AICTE Mandatory Disclosures

Information of Infrastructure and Other Resources Available
- Number of Class Rooms and size of each : 1 (80 Sqm)
- Number of Tutorial rooms and size of each : 1 (83 Sqm)
- Number of Laboratories and size of each : 1 (83 Sqm)
- Number of Drawing Halls with capacity of each : 1 (136) Sqm
- Number of Computer Centres with capacity of each : 1 (83 Sqm)
- Barrier Free Built Environment for disabled and elderly persons : Available (Certified by competent authority)
- Occupancy Certificate : Available (Certified by competent authority)
- Fire and Safety Certificate : Available (Certified by competent authority)

Library
- Number of Library books/ Titles/ Journals available (program-wise) : 2209
- List of online National/ International Journals subscribed : 15
- E- Library facilities : Available

Computing Facilities
- Internet Bandwidth : 1Gbps
- Number and configuration of System : 30
- Total number of system connected by LAN : 30
- Total number of system connected by WAN : 30
- Major software packages available : MsOffice, Matlab, R, Python, Wireshark

List of facilities available
- Games and Sports Facilities
  - Table Tennis
  - Carroms
  - Chess
- Extra-Curricular Activities
- Soft Skill Development Facilities : Yes

M.Tech Information Security:
- Title of the Course : M.Tech. Information Security (With specialization in Cyber Security)
- Curricula and Syllabi : Given Below
- Laboratory facilities exclusive to the Post Graduate Course : 1 Lab (20PCs) + 2 Research Labs

Enrollment of students in the last 3 years

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Students Enrolled</td>
<td>13</td>
<td>14</td>
<td>16</td>
<td>8</td>
</tr>
</tbody>
</table>

Teaching Learning Process
Vision Statement:
To disseminate advances made in the Disciplines of Mathematics, Statistics and Computer Science.
To conduct, Promote, Carry out research and advanced study in Mathematics, Statistics and Computer Science

Mission Statements:
To work in the cutting edge areas of Mathematics, Statistics and Computer Science and vigorously pursue their application in making our lives better.

MS-1: To conduct Courses, Conferences, Seminars, Colloquia, Workshops and undertake related activities in the disciplines of Mathematics, Statistics and Computer Science for Human Resource Development.

MS-2: To conduct, promote and carry out research and advanced study in Mathematics, Statistics and Computer Science and to disseminate the advances made in these trinity of areas.
C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: M.Tech (Information Security)

Program Educational Objectives (PEOs)

PEO-1: To provide students with strong foundational concepts in Computer Science and Mathematics to understand the advances in Cyber space.

PEO-2: To enable students for innovative products and solutions.

PEO-3: To inculcate students a constant learning practice pace with changing landscape of technologies.

PEO-4: To nurture talent for designing and developing cyber security applications

PEO-5: To impart critical analysis thought in information security domain.

Mapping Program Educational Objectives (PEOs) with Mission Statements (MS)

<table>
<thead>
<tr>
<th></th>
<th>MS-1</th>
<th>MS-2</th>
<th>MS-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>PEO-1</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>PEO-2</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>PEO-3</td>
<td>2</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>PEO-4</td>
<td>3</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>PEO-5</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: M.Tech (Information Security)

Program Outcomes (POs)

PO-1: To enable students with latest technology trends in cyber world
PO-2: To provide wider understanding of information technology
PO-3: In-depth understanding of core system technologies in the security point of view
PO-4: To provide students with solid foundation in various cyberattack methods
PO-5: To prepare students to excel in analyze the information security threats and the network traffic
PO-6: To prepare students for bringing out new solutions in cyber security

Program Specific Outcomes (PSOs)

PSO-1: In-depth understanding of cryptography and security tools implementation
PSO-2: To inculcate students with ability to analyze new security requirements and development of new tools
PSO-3: To train students with good in cybersecurity so as to comprehend, analyze, design and create secure computing solutions for the real life problems.
Mapping of Program Outcomes (POs) and Program Specific Outcomes (PSOs) with Program Educational Objectives (PEOs)

<table>
<thead>
<tr>
<th></th>
<th>PEO-1</th>
<th>PEO-2</th>
<th>PEO-3</th>
<th>PEO-4</th>
<th>PEO-5</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO-1</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>PO-2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>PO-3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>PO-4</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>PO-5</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>PO-6</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>PSO-1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>PSO-2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>PSO-3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Mapping of Program Specific Outcomes (PSOs) where applicable.

Write ‘3’ in the box for ‘high-level’ mapping, 2 for ‘Medium-level’ mapping, 1 for ‘Low-level’ mapping.
# M.Tech (Information Security) Scheme

## Semester I

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS401</td>
<td>Mathematical Foundation for Information Security</td>
<td>4-0-0</td>
</tr>
<tr>
<td>IS402</td>
<td>Secure Operating System and Computer Organization</td>
<td>3-1-0</td>
</tr>
<tr>
<td>IS403</td>
<td>Laboratory: Reverse Engineering and Malware Analysis</td>
<td>1-0-2</td>
</tr>
<tr>
<td>CS425</td>
<td>Cryptography</td>
<td>4-0-0</td>
</tr>
<tr>
<td></td>
<td>Elective – 1.1</td>
<td>3/4</td>
</tr>
<tr>
<td></td>
<td>Elective – 1.2</td>
<td>3/4</td>
</tr>
<tr>
<td><strong>Credits</strong></td>
<td><strong>Min:22/Max:24</strong></td>
<td><strong>22/24</strong></td>
</tr>
</tbody>
</table>

## Semester II

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS476</td>
<td>Advanced Computer Networks</td>
<td>4-0-0</td>
</tr>
<tr>
<td>IS451</td>
<td>Security Tools and Technologies</td>
<td>3-1-0</td>
</tr>
<tr>
<td>IS452</td>
<td>Ethical Hacking &amp; Computer Forensics</td>
<td>3-1-0</td>
</tr>
<tr>
<td>IS453</td>
<td>Laboratory: Cyber Security</td>
<td>1-0-2</td>
</tr>
<tr>
<td></td>
<td>Elective - 2.1</td>
<td>3/4</td>
</tr>
<tr>
<td></td>
<td>Elective - 2.2</td>
<td>3/4</td>
</tr>
<tr>
<td><strong>Credits</strong></td>
<td><strong>Min:22/Max:24</strong></td>
<td><strong>22/24</strong></td>
</tr>
</tbody>
</table>

## Semester III-IV

<table>
<thead>
<tr>
<th>Course Name</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISSERTATION</td>
<td>18</td>
</tr>
<tr>
<td><strong>Credits</strong></td>
<td><strong>Min, Max:18</strong></td>
</tr>
</tbody>
</table>

Grand Total Credits = 62 (Min) / 64 (Max)

<table>
<thead>
<tr>
<th>Electives</th>
<th>Semester I</th>
<th>Semester II</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Information Security</td>
<td>CS426 BlockChain Technology</td>
<td>AI473 Machine Learning</td>
</tr>
<tr>
<td></td>
<td>IS423 Coding Theory and Information Theory</td>
<td>IS472 Statistics and Probability</td>
</tr>
<tr>
<td></td>
<td>IS422 Big Data Security</td>
<td>IS471 Information System Control and Audit</td>
</tr>
</tbody>
</table>
Name of the Academic Program: M.Tech (Information Security) (M.Tech-1)

Course Code: IS401  
Title of the Course: Mathematical Foundation for Information Security  
L-T-P : 4-0-0  
Credits : 4

Prerequisite Course / Knowledge (If any): Permutations and combinations, number system

Course Outcomes (COs)

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

- CO-1: Develop problem solving techniques needed to calculate probabilities and number theory (Evaluate).
- CO-2: Apply Euler’s Phi Function and concept of Prime Numbers to information security algorithms (Apply).
- CO-3: Apply concepts of power modulo in the real time application of security (Apply).
- CO-4: Explain the concept of Quadratic Reciprocity (Understand).
- CO-5: Apply the concepts of Elliptic Curves in secure communication (Apply).

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

<table>
<thead>
<tr>
<th></th>
<th>PO1</th>
<th>PO2</th>
<th>PO3</th>
<th>PO4</th>
<th>PO5</th>
<th>PO6</th>
<th>PSO1</th>
<th>PSO2</th>
<th>PSO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>CO2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>CO3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>CO4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>CO5</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>CO6</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
Detailed Syllabus:

UNIT-I - Probability and Basics of Number Theory
Basic asymptotic complexity and order notation (big-O), random number generation, Elementary discrete probability. Introduction to Number Theory, Pythagorean Triples and the UNIT Circle, Sums of Higher Powers and Fermat's Last Theorem, Divisibility and the Greatest Common Divisor, Linear Equations and the Greatest Common Divisor,

UNIT-II - More on Number Theory
Factorization and the Fundamental Theorem of Arithmetic, Congruence: Powers, and Fermat's Little Theorem, Powers, and Euler's Formula, Euler's Phi Function, Prime Numbers: Counting Primes, Mersenne Primes and Perfect Numbers,

UNIT-III - Power modulo
Powers Modulo m and Successive Squaring, Computing k'th Roots Modulo m, Powers, Roots, and "Unbreakable" Codes, Euler's Phi Function and Sums of Divisors, Powers Modulo p and Primitive Roots, Primitive Roots and Indices,

UNIT-IV - Quadratic Reciprocity
Squares Modulo p, Quadratic Reciprocity, Which Primes Are Sums of Two Squares? Which Numbers Are Sums of Two Squares? The Equation $X^4+Y^4=Z^4$, Pell's Equation, Diophantine Approximation and Pell's Equation,

UNIT-V - Elliptic Curves
Cubic Curves and Elliptic Curves, Elliptic Curves with Few Rational Points, Points on Elliptic Curves modulo p, Defect Bounds and Modularity Patterns, Elliptic Curves and Fermat's Last Theorem

Reference Books

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: M.Tech (Information Security) (M.Tech-I)

Course Code: IS402  Title of the Course: Secure Operating System and Computer Organization
L-T-P: 3-0-1  Credits  4
Prerequisite Course / Knowledge (If any): components of Computers and Operating Systems

Course Outcomes (COs)

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

- CO-1: Explain the computer organization and I/O operations of computer. (Understand)
- CO-2: Demonstrate the representation of data at the machine level. (Apply)
- CO-3: Categorize the security requirements of Operating System. (Analyze)
- CO-4: Assess the OS protection principles. (Evaluate)
- CO-5: Appraise the Trusted Operating System concepts (Evaluate)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

<table>
<thead>
<tr>
<th></th>
<th>PO1</th>
<th>PO2</th>
<th>PO3</th>
<th>PO4</th>
<th>PO5</th>
<th>PO6</th>
<th>PSO1</th>
<th>PSO2</th>
<th>PSO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO1</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>CO2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>CO3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>CO4</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>CO5</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>
Detailed Syllabus


UNIT – II: Memory Organization: Memory Hierarchy, Main Memory, Auxiliary Memory, Associate Memory, Cache Memory. Pipeline and Vector Processing: Parallel Processing, Pipelining, Arithmetic Pipeline, Instruction Pipeline, RISC Pipeline, Vector Processing, Array Processors.


References Books:

Course Code: IS421 Title of the Course: Current trends in Web Security
L-T-P: 3-0-0 Credits 3
Prerequisite Course / Knowledge (If any): Basics of Operating System and Web Technology.

Course Outcomes (COs)

After completion of this course successfully, the students will be able to

- CO-1: Evaluate various cyber security threats of the internet (Evaluate)
- CO-2: Compare and Contrast appropriate Intrusion Detection Mechanism (Analyze)
- CO-3: Appraise about the various cryptographic techniques used in Internet (Analyze)
- CO-4: Compare and Contrast different attacks in the web –Trojans, worms and virus(Analyze)
- CO-5: Design and develop of Firewalls for enhanced web security (Create)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

<table>
<thead>
<tr>
<th>CO</th>
<th>PO1</th>
<th>PO2</th>
<th>PO3</th>
<th>PO4</th>
<th>PO5</th>
<th>PO6</th>
<th>PSO1</th>
<th>PSO2</th>
<th>PSO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO1</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>CO2</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>CO3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>CO4</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>CO5</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
Detailed Syllabus:

UNIT I

UNIT II

UNIT III
Theory of Cryptography, Simple ciphers, Symmetric cryptography, stream ciphers, Block ciphers, Public key cryptography, Ciphers with public key, Cryptographic Hash functions, Different hash algorithms, Digital signatures.

UNIT IV
Trojans and Backdoors, Viruses and Worms: Sniffers, Phishing, Web Application Security- Secured authentication mechanism, secured session management, Cross-site Scripting, SQL Injection and other vulnerabilities Denial-of Service Attacks, Session Hijacking, Spoofing v Hijacking, TCP/IP hijacking, CAPTCHA Protection

UNIT V

REFERENCE BOOKS:

Name of the Academic Program: M.Tech (Information Security) (MTECH-I)

Course Code: IS403
Title of the Course: Reverse Engineering and Malware Analysis Lab
L-T-P: 1-0-2
Credits: 3

Prerequisite Course / Knowledge (If any): Basics of Operating System and Web Technology.

Course Outcomes (COs)

After completion of this course successfully, the students will be able to

CO-1: Categorize and Identify appropriate Open Source tools for reverse engineering (Analyze).

CO-2: Analyze the commonly used file formats using reverse engineering tools (Analyze)

CO-3: Explain how the malware works, identified, detected and eliminated for the computer. (Understand)

CO-4: Evaluate & assess various malware threats. (Evaluate).

CO-5: Appraise about the various malware attacking techniques (Analyze)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

<table>
<thead>
<tr>
<th></th>
<th>PO1</th>
<th>PO2</th>
<th>PO3</th>
<th>PO4</th>
<th>PO5</th>
<th>PO6</th>
<th>PSO1</th>
<th>PSO2</th>
<th>PSO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO1</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>CO2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>CO3</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>CO4</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>CO5</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
Detailed Syllabus:

<table>
<thead>
<tr>
<th>Week</th>
<th>Task</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction to reverse engineering, tools (gdb) to extract assembly code</td>
<td>understanding the essence of the reverse engineering, tools required.</td>
</tr>
<tr>
<td>2</td>
<td>Recognizing main function’s stack frame, variables, memory allocation, branching (if-else)</td>
<td>understanding the memory dump of runnable programs.</td>
</tr>
<tr>
<td>3</td>
<td>Recognizing loops (while, for, do while), dynamic/static initialization of variables</td>
<td>understanding how different loop constructs work in assembly level.</td>
</tr>
<tr>
<td>4</td>
<td>Recognizing function calls, nested function calls (inbuilt/user defined), recursion</td>
<td>understanding memory dump during function calls.</td>
</tr>
<tr>
<td>5</td>
<td>Introduction to malware analysis, virtual box set up (windows_xp, remnux)</td>
<td>understanding the essence of malware analysis, tools required.</td>
</tr>
<tr>
<td>6</td>
<td>Exploring the different tools available in the v-box set up</td>
<td>understanding the usability of tools.</td>
</tr>
<tr>
<td>7</td>
<td>Dynamic analysis of malwares (srvcp.exe) making use of different tools (wireshark, etc)</td>
<td>detecting the malware by making use of tools.</td>
</tr>
<tr>
<td>8</td>
<td>Introduction to buffer over flow attack, understanding memory dump with the help of tools</td>
<td>understanding concept of buffer, buffer overflow vulnerability.</td>
</tr>
<tr>
<td>9</td>
<td>Demo of buffer over flow exploit</td>
<td>understanding how we can access the sudo power by making use of buffer overflow vulnerability.</td>
</tr>
<tr>
<td>10</td>
<td>Demo of pdf analysis, tools</td>
<td>understanding the header metadata of pdf, injecting malware (keylogger) into pdf, detecting embedded scripts in the pdf.</td>
</tr>
</tbody>
</table>

Suggested reading:

C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: M.Tech (Information Security) (MTECH-I)

Course Code: IS422
Title of the Course: Big Data Security L-
T-P : 4-0-0
Credits 4

Prerequisite Course / Knowledge (If any): Basic understanding of distributed computing, networking.

Course Outcome (COs)

After completion of this course successfully, the students will be able to...

- CO-1: Describe the challenges of securing distributed systems (Understanding)
- CO-2: Discuss cryptographic protocols required for secure big data communication process. (Understanding)
- CO-3: Examine the complexity and security measures for Cryptographically enforced systems (Analyze)
- CO-4: Design a secure Hadoop and Spark Cluster using the best practices. (Create)
- CO-5: Practice network security and operating systems security principles in real world domains. (Apply)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

<table>
<thead>
<tr>
<th>CO</th>
<th>PO1</th>
<th>PO2</th>
<th>PO3</th>
<th>PO4</th>
<th>PO5</th>
<th>PO6</th>
<th>PSO1</th>
<th>PSO2</th>
<th>PSO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>CO2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>CO3</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>CO4</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>CO5</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
Detailed Syllabus:

UNIT – I
Definitions of Big data, Sources of Big data, Types of data, Big data Challenges, Big Data applications - Detecting Fraud, Anti-Money Laundering, Terrorism.

UNIT – II

UNIT – III
Cryptographically enforced secure access control mechanisms, Cryptographic protocols required for secure big data communication process, complexity and security measures

UNIT – IV
Secure Computational Platforms for Big data analytics, Hadoop overview, Hadoop ecosystem, Architecture, HDFS Storage, Map-Reduce distributed Processing, example data sets, Spark Overview, Hadoop vs Spark, Introduction to HPC, HPC cluster components

UNIT – V
Data Protection, Encryption Algorithms, Encrypting Data at Rest, Encryption and Key Management, HDFS Data-at-Rest Encryption, MapReduce Intermediate Data Encryption, Filesystem Encryption

References Books:
C R Rao Institute of Advanced Mathematics, Statistics & Computer Science

Name of the Academic Program: M.Tech (Information Security) (MTECH-I)

Course Code: IS423                Title of the Course: Coding Theory and Information Theory
T-P: 4-0-0                     Credits 4

Pre-requisite Course: Basic understanding of coding

Course Outcome (COs)

After completion of this course successfully, the students will be able to

- CO-1: Analyze the robustness of coding techniques. (Analyze)
- CO-2: Describe the error correcting codes (Understanding)
- CO-3: Apply error correcting codes. (Apply)
- CO-4: Discuss various convolution encoding techniques. (Understanding)
- CO-5: Apply randomized network coding application of network coding. (Apply)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

<table>
<thead>
<tr>
<th></th>
<th>PO1</th>
<th>PO2</th>
<th>PO3</th>
<th>PO4</th>
<th>PO5</th>
<th>PO6</th>
<th>PSO1</th>
<th>PSO2</th>
<th>PSO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>13</td>
<td>2</td>
</tr>
<tr>
<td>CO2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>22</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>CO3</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>CO4</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>CO5</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
**Detailed Syllabus:**

UNIT – I
Information Theory: Entropy, its characterization and related properties, Huffman codes, Shannon-Fano coding, robustness of coding techniques, Information measure-noiseless coding, discrete memoryless channel – channel capacity, fundamental theorem of information theory.

UNIT – II
Coding Theory: Error correcting codes, minimum distance principles, Hamming bound, general binary code, group code, and linear group code.

UNIT – III
Convolution encoding: algebraic structure, Gilbert bound. Threshold decoding: threshold decoding for block codes. Cyclic binary codes: BCH codes, generalized BCH code and decoding, optimum codes, concepts of non-cyclic codes.

UNIT – IV

UNIT – V

**Suggested Reading:**

M.Tech (Information Security)

II-Semester
Name of the Academic Program: M.Tech (Information Security) (MTECH-II)

Course Code: IS451 Title of the Course: Security Tool and Technologies
L-T-P: 4-0-0 Credits 4

Pre-requisite Course: Basic understanding of coding

Course Outcome (COs)

After completion of this course successfully, the students will be able to

- CO-1: Design of Access Control and Authentication mechanisms for security (Create)
- CO-2: Appraise the perimeter security fundamentals (Evaluate)
- CO-3: Assemble the router security to set it up as a security device (Create)
- CO-4: Describe PKI security protocols and Digital Certificate (Understand)
- CO-5: Assess host hardening for various attacks. (Evaluate)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

<table>
<thead>
<tr>
<th>CO</th>
<th>PO1</th>
<th>PO2</th>
<th>PO3</th>
<th>PO4</th>
<th>PO5</th>
<th>PO6</th>
<th>PSO1</th>
<th>PSO2</th>
<th>PSO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>13</td>
<td>2</td>
</tr>
<tr>
<td>CO2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>CO3</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>CO4</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>CO5</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
Detailed Syllabus:

UNIT I
Securing Information Using Authentication and Access Control: introduction to Access Control, Implementing an Authentication Strategy, Implementing an Access Control Strategy, Cryptography, PKI: Introduction to Certificates, Introduction to Public Key Infrastructure, Deploying and Managing Certificates

UNIT II

UNIT III
Proxy firewalls: Proxy or application gateway firewalls, Protocol issues for proxies, Security policy, Router as a security device, Router hardening

UNIT IV
Network Intrusion Detection: The roles of network IDS in a perimeter defence, IDS sensor placement, Virtual Private Networks: Advantages and Disadvantages of VPNs, IPSec basics, Other VPN, protocols PPTP & L2TP

UNIT V
Security protocols & Implementations: SSL/TLS, SSH, PGP, SHTTP, IPSec, Open SSL, Host hardening: Against local attacks, against network attacks, against application attacks, Antivirus solutions and deployment, Software updates and patches.

Reference books:


Name of the Academic Program: **M.Tech (Information Security) (MTECH-II)**

Course Code: IS452 

Title of the Course: Ethical Hacking & Computer Forensics

L-T-P: 3-0-0 

Credits 3

**Pre-requisite Course:** Programming Methodology, Operating Systems, DBMS, Computer Networks, Information Security

**Course Outcome (COs)**

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

CO-1: Explain the concepts of Ethical Hacking (Understand)
CO-2: Explain the types of Hackers and their roles in IT industry (Understand)
CO-3: Write Batch programming for hacking (Create)
CO-4: Set up hacking environment using virtualization platform by creating virtual machine to simulate hacking (Create)
CO-5: Describe password cracking techniques and various tools (Understand)
CO-6: Explain the concepts of Packet sniffing, Email spoofing, DNS cache poisoning, Proxies/VPN, google dorks, Steganography, DDoS attacks, etc. (Understand)
CO-7: Describe the phases in computer forensics (Understand)
CO-8: Discuss the file system concepts used in Windows and Linux (Understand)
CO-9: Review various digital forensic tools for Seizure, Acquire and Analysis (Understand)
CO-10: Design and develop given tasks on Ethical Hacking / Computer forensics (Create)

**Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)**

<table>
<thead>
<tr>
<th>CO1</th>
<th>CO2</th>
<th>CO3</th>
<th>CO4</th>
<th>CO5</th>
<th>CO6</th>
<th>CO7</th>
<th>CO8</th>
<th>CO9</th>
<th>CO10</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>PO2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>PO3</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>PO4</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>PO5</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>PO6</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>PSO1</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>PSO2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>PSO3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>
Detailed Syllabus:

UNIT-I: Introduction: Aims and Objectives, Technology involved and current issues in the IT industry, glimpse of information security, Ethical Hacking and Computer forensics.


UNIT-IV: Introduction to Packet sniffing (WireShark, TCPDump, NetworkMiner, etc.), Keyloggers (keyghost/kidlogger, form grabbing), Email spoofing, DNS cache poisoning, Proxies/VPN (cyber ghost VPN), google dorks, Steganography (Invisible secrets, S tools), etc.


UNIT-VI: Introduction to file systems. File structural details of how files get created and deleted at system level (for file systems: FAT, NTFS, Ext2/Ext3). Exploring computer forensic tools: TrueBack, CyberCheck, FTKImager, DFF (digital forensic framework), TSK (The sleuth Kit), Volatility framework, etc.

Text Books:

Reference Books:
Name of the Academic Program: M.Tech (Information Security) (MTECH-II)

Course Code: IS453

Title of the Course: Cyber Security Lab

L-T-P: 1-0-2

Credits 3

Pre-requisite Course: Basics of Operating Systems and Web Technology

Course Outcome (COs)

After completion of this course successfully, the students will be able to

- CO-1: Evaluate and assess the various cyber security threats (Evaluate)
- CO-2: Categorize and identify appropriate Open Source tools for CS (Analyze)
- CO-3: Appraise about the various attacking techniques used in the Internet (Analyze)
- CO-4: Compare and Contrast different attacks in the web (Analyze)
- CO-5: Evaluate the web site vulnerabilities using scanning tools (Evaluate)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

<table>
<thead>
<tr>
<th></th>
<th>PO1</th>
<th>PO2</th>
<th>PO3</th>
<th>PO4</th>
<th>PO5</th>
<th>PO6</th>
<th>PSO1</th>
<th>PSO2</th>
<th>PSO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO1</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>CO2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>CO3</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>CO4</td>
<td>2</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>CO5</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
## Detailed Syllabus:

<table>
<thead>
<tr>
<th>Week</th>
<th>Name of the Experiment</th>
<th>Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab-1</td>
<td>Install 2 VMs with different OSs and establish communication between two hosts and remote access of either host</td>
<td>To understand the installation and remote access procedure of the VM</td>
</tr>
<tr>
<td>Lab-2</td>
<td>Using Burp Suite tool to scan local website and make a report of all vulnerabilities.</td>
<td>To understand the functioning of the scanning tool and site vulnerabilities thereof.</td>
</tr>
<tr>
<td>Lab-3</td>
<td>TCP scanning using NMAP</td>
<td>To understand the functioning of network ports.</td>
</tr>
<tr>
<td>Lab-4</td>
<td>TCP / UDP connectivity using Netcat</td>
<td>To understand the connectivity in the network.</td>
</tr>
<tr>
<td>Lab-5</td>
<td>Network vulnerability using OpenVAS</td>
<td>To understand the network related.</td>
</tr>
<tr>
<td>Lab-6</td>
<td>Web application testing using DVWA</td>
<td>To understand the processes of securing web applications</td>
</tr>
<tr>
<td>Lab-7</td>
<td>Manual SQL injection using DVWA</td>
<td>To understand and execute malicious SQL statements that control a web application's database server.</td>
</tr>
<tr>
<td>Lab-8</td>
<td>XSS using DVWA</td>
<td>To understand XSS statements and their effect on web application.</td>
</tr>
</tbody>
</table>

### Suggested Readings

Name of the Academic Program: M.Tech (Information Security) (M.Tech-II)

Course Code: IS471  
Title of the Course: Information System Control and Audit  
L-T-P: 3-1-0  
Credits 4

Pre-requisite Course: Information Systems

Course Outcome (COs)

After completion of this course successfully, the students will be able to

- CO-1: Describe the Control and Audit process. (Understand)
- CO-2: Demonstrate the Information Systems Audit. (Apply)
- CO-3: Evaluate the planning and leading function of IS Audit (Evaluate)
- CO-4: Assess the Application Control Framework. (Evaluate)
- CO-5: Evaluate asset Safeguarding and Data Integrity. (Evaluate)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

<table>
<thead>
<tr>
<th></th>
<th>PO1</th>
<th>PO2</th>
<th>PO3</th>
<th>PO4</th>
<th>PO5</th>
<th>PO6</th>
<th>PSO1</th>
<th>PSO2</th>
<th>PSO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO1</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>CO2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>CO3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>CO4</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>CO5</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>
Detailed Syllabus

UNIT- I

UNIT - II

UNIT-III
The Application Control Framework-I: Boundary Controls, Input Controls, Communication Controls. The Application Control Framework-II: Processing Controls, Database Controls, output Controls.

UNIT - IV

UNIT -V

References Books:

3. Jalote : Software Project Management in Practice, Pearson Education
4. Royce : Software Project Management, Pearson Education.
Name of the Academic Program: M.Tech (Information Security) (MTECH-II)

Course Code: IS472  
Title of the Course: Statistics & Probability

L-T-P: 3-0-0  
Credits 3

Pre-requisite Course: Prior knowledge of the counting aspects of discrete mathematics is desirable including permutations and combinations

Course Outcome (COs)

After completion of this course successfully, the students will be able to

- CO-1: Describe the process of data collection and its analysis (Understanding)
- CO-2: Evaluate moments, kurtosis and skewness (Evaluate)
- CO-3: Apply correlation and regression to data analysis (Apply)
- CO-4: Apply the results of distributions and sampling distribution to the given data
- CO-5: Test a given hypothesis (Analyze)

Mapping of Course Outcomes (COs) with Program Outcomes (POs) and Program Specific Outcomes (PSOs)

<table>
<thead>
<tr>
<th>PO1</th>
<th>PO2</th>
<th>PO3</th>
<th>PO4</th>
<th>PO5</th>
<th>PO6</th>
<th>PSO1</th>
<th>PSO2</th>
<th>PSO3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>CO2</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>CO3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>CO4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>CO5</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>
Detailed Syllabus:

Unit I:
Data analysis and its Phases: Stating and refining the question, Exploring the data, Building formal statistical models, interpreting the results, communicating the results. Dimensionality reduction and its importance in data analysis.

Unit II:
Measures of Central Tendency: Arithmetic mean, Median, Quartiles, Deciles, Percentiles, the mode, geometric mean. Measures of dispersion: the range, quartile deviation, mean deviation, coefficient of mean deviation, standard deviation, variance, coefficient of variation. Moments, moments about the mean, Skewness, Kurtosis.

Unit III:
Correlation and Regression: correlation, degree of correlation, causation of correlation, simple and multiple linear regression, Karl-Pearson’s coefficient of correlation, multiple correlation analysis.

Unit IV:
Probability, A priori probability, conditional probabilities, Baye’s theorem, random variables, expectations, probability distributions: binomial, normal, Poisson distribution, random sampling, sampling distributions

Unit V:
Estimation and Testing of Hypothesis: estimation and confidence level, standard error estimation, statistical inferences and testing of hypothesis.

Reference Books
Academic Time Table with the name of the Faculty members handling the Course

M.Tech Information Security (Sem-1)

Tentative Time Table (Nov-2021)

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Faculty</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS401</td>
<td>Mathematical Foundation for Information Security (MFIS)</td>
<td>Dr. G. Padmavathi (C R Rao AIMSCS)</td>
</tr>
<tr>
<td>IS402</td>
<td>Secure Operating System and Computer Organization (SOS)</td>
<td>Dr. Sirisha V (C R Rao AIMSCS)</td>
</tr>
<tr>
<td>CS425</td>
<td>Cryptography</td>
<td>Dr. Y. V. Subba Rao (SCIS)</td>
</tr>
<tr>
<td>IS453</td>
<td>Laboratory: Reverse Engineering and Malware Analysis (RE)</td>
<td>Dr. Appala Naidu/Dr. Barnali Gupta (C R Rao AIMSCS)</td>
</tr>
</tbody>
</table>

Electives

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Faculty</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS426</td>
<td>BlockChain Technology (BCT)</td>
<td>Dr. N. Rukma Rekha (SCIS)</td>
</tr>
<tr>
<td>IS421</td>
<td>Current trends in Web Security (CTWS)</td>
<td>Dr. Pradeepthi K. V. (C R Rao AIMSCS)</td>
</tr>
</tbody>
</table>

- Internal Continuous Evaluation System in place: Yes
- Student’s assessment of Faculty, System in place: Yes