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

Code No.	Name of Subject	Credits	Hrs / week	End Sem Exam (Hours)	Marks			Remarks
					Internal Continuous Assessment	End Semester Exam	Total	
RCC 1001	Mathematical Foundations of Computer Science	3	3	3	40	60	100	End-of-Semester Exam by University
RIC 1001	Foundations of Information Security	3	3	3	40	60	100	-do-
RCC 1002	Topics in Database Technology	3	3	3	40	60	100	-do-
RCC1003	Advanced Data Structures and Algorithms	3	3	3	40	60	100	-do-
RCC 1004	Advanced Software Engineering	3	3	3	40	60	100	-do-
RIC 1002	Number Theory and Cryptography	3	3	3	40	60	100	-do-
RIC 1101	Seminar	2	2	-	100	-	100	No End-of-sem Exam
RIC 1102	Secure Computing Laboratory - I	1	2	-	100	-	100	-do-
	TOTAL	**21**	**22**	**18**	**440**	**360**	**800**	

Semester 2

Code No.	Name of Subject	Credits	Hrs / week	End Sem Exam hours	Marks			Remarks
					Internal Continuous Assessment	End Semester Exam	Total	
RIC 2001	Formal Methods in Secure Computing	3	3	3	40	60	100	End-of-Semester Exam by University
RIC 2002	Network Security	3	3	3	40	60	100	-do-
*	Elective -1(Stream Elective)	3	3	3	40	60	100	-do-
*	Elective -II (Stream Elective)	3	3	3	40	60	100	-do-
*	Elective -III (Department Elective)	3	3	3	40	60	100	-do-
	Research Methodologies	2	2	3	40	60	100	-do-
RCC 2000	Research Methodology	2	2	3	40	60	100	-do-
RIC 2101	Seminar	2	2	-	100	-	100	No End-of-sem Exam
RIC 2102	Thesis Preliminary-Part I	2	2	-	100	-	100	-do-
RIC 2103	Secure Computing Laboratory - II	1	2	-	100	-	100	-do-
	TOTAL	**22**	**23**	**18**	**540**	**360**	**900**	

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		**Stream Elective 2**	
RIE 2001	Database Security	RIE 2004	Web Security Testing
RIE 2002	Access Networks and Cellular Communication	RIE 2005	Public Key Infrastructure & Trust Management
RIE 2003	Biometric Authentication	RIE 2006	Information Theory & Coding

* The student has to choose Elective 1, El 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

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

Electives for Semester 3:

Stream Elective 3		**Stream Elective 4**	
RIE 3001	Information Security Policies & Risk Analysis	RIE 3004	Cyber Forensics & Investigation
RIE 3002	Distributed Algorithms	RIE 3005	Advanced Topics in Information Security
RIE 3003	Information Security Metrics	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.

Semester 4

Code No.	Name of Subject	Credits	Hrs / week	*Evaluation(Marks)*				
				Internal		**External**		**Total**
				Sessional	**Guide**	**Thesis**	**Viva Voce**	
RIC4101	Thesis-Final	12	21	150	150	200	100	600
	TOTAL	**12**	**21**	**150**	**150**	**200**	**100**	**600**

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

Fundamental principles of counting, pigeonhole principle, countable and uncountable sets, principle of inclusion and exclusion – applications, derangements, permutation and combination, Pascal's triangles, binomial theorem, Probability theory – Properties of Probability, Methods of Enumeration, Conditional Probability, Independent Events, Bayes Theorem, Mathematical Expectation, Random variables Discrete Distribution, Binomial Distribution, Mean and variance The Poisson Distribution, Continuous Distribution. Uniform and Exponential Distributions, Normal Distribution

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

1. J. P. Tremblay, R. Manohar, "Discrete Mathematical Structures with Application to Computer Science", Tata McGrawHill, 2000
2. Kenneth H. Rosen, "Discrete Mathematics and its Applications", 7/e, McGraw Hill Inc, 2011
3. Richard Johnson, "Probablity and Statistics for Engineers", 7/e, Prentice-Hall India Private Limited, 2005
4. Robert V. Hogg, Elliot A. Tanis, Meda J. M. Rao, "Probability and Statistical Inference", 7/e,, Pearson Education India, 2006
5. Michael Huth, Mark Ryan "Logic in Computer Science", 2/e, Cambridge University Press, 2004.
6. J. Truss, "Discrete Mathematics for Computer Scientists", 2/e, Addison Wesley, 1999.
7. Bernard Kolman, Robert C Busby,Sharon Kutler Ross, "Discrete Mathematical Structures", 2/e, Prentice-Hall India Private Limited, 1996.

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 scecurity

Learning Outcomes

- Conceptual understanding of the principles of information security, its significance and the domain specific security issues.

MODULE 1

Security Models as basis for OS security, Introduction to DB Security, Software vulnerabilities Buffer and stack overflow, Phishing. Malware Viruses, Worms and Trojans. Topological worms. Internet propagation models for worms. Cryptography Topics: Cryptographic hash SHA1, Discrete Log Diffie Helman, Digital certificates. Steganography watermarking.

MODULE 2

*Protocol topics: One way and two w*ay authentication, NeedhamSchroeder protocol, Kerberos basics, Biometrics for authentication. Network security topics: Network layer security – IPSec – overview, IP and IPv6, AH, ESP. Transport layer security SSL. Attacks DoS, DDoS, ARP spoofing - firewalls.

MODULE 3

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

References:

1. Bernard Menezes, "Network security and Cryptography", Cengage Learning India, 2010.
2. Behrouz A. Forouzan, "Cryptography and Network Security", Special Indian Edition, Tata McGraw Hill, 2007
3. William Stallings, "Cryptography and Network Security: Principles and Practice", 6/e Pearson Education, 2013.
4. Dieter Gollmann. "Computer Security", John Wiley and Sons Ltd., 2006.
5. Whitman and Mattord, "Principles of Information Security", Cengage Learning, 2006.
6. D. Bainbridge, "Introduction to Computer Law", 5/e, Pearson Education, 2004.
7. C. Kaufman, R. Perlman and M. Speciner, "Network Security: Private Communication in a public World", 2/e, Prentice Hall, 2002.
8. W. Mao, "Modern Cryptography: Theory & Practice", Pearson Education, 2004.
9. H. Delfs and H. Knebl, "Introduction to Cryptography: Principles and Applications", Springer Verlag, 2002.

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

Query Processing Algorithms – Query Optimization Techniques – Transaction Management: Transaction Processing Concepts - Concurrency Control – Deadlocks – Recovery Techniques – Database Security.

Database System Architectures: Centralized and Client-Server Architectures – Server System Architectures – Parallel Systems- Distributed Systems – Parallel Databases: I/O Parallelism – Inter and Intra Query Parallelism – Inter and Intra operation Parallelism – Distributed Database – Functions – Distributed RDB design- Transparency– Distributed Transactions - Commit Protocols – Concurrency Control –Deadlocks – Recovery - Distributed Query Processing .

MODULE 2

Concepts for Object Databases: Object Identity – Object structure – Type Constructors – Encapsulation of Operations – Methods – Persistence – Type and Class Hierarchies – Inheritance – Complex Objects Object Relational Systems – Case studies : Oracle and Informix, Postgres.

Web Technology and Databases – Structure of Web pages – HTTP and HTML. Scripting Languages: Javascript, VbScript, PHP – CGI and API – Database Connectivity – JDBC and SQLJ JSP, ASP, JWS and OracleAS – Semi-structured Data and XML Databases: XML Data Model – DTD - XML Schema – XPath and XQuery – Example Queries. Storing XML in databases - RDF (Fundamental Concepts only).

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

1. R. Elmasri, S.B. Navathe, "Fundamentals of Database Systems", 5/e, Pearson Education/Addison Wesley, 2011
2. Patrick O'Neil , Elizabeth O'Neil , "Database: Principles, Programming and Performance", 2/e, Morgan Kaufmann, 2011
3. Thomas Cannolly and Carolyn Begg, "Database Systems, A Practical Approach to Design, Implementation and Management", 3/e, Pearson Education, 2010.
4. Henry F Korth, Abraham Silberschatz, S. Sudharshan, "Database System Concepts", 5/e, Tata McGraw Hill, 2006.
5. C.J. Date, A.Kannan and S. Swamynathan,"An Introduction to Database Systems", 8/e, Pearson Education India, 2006.
6. Joe Fawcett, Danny Ayers , Liam R. E. Quin, Beginning XML, 5/e, John Wiley & Sons, 2012
7. Grigoris Antoniou. Frank van Harmelen, "A Semantic Web Primer", The MIT Press, Cambridge, Massachusetts, 2003
8. Jules J. Berman, "Principles of Big Data: Preparing, Sharing and Analyzing Complex Information", Morgan Kufmann, 2013.
9. Pete Warden, "Big Data Glossary", O'Reilly Media Inc, 2011

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

Overview of basic data structures. Amortized Analysis – aggregate , accounting, potential methods. Advanced data structures: binomial heap, fibonacci heap, disjoint sets, Weight-balanced trees, min-max heaps, treaps – analysis of associated algorithms, applications.

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

Probabilistic algorithms: basics of probability theory, pseudorandom generators, Numerical algorithms, integration, counting, Monte-Carlo algorithms - verifying matrix multiplication, min-cut in a network. Las Vegas algorithms – eight-queens problem, selection, quicksort, universal hashing, Dixon's factorization

Geometric Algorithms: Plane sweep technique, role of ***sweep- line - status*** and ***event-point-schedule***, line segment intersection problem. Convex Hull : Graham's scan algorithm, Jarvis march algorithm. Finding closest pair of points, proof of correctness.

MODULE 3

Number-Theoretic algorithms: GCD algorithm, modular arithmetic, primality testing, Miller-Rabin test, Integer factorization - Pollard Rho heuristic.

Matrix algorithms: multiplication, decomposition, inversion. String matching: Rabin-Karp, Knuth-Morris-Pratt algorithms.

Overview of Complexity classes – P, NP, Co-NP, NP-hard, NP complete. Space complexity. Complexity classes in randomized algorithms – RP, PP, ZPP, BPP.

References:

1. T. H. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein, "Introduction to algorithms", Prentice-hall of India Private Limited, New Delhi, 2010.

2. Sartaj Sahni, "Data Structures, Algorithms, and Applications in C++", Mc-GrawHill, 1999.
3. Gilles Brassard and Paul Bratley, "Fundamentals of algorithms", Prentice-hall of India Private Limited, New Delhi, 2001.
4. R.C.T. Lee, S.S. Tesng, R.C. Cbang and Y.T. Tsai "Design and Analysis of Algorithms, A strategic Approach", TMH, 2010
5. Rajeev Motwani, Prabhakar Raghavan, "Randomized Algorithms", Cambridge University Press, 2000.
6. Dexter C. Kozen, "The Design and Analysis of Algorithms", Springer.
7. Jon Kleinberg and Eva Tardos, "Algorithm Design", Pearson Education, 2006.
8. M. H. Alsuwaiyal, "Algorithms Design Techniques and Analysis", World Scientific Publishing Co. Beijing, 1999.
9. S. K. Basu, "Design Methods and Analysis of Algorithms", Prentice Hall India, 2005.

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 sub-divisions) 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

Introduction: Role of Software Engineer- Quality of software process and product – Systems Approach to Software Engineering – An Engineering Approach to Software Engineering – How has Software Engineering Changed? Modeling the Process and Life Cycle – Software Process Models – Waterfall Model – V Model - Prototyping Model – Spiral Model – Agile methods – Tools and Techniques for Process Modeling – Planning and Managing the Project - Tracking project progress - Project personnel and organization – Effort and schedule estimation - Risk Management – Process Models and Project Management .

MODULE 2

Capturing the Requirement – Eliciting Requirements – Modelling requirements – Reviewing requirements to ensure quality – Documenting requirements – Designing the architecture – Views of Software Architecture – Common Architectural Patterns – Architecture Evaluation and Refinement Criteria for evaluating and comparing design alternatives – Software architecture documentation - Designing Modules – Design Methodology – Design Principles – Object Oriented (OO) design – Representing designs using UML – OO Design Patterns - OO Measurement - Design Documentation Programming Standards and Procedures – Programming Guidelines – Documentation.

MODULE 3

Testing the Programs - Principles of System Testing - Function Testing - Performance Testing – Reliability - Availability and Maintainability - Basics of reliability theory - The Software Reliability Problem - Parametric reliability growth models - Predictive accuracy - The recalibration of software- reliability growth predictions - Acceptance Testing - Installation Testing - Automated System Testing - Test Documentation - Testing Safety Critical Systems -Maintaining the System – Evaluating Products, Processes, and Resources.

References:

1. Shari Lawrence Pfleeger, Joanne M Atlee, "Software Engineering Theory and Practice", 4/e, Pearson Education, 2011.
2. Software Engineering: A Practitioner's Approach, Roger S Pressman, 7/e,. McGraw Hill Int.Ed., 2010.

3. Ian Somerville, "Software Engineering", 8/e, Addison-Wesley 2007
4. Carlo Ghezzi, Mehdi Jazayeri, Dino Mandrioli, "Fundamentals of Software Engineering", 2/e, PHI Learning Private Ltd., 2010
5. Pankaj Jalote, "An Integrated Approach to Software Engineering", 3/e, Springer 2005.
6. K.K Aggarwal & Yogesh Singh, "Software Engineering", New Age International 2007.
7. Norman E Fenton, Shari Lawrence Pfleeger, "Software Metrics: A Rigorous and Practical Approach. 1998

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.

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 cryptoraphic algorithms and 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 ϕ 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

Public key Cryptosystems: RSA proof and its correctness- security of RSA- attacks , Modular Exponentiations, Rabin and El Gammal Crypto systems – elliptic curve cryptography, Knapsack cryptosystem, Diffie-Hellman key exchange-man-in-the middle attack, Message Authentication – Digital Signature algorithms. Factorization, Factorization methods- Pollard rho method, Pollard $p - 1$ Algorithm, Zero knowledge proof -Fiat Shamir protocol.

References

1. Ivan Niven, Herbert S. Zuckerman and Hugh L. Montgomery, "An Introduction to the Theory of Numbers", 5/e, Wiley India, New Delhi, 2008.
2. C. Kaufman, R. Perlman and M. Speciner, "Network Security: Private Communication in a public World", 2/e, Prentice Hall, 2002.

3. William Stallings, "Cryptography and Network Security", 4/e, Pearson Education India, 2006.
4. Joachim Gathan, Jurgen Gerhard, "Modern Computer Algebra", 2/e, Cambridge University Press, 2003.
5. Wenbo Mao, "Modern Cryptography: Theory & Practice", 1/e, Pearson Education India, 2006.
6. Neal Koblitz, "Course on Number Theory and Cryptography", 2/e, Springer, 2004.
7. Neal Koblitz, "Algebraic Aspects of Cryptography", SpringerVerlag, 2004.

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.

RIC1101
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 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

Object oriented, Resource allocation monitor models. Security protocols, security properties, public key certificates, digital signatures, protocol vulnerabilities, limits of formal analysis. Modeling security protocols trustworthy processes, data types for protocol models, modeling an intruder.

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:

1. Peter Ryan, Steve Schneider, M. H. Goldsmith, "Modelling and Analysis of Security Protocols", Pearson Education, 2010.
2. Theo Dimitrakos, Fabio Martinelli, "Formal Aspects In Security And Trust: Ifip TN Wg1.7", Workshop on Formal Aspects in Security, Springer, 2005.
3. W. Mao, "Modern Cryptography: Theory & Practice", Pearson Education, 2004.
4. Giampaolo Bella, "Formal Verification of Security Protocols", Springer, 2007.
5. Colin Boyd, Anish Mathuria, "Protocols for Authentication and Key Establishment", Springer, 2003.
6. Giampaolo Bella, "Formal Correctness of Security Protocols (Information Security and Cryptography)", Springer, 1e, 2007.

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

Introduction: Security trends, security attacks, security mechanisms, Network Security model, Review of intrusion detection systems. Review of cryptographic algorithms and protocols: cryptanalysis, Message authentication, secure hash functions, Digital signatures. Standards: Kerberos v4 – configuration, authentication, encryption, message formats. Kerberos v5 – cryptographic algorithms, message formats. PKI – trust models, revocation. Real-time communication security, IPSec overview, AH, ESP, IKE – phases.

MODULE 2

Email security, Security services for Email, establishing keys, privacy, authentication, message integrity. PEM & S/MIME – structure of messages, encryption, source authentication and integrity protection, message formats. PGP encoding, anomalies, object formats. Web security: Web security considerations, SSL/TLS – attacks, exportability, encoding. Secure electronic transaction.

MODULE 3

Network management security: SNMP, Basic concepts of SNMPv1, SNMPv3. Wireless security: Wireless LAN Specifications. Wireless network security stack, WEP. Firewalls: Firewall design principles, trusted systems, packet filters, application level gateways, encrypted tunnels.

References:

1. C. Kaufman, R. Perlman and M. Speciner, "Network Security: Private Communication in a Public World", 2/e, PHI, 2002.
2. W. Stallings, "Cryptography and Network Security Principles and practice", 3/e, Pearson Education Asia, 2003.
3. William Stallings, "Network Security Essentials", 2/e, Prentice Hall, 2003.
4. Schiller J., "Mobile Communications", Pearson Education Asia, 2/e, 2009.

5. Roberta Bragg et. al., "Network Security: The Complete Reference", TMH, 2008.

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.

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

Research design and methods: Research design - Basic Principles- Need for research design — Features of a good design. Important concepts relating to research design: Observation and Facts, Laws and Theories, Prediction and explanation, Induction, Deduction. Development of Models and research plans: Exploration, Description, Diagnosis, Experimentation and sample designs. Data Collection and analysis: Execution of the research - Observation and Collection of data - Methods of data collection - Sampling Methods- Data Processing and Analysis strategies - Data Analysis with Statistical Packages - Hypothesis-Testing -Generalization and Interpretation.

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:

1. C.R Kothari, Research Methodology, Sultan Chand & Sons, New Delhi,1990.
2. Panneerselvam, "Research Methodology", Prentice Hall of India, New Delhi, 2012.
3. J.W Bames," Statistical Analysis for Engineers and Scientists", McGraw Hill, New York.
4. Donald Cooper, "Business Research Methods", Tata McGraw Hill, New Delhi.
5. Leedy P D, "Practical Research: Planning and Design", MacMillan Publishing Co.
6. Day R A, "*How to Write and Publish a Scientific Paper*", Cambridge University Press, 1989.
7. Manna, Chakraborti, "Values and Ethics in Business Profession", Prentice Hall of India, New Delhi, 2012.
8. Sople,"Managing Intellectual Property: The Strategic Imperative", Prentice Hall of India, New Delhi, 2012.

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

The experiments are based on the topics related to security covered in the semester, particularly those in *RIC 2001: Formal Methods in Secure Computing* and *RIC 2002: Network Security*.

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

Similarity measures, Bayes Theorem, Classification -regression, Bayesian classification, Decision tree based algorithm-ID3, Neural network based algorithm- supervised learning, back propagation, gradient-descent algorithm, Rule based algorithm-IR, PRISM, Clustering algorithm – Hierarchical algorithm –Dendrograms- Single link algorithm, Partitional algorithm-Minimum spanning tree, squared error, K-means, PAM algorithm.

MODULE 3

Association Rules : Apriori algorithm, Sampling algorithm, Partitioning algorithm, Parallel and distributed algorithms, Web mining-web content mining, web structure mining, web usage mining, Spatial mining- spatial queries, spatial data structures, Generalization and specialization, spatial classification, spatial clustering, Introduction to temporal mining.

References:

1. Margaret H Dunham, "Data Mining – Introductory and Advanced Topics", Pearson India, 2005.
2. Ian H. Witten, Eibe Frank, Mark A. Hall," Data Mining: Practical Machine Learning Tools and Techniques", 3/e, Morgan Kaufmann, 2011.
3. J. Han, M. Kamber, "Data Mining: Concepts and Techniques", 2/e, Morgan Kaufman,

2006.

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 Assurance Framework and Standards SQA Framework: Software Quality Assurance, Components of Software Quality Assurance Software Quality Assurance Plan: Steps to develop and implement a Software Quality Assurance Plan â€“ Quality Standards: ISO 9000 and Companion ISO Standards, CMM, CMMI, PCMM, Malcom Balridge, 3 Sigma, 6 Sigma

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

Software Testing Tools Taxonomy of Testing tools, Methodology to evaluate automated testing tools, Load Runner, Win runner and Rational Testing Tools, Java Testing Tools, JMetra, JUNIT and Cactus.

Testing Process Eleven Step Testing Process: Assess Project Management Development Estimate and Status, Develop Test Plan, Requirements Phase Testing, Design Phase Testing, Program Phase Testing, Execute Test and Record Results, Acceptance Test, Report test results, testing software installation, Test software changes, Evaluate Test Effectiveness.

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

References:

1. William E. Perry, "Effective Methods for Software Testing", 2/e, Wiley
2. Mordechai Ben Menachem, Garry S. Marliss, "Software Quality", Thomson Learning

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 modelling and simulation of various genre of systems.
-

MODULE 1

Types of evaluation strategies (experimentation, simulation, and modelling). Modelling: Types of modelling (physical and analytical). Analytical Modelling (queueing theory): Single server and multiple server model. Case studies from Operating systems, Computer Networks, Computer Organization. Operational Laws, Asymptotic Analysis, Bounds on System throughput and response time. Balanced bound analysis, Mean-value analysis (MVA), Approximate-MVA, Convolution Algorithm. Limitations of analytical modelling (queueing theory). Simulation: Types of simulation. Advantages and limitations. Discrete event simulation: Simulation of single server, two servers connected in series, and servers in parallel.

MODULE 2

Modelling arrival time/service time/inter-arrival time of jobs using probability distributions (random variables). Introduction to random variables: random number generation, uniform random number generation, random variables, expectation, variance. Generation of non-uniform random variables: Bernoulli, Binomial, Poisson, Geometric, Exponential, Negative binomial, and Pascal. CS applications of each random variables. Poisson process, homogeneous/non-homogeneous poisson processes. Random variate generation. Inverse transformation method, rejection method.

MODULE 3

Analysis of simulation results. Introduction to MATLAB/Sci-LAB. Methods for curve fitting. Numerical method techniques for root finding, solving linear equations.

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:

1. Ross, Simulation, Academic Press, 2002. Chapters 1-6.
2. Raj Jain, The art of computer systems performance analysis, John Wiley and Sons 1991. Chapters 1,2,3, 30-35, 24-29.
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, Non binary Huffman Algorithms, Adaptive Coding, applications,Arithmetic Coding,applications, Finite Context Modeling.

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 York. 2000.
2. Stephen Welstead, Fractal and wavelet Image Compression techniques , PHI, 1999.
3. Khalid Sayood, Introduction to data compression, Morgan Kaufmann Publishers, 2003.
4. Sleinreitz ―Multimedia System‖ Addison Wesley.

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

1. D. Bainbridge, *Introduction to Computer Law*, 5/e, Pearson Education, 2004.
2. Harish Chander, *Cyber Laws and IT Protection*, PHI Learning Private Limited, 2012.
3. P. Duggal, *Cyber law: the Indian Perspective*, Saakshar Law Publications, Delhi, 2005.
4. C. P. Fleeger and S. L. Fleeger, *Security in Computing*, 3/e, Pearson Education, 2003.

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

Definition of Distributed System, Goals, Types of Distributed Systems, System Architecture : Centralized, Decentralized & Hybrid Architecture. Processes: Threads, Virtualization, Clients, Servers, Code migration. Communication: Message Oriented, Stream Oriented and Multicast Communication.

Naming**:** Names, Identifiers and Addresses, Flat Naming, Structured Naming and Attribute Based Naming. Consistency and Replication: Reasons for Replication, Data Centric and Client Centric Consistency Models, Replica Management, Consistency Protocols. Distributed Object Based Systems: Architecture, Processes, Communication, Naming, Synchronization, Consistency and Replication, Fault Tolerance, Security.

MODULE 2

Distributed Algorithms: Models of Distributed Computation, Preliminaries, Causality, Distributed Snapshots, Modeling a Distributed Computation, Failures in a Distributed System. Algorithms in General Synchronous Networks: Leader Election, Breadth First Search, Minimum Spanning Tree, Shortest Path, Maximal Independent Set.

MODULE 3

Hadoop: Introduction, Comparison with Other Systems. Analyzing Data with Hadoop- Map and Reduce, Scaling Out: Data Flow, Combiner Functions, Running a Distributed Map Reduce Job. Map Reduce Types and Formats, Features. Hadoop Distributed File System: Concepts and Basic Operations. Administering Hadoop.

References:

1. Andrew S. Tanenbaum, Maarten Van Steen." Distributed Systems – Principles and Paradigms ", 2/e, PHI, 2004.
2. Randy Chow Theodore Johnson, "Distributed Operating Systems and Algorithm Analysis", Pearson Education, 2009.

3. Nancy A. Lynch, Morgan," Distributed Algorithms", Kaufmann Publishers, Inc, 1996.
4. Tom White, "Hadoop: The Definitive Guide", 1/e, O'reilly, 2012.

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

Cloud Computing – History of Cloud Computing – Cloud Architecture – Cloud Storage – Why Cloud Computing Matters – Advantages of Cloud Computing – Disadvantages of Cloud Computing – Companies in the Cloud Today – Cloud Services Web-Based Application – Pros and Cons of Cloud Service Development – Types of Cloud Service Development – Software as a Service – Platform as a Service – Web Services – On-Demand Computing – Discovering Cloud Services Development Services and Tools – Amazon Ec2 – Google App Engine – IBM Clouds.

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

Collaborating on Calendars, Schedules and Task Management – Exploring Online Scheduling Applications – Exploring Online Planning and Task Management – Collaborating on Event Management – Collaborating on Contact Management – Collaborating on Project Management – Collaborating on Word Processing - Collaborating on Databases – Storing and Sharing Files. Collaborating via Web-Based Communication Tools – Evaluating Web Mail Services – Evaluating Web Conference Tools – Collaborating via Social Networks and Groupware – Collaborating via Blogs and Wikis.

References

1. Dan C. Marinescu , Cloud computing: Theory and Practice, Morgan Kaufmann, 2013
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
3. Michael Miller, Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online, Que Publishing, 2008.

4. Haley Beard, Cloud Computing Best Practices for Managing and Measuring Processes for Ondemand Computing, Applications and Data Centers in the Cloud with SLAs, Emereo Pty Limited, 2008.

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:

1. Bhavani Thuraisingham, “Database and Applications Security”, Auerbach Publications, 2005.
2. Rose Anderson, “Security Engineering: A Guide to Building Dependable Distributed Systems”, John Wiley & Sons, 2001.
3. Michael Gertz, Sushil Jajodia, "Handbook of Database Security Applications and Trends", Springer, 2008.
4. Ron Ben Natan, "Implementing Database Security and Auditing”, Elsevier, 2005.
5. Silvana Castano, “Database Security”, ACM Press.
6. Alfred Basta, Melissa Zgola, “Database Security”, Cengage Learning,

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

Mobile Radio Propagation-Propagation Models, Propagation Mechanisms, Path Loss models, Small scale Multipath Propagation, Parameters of Mobile Multipath Channels , Rayleigh and Ricean Distributions, level crossing and fading statistics. Wireless Communication Systems and Standards, WLL, PACS, cellular data services, satellite base wireless systems.

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

Optical Access Networks: PON Architecture, Broadband PON, Gigabit capable PON, Ethernet PON, Next generation optical access network, WDM-PON components and Network Architecture, Hybrid TDM/WDM PON, WDM-PON protocol and Scheduling algorithm. Hybrid optical wireless access networks: Technologies, architecture, routing algorithm.

References

1. T.S.Rappaport, "Wireless Communications: Principles and Practice", 2/e, Pearson Education, 2003.
2. W.C.Y.Lee, "Mobile Communications Engineering: Theory and Applications", 2/e, McGraw-Hill International, 1998.
3. Andreas F.Molisch, "Wideband Wireless Digital Communications", Pearson Education, 2001.

4. R. Blake, “Wireless Communication Technology”, Thomson Delmar, 2003.
5. Leonid G. Kazovsky, Ning Cheng, Wei-Tao Shaw, David Gutierrez, Shing-Wa Wong “Broadband Optical Access Networks”, Wiley.

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:

1. Anil K. Jain, Arun A. Ross, Karthik Nandakumar, "Introduction to Biometrics", Springer, 2011
2. Jain, P. Flynn, A. Ross, "Handbook of Biometrics" Springer. .2008
3. John R. Vacca, "Biometric Technologies and Verification Systems", Elsevier, 2007

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:

1. Paco Hope, Ben Walther, "Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast", O'REILLY media, 2009.
2. Steven Splaine, "Testing Web security: assessing the security of Web sites and applications", Wiley Publishing, 2002.
3. T. J. Klevinsky, Scott Laliberte, Ajay Gupta, "Hack I.T.: security through penetration testing", Pearson Education, 2002.
4. Mike Andrews, James A. Whittaker, "How to Break Web Software", Pearson Education, 2006.

5. David MacKey, “Web Security: For Network and System Administrators”, Cengage Learning, 2006.

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

Overview of PKI technology- Basic Security Concepts, Components of PKI-Working with PKI - Processes in PKI ,PKI architecture – Single CA Architecture-Enterprise PKI-Hybrid PKI, Work Performed by Certificate Authorities- Issuing Certificates-Revoking Certificates-Formulating a Certificate Policy-CPS- Attacks on CA- External and Internal Attacks-Protecting the CA root key from attacks

MODULE 2

Certificate Management – Certificate Enrollment and Registration Authority-Maintaining keys and Certificates- Certificate retrieval and validation-methods of certificate revocation-PKI Management protocols and standards- PKCS#10,PKCS#7-Certificate Management Protocol-Simple Certificate Enrollment Protocol-X Series Standards

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:

1. Suranjan Choudhary,Karthik Bhatnagar,Wasim Haque, "Public Key Infrastructure Implementation and Design", M & T Books, New York 2002.
2. JeanMarc Seigneur, Adam Slagell, "Collaborative Computer Security and Trust Management", Information Science Reference, New York (IGI Global), 2010.
3. John R. Vacca, "Public Key Infrastructure", Auerbach publications, New york, 2004.
4. Klaus Schmeh, "Cryptography and Public Key Infrastructure on the Internet", Allied Publishers, 2004.
5. Carlisle Adams, Steve Lloyd, "Understanding PKI: Concepts, Standards, and Deployment Considerations", Addison Wesley, 2003.

6. Kapil Raina, “PKI Security Solutions for the Enterprise”, Wiley, 2003.
7. Brian Komar, "Windows Server 2008 PKI and Certificate Security", Microsoft Press, 2008.
8. W. Mao, “Modern Cryptography: Theory & Practice”, Pearson Education, 2004.

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:

1. Thomas M. Cover, Joy A. Thomas, "Elements of Information Theory", 2/e, Wiley – Interscience, 2006
2. A. Neubauer, J. Freudenberger, V. Kuhn, "Coding Theory: Algorithms, Architectures and Applications", John Wiley India, 2012.
3. Shu Lin, Daniel J. Costello Jr., "Error Control Coding: Fundamentals and 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

Risk analysis: Introduction, risk management, risk assessment process – threat identification, quantitative and qualitative risk assessment, hazard impact analysis, questionnaires.

MODULE 3

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

References:

1. Thomas R. Peltier, “Information Security Policies and Procedures”, 2/e, Auerbach Publication, New york, 2004.
2. Thomas R. Peltier, “Information Security Risk Analysis”, 2/e, Auerbach Publication, New york, 2005.
3. Mariagrazia Fugini, Carlo Bellettini, "Information SecurityPolicies and Actions in Modern Integrated Systems”, Idea Group Publishing, 2004.
4. Detmar W. Straub, Seymour Goodman, Richard Baskerville, “Information Security: Policy, Processes, and Practices”, M.E. Sharpe, 2008.
5. Evan Wheeler, "Security Risk Management: Building an Information Security Risk Management Program from the Ground Up", Syngress, 2011.
6. Douglas J. Landoll, “The Security Risk Assessment Handbook”, 2/e, Taylor & Francis Group, CRC Press.
7. W. Mao, “Modern Cryptography: Theory & Practice”, Pearson Education, 2004.

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

Synchronous Network Algorithm: Synchronous Network Model, Leader election in a synchronous ring, Algorithms in General Synchronous Networks- Flooding algorithm – Breadth First Search – Shortest Paths- Minimum Spanning Tree – Maximal Independent Algorithm- Distributed consensus with link failures.

MODULE 2

Asynchronous Algorithms: Asynchronous System model - I/O automata- Operations on automata – Fairness – Inputs and outputs for problems – Properties and proof methods.
Asynchronous Shared Memory Algorithms: Asynchronous Shared Memory Model, Mutual Exclusion – Dijkstra's Mutual Exclusion algorithm – Lock out free Mutual Exclusion algorithms, Mutual Exclusion using Read – Modify - Write Variables - TicketME algorithm, Resource allocation, Consensus.

MODULE 3

Asynchronous Network Algorithms: Asynchronous Network Model, Basic asynchronous network algorithms, synchronizers -The Local synchronizer – The safe synchronizer – Implementations - Applications.
Partially synchronous algorithms – MMT Timed automata – General Timed automata – Basic Definitions and operations – Transforming MMT automata into General Timed Automata.

References

1. Distributed Systems. S. Mullender (ed.). Addison-Wesley, 1993
2. Distributed Algorithms. N. Lynch. Morgan Kaufmann, 1996

3. Introduction to Distributed Algorithms. G. Tel. Cambridge Univ. Press, 2000.

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 question are to be answered by the students.

Stream Elective 3

RIE3003
INFORMATION SECURITY METRICS

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

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:

1. Andrew Jaquith, "Security Metrics: Replacing Fear, Uncertainty, and Doubt", 1/e, Addison-Wesley Professional, 2007.
2. Caroline Wong, "Security Metrics, A Beginner's Guide", 1/e, McGraw-Hill Osborne Media, 2011.
3. Lance Hayden, "IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data", 1/e, McGraw-Hill Osborne Media, 2010.
4. Carl Young, "Metrics and Methods for Security Risk Management", 1/e, Syngress, 2010.

5. W. Krag Brotby CISM, "Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement", 1/e, Auerbach Publications, 2009.
6. Douglas Landoll, "The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments", 2/e, Second Edition

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 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

Cyber Forensic Tools and Utilities, Concealment Techniques, Digital Forensic Laboratory Accreditation Standards, Performing a Cyber Forensic Investigation Flowchart for the Seizure of Electronic Evidence and Associated Internal Control Questionnaire , Privacy and Cyber Forensics, Forensic Value and Corporate Exposure, Cyber Forensics and the Law: Legal Considerations, Cyber-Forensics and the Changing Face of Investigating Criminal Behavior, Electronically Stored Information and Cyber Forensics.

MODULE 2

Protocol Analysis, Packet Analysis, Flow Analysis, Higher-Layer Traffic Analysis, Statistical Flow Analysis, Process Overview , Sensors , Flow Record Export Protocols, Collection and Aggregation, Analysis 17, Wireless: Network Forensics, The IEEE Layer 2 Protocol Series, Wireless Access Points (WAPs), Wireless Traffic Capture and Analysis , Common Attacks, Locating Wireless Devices, Network Intrusion Detection and Analysis, Why Investigate NIDS/NIPS? Typical NIDS/NIPS Functionality, Modes of Detection, Types of NIDS/NIPSs , NIDS/NIPS Evidence Acquisition, Comprehensive Packet Logging , Snor.

MODULE 3

Event Log Aggregation, Correlation, and Analysis , Sources of Logs, Network Log Architecture , Collecting and Analyzing Evidence , Switches, Routers, and Firewalls, Storage Media, Web Proxies , Why Investigate Web Proxies? Web Proxy Functionality , Evidence , Squid , Web Proxy Analysis, Encrypted Web Traffic , Network Tunneling , Tunneling for Functionality, Tunneling for Confidentiality , Covert Tunneling, Malware Forensics Trends in Malware Evolution, Network Behavior of Malware, The Future of Malware and Network Forensics

References:

1. Albert Marcella, Jr., LLC; Doug Menendez, "Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes", 2/e, CRC Press, 2007.

2. Cory Altheide, Harlan Carvey, "Digital Forensics with Open Source Tools", 1/e, Syngress, 2011.
3. Sherri Davidoff, Jonathan Ham, "Network Forensics: Tracking Hackers through Cyberspace", 1/e, Prentice Hall, 2012.
4. John Sammons, "The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics, 1/e, Syngress, 2012.
5. Harlan Carvey , "Windows Forensic Analysis Toolkit: Advanced Analysis Techniques for Windows 7", 3/e, Syngress, 2012.

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

Wireless Ad Hoc, Sensor and Mesh Networks -Ad Hoc Networks and Applications, Sensor and Actuator Networks, Mesh Networks, Factors Influencing the Design of Wireless Ad Hoc, Sensor and Mesh Networks, Routing in Wireless Ad Hoc Networks, Routing in Wireless Sensor Networks, Security Issues in Ad Hoc Networks- Vulnerabilities, Security requirements and attacks, secure routing, key management, Attacks and defenses of routing mechanisms in adhoc and sensor networks, Privacy and Anonymity in Mobile Ad Hoc Networks, Authentication in wireless sensor networks, False Data Detection and Secure Data Aggregation in Wireless Sensor Networks, MAC layer attacks in sensor networks, Key management in wireless sensor networks, Underwater Sensor Networks, Satellite Networks

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:

1. Erdal Cayirci, Chunming Rong, "Security in Wireless Ad Hoc and Sensor Networks", WILEY, 2009.
2. Tim Mather, Subra Kumaraswamy, Hahed Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance", O'reilly Media, 2009.

3. C. S. R. Prabhu, "Grid and Cluster Computing", Prentice-hall Of India Pvt Ltd, 2008.
4. Yang Xiao, "Security in Sensor Networks", Auerbach Publications, 2006.
5. David Kleidermacher, Mike Kleidermacher, "Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development", 1/e, Newnes, 2012.

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

Perimeter security fundamentals. Stateful firewalls – filtering, inspection. Proxy firewalls – pros and cons, types, tools. Security policy – perimeter considerations. The role of a router, VPN – basics, advantages and disadvantages, IPSec, PPTP, L2TP. Network intrusion detection roles of network IDS. Host hardening. Host defence components antivirus software, host based firewalls, host based intrusion detection, challenges. Intrusion prevention systems – IPS, NIPS, host based intrusion prevention systems.

MODULE 2

Fundamentals of secure perimeter design – requirements, elements. Resource separation security zones, VLAN based separation. Wireless network security – auditing. Software architecture software component placement, software architecture issues, software testing, network defense design. VPN integration secure shell, secure sockets layer, remote desktop solutions, IPSec.

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:

1. Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent and Ronald W. Ritchey, “Inside Network Perimeter Security”, 2/e, Pearson Education, 2005.
2. Cliff Riggs, “Network Perimeter Security: Building Defense InDepth”, Auerbach Publications, 2003.
3. Michael J. Arata, "Perimeter Security", McGrawHill Professional, 2005.
4. E. Cole, R. Krutz, and J. Conley, “Network Security Bible”, Wiley Dreamtech, 2005.
5. M. Bishop, “Computer Security: Art and Science”, Pearson Education, 2003.

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.