GANDHI INSTITUTE OF TECHNOLOGY AND MANAGEMENT (GITAM)
(Deemed to be University) (Estd. u/s 3 of the UGC Act, 1956)
VISAKHAPATNAM ★ HYDERABAD ★ BENGALURU
NAAC accredited with ‘A+’ Grade

REGULATIONS AND SYLLABUS of
Master of Technology in
Cyber Forensics and Information Security
(w.e.f 2017-18 admitted batch)

GITAM Committed to Excellence
VISION
To become a global leader in higher education.

MISSION
To impart futuristic and comprehensive education of global standards with a high sense of discipline and social relevance in a serene and invigorating environment.
REGULATIONS & SYLLABUS
OF
M.Tech. (Cyber Forensics and Information Security)
(w.e.f 2017-18 admitted batch)

GITAM Committed to Excellence
M.Tech. in Cyber Forensics and Information Security
REGULATIONS
(w.e.f. 2017-18 admitted batch)

1. ADMISSION
1.1 Admission into M.Tech. in CFIS program of GITAM is governed by GITAM admission regulations.

2. ELIGIBILITY CRITERIA
2.1 • First class or equivalent grade in the qualifying examination from recognized university with a minimum of 60% aggregate marks and rank obtained in GAT (PGT).
• B.E./B.Tech./AMIE in CSE / IT / ECE / EEE / EI / CSIT or its equivalent.

2.2 Admissions into M.Tech. will be based on the following:
   (i) Score obtained in GAT (PG), if conducted.
   (ii) Performance in Qualifying Examination / Interview.

2.3 The actual weightage to be given to the above items will be decided by the authorities before the commencement of the academic year. Candidates with valid GATE score shall be exempted from appearing for GAT (PG).

3. CHOICE BASED CREDIT SYSTEM
3.1 Choice Based Credit System (CBCS) is introduced with effect from the admitted Batch of 2015-16 based on UGC guidelines in order to promote:
   • Student Centered Learning
   • Cafeteria approach
   • Students to learn courses of their choice
   • Learning at their own pace
   • Inter-disciplinary learning

3.2 Learning goals/ objectives and outcomes are specified leading to what a student should be able to do at the end of the program.

4. STRUCTURE OF THE PROGRAM
4.1 The Program Consists of
   i) Core Courses (compulsory) which give general exposure to a Student in CFIS and subject related area.
   ii) Programme Electives.
   iii) Interdisciplinary Electives.
4.2 Each course is assigned a certain number of credits depending upon the number of contact hours (lectures/tutorials/practical) per week.

4.3 In general, credits are assigned to the courses based on the following contact hours per week per semester:
   - One credit for each Lecture / Tutorial hour per week.
   - One credit for two hours of Practicals per week.
   - Two credits for three (or more) hours of Practicals per week.

5. MEDIUM OF INSTRUCTION
The medium of instruction (including examinations and project reports) shall be English.

6. REGISTRATION
Every student has to register himself/herself for each semester individually at the time specified by the Institute / University.

7. ATTENDANCE REQUIREMENTS
7.1 A student whose attendance is less than 75% in all the courses put together in any semester will not be permitted to attend the end-semester examination and he/she will not be allowed to register for subsequent semester of study. He/she has to repeat the semester along with his / her juniors.

7.2 However, the Vice Chancellor on the recommendation of the Principal / Director of the Institute/School may condone the shortage of attendance to the students whose attendance is between 66% and 74% on genuine grounds and on payment of prescribed fee.

8. EVALUATION
8.1 The assessment of the student’s performance in a Theory course shall be based on two components: Continuous Evaluation (40 marks) and Semester-end examination (60 marks).

8.2 A student has to secure an aggregate of 40% in the course in the two components put together to be declared to have passed the course, subject to the condition that the candidate must have secured a minimum of 24 marks (i.e. 40%) in the theory component at the semester-end examination.

8.3 Practical/ Project Work/ Industrial Training/ Viva voce/ Seminar etc. course are completely assessed under Continuous Evaluation for a maximum of 100 marks, and a student has to obtain a minimum of 40% to secure Pass Grade. Details of Assessment Procedure are furnished below in Table 1.
### Table 1: Assessment Procedure

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Component of Assessment</th>
<th>Marks Allotted</th>
<th>Type of Assessment</th>
<th>Scheme of Evaluation</th>
</tr>
</thead>
</table>
| 1     | Theory                  | 40             | Continuous         | i) Thirty (30) marks for mid Semester examinations. Three mid examinations shall be conducted for 15 marks each; performance in best two shall be taken into consideration.  
                            |               |                 | ii) Ten (10) marks for Quizzes, Assignments and Presentations.  
                            |               |                 | Sixty (60) marks for Semester-end examinations |
|       |                         | 60             | Semester-end       |                      |
|       |                         |                | Evaluation         |                      |
|       |                         |                |                    |                      |
|       |                         |                |                    |                      |
|       |                         |                |                    |                      |
|       |                         |                |                    |                      |
| Total |                         | 100            |                    |                      |
| 2     | Practicals              | 100            | Continuous         | i) Fifty (50) marks for regularity and performance, records and oral presentations in the laboratory. Weightage for each component shall be announced at the beginning of the Semester.  
                            |               |                 | ii) Ten (10) marks for case studies.  
                            |               |                 | iii) Forty (40) marks for two tests of 20 marks each (one at the mid-term and the other towards the end of the Semester) conducted by the concerned lab Teacher. |
| 3     | Project work (III Semester ) | 100           | Continuous         | i) Forty (40) marks for periodic evaluation on originality, innovation, sincerity and progress of the work, assessed by the Project Supervisor.  
                            |               |                 | ii) Thirty (30) marks for mid-term evaluation for defending the Project, before a panel of examiners.  
                            |               |                 | iii) Thirty (30) marks for final Report presentation and Viva-voce, by a panel of examiners |
| 4     | Project work (IV Semester) | 50            | Continuous         | i) Twenty (20) marks for Periodic evaluation on originality innovation, sincerity and progress of the work, assessed by the Project Supervisor.  
<pre><code>                        |               |                 | ii) Fifteen (15) marks for mid-term evaluation for defending the Project, before a panel of examiners*. |
</code></pre>
<table>
<thead>
<tr>
<th>5</th>
<th>Technical Seminar</th>
<th>100</th>
<th>Continuous Evaluation</th>
<th>iii) Fifteen (15) marks for interim Report presentation and Viva-voce. Fifty (50) marks for final Report presentation and Viva-voce assessed by external examiners.</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Comprehensive Viva-voce (II Semester)</td>
<td>100</td>
<td>Continuous Evaluation</td>
<td>Through five periodic Viva-voce exams for 20 marks each, conducted by a panel of examiners. The course content for Viva exams shall be announced at the beginning of the Semester.</td>
</tr>
</tbody>
</table>

*Panel of Examiners shall be appointed by the concerned Head of the Department*

9. **REAPPEARANCE**

9.1 A student who has secured ‘F’ grade in a Theory course shall have to reappear at the subsequent Semester end examination held for that course.

9.2 A student who has secured ‘F’ grade in a Practical course shall have to attend Special Instruction Classes held during summer.

9.3 A student who has secured ‘F’ Grade in Project work / Industrial Training etc shall have to improve his/her report and reappear for Viva – voce at the time of Special Examination to be conducted in the summer vacation.

10. **SPECIAL EXAMINATION**

10.1 A student who has completed his/her period of study and still has “F” grade in a maximum of three theory courses is eligible to appear for Special Examination normally held during summer vacation.

11. **BETTERMENT OF GRADES**

A student who has secured only a Pass or Second class and desires to improve his/her Class can appear for Betterment Examinations only in Theory courses of any Semester of his/her choice, conducted in Summer Vacation along with the Special Examinations. Betterment of Grades is permitted ‘only once’ immediately after completion of the program of study.
12. GRADING SYSTEM

12.1 Based on the student performance during a given semester, a final letter grade will be awarded at the end of the semester in each course. The letter grades and the corresponding grade points are as given in Table 2.

<table>
<thead>
<tr>
<th>Sl.No.</th>
<th>Grade</th>
<th>Grade Points</th>
<th>Absolute Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>O (outstanding)</td>
<td>10</td>
<td>90 and above</td>
</tr>
<tr>
<td>2</td>
<td>A+ (Excellent)</td>
<td>9</td>
<td>80 to 89</td>
</tr>
<tr>
<td>3</td>
<td>A (Very Good)</td>
<td>8</td>
<td>70 to 79</td>
</tr>
<tr>
<td>4</td>
<td>B+ (Good)</td>
<td>7</td>
<td>60 to 69</td>
</tr>
<tr>
<td>5</td>
<td>B (Above Average)</td>
<td>6</td>
<td>50 to 59</td>
</tr>
<tr>
<td>6</td>
<td>C (Average)</td>
<td>5</td>
<td>45 to 49</td>
</tr>
<tr>
<td>7</td>
<td>P (Pass)</td>
<td>4</td>
<td>40 to 44</td>
</tr>
<tr>
<td>8</td>
<td>F (Fail)</td>
<td>0</td>
<td>Less than 40</td>
</tr>
<tr>
<td>9</td>
<td>Ab. (Absent)</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>

12.2 A student who earns a minimum of 4 grade points (P grade) in a course is declared to have successfully completed the course, and is deemed to have earned the credits assigned to that course, subject to securing a GPA of 5 for a Pass in the semester.

13. GRADE POINT AVERAGE

13.1 A Grade Point Average (GPA) for the semester will be calculated according to the formula:

\[
GPA = \frac{\sum_i C_i G_i}{\sum_i G_i}
\]

Where
- \( C_i \) = number of credits obtained for the ith course
- \( G_i \) = number of credits obtained for the ith course

13.2 To arrive at Cumulative Grade Point Average (CGPA), a similar formula is used considering the student’s performance in all the courses taken, in all the semesters up to the particular point of time.

13.3 CGPA required for classification of class after the successful completion of the program is shown in Table 3.
Table 3: CGPA required for award of Class

<table>
<thead>
<tr>
<th>Class</th>
<th>CGPA Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Class with Distinction</td>
<td>&gt; 8.0*</td>
</tr>
<tr>
<td>First Class</td>
<td>&gt; 6.5</td>
</tr>
<tr>
<td>Second Class</td>
<td>&gt; 5.5</td>
</tr>
<tr>
<td>Pass Class</td>
<td>&gt; 5.0</td>
</tr>
</tbody>
</table>

* In addition to the required CGPA of 8.0 or more, the student must have necessarily passed all the courses of every semester in first attempt.

14. ELIGIBILITY FOR AWARD OF THE M.Tech. DEGREE

14.1 Duration of the program: A student is ordinarily expected to complete the M.Tech. program in four semesters of two years. However a student may complete the program in not more than four years including study period.

14.2 However the above regulation may be relaxed by the Vice Chancellor in individual cases for cogent and sufficient reasons.

14.3 A student shall be eligible for award of the M.Tech. Degree if he / she fulfills all the following conditions.

a) Registered and successfully completed all the courses and projects.

b) Successfully acquired the minimum required credits as specified in the curriculum corresponding to the branch of his/her study within the stipulated time.

c) Has no dues to the Institute, hostels, Libraries, NCC / NSS etc, and

d) No disciplinary action is pending against him / her.

15. DISCRETIONARY POWER

Not withstanding anything contained in the above sections, the Vice Chancellor may review all exceptional cases, and give his decision, which will be final and binding.
M.Tech.in Cyber Forensics and Information Security (CFIS)
Department of Computer Science and Engineering
Effective from academic year 2017-2018 admitted batch

**Semester I**

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Course Code</th>
<th>Course Title</th>
<th>Category</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ECS701</td>
<td>Advanced Data Structures &amp; Algorithms</td>
<td>CE</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>ECS703</td>
<td>Advanced Operating Systems</td>
<td>CE</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>ECS709</td>
<td>Number Theory &amp; Cryptography</td>
<td>CE</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>ECS7XX</td>
<td>Program Elective-I</td>
<td>PE(PE)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>ECS7XX</td>
<td>Program Elective-II</td>
<td>PE(PE)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>ECS7XX/ EID7XX</td>
<td>Interdisciplinary Elective-I</td>
<td>IDE</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>ECS721</td>
<td>Advanced Data Structures &amp; Algorithms Lab</td>
<td>CE</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>ECS727</td>
<td>Network Security &amp; Cryptography Lab</td>
<td>CE</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

**Semester II**

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Course Code</th>
<th>Course Title</th>
<th>Category</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ECS702</td>
<td>Advanced Computer Networks</td>
<td>CE</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>ECS710</td>
<td>Cyber Forensics</td>
<td>CE</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>ECS712</td>
<td>Pragmatics of Information Security</td>
<td>CE</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>ECS7XX</td>
<td>Program Elective -III</td>
<td>PE(PE)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>ECS7XX</td>
<td>Program Elective -IV</td>
<td>PE(PE)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>EID7XX/ ECS7XX</td>
<td>Interdisciplinary Elective-II</td>
<td>IDE</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>ECS728</td>
<td>Cyber Forensics Lab</td>
<td>CE</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>ECS730</td>
<td>IOT Security Lab</td>
<td>CE</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>9</td>
<td>ECS792</td>
<td>Technical Seminar</td>
<td>CE</td>
<td>0</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>
### Semester III

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Course Code</th>
<th>Course Title</th>
<th>Category</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ECS891</td>
<td>Project Work-I</td>
<td>PP(PW)</td>
<td></td>
<td></td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>2</td>
<td>ECS893</td>
<td>Comprehensive Viva Voce</td>
<td>CE</td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
</tbody>
</table>

### Semester IV

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Course Code</th>
<th>Course Title</th>
<th>Category</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ECS892</td>
<td>Project work-II</td>
<td>PP(PW)</td>
<td></td>
<td></td>
<td></td>
<td>14</td>
</tr>
</tbody>
</table>

### Number of Credits:

<table>
<thead>
<tr>
<th>Semester</th>
<th>I</th>
<th>II</th>
<th>III</th>
<th>IV</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credits</td>
<td>25</td>
<td>27</td>
<td>10</td>
<td>14</td>
<td>76</td>
</tr>
</tbody>
</table>

### Interdisciplinary Elective - I

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Course Code</th>
<th>Course Title</th>
<th>Category</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ECS749</td>
<td>Internet of Things</td>
<td>IDE</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>EID763</td>
<td>Multivariate Techniques for Data Analysis</td>
<td>IDE</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>EID769</td>
<td>Cyber Laws and IT Protection</td>
<td>IDE</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

### Interdisciplinary Elective - II

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Course Code</th>
<th>Course Title</th>
<th>Category</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ECS751</td>
<td>Service Oriented Architecture</td>
<td>IDE</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>EID760</td>
<td>Programming with R</td>
<td>IDE</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>EID771</td>
<td>Enterprise Cyber Security</td>
<td>IDE</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>
### PROGRAMME ELECTIVES

#### Programme Elective-I

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Course Code</th>
<th>Course Title</th>
<th>Category</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ECS763</td>
<td>Ethical Hacking</td>
<td>PE(PE)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>ECS765</td>
<td>Introduction to Machine Learning</td>
<td>PE(PE)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>ECS767</td>
<td>Steganography</td>
<td>PE(PE)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

#### Programme Elective-II

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Course Code</th>
<th>Course Title</th>
<th>Category</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ECS769</td>
<td>Secure Systems Engineering</td>
<td>PE(PE)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>ECS771</td>
<td>Web Applications Security</td>
<td>PE(PE)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>ECS773</td>
<td>Operating Systems Security</td>
<td>PE(PE)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

#### Programme Elective-III

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Course Code</th>
<th>Course Title</th>
<th>Category</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ECS764</td>
<td>Advanced Cryptography</td>
<td>PE(PE)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>ECS766</td>
<td>Forensic Psychology</td>
<td>PE(PE)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>ECS768</td>
<td>Mobile Device Forensics</td>
<td>PE(PE)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

#### Programme Elective-IV

<table>
<thead>
<tr>
<th>S. No.</th>
<th>Course Code</th>
<th>Course Title</th>
<th>Category</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ECS770</td>
<td>Computer Forensics and Investigations</td>
<td>PE(PE)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>ECS772</td>
<td>Biometric Security</td>
<td>PE(PE)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>ECS774</td>
<td>Cloud Computing and Security</td>
<td>PE(PE)</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>
ECS701: ADVANCED DATA STRUCTURES AND ALGORITHMS

L  T  P  C
4  0  0  4

Module I
12hrs

Module II
10hrs
Introduction to Graphs, Graph Traversal. Introduction to Trees and Tree Traversals, Binary Search Trees, AVL Trees, B-Trees, Priority Queues.

Module III
10hrs

Module IV
10hrs
Dynamic Programming: General Method, Matrix Chain Multiplication, Longest Common Subsequence, Reliability Design, Traveling Sales Person Problem. Back Tracking: General Method, 8 Queens Problem, Hamiltonian Cycle, Graph Coloring Problem.

Module V
10hrs
Text Book(s)
2. Sartaj Sahni, Data Structures, Algorithms and Applications in C++, 2/e, Universities Press.

References

Web Resources
http://www.personal.kent.edu/~rmuhamma/Algorithms/algorithm.html
Module I 10 hrs

Module II 10 hrs
Direct Link Networks - Reliable Transmission - Stop-and-Wait, Sliding Window, Concurrent Logical Channels; Ethernet (802.3) - Physical Properties, Access Protocol, Experience with Ethernet; Rings - Token Ring Media Access Control, Token Ring Maintenance, FDDI, Resilient Packet Ring (802.17); Wireless - Bluetooth (802.15.1), Wi-Fi (802.11), WiMAX (802.16), Cell Phone Technologies; Sensor Networks; Packet Switching - Switching and Forwarding, Datagrams, Virtual Circuit Switching, Source Routing; Bridges and LAN Switches - Learning Bridges, Spanning Tree Algorithm, Broadcast and Multicast, Limitations of Bridges.

Module III 10 hrs
Internetworking - Simple Internetworking (IP) - What Is an Internetwork? Service Model, Global Addresses, Datagram Forwarding in IP, Address Translation (ARP), Host Configuration (DHCP), Error Reporting (ICMP), Virtual Networks and Tunnels; Routing - Network as a Graph, Distance Vector (RIP), Link State (OSPF), Metrics, Routing for Mobile Hosts; Subnetting - Classless Routing (CIDR), Inter-domain Routing (BGP), Routing Areas, IP Version 6 (IPv6); Multiprotocol Label Switching - Destination-Based Forwarding, Explicit Routing, Virtual Private Networks and Tunnels ; Deployment of IPv6.

Module IV 12 hrs
End-to-End Protocols - Simple Demultiplexer (UDP); Reliable Byte Stream (TCP) - End-to-End Issues, Segment Format, Connection Establishment and Termination, Sliding Window Revisited, Triggering Transmission,

Module V 10 hrs
Applications - Traditional Applications - Electronic Mail (SMTP, MIME, IMAP), World Wide Web (HTTP), Name Service (DNS), Network Management (SNMP); Web Services - Custom Application Protocols (WSDL, SOAP), A Generic Application Protocol (REST), Multimedia Applications, Session Control and Call Control (SDP, SIP, H.323), Resource Allocation for Multimedia Applications; Overlay Networks - Routing Overlays, Peer-to-Peer Networks (Gnutella, BitTorrent), Content Distribution Networks.

Text Books
1. Larry L. Peterson, Bruce S. Davie, Computer Networks, A Systems Approach, 4/e, Morgan Kaufmann.
2. D. Bertsekas, R. Gallager, Data Networks, PHI.

References
2. J. Walrand, P. Varaiya, High Performance Communication Networks, Morgan Kaufmann
6. Darren L Spohn, Data Network Design, TMH.
Module I 11 hrs

Module II 11 hrs

Module III 10 hrs

Module IV 10 hrs
Module V 10 hrs

Text Book

References
Module I 9 hrs
Topics in elementary number theory: O and Θ notations, time estimates for doing arithmetic, divisibility and the Euclidean algorithm. Congruence's: Definitions and properties, linear congruencies, residue classes, Euler's phi function, Fermat's Little Theorem, Chinese Remainder Theorem, Applications to factoring, finite fields, quadratic residues and Reciprocity: Quadratic residues, Legendre symbol, Jacobi symbol.

Module II 9 hrs
Simple Cryptosystems: Enciphering Matrices - Block ciphers Principles - Data Encryption Standard (DES) - The Strength of DES- Differential & Linear Crypt analysis-Block Cipher Design principles.

Module III 10 hrs

Module IV 9 hrs
Primality and Factoring: Pseudo primes, the rho (?) method, Form factorization and factor bases, the continued fraction method, the quadratic sieve method.

Module V 9 hrs
Number Theory and Algebraic Geometry: Elliptic curves, basic facts, elliptic curve cryptosystems, elliptic curve primality test - elliptic curve factorization.
Text Book(s)

References
ECS710: CYBER FORENSICS

L T P C
4 0 0 4

Module I

Module II

Module III

Module IV
Introduction to Cyber Crime Investigation, Investigation Tools, ediscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, Email Recovery, Hands on Case Studies, Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.

Module V
Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC, Electronic Communication Privacy ACT, Legal Policies.
Text Book(s)

References
Module I 10 hrs

Module II 10 hrs

Module III 10 hrs

Module IV 10 hrs

Module V 10 hrs

Text Book

References
1. Program to perform insertion, deletion and search operations on the following:
2. Develop programs to demonstrate at least 3 applications of Stacks.
3. Develop a program to demonstrate the concept of double ended queue.
4. Program to represent a graph by using Adjacency Matrix and Adjacency List representation for the given set of Vertices and Edges. Traverse it by using Breadth First Search and Depth First Search Techniques.
5. Develop a program to perform insertion, deletion and search operations on the following Trees
   a. Binary Search Tree b. AVL Tree
6. Develop programs for
   a) Heap Sort  b) Merge Sort  c) Quick sort by taking random element as pivot  d) Selection
7. Implement the code for the following problems by using Greedy Method:
   a. Finding Minimum Cost Spanning Tree by using Kruskal's Algorithm.
   b. Single Source Shortest Path Problem.
8. Implement the code for the following problems using Dynamic Programming:
   a. Matrix Chain Multiplication Problem.
   b. String Editing.
   c. Traveling Salesman Problem
9. Implement code for the following problems by using Back-Tracking:
   a. Hamiltonian Cycle b. 8 Queens Problem
10. Implement code for Traveling Salesperson Problem by using Least-Cost Branch-and-Bound
The following programs should be implemented preferably on platform Windows/Unix using C language (for 1-5) and other standard utilities available with UNIX systems (for 6-15):-

1. Implement the encryption and decryption of 8-bit data using Simplified DES Algorithm (created by Prof. Edward Schaefer) in C
2. Write a program to break the above DES coding
3. Implement Linear Congruential Algorithm to generate 5 pseudo-random numbers in C
4. Implement Rabin-Miller Primality Testing Algorithm in C
5. Implement the Euclid Algorithm to generate the GCD of an array of 10 integers in C
6. a) Implement RSA algorithm for encryption and decryption in C
    b) In an RSA System, the public key of a given user is e=31,n=3599. Write a program to find private key of the User.
7. Configure a mail agent to support Digital Certificates, send a mail and verify the correctness of this system using the configured parameters.
8. Configure SSH (Secure Shell) and send/receive a file on this connection to verify the correctness of this system using the configured parameters.
10. Implement encryption and decryption with openssl.
11. Implement Using IP TABLES on Linux and setting the filtering rules.
12. Implementation of proxy based security protocols in C or C++ with features like confidentiality, integrity and authentication
The following exercises have to be performed using various software tools/ utilities mentioned: Software Tools:
1. CyberCheck 4.0 - Academic Version
2. CyberCheckSuite
3. MobileCheck
4. Network Session Analyser
5. Win-LiFT
6. TrueImager
7. TrueTraveller
8. PhotoExaminer Ver 1.1
9. CDRAnalyzer

Forensics Exercises:
I) Disk Forensics:
1. Identify digital evidences
2. Acquire the evidence
3. Authenticate the evidence
4. Preserve the evidence
5. Analyze the evidence
6. Report the findings

II) Network Forensics:
• Intrusion detection
• Logging (the best way to track down a hacker is to keep vast records of activity on a network with the help of an intrusion detection system)
• Correlating intrusion detection and logging

III) Device Forensics
1. PDA
2. Mobile phone
3. Digital Music
4. Printer Forensics
5. Scanner Forensics
Arduino
1) Programming the Arduino to make the LED Blink using delay.
2) Integration of analog/digital sensors/components with Arduino and Programming

<table>
<thead>
<tr>
<th>Analog Sensor</th>
<th>Digital Sensor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gas Sensor (MQ2) - Analog</td>
<td>PIR Sensor</td>
</tr>
<tr>
<td>Temperature Sensor (LM35)</td>
<td>IR Sensor</td>
</tr>
<tr>
<td>LDR Sensor</td>
<td>DC/Gear/Stepper Motor</td>
</tr>
</tbody>
</table>

3) Serial Communication in Arduino with Wireless Module and Programming
   • Bluetooth (HC-05)
   • ZigBee (TI -CC2500)

Raspberry Pi
1) Programming the Raspberry Pi to make the LED Blink using Python.
2) Integration of sensors/components with Raspberry Pi and Programming
   • LED
   • PIR Sensor
   • Ultra-Sonic Sensor (HC-SR04)
   • DC/Gear/Stepper Motor (using Motor Drivers)
3) Serial Communication Between Arduino and Raspberry Pi using Universal Serial Bus (USB)

Security
1. Program to generate Hash of given data using Hash Algorithms (MD5, SHA1, SHA256)
2. Program to Encrypt and Decrypt given data using RSA and AES Algorithms
3. Program to Obfuscate a given data using python
Arduino - Security
1. Implementing Hash Algorithms (MD5, SHA1, SHA256) in Arduino using Hash Functions.
2. Implementing RES and AES Algorithms in Arduino using Arduino Cryptographic Library.
3. Using Hash and Cryptographic Algorithms to secure the Sensor Data in Arduino

Raspberry Pi - Security
1. Implementing Hash Algorithms (MD5, SHA1, SHA256) in Raspberry Pi
2. Implementing RES and AES Algorithms in Raspberry Pi using Cryptographic Algorithms
3. Using Hash and Cryptographic Algorithms to secure the Sensor Data in Raspberry Pi

Arduino - Raspberry Pi - Security
1. Implementing Hash and Cryptographic Algorithms to secure data between 2 Arduino using ZigBee/Bluetooth
2. Implementing Hash and Cryptographic Algorithms to secure data between Serial Communication of Arduino and Raspberry Pi

Implementing the Obfuscation techniques to secure Arduino and Raspberry Pi Programming
ECS749: INTERNET OF THINGS

Module I 10 hrs
Introduction: The Internet of Things, An Overview, the flavour of the internet of things, the internet of things, the technology of the internet of things, enchanted objects, who is making the internet of things, Design principles for connected devices: Calm and ambient technology, magicas metaphor, privacy, web thinking for connected devices, affordances.

Module II 10 hrs
Internet Principles: Internet communications, An overview (IP, TCP, the IP protocol suite (TCP/IP), UDP), IP addresses (DNS, Static IP Address assignment, dynamic IP address assignment, IPv6), MAC addresses, TCP and UDP ports, application layer protocols.

Module III 10 hrs
Prototyping: Thinking About Prototyping: Sketching, familiarity, costs versus ease of prototyping, prototypes and production, open source versus closed source, tapping into the community. Prototyping embedded devices: Electronics, embedded computing basics, developing on the arduino, raspberry pi, beaglebone black, electric imp, mobile phone and tablets, plug computing, always on internet of things.

Module IV 10 hrs
Prototyping the Physical Design: Preparation, sketch, iterate and explore, non digital methods, laser cutting, 3D printing, CNC milling, repurposing/recycling. Techniques for Writing Embedded Code: Memory management, performance and battery life, libraries, debugging.

Module V 10 hrs
Prototype to Reality: Business Models, A short history of business models, the business model canvas, models, funding an internet of things startup, lean startups. Moving to manufacture: Designing kits, designing printed circuit boards, manufacturing printed circuit boards, mass producing the case and other fixtures, certification, costs, scaling up software.
**Text Book**
1. Adrian McEwen, Hakim Cassimally, Designing the Internet of Things, 1/e, Wiley publication, 2013

**References**
1. Charalampos Doukas, Building Internet of Things with the Arduino, Create space, 2002.
ECS751: SERVICE ORIENTED ARCHITECTURE

L T P C
3 0 0 3

Module I 8 hrs
Fundamentals of SOA: Introduction, defining SOA, evolution of SOA, service oriented enterprise, comparing SOA to client server and distributed internet architectures, basic SOA architecture concepts, key service characteristics, technical benefits, business benefits.

Module II 10 hrs
Combining SOA and Web Services: Web services, service descriptions, messaging with SOAP, message exchange patterns, web service platform, service contract, service level data model, service discovery, service level security, service level interaction patterns, atomic and composite services, service enabling legacy system, enterprise service bus pattern.

Module III 10 hrs
Multi Channel Access and Web Services Composition: SOA for multi-channel access, business benefits, tiers, business process management, web service composition, BPEL, RESTFUL services, comparison of BPEL and RESTFUL services.

Module IV 10 hrs
Java Web Services: SOA support in J2EE, Java API for XML based web services (JAX,WS), Java architecture for XML binding (JAXB), Java API for XML registries (JAXR), Java API for XML based RPC (JAX,RPC), web services interoperability, SOA support in .NET, ASP.NET web services, case studies, web services enhancements (WSE).

Module V 8 hrs
Web Services Security and Transaction: Meta datamanagement, advanced messaging, addressing, reliable messaging, policies, WS-policy, security, WS-security, notification and eventing, transaction management.
Text Book(s)

References
Module I 10 hrs

Module II 10 hrs
Securing permission: Securing file and folder permission, Using the encrypting file system, Securing registry permissions. Securing service: Managing service permission, Default services in windows 2000 and windows XP. Unix: The Quest for Root, Remote Access vs Local access, Remote access, Local access., After hacking root.

Module III 10 hrs
Dial-up, PBX, Voicemail and VPN hacking, Preparing to dial up, War-Dialing, Brute-Force Scripting PBX hacking, Voice mail hacking, VPN hacking, Network Devices: Discovery Autonomous System Lookup, Public Newsgroups, Service Detection, Network Vulnerability, Detecting Layer 2 Media.

Module IV 10 hrs

Module V 10 hrs
Remote Control Insecurities, Discovering Remote Control Software, Connection, Weakness.VNC, Microsoft Terminal Server and Citrix ICA, Advanced Techniques Session Hijacking, Back Doors, Trojans, Cryptography, Subverting the systems Environment, Social Engineering, Web Hacking, Web server hacking web application hacking, Hacking the internet Use, Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global countermeasures to Internet User Hacking.
Text Book(s)

References
2. Rafay Baloch, A Beginners Guide to Ethical Hacking.
ECS764: ADVANCED CRYPTOGRAPHY

<table>
<thead>
<tr>
<th>Module I</th>
<th>10 hrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>OSI security architecture: Classical encryption techniques, Cipher principles, Data encryption standard, Block cipher design principles and modes of operation, Evaluation criteria for AES, AES cipher, Triple DES, Placement of encryption function, Traffic confidentiality.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module II</th>
<th>10 hrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key management: Diffie Hellman key exchange, Elliptic curve architecture and cryptography, Introduction to number theory, Confidentiality using symmetric encryption, Public key cryptography and RSA.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module III</th>
<th>10 hrs</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Module IV</th>
<th>10 hrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantum Cryptography and Quantum Teleportation: Heisenberg uncertainty principle, polarization states of photons, quantum cryptography using polarized photons, local vs. non local interactions, entanglements, EPR paradox, Bell's theorem, Bell basis, teleportation of a single qubit theory and experiments.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module V</th>
<th>10 hrs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Future trends: Review of recent experimental achievements, study on technological feasibility of a quantum computer candidate physical systems and limitations imposed by noise.</td>
<td></td>
</tr>
</tbody>
</table>
Text Book(s)

References
ECS765: INTRODUCTION TO MACHINE LEARNING

<table>
<thead>
<tr>
<th></th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

**Module I**

10 hrs
Introduction: overview of machine learning, related areas, applications, parametric regression: linear regression, polynomial regression, locally weighted regression, numerical optimization, gradient descent, kernel methods.

**Module II**

10 hrs

**Module III**

9 hrs
Neural Networks And Genetic Algorithms: Neural network representation, problems, perceptions, multilayer networks and back propagation algorithms, advanced topics, Genetic algorithms, hypothesis space search, genetic programming, models of evaluation and learning.

**Module IV**

9 hrs
Bayesian and Computational Learning: Bayes theorem, concept learning, maximum likelihood, minimum description length principle, Bayes optimal classifier, Gibbs Algorithm, Naïve Bayes Classifier, Bayesian belief network, EM algorithm, probability learning, sample complexity, finite and infinite hypothesis spaces, mistake bound model
Instance Based Learning: K-Nearest neighbor learning, locally weighted regression, radial basis functions, case based learning.

**Module V**

9 hrs
Hidden Markov Models: Introduction, discrete Markov processes, hidden Markov models, three basic problems of HMMs evaluation problem, finding the state sequence, learning model parameters, continuous observations, the HMM with input, model selection in HMM.
Text Book(s)

References
Module I 10 hrs
Historical roots: Modern major perspectives of psychology, distinguishing professional and pseudo-psychology, types of psychological professionals. The science and research methods, professional ethics of research, research challenges.

Module II 10 hrs
The biology underlying behavior: Nerves and neurons, structure and functions of neurons, neurotransmitters, Central Nervous System, peripheral nervous system. The human brain: its structure and function, sensory system and endocrine system, Stages of sleep, REM sleep, sleep disturbances, States of consciousness, altered states of consciousness, attention and awareness, sensation of perception, problems in attention and perception.

Module III 10 hrs

Module IV 10 hrs

Module V 10 hrs
Personality: Theories-Psychoanalytic approaches to personality, Trait approaches, learning approaches, biological approaches, and humanistic approaches. Assessing personality: Self report measures of personality, projective methods and behavioral assessment.
Text Book

References
1. Study Guide for Psychology: from science to practice by Baron, R.A. & Kolsher MJ
2. Forensic Psychology by Christopher Cronin
3. Introduction to Psychology by Dennis Coon
4. Introduction to forensic psychology: Research and Application, 3rd edition (paperback) by Curt R Bartol, Anne M Bartol
**ECS767: STEGANOGRAPHY**

<table>
<thead>
<tr>
<th>L</th>
<th>T</th>
<th>P</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

**Module I**


**Module II**


**Module III**

Steganography: Steganography communication, the channel, the building blocks, notation and terminology, information, theoretic foundations of Steganography, cachin's definition of Steganography security, practical Steganography methods, statistics preserving Steganography, model based Steganography, masking embedding as natural processing, minimizing the embedding impact, matrix embedding, non-shared selection rule.

**Module IV**

Steganalysis: Steganalysis scenarios, detection, forensic steganalysis, the influence of the cover work on steganalysis, some significant steganalysis algorithms, LSB embedding and the histogram attack, sample pairs analysis, blind steganalysis of JPEG images using calibration, blind steganalysis in the spatial domain.

**Module V**

Applications: Applications of Steganography, Steganography for Dissidents, Steganography for Criminals.
Text Book

Reference
## ECS768: MOBILE DEVICE FORENSICS

<table>
<thead>
<tr>
<th>Module</th>
<th>Credit Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module I</td>
<td>10 hrs</td>
</tr>
<tr>
<td>Android and mobile forensics: Introduction, Android platform, Linux, Open source software and forensics, Android Open Source Project, Internationalization, Android Market, Android forensics</td>
<td></td>
</tr>
</tbody>
</table>

### Module II
10 hrs
Android hardware platforms: Overview of core components, Overview of different device types, Read-only memory and boot loaders, Manufacturers, Specific devices

### Module III
10 hrs
Android software development kit and android debug bridge: Android platforms, Software development kit (SDK), Android security model, Forensics and the SDK.

### Module IV
10 hrs
Android file systems and data structures: Data in the shell, Type of memory, File systems, Mounted file systems and directory structures. Android forensic techniques: Procedures for handling an Android device, Imaging Android USB mass storage devices, Logical techniques, Physical techniques

### Module V
10 hrs
Android device data and app security: Data theft targets and attack vectors, Security considerations, Individual security strategies, Corporate security strategies, App development security strategies. Android application and forensic analysis: Analysis techniques, FAT forensic analysis, YAFFS2 forensic analysis, Android app analysis
Text Book

References
2. Andrew Martin, Mobile Device Forensics, SANS Institute, 2009

Web Resources
Module I
Introduction, Purpose and applicability, Target audience, the fundamentals, system security engineering, system and system elements

Module II
System Security perspective, protection capability and Security, System Security and failure, strategy for system security, beyond verification and validation-demonstration, system characteristics and system security, role of system security engineering

Module III

Module IV

Module V

Text Book

Reference
Module I 10 hrs

Module II 10 hrs

Module III 10 hrs

Module IV 10 hrs

Module V 10 hrs
Report Writing for High-Tech Investigations: Understanding the Importance of Reports, Guidelines for Writing Reports, Generating Report Findings with Forensics Software Tools, Applying Ethics and Codes to Expert Witnesses, Organizations with Codes Ethics, Ethical Difficulties in Expert Testimony.

Textbook

References
2. Computer Investigation by Elizabeth Bauchne.
Module I

Module II
Web Application Technologies: The HTTP Protocol, HTTP Requests, HTTP Responses, HTTP Methods, URLs, REST, HTTP Headers, Cookies, Status Codes, HTTPS, HTTP Proxies, HTTP Authentication, Web Functionality, Server-Side Functionality, Client-Side Functionality, State and Sessions, Encoding Schemes, URL Encoding, Unicode Encoding, HTML Encoding, Base64 Encoding, Hex Encoding, Remoting and Serialization Frameworks.

Module III

Module IV
Module V 12 hrs


Text Book

References
1. Andres Andreu, Professional Pen Testing for Web application, Wrox Press
4. OReilly Web Security Privacy and Commerce 2/e, 2011
6. Hassan, Database Security and Auditing, Cengage Learning
Module I
10 hrs
Biometrics: Introduction, 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.

Module II
10 hrs

Module III
10 hrs
Behavioral Biometric Technologies: Handprint Biometrics, DNA Biometrics, signature and handwriting technology, Technical description, classification, keyboard / keystroke dynamics, Voice, data acquisition, feature extraction, characteristics, strengths, weaknesses deployment.

Module IV
10 hrs
Multi biometrics: Multi biometrics and multi factor biometrics, two-factor authentication with passwords, tickets and tokens, executive decision, implementation plan.

Module V
10 hrs
Case studies on Physiological, Behavioral and multifactor biometrics in identification systems.
Text Book(s)

Reference
ECS773: OPERATING SYSTEMS SECURITY

Module I 10 hrs

Module II 10 hrs

Module III 10 hrs
Security in ordinary operating system: UNIX security, windows security Verifiable security goals: Information flow, information flow secrecy, models, information flow integrity model, the challenges of trusted, process, covert channels.

Module IV 10 hrs
Security Kernels: The Security Kernels, secure communications, processor Scomp, Gemini secure OS, Securing commercial OS, Retrofitting security into a commercial OS, History Retrofitting commercial OS, Commercial era, microkernel era, UNIX era- IX, domain and type enforcement.

Module V 10 hrs
Case study: Solaris Extensions Trusted extensions, access control, Solaris compatibility, trusted extensions, mediations process rights management, role based access control, trusted extensions, networking trusted extensions, multilevel services, trusted extensions administration. Case study: Building secure OS for Linux: Linux security modules, security enhanced Linux.

Text Book

References
1. Michael Palmer, Guide to Operating system Security Thomson
2. Andrew S Tanenbaum, Modern Operating systems, 3rd Edition
Module I 10 hrs

Module II 10 hrs
Compliance and Audit: Cloud customer responsibilities, Compliance and Audit Security Recommendations. Portability and Interoperability: Changing providers reasons, Changing providers expectations, Recommendations all cloud solutions, IaaS Cloud Solutions, PaaS Cloud Solutions, SaaS Cloud Solutions.

Module III 10 hrs

Module IV 10 hrs

Module V 10 hrs

Text Book

Reference
EID760: PROGRAMMING WITH R

L T P C
3 0 0 3

Module I 10 hrs
Introduction to R programming, Introduction to Functions, Preview of Important R Data Structures, Vectors, Recycling, Common Vector Operations, Vectorized Operations, Filtering Matrices and Arrays

Module II 9 hrs
Lists, Creating Lists, General List Operations Accessing List Components and Values, Applying Functions to Lists, Recursive Lists, Data Frames, Creating Data Frames, Other Matrix-Like Operations, Merging Data Frames, Applying Functions to Data Frames, Factors and Tables, Factors and Levels, Common Functions Used with Factors, Working with Table, Table-Related Functions

Module III 10 hrs

Module IV 9 hrs
Math and Simulations in R, Math Functions, Functions for Statistical Distributions, Sorting, Linear Algebra Operations on Vectors and Matrices, Set Operations, Simulation Programming in R, Object-Oriented Programming, S3 Classes, S4 Classes, S3 Versus S4, Managing Your Objects

Module V 10 hrs
Input/Output, Accessing the Keyboard and Monitor, Reading and Writing Files, Accessing the Internet, String Manipulation, String-Manipulation
Functions, Regular Expressions, Use of String Utilities in the edtdbg Debugging Tool, Creating Graphs, Customizing Graphs, Saving Graphs to Files Creating Three-Dimensional Plots

**Text Book**
1. Norman Matloff, Art of R programming, Safari books online Publisher, Nostarch Press

**References**
1. Mark gardener, Beginning R: The Statistical Programming Language , Wrox publication
2. lary pace, Beginning R, Appress Publishers
3. Andrie De Vries and Joris Meys , R Programming for Dummies, 1/e,Wiley India Private Limited,
EID763: MULTIVARIATE TECHNIQUES FOR DATA ANALYSIS

L T P C
3 0 0 3

Module I 8 hrs
Introduction To Multivariate Analysis: Meaning of Multivariate Analysis, Measurements Scales - Metric measurement scales and Non- metric measurement scales, Classification of multivariate techniques (Dependence Techniques and Inter-dependence Techniques), Applications of Multivariate Techniques in different disciplines.

Module II 8 hrs
Factor Analysis: Meanings, Objectives and Assumptions, Designing a factor analysis, Deriving factors and assessing overall factors, Interpreting the factors and validation of factor analysis.

Module III 8 hrs
Cluster Analysis: Objectives and Assumptions, Research design in cluster analysis, Deriving clusters and assessing overall fit (Hierarchical methods, Non Hierarchical Methods and Combinations), Interpretation of clusters and validation of profiling of the clusters.

Module IV 8 hrs
Discriminant Analysis- concept, objective and applications. Procedure for conducting discriminant analysis. Stepwise discriminate analysis and Mahalanobis procedure. Logit model.

Module V 8 hrs

Text Book(s)

References
Module I

10 hrs
Understanding Computers Internet and Cyber Laws, Modern Era: The Scene and Problems, Need for Cyber Laws, Historical Perspective, Impact of the Internet and Information Technology (IT) on Business and Society The Character and Use of Internet Technologies.
Conceptual Framework of E-commerce: E-governance what is E-commerce? Growth and Development of E-commerce Various Modes of E-commerce, Mechanism Involved in the Operation of Internet Type of Players in E-commerce, Web Development and Hosting Agreements Web Hosting The Problem of Internet Jurisdiction Illustrative Cases about Cyberspace Jurisdiction Type of Websites

Module II

10 hrs

Module III

10 hrs

**Module IV**  
10 hrs  
Protection of Intellectual Property Rights in Cyberspace in India: The Cyberspace The Relevance of Domain Names in Intellectual Property Rights, Deception by Squatting in Cyberspace, Bad Faith in Relation to Domain Name Infringement, Some Leading Cases Involving Complaints from India before WIPO, Protection of Copyright on Cyberspace, Rights of Software Copyright Owners, Infringement of Copyright on Cyberspace, Cyberspace, the Internet, Websites and the Nature of the Copyright, Linking, Hyper-Linking and Framing, Remedies for Infringement of Copyright on Cyberspace, The Liabilities of an Internet Services Provider (ISP) in Cyberspace, Cyberspace and the Protection of Patents in India, Patent as a Form of Intellectual Property

**Module V**  
10 hrs  
Penalties, Compensation and Adjudication of Violations of Provisions of IT Act and Judicial Review: Penalty and Compensation for Damage to Computer, Computer System, Compensation for Failure to Protect Data, Penalty for Failure to Furnish Information, Return or any Other Penalty, Adjudication of Disputes under the IT Act, Cyber Appellate Tribunal, Its Functions and Powers under the IT Act, Some Important Offences under the Cyberspace Law and the Internet in India: Obscenity and Pornography on Cyberspace, Hacking on the Cyberspace and Internet, Other Offences-Computer Resource, Violation of the Right of Privacy on Cyberspace/Internet, Punishment for Violation of Privacy, Breach of Confidentiality, and Privacy under the IT Act, Terrorism on Cyber Space/Internet

**Text Book**  
1. Harish Chander, Cyber Laws and IT protections, PHI Edition

**Reference**  
1. Dumortier, International Encyclopedia Of Cyber Law (3vol) , Jos
Module I 9 hrs

Module II 9 hrs

Module III 10 hrs

Module IV 9 hrs

Module V 9 hrs
Managing a Cyber security Crisis: Devastating Cyber attacks and Falling Off the Cliff, Keeping Calm and Carrying On, Recovering Cyber security and IT Capabilities, Ending the Crisis.

Text Book

Reference
1. Gurpreet Dhillon, Enterprise Cyber Security,2/e, Chegg Publishers
Chandrahans ICT Bhavan - Institute of Technology, Visakhapatnam Campus

School of Technology, Hyderabad Campus

Sir Visvesvaraya Bhavan - GITAM School of Technology, Bengaluru Campus