr>
<td>Outcomes</td>
<td>On successful completion of the course, the students will be able to:</td>
</tr>
<tr>
<td></td>
<td>• Apply for patents in India and Abroad</td>
</tr>
<tr>
<td></td>
<td>• Develop a business plan that advances the value of their intellectual property portfolio</td>
</tr>
<tr>
<td></td>
<td>• Develop a strategy of marketing their intellectual property and understand some negotiation basics.</td>
</tr>
<tr>
<td></td>
<td>• Explain some of the limits of their intellectual property rights and comprehend some basic legal pitfalls</td>
</tr>
</tbody>
</table>

**UNIT – I**


**UNIT – II**

**Copy right:** Copyright and its uses - Subject matter of copyright- Artistic, Literary, musical and cinematographic works-Definition-History-International Copyright Treaties- Internet treaties-Amendments in Indian Copyright Law and their significance-Protection of Software and digital innovations-Rights afforded by copyright law; Rights of Distribution and Communication to the Public-Exceptions in copyright- Plagiarism vs Copyright Infringement- Dr.Mashelkar Committee Report and Kaavya Vishwanathan Case;-Case Studies-Practical aspects of Copyright Registration and Transfer - Procedural and practical aspects related to registration of copyright – Forms, Fee, Timeline- Ownership issues, transfer and duration. Enforcement at National and Global level-Remedies available under the Copyright Act-Forms for copy rights

Design registration: Industrial Design Registration and its usefulness in Engineering – Importance of industrial design registration for engineers-Indian Law related to Registration of Industrial Designs-Essential Requirements for Registration of a Design in India- Limitations-American Law- International Agreements- The Hague System; Conflicts related to Registration of Design, Copyright or Trademark; Legal rights and advantages of Industrial Design Registration- The Tupperware Case-Practical aspects of Industrial Design Registration in India and Abroad - Practical aspects of Industrial Design Registration in India-Forms, Fee, Timelines. Procedural aspects. Enforcement at National and Global level. Guide and forms for registering the design

**UNIT – III**

Trade Secrets and trademarks: Trade Secrets- Importance – Trade Secrets- Importance Elements of Trade Secrets-
UNIT – IV


UNIT – V

Digital Products and Law: Digital Innovations and Developments as Knowledge Assets – Significance of IP in Content for the Internet and Tech Sector- Symbols and trademarks as Business Assets in the Information Age; Internet and the WWW; Applications of computer technology - advantages/disadvantages-Cyber Technology- e-commerce and e-governance; Electronic records and digital signatures; The Employment Relationship in the Internet and Tech Sector - role of CDAs and contracts-Trolls, landmines and other metaphors-Cyber etiquette. IP Laws, Cyber laws and Digital Content Protection - IP laws and Cyberlaws- Linkages; IPR issues vs Regulatory issues-E-commerce and Cyber Laws- Cyber Crime and Legislation- Need, Objective and Scope; UNCITRAL model law –Objectives- its relevance to India; Objects of the IT Act, 2000; Information Technology and Information Security-Case studies.

Total contact Hours: 45
Total Tutorials: 15
Total Practical Classes: -
Total Hours: 60

Text Books:

Reference Books:

Websites:
1. http://www.ipindia.nic.in/
2. www.uspto.gov/
Department: Computer Science and Engineering  
Programme: M.Tech. (Information Security)  

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSE84</td>
<td>Information Security Policies</td>
<td>3</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>

**Prerequisite:** -  

**Objectives:**  
- To Introduce and understand the Information Security Policies with aspects of security  
- To understand how to write the Security Policies  
- To understand how to establish Viruses Protection in an organization

**Outcomes:** On successful completion of the course, the students will be able to:  
- Maintain the Policies in an organization.  
- Have skill to write the Security Policies for an organization.  
- Asses the Viruses and suggest Protection mechanism for organization

**UNIT – I**  
Hours: 09

**UNIT – II**  
Hours: 09

**UNIT – III**  
Hours: 09

**UNIT – IV**  
Hours: 09

**UNIT – V**  
Hours: 09

Total contact Hours: 45  
Total Tutorials: 15  
Total Practical Classes: -  
Total Hours: 60

**Text Books:**  

**Reference Books:**  

**Websites:**  
1. http://www.sans.org/security-resources/policies/
4. www.csoonline.com/article/495017
<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSE85</td>
<td>Secure Coding</td>
<td>3 1</td>
<td>4</td>
<td>40 60 100</td>
</tr>
</tbody>
</table>

**Prerequisite**
- None

**Objectives**
- To introduce basic concepts, policies, and mechanisms in designing and coding secure software systems
- To examine the concepts that apply to programming "in the large" as well as specifics on things like buffer overflow
- To deal with C and C++ code for secure software system development

**Outcomes**
On successful completion of the course, the students will be able to:
- Analyze the essential techniques for secure coding which are used in current practice
- Apply and analyze techniques for secure coding used in current practice
- Evaluate the use of type-safe languages, certifying compilers, proof-carrying code, run-time monitoring, and stack inspection,
- Analyze legal and ethical issues underlying secure coding of software systems

**UNIT – I**
**Introduction:** Software security- Security concepts-Security policy-security flaws-vulnerabilities-exploits-mitigation-

**UNIT – II**
**Pointer Subterfuge:** Data Locations-Function Pointers-Data Pointers-Modifying the Instruction Pointer-Global Offset Table-The .dtors Section-Virtual Pointers-atexit(), on-exit(), longjmp()-Exception Handling-Mitigation Strategies. Dynamic Memory Management: Common Dynamic Memory Management Errors-Doug Lea's Memory Allocator-RtlHeap Mitigation Strategies.

**UNIT – III**

**UNIT – IV**

**UNIT – V**

**Text Books:**

**Reference Books:**

**Websites:** -
**Department**: Computer Science and Engineering  
**Programme**: M.Tech. (Information Security)  

<table>
<thead>
<tr>
<th>Subject Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credit</th>
<th>Maximum Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>L  T  P  C  CA  SE  TM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSE86</td>
<td>Web Application Security</td>
<td>3  1  -  4  40  60  100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Prerequisite**:  

**Objectives**:  
- To identify various components of an web application from the security view point  
- To have knowledge of web application testing methodologies  

**Outcomes**:  
On successful completion of the course, the students will be able to:  
- Design secured web application  
- Build web testing tools  

**UNIT – I**  
**Hours: 09**  

**UNIT – II**  
**Hours: 09**  
Browser security principles - cross-site scripting - cross-site request forgery - Database security principles - SQL injection - setting database permission - stored procedure security - Insecure Direct object references.  

**UNIT – III**  
**Hours: 09**  
File security principles - source code secret - forceful browsing - directory traversal - secure development methodologies - application security - industry standard secure development methodologies and maturity models - SDL - CLASP - SAMM - BSIMM.  

**UNIT – IV**  
**Hours: 09**  
Web Applications Testing Fundamentals, Basic Observation HTML Page Source, Web-Oriented Data Encoding, Tampering with Input, Automated Bulk Scanning, Automating Specific Tasks with cURL.  

**UNIT – V**  
**Hours: 09**  
Automating with LibWWWPerl, Seeking Design Flaws, Attacking AJAX, Manipulating Sessions, Multifaceted Tests.  

**Total contact Hours: 45**  
**Total Tutorials: 15**  
**Total Practical Classes: -**  
**Total Hours: 60**  

**Text Books**:  

**Reference Books**:  

**Websites**:  
1. https://www.owasp.org/