UNIVERSITY OF KERALA

REGULATIONS, SCHEME
&
SYLLABUS
for
M.Tech Degree Programme
in
Computer Science & Engineering
(Information Security)

2013 Scheme
## University of Kerala
### Scheme of Studies for Master of Technology

**Stream**: Information Security  
**Semester 1**

<table>
<thead>
<tr>
<th>Code No.</th>
<th>Name of Subject</th>
<th>Credits</th>
<th>Hrs / week</th>
<th>End Sem Exam (Hours)</th>
<th>Marks</th>
</tr>
</thead>
<tbody>
<tr>
<td>RCC 1001</td>
<td>Mathematical Foundations of Computer Science</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>40</td>
</tr>
<tr>
<td>RIC 1001</td>
<td>Foundations of Information Security</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>40</td>
</tr>
<tr>
<td>RCC 1002</td>
<td>Topics in Database Technology</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>40</td>
</tr>
<tr>
<td>RCC1003</td>
<td>Advanced Data Structures and Algorithms</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>40</td>
</tr>
<tr>
<td>RCC 1004</td>
<td>Advanced Software Engineering</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>40</td>
</tr>
<tr>
<td>RIC 1002</td>
<td>Number Theory and Cryptography</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>40</td>
</tr>
<tr>
<td>RIC 1101</td>
<td>Seminar</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td>RIC 1102</td>
<td>Secure Computing Laboratory - I</td>
<td>1</td>
<td>2</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td></td>
<td>21</td>
<td>22</td>
<td>18</td>
<td>440</td>
</tr>
</tbody>
</table>

**Remarks**:  
- End-of-Semester Exam by University  
- No End-of-Sem Exam  
- End-of-Sem Exam by University
<table>
<thead>
<tr>
<th>Code No.</th>
<th>Name of Subject</th>
<th>Credits</th>
<th>Hrs/week</th>
<th>End Sem Exam hours</th>
<th>Marks</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>RIC 2001</td>
<td>Formal Methods in Secure Computing</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>40</td>
<td>60</td>
</tr>
<tr>
<td>RIC 2002</td>
<td>Network Security</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>40</td>
<td>60</td>
</tr>
<tr>
<td>*</td>
<td>Elective -I (Stream Elective)</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>40</td>
<td>60</td>
</tr>
<tr>
<td>*</td>
<td>Elective -II (Stream Elective)</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>40</td>
<td>60</td>
</tr>
<tr>
<td>*</td>
<td>Elective -III (Department Elective)</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>40</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>Research Methodologies</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>40</td>
<td>60</td>
</tr>
<tr>
<td>RCC 2000</td>
<td>Research Methodology</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>40</td>
<td>60</td>
</tr>
<tr>
<td>RIC 2101</td>
<td>Seminar</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>100</td>
<td>-</td>
</tr>
<tr>
<td>RIC 2102</td>
<td>Thesis Preliminary-Part I</td>
<td>2</td>
<td>2</td>
<td>-</td>
<td>100</td>
<td>-</td>
</tr>
<tr>
<td>RIC 2103</td>
<td>Secure Computing Laboratory - II</td>
<td>1</td>
<td>2</td>
<td>-</td>
<td>100</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>TOTAL</td>
<td>22</td>
<td>23</td>
<td>18</td>
<td>540</td>
<td>360</td>
</tr>
</tbody>
</table>
Electives for Semester 2:

**Department Electives**

- RCD 2001 Data Warehousing & Mining
- RCD 2002 Software Quality Assurance and Testing
- RCD 2003 Simulation & Modeling
- RCD 2004 Data Compression
- RID 2001 Cyber Laws & Ethics
- RID 2002 Advanced Topics in Distributed Systems
- RID 2003 Cloud Computing

**Stream Elective 1**

- RIE 2001 Database Security
- RIE 2002 Access Networks and Cellular Communication
- RIE 2003 Biometric Authentication

**Stream Elective 2**

- RIE 2004 Web Security Testing
- RIE 2005 Public Key Infrastructure & Trust Management
- RIE 2006 Information Theory & Coding

* The student has to choose Elective 1, Elective 2 and Elective 3 from the lists *Stream Elective 1*, *Stream Elective 2* and *Departmental Electives* respectively, as advised by the course coordinator.
## Semester 3

<table>
<thead>
<tr>
<th>Code No.</th>
<th>Name of Subject</th>
<th>Credits</th>
<th>Hrs/week</th>
<th>End Sem Exam hours</th>
<th>Internal Continuous Assessment</th>
<th>End Semester Exam</th>
<th>Total</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Elective IV (Stream Elective 3)</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>40</td>
<td>60</td>
<td>100</td>
<td>End-of-Semester Exam by University</td>
</tr>
<tr>
<td>*</td>
<td>Elective V (Stream Elective 4)</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>40</td>
<td>60</td>
<td>100</td>
<td>-do-</td>
</tr>
<tr>
<td>**</td>
<td>Elective VI (Non Department Elective)</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>40</td>
<td>60</td>
<td>100</td>
<td>-do-</td>
</tr>
<tr>
<td>RIC 3101</td>
<td>Thesis Preliminary-Part II</td>
<td>5</td>
<td>15</td>
<td>0</td>
<td>200</td>
<td>200</td>
<td></td>
<td>No End-of-sem Exam</td>
</tr>
<tr>
<td></td>
<td><strong>TOTAL</strong></td>
<td><strong>14</strong></td>
<td><strong>23</strong></td>
<td><strong>09</strong></td>
<td><strong>320</strong></td>
<td><strong>180</strong></td>
<td><strong>500</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Electives for Semester 3:

**Stream Elective 3**

- RIE 3001 Information Security Policies & Risk Analysis
- RIE 3002 Distributed Algorithms
- RIE 3003 Information Security Metrics

**Stream Elective 4**

- RIE 3004 Cyber Forensics & Investigation
- RIE 3005 Advanced Topics in Information Security
- RIE 3006 Perimeter Security

### Inter-disciplinary Electives:

- RCI2001 Object Oriented Modeling and Designing
- RCI2002 Software Project Management
- RCI2003 Basic Data Structures and Algorithms
- RII 2001 .NET Programming
- RII 2002 Java Programming

* The student has to choose Elective 3 and Elective 4 from the lists of *Stream Elective 3* and *Stream Elective 4*, respectively as advised by the course coordinator.

**Non-departmental electives** should be selected from the list of inter-disciplinary electives **offered by other departments**, as advised by the course coordinator.
<table>
<thead>
<tr>
<th>Code No.</th>
<th>Name of Subject</th>
<th>Credits</th>
<th>Hrs./week</th>
<th>Evaluation (Marks)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Internal</td>
<td>External</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sessional</td>
<td>Guide</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>External</td>
<td>Thesis</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Viva</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Voce</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Total</td>
</tr>
<tr>
<td>RIC4101</td>
<td>Thesis-Final</td>
<td>12</td>
<td>150</td>
<td>150</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>200</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>600</td>
</tr>
<tr>
<td>TOTAL</td>
<td></td>
<td>12</td>
<td>150</td>
<td>150</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>200</td>
<td>100</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>600</td>
</tr>
</tbody>
</table>

Note: 6 to 8 hours per week is for department assistance
RCC 1001
MATHEMATICAL FOUNDATIONS OF COMPUTER SCIENCE

Lecture : 3 hrs/ Week  Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
- To understand the fundamental concepts in
  - theorem proving
  - Recurrence relations
  - Counting and probability
  - Probability distributions
  - Special graphs and circuits
  - Important structures

Learning Outcomes
- Conceptual understanding of the above topics and ability to apply them in practical situations.

MODULE 1
Techniques for theorem proving: Direct Proof, Proof by Contra position, Proof by exhausting cases and proof by contradiction, Linear-time temporal logic and Branching-time logic-Syntax, Semantics, Practical patterns of specifications, Important equivalences, Adequate sets of connectives. Principle of mathematical induction, principle of complete induction. Recursive definitions, Generating functions, function of sequences calculating coefficient of generating function, solving recurrence relation by substitution and generating functions Solution methods for linear, first-order recurrence relations with constant coefficient, characteristic roots

MODULE 2

MODULE 3
Graphs, Terminology, Euler tours, planar graphs, Hamiltonian graphs, Euler’s formula (proof), four colour problem (without proof) and the chromatic number of a graph, five colour theorem, chromatic polynomials, Warshall’s algorithm, Decision Trees, weighted trees
Groups and subgroups, homomorphism theorems, cosets and normal subgroups, Lagrange’s theorem, rings, finite fields, polynomial arithmetic, quadratic residues, reciprocity, discrete logarithms, elliptic curve arithmetic.

References


Structure of the Question paper
For the End Semester Examination the question paper will consist of at least 80% analytical/design problems. There will be three questions (with sub-divisions) from each module out of which two questions are to be answered.
RIC 1001  
FOUNDATIONS OF INFORMATION SECURITY

Lecture : 3 hrs/ Week  
Credits : 3

Internal Continuous Assessment : 40 Marks

End Semester Examination : 60 Marks

Course Objectives
• To understand the founding principles of Information security

Learning Outcomes
• Conceptual understanding of the principles of information security, its significance and the domain specific security issues.

MODULE 1

MODULE 2

MODULE 3
Law and ethics: Intellectual property rights, computer software copyrights, security policy, ethical hacking, security tools.

References:
Structure of the Question paper

For the End Semester Examination the question paper will consist of at least 50% analytical problems. There will be three questions (with sub-divisions) from each module out of which two questions are to be answered.
RCC 1002
TOPICS IN DATABASE TECHNOLOGY

Lecture : 3 hrs/ Week   Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
- To understand the implementation and management aspects of databases.
- To understand the principles of distributed databases.
- To understand object based data models and their implementation.
- To understand the recent advances in database technology.

Learning Outcomes
- Conceptual understanding of various implementation issues in databases.
- Conceptual understanding of distributed databases.
- Conceptual understanding and ability to work with object based database systems.
- Conceptual understanding of recent technological trends in databases.

MODULE 1

MODULE 2

MODULE 3
Mobile Databases: Location and Handoff Management - Effect of Mobility on Data Management - Location Dependent Data Distribution - Mobile Transaction Models - Concurrency Control - Transaction Commit Protocols Active Database Concepts - Triggers – Temporal & Spatial Databases – Multimedia Databases- NoSQL Databases and Big Data
References


Structure of the Question paper
For the End Semester Examination the question paper will consist of at least 60% analytical/design problems. There will be three questions from each module (with sub-divisions) (with sub-divisions) out of which two questions are to be answered.
RCC 1003
ADVANCED DATA STRUCTURES AND ALGORITHMS

Lecture : 3 hrs/ Week Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
• To understand about advanced data structures.
• To understand how to analyze and establish correctness of algorithms
• To understand theory behind various classes of algorithms.

Learning Outcomes
• The student should have deep conceptual understanding of advanced data structures and their applications
• He should know the theory behind various classes of algorithms.
• He should be able to design, prove the correctness and analyse new algorithms

MODULE 1
Network flow algorithms: properties, Ford-Fulkerson method, maxflow-mincut theorem, Edmonds-Karp heuristics, push-relabel, relabel-to-front algorithms, Dinic’s algorithm, MPM algorithm, maximum bipartite matching - analysis of associated algorithms, applications.

MODULE 2

MODULE 3
Number-Theoretic algorithms: GCD algorithm, modular arithmetic, primality testing, Miller-Rabin test, Integer factorization - Pollard Rho heuristic.
Overview of Complexity classes – P, NP, Co-NP, NP-hard, NP complete. Space complexity. Complexity classes in randomized algorithms – RP, PP, ZPP, BPP.

References:

Structure of the Question paper
For the End Semester Examination the question paper will consist of at least 70% analytical/design problems. There will be three questions from each module (with subdivisions) out of which two questions are to be answered by the students.
RCC 1004
ADVANCED SOFTWARE ENGINEERING

Lecture : 3 hrs/ Week Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
- To gain a deep understanding of the issues and approaches in modelling, analysing and testing software systems.

Learning Outcomes
- Conceptual understanding of the principles of software modelling and testing.
- Ability to apply the principles in real-cases.

MODULE 1

MODULE 2

MODULE 3

References:

Structure of the Question paper

For the End Semester Examination the question paper will consist of at least 50% analytical/design problems. There will be three questions from each module (with subdivisions) out of which two questions are to be answered by the students.
RIC 1002
NUMBER THEORY AND CRYPTOGRAPHY

Lecture : 3 hrs/ Week  Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
- To understand the concepts of number theory.
- Familiarize with the properties of Finite fields, Group, ring etc.
- To understand the modular arithmetic and quadratic residue.
- To understand various cryptographic algorithms and their security analysis.

Learning Outcomes
- Conceptual understanding of number theory and its applications in cryptographic algorithms.
- Conceptual understanding of properties of finite fields, groups, rings and applications in information security.
- Conceptual understanding of underlying mathematical fundamentals of public key cryptography which enables the system more secure.
- Conceptual understanding of cryptographic algorithms and its security analysis.

MODULE 1
Number theory: Introduction, divisibility, Greatest Common Divisor, prime numbers, Modular Arithmetic Preliminary ideas of factoring and primality testing-Miller Rabin, Congruences, Solution of congruences, quadratic residue, Complete residue systems. Euler’s Theorem and Fermat’s Little theorem – Euler’s $\phi$ function, Wilson’s theorem, Chinese remainder theorem

MODULE 2
Groups, cyclic groups, rings, Finite fields. One way functions and Two way function, Trapdoor, Discrete Logarithm, Stream and block cipher, Hash function, MAC, Cryptographic hash SHA1, Needham Schroeder protocol, Cryptography and cryptanalysis Symmetric key encryption: DES- strength of DES, Differential and linear cryptanalysis, Triple DES, AES

MODULE 3

References

Structure of the Question paper
For the End Semester Examination the question paper will consist of at least 60% analytical/design problems. There will be three questions from each module (with subdivisions) out of which two questions are to be answered by the students.
RIC1101
SEMINAR

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lecture</td>
<td>0 hrs/ Week</td>
<td>2</td>
</tr>
<tr>
<td>Credits</td>
<td>Internal Continuous Assessment</td>
<td>100 Marks</td>
</tr>
<tr>
<td></td>
<td>End Semester Examination</td>
<td>0 Marks</td>
</tr>
</tbody>
</table>

Each student is required to select a topic on advanced technologies in Computer Science and allied subject domains and get it approved by the faculty-in-charge of seminar. He/she should give a presentation with good quality slides. An abstract of the seminar should be submitted to the faculty members well in advance before the date of seminar. He/she should also prepare a well documented report on the seminar in an approved format and submit to the department. The seminar presentation and report will be evaluated for the award of sessional marks.
RIC1102
SECURE COMPUTING LABORATORY - 1

Practical : 2hrs/ Week  Credits : 1
Internal Continuous Assessment : 100 Marks
End Semester Examination : 0 Marks

The experiments are based on, but need not be limited to, the topics related to security covered in RIC 1001: Foundations of Information Security and RIC 1002: Number Theory and Cryptography.
RIC 2001
FORMAL METHODS IN SECURE COMPUTING

Lecture : 3 hrs/ Week  Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
• To understand the formal models, protocols and methods associated with secure computing

Learning Outcomes
• The student gains fundamental knowledge in formal aspects of secure computing.

MODULE 1

MODULE 2
Protocol goals - Yahalom protocol, secrecy, authentication, nonrepudiation, anonymity. Theorem proving rank functions, secret of a shared key, authentication, machine assistance. Simplifying transformations on protocols, structural transformations, case study.

MODULE 3
Other approaches: introduction, DolevYao model, BAN logic and derivatives, FDM and Inajo, NRL Analyser, Bmethod approach, noninterference approach, strand spaces, inductive approach, Spi calculus.

References:

Structure of the Question paper
For the End Semester Examination the question paper will consist of three questions from each module (with sub-divisions) out of which two questions are to be answered by the students.
RIC 2002
NETWORK SECURITY

Lecture : 3 hrs/ Week    Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
- To understand the concepts, issues and solution approaches pertaining to security of networks.

Learning Outcomes
- The student gets a deeper understanding of the security aspects of networks and gains ability to assess and suggest the security requirements in a practical network design.

MODULE 1

MODULE 2

MODULE 3

References:

Structure of the Question paper
For the End Semester Examination the question paper will consist of at least 50% analytical/design problems. There will be three questions from each module (with subdivisions) out of which two questions are to be answered by the students.
RCC 2003
RESEARCH METHODOLOGY

 Lecture : 2hrs/ Week  Credits : 2
 Internal Continuous Assessment : 40 Marks
 End Semester Examination : 60 Marks

Course Objective:
• To formulate a viable research question
• To distinguish probabilistic from deterministic explanations
• To analyze the benefits and drawbacks of different methodologies
• To understand how to prepare and execute a feasible research project

Learning Outcome:
• Students are exposed to the research concepts in terms of identifying the research problem, collecting relevant data pertaining to the problem, to carry out the research and writing research papers/thesis/dissertation.

MODULE 1
Introduction to Research Methodology - Objectives and types of research: Motivation towards research - Research methods vs. Methodology. Type of research: Descriptive vs. Analytical, Applied vs. Fundamental, Quantitative vs. Qualitative, and Conceptual vs. Empirical. Research Formulation - Defining and formulating the research problem - Selecting the problem - Necessity of defining the problem - Importance of literature review in defining a problem. Literature review: Primary and secondary sources - reviews, treatise, monographs, patents. Web as a source: searching the web. Critical literature review - Identifying gap areas from literature review - Development of working hypothesis.

MODULE 2

MODULE 3
Reporting and thesis writing - Structure and components of scientific reports - Types of report - Technical reports and thesis - Significance - Different steps in the preparation, Layout, structure and Language of typical reports, Illustrations and tables, Bibliography, referencing and footnotes. Presentation; Oral presentation - Planning - Preparation - Practice - Making presentation - Use of audio-visual aids - Importance of effective communication. Application of results of research outcome: Environmental impacts - Professional ethics - Ethical issues - ethical committees. Commercialization of the work - Copy right - royalty - Intellectual property rights and patent law - Trade Related aspects of Intellectual Property Rights
- Reproduction of published material - Plagiarism - Citation and acknowledgement - Reproducibility and accountability.

References:

Structure of the Question paper
For the End Semester Examination the question paper will consist of three questions from each module (with sub-divisions) out of which two questions are to be answered by the students.
RIC2101
SEMINAR

Lecture : 0 hrs/ Week   Credits : 2
Internal Continuous Assessment : 100 Marks
End Semester Examination : 0 Marks

Each student is required to select a topic on advanced technologies in Computer Science and allied subject domains, preferably one which also relevant as his/her thesis topic, and get it approved by the faculty-in-charge of seminar. He/she should give a presentation with good quality slides. An abstract of the seminar should be submitted to the faculty members well in advance before the date of seminar. He/she should also prepare a well documented report on the seminar in an approved format and submit to the department. The seminar presentation and report will be evaluated for the award of sessional marks.
RIC2102
THESIS PRELIMINARY – PART 1

Hours/week : 2  
Credits : 2  
Internal Continuous Assessment : 100 Marks

The main objective of the thesis is to provide an opportunity to each student to do an independent study and research on the area of specialization under the guidance of a faculty member. The student is required to explore in depth a topic of his/her own choice, which adds significantly to the body of knowledge existing in the relevant field. The student has to undertake and complete preliminary work on the stream of specialization during the semester. The thesis work starts in the second semester and has three parts: Preliminary – Part 1 (in Semester 2), Preliminary – Part 2 (in semester 3) and Final (in semester 4).

In Preliminary – Part 1, the student is expected to identify a domain, do enough exploration by reviewing the literature. The student should also identify his problem and objectives. The progress will be assessed by two seminars. The student is also expected to submit an interim report at the end of the semester.
RIC2103
SECURE COMPUTING LABORATORY 2

Practical : 2hrs/ Week   Credits : 1
Internal Continuous Assessment : 100 Marks
End Semester Examination : 0 Marks

RIC3101
THESIS PRELIMINARY – PART 2

Hours/week : 15   Credits : 5
Internal Continuous Assessment : 200 Marks

In Preliminary – Part 2, the student is expected further explore his problem, identify solutions, do initial experimentation and result evaluation. The student should also prepare a literature survey report and submit it for review to a suitable journal as advised by the thesis supervisor. The progress will be assessed by the review committee through two seminars and an end-of-semester report.
RIC4101
THESIS FINAL

Hours/week : 21  
Credits : 12
Internal Continuous Assessment : 300 Marks
External Assessment : 300 Marks

By the first quarter of the semester, the student should compile his/her work by doing the final experimentation and result analysis. Towards the middle of the semester there would be a pre-submission seminar to assess the quality and quantum of work by the department evaluation committee. This would be the pre-qualifying exercise for the students for getting approval for the submission of final thesis. The decision of the departmental committee in this regard is final and binding. The committee can make recommendations to improve the quality or quantity of the work done. The student is expected to publish technical papers related to his/her research in peer reviewed journals/conferences. The final evaluation of the thesis would be done by an external examiner. The external examiner’s comments regarding the quality and quantity of work is an important decisive factor in the final acceptance/rejection of the thesis.
ELECTIVES
Departmental Elective

RCD 2001
DATA WAREHOUSING & MINING

Lecture : 3 hrs/ Week       Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
To understand the fundamental and advanced concepts Data Warehousing and Data Mining

Learning Outcomes
• Conceptual understanding of
  • Data cleaning, analysis and visualization
  • Data mining techniques.
  • Web mining and Spatial mining

MODULE 1
Data warehousing – Multidimensional data model, OLAP operation, Warehouse schema, Data Warehousing architecture, warehouse server, Metadata, OLAP engine, Data warehouse Backend Process, Data Warehousing to Data Mining. Basic Data Mining Tasks, Data Mining Issues, Data Mining Metrics, Data Mining from a Database Perspective, Knowledge Discovery in Database Vs Data mining. Data Preprocessing: Preprocessing, Cleaning, Integration, Transformation, Reduction, Discretization, Concept Hierarchy Generation, Introduction to DMQL.

MODULE 2

MODULE 3

References:
3. J. Han, M. Kamber, “Data Mining: Concepts and Techniques”, 2/e, Morgan Kaufman,
Structure of the Question paper
For the End Semester Examination the question paper will consist of at least 60% analytical/query/design problems. There will be three questions from each module (with sub-divisions) out of which two questions are to be answered by the students.
Departmental Elective

RCD 2002
SOFTWARE QUALITY ASSURANCE AND TESTING

Lecture : 3 hrs/ Week Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
- Understand the theoretical aspects of software testing
- Demonstrate the knowledge of the existing testing methods
- Demonstrate the knowledge of static and dynamic analysis methods
- Demonstrate the knowledge of applying testing and analysis methods in software development and maintenance

Learning Outcomes
- Students get in-depth skill to quantitatively assess the quality of software; they also understand the fundamental principles and tools for software-testing and quality assurance.

MODULE 1
Software Quality Metrics: Product Quality metrics, In-process Quality Metrics, Metrics for Software Maintenance, Examples of Metric Programs Software Quality metrics methodology: establishing quality requirements, Identifying Software quality metrics, Implement the software quality metrics, analyze software metrics results, validate the software quality metrics â€” Software quality indicators, Fundamentals in Measurement theory.

MODULE 2
Software Testing Strategy and Environment Establishing testing policy, structured approach to testing, test factors, Economics of System Development Life Cycle (SDLC) Testing Software Testing Methodology Defects hard to find, verification and validation, functional and structural testing, workbench concept, eight considerations in developing testing methodologies, testing tactics checklist, Software Testing Techniques Black Box, Boundary value, Bottom up, Branch coverage, Cause Effect graphing, CRUD, Database, Exception, Gray Box, Histograms, Inspections, JADs, Pareto Analysis, Prototyping, Random Testing, Risk based Testing, Regression Testing, Structured Walkthroughs, Thread Testing, Performance Testing, White Box Testing
MODULE 3

Testing Process

Testing Specialized Systems and Applications Testing Client/Server Web applications, Testing off the Shelf Components, Testing Security, Testing a Data Warehouse

References:

Structure of the Question paper
For the End Semester Examination the question paper will consist of at least 50% analytical/design problems. There will be three questions from each module (with sub-divisions) out of which two questions are to be answered by the students.
Departmental Elective

RCD 2003
SIMULATION & MODELING

Lecture :  3 hrs/ Week    Credits :  3
Internal Continuous Assessment :  40 Marks
End Semester Examination :  60 Marks

Course Objectives
- To understand the methodology for modeling and simulation of continuous, discrete time as well as discrete-event systems.
- To have basic knowledge on simulation software and use it in solving of engineering problems, analysis and validation of the results

Learning Outcomes
- The student attains theoretical and practical skills in modeling and simulation of various genre of systems.

MODULE 1

MODULE 2

MODULE 3

Computer Modelling and Simulation Practice: Introduction to simulation languages: Simscript and simulators like NS2, Opnet. Simulation of Single server/multiple servers. Using Simscript/C/C++, Simulation of Deterministic automaton, Push down automaton,
and Turing Machines. Simulation of Stop and wait and sliding window protocols.
Simulation of CSMA/CD LAN. Simulation of Wireless LAN.

References:
2. Raj Jain, The art of computer systems performance analysis, John Wiley and Sons
3. Edward D.Lazowska et.al. Quantitative System Performance (Computer System
   Analysis Using Queueing Network Models); chapters 1-6.
4. Lecture notes of Professor Raj Jain, Washington University in Saint Louis.

Structure of the Question paper
For the End Semester Examination the question paper will consist of at least 50% analytical/design
problems. There will be three questions from each module (with sub-divisions) out of which two
questions are to be answered by the students.
Departmental Elective

RCD 2004
DATA COMPRESSION

Lecture : 3 hrs/ Week  Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
• Develop theoretical foundations of data compression, concepts and algorithms for
  lossy and lossless data compression, signal modelling and its extension to
  compression with applications to speech, image and video processing.

Learning Outcomes
• Awareness about various data compression techniques and their practical
  significance.

MODULE 1
Compression techniques, Compression ratio, lossless & lossy compression, Huffman coding,
Dictionary based Compression, Sliding Window Compression, LZ77, LZ78, LZW
compression. Predictive Coding - prediction and partial match, move to front coding, Run
Length encoding.

MODULE 2
Speech Compression & Synthesis: Digital Audio concepts, Sampling Variables, Lossless
compression of sound, lossy compression & silence compression. Image Compression,
Transform based techniques, Wavelet Methods, adaptive techniques. Images standards,
JPEG Compression, Zig Zag Coding.

MODULE 3
Video Compression- motion compensation, MPEG standards, recent development in
Multimedia Video compression, packet video, Fractal techniques. Comparison of
compression algorithms, Implementation of compression algorithms.

References:
1. David Solomon, Data compression: the complete reference, 2/e, Springer-verlag, New
Structure of the Question paper
For the End Semester Examination the question paper will consist of at least 40% analytical/design problems. There will be three questions from each module (with sub-divisions) out of which two questions are to be answered by the students.
Departmental Elective

RID 2001
CYBER LAWS & ETHICS

Lecture : 3 hrs/ Week Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
• To impart sufficient knowledge on the fundamental principles of IPR, various types of cyber crimes and Indian and international cyber laws.

Learning Outcomes
• The student gains insight into ethical issues, cyber crimes and cyber laws.

MODULE 1
Intellectual property rights, computer software copyrights, copyright in databases and electronic publishing, law of confidence, patent laws, trademarks, product designs, international law.
Computer contracts, liability for defective hardware and software, software contracts, web and hardware contracts, electronic contracts and torts, liabilities.

MODULE 2
Computer crime, computer fraud, hacking, unauthorized modification of information, piracy, computer pornography and harassment.

MODULE 3
Cyber laws in India, IT Act 2000, Offences under IT act. Protection pf IPR in Cyber space in India. International cyber laws and crimes, COE convention of cyber crimes. data subjects’ rights, ethical issues in computer security, case studies.

References

Structure of the Question paper
For the End Semester Examination the question paper will consist of three questions from each module out of which two questions are to be answered by the students.
Departmental Elective

RID 2002
ADVANCED TOPICS IN DISTRIBUTED SYSTEMS

Lecture : 3 hrs/ Week  Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
- To impart deeper understanding in
  - Architecture and issues of distributed systems
  - Distributed algorithms
  - Hadoop system

Learning Outcomes
- The student gains insight into conceptual and practical aspects of distributed systems.

MODULE 1

MODULE 2

MODULE 3

References:

**Structure of the Question paper**

For the End Semester Examination the question paper will consist of at least 60% analytical/design problems. There will be three questions from each module (with sub-divisions) out of which two questions are to be answered by the students.
Departmental Elective

RID 2003
CLOUD COMPUTING

Lecture: 3 hrs/Week  Credits: 3
Internal Continuous Assessment: 40 Marks
End Semester Examination: 60 Marks

Course Objectives
- Understanding cloud computing, and compare with existing technologies.
- Understand how to develop a cloud service

Learning Outcomes
- Design and develop cloud services for everyone.
- Use Cloud Service and collaborate it with various application and taking it online.

MODULE 1

MODULE 2
Centralizing Email Communications – Collaborating on Schedules – Collaborating on To-Do Lists – Collaborating Contact Lists – Cloud Computing for the Community – Collaborating on Group Projects and Events – Cloud Computing for the Corporation.

MODULE 3

References
2. Kai Hwang, Geoffrey C. Fox, Jack J. Dongarra, Distributed and Cloud Computing.: From Parallel Processing to the Internet of Things, 1/e, Morgan Kaufmann , 2011

**Structure of the Question paper**

For the End Semester Examination the question paper will consist of three questions from each module (with sub-divisions) out of which two questions are to be answered by the students.
Stream Elective 1

RIE 2001
DATABASE SECURITY

Lecture : 3 hrs/ Week  Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
• To understand the fundamental issues and solution approaches related to database security.

Learning Outcomes
• The student gains in depth understanding of the principles of database security and ability to use them in real-world scenarios.

MODULE 1
Introduction to DBMS, security policies for database systems. Discretionary security - security policy, policy enforcement. Mandatory security - multilevel secure database systems, design principles. Multilevel secure database systems
Multilevel relational data model, security impact, prototypes.

MODULE 2
Secure distributed and heterogeneous database systems: Discretionary security for distributed database systems, multilevel security, secure heterogeneous and federated database systems. Secure object and multimedia systems: Discretionary and multilevel security for object database systems, secure multimedia data management systems.

MODULE 3
Secure data warehousing, data mining for security applications, secure web data management and digital libraries - threats, security solutions. security for XML, RDF and semantic web.

References:
Structure of the Question paper
For the End Semester Examination the question paper will consist of at least 40% analytical/design problems. There will be three questions from each module (with sub-divisions) out of which two questions are to be answered by the students.
Stream Elective 1

RIE 2002
ACCESS NETWORKS AND CELLULAR COMMUNICATION

Lecture : 3 hrs/ Week  Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
• The course describes in detail how communication services are conceived, developed and deployed in wireless networks.
• Describes optical access networks, its architecture, routing techniques and types of passive optical networks.

Learning Outcomes
• The ability to understand technologies used in wireless and mobile communication
• Able to understand access network technologies, its architecture, routing techniques and analyse the working of different types of passive optical networks.

MODULE 1

MODULE 2
Cellular System Design & Signalling-Channel assignment, cell planning, power control, erlang capacity, database and mobility management, power control, interference and system capacity, signalling standards, antennas for mobile radio. WAP- Architecture, protocols, security issues, Routing Techniques in Ad Hoc wireless networks.

MODULE 3

References

**Structure of the Question paper**

For the End Semester Examination the question paper will consist of at least 40% analytical/design problems. There will be three questions from each module (with sub-divisions) out of which two questions are to be answered by the students.
Stream Elective 1

RIE 2003

BIOMETRIC AUTHENTICATION

Lecture : 3 hrs/ Week  Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
• To impart fundamental knowledge about concepts and applications of biometric authentication

Learning Outcomes
• On completion of the course the student will be able to:
  • use the techniques developed for biometrics and apply them to solve real problems.
  • understand the different methods and algorithms used in biometrics.
  • develop useful applications for biometrics and biometric authentication.

MODULE 1
Introduction to Biometrics: biometric systems, enrollment and recognition, sensors, feature extraction, database, matching, Functionalities: verification and identification, performance measures, design cycle, applications, security and privacy issues. Fingerprint recognition: Friction ridge patterns, Acquisition, feature extraction, matching, indexing, synthesis, palm print

MODULE 2
Face recognition: Introduction, image acquisition, face detection, feature extraction, matching, heterogeneous face recognition. Iris recognition, Image acquisition, iris segmentation, normalization, encoding and matching, quality assessment, performance evaluation.

MODULE 3
Ear detection and recognition – challenges, gait and hand geometry: feature extraction and matching. Security of bio-metric systems: adversary attacks, attacks on user interface, attacks on bio-metric processing, database attacks. biometric standards, biometric databases.

References:

Structure of the Question paper
For the End Semester Examination the question paper will consist of three questions from each module (with sub-divisions) out of which two questions are to be answered by the students.
Stream Elective 2

RIE 2004
WEB SECURITY TESTING

Lecture : 3 hrs/ Week Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
• To understand the encoding and security testing schemes in Web-based applications.

Learning Outcomes
• The student gains theoretical and practical insight into web security testing.

MODULE 1
Introduction to security testing – introduction, HTTP, web application fundamentals, study of tools. Basic observation observing live request headers, observing live post data, highlighting and detecting JavaScript events. Web oriented data encoding – working with base36, base 64, URL encoded and HTML entity data. Tampering with input – tampering with URL, editing cookies, falsifying browser header information, uploading large and malicious files. Automated bulk scanning - spidering a web site, mirroring a web site, scanning a web site.

MODULE 2
Automating specific tasks with cURL – fetching variations on a URL, checking for cross-site scripting, checking for directory traversal, impersonating a web browser or device, imitating a search engine, POST, manipulating session state, manipulating cookies, Automating with LibWWW Perl – simulating form input, capturing and storing cookies, checking session expiration, sending malicious cookie values, uploading malicious files and viruses.

MODULE 3
Seeking design flaws – bypassing required navigation, abusing password recovery, predictable identifiers, repeatability, high load actions, restrictive functionality and race conditions. Attacking AJAX. Manipulating sessions – finding session identifiers, analyzing session identifiers. Multifaceted tests – stealing cookies, creating overlays, attempting cross-site tracing, attempting command injection, attempting SSI.

References:

*Structure of the Question paper*

For the End Semester Examination the question paper will consist of three questions from each module (with sub-divisions) out of which two questions are to be answered by the students.
Stream Elective 2

RIE 2005
PUBLIC KEY INFRASTRUCTURE AND TRUST MANAGEMENT

Lecture : 3 hrs/ Week  Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives

• To gain a good understanding about the Public key infrastructure concepts, the issues involved in setting up and deploying a PKI system and existing PKI technologies

Learning Outcomes

• The student gains insight into the technology behind PKI systems and the issues in the design and deployment of a PKI system.

MODULE 1

MODULE 2

MODULE 3
IPKI enabled services -SSL-S/MIME -IPSec, Evaluating PKI Solutions-Operational requirements for PKI- deploying PKI-Problems in PKI deployment. Trust management challenges, taxonomy framework, architecture, system components, system setting and operations.

References:

Structure of the Question paper
For the End Semester Examination the question paper will consist of three questions from each module (with sub-divisions) out of which two questions are to be answered by the students.
Stream Elective 2

RIE 2006
INFORMATION THEORY AND CODING

Lecture: 3 hrs/ Week  Credits: 3
Internal Continuous Assessment: 40 Marks
End Semester Examination: 60 Marks

Course Objectives
• To introduce the basic concepts of information theory, as well as the different error
controlling coding schemes

Learning Outcomes
• The student gains an understanding of the fundamentals of information theory, as well
as the limits of data compression and data transmission

MODULE 1
Information theory: entropy, relative entropy and mutual information – Data compression –
Kraft inequality – Huffman Codes – Shannon-Fano-Elias Coding – Channel Capacity –
Channel Coding Theorem – Zero Error Codes – Hamming Codes

MODULE 2
Algebraic coding theory: block codes - maximum likelihood decoding - BS channel - error
detection and correction. Linear block codes - generator matrix - parity-check matrix -
syndrome and cosets - dual code - examples. Cyclic codes - generator and parity-check
polynomials - dual codes - Reed-Solomon codes - decoding algorithm

MODULE 3
Convolutional codes: encoding - state diagram - generator matrix - termination and
puncturing - Minimum distance decoding – trellises - Viterbi algorithm – distance properties
and error bounds – free distances – active distances – weight enumerators for terminated
codes – path enumerators – pairwise error probability - Viterbi bound

References:
   Interscience, 2006
2. A. Neubauer, J. Freudenberger, V. Kuhn, “Coding Theory: Algorithms, Architectures
   and Applications”, John Wiley India, 2012.
   Applications”, 2/e, Pearson India, 2011
4. Simon Haykin, “Digital Communications”, 1/e, Wiley India, 2006

Structure of the Question paper
For the End Semester Examination the question paper will consist of at least 50% analytical/design
problems. There will be three questions from each module (with sub-divisions) out of which two
questions are to be answered by the students.
Stream Elective 3

RIE 3001
INFORMATION SECURITY POLICIES & RISK ANALYSIS

Lecture : 3 hrs/ Week Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
• To impart sufficient understanding of security policies and risk analysis principles.

Learning Outcomes
• The student gains deeper insight into various aspects of security policies and risk analysis.

MODULE 1
Introduction, planning and preparation, developing policies, asset classification policy, developing standards, developing procedures, creating a table of contents. Understanding how to sell policies, standards and procedures, typical tier 1 policies, typical tier 2 policies.

MODULE 2

MODULE 3
Facilitated Risk analysis and assessment process (FRAAP) – skills, session agreements, preFRAAP, postFRAAP, infrastructure FRAAP, mapping controls, business impact analysis.

References:
Structure of the Question paper
For the End Semester Examination the question paper will consist of three questions from each module (with sub-divisions) out of which two questions are to be answered by the students.
Stream Elective 3

RIE 3002
DISTRIBUTED ALGORITHMS

Lecture : 3 hrs/ Week Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives

- Provide an introduction to the most important basic results in the area of distributed Algorithms.
- Should be able to use basic distributed algorithms and impossibility results
- Ability to apply distributed algorithms in large computer networks to multiprocessor shared-memory systems.

Learning Outcomes

- Understand various synchronous algorithms and consensus problems
- Understand various asynchronous shared memory algorithms and asynchronous network algorithms with the help of I/O automata.
- Understand partially synchronous algorithms

MODULE 1

MODULE 2

MODULE 3

References

1. Distributed Systems. S. Mullender (ed.). Addison-Wesley, 1993

Structure of the Question paper
For the End Semester Examination the question paper will consist of at least 50% analytical/design problems. There will be three questions from each module (with subdivisions) out of which two question are to be answered by the students.
Course Objectives

- To understand various techniques and metrics to assess the information security.

Learning Outcomes

- The student become aware of various security metrics

MODULE 1

Why we measure security? Why security metrics are needed? Modeling security metrics, Decide what to measure, Identify core Competencies, Information security work, and resourcing options, Identify targets, good and bad metrics, State of IT security metrics, Diagnosing problems and measuring technical security, Measuring program effectiveness

MODULE 2

Analysis techniques, Mean, Median, Standard Deviation, Grouping and Aggregation, Time series analysis, Cross sectional analysis, Quartile analysis, Correlation matrices, Visualization, Design principles, Stacked bar charts, Waterfall charts, Time series charts, Bivariate charts, Matrices, Tables, Treemaps, Automatic metric calculations, Automation benefits, Technical requirement for automation software, Data model, Data sources and sinks, Data interfaces, Metrics program management, Security process management framework (SPM), Security measurement project (SMP), Practical examples of SMP

MODULE 3

Designing security score cards, Balanced score card, Creating balanced security score card, Organizational consideration for balanced security card, Security metrics for cloud computing, Explore how to take a security metrics program and adapt it strategically to a variety of organizational contexts and environments

References:


Structure of the Question paper
For the End Semester Examination the question paper will consist of at least 40% analytical/design problems. There will be three questions from each module (with subdivisions) out of which two question are to be answered by the students.
Stream Elective 4

RIE 3004
CYBER FORENSICS & INVESTIGATION

Lecture : 3 hrs/ Week  Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
- To provide basic understanding of principles, tools and techniques involved in investigation of cyber crimes.

Learning Outcomes
- The student gets a reasonable understanding of the forensic and investigation techniques in cyber-related crimes and gains ability to apply them in practical scenarios.

MODULE 1

MODULE 2

MODULE 3

References:

Structure of the Question paper
For the End Semester Examination the question paper will three questions from each module (with sub-divisions) out of which two questions are to be answered by the students.
Stream Elective 4

RIE 3005
ADVANCED TOPICS IN INFORMATION SECURITY

Lecture : 3 hrs/ Week  Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives

• To impart a deeper understanding, beyond the fundamentals, of various aspects of information security.

Learning Outcomes

• The student gains knowledge in advanced aspects of information security.

MODULE 1
Embedded system security, Embedded security trends, Core Embedded Operating System Security Requirements, Secure embedded software, Embedded cryptography, Key management for embedded systems, Data protection protocols for embedded systems, Data in motion protocols, Data at rest protocols, Automotive security, Secure android.

MODULE 2

MODULE 3
Cloud computing, framework for cloud computing, relevant technologies in cloud computing, service models, cloud deployment model, key drivers to adopting the cloud, the impact of cloud computing on users, Examples of cloud service providers, Security management in the cloud - availability management, access control, security vulnerability, patch and configuration management, key privacy concerns in the cloud, legal and regulatory implications.

References:


Structure of the Question paper
For the End Semester Examination the question paper will three questions from each module (with sub-divisions) out of which two questions are to be answered by the students.
Stream Elective 4

RIE 3006
NETWORK PERIMETER SECURITY

Lecture : 3 hrs/ Week  Credits : 3
Internal Continuous Assessment : 40 Marks
End Semester Examination : 60 Marks

Course Objectives
• To familiarize and gain deeper knowledge about the various concepts and techniques of securing networks

Learning Outcomes
• The student understands the various challenges faced in securing networks and learns about the approaches to overcome the same

Module 1

Module 2

Module 3
Maintaining a security parameter system and network monitoring. Network log analysis network log files, log analysis, router logs, network firewall logs, host based firewall and IDS logs. Troubleshooting defence analysis, assessment techniques.

References:
Structure of the Question paper
For the End Semester Examination the question paper will consist of three questions from each module (with sub-divisions) out of which two questions are to be answered by the students.