KERALA TECHNOLOGICAL UNIVERSITY

Master of Technology

Curriculum, Syllabus and Course Plan

Cluster : ***1***

Branch : ***Computer Science & Engineering***

Stream : ***Cyber Forensics and Information Security***

Year : ***2015***

SEMESTER 1

Examination Slot	Course Number	Name	L-T-P	Internal Marks	End Semester Examination		Credits
					Marks	Duration (hours)	
A	01MA6041	Engineering Mathematics and Statistics for Forensic Science	3-0-0	40	60	3	3
B	01CS6301	Computer Algorithms	3-1-0	40	60	3	4
C	01CS6303	Cyber Forensics Basics	3-1-0	40	60	3	4
D	01CS6305	Information Security Basics	3-0-0	40	60	3	3
E		Elective I	3-0-0	40	60	3	3
S	01CS6999	Research Methodology	0-2-0	100			2
T	01CS6391	Seminar I	0-0-2	100			2
U	01CS6393	Forensics Laboratory	0-0-2	100			1
		TOTAL	**15-4-4**	**500**	**300**	**-**	**22**

TOTAL CONTACT HOURS : 23
TOTAL CREDITS : 22

Elective I

01CS6311	File System Forensic Analysis
01CS6313	Applied Cryptography
01CS6315	Malware Forensics
01CS6317	Cloud Computing and Security

SEMESTER 2

Examination Slot	Course Number	Name	L-T-P	Internal Marks	End Semester Examination		Credits
					Marks	Duration (hours)	
A	01CS6302	Network and Wireless Security	3-1-0	40	60	3	4
B	01CS6304	Operating Systems Security	3-0-0	40	60	3	3
C	01CS6306	Ethical Hacking	3-0-0	40	60	3	3
D		Elective II	3-0-0	40	60	3	3
E		Elective III	3-0-0	40	60	3	3
V	01CS6392	Mini Project	0-0-4	100			2
U	01CS6394	Network and OS Security Laboratory	0-0-2	100			1
		TOTAL	**15-1-6**	**400**	**300**	**-**	**19**

TOTAL CONTACT HOURS : 22
TOTAL CREDITS : 19

Elective II

01CS6312 Web Security Testing

01CS6314 Windows and Linux Forensics

01CS6316 Virtual Forensics and Security

Elective III

01CS6318 Image Forensics and Security

01CS6322 Coding Theory

01CS6324 Digital Watermarking and Steganography

SEMESTER 3

Examination Slot	Course Number	Name	L-T-P	Internal Marks	End Semester Examination		Credits
					Marks	Duration (hours)	
A		Elective IV	3-0-0	40	60	3	3
B		Elective V	3-0-0	40	60	3	3
T	01CS7391	Seminar II	0-0-2	100			2
W	01CS7393	Project (Phase 1)	0-0-12	50			6
		TOTAL	**6-0-14**	**230**	**120**	**-**	**14**

TOTAL CONTACT HOURS : 20
TOTAL CREDITS : 14

Elective IV

01CS7311 Security Policies and Governance
01CS7313 Biometric Security
01CS7315 Data Compression
01CS7317 Neural Networks

Elective V

01CS7319 Advanced Operating System Design
01CS7321 Parallel Architectures and Algorithms
01CS7323 Cyber Crimes and Legal Issues
01CS7325 Theory of Computation

SEMESTER 4

Examination Slot	Course Number	Name	L-T-P	Internal Marks	End Semester Examination		Credit
					Marks	Duration (hours)	
W	01CS7394	Project (Phase 2)	0-0-23	70	30		12
		TOTAL	**0-0-23**	**70**	**30**	**-**	**12**

TOTAL CONTACT HOURS : 23
TOTAL CREDITS : 12

TOTAL NUMBER OF CREDITS: 67

SEMESTER - I

Syllabus and Course Plan

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01MA6041	Engineering Mathematics and Statistics for Forensic Science	**3-0-0**	**3**	**2015**

Course Objectives

- Understand the principles and problems of computation of mathematics.

Syllabus

Counting- Basic counting, Functions, Functions as relations, Graphs, Warshall'salgorithm, Cryptography and Modular Arithmetic, Introduction to Cryptography, Private Key cryptography, Public-key Cryptosystems, Recursion Trees, Three Different Behaviors, Master Theorem, Solving More General Kinds of Recurrences, Probability and probability computations.

Expected Outcome

- Students gain in-depth the principles and problems of computation of mathematics.

References

1. Discrete Mathematics for Computer Science- Kenneth Bogart, Clifford Stein, Key Curriculum Press, 2006
2. Schaum's Outline Discrete Mathematics - Seymour Lipschutz and Marc Lipson,Third Edition, McGraw Hill, 2007.
3. Discrete Mathematics using a Computer- John O' Donnell, Cordelia Hall, Rex Page, Springer- Verlag, 2006

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Counting- Basic counting-The Sum Principle, Abstraction, Summing consecutive integers, The Product Principle, Two-Element subsets, Important Concepts, Formulas, and Theorems, Counting Lists, Permutations and Subsets- Using the Sum and Product Principles, Lists and functions, The Bijection Principle, *k*-element permutations of a set, Counting subsets of a set, Binomial coefficients-Pascal's Triangle , A proof using the Sum Principle.	5	15
	The Binomial Theorem, Labeling and trinomial coefficients, equivalence relations and counting-The Symmetry Principle, Equivalence Relations, The Quotient Principle, Equivalence class counting, Multisets, The bookcase arrangement problem, The number of *k*-element multisets of an *n*-element set, Using the quotient principle to explain a quotient.	3	
II	Functions, Functions as relations, One-to-One, Onto and Invertible functions, Mathematical functions, Exponential and Logarithmic functions, Sequences, Indexed classes of Sets, Recursion, First order linear recurrences.	2	15
	Iterating a recurrence, Geometric series, Recursively defined functions, Cardinality, Algorithms and functions, Complexity of algorithms, Mathematical Induction, Strong Induction, Induction in general	3	
FIRST INTERNAL EXAM			
III	Graphs- The degree of a vertex, Paths, Connectivity, Cycles, Trees, Other Properties of Trees, Multigraphs, Planar graphs, Representing graphs in computer memory, Graph algorithms, Directed graphs, Basic definitions, Spanning trees, Rooted Trees	3	20
	Warshall'salgorithm: Shortest paths, Linked representation of directed graphs, Pruning algorithm for shortest path, Dijkstra's shortest path algorithm, Matching Theory- The idea of a matching, Making matchings bigger, Matching in Bipartite Graphs, The Augmentation-Cover algorithm.	3	
IV	Cryptography and Modular Arithmetic, Introduction to Cryptography, Private Key cryptography, Public-key Cryptosystems, Arithmetic modulo *n*, Cryptography using multiplication mod *n*, Solutions to Equations and Inverses mod *n*, Inverses mod *n* , Converting Modular	4	20

	Equations to Normal Equations, GCD, Euclid's Division Theorem		
	The GCD Algorithm, Extended GCD algorithm, Computing Inverses, Exponentiation mod n, The Rules of Exponents, Fermat's Little Theorem, The RSA Cryptosystem, The Chinese Remainder Theorem, Practical Aspects of Exponentiation mod n , Finding large primes.	4	
SECOND INTERNAL EXAM			
V	Recursion Trees, Three Different Behaviors, Master Theorem, Solving More General Kinds of Recurrences, Recurrence Inequalities	3	20
	Recurrences and Selection, The idea of selection, A recursive selection algorithm, Selection without knowing the median in advance, An algorithm to find an element in the middle half, Uneven Divisions.	4	
VI	Introduction to Probability, Some examples of probability computations, Complementary probabilities, Probability and hashing, The Uniform Probability Distribution, The probability of a union of events, Principle of inclusion and exclusion for probability.	4	10
	The principle of inclusion and exclusion for counting, Conditional Probability, Independence, Tree diagrams, What are Random Variables?, Binomial Probabilities, Expected Value, Expected Values of Sums and Numerical Multiples, Probability Calculations in Hashing, Conditional Expectations, Recurrences and Algorithms, Probability Distributions and Variance.	4	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6301	Computer Algorithms	3-1-0	4	2015

Course Objectives

- The course provides a comprehensive introduction to the modern study of computer algorithms**.** Each topic includes an algorithm, a design technique, an application area or a related topic.

Syllabus

The Role of Algorithms in Computing, Growth of Functions, Recurrences, Heap sort ,Quicksort ,Sorting in Linear Time, Elementary Data Structures ,Hash Tables ,Binary Search Trees , Red-Black Trees ,Augmenting Data Structures, Dynamic programming, Greedy Algorithms, Amortized analysis, B-Trees, Binomial Heaps , Fibonacci Heaps, Data Structures for Disjoint Sets, Graph Algorithms- Elementary Graph Algorithms , Minimum Spanning Trees , Single-Source Shortest Paths , All-Pairs Shortest Paths , Maximum Flow, String Matching

Expected Outcome

- The students will be familiarized with specific algorithms for a number of important computational problems like sorting, searching, and graphs, etc.
- The student will be able to decide on the suitability of a specific algorithm design technique for a given problem.
- They will also be able to design efficient algorithms.

References

1. Cormen, Thomas H, Leiserson, Charles E & Rivest, Ronald L, "Introduction to Algorithms", Prentice Hall of India Private Limited, New Delhi, Third Edition, 2009
2. Horowitz, Sahni, Rajasekharan ,"Computer Algorithms", Silicon Press, 2nd edition, 2008
3. Jon Kleinberg and Eva Tardos "Algorithm Design", AW ,2005

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	The role of algorithms in computing, Insertion sort, Analyzing algorithms, Designing algorithms, Growth of functions- Asymptotic notations, Standard notations & common functions, Divide-and-Conquer – The maximum-subarray problem, Strassen's algorithm for matrix multiplication	6	15
	The substitution method for solving recurrences, The recursion-tree method for solving recurrences, The master method for solving recurrences, Proof of the master theorem.	4	
II	Heap sort- The heap sort algorithm, Priority queues, Quicksort- Description of quick sort, Performance of quick sort, Analysis of quicksort.	5	20
	Sorting in Linear time- Lower bounds for sorting, Counting sort, Radix sort, Bucket sort ,Hash tables- Direct-address tables, Hash tables, Hash functions, Open addressing, Perfect hashing.	5	
FIRST INTERNAL EXAM			
III	Binary search trees, Randomly built binary search trees, Red-black tree- Properties, Insertion, Deletion, Rotations, Augmenting Data Structures- Dynamic order statistics, Interval trees.	6	20
	Dynamic programming- Rod cutting, Matrix chain multiplication, Longest common subsequence, Optimal binary search trees.	4	
IV	Greedy Algorithms- An activity selection problem, Elements of the greedy strategy, Huffman codes, Matroids and greedy methods, A task scheduling problem as a matroid.	4	15
	Amortized analysis- Aggregate analysis, the Accounting method, The potential method, Dynamic tables. B-Trees, Fibonacci Heaps, van Emde Boas trees, Data structures for disjoint sets.	5	

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
SECOND INTERNAL EXAM			
V	Graph Algorithms–BFS, DFS, Topological sort, strongly connected components, Growing a minimum spanning tree, The algorithms of Kruskal and Prim	3	20
	The Bellman-Ford algorithm, Single-source shortest paths in directed acyclic graphs, Dijkstra's algorithm, Difference constraints and shortest paths, Proofs of shortest-paths properties, Shortest paths and matrix multiplication, The Floyd-Warshall algorithm, Johnson's algorithm for sparse graphs.	6	
VI	Flow networks- The Ford-Fulkerson method, Maximum bipartite matching, Push-relabel algorithms, The relabel-to-front algorithm.	3	10
	The naive string-matching algorithm, The Rabin-Karp algorithm, String matching with finite automata, The Knuth-Morris-Pratt algorithm, Line-segment properties, segments intersections, convex hull, closest pair of points	5	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6303	Cyber Forensics Basics	**3-1-0**	**4**	**2015**

Course Objectives

- To understand concepts, developments, challenges, and directions in cyber Forensics
- Understanding Laws relating to computer crime investigations
- An in-depth study of each phases involved in a forensics investigation processes

Syllabus

Introduction to Computer Forensics, Understanding Computer Investigations , Requirements for forensic lab certification **,** Data Acquisition , Processing Crime and Incident Scene, Working with windows and DOS systems, Analysis and validation , Recovering Graphics Files , Network Forensics , Email Investigations , Cell Phone and Mobile Device forensics **,** Report writing for high tech investigations , Expert Testimony in High Tech Investigations **,** Ethics for the Expert Witness

Expected Outcome

- The student will be able to understand the role and importance of digital forensics
- Will be able to conduct a forensics investigation using standard procedures
- Will have relevant knowledge in report writing

References

1. Bill Nelson, Amelia Phillips, Frank Enfinger, Christofer Steuart , "Computer Forensics and Investigations", Second Indian Reprint , Cengage Learning India Private Limited,2009**.**
2. Eoghan Casey , "Digital Evidence and Computer Crime ", Edition 3, Academic Press, 2011

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Introduction to Computer Forensics, history of computer forensics, understanding case law, developing computer forensics resources, preparing for computer investigations, understanding law enforcement agency investigations, understanding corporate investigations, maintaining professional conduct	4	10
	Understanding Computer Investigations - Preparing a computer investigation, taking a systematic approach, procedures for corporate high tech investigations, understanding data recovery workstations and software, conducting an investigation, completing the case. Requirements for forensic lab certification-determining the physical requirements for a computer forensics lab, selecting a basic forensic workstation, building a business case for developing a forensic lab.	5	
II	Data Acquisition - storage formats for digital evidence, determining the best acquisition method, contingency planning for image acquisitions, using acquisition tools, validating data acquisitions, performing RAID data acquisitions, using remote network acquisition tools, using other forensic acquisition tools	5	20
	Processing Crime and Incident Scene -identifying digital evidence, collecting evidence in private sector incident scenes, processing law enforcement crime scenes, preparing for a search, securing a computer incident or crime scene, Seizing digital evidence at the scene, storing digital evidence, obtaining a digital hash.	5	

FIRST INTERNAL EXAM			
III	Working with windows and DOS systems - whole disk encryption, the windows registry, Microsoft and MS-DOS start up tasks, virtual machines.	4	15
	Evaluating Computer Forensics Tool needs- computer forensics software and hardware tools, validating and testing forensics software. the Macintosh file structure and boot process, examining UNIX and LINUX disk structures and boot processes, examining CD data structures, examining SCSI Disk, examining IDE/EIDE and SATA devices	6	
IV	Analysis and validation-determining what data to collect and analyse, validating forensic data, addressing data-hiding techniques, performing remote acquisitions.	4	20
	Recovering Graphics Files-Recognizing, locating and recovering graphic files, understanding data compression, copy rights issues with graphics, identifying unknown file formats, copyright issues with graphics.	3	
	Network Forensics-overview, performing live acquisitions, developing standard procedures for network forensics, using network tools.	3	
SECOND INTERNAL EXAM			
V	Email Investigations-role of E-mail in investigations, exploring the roles of the client and server, investigating email crimes and violations, understanding E-mail servers, specialized E-mail forensic tools	5	20
	Cell Phone and Mobile Device forensics- Mobile device forensics, acquisition procedures for cell phones and mobile devices	4	
VI	Report writing for high tech investigations – importance of reports, guidelines for writing, generating report findings with forensics software tools	3	15
	Expert Testimony in High Tech Investigations- Preparing for testimony, testifying in court, preparing for a deposition or hearing, preparing Forensic evidence for testimony. Ethics for the Expert Witness-applying ethics and codes to expert witnesses, organizations with codes of ethics, ethical difficulties in expert testimony	3	
		2	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6305	Information Security Basics	**3-0-0**	**3**	**2015**

Course Objectives

- To understand the concepts of Information Security.

Syllabus

Information Security, Components of an Information system, The systems development life cycle, The need for security, Threats, Attacks, Laws and ethics in Information security, Risk management, Risk identification, Risk assessment, Risk Management discussions: Residual risks, Documenting results.

Expected Outcome

- Upon successful completion of this course, the students will get an in-depth knowledge in information security.

References

1. Principles of Information Security- Michael E. Whitman, Herbert J. Mattord, Cengage Learning, Fourth edition, 2011
2. Computer Security basics- Rick Lehtinen, O'Reilly, 2nd edition, 2006
3. Information Security Management Principles- Andy Taylor, David Alexander, Amanda Finch, David Sutton, BCS publishers, 2008

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Introduction to Information Security, The history of Information security, What is security, security concepts, characteristics of information, CNSS security model	4	15
	Components of an Information system, Balancing Information security and access, Approaches to Information security implementation, The systems development life cycle, The security systems development life cycle.	4	
II	The need for security- Introduction, Threats- Compromises to individual property	3	20
	Deliberate software attacks, Deviations in quality of service, Espionage, Sabotage, Theft.	3	
FIRST INTERNAL EXAM			
III	Attacks- Malicious code, Hoaxes, Back doors, Password crack, Brute force, Dictionary, Denial of service and Distributed denial of service, Spoofing, Man-in-the-middle, Spam, Mail bombing, Sniffers.	4	20
	Social Engineering, Pharming, Timing attack, Secure software development.	3	
IV	Laws and ethics in Information security, General computer crime laws, Privacy, Export and espionage law, State and local regulations	3	15
	International laws and legal bodies, Ethical differences across cultures, Ethical decision evaluation, Ethics and education, Deterring unethical and illegal behavior.	3	
SECOND INTERNAL EXAM			
V	Risk management- Overview, types, Risk identification: components of risk identification, asset identification, people, procedures and data,	4	20

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
	hardwares/softwares.		
	Data classification and management, classifying and prioritizing information assets, information asset valuation, identifying and prioritizing threats, vulnerability identification, TVA worksheet.	3	
VI	Risk assessment: risk determination, identify possible controls, documenting the results, Risk control strategies- defend, transfer, mitigate, IR plan, DR plan, BC plan, accept, terminate	4	10
	CBA analysis, CBA formula, Risk appetite, Risk Management discussions: Residual risks, Documenting results	4	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6311	File System Forensics Analysis	**3-0-0**	**3**	**2015**

Course Objectives

- To understand the concepts of advanced analysis of the FAT, NTFS, EXT, and UFS file systems.
- It provides a clear understanding about how data is stored at the file system level.
- A focus is placed on specific artifacts that would be of value to a forensic examiner.

Syllabus

Digital investigation foundation, Computer foundations, Hard disk data acquisition, Volume Analysis, PC based partitions, Server based partitions, File system analysis, FAT concepts and analysis, FAT data structure, NTFS concepts and analysis, NTFS data structure, Ext2 and Ext3 concepts, Ext2 and Ext3 data structures, UFS1 and UFS2 concepts and analysis, UFS1 and UFS2 data structures.

Expected Outcome

- The student will have an in-depth knowledge about basic concepts and theory of a volume and file systems and their analysis techniques.
- The student will be able to analyze disk images and identify various data in different file systems.

References

1. Brian Carrier , "File System Forensic Analysis" , Addison Wesley, 2005
2. Casey, Eoghan, "Digital Evidence and Computer Crime", edition 2, Academic Press, 2004.
3. Bill Nelson, Amelia Phillips, Frank Enfinger, Chris Steuart, "Guide to Computer Forensics and Investigations", Thomson Course Technology, 2004
4. Dan Farmer & Wietse Venema ,"Forensic Discovery", Addison Wesley, 2005

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Digital investigation foundation- Digital investigations and evidence, Digital crime scene investigation process, Data analysis, overview of toolkits.	2	15
	Computer foundations- Data organizations, booting process, Hard disk technology, Hard disk data acquisition- introduction, reading the source data, writing the output data, a case study.	4	
II	Volume Analysis – Introduction, Background, Analysis Basics, PC based partitions- DOS partitions, Analysis considerations, Apple partitions, removable media.	3	15
	Server based partitions- BSD partitions, Sun Solaris slices, GPT partitions, Multiple disk volumes- RAID, Disk Spanning.	3	
FIRST INTERNAL EXAM			
III	File system analysis- What is a file system, File system category, Content category, Metadata category, Filename category, Application category, Application-level search techniques, Specific file systems.	2	20
	FAT concepts and analysis - Introduction, File system category, Content category, Metadata category, File name category, The big picture, File recovery, determining the type, Consistency check., FAT data structure – Boot sector, FAT 32 FS info, FAT, Directory entries, Long file name directory entries.	6	
IV	NTFS concepts- Introduction, Everything is a file, MFT concepts, MFT entry attribute concepts, Other attribute concepts, Indexes, Analysis tools.	2	15
	NTFS Analysis- File system category, Content category, Metadata category, File name category, The big picture, File recovery, determining the type, Consistency check. NTFS data structure- Basic concepts, Standard file attributes, Index attributes and data structures, File system metadata files.	6	

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
SECOND INTERNAL EXAM			
V	Ext2 and Ext3 concepts- File system category, Content category, Metadata category, File name category, The big picture, File recovery, determining the type, Consistency check.	4	20
	Ext2 and Ext3 data structures- Super block, group descriptor tables, Block bitmap, Inodes, Extended attributes, Directory Entry, Symbolic Link, Hash trees, Journal data structures.	4	
VI	UFS1 and UFS2 concepts and analysis- Introduction, File system category, Content category, Metadata category, File name category, The big picture, File recovery, determining the type, Consistency check.	3	15
	UFS1 and UFS2 data structures- UFS1 superblock, UFS2 superblock, Cylinder group summary, UFS1 group descriptor, UFS2 group descriptor, Block and fragment bitmaps, UFS1 Inodes, UFS2 Inodes, UFS2 Extended attributes, Directory entries.	3	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6313	Applied Cryptography	**3-0-0**	**3**	**2015**

Course Objectives

- To understand the concepts of Applied Cryptography

Syllabus

Cryptography basics, Cryptographic protocols, Intermediate protocols, Advanced protocols, Various Cryptographic techniques, Algorithms types and modes, Study of various Cryptographic algorithms and applications.

Expected Outcome

- Students will get an in-depth knowledge in applied cryptography.

References

1. Jonathan Katz, Yehuda Lindell, " Introduction to Modern Cryptography", Edition 1,Chapman and Hall/CRC, 2007
2. Chritof Paar, Jan Pelzl, Bart Preneel, " Understanding Cryptography", Edition 2, Springer , 2010
3. Carl Meyer, SM Matyas," Cryptography: A New Dimension in Computer Data Security", John Wiley & Sons, 1982

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Introduction and preliminaries, Cryptographic protocols, Protocol Building Blocks- Communication using symmetric cryptography, One-way functions, One-way Hash functions, Communications using Public key cryptography, Digital signatures with encryption, Random and pseudo-random sequence generation	**4**	15
	Basic protocols- Authentication and key exchange, Formal analysis of authentication and key exchange protocols, Multiple- key Public-key cryptography, Secret splitting, Secret sharing, cryptographic protection of databases	**4**	
II	Intermediate protocols- Time stamping services, Subliminal channel, Undeniable digital signatures, Designated Confirmer signatures, Proxy signatures, Group signatures, Fail-stop digital signatures	**4**	15
	Computing with encrypted data, Bit Commitment, Fair coin flips, Mental Poker, One-way accumulators, All-or-nothing disclosure of secrets, Key escrow	**2**	
FIRST INTERNAL EXAM			
III	Advanced protocols- Zero-knowledge proofs, Blind Signatures, Identity-Based public-key cryptography, Oblivious transfer, Oblivious signatures, Simultaneous contract signing, Digital certified mail, Simultaneous exchange of secrets	**3**	15
	Esoteric protocols- Secure elections, Secure multiparty computation, Anonymous message broadcast, Digital cash	**3**	
IV	Cryptographic techniques- Key Length- Symmetric key length, Public-key key length, Birthday attacks against One-Way Hash functions, Caveat Emptor, Key Management- Generating keys	**3**	15
	Nonlinear keyspaces, Transferring ,Verifying, Using, Updating and Storing keys, Backup Keys, Compromised keys, Lifetime of keys, Destroying keys, Public-key management	4	
SECOND INTERNAL EXAM			

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
V	Algorithms types and Modes- Electronic Codebook mode, Block replay, Cipher block chaining mode, Stream ciphers- Self-synchronizing, Cipher feedback mode, Synchronous ciphers, Output feedback mode, Counter mode, Other block-cipher modes, Choosing a cipher mode, Interleaving	4	20
	Choosing an algorithm, Public key cryptography versus Symmetric cryptography, Encrypting communication channels, Encrypting data for storage, Hardware versus software encryption.	3	
VI	Cryptographic algorithms- Information theory, Complexity theory, Number theory, Data Encryption and Standard-Description, Security, Differential and Linear cryptanalysis, DES variants, Block Ciphers- Lucifer, NewDES, FEAL,RC2, IDEA, MMB	4	20
	Other Block algorithms, Theory of Block Cipher Design, Using One-Way Hash functions, Choosing a block algorithm, One-Way Hash Functions- MD2, MD4,MD5, SHA,HAVAL, Using symmetric key algorithms, Using public key algorithms, Knapsack, RSA, DSA, Secret-sharing algorithms.	4	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6315	Malware Forensics	**3-0-0**	**3**	**2015**

Course Objectives

- To provide students with the core knowledge, skills and tools needed to combat the growing malware attacks against Windows and Linux systems.

Syllabus

Malware Incident response: Volatile Data Collection and Examination and Non-volatile Data collection from a live Windows and Linux systems, Tools for conducting Memory Forensics in Windows and Linux systems, Post-Mortem Forensics which involves Malware Discovery and Extraction from a Windows and Linux system, Overview of the File Profiling process in Windows and Linux system, Analysis of malware specimen in Windows and Linux systems.

Expected Outcome

- Students will have the ability to identify malware on Windows and Linux systems.
- Examine malware to uncover its functionality and purpose.
- Determine malware impact on subject system.

References

1. James M. Aquilina, Cameron H. Malin, Eoghan Casey , Malware Forensics Field Guide for Windows Systems: Digital Forensics Field Guides, Syngress Publishing, 2012
2. James M. Aquilina, Cameron H. Malin, Eoghan Casey , Malware Forensics Field Guide for Linux Systems: Digital Forensics Field Guides, Syngress Publishing, 2014
3. James M. Aquilina, Eoghan Casey, Cameron H. Malin, Malware Forensics Investigating and Analyzing Malicious code, Syngress Publishing, 2008

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Malware Incident response: Volatile Data Collection and Examination on a Live Windows and Linux Systems - Volatile Data collection methodology from Windows and Linux systems,	3	15
	Collecting process information from Windows systems, Correlate open ports with running processes and programs from windows system, Non-volatile Data collection from a live Windows and Linux systems.	2	
II	Memory Forensics: Analyzing Physical and Process Dumps for Malware Artifacts- Memory Forensics Overview, Windows Memory Forensics Tools, How Windows Memory Forensics Tools work, Windows Process Memory Dumping and dissecting	4	20
	Linux Memory Forensics Tools, How Linux Memory Forensics Tools work, interpreting various data structures in Linux memory, Linux Process Memory Dumping and Dissecting.	3	
FIRST INTERNAL EXAM			
III	Post-Mortem Forensics - Malware Discovery and Extraction from a Windows and Linux system, Examine Windows and Linux file system , Examine application traces	4	20
	Examine Windows registry, keyword searching from Windows and Linux systems, Forensic reconstruction of compromised Linux and Windows system.	3	
IV	File Identification and profiling: Initial Analysis of a suspect file on a Windows and Linux system-Overview of the File Profiling process, Working with Linux Executables.	5	20
	similarity indexing, File Visualization, Symbolic and Debug information, edded file metadata, File Obfuscation, Elf file structure, Profiling suspect ment files in windows	5	
SECOND INTERNAL EXAM			

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
V	Analysis of malware specimen in Windows and Linux- Analysis Goals, Guidelines for examining a malicious executable program.	3	15
	Establishing the environment baseline, Pre-execution preparation: system and network monitoring, Observing, File system.	2	
VI	Analysis of malware specimen in Windows and Linux- Execution trajectory analysis, Embedded Artifact Extraction revisited Exploring and verifying specimen functionality and purpose.	4	10
	Event reconstruction and artifact review: File system, Registry, Process and Network Activity Post-run Data Analysis	4	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6317	Cloud Computing and Security	**3-0-0**	**3**	**2015**

Course Objectives

- To understand the concepts of cloud computing and architecture.
- Understand the challenges, applications and services of cloud computing.
- To understand the security concepts and virtualization in cloud computing.

Syllabus

Cloud Computing Fundamentals, Cloud types, Benefits and challenges of cloud computing and cloud architecture, Cloud Applications, its advantages and disadvantages, Cloud Services Management, Cloud Economics, Application Development, Cloud IT Model, Security Concepts, Virtualization System Vulnerabilities.

Expected Outcome

- In-depth knowledge of cloud computing and security.

References

1. Tim Mather, SubraKumaraswamy, ShahedLatif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance" O'Reilly Media; 1 edition [ISBN: 0596802765], 2009.
2. Toby Velte, Anthony Velte, Robert Elsenpeter, Cloud Computing, A Practical Approach [ISBN: 0071626948]

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Cloud Computing Fundamentals: Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing, public vs private clouds, role of virtualization in enabling the cloud.	4	15
	Business Agility: Benefits and challenges to Cloud architecture. Application availability, performance, security and disaster recovery; next generation Cloud Applications.	3	
II	Cloud Applications: Technologies and the processes required when deploying web services	4	15
	Deploying a web service from inside and outside a cloud architecture, advantages and disadvantages.	3	
FIRST INTERNAL EXAM			
III	Cloud Services Management: Reliability, availability and security of services deployed from the cloud. Performance and scalability of services, tools and technologies used to manage cloud services deployment	3	20
	Cloud Economics: Cloud Computing infrastructures available for implementing cloud based services.	3	
IV	Application Development: Service creation environments to develop cloud based applications.	3	20
	Development environments for service development; Amazon, Azure, Google App.	3	
SECOND INTERNAL EXAM			
V	Cloud IT Model: Analysis of Case Studies when deciding to adopt cloud computing architecture. How to decide if the cloud is right for your requirements.	4	20
	Cloud based service, applications and development platform	3	

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
	deployment so as to improve the total cost of ownership (TCO)		
VI	Security Concepts: Confidentiality, privacy, integrity, authentication, non-repudiation, availability, access control, defence in depth, least privilege, how these concepts apply in the cloud, what these concepts mean and their importance in PaaS, IaaS and SaaS. e.g. User authentication in the cloud.	5	10
	Multi-tenancy Issues: Isolation of users/VMs from each other. How the cloud provider can provide this; Virtualization System Security Issues: e.g. ESX and ESXi Security, ESX file system security, storage considerations, backup and recovery; Virtualization System Vulnerabilities: Management console vulnerabilities, management server vulnerabilities, administrative VM vulnerabilities, guest VM vulnerabilities, hypervisor vulnerabilities, hypervisor escape vulnerabilities, configuration issues, malware (botnets etc).	4	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6999	Research methodology	0-2-0	2	2015

Course Objectives

1. To prepare the student to do the M. Tech project work with a research bias.
2. To formulate a viable research question.
3. To develop skill in the critical analysis of research articles and reports.
4. To analyze the benefits and drawbacks of different methodologies.
5. To understand how to write a technical paper based on research findings.

Syllabus

Introduction to Research Methodology-Types of research- Ethical issues- Copy right-royalty-Intellectual property rights and patent law-Copyleft- Openacess-
Analysis of sample research papers to understand various aspects of research methodology:
Defining and formulating the research problem-Literature review-Development of working hypothesis-Research design and methods- Data Collection and analysis- Technical writing- Project work on a simple research problem

Approach

Course focuses on students' application of the course content to their unique research interests. The various topics will be addressed through hands on sessions.

Expected Outcome

Upon successful completion of this course, students will be able to
1. Understand research concepts in terms of identifying the research problem
2. Propose possible solutions based on research
3. Write a technical paper based on the findings.
4. Get a good exposure to a domain of interest.
5. Get a good domain and experience to pursue future research activities.

References

1. C. R. Kothari, Research Methodology, New Age International, 2004
2. Panneerselvam, Research Methodology, Prentice Hall of India, New Delhi, 2012.
3. J. W. Bames, Statistical Analysis for Engineers and Scientists, Tata McGraw-Hill, New York.
4. Donald Cooper, Business Research Methods, Tata McGraw-Hill, New Delhi.
5. Leedy P. D., Practical Research: Planning and Design, McMillan 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 ofIndia, New Delhi, 2012.

COURSE PLAN

Module	Contents	Hours Allotted	% of Marks in End-Semester Examination
I	Introduction to Research Methodology: Motivation towards research - Types of research: Find examples from literature. Professional ethics in research - Ethical issues-ethical committees. Copy right - royalty - Intellectual property rights and patent law - Copyleft-Openacess -Reproduction of published material - Plagiarism - Citation and acknowledgement. Impact factor. Identifying major conferences and important journals in the concerned area. Collection of at least 4 papers in the area.	5	
II	Defining and formulating the research problem - Literature Survey- Analyze the chosen papers and understand how the authors have undertaken literature review, identified the research gaps, arrived at their objectives, formulated their problem and developed a hypothesis.	4	
FIRST ASSESSMENT			
III	Research design and methods: Analyze the chosen papers to understand formulation of research methods and analytical and experimental methods used. Study of how different it is from previous works.	4	No end semester written examination
IV	Data Collection and analysis. Analyze the chosen papers and study the methods of data collection used. - Data Processing and Analysis strategies used – Study the tools used for analyzing the data.	5	
SECOND ASSESSMENT			

V	Technical writing - Structure and components, contents of a typical technical paper, difference between abstract and conclusion, layout, illustrations and tables, bibliography, referencing and footnotes- use of tools like Latex.	5	
VI	Identification of a simple research problem – Literature survey- Research design- Methodology –paper writing based on a hypothetical result.	5	
END SEMESTER ASSESSMENT			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6391	SEMINAR I	**0-0-2**	**2**	**2015**

Course Objectives

To make students

1. Identify the current topics in the specific stream.
2. Collect the recent publications related to the identified topics.
3. Do a detailed study of a selected topic based on current journals, published papers and books.
4. Present a seminar on the selected topic on which a detailed study has been done.
5. Improve the writing and presentation skills.

Approach

Students shall make a presentation for 20-25 minutes based on the detailed study of the topic and submit a report based on the study.

Expected Outcome

Upon successful completion of the seminar, the student should be able to

1. Get good exposure in the current topics in the specific stream.
2. Improve the writing and presentation skills.
3. Explore domains of interest so as to pursue the course project

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6393	Forensics Laboratory	**0-0-2**	**1**	**2015**

Course Objectives

- To analyze a particular media if any information of evidentiary value is contained within it and generate report of those findings using several forensics tools.

Syllabus

Familiarization of various cyber forensics tools such as FTK, Prodiscover, Encase, Cyber Check for forensic applications.

Expected Outcome

- The student will have hands on experience on all the stages of cybercrime investigation using several forensics tools like FTK, Encase, ProDiscover, CyberCheck.

Experiments

Experiment No.	Description	Hours Allotted
1	Analyze an Image file using FTK	2
2	Analyze an Image file using ProDiscover	2
3	Analyze an Image file using Encase	2
4	Analyze an Image file using Cybercheck	2
5	Addressing Data Hiding Techniques using Hex Workshop/Win hex	2
6	Examining disk partitions using Norton Disk Edit/Hex Workshop	2
7	Extraction and Examination of Registry files	2

8	Creating a Virtual Machine	2
9	Validating using Hexadecimal Editors	1
10	Examining Graphics File	2
11	Familiarizing Ps Tools	2
12	Examining Email messages	2
13	Acquisition and analysis using MobileCheck	2
14	Generate Report using ProDiscover	2
15	Generate Report using FTK	1

SEMESTER – II

Syllabus and Course Plan

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6302	Network and Wireless Security	**3-1-0**	**4**	**2015**

Course Objectives

- To provide comprehensive coverage of the fundamental concepts of network and wireless security and the processes and means required to implement a secure network.

Syllabus

Network security, principles, Database Security, Windows Security, Attacks against the Windows workstation, Linux Security, Web Browser and Client risk, E-mail security, Domain Name System, Cryptography, Steganography, Digital Watermarking, Wireless Security, Security In Data Networks.

Expected Outcome

- The student will be familiar with the popular operating systems, Internet security, and Web security. Wireless communications, network architectures and cryptography provides an understanding of networking and communications.
- The student will also have an idea about intrusion detection and information security assessment methodologies.

References

1. Eric Cole, Ronald Krutz, James W. Conley, Network Security Bible, Edition Wiley India Pvt Ltd, 2010
2. William Stallings, Network Security Essentials , Edition 4, Pearson Education, 2011
3. Eric Maiwald , Fundamentals of Network Security , Tata McGraw-Hill, 2011
   William Stallings, Cryptography and Network Security, Pearson Education,Edition 4, 2010

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	An enterprise Security Methodology, Key principles of network security. E-mail security- The e-mail risk, Protocols, Network segments-Perimeter Defense, NAT, Basic architecture issues, Subnetting , switching and VLANs, Address Resolution protocol and media access control, Dynamic Host Configuration Protocol and Addressing Control.	4	15
	Database Security: Introduction to Database, Basics of SQL, Security requirements, Reliability and integrity, Sensitive data, Interface, Multilevel database, Proposals for multilevel security.	5	
II	Windows Security- Windows Security at the heart of the defense, Out-of-the-box Operating system hardening, Installing applications, Putting the workstation on the network, Operating Windows safely, Upgrades and Patches, Maintain and test the security, Attacks against the Windows workstation	6	15
	Linux Security- Physical security, Controlling the configuration, Operating Linux safely, Hardening Linux.	4	
FIRST INTERNAL EXAM			
III	Web Browser and Client risk- How a web browser works, Web browser attacks, Operating safely, Web security- How HTTP works, Server and Client contents, State, Attacking Web servers, Web Services.	5	20
	E-mail security- The e-mail risk, Protocols, Authentication, Operating safely when using email, Domain Name System – DNS basics, Purpose of DNS, Security Issues with DNS, DNS attacks.	5	

IV	Cryptography- Principles, four cryptographic primitives, Proprietary versus open source algorithms.	4	20
	Steganography - overview, Core areas of network security and their relation to steganography, Principles of Steganography, Types of Steganography, Steganography Versus Digital Watermarking, Types of Digital Watermarking, Goals of Digital Watermarking.	5	
SECOND INTERNAL EXAM			
V	Wireless Security- The Cellular phone network,Placing a cellular Telephone Call, Wireless transmission systems, IEEE Wireless LAN specification,IEEE 802.11,IEEE 802.11 Wireless Security, Bluetooth, WAP, Network segments- Perimeter Defense, NAT, Basic architecture issues, Subnetting, switching and VLANs, Address Resolution protocol and media access control, Dynamic Host Configuration Protocol and Addressing Control.	5	20
	Security In Data Networks: Wireless Device security issues - CDPD security, GPRS security, GSM security, IP security. Wireless Transport Layer Security: Secure Socket Layer - Wireless Transport Layer Security - WAP Security Architecture - WAP Gateway.	5	
VI	Firewalls-types, rules, personal firewalls, Intrusion detection systems, responses to intrusion detection, Penetration testing, Auditing and Monitoring.	4	10
	Integrated cyber security- Validating your security- overview, Current state of penetration testing, Formal penetration testing methodology, General tips for protecting a site, security best practices.	4	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6304	Operating Systems Security	**3-0-0**	**3**	**2015**

Course Objectives

- To understand and use advanced concepts in operating systems
- It gives a clear understanding about concepts related to distributed systems, recovery and fault tolerance and OS security

Syllabus

Overview of operating systems- synchronization mechanisms, deadlocks, memory management. Distributed operating systems-Architectures, Theoretical Foundations, Distributed Mutual exclusion, Token and non-token based Algorithms. Distributed Systems-Introduction, Architectures, Threads, Virtualization, Clients, Servers, Code Migration, Communication. Failure recovery and Fault Tolerance. Secure operating systems-Introduction, Access Control fundamentals, Multics. Security in Windows and UNIX, Security kernels, Case Study, Secure Virtual Machine Systems.

Expected Outcome

- Explain advanced concepts in operating systems
- Identify the core concepts of distributed systems
- Compare operating systems on their security merits
- How to design and build secure operating systems

References

1. Mukesh Singhal , Niranjan Shivarathri , "Advanced Concepts in Operating Systems", Edition 1 , Tata McGrawHill , 2001
2. Trent Jaeger, "Operating Systems Security", Morgan & Claypool Publishers, 2008
3. William Stallings, "Operating Systems Internals and Design Principles," Sixth edition. Prentice Hall.
4. Tannenbaum, Maarten Van Steen , "Distributed systems, Principles and Paradigms", Edition 2, Prentice Hall, 2007

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Overview-Functions of Operating system, Design Approaches, Types. Synchronization Mechanisms-Concept of a process, states, Processes and threads, Symmetric multiprocessing.	2	15
	Process Deadlocks-Introduction, Causes, Models, Graph theoretic model of a system state, Necessary and Sufficient conditions for a deadlock, Deadlock Prevention, Deadlock avoidance, Deadlock Detection.	3	
	Memory management-paging, segmentation. Uniprocessor scheduling-Types, algorithms. Multiprocessor scheduling, real time scheduling, case study	3	
II	Distributed Operating Systems-Architectures of Distributed Systems, Theoretical Foundations-Limitations of Distributed System, Clock Synchronization Algorithms, Lamports logical clocks, Vector clocks, Causal ordering of messages, Chandy-Lamport's Global State Recording Algorithm	3	20
	Distributed Mutual Exclusion Requirements, Centralized, Decentralized, Distributed, Token Ring Algorithms and their comparison Non-Token based algorithms-Ricart - Agrawala, Maekawa, Token Based Algorithms, Comparative Performance Analysis. Election Algorithms	4	
FIRST INTERNAL EXAM			
III	Distributed Systems-Introduction-Goals, Types. Architectures-Styles, System Architectures, Architecture Versus middleware	2	20
	Threads, Virtualization, Clients, Servers, Code Migration	2	
	Communication-Layered Protocols, Types of communication, RPC, Message-oriented, Stream-Oriented and Multicast Communication	2	

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
IV	Recovery-Classification, Checkpoint Algorithm, Rollback recovery algorithm, Scheme for Asynchronous Checkpointing and recovery.	3	15
	Fault tolerance-Basic Concepts, Failure Models. Process Resilience, Reliable Client-Server Communication, Distributed Commit.	3	
SECOND INTERNAL EXAM			
V	Introduction-Secure operating systems, Security Goals, Trust Model, Threat Model.	3	15
	Access Control fundamentals –Lampson's Access Matrix, Mandatory Protection Systems, Reference Monitor, Secure OS Definition, Assessment Criteria.	3	
	Multics – History, Multics System, Security, vulnerability Analysis	2	
VI	Security in Windows and UNIX Protection system, Authorization, Security Analysis and Vulnerabilities	2	15
	The security kernel, Secure communications processor, Retrofitting security into operating systems, Commercial, Microkernel and UNIX Era Case Study: Building a Secure OS for Linux.	2	
	Secure Virtual Machine Systems Separation Kernels, VAX VMM Security Kernel, Security in Other Virtual Machine Systems	3	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6306	Ethical Hacking	**3-0-0**	**3**	**2015**

Course Objectives

- The goal of this subject is to help students master an ethical hacking knowledge and methodology that can be used in a penetration testing or ethical hacking situation.

Syllabus

Ethical Hacking overview, Reconnaissance, Scanning and how to Gain access using operating system and application system attacks, How to Gain access using Network attacks, Denial of service attacks, Marinating access and Defending against Traditional and kernel level rootkits Covering tracks and hiding and Web Hacking, Attacking Applications, Wireless Network Hacking. Physical site security, Bypassing Network Security, Performing a Penetration Test.

Expected Outcome

- Students will have the ability to identify different types of computer attacks.
- Students will have a thorough knowledge on ethical hacking techniques and tools.

References

1. Michael T Simpson, Kent Backman, James Corley, Hands on ethical hacking and network defense, Cengage Learning, 2nd edition, 2010
2. Ed Skoudis and Tom Liston, Counter Hack Reloaded: A step-by-step guide to computer attacks and effective defenses, Prentice Hall Series in Computer Networking and security, 2nd edition,2006
3. Kimberly Graves, Certified Ethical Hacker :A Study Guide, 2010 by Wiley Publishing, Inc.
4. Stuart McClure, Joel Scambray, Hacking Exposed 7: Network Security Secrets & Solutions, edition 7, McGraw-Hill publishing, 2012

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Ethical Hacking overview, Network and computer attacks, Footprinting and social Engineering, Port Scanning, Enumeration, programming for security professionals, Desktop and server OS vulnerabilities.	4	20
	Embedded Operating Systems: the hidden threat, Hacking web servers, Hacking wireless networks, network protection systems, Virtualization and ethical hacking.	4	
II	Reconnaissance- Low technology reconnaissance, Search the fine web, Whois databases, DNS. Scanning- War dialing, Network mapping, Open ports using port scanners, Intrusion detection system evasion.	2	15
	Gaining access using operating system and application system attacks - Script kiddie Exploit trolling, Stack based buffer overflow attacks, Password attacks, web application attacks.	3	
FIRST INTERNAL EXAM			
III	Gaining access using Network attacks- Sniffing, IP address spoofing, Session Hijacking. Denial of service attacks- Stopping local services, Locally exhausting resources, Remotely stopping services, Remotely exhausting resource.	3	20
	Marinating access- Trojan horses, Back doors, Traditional and kernel level rootkits, Defending against Traditional and kernel level rootkits	3	
IV	Covering tracks and hiding- Hiding evidence by altering event log, Defenses against log and accounting file attacks, Hiding evidence on the network.	3	15
	System hacking: Password Cracking, Escalating Privileges, and Hiding Files. Web Hacking: Google, Web Servers, Web Application Vulnerabilities, and Web-Based Password Cracking Techniques.	3	
SECOND INTERNAL EXAM			
V	Attacking Applications: SQL Injection and Buffer Overflows. Wireless Network Hacking, Physical site security.	4	10

	Bypassing Network Security- Evading IDSs, Honey pots, and Firewalls, Performing a Penetration Test.	5	
VI	End point and server hacking- hacking windows, UNIX, cyber crime and advanced persistent threats	4	20
	Infrastructure hacking- remote connectivity and VOIP hacking, hacking hardware.	4	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6312	Web Security Testing	**3-0-0**	**3**	**2015**

Course Objectives

- To understand the common techniques for penetrating web applications and web servers.

Syllabus

Introduction to security testing Fundamentals, Automating specific tasks with cURL, Seeking design flaws, Infrastructure mapping and profiling, Scoping the app from a hacker's perspective Web Authorization - Understanding authorization, Script Hacking and Defensive Coding, Securing Databases and Database Access, Denial of Service, Web Application Management, Web Client Security, Threat Modeling.

Expected Outcome

- The student gains theoretical and practical insight into web application security.

References

1. Paco Hope, Ben Walther, "Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast", O'REILLY media, 2009.
2. Mike Andrews, James A. Whittaker, "How to Break Web Software", Pearson Education 2006.
3. David MacKey, "Web Security: For Network and System Administrators", Cengage Learning

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Introduction to security testing Fundamentals - HTML - HTTP - Client-side scripting - Server-side scripting, 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.	4	15
	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. Web server architecture - Windows & Linux - IIS and LAMP servers - Network topologies and DMZ - Hacking these platforms.	3	
II	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.	4	20
	Web applications - Introduction to web applications - Web application hacking - Overview of browsers, extensions, and platforms	3	
FIRST INTERNAL EXAM			
III	Seeking design flaws – bypassing required navigation, abusing password recovery, predictable identifiers, repeatability, high load actions, restrictive functionality and race conditions. Attacking AJAX	4	20
	Manipulating sessions – finding session identifiers, analyzing session identifiers. Multifaceted tests – stealing cookies, creating overlays, attempting crosssite tracing, attempting command injection, attempting SSI.	3	

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
IV	Infrastructure mapping and profiling - Scoping the app from a hacker's perspective - Platform profiling and mapping - Application identification and profiling - Profiling countermeasures	4	15
	Web Authentication - Overview of web authentication - Hacking passwords - Digital signatures	3	
SECOND INTERNAL EXAM			
V	Web Authorization - Understanding authorization - Hacking access control lists - Session IDs and Cookies - Hijacking URLs - Protecting Authorization	4	20
	Script Hacking and Defensive Coding - Attack Vectors - Buffer Overflows - Input validation Securing Databases and Database Access - Introduction to SQL - SQL Injection - Database Platform Attacks and Security - Database Encryption	3	
VI	Denial of Service - DoS attacks - DoS countermeasures Web Application Management - WebDAV - Configurations and Misconfigurations - Data leakage	4	10
	Web Client Security - Web browser hacking and security - Phishing - Adware/Spyware Threat Modeling - Modeling attack vectors and defense strategies - Threat and mitigation strategies - Code review and binary analysis	3	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6314	Windows and Linux Forensics	**3-0-0**	**3**	**2015**

Course Objectives

- To provide comprehensive coverage of the fundamental concepts Windows and Linux incidence response and Forensic analysis.

Syllabus

Windows Forensic Analysis- Live Response: Data Collection, Nonvolatile Information, Live-Response Methodologies. Windows Memory Analysis- Collecting Process Memory, Dumping Physical Memory, Registry Analysis, File Analysis, Executable File Analysis- Static Analysis, Dynamic Analysis. Rootkits, Rootkit Detection and Prevention. Linux Forensic Analysis- Live Response Data Collection, Data Analysis, File Analysis

Expected Outcome

- The students will have knowledge about forensic analysis of Windows and Linux Systems.

References

1. Chris Pogue, Cory Altheide, Todd Haverkos ,Unix and Linux Forensic Analysis DVD ToolKit, Syngress Inc. , 2008
2. Harlan Carvey ,Windows Forensic Analysis DVD Toolkit, Edition 2, Syngress Inc. , 2009
3. Harlan Carvey ,Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry , Syngress Inc, Feb 2011
4. Eoghan Casey, Handbook of Digital Forensics and Investigation, Academic Press, 2009

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Windows Forensic Analysis- Live Response: Data Collection- Introduction , Live Response- Locard's Exchange Principle, Order of Volatility ,When to Perform Live Response ,What Data to Collect- System Time, Logged-on Users , Open Files, Network Information , Network Connections ,Process Information,Process-to-Port Mapping, Process Memory, Network Status, Nonvolatile Information.	4	20
	Live-Response Methodologies, Live Response: Data Analysis- Data Analysis, Agile Analysis.	3	
II	Windows Memory Analysis- Collecting Process Memory, Dumping Physical Memory, Alternative Approaches for Dumping Physical Memory, Analyzing a Physical Memory Dump.	3	20
	Registry Analysis- Inside the Registry, Registry Analysis- RegRipper, System Information, Autostart Locations, USB Removable Storage Devices, Mounted Devices, Portable Devices, Finding Users, Tracking User Activity, Redirection, Virtualization, Deleted Registry Keys.	5	
FIRST INTERNAL EXAM			
III	File Analysis- Log Files, Event Logs, Other Log files, Recycle Bin, XP System Restore Points, Vista Volume Shadow Copy Service, Prefetch and Shortcut files.	3	15
	File Metadata, File Signature Analysis, NTFS Alternate Data Streams, Alternative Methods of Analysis, Executable File Analysis- Static Analysis, Dynamic Analysis.	4	
IV	Rootkits, Rootkit Detection-Live Detection, GMER, Helios, MS Strider GhostBuster, F-Secure BlackLight, Sophos Anti-Rootkit, Postmortem Detection, Prevention, Case studies.	3	10
	Performing Analysis on a Budget- Documenting Your Analysis, Tools- Acquiring Images, Image Analysis, File Analysis, Network Tools, Search Utilities.	3	
SECOND INTERNAL EXAM			

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
V	Linux Forensic Analysis- Live Response Data Collection- Prepare the Target Media, Format the Drive, Gather Volatile Information, Acquiring the Image.	3	20
	Initial Triage and Live Response: Data Analysis- Log Analysis, Keyword Searches, User Activity, Network Connections, Running Processes, Open File Handlers, The Hacking Top Ten, Reconnaissance Tools, The /Proc File System- Introduction , Process IDs.	5	
VI	File Analysis- The Linux Boot Process, System and Security Configuration Files- Users, Groups, and Privileges, Cron Jobs , Log Files.	2	15
	Identifying Other Files of Interest- . SUID and SGID Root Files, Recently Modified/Accessed/Created Files, Modified System Files, Out-of-Place inodes, Hidden Files and Hiding Places, Malware- Introduction, Viruses, Storms on the Horizon, Scanning the Target Directory.	4	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6316	Virtual Forensics and Security	**3-0-0**	**3**	**2015**

Course Objectives

- To understand the concepts of Virtualization Forensics and Security.

Syllabus

Requirement of virtualization, working, desktop virtualization, Fundamentals of investigating live virtual environments, artifacts, processes and ports, log files, Detecting Rogue virtual machines, alternate data streams and Rogue virtual machines, Virtualization System- Specific Attacks, Virtualization challenges, Malware and virtualization.

Expected Outcome

- Upon successful completion of this course, the students will get an in-depth knowledge in Virtualisation Forensics and Security.

References

1. Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtual Environments, Diane Barrett, Greg Kipper, Elsevier Science & Technology, 2010
2. Cloud Computing : Insights into new- era infra structure- Dr Kumar Saurabh, Wiley Publishers, April 2011
3. Evelyn Brown NIST "Guide to Security for Full Virtualization Technologies", 2011.

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Requirement of virtualization, How virtualization works- virtualizing operating systems, hardware platforms and servers, hypervisors- bare-metal, embedded, hosted	2	15
	Categories of virtualization- full virtualization, paravirtualization, hardware-assisted virtualization , operating system virtualization, application server virtualization , application virtualization , network virtualization , storage virtualization , service virtualization ,	4	
	Benefits of virtualization, cost of virtualization, Purpose of server virtualization, server virtualization the bigger picture, differences between desktop and server virtualization, common virtual servers	2	
II	What is desktop virtualization, common virtual desktops, virtual appliances and forensics, virtual desktops as a forensic platform, portable virtualization-MajoPac, MokaFive, preconfigured virtual Environments, virtual appliance providers, Jumpbox virtual appliances, virtual Box, virtualization hardware devices, virtual privacy machine, virtual emulators.	5	15
	Investigating dead Virtual environments – Install files, Remnants, registry , Microsoft disk image format, data to look for.	2	
FIRST INTERNAL EXAM			
III	Fundamentals of investigating live virtual environments, artifacts, processes and ports, log files, VM memory usage, memory analysis, Microsoft analysis tools, trace collection for a virtual machine, separate swap files for different virtual machines in a host computer.	3	20
	Profile based creation of virtual machine in a virtualization environment, system and methods for enforcing software license compliance with virtual machine as well as for improving memory locality of virtual machines, mechanisms for providing virtual machines for multiple users.	3	

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
IV	Detecting Rogue virtual machines, alternate data streams and Rogue virtual machines, virtual machine traces- prefetch file, link files, registry files, imaging virtual machines, snapshots and snapshot files, VMotion, Identification and conversion tools, Environment to environment conversion.	3	20
	Virtual environment and compliance- standards, compliance, regulatory requirements, discoverability of virtual environment, legal and protocol document language, organizational chain of custody, data retention policies, backup and data recovery.	3	
SECOND INTERNAL EXAM			
V	Virtualization System- Specific Attacks : Guest hopping, attacks on the VM (delete the VM, attack on the control of the VM, code or file injection into the virtualized file structure), VM migration attack, hyperjacking.	4	20
	Technologies For Virtualization-Based Security Enhancement: IBM security virtual server protection, virtualization-based sandboxing; Storage Security- HIDPS, log management, Data Loss Prevention. Location of the Perimeter.	4	
VI	Virtualization challenges- Data Centers, Storage Area networks, Direct attached storage and network attached storage, cluster file systems, Analysis of cluster file systems, security considerations- technical guidance, VM threats, Hypervisors, virtual appliances.	4	10
	Malware and virtualization- detection, Red Pill, Blue Pill, No Pill, Other methods of finding VMs, Additional challenges- encryption, solid-state drives, new file systems and disk types, compression and data deduplication, virtualization drawbacks.	3	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6318	Image Forensics and Security	**3-0-0**	**3**	**2015**

Course Objectives

- To understand the concepts of Image Forensics and Security

Syllabus

Image Processing, Digital Image Processing, Digital Image Formation, Image Forensics, Pixel-Based, Statistical-Based, Camera-Based, Video Forensics, Image Hiding, Image Coding, Image security techniques: visual cryptography, steganography, water marking.

Expected Outcome

- Upon successful completion of this course, the students will get an in-depth knowledge in image and video forensics and its security techniques.

References

1. Gonzales/ Woods/ Eddins, Digital Image Processing using MATLAB, 2nd edition, Gatesmark Publishing, ISBN 9780982085400
2. N.Efford, Digital Image Processing, Addison Wesley 2000, ISBN 0-201-59623-7
3. M Sonka, V Hlavac and R Boyle, Image Processing, Analysis and Machine Vision, PWS 1999, ISBN 0-534-95393-
4. Pratt.W.K., Digital Image Processing, John Wiley and Sons, New York, 1978

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Introduction to Image Processing, Background, Digital Image Representation, Fundamental steps in Image Processing	4	15
	Elements of Digital Image Processing- Image Acquisition, Storage, Processing, Communication, Display.	3	
II	Digital Image Formation: Image formation, image compression, point processing, neighbourhood operations, image analysis.	4	15
	Morphological Image Processing : Dilation and Erosion, Opening and Closing, Extensions to gray level images	3	
FIRST INTERNAL EXAM			
III	Image Forensics: Format-Based Forensics- Fourier, JPEG	3	20
	Camera-Based Forensics. Pixel-Based Forensics: Resampling, Cloning, Thumbnails.	4	
IV	Statistical-Based Forensics: Principal Component Analysis	3	20
	Linear Discriminant Analysis, Computer Generated or Photographic: Perception.	4	
SECOND INTERNAL EXAM			
V	Video Forensics: Motion, Re-Projected, Projectile, Enhancement.	4	20
	Physics-Based Forensics: 2-D Lighting, Lee Harvey Oswald (case study). Image Hiding, Image Coding.	3	
VI	Image security techniques: visual cryptography	4	10
	Steganography, water marking.	3	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6322	Coding Theory	**3-0-0**	**3**	**2015**

Course Objectives

- To impart fundamental knowledge and concepts of coding theory.

Syllabus

Introduction to Information Theory**,** Concept of amount of information, units – entropy, Error detection: correction and decoding, Hamming codes – encoding and decoding, Cyclic codes: Definitions, Generator polynomials, Image and Video Formats, Image compression , Video Compression, MPEG standards.

Expected Outcome

- The student will be able to understand the concepts and techniques of coding theory.

References

1. R Bose, "Information Theory, Coding and Crptography", **2/e** ,TMH 2007, New Delhi
2. P.S. Sathya Narayana: Concepts of Information Theory & Coding , Dynaram Publications,2005
3. Fred Halsall, "Multidedia Communications: Applications, Networks, Protocols and Standards", Perason Education Asia, 2002

COURSE PLAN

Module	Contents	Hours Allotted	% of Marks in End-Semester Examination
I	Introduction to Information Theory. Concept of amount of information, units – entropy, marginal, conditional and joint entropies.	4	15
	Relation among entropies – mutual information, information rate, classification of codes, Kraft McMillan inequality.	3	
II	Error detection: correction and decoding: Communication channels, Maximum likelihood decoding.	3	15
	Hamming distance, Nearest neighbour/ minimum distance decoding, Distance of a code.	4	
FIRST INTERNAL EXAM			
III	Hamming codes – encoding and decoding, cyclic codes – polynomial and matrix descriptions. Linear codes, Hamming weight, Bases of linear codes	4	20
	Source Coding: Adaptive Huffman Coding, Arithmetic Coding, LZW algorithm.	4	
IV	Cyclic codes: Definitions, Generator polynomials, Generator and parity check matrices, Decoding of cyclic codes, Burst-error-correcting codes.	4	20
	Some special cyclic codes: BCH codes, Definitions, Parameters of BCH codes, Decoding of BCH codes.	4	
SECOND INTERNAL EXAM			
V	Image and Video Formats – GIF, TIFF, SIF, CIF, QCIF	3	20
	Image compression: READ, JPEG.	3	
VI	Video Compression: Principles- I,B,P frames, Motion estimation	3	10
	Motion compensation, MPEG standards.	3	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6324	Digital Watermarking and Steganography	**3-0-0**	**3**	**2015**

Course Objectives

- To understand data hiding schemes.
- Analyze the embedding and security requirements of watermarking and steganography.
- Understand hiding in multimedia information.
- Perform authentication and copyright protection**.**

Syllabus

Introduction , Watermarking Models & Message Coding , Watermarking With Side Information & Analyzing Errors, Perceptual Models, Watermark Security & Authentication, Steganography.

Expected Outcome

- Able to understand embedding and extraction processes.
- Distinguish various types of attacks on the watermarked data.
- Know how to apply embedding based on region sensitivity

References

1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, "Digital Watermarking and Steganography", Margan Kaufmann Publishers, New York, 2008.
2. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, "Digital Watermarking", Margan Kaufmann Publishers, New York, 2003.
3. Michael Arnold, Martin Schmucker, Stephen D. Wolthusen, "Techniques and Applications of Digital Watermarking and Contest Protection", Artech House, London, 2003.
4. Juergen Seits, "Digital Watermarking for Digital Media", IDEA Group Publisher, New York, 2005.

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Introduction: Information Hiding, Steganography and Watermarking – History of watermarking.	3	15
	Importance of digital watermarking – Applications – Properties – Evaluating watermarking systems.	3	
II	Watermarking Models & Message Coding: Notation – Communications – Communication based models – Geometric models.	3	15
	Mapping messages into message vectors – Error correction coding – Detecting multi-symbol watermarks.	3	
FIRST INTERNAL EXAM			
III	Watermarking With Side Information & Analyzing Errors: Informed Embedding – Informed Coding – Structured dirty-paper codes.	3	15
	Message errors – False positive errors – False negative errors – ROC curves – Effect of whitening on error rates.	4	
IV	Perceptual Models: Evaluating perceptual impact – General form of a perceptual model – Examples of perceptual models .	4	15
	Robust watermarking approaches - Redundant Embedding, Spread Spectrum Coding, Embedding in Perceptually significant coefficients	3	
SECOND INTERNAL EXAM			
V	Watermark Security & Authentication: Security requirements – Watermark security and cryptography – Attacks.	4	20
	Exact authentication – Selective authentication – Localization – Restoration.	4	

VI	Steganography: Steganography communication – Notation and terminology – Information-theoretic foundations of steganography.	4	20
	Practical stegnographic methods – Minimizing the embedding impact – Steganalysis	4	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6392	Mini Project	0-0-4	2	2015

Course Objectives

To make students

Design and develop a system or application in the area of their specialization.

Approach

The student shall present two seminars and submit a report.The first seminar shall highlig objectives, methodology, design and expected results. The second seminar is the presentation / hardwareimplementation.

Expected Outcome

Upon successful completion of the miniproject, the student should be able to

1. Identify and solve various problems associated with designing and implementing a system o application.
2. Test the designed system or application.

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS6394	Network and OS Security Laboratory	**0-0-2**	**1**	**2015**

Course Objectives

- To understand about the various tools used in security

Syllabus

Familiarization of various security tools**.**

Expected Outcome

- The student will have hands on experience on security tools

Experiments

Experiment No.	Description	Hours Allotted
1	Sniff the username and password using Wireshark tool.	1
2	Perform Cookie injection using Wireshark tool	2
3	Implement Caesar cipher for encryption and decryption.	1
4	Implement a C-program to perform encryption and decryption using RSA**.**	2
5	Perform Cryptography using CrypTool.	1
6	Perform Steganography using Camouflage Tool.	1
7	Familiarize Metasploit framework and its basic commands.	3
8	Familiarize iptables.	2
9	Familiarize nmap.	1
10	Demonstrate Intrusion Detection System (IDS) using Snort Software.	2
11	Implement Bully algorithm.	1

12	Implement Ring algorithm.	1
13	Introduction to linux operating system and install Ubuntu in VirtualBox.	2
14	Implement the following system calls - fork,exec,getpid,exit,wait	1
15	Implement inter-process communication using pipes, shared memory and message queues.	2
16	Implementing Scheduling algorithms - FCFS, SJF, Priority, Round robin	3
17	Preventing PC against latest threats using Windows Defender.	1
18	Protecting PC using Microsoft Security Essentials.	1

SEMESTER - III

Syllabus and Course Plan

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS7311	Security Policies and Governance	**3-0-0**	**3**	**2015**

Course Objectives

- To impart fundamental knowledge and concepts of information security policies and governance.

Syllabus

Information security planning and governance, Governance definition, Information Security Governance, Six Outcomes of Effective Security Governance, Information, Data, Knowledge, Value of Information, Legal and Regulatory Requirements, Strategic Metrics -Governance Objectives, Objectives of Information Security Architectures, SABSA Model, Risk Management Objectives.

Expected Outcome

- The student will be able to understand the concepts of information security policies and governance.

References

1. Information Security Governance- A practical development and implementation approach by Krag Brotby, 2009.
2. Information Security Governance by S.H. von Solms, Rossouw von Solms, 2008
3. Information Security Governance by Todd Fitzgerald, 2011

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Information security planning and governance- Planning levels, Planning and the CISO, Information security governance, Information security policy, standards and practices	4	15
	Definitions, EISP, ISSP, SysSP, Policy management, Security education training and awareness program.	4	
II	Governance definition, Information Security Governance, Six Outcomes of Effective Security Governance, Information, Data, Knowledge, Value of Information. Why Governance?- Benefits of Good Governance, Aligning Security with Business, Objectives, Providing the Structure and Framework to Optimize, Allocations of Limited Resources	4	20
	Providing Assurance that Critical Decisions are Not Based on Faulty Information, Ensuring Accountability for Safeguarding Critical Assets, Increasing Trust of Customers and Stakeholders, Increasing the Company's Worth, Reducing Liability for Information Inaccuracy or Lack of Due Care in Protection, Increasing Predictability and Reducing Uncertainty of Business Operations.	3	
FIRST INTERNAL EXAM			
III	Legal and Regulatory Requirements- Security Governance and Regulation.	3	20
	Roles and Responsibilities- The Board of Directors, Executive Management, Security Steering Committee, The CISO.	3	
IV	Strategic Metrics -Governance Objectives, Strategic Direction, Ensuring Objectives are Achieved, Risks Managed Appropriately, Verifying that Resources are Used Responsibly. Information Security Outcomes - Defining Outcomes, Strategic Alignment	4	15
	Risk Management, Business Process Assurance/Convergence—Integrating, All Relevant Assurance Processes to Improve Overall Security and Efficiency, Value Delivery—Optimizing Investments in Support of Organizational Objectives, Resource Management,	4	

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
	Performance Measurement		
SECOND INTERNAL EXAM			
V	Objectives of Information Security Architectures, SABSA Model- SABSA Development Process, SABSA Life Cycle	4	20
	CobiT, CMM, ISO/IEC 27001, 27002	3	
VI	Risk Management Objectives - Risk Management Responsibilities, Managing Risk Appropriately, Determining Risk Management Objectives	3	10
	Recovery Time Objectives. Current State - Current State of Security	3	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS7313	Biometric Security	**3-0-0**	**3**	**2015**

Course Objectives

- To impart fundamental knowledge about concepts and applications of biometric security.

Syllabus

Introduction to Biometrics: biometric systems, enrollment and recognition, sensors, feature extraction, database, matching, Functionalities, Fingerprint recognition, Iris recognition, Ear detection and recognition, Security of bio-metric systems, biometric standards, biometric databases.

Expected Outcome

- The student will be able to understand the techniques, algorithms and applications developed for biometrics and apply them to solve real problems.

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

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Introduction to Biometrics: biometric systems, enrollment and recognition, sensors, feature extraction, database, matching	4	15
	Functionalities: verification and identification, performance measures, design cycle, applications, security and privacy issues.	4	
II	Fingerprint recognition: Friction ridge patterns, Acquisition	3	20
	Feature extraction, matching, indexing, synthesis, palm print.	3	
FIRST INTERNAL EXAM			
III	Face recognition: Introduction, image acquisition, face detection.	4	20
	Feature extraction of face recognition, matching, heterogeneous face recognition.	4	
IV	Iris recognition, Image acquisition, iris segmentation, normalization	4	15
	Encoding and matching, quality assessment, performance evaluation	4	
SECOND INTERNAL EXAM			
V	Ear detection and recognition – challenges, gait and hand geometry	3	20
	Feature extraction and matching.	2	
VI	Security of bio-metric systems: adversary attacks, attacks on user interface, attacks on bio-metric processing, database attacks.	4	10
	Biometric standards, biometric databases.	3	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS7315	Data Compression	**3-0-0**	**3**	**2015**

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.

Syllabus

Compression techniques, Compression ratio, lossless & lossy compression, Finite Context Modeling, Speech Compression & Synthesis, Image Compression, Transform based techniques, Video Compression- motion compensation, MPEG standards, Comparison of compression algorithms, Implementation of compression algorithms.

Expected Outcome

- In-depth knowledge about various data compression techniques and their practical significance.

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.

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Compression techniques, Compression ratio, lossless & lossy compression, Huffman coding	4	15
	Non binary Huffman Algorithms, Adaptive Coding, applications, Arithmetic Coding, applications	4	
II	Finite Context Modeling. Dictionary based Compression, Sliding Window Compression, LZ77,LZ78, LZW compression.	4	20
	Predictive Coding - prediction and partial match, move to front coding, Run Length encoding.	3	
FIRST INTERNAL EXAM			
III	Speech Compression & Synthesis: Digital Audio concepts, Sampling Variables	4	20
	Lossless compression of sound, lossy compression & silence compression.	3	
IV	Image Compression, Transform based techniques, Wavelet Methods, adaptive techniques.	4	15
	Images standards, JPEG Compression, Zig Zag Coding .	3	
SECOND INTERNAL EXAM			
V	Video Compression- motion compensation, MPEG standards	3	20
	Recent development in Multimedia Video compression, packet video, Fractal techniques.	4	
VI	Comparison of compression algorithms	3	10
	Implementation of compression algorithms.	3	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS7317	Neural Networks	**3-0-0**	**3**	**2015**

Course Objectives

- To understand the concepts of neural networks

Syllabus

Introduction to Neural Networks, Biological Neurons and Neural Networks, Basic neural network models ADALINE networks, Radial Basis Function Networks, Applications of Multi-layer Perceptrons, Neural networks as associative memories, Hopfield network, BAM, Self Organizing Maps and Applications of Artificial Neural Networks.

Expected Outcome

- Upon successful completion of this course, students will be acquainted with neural networks, various learning algorithms, and applications.

References

1. Hagan, Demuth and Beale, "Neural network design", Vikas Publishing House Pvt. Ltd., New Delhi , 2002
2. Christopher M. Bishop, Neural Networks for Pattern Recognition, Oxford University Press, 1995
3. Martin T. Hagan, Howard B. Demuth, Mark Beale, Neural Network Design, Vikas Thomson Learning, 2003
4. Simon Haykin, 'Neural Networks', 2nd Edition, Prentice Hall, 1999

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Introduction to Neural Networks, Biological Neurons and Neural Networks, Networks of Artificial Neurons. Single Layer Perceptron, Learning and Generalization in Single Layer Perceptron	4	15
	Hebbian Learning, Gradient Descent Learning, learning rates, Widrow-Hoff Learning , The Generalized Delta Rule, Practical Considerations.	4	
II	Basic neural network models ADALINE networks, LMS algorithm	3	20
	Learning in Multi- Layer Perceptrons. Back-Propagation algorithms.	3	
FIRST INTERNAL EXAM			
III	Radial Basis Function Networks: Fundamentals, Algorithms and Applications, Learning with Momentum.	4	20
	Conjugate Gradient Learning, Bias and Variance. Under-Fitting and Over-Fitting.	3	
IV	Applications of Multi-layer Perceptrons. Basic learning models Associative Learning.	4	15
	Competitive Networks, Winner-take-all networks, Adaptive Resonance Theory (ART).	3	
SECOND INTERNAL EXAM			
V	Neural networks as associative memories, Hopfield network, BAM, Self Organizing Maps: Fundamentals, Algorithms and Applications.	4	20
	Learning Vector Quantization, Optimization problems solving using neural networks, Stochastic neural networks, Boltzmann machine.	4	

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
VI	Applications of Artificial Neural Networks: Application areas like system identification and control, decision making.	3	10
	Applications in pattern recognition, and sequence recognition.	3	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS7319	Advanced Operating System Design	**3-0-0**	**3**	**2015**

Course Objectives

- To understand the concepts of operating system design.

Syllabus

Operating Systems, types, Introduction to the Linux Kernel, Interrupts and Interrupt Handlers, Memory Management, Distributed Operating Systems, Distributed System Goals, types of distributed systems, Fault Tolerance, Security, Over View Of UNIX, LINUX, Windows NT , Android And IOS Operating systems.

Expected Outcome

- Upon successful completion of this course, the students will get an in-depth knowledge in operating system design.

References

1. Operating Systems: Internals and Design Principles- Stallings , PH,2011
2. Robert Love, "Linux Kernel Development", 3/e, Addison-Wesley, 2010.
3. Daniel Bovet, Marco Cesati, "Understanding the Linux Kernel", 3/e, OReilly Media Inc., 2005.
4. Reilly Christian Benvenuti, "Understanding Linux Network Internals", 1/e, OReilly Media Inc.,2005.

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Introduction To Operating Systems, Types Of Operating Systems, Operating System Structures.	3	15
	Operating System Services, System Calls, Virtual Machines, Operating System Design And Implementation.	3	
II	Introduction to the Linux Kernel - History of Unix, Introduction to Linux, Overview of Operating Systems and Kernels, Linux Versus Classic Unix Kernels, Linux Kernel Versions. Process Management - Process Descriptor and the Task Structure, Process Creation,The Linux Implementation of Threads, Process Termination.	4	20
	Process Scheduling - Linux's Process Scheduler, Policy, Linux Scheduling Algorithm, Preemption and Context Switching, Real-Time Scheduling Policies.System Calls - Communicating with the Kernel, Syscalls, System Call Handler, System Call Implementation.	4	
FIRST INTERNAL EXAM			
III	Interrupts and Interrupt Handlers - Registering an Interrupt Handler, Writing an Interrupt Handler, Interrupt Context, Interrupt Control, Bottom Halves – Task Queues, Softirqs, Tasklets, Work Queues. Kernel Synchronization – Introduction, Critical Regions and Race Conditions, Locking, Deadlocks, Contention and Scalability.	4	20
	Kernel Synchronization Methods - Atomic Operations, Spin Locks, Semaphores, Mutexes, Completion Variables, BKL: The Big Kernel Lock, Sequential Locks, Preemption Disabling. Timers and Time Management - Kernel Notion of Time, Jiffies, Hardware Clocks and Timers, Using Timers, Delaying Execution.	3	
IV	Memory Management - Pages and Zones, Slab Layer, Static Allocation on the Stack, High Memory Mappings, Per-CPU Allocations. The Virtual Filesystem - Filesystem Abstraction Layer, Unix Filesystems, VFS Objects and Data Structures, Superblock Object, Inode Object, Dentry Object, File Object.	3	15
	The Block I/O Layer - Buffers and Buffer Heads, Request Queues, I/O Schedulers. Process Address Space - Address Spaces, Memory Descriptor, Virtual Memory Areas, Page Tables. Devices and Modules - Device Types, Modules, Device Model.	4	
SECOND INTERNAL EXAM			

V	Distributed Operating Systems: Distributed System Goals, Types Of Distributed Systems, Styles & Architecture Of Distributed Systems	4	20
	Distributed Systems & Synchronization: Clock Synchronization, Logical Clocks, Mutual Exclusion, Global Positioning Of Nodes, Data-Centric Consistency Models, Client-Centric Consistency Models, Consistency Protocols.	4	
VI	Fault Tolerance, Security: Introduction To Fault Tolerance, Process Resilience,, Reliable Client-Server Communication, Reliable Group Communication, Distributed Commit, Recovery, Secure Channels, Access Control, Security Management	4	10
	Case Study: Over View Of UNIX, LINUX, Windows NT , Android And IOS Operating systems	3	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS7321	Parallel Architectures and Algorithms	**3-0-0**	**3**	**2015**

Course Objectives

- Understand the principles and applications of parallel algorithms learning.

Syllabus

Parallel computer, Needs, Parallel Architectures, Parallel Programs, Programming for Performance, Shared Memory Multiprocessors, Scalable Multiprocessors, Performance Characteristics, Matrix Multiplication & Fast fourier transform, Matrix Transposition, Matrix operations, Numerical problems – finding roots of nonlinear equations, Solving Linear System.

Expected Outcome

- Students gain in-depth theoretical and practical knowledge on parallel algorithms.

References

1. B. Wilkinson, M. Allen, "Parallel Programming", 2/e, Pearson Education Inc, 2007.
2. M .J. Quin, "Parallel Programming in C with MPI and openMP", Tata McGraw Hill, 2007.
3. V. Kumar, A. Grama, A. Gupta, and G. Karypis, "Introduction to Parallel Computing", San Francisco: Benjamin Cummings / Addison Wesley, 2002

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Parallel computer. Need of parallel computers, models of computation, Analyzing algorithms, expressing algorithms. Broadcast, All sums and selection algorithms on SIMD. Searching a sorted sequence – EREW, CREW SMSIMD algorithms. Searching a random sequence – SMSIMD, tree and Mesh interconnection super computers. Sorting – Sorting on a linear array, sorting on a mesh, sorting on EREW SIMD computer, MIMD enumeration sort, MIMD quick sort, sorting on other networks.	4	15
	Parallel Architectures, A Generic Parallel Architecture, Fundamental Design Issues, Communication Abstraction, Programming Model Requirements, Naming, Ordering, Communication and Replication, Performance.	3	
II	Parallel Programs : Introduction, Parallel Application Case Studies, Simulating Ocean Currents, Simulating the Evolution of Galaxies, Visualizing Complex Scenes using Ray Tracing, Mining Data for Associations, The Parallelization Process, Steps in the Process, Parallelizing Computation versus Data, Goals of the Parallelization Process, Parallelization of an Example Program, A Simple Example: The Equation Solver Kernel, Decomposition, Assignment, Orchestration under the Data Parallel Model, Orchestration under the Shared Address Space Model, Orchestration under the Message Passing Model.	4	20
	Programming for Performance : Introduction, Partitioning for Performance, Load Balance and Synchronization Wait Time, Reducing Inherent Communication, Reducing the Extra Work, Data Access and Communication in a Multi-Memory System, A Multiprocessor as an Extended Memory Hierarchy, Artifiactual Communication in the Extended Memory Hierarchy, Orchestration for Performance, Reducing Artifiactual Communication, Structuring Communication to Reduce Cost, Performance Factors from the Processors' Perspective, Applications.	4	
FIRST INTERNAL EXAM			
III	Shared Memory Multiprocessors : Introduction, Cache Coherence, The Cache Coherence Problem, Cache Coherence Through Bus Snooping, Memory Consistency, Sequential Consistency, Sufficient Conditions for Preserving Sequential Consistency, Design Space for Snooping Protocols, A 3-state (MSI) Write-back Invalidation Protocol, A 4-state (MESI) WriteBack Invalidation Protocol, A 4-state (Dragon) Write-back	4	20

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
	Update Protocol, Assessing Protocol Design Tradeoffs, Workloads, Impact of Protocol Optimizations.		
	Scalable Multiprocessors : Introduction, Scalability, Bandwidth Scaling, Latency Scaling, Cost Scaling, Physical scaling, Scaling in a Generic Parallel Architecture, Realizing Programming Models, Primitive Network Transactions, Shared Address Space, Message Passing, Common challenges, Communication architecture design space, Physical DMA, A Case Study: nCUBE/2, User-level Access.	3	
IV	Performance Characteristics : Cache-based Directory Protocols: The Sequent NUMA-Q Cache Coherence Protocol Dealing with Correctness Issues Protocol Extensions, Overview of NUMA-Q Hardware Protocol, Interactions with SMP Node IQ-Link Implementation, Comparison	2	15
	Interconnection Network Design : Introduction, Basic definitions, Basic communication performance, Organizational Structure, Links, Switches, Network Interfaces, Interconnection Topologies, Fully connected network, Linear arrays and rings, Multidimensional meshes and tori, Trees, Butterflies, Hypercubes, Evaluating Design Trade-offs in Network Topology, Unloaded Latency, Latency under load,	2	
	Routing, Routing Mechanisms. , Deterministic Routing, Deadlock Freedom, Virtual Channels, Up*-Down* Routing, Turn-model Routing, Adaptive Routing, Switch Design, Ports, Link-level flow control, End-to-end flow control, Case Studies, Cray T3D Network, IBM SP-1, SP-2 Network, Scalable Coherent Interconnect, SGI Origin Network, Myricom Network.	3	
SECOND INTERNAL EXAM			
V	Matrix Multiplication & Fast fourier transform : Sequential matrix multiplication algorithm for multiprocessor, processor array algorithm multi-row-column oriented multiplication , block-oriented algorithm , Discrete fourier transform ,inverse discrete fourier transform, implementation of the hypercube multi-computer and other computer	4	20

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
	systems.		
	Matrix Transposition, Mesh transpose, shuffle transpose, EREW transpose. Matrix operations – matrix-by-matrix multiplications, mesh multiplications, cube multiplication, Matrix by vector multiplication. Linear array multiplication, tree multiplications. Solving numerical problems, solving systems of linear equations SIMD algorithms and MIMD algorithms.	3	
VI	Numerical problems – finding roots of nonlinear equations – SIMD and MIMD algorithms, solving partial differential equations, computing eigen values.	2	10
	Graph theoretical problems – solving graph theoretical problems, computing connectivity matrix, finding connected components, all pairs shortest path, traversing combinatorial spaces, sequential tree traversals, Minimal Alpha-Beta tree, MIMD Alpha-Beta algorithms, parallel cutoff storage requirements, recent trends and developments.	2	
	Solving Linear System : Back substituting odd even reduction, Gaussian elimination the jacoib algorithm, Gauss Scidal algorithm, Jacoib over relaxation & successive over relaxation multi grid method, conjugate gradient method	2	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS7323	Cyber Crimes and Legal Issues	**3-0-0**	**3**	**2015**

Course Objectives

- To impart fundamental knowledge and concepts of cybercrimes and legal issues

Syllabus

Computer Information Systems- Bulletin Board Systems, Teletext and Videotex, Information distribution systems, Legal issues in archiving internet resources, Criminal Intelligence and Investigation practices, Evolution of Cyber Law- Evolution of property rights, Legal Measures to protect the integrity on the Internet, The Information Technology Act 2000.

Expected Outcome

- The student will be able to understand the concepts of cybercrimes and legal issues.

References

1. Paul T. Augastine, "Cyber Crime and Legal Issues" , Crescent Publishing Corporation,2007
2. Rohas Nagpal, "Cyber Crime & Corporate Liability", Kluwer Publications, 2008
3. Rohas Nagpal, "Cyber Crime – Prosecution & Defence", Asian School of Cyber Laws, 2008

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Computer Information Systems- Bulletin Board Systems, Teletext and Videotex, Information distribution systems, Networks in Computer Information system, Legal Issues in Computer Information systems, Liability of Illegal activities, Regulatory environment, Defamation, Advocating lawless action, Fighting words, Child pornography	4	15
	Regulation of computer crime, Communications Services for unauthorized use, Protection from viruses and hackers, computer information system content- As Press, As Publisher, As Common carrier, As Traditional mail, Public forum, Bulletin Board, As Broadcaster.	4	
II	Legal issues in archiving internet resources- Internet archiving, Web archiving in India	2	15
	Crime prevention in cyber space- Assets in computer environment, Measures of security, Enforcement of law and legal training, Support of victims in reporting computer crime, Ethical standard and principles, Understanding international security systems	4	
FIRST INTERNAL EXAM			
III	Criminal Intelligence and Investigation practices- Investigations and law enforcement, Crime Investigation practices, Methods of investigation, Intelligence, Use of gathering Police information, Use and quality of information	4	15
	Information collecting and sharing- Factors for information and non-information sharing and non-sharing, Trust develops, Need for adequate training.	3	
IV	Evolution of Cyber Law- Evolution of property rights, Impacts of factors in the evolution of property rights, Security of property rights, Assurance problems, Determinants of trust, Reputation and recourse, Dispute resolution of third party, Customary law, Polycentric governance.	4	20

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
	Institutional developments in cyber space- Evolving property rights, Externalities and the evolution of property rights, Impact of factors in the evolution of property rights, security of property rights, Assurance problems and sources of credibility, Third party dispute resolution, Customary law, Polycentric cyber governance, Benefits of polycentric customary law.	4	
SECOND INTERNAL EXAM			
V	Legal Measures to protect the integrity on the Internet- Use of agent technology, Agent platforms, Upcoming issues, Procedural laws- Coercive powers of prosecuting authorities, Search and seizure, Active cooperation, Wire-tapping and Eavesdropping on Computer systems	3	20
	Problems in Personal data- Tolerability of Computer-generated evidence, Harmonization of Cyber laws- Integrity and correctness of information, Exclusive use of information, Intellectual property law, Coordination and Harmonization efforts, Necessity of Criminal laws	4	
VI	The Information Technology Act 2000- Definitions, Secure Digital signature, Secure Electronic records, Regulation of certifying authorities	3	15
	Duties of subscribers, Penalties and Adjudication, The Cyber Regulations Appellate.	3	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS7325	Theory of Computation	**3-0-0**	**3**	**2015**

Course Objectives

- Understand basic properties of formal languages and formal grammars.
- Understand basic properties of deterministic and nondeterministic finite automata.
- Understand the relation between types of languages and types of finite automata.
- Understand basic properties of Turing machines and computing with Turing machines.
- Understand the concepts of tractability and decidability, the concepts of NP-completeness and NP-hard problems.

Syllabus

Numbers and their Representation, Finite automata and Regular Languages, Universal Models of Computation, Computability Theory, Complexity Theory: Classes of Complexity - Hierarchy, Complexity Theory in Practice: Circumscribing Hard Problems.

Expected Outcome

- Have a good knowledge of formal computation and its relationship to languages.
- Be able to classify languages into their types.
- Be able to understand formal reasoning about languages.
- Understand the basic concepts of complexity theory.

References

1. Bernard Moret," The Theory of Computation", AW, 1998
2. John E Hopcroft, " Introduction to Automata Theory, Languages and Computation", AW, 2001
3. John E. Savage, "Models of Computation –Exploring the power of computing", AW, 1998

COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Numbers and their Representation - Problems, Instances, and Solutions - Asymptotic Notation.	3	15
	Graphs - Alphabets, Strings, and Languages - Functions and Infinite Sets	3	
	Pairing Functions - Cantor's Proof: the Technique of Diagonalization - Implications for Computability	2	
II	Finite automata and Regular Languages: States and Automata - Finite Automata as Language Acceptors - Determinism and Non-determinism - Checking vs. Computing .	4	15
	Properties of Finite Automata - Equivalence of Finite Automata Epsilon Transitions - Regular Expressions and Finite Automata - Reviewing the Construction of Regular Expressions from Finite Automata.	3	
FIRST INTERNAL EXAM			
III	Universal Models of Computation - Encoding Instances - Choosing a Model of Computation - Issues of Computability -	3	20
	The Turing Machine - Multitape Turing Machines - The Register Machine - Translation Between Models	3	
IV	Computability Theory - Primitive Recursive Functions -Defining Primitive Recursive Functions - Partial Recursive Functions.	3	20
	Rice's Theorem and the Recursion Theorem - Degrees of Unsolvability.	3	

SECOND INTERNAL EXAM			
V	Complexity Theory: Classes of Complexity - Hierarchy Theorems - Model-Independent Complexity Classes - Deterministic Complexity Classes - Certificates and nondeterminism -	4	20
	Complete Problems. NP-Completeness: Cook's Theorem - Space Completeness - Polynomial Space - Polylogarithmic Space - Provably Intractable Problems	4	
VI	Complexity Theory in Practice: Circumscribing Hard Problems - Restrictions of Hard Problems - Promise Problems - Strong NP-Completeness.	4	10
	The Complexity of Approximation – Definitions - Constant-Distance Approximations - Approximation Schemes - Fixed-Ratio Approximations and the Class OptNP - The Power of Randomization.	3	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS7391	Seminar II	0-0-2	1	2015

Course Objectives

To make students

1. Identify the current topics in the specific stream.
2. Collect the recent publications related to the identified topics.
3. Do a detailed study of a selected topic based on current journals, published papers and books.
4. Present a seminar on the selected topic on which a detailed study has been done.
5. Improve the writing and presentation skills.

Approach

Students shall make a presentation for 20-25 minutes based on the detailed study of the topic and submit a report based on the study.

Expected Outcome

Upon successful completion of the seminar, the student should be able to

1. Get good exposure in the current topics in the specific stream.
2. Improve the writing and presentation skills.
3. . Explore domains of interest so as to pursue the course project.

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS7393	Project (Phase I)	0-0-12	6	2015

Course Objectives

To make students

1. Do an original and independent study on the area of specialization.
2. Explore in depth a subject of his/her own choice.
3. Start the preliminary background studies towards the project by conducting literature survey in the relevant field.
4. Broadly identify the area of the project work, familiarize with the tools required for the design and analysis of the project.
5. Plan the experimental platform, if any, required for project work.

Approach

The student has to present two seminars and submit an interim Project report. The first seminar would highlight the topic, objectives, methodology and expected results. The first seminar shall be conducted in the first half of this semester. The second seminar is the presentation of the interim project report of the work completed and scope of the work which has to be accomplished in the fourth semester.

Expected Outcome

Upon successful completion of the project phase 1, the student should be able to

1. Identify the topic, objectives and methodology to carry out the project.
2. Finalize the project plan for their course project.

SEMESTER – IV

Syllabus and Course Plan

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01CS7394	Project (Phase II)	0-0-23	12	2015

Course Objectives

To continue and complete the project work identified in project phase 1.

Approach

There shall be two seminars (a mid term evaluation on the progress of the work and pre submission seminar to assess the quality and quantum of the work). At least one technical paper has to be prepared for possible publication in journals / conferences based on their project work.

Expected Outcome

Upon successful completion of the project phase II, the student should be able to

1. Get a good exposure to a domain of interest.
2. Get a good domain and experience to pursue future research activities.