NEHRU COLLEGE OF ENGINEERING AND RESEARCH CENTRE

(Accredited by NAAC,ISO 9001-2015 certified, Approved by AICTE New Delhi, Affiliated to APJKTU) **Pampady, Thiruvilwamala(PO), Thrissur(DT), Kerala 680 588**

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SYLLABUS BOOK FOR STUDENTS

CALICUT UNIVERSITY SYLLABUS FOR M. Tech Cyber Security

VISION OF THE INSTITUTION

To mould true citizens who are millennium leaders and catalysts of change through excellence in education.

MISSION OF THE INSTITUTION

NCERC is committed to transform itself into a center of excellence in Learning and Research in Engineering and Frontier Technology and to impart quality education to mould technically competent citizens with moral integrity, social commitment and ethical values.

We intend to facilitate our students to assimilate the latest technological know-how and to imbibe discipline, culture and spiritually, and to mould them in to technological giants, dedicated research scientists and intellectual leaders of the country who can spread the beams of light and happiness among the poor and the underprivileged.

ABOUT DEPARTMENT

- Established in: 2002
- Courses offered : B.Tech in Computer Science and Engineering

  M.Tech in Computer Science and Engineering

  M.Tech in Cyber Security
- Approved by AICTE New Delhi and Accredited by NAAC
- Certified by ISO 9001-2015.
- Affiliated to the A P J Abdul Kalam Technological University.

DEPARTMENT VISION

Producing Highly Competent, Innovative and Ethical Computer Science and Engineering Professionals to facilitate continuous technological advancement.

DEPARTMENT MISSION

1. To Impart Quality Education by creative Teaching Learning Process
2. To Promote cutting-edge Research and Development Process to solve real world problems with emerging technologies.
3. To Inculcate Entrepreneurship Skills among Students.
4. To cultivate Moral and Ethical Values in their Profession.

PROGRAMME EDUCATIONAL OBJECTIVES

PEO1: Graduates will be able to Work and Contribute in the domains of Computer Science and Engineering through lifelong learning.

PEO2: Graduates will be able to Analyse, design and development of novel Software Packages, Web Services, System Tools and Components as per needs and specifications.

PEO3: Graduates will be able to demonstrate their ability to adapt to a rapidly changing environment by learning and applying new technologies.

PEO4: Graduates will be able to adopt ethical attitudes, exhibit effective communication skills, Teamworkand leadership qualities.

PROGRAM OUTCOMES (POs)

Engineering Graduates will be able to:

1. Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

2. **Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

3. **Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

4. **Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

5. **Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

6. **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

7. **Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

9. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

10. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write

effective reports and design documentation, make effective presentations, and give and receive clear instructions.

11. **Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one‟s own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

12. **Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES (PSO)

PSO1: Ability to Formulate and Simulate Innovative Ideas to provide software solutions for Real-time Problems and to investigate for its future scope.

PSO2: Ability to learn and apply various methodologies for facilitating development of high quality System Software Tools and Efficient Web Design Models with a focus on performance optimization.

PSO3: Ability to inculcate the Knowledge for developing Codes and integrating hardware/software products in the domains of Big Data Analytics, Web Applications and Mobile Apps to create innovative career path and for the socially relevant issues.

SYLLABUS
FOR
M. Tech
Cyber Security

File Ref.No.33651/GA - IV - E2/2014/CU

UNIVERSITY OF CALICUT

Abstract

Faculty of Engineering - Syllabus -M.Tech Programme in Cyber Security - with effect from 2013 admission onwrds - Approved - Sanctioned - Orders issued..

G & A - IV - E

U.O.No. 4153/2014/Admn Dated, Calicut University.P.O, 26.04.2014

Read:-1. U.O. No. 4728/2013/CU dated 11-10-2013.

2. Item No. I of the Minutes of the meeting of the Board of Studies in Engineering(PG) held on 03-03-2014.

3. Item No. I.29 of the minutes of the meeting of the Academic Council held on 20-03-2014.

ORDER

As per paper read as 1st above, an Expert Committee was constituted for framing syllabus for M.Tech Programme in Cyber Security.

The Report and Syllabus submitted by the Expert Committee was considered by the Board of Studies in Engineering (PG), in it's meeting held on 03-03-2014 and resolved vide paper read as 2nd above, to approve the syllabus for M.Tech Programme in Cyber Security with a modification in the Subject Code and to fix the eligibility criteria for admission to the course to be B.Tech Degree in Computer Science Engineering / Information Technology.

Vide paper read as 3rd above, the Academic Council at its meeting held on 20-03-2014 has approved the minutes of the meeting of the Board of Studies in Engineering(PG) held on 03-03-2014.

Sanction has therefore been accorded for implementing the syllabus of M.Tech Course in Cyber Security with eligibility criteria for admission to the course to be B.Tech Degree in Computer Science and Engineering / Information Technology.

Orders are issued accordingly.

Muhammed S
Deputy Registrar

To

Copy to : - Chairman, BS in Engineering(PG)/ Dean, Faculty of Engineering/ Chairman, Expert Committee/
PS to VC/ PA to PVC/ PA to Reg/ PA to CE/ Section Dealing with M.Tech Courses,PB/SF-2014/ SA(with a
request to upload the U.O. & Syllabus in the University website)

Forwarded / By Order

Section Officer

M.Tech. DEGREE COURSE
CYBER SECURITY

Curricula, Scheme of Examinations and Syllabi

Scheme of M.Tech Programme in Cyber Security

Semester I

Course Code	Subject	Hours/Week			Marks		Total Marks	Sem End Exam Duration Hours	Credits
		L	T	P/D	Internal	Sem-End			
MCY 10 101	Mathematical Foundations of Computer Science	3	1	0	100	100	200	3	4
MCY 10 102	Internetworking-Protocols and Security	3	1	0	100	100	200	3	4
MCY 10 103	Advanced Cryptography	3	1	0	100	100	200	3	4
MCY 10 104	Advanced Computer Architecture	3	1	0	100	100	200	3	4
MCY 10 105	Elective I	3	1	0	100	100	200	3	4
MCY 10 106(P)	Seminar I	0	0	2	100	0	100	-	2
MCY 10 107(P)	Advanced Software Lab	0	0	2	100	0	100	-	2
TOTAL		**15**	**5**	**4**	**700**	**500**	**1200**		**24**

Elective I

MCY 10 105 (A) HIGH SPEED NETWORKS
MCY 10 105 (B) ADVANCED DISTRIBUTED COMPUTING
MCY 10 105 (C) COMPUTATIONAL INTELLIGENCE
MCY 10 105 (D) MATHEMATICAL MODELS OF INTERNET

Note: Remaining 6 hours / week is meant for departmental assistance by students
L-Lecture T-Tutorial P-Practical

Semester – II

Course Code	Subject	Hours/Week			Marks		Total Marks	Sem End Exam Duration Hours	Credits
		L	T	P/D	Internal	Sem End			
MCY 10 201	Mobile and Wireless Network Security	3	1	0	100	100	200	3	4
MCY 10 202	Secure Coding	3	1	0	100	100	200	3	4
MCY 10 203	Digital Forensics	3	1	0	100	100	200	3	4
MCY 10 204	Elective II	3	1	0	100	100	200	3	4
MCY 10 205	Elective III	3	1	0	100	100	200	3	4
MCY 10 206(P)	Seminar II	0	0	2	100	0	100	-	2
MCY 10 207(P)	Cyber Security Lab	0	0	2	100	0	100	-	2
TOTAL		**15**	**5**	**4**	**700**	**500**	**1200**		**24**

Elective II

MCY 10 204 (A) DATA COMPRESSION
MCY 10 204 (B) INTERACTIVE PROGRAMMING WITH PYTHON
MCY 10 204 (C) COMPUTER AND INFORMATION SECURITY MANAGEMENT

Elective III

MCY 10 205 (A) COMPUTER LAW AND ETHICS
MCY 10 205 (B) BIO-INFORMATICS
MCY 10 205 (C) SOFT COMPUTING

Note: Remaining 6 hours / week is meant for departmental assistance by students

Semester III

Course Code	Subject	Hours/Week			Marks		Total Marks	Sem- end Exam Duration Hours	Credits
		L	T	P/D	Internal	Sem-End			
MCY 10 301	Elective IV	3	1	0	100	100	200	3	4
MCY 10 302	Elective V	3	1	0	100	100	200	3	4
MCY 10 303(P)	Industrial Training	0	0	0	50	-	50	-	1
MCY 10 304(P)	Master Research Project Phase I	0	0	22	GUIDE 150 EC* 150	-	300	-	6
TOTAL		**6**	**2**	**22**	**550**	**200**	**750**		**15**

NB: The student has to undertake the departmental work assigned by HOD
*EC - Evaluation Committee

Electives –IV

MCY 10 301 (A) DIGITAL WATERMARKING
MCY 10 301 (B) RESEARCH METHODOLOGIES
MCY 10 301 (C) DATABASE SECURITY

Electives –V

MCY 10 302 (A) CLOUD AND UTILITY COMPUTING
MCY 10 302 (B) CRYPTOCOMPLEXITY
MCY 10 302 (C) SECURITY POLICIES AND ASSURANCE

Semester IV

Course Code	Subject	Hours/Week			Internal Marks		Sem-End		Total Marks	Credits
		L	T	P/D	Guide	EC*	Ext. Guide	Viva Voce		
MCY 10 401(P)	Master Research Project Phase II	-	-	30	150	150	150	150	600	12
TOTAL				30	150	150	150	150	600	12

NB: The student has to undertake the departmental work assigned by HOD

SEMESTER I

MCY 10 101: MATHEMATICAL FOUNDATIONS OF COMPUTER SCIENCE

Prerequisite: Discrete Computational Structures

Teaching scheme:
Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:
To familiarize the students with the fundamental theorems, group and subgroups properties, fundamental principles of counting and graphs. And these concepts will help the students in their master research project work.

Module I: (13Hrs)
Divisibility, gcd, prime numbers, fundamental theorem of arithmetic,Congruences, Fermat's theorem, Euler function, Primality testing, solution of congruences, Chinese remainder theorem, Wilson's theorem.

Module II: (13Hrs)
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.

Module III: (14Hrs)
Fundamental principles of counting, pigeonhole principle, countable and uncountable sets, principle of inclusion and exclusion, derangements, equivalence relations and partitions, partial order, lattices and Boolean algebra, generating functions, recurrence relations, solution of recurrences.

Module IV: (13Hrs)
Graphs, Euler tours, planar graphs, Hamiltonian graphs, Euler's formula, applications of Kuratowski's theorem, graph coloring, chromatic polynomials, trees, weighted trees, shortest path algorithms, spanning trees, the max-flow min-cut theorem.

References

1. Niven, H.S. Zuckerman and Montgomery, An Introduction to the Theory of Numbers, 3/e, John Wiley and Sons, New York, 1992.
2. R. P. Grimaldi, Discrete and Combinatorial Mathematics: An Applied Introduction,3/e, Addison-Wesley, New Delhi, 1994.
3. B. Kolman and R.C. Busby, Discrete Mathematical Structures for Computer Science, PHI, New Delhi, 1994.
4. J. Clark and D. A. Holton, A First Look at Graph Theory, Allied Publishers (World Scientific), New Delhi, 1991.

5. C. L. Liu, Elements of Discrete Mathematics, McGraw Hill, 2/e, Singapore, 1985.

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I

Question 1: 20 marks
Question 2: 20 marks

Module II

Question 3: 20 marks
Question 4: 20 marks

Module III

Question 5: 20 marks
Question 6: 20 marks

Module IV

Question 7: 20 marks
Question 8: 20 marks

MCY 10 102:INTERNETWORKING - PROTOCOLS AND SECURITY

Prerequisite: Computer Networks

Teaching scheme:
Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:
To provide the students with the concepts of network services and architectures.
An introduction to network management security issues is also given.

Module I: (13Hrs)
Network services and applications: DNS, HTTP, SMTP, peer-to-peer systems
Module II: (13Hrs)
Network transport architectures, TCP, UDP, ICMP, TCP congestion control, Routing and forwarding, intra-domain and inter-domain routing algorithms, Link layers and local area networks
Module III: (13Hrs)
Ethernet, Wi-Fi, and mobility, Multimedia communications and quality of service, Network measurement, inference, and management, Network experimentation and performance analysis.
Module IV: (13Hrs)
Security: ARP attacks and ARP poisoning, DNS attacks, SYN flood attacks and its mitigation, UDP ping-pong and fraggle attacks, TCP port scanning and reflection attacks.

References
1. James F Kurose and Keith W. Ross, "Computer Networking - A Top Down Approach", Fifth Edition, Addison-Wesley, 2010.
2. L. Peterson and B. Davie, "Computer Networks: A Systems Approach", Fifth Edition, Elsevier Inc., 2011.
3. W. Richard Stevens, "TCP/IP Illustrated, Volume 1: The Protocols", Addison-Wesley,1994.

Internal continuous assessment: 100 marks
Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I

Question 1: 20 marks

Question 2: 20 marks

Module II

Question 3: 20 marks

Question 4: 20 marks

Module III

Question 5: 20 marks

Question 6: 20 marks

Module IV

Question 7: 20 marks

Question 8: 20 marks

MCY 10 103: ADVANCED CRYPTOGRAPHY

Teaching scheme:
Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:
To provide the students with the concepts of cryptography algorithms and schemes to handle the security issues. An introduction to web security and message authentication are also given.

Module I: (13Hrs)
Review of number theory and algebra, computational complexity, probability and information theory, primality testing.

Module II: (13Hrs)
Cryptography and cryptanalysis, symmetric key encryption, DES, Triple DES, AES, RC4, modes of operation.

Module III: (13Hrs)
public key encryption, RSA cryptosystem, Diffie-Hellman, elliptic curve cryptography, Rabin, ElGamal, Goldwasser-Micali, Blum-Goldwasser cryptosystems.

Module IV: (13Hrs)
Message authentication, digital signature algorithms, Security handshake pitfalls, Strong password protocols.

References

1. W. Mao, *Modern Cryptography: Theory & Practice*, Pearson Education, 2004.
2. C. Kaufman, R. Perlman and M. Speciner, Network Security: Private Communication in a public World, 2/e, Prentice Hall, 2002.
3. W. Stallings, *Cryptography and Network Security Principles and practice*, 3/e, Pearson Education Asia, 2003.
4. H. Delfs and H. Knebl, *Introduction to Cryptography: Principles and Applications*, Springer-Verlag, 2002.

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern
Answer any 5 questions by choosing at least one question from each module.

Module I
Question 1: 20 marks
Question 2: 20 marks

Module II
Question 3: 20 marks
Question 4: 20 marks

Module III
Question 5: 20 marks
Question 6: 20 marks

Module IV
Question 7: 20 marks
Question 8: 20 marks

MCY 10 104: ADVANCED COMPUTER ARCHITECTURE

Prerequisite: Computer Organization and Design

Teaching scheme:
Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:
To familiarize the students with the concepts of processor architecture, support for parallelism and multiprocessor systems.

Module I: (13Hrs)
Performance evaluation, Processor architecture, pipelining, pipeline hazards, issues in pipelined processor implementation.

Module II: (13Hrs)
Instruction level parallelism, hardware and compiler support for branch prediction, out-of-order Instruction issue, speculative execution and other techniques for high-performance

Module III: (13Hrs)
Instruction and data cache organizations, multilevel caches, parallel memory systems, Support for virtual memory. Interconnection networks, shared memory system, memory models, cache coherence.

Module IV: (13Hrs)
Multiple processor systems, Parallel algorithms architecture, Multicore processing, New programming paradigms-Hadoop, map reduce.

References

1. Hennessy J. L., D. Patterson, *Computer Architecture – A quantitative Approach*, Morgan Koffman (3/e), 2003
2. John Paul Shen, MikkoLipasti. *Modern Processor Design – Fundamentals of SuperscalarProcessors*.McGraw Hill International Edition, 2005.
3. DezsoSima, Terence Fountain, Peter Kacsuk. *Advanced Computer Architecture – A Design Space Approach,* Addison Wesley, 2000.

5. Fayez Gebali, Algorithms and Parallel Computing – A John wiley and Sons,Inc., Publication,2011

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I
Question 1: 20 marks
Question 2: 20 marks

Module II
Question 3: 20 marks
Question 4: 20 marks

Module III
Question 5 : 20 marks
Question 6: 20 marks

Module IV
Question 7 : 20 marks
Question 8: 20 marks

ELECTIVE I

MCY 10 105(A): HIGH SPEED NETWORKS

Teaching scheme:
Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:
To familiarize the students with the concepts of high speed networks like frame relays,ATMs etc. Gives details about congestion control in high speed networks, discussesintegrated and differentiated services etc.

Module I: (13 Hrs)
Frame Relay Networks – Asynchronous transfer mode – ATM Protocol Architecture,
ATM logical Connection, ATM Cell – ATM Service Categories – AAL. High Speed LAN's: Fast Ethernet, Gigabit Ethernet, Fibre Channel – Wireless LAN's. Queuing Analysis- Queuing Models – Single Server Queues – Effects of Congestion – CongestionControl – Traffic Management – Congestion Control in Packet Switching Networks –Frame Relay Congestion Control.

Module II: (14 Hrs)
TCP Flow control – TCP Congestion Control – Retransmission – Timer Management –Exponential RTO back off – KARN's Algorithm – Window management – Performanceof TCP over ATM. Traffic and Congestion control in ATM – Requirements – Attributes– Traffic Management Frame work, Traffic Control – ABR traffic Management – ABRrate control, RM cell formats, ABR Capacity allocations – GFR traffic management.

Module III: (12 Hrs)
Integrated Services Architecture – Approach, Components, Services- Queuing Discipline, FQ, PS, BRFQ, GPS, WFQ – Random Early Detection, Differentiated Services.

Module IV: (12 Hrs)

RSVP – Goals & Characteristics, Data Flow, RSVP operations, Protocol Mechanisms – Multiprotocol Label Switching – Operations, Label Stacking, Protocol details – RTP –Protocol Architecture, Data Transfer Protocol, RTCP.

References

1. William Stallings, "HIGH SPEED NETWORKS AND INTERNET", Pearson Education, Second Edition, 2002.
2. Warland & Pravin Varaiya, "HIGH PERFORMANCE COMMUNICATION NETWORKS", Jean Harcourt Asia Pvt. Ltd., II Edition, 2001.
3. Irvan Pepelnjk, Jim Guichard and Jeff Apcar, "MPLS and VPN architecture", Cisco Press, Volume 1 and 2, 2003.

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks
Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I
Question 1: 20 marks
Question 2: 20 marks

Module II
Question 3: 20 marks
Question4: 20 marks

Module III
Question 5: 20 marks
Question 6: 20 marks

Module IV
Question 7: 20 marks
Question 8: 20 marks

MCY 10 105(B): ADVANCED DISTRIBUTED COMPUTING

Prerequisite: Distributed Systems

Teaching scheme:
Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:

- *To familiarize the concepts of distributed systems and models.*
- *Study the issues concerning Remote procedure call and distributed file systems.*
- *Discuss the issues concerning distributed transaction process in detail.*

Module I: (14Hrs)
Characterization of Distributed Systems, System Models, Networking and Internetworking, Inter Process communication, Distributed Objects and Remote Invocation, RPC, Processes and threads.

Module II: (13Hrs)
Name Services and Domain Name System, Directory and Discovery Systems, Synchronizing physical clocks, logical time and logical clocks, Distributed Mutual Exclusion, Elections.

Module III: (13Hrs)
Transactions and Concurrency Control, Distributed Transactions, Distributed Deadlocks, Transaction Recovery, Fault-tolerant Services, Distributed Shared Memory,.

Module IV: (12Hrs)
Distributed File systems, Grid Computing – motivation, comparison, Grid Architecture, GRID standards – OGSA, OGSI, WSRF Data management, Grid Scheduling and Information Services, Grid Workflow , Fault Tolerance in Grids , Security in Grid Computing.

References

1. Coulouris G., Dollimore J. &Kindberg T., "*Distributed Systems Concepts And Design*", 3/e, Addison Wesley 2004
2. Tanenbaum S, Maarten V.S., Distributed Systems Principles and Paradigms, Pearson Education 2004
3. Chow R. & Johnson T., "*Distributed Operating Systems and Algorithms*", Addison Wesley 2003
4. Tanenbaum S., "*Distributed Operating Systems*", Pearson Education 2005
5. Frederic Magoules , Jie Pan , Kiat An Tan , Abhinit Kumar ," Introduction to Grid Computing", Chapman & Hall/CRC press 2009

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I

Question 1: 20 marks

Question 2: 20 marks

Module II

Question 3: 20 marks

Question 4: 20 marks

Module III

Question 5: 20 marks

Question 6: 20 marks

Module IV

Question 7: 20 marks

Question 8: 20 marks

MCY 10 105(C): COMPUTATIONAL INTELLIGENCE

Teaching scheme:
Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:

- *To provide the students with the concepts Artificial Intelligence and representation of knowledge.*
- *To familiarize fundamental models of machine learning and expert systems.*
- *Discuss various Languages and Programming Techniques for Artificial Intelligence.*

Module I: (13Hrs)
Artificial Intelligence: History and Applications, Production Systems, Structures and Strategies for state space search- Data driven and goal driven search, Depth First and Breadth First Search, DFS with Iterative Deepening, Heuristic Search- Best First Search, A* Algorithm, AO* Algorithm, Constraint Satisfaction, Using heuristics in games- Minimax Search, Alpha Beta Procedure.

Module II: (13Hrs)
Knowledge representation - Propositional calculus, Predicate Calculus, Theorem proving by Resolution, Answer Extraction, AI Representational Schemes- Semantic Nets, Conceptual Dependency, Scripts, Frames, Introduction to Agent based problem solving.

Module III: (13Hrs)
Machine Learning- Symbol based and Connectionist, Social and Emergent models of learning, The Genetic Algorithm- Genetic Programming, Overview of Expert System Technology- Rule based Expert Systems, Introduction to Natural Language Processing.

Module IV: (13Hrs)
Languages and Programming Techniques for AI- Introduction to PROLOG and LISP, Search strategies and Logic Programming in LISP, Production System examples in PROLOG[Programming in Octave/Matlab].

References

1. GEORGE.F.LUGER, *Artificial Intelligence- Structures and Strategies for Complex Problem Solving*, 4/e, 2002, Pearson Education.
2. E. RICH, K.KNIGHT, *Artificial Intelligence*, 2/e, Tata McGraw Hill
3. WINSTON. P. H, LISP, Addison Wesley
4. IVAN BRATKO, *Prolog Programming for Artificial Intelligence*, 3/e, Addison Wesley, 2000
5. Online documentation for Octave.

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks
Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I
Question 1: 20 marks
Question 2: 20 marks

Module II
Question 3: 20 marks
Question 4: 20 marks

Module III
Question 5: 20 marks
Question 6: 20 marks

Module IV
Question 7: 20 marks
Question 8: 20 marks

MCY 10 105(D): MATHEMATICAL MODEL OF INTERNET

Teaching scheme:
Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:

- *To provide the students with the concepts modeling the queuing systems and moving networks.*
- *Discuss the application of various model used in internet based applications.*

Module I: (13Hrs)
Definition and characteristics of mathematical models.

Module II: (12Hrs)
Modeling the network - queuing systems, modeling the QoS for improvement. Mathematical models of fairness and stability**.**

Module III: (13Hrs)
Modeling a self-managed internet. Moving away from the end to end concept. Modeling required in an untrustworthy world.

Module IV : (13Hrs)
Modeling of an internet based application.

References

1. Harold Tipton, Micki Krause, *Information Security Management Handbook,* 5th Edition, Auerbach / CRC Press 2004
2. Seymour Bosworth, M E Kabay .*Computer Security Handbook*, 4th Edition. John Wiley, 2002.
3. Theo Dimitrakos, Fabio Martinelli, (Editors). *Formal Aspects in Security and Trust:* Proceedings of IFIP Workshop on Formal Aspects in Security and Trust (FAST) 2004
4. Ali E Abdallah, Peter Ryan, Steve Schneider (Editors). *Formal Aspects of Security:* Proceedings of First International Conference, FASec 2002. LNCS 2629, Springer2003

5.Markus Schumacher. *Security Engineering with patterns: origins, theoretical model, Andnew applications.* LNCS 2754, Springer.

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I

Question 1: 20 marks
Question 2: 20 marks

Module II

Question 3: 20 marks
Question 4: 20 marks

Module III

Question 5: 20 marks
Question 6: 20 marks

Module IV

Question 7: 20 marks
Question 8: 20 marks

MCY 10 106(P) SEMINAR I

Hours per week: 2 hours practical **Credits:** 2

Objective:

To assess the debating capability of the student to present a technical topic. Also to impart training to a student to face audience and present his/her ideas and thus creating self esteem and courage that are essential for an engineer.

Each student is expected to present a seminar on a topic of current relevance in Cyber/Information Security or Forensics for about 45 minutes. They are expected to refer current research and review papers from standard journals like ACM, IEEE, JPDC, IEE etc. – at least three cross references must be used - the seminar report must not be the reproduction of the original paper. A committee consisting of at least three faculty members shall assess the presentation of the seminar and award marks to the students based on merits of topic of presentation. Each student shall submit two copies of a write up of the seminar topic. One copy shall be returned to the student after duly certifying it by the chairman of the assessing committee and the other will be kept in the departmental library. Internal continuous assessment marks are awarded based on the relevance of the topic, presentation skill, quality of the report and participation.

Internal Continuous Assessment *(Maximum Marks-100)*

Presentation +Discussion	: 60
Relevance + Literature	: 10
Report	: 20
Participation	: 10
Total marks	**: 100**

MCY 10 107 (P) ADVANCED SOFTWARE LAB

1. Study of Architecture Characteristics Using Simulators (Like Simple Scalar or equivalent).

2. TCP Client Server Program Using Sockets in Java/Python

3. Simulation of Congestion/QoS Protocols

4. Implementation of Heap Structures

5. Implementation of Search Structures

6. Implementation of Multimedia Data Structures

7. Implementation of Data Structure Applications.

8. Study of Case Tools (Rational Rose, Eclipse or other equivalent).

9. Implementation of TCP cubic in NS2

10. Implementation of TCP compound in NS2

Internal Continuous Assessment *(Maximum Marks-100):*

Regularity & Class work	- 30 marks
Record	- 20 marks
Tests, Viva	- 50 marks

SEMESTER II

MCY 10 201: MOBILE AND WIRELESS NETWORK SECURITY

Teaching scheme:
Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:

- *To teach the transmission fundamentals and* Wireless *System Operations and Standards.*
- *To discuss the issues concerning various threats to wireless networks, encryption and decryption.*
- *To provide students with the concepts of security mechanisms for Blue-tooth, WLAN, WIMAX, satellite network etc.*

Module I: (13Hrs)
Transmission Fundamentals, Antennas and Wave Propagation Cellular Wireless networks, Third Generation Systems, 4G, Signal Encoding Techniques, Spread Spectrum, Coding and Error Control, Multiple Access in Wireless Systems.

Module II: (13Hrs)
Satellite Networks, Wireless System Operations and Standards. Wi-Max and Ultra Wide Band technologies, Mobile IP and Wireless Access : Protocol. Wireless LAN Technology, Wi-Fi and IEEE 802.11 Wireless LAN Standard, Blue-tooth and IEEE 802.15 standard.

Module III: (13Hrs)
Threats to Wireless networks, ESM, ECM and ECCM, Proliferation of device and technologies, Practical aspects, Wireless availability, Privacy Challenges. Risks: Denial of Service, Insertion Attacks, interception and monitoring wireless traffic, Misconfiguration. Wireless Attack: Surveillance, War Driving, Client-to-Client Hacking, Rogue Access Points, Jamming and Denial of Service.

Module IV: (13Hrs)
Authentication, Encryption, Decryption in GSM, Securing the WLAN, WEP Introduction, RC Encryption, Data Analysis, IV Collision, Key Extraction, WEP Cracking WPA/ WPA2, AES, Access Point-Based Security Measures Thin Party Security Methods, Funk's Steel-Belted Radius, VVLAN Protection Enhancements, Blue-tooth Security Implementation, Security in WI MAX, UWB security, Satellite network security.

References

1.Kaveh Pahlavan and Preshant Krishnamurthy, Principles Wireless Networks, Prentice Hall, 2006.
2. Cyrus Peikari and Seth Fogie, °Maximum Wireless Security.Sams, 2002.
3. Hideki /mai, Mohammad Ghulam Rahman and Kazukuni Koba "Wireless Communications Security, Universal Persor Communications of Adech House, 2006.
4. Stallings William, "Wireless Communications and Network: Second Edition, Pearson Education Ltd, 2009.
5. Jon Edney and William A. Arbaugh, " Real 802.11 Security: Wi Protected Access and 802.11i", Addison-Wesley Professional

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I
Question 1: 20 marks
Question 2: 20 marks

Module II
Question 3: 20 marks
Question 4: 20 marks

Module III
Question 5: 20 marks
Question 6: 20 marks

Module IV
Question 7: 20 marks
Question 8: 20 marks

MCY 10 202: SECURE CODING

Teaching scheme:
Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:
To provide the students with the concepts of secure programming, threat modeling, attacks, resource management and secure testing methodologies.

Module I: (13 Hrs)
A brief overview of Application Security and Secure Programming concepts. Secure Coding in C and C++, Stack overflow, Strings, Integers, Arrays, File I/O, Race conditions, Signal handling, Recommended Practice

Module II: (13 Hrs)
Secure Coding in Java and Web Applications-Web as a primary vector for Cyber attacks, Anatomy of attacks, data breach case studies, Threat modeling, Cross Site Scripting (XSS) vulnerabilities, Injection flaws (SQL, process, path etc.), Buffer overflows

Module III: (13 Hrs)
Resource leaks and resource lifetime management, Threat modeling and Security design review, Software Assurance and Testing-Software Assurance overview, Testing threat categories, Assessing Risk

Module IV: (13 Hrs)
Secure Testing Methodologies - Attacking Dependencies, Attacking through the User Interface, Attacking Design, Attacking Implementation, Software engineering practices for development of high assurance code, Model Checking, Static Analysis techniques for analyzing software.

References

1. Robert C. Seaford, 'Secure Coding in C and C++', Addison-Wesley Professional, 2005.
2. James A. Whittaker and Herbert H. Thompson, "How to Break Software Security", Addison Wesley, 2003
3. John C. Mitchell and Krzysztof Apt, "Concepts in Programming Languages", Cambridge

University Press, 2001

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern
Answer any 5 questions by choosing at least one question from each module.

Module I
Question 1: 20 marks
Question 2: 20 marks

Module II
Question 3: 20 marks
Question 4: 20 marks

Module III
Question 5: 20 marks
Question 6: 20 marks

Module IV
Question 7: 20 marks
Question 8: 20 marks

MCY 10 203: DIGITAL FORENSICS

Prerequisite:Computer Organization

Teaching scheme:
Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:
To provide the students with the concepts security audit mechanisms for various file systems, database and networks. An introduction to applications of digital forensic analysis in mobile and smart phones and vehicular systems are also given.

Module I: (13Hrs)
Framework for digital forensic evidence collection and processing. Fundamentals of host forensics for Microsoft windows, including kernel architecture, device driver architecture, registry, auditing and security architecture, file system handling, reconstruction of files and directory structures on the FAT and NTFS file system families.

Module II: (13Hrs)
Fundamentals of host forensics for UNIX derivatives use the Linux operating system, including kernel and device drives architecture, security and audit mechanisms, file system and pseudo file systems, and the reconstruction of file and directory structures using UFS and Ext2/3fs as exemplars.

Module III: (13Hrs)
Forensic Analysis of Database Systems [MySQL/MariaDB/PostgreSQL], Database Tampering, Forensic analysis of Database Components, table storage, transaction log, indexes, Forensic recovery for table storage. Fundamentals of network forensics from data capturing and collection to network file systems and supplementary protocols and selection application layer protocols and techniques used for identifying and reverse- engineering protocols used on networks

Module IV: (13Hrs)

Application to malware detection, anti-forensic and propagation techniques, Application to stenographic and steganalysis, Application to non standard storage mechanisms like mobile and smart phones and vehicular systems and network based search and storage mechanism.

References

1. K. J. Jones, R. Beftlich and C. W. Rose, Real Digital Forensics', Addison- Wesley, 2006.
2. D. P Bovet and M. Cesati, "Understanding the Linux Kernel", Third Edition, O'Reiry, 2006.
3. B. Carrier, "File System Forensic Analysis", Addison- Wesley, 2005.
4. M. Russinovich, D. A. Soiomon and A. lonescu, "Windows InternalsTM, Fifth Edition, Microsoft Press, 2008.
5. Chang-Tsun Li, "Multimedia Forensics and Security", Information Science Reference, Hershey, New York, 2008.
6. Online Documentation of MySQL,MariaDB and PostgreSQL

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I

Question 1: 20 marks

Question 2: 20 marks

Module II

Question 3: 20 marks

Question 4: 20 marks

Module III

Question 5: 20 marks

Question 6: 20 marks

Module IV

Question 7: 20 marks
Question 8: 20 marks

MCY 10 204 (A) DATA COMPRESSION

Teaching scheme:

Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:

To familiarize the students with the different data compression techniques for image Compression, audio compression, video compression etc. It also gives a comparison of different compression algorithms and their implementation.

Module I : (12 hrs)

Introduction, Basic Techniques, Dictionary Methods

Module II: (13 hrs)

Image Compression, Transform based techniques, Wavelet Methods, adaptive techniques

Module III: (14 hrs)

Video compression, Audio Compression, Fractal techniques.

Module IV: (14 hrs)

Comparison of compression algorithms.Implementation of compression algorithms.

References

1. David Solomon, *Data compression: the complete reference*, 2nd edition, Springerverlag,New York. 2000.
2. Stephen Welstead, *Fractal and wavelet Image Compression techniques*, PHI, NewDelhi-1, 1999.
3. Khalid Sayood, *Introduction to data compression*, Morgan Kaufmann Publishers,

2003 reprint.

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination:100 marks

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I
Question 1: 20 marks
Question 2: 20 marks

Module II
Question 3: 20 marks
Question 4: 20 marks

Module III
Question 5: 20 marks
Question 6: 20 marks

Module IV
Question 7: 20 marks
Question 8: 20 marks

MCY 10 204 (B) INTERACTIVE PROGRAMMING WITH PYTHON

Prerequisite-Web systems and Network security

Teaching scheme:

Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective :

To provide the students with the concept of high level dynamic data types with full modularity.

Module I: (13 hours)

Introduction to Interpreted Languages and Python - Data Types and variables - Operators and Expressions - Program Structure and Control - Functions and Functional Programming - Classes, Objects and other OOPS concepts . I/O in Python - File and Directory Access -

Module II: (13 hours)

Multithreading and Concurrency - Inter Process Communication (IPC) - Permissions and Controls , Raw Socket basics -Socket Libraries and Functionality - Programming Servers and Clients - Programming Wired and Wireless Sniffers - Programming arbitrary packet injectors - PCAP file parsing and analysis.

Module III: (13 hours)

Web Servers and Client scripting - Web Application Fuzzers - Scraping Web Applications – HTML and XML file analysis - Web Browser Emulation - Attacking Web Services - Application Proxies and Data Mangling - Automation of attacks such as SQL Injection, XSS etc.

Module IV: (11 hours)

Exploit Development techniques - Immunity Debuggers and Libs - Writing plugins in Python - Binary data analysis - Exploit analysis Automation.

References

1.MikeDawson,"More Python programming for Absolute Beginner", Cengage Learning PTR; 3rd edition,2010, ISBN-10: 1435455002, ISBN-13: 978-14354550092.

2.Mark Lutz," Python Pocket reference", O'Reilly Media; 4 thedition ,2009,ISBN-10: 0596158084, ISBN-13: 978-0596158088

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I
Question 1: 20 marks
Question 2: 20 marks

Module II
Question 3: 20 marks
Question 4: 20 marks

Module III
Question 5: 20 marks
Question 6: 20 marks

Module IV
Question 7: 20 marks
Question 8: 20 marks

MCY 10 204(C): COMPUTER AND INFORMATION SECURITY MANAGEMENT

Pre-requisite-Knowledge of TCP/IP, Cryptography and Network security is preferred

Objective

The ubiquity of computers and internet in the life of human beings has enabled chance, motive and means to do harm. With such endangers in front of us, it becomes necessary security for security professionals, to learn about how manage computer and information security aspects. Hence this course provides methods to develop new framework for information security, overview of security risk assessment and management and security planning in an organization.

Module I: (12 hours)

The big picture-Learning from experience-Weaknesses in Information Security-The extent of crime in cyberspace- The cyberspace crimoid syndrome-Policies and technologies- A new framework for information security. Risk assessment-Richard Baskerville's risk assessment methodology-Generations of risk assessment techniques- Quantitative approach to risk assessment-Problems with Quantitative approach – NIST ALE- Baseline approach

Module II: (11 hours)

Measuring ROI on security- Security patch management- Purposes of Information Security management- The building blocks of information security- Human side of information security-Security management- Securing new information technology

Module III: (13 hours)

Overview of SSE CMM- SSE CMM relationship to other initiatives- Capability levels- Security Engineering- Security Engineering process overview- Basic process areas- Configuration management- Base practices- Establish configuration management

Module IV: (12 hours)

Maintaining information security during downsizing- Business case for Information Security- Information Security Management in healthcare industry- Protecting high tech trade secrets- Outsourcing Security

References

1. Donn Parkers, " Fighting Computer Crime: A New Framework for Protecting Information", John Wiley&Sons, 2003
2. Micki Krause, Harold F.Tripton, " Information Security Management Handbook", Auerbach Publications, 2012.

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I

Question 1: 20 marks

Question 2: 20 marks

Module II

Question 3: 20 marks

Question 4: 20 marks

Module III

Question 5: 20 marks

Question 6: 20 marks

Module IV

Question 7: 20 marks

Question 8: 20 marks

MCY 10 205(A) : COMPUTER LAW AND ETHICS

Teaching scheme:

Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:

To provide the students with the concepts of Intellectual property rights, issues in equipment contracts.Discusses the ethical issues in computer security, cyber laws *in India and* IT Act 2000.

Module I (10 Hrs)

Intellectual property rights, computer software copyrights, copyright in databases and electronic publishing, law of confidence, patent laws, trademarks, product designs, international law.

Module II (12 Hrs)

Computer contracts, liability for defective hardware and software, software contracts, web and hardware contracts, electronic contracts and torts, liabilities.

Module III (10 Hrs)

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

Module IV (10 Hrs)

Cyber laws in India, IT Act 2000, data subjects' rights, ethical issues in computer security, case studies.

References

1. D. Bainbridge, *Introduction to Computer Law*, 5/e, Pearson Education, 2004.
2. P. Duggal, *Cyber law: the Indian Perspective*, 2005.
3. C. P. Fleeger and S. L. Fleeger, *Security in Computing*, 3/e, Pearson Education, 2003.

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I

Question 1: 20 marks

Question 2: 20 marks

Module II

Question 3: 20 marks

Question 4: 20 marks

Module III

Question 5: 20 marks

Question 6: 20 marks

Module IV

Question 7: 20 marks

Question 8: 20 marks

MCY 10 205(B) BIO-INFORMATICS

Teaching scheme:

Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:
Bio- Informatics is an emerging field and this course will give the students an introduction to this area and various concepts related to bio- informatics such as search engines, data mining, pattern matching etc.

Module I: (14 Hrs)

The Central Dogma – The Killer Application – Parallel Universes – Watson's Definition– Top Down Versus Bottom up – Information Flow – Convergence – Databases – Data Management – Data Life Cycle – Database Technology – Interfaces – Implementation –Networks – Geographical Scope – Communication Models – Transmissions Technology– Protocols – Bandwidth – Topology – Hardware – Contents – Security – Ownership –Implementation – Management.

Module II: (12 Hrs)

The search process – Search Engine Technology – Searching and Information Theory – Computational methods – Search Engines and Knowledge Management – Data Visualization – sequence visualization – structure visualization – user Interface –Animation Versus simulation – General Purpose Technologies.

Module III: (12 Hrs)

Statistical concepts – Microarrays – Imperfect Data – Randomness – Variability –Approximation – Interface Noise – Assumptions – Sampling and Distributions –Hypothesis Testing – Quantifying Randomness – Data Analysis – Tool selection statistics of Alignment – Clustering and Classification – Data Mining – Methods – Selection and Sampling – Preprocessing and Cleaning – Transformation and Reduction – Data Mining Methods – Evaluation – Visualization – Designing new queries – Pattern Recognition and Discovery – Machine Learning – Text Mining – Tools.

Module IV: (14 Hrs)

Pair wise sequence alignment – Local versus global alignment –Multiple sequence alignment – Computational methods – Dot Matrix analysis – Substitution matrices –Dynamic Programming – Word methods – Bayesian methods – Multiple sequence alignment – Dynamic Programming – Progressive strategies – Iterative strategies – Tools– Nucleotide Pattern Matching – Polypeptide pattern matching – Utilities – Sequence Databases. Drug Discovery – components – process – Perspectives – Numeric considerations – Algorithms – Hardware – Issues – Protein structure – Ab Initio Methods– Heuristic methods – Systems Biology – Tools – Collaboration and Communications –standards - Issues – Security – Intellectual property.

References

1. Bryan Bergeron, “Bio Informatics Computing”, Second Edition, Pearson Education,2003.
2. D. E. Krane and M. L. Raymer, Fundamental Concepts of Bioinformatics, Pearson Education, 2003.
3. T. K. Attwood and D. J. Parry-Smith, Introduction to Bioinformatics, Pearson Education, 2003.
4. J. H. Zar, Biostatistical Analysis, 4/e, Pearson Education, 1999.
5.

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks
Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I
Question 1: 20 marks
Question 2: 20 marks

Module II
Question 3: 20 marks
Question 4: 20 marks

Module III
Question 5: 20 marks
Question 6: 20 marks

Module IV
Question 7: 20 marks
Question 8: 20 marks

MCY 10 205 (C) SOFT COMPUTING

Teaching scheme:

Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:

To provide the students with the concepts of soft computing techniques such as neural networks, fuzzy systems, genetic algorithms etc.

Module I: (12 Hrs)
Evolution of Computing - Soft Computing Constituents – From Conventional AI to Computational Intelligence - Adaptive Networks – Feed forward Networks – Supervised Learning Neural Networks – Radia Basis Function Networks - Reinforcement Learning –Unsupervised Learning Neural Networks – Adaptive Resonance architectures.

Module II: (13 Hrs)
Fuzzy Sets – Operations on Fuzzy Sets – Fuzzy Relations - Fuzzy Rules and Fuzzy Reasoning – Fuzzy Inference Systems – Fuzzy Logic – Fuzzy Expert Systems – Fuzzy Decision Making.

Module III: (14 Hrs)

Adaptive Neuro-Fuzzy Inference Systems – Coactive Neuro-Fuzzy Modeling – Classification and Regression Trees – Data Clustering Algorithms – Rule base Structure Identification – Neuro-Fuzzy Control.

Module IV: (14 Hrs)

Machine Learning Techniques – Machine Learning Using Neural Nets – Genetic Algorithms (GA) – Applications of GA in Machine Learning - Machine Learning Approach to Knowledge Acquisition. Support Vector Machines for Learning – Linear Learning Machines – Support Vector Classification – Support Vector Regression -Applications.

References

1. Jyh-Shing Roger Jang, Chuen-Tsai Sun, EijiMizutani, "Neuro-Fuzzy and Soft Computing", Prentice-Hall of India, 2003.
2. James A. Freeman and David M. Skapura, "Neural Networks Algorithms, Applications, and Programming Techniques", Pearson Edn., 2003.
3. George J. Klir and Bo Yuan, "Fuzzy Sets and Fuzzy Logic-Theory and Applications", Prentice Hall, 1995.
4. Amit Konar, "Artificial Intelligence and Soft Computing", First Edition, CRC Press, 2000.
5. Simon Haykin, "Neural Networks: A Comprehensive Foundation", Second Edition Prentice Hall, 1999.
6. Mitchell Melanie, "An Introduction to Genetic Algorithm", Prentice Hall,1998.
7. David E. Goldberg, "Genetic Algorithms in Search, Optimization and Machine Learning", Addison Wesley, 1997.

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I

Question 1: 20 marks

Question 2: 20 marks

Module II

Question 3: 20 marks

Question 4: 20 marks

Module III
Question 5: 20 marks
Question 6: 20 marks

Module IV
Question 7: 20 marks
Question 8: 20 marks

MCY 10 206 (P) SEMINAR II

Hours per week: 2 hours practical **Credits:** 2

Objective:
To assess the debating capability of the student to present a technical topic. Also toimpart training to a student to face audience and present his/her ideas and thus creating self-esteem and courage that are essential for an engineer.

Each student is expected to present a seminar on a topic of current relevance in Cyber/Information Security or Forensics for about 45 minutes. They are expected to refer current research and review papers from standard journals like ACM, IEEE, JPDC, IEE etc. – atleast three cross references must be used - the seminar report must not be there production of the original paper. A committee consisting of at least three faculty members shall assess the presentation of the seminar and award marks to the students based on merits of topic of presentation. Each student shall submit two copies of a write-up of the seminar topic. One copy shall be returned to the student

after duly certifying it by the chairman of the assessing committee and the other will be kept in the departmental library. Internal continuous assessment marks are awarded based on the relevance of the topic, presentation skill, quality of the report and participation.

Internal Continuous Assessment *(Maximum Marks-100)*

Presentation +Discussion	- 60
Relevance + Literature	-10
Report	- 20
Participation	- 10
Total marks	**: 100**

MCY 10 207(P) CYBER SECURITY LABORATORY

1. Implementation of Substitution and Transposition ciphers
2. Implementation of Data Encryption Standard
3. Implementation of International Data Encryption Algorithm
4. Implementation of Advanced Encryption Standard
5. Implementation of RSA Algorithm
6. Implementation of Diffie-Hellman Key Exchange
7. Implementation of Message Authentication Codes
8. Implementation of Hash functions
9. Implementation of Digital Signature Standard

10. Hiding of confidential information within Image
11. Implementation in FOSS based security mechanisms'

Internal Continuous Assessment *(Maximum Marks-100):*

Regularity & Class work - 30 marks
Record - 20 marks
Tests, Viva - 50 marks

SEMESTER III

ELECTIVE IV

MCY 10 301(A) DIGITAL WATERMARKING

Teaching scheme:

Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:

To provide the students with the concepts of modelingof watermarking, message coding. Also teach Watermark security and cryptography.

Module I: (13 Hrs)

Watermarking host signals: Image, Video, Audio. Multimedia compression and decompression, Lossless compression, Models of watermarking, Communication-based models of watermarking. Geometric models of watermarking, Modeling watermark detection by correlation

Module II: (13 Hrs)

Basic message coding, Mapping message into message vectors, Error correction coding, detecting multi-symbol watermarks, Watermarking with side information

Module III: (13 Hrs)

Informed embedding, Informed coding, Structured dirty-paper codes, Analyzing errors, Message errors, ROC curves, The effect of whitening on error rates, Analysis of normalized correlation, Using perceptual models

Module IV: (13 Hrs)

Evaluating perceptual impact of watermarks, General forms of a perceptual model, Perceptual adaptive watermarking, Robust watermarking, Watermark security, Watermark security and cryptography, Content authentication, Exact authentication, Selective authentication, Localization, Restoration. .

References

1. Cox I., M. Miller, J. Bloom, J. Fridrich and T Kalker, "Digital Watermarking and Steganography", Second Edition, Morgan Kaufmann Publishers, 2008.

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I

Question 1: 20 marks

Question 2: 20 marks

Module II
Question 3: 20 marks
Question 4: 20 marks

Module III
Question 5: 20 marks
Question 6: 20 marks

Module IV
Question 7: 20 marks
Question 8: 20 marks

MCY 10 301(B) RESEARCH METHODOLOGY

Teaching scheme:
Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:
Gives students an insight into the steps to be followed in doing a research, provide an idea about technical report writing etc.

Module I: (12 Hrs)
Introduction, Research and Scientific methods, Objectives and Motivation of Research, Criteria of Good Research, research Approaches, Significance of research, Type of Researches, Research

methods VS Methodology, Research problems, Defining a research problem, Research Design, Sampling Design

Module II: (13 Hrs)

Collection of Primary Data, Observation method, Interview Method, Collection of data through Questionnaires and Schedules, Secondary Data, Processing operations, Statistics in research, Measures of central Tendency, Other methods of data collection, Collection of secondary data, Processing operations, Types of analysis, statistics in research, Dispersion, Asymmetry, relationship, Simple regression analysis, Partial correlation

Module III: (14 Hrs)

Hypothesis-I - Introduction, Testing of Hypothesis, Procedure for hypothesis testing, Flow diagram for hypothesis testing, Measuring the power of hypothesis test, Tests of Hypothesis, Hypothesis testing of Means, Proportions, Correlation Coefficients, Chisquare test, Phi Coefficient, Hypothesis-II - Introduction, Nonparametric, Distribution free Tests, Sign tests, Fisher-Irwin test, Spearman's Rank Correlation, Kendall's Coefficient of concordance

Module IV: (14 Hrs)

Report writing – Introduction and Significant, Interpretation – Meaning, Techniques, and Precautions, Layout of research reports, Types of report, Mechanics and precautions of writing a research report, Computer role in research, computers and computer technology, computer system, Characteristics

References

1. CR Kothari, "Research Methodologies – Methods and Techniques", Second Edition, New Age International
2. John W Best and James V Kahn, "Research in Education", Fifth Edition, PHI, New Delhi
3. Pauline V Young, Scientific Social Surveys and Research, Third Editions, PHI New York

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I
Question 1: 20 marks
Question 2: 20 marks

Module II
Question 3: 20 marks
Question 4: 20 marks

Module III
Question 5: 20 marks
Question 6: 20 marks

Module IV
Question 7: 20 marks
Question 8: 20 marks

MCY 10 301(C) DATABASE SECURITY

Prerequisite: Database Management System

Teaching scheme:
Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:

- *To provide the students with the concepts modeling database, authentication and access control mechanisms.*
- *Discuss various issues concerning private database management.*

Module I: (13Hrs)
Introduction to databases: database modeling, conceptual database design, overview of SQL and relational algebra

Module II: (12Hrs)
Access control mechanisms in general computing systems: Lampson's access controi matrix. Mandatory access control

Module III: (13Hrs)
Authentication mechanisms in databases, DAC in databases: Griffiths and Wade, MAC mechanisms in databases: SeaView. RBAC in databases, SQL Injection, Auditing in databases, Statistical inferencing in databases

Module IV: (13Hrs)
Private information retrieval viewed as a database access problem. Privacy in data publishing, Virtual Private Databases, Security of outsourced databases.

References

1. Ron Ben Natan, "Implementing Database Security and Auditing", Elsevier, 2005.
2. Hassan A. Afyouni, "Database Security and Auditing: Protecting Data Integrity and Accessibility", Course Technology, 2005.
3. Michael Gertz and Sushi! Jajodia, "Handbook of Database Security—Applications and Trends", Springer, 2008.

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars ora combination of all whichever suits best. There will be minimum of two tests persubject. The assessment details are to be announced right at the beginning of the semesterby the teacher.

End semester Examination:100 marks

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I
Question 1: 20 marks
Question 2: 20 marks

Module II
Question 3: 20 marks
Question 4: 20 marks

Module III
Question 5: 20 marks
Question 6: 20 marks

Module IV
Question 7: 20 marks
Question 8: 20 marks

ELECTIVE V

MCY 10 302 (A) CLOUD AND UTILITY COMPUTING

Teaching scheme:
Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:

To provide the students with concept of on-demand network access to a shared pool of configurable computing.

Module I: (14 Hrs)

Introduction to Cloud Computing- The Evolution of Cloud Computing – Hardware Evolution – Internet Software Evolution – Server Virtualization - Web Services Deliver from the Cloud – Communication-as-a-Service – Infrastructure-as-a-Service – Monitoring-as-a-Service – Platform-as-a-Service – Software-as-a-Service – Building Cloud Network. Federation in the Cloud - Presence in the Cloud - Privacy and its Relation to Cloud-Based Information Systems – Security in the Cloud - Common Standards in the Cloud – End-User Access to the Cloud Computing

Module II: (15 Hrs)

Introduction - Advancing towards a Utility Model – Evolving IT infrastructure – Evolving Software Applications – Continuum of Utilities- Standards and Working Groups – Standards Bodies and Working Groups – Service Oriented Architecture – Business Process Execution Language – Interoperability Standards for Data Center Management - Utility Computing Technology – Virtualization – Hyper Threading – Blade Servers - Automated Provisioning - Policy Based Automation – Application Management – Evaluating Utility Management Technology - Virtual Test and development Environment - Data Center Challenges and Solutions - Automating the Data Center

Module III: 10 Hrs)

Software Utility Application Architecture - Characteristics of an SaaS - Software Utility Applications - Cost Versus Value - Software Application Services Framework – Common Enablers – Conceptual view to Reality – Business Profits - Implementing Database Systems for Multitenant Architecture

Module IV: (12 Hrs)

Other Design Considerations - Design of a Web Services Metering Interface – Application Monitoring Implementation - A Design for an Update and Notification Policy - Transforming to Software as a Service - Application Transformation Program – Business Model Scenarios - Virtual Services for Organizations - The Future.

References

1. John W. Rittinghouse and ames F. Ransome, “Cloud Computing Implementation, Management and Security”, CRC Press, Taylor & Francis Group, Boca Raton London New York. 2010 [Unit -11and Unit II]
2. Alfredo Mendoza, “Utility Computing Technologies, Standards, and Strategies”, Artech House INC, 2007. [Unit -11I to Unit V]
3. Guy Bunker and Darren Thomson, “Delivering Utility Computing”, John Wiley &

Sons Ltd, 2006.

Internal continuous assessment: 100 marks
Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern
Answer any 5 questions by choosing at least one question from each module.

Module I
Question 1: 20 marks
Question 2: 20 marks

Module II
Question 3: 20 marks
Question 4: 20 marks

Module III
Question 5: 20 marks
Question 6: 20 marks

Module IV
Question 7: 20 marks
Question 8: 20 marks

MCY 10 302 (B) CRYPTOCOMPLEXITY

Prerequisite: Analysis of Algorithms

Teaching scheme:

Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:

To provide the students with the concepts of cryptology and complexity theory. Discusses the different protocols like diffie hellman, elgamal etc and randomized algorithms and complexity classes.

Module I: (12 hours)
Review of Relevant Mathematics, Complexity Theory, Foundations of Cryptology, Hierarchies based on NP.

Module II: (13 hrs)
Randomized algorithms and Complexity classes, probabilistic Polynomial time classes,Quantifiers, Graph Isomorphism and lowness.

Module III: (13 hrs)
RSA Cryptosystem, Primality and factoring, Primality Tests, Factoring Methods, Security of RSA.

Module IV: (14 hrs)
Diffie Hellman's, ElGamal's and other protocols, Arthur Merlin Games and Zero Knowledge.

References

1. Jorg Roth, *Complexity Theory and Cryptology – An introduction to cryptocomplexity*, Springer, 2005.
2. H. Anton, *Elementary Linear algebra*, John Wiley and Sons, New York, eighth edition,2000.
3. G. Brassard. *A note on the complexity of cryptography*, IEEE Transactions on Information Theory, 25(2):232-233, 1979

Internal continuous assessment: 100 marks
Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern

Answer any 5 questions by choosing at least one question from each module.

Module I

Question 1: 20 marks

Question 2: 20 marks

Module II

Question 3: 20 marks

Question 4: 20 marks

Module III

Question 5: 20 marks

Question 6: 20 marks

Module IV

Question 7: 20 marks

Question 8: 20 marks

MCY 10 302(C) SECURITY POLICIES AND ASSURANCE

Teaching scheme:

Credits: 4 *3 hours lecture & 1 hour tutorial per week*

Objective:

To impart knowledge to the students to know the standards of security policies, guidelines and procedures.

Module I: (10 Hrs)

Security policies, policy languages, confidentiality policies, Bell-LaPadula model, controversies over the model.

Module II: (12 Hrs)

Integrity policies, Biba model, Lipner's model, Clark-Wilson models, Chinese wall model, clinical information systems security policy, noninterference and policy composition.

Module III: (10 Hrs)

Assurance and trust, building secure and trusted systems, waterfall model, other models of development.

Module IV: (10 Hrs)

Assurance in requirements definition and analysis, assurance during system and software design, assurance during implementation and integration.

References:

1. M. Bishop, *Computer Security: Art and Science*, Pearson Education, 2003.
2. W. Mao, *Modern Cryptography: Theory & Practice*, Pearson Education, 2004.
3. C. P. Fleeger and S. L. Fleeger, *Security in Computing*, 3/e, Pearson Education, 2003.

Internal continuous assessment: 100 marks

Internal continuous assessment is in the form of periodical tests, assignments, seminars or a combination of all whichever suits best. There will be a minimum of two tests per subject. The assessment details are to be announced right at the beginning of the semester by the teacher.

End semester Examination: 100 marks

Question pattern
Answer any 5 questions by choosing at least one question from each module.

Module I
Question 1: 20 marks
Question 2: 20 marks

Module II
Question 3: 20 marks
Question 4: 20 marks

Module III
Question 5: 20 marks
Question 6: 20 marks

Module IV
Question 7: 20 marks
Question 8: 20 marks

MCY 10 303(P): INDUSTRIAL TRAINING

Teaching scheme: 1 hour per week **Credits:** 1

The students have to undergo an industrial training of minimum two weeks in an Industry during the semester break after second semester and complete within 15 calendar days from the start of third semester. The students have to submit a report of the training undergone and present the contents of the report before the evaluation committee constituted by the department. An internal evaluation will be conducted for examining the quality and authenticity of contents of the report and award the marks at the end of the semester.

Internal continuous assessment: Marks 50

MCY 10 304(P): MASTER'S RESEARCH PROJECT (PHASE – I)

Teaching scheme: 22 hours per week **Credits:** 6

Objective:

To improve the professional competency and research aptitude by touching the areas which otherwise not covered by theory or laboratory classes. The project work aims to develop the work practice in students to apply theoretical and practical tools/techniques to solve real life problems related to industry and current research.

The project work should be a project related to cyber security or allied topics.The project work is allotted individually on different topics. The students shall be encouraged to do their project work in the parent institute itself. If found essential, they may be permitted to do their project outside the parent institute subject to the conditions in clause 10 of M.Tech regulations. Department will constitute an Evaluation Committee to review the project work. The Evaluation committee consists of at least three faculty members of which internal guide and another expert in the specified area of the project shall be two essential members.

The student is required to undertake the masters research project phase-I during the third semester and the same is continued in the 4th semester.(Phase-II). Phase-I consists of preliminary thesis work, two reviews of the work and the submission of preliminary report. First review would highlight the topic, objectives, methodologyandexpected results. Second review evaluates the progress of the work, preliminary report and scope of the work which is to be completed in the 4th semester.

Internal Continuous assessment:

First Review:

Guide	- 50 marks
Evaluation Committee	- 50 marks

Second review:

Guide	- 100 marks
Evaluation Committee	- 100 marks

Total **- 300 marks**

SEMESTER IV

MCY 10 401(P): MASTER RESEARCH PROJECT PHASE 2

Teaching scheme: 30 hours per week **Credits:** 12

Objectives:

To improve the professional competency and research aptitude by touching the areas which otherwise not covered by theory or laboratory classes. The project work aims to develop the work practice in students to apply theoretical and practical tools/techniques to solve real life problems related to industry and current research.

Masters Research project phase-II is a continuation of project phase-I started in the third semester. Before the end of the fourth semester, there will be two reviews, one at middle of the fourth semester and other towards the end. In the first review, progress of the project work done is to be assessed. In the second review, the complete assessment (quality, quantum and authenticity) of the Thesis is to be evaluated. Both the reviews should be conducted by guide and Evaluation committee. This would be a pre qualifying exercise for the students for getting approval for the submission of the thesis. At least one technical paper is to be prepared for possible publication in journal or conferences. The technical paper is to be submitted along with the thesis. The final evaluation of the project will be external evaluation.

Internal Continuous assessment:

First review:

Guide	- 50 marks
Evaluation committee	- 50 marks

Second review:

Guide	- 100 marks
Evaluation committee	- 100 marks

End Semester Examination:

Project Evaluation by external examiner	-150 marks
Viva Voce by external / internal examiner	-150 marks (75 each)

Total **- 600 marks**