SCHEME , SYLLABUS AND COURSE PLAN

FOR

M.TECH (FULL TIME) DEGREE COURSE

in

COMPUTER SCIENCE AND ENGINEERING(2015 Scheme)

(Specialization: ***Cyber Forensics and Information Security*****)**
(*Faculty of Engineering*)

At

ALAPPUZHA / PATHANAMTHITTA CLUSTER
(*Cluster code*: 03)

of the

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

SEMESTER 1

Examination Slot	Course Number	Name	L-T-P	Internal Marks	End Semester Examination		Credits
					Marks	Duration (hours)	
A	03 CS 6001	Mathematical foundations for Cyber Forensics	4-0-0	40	60	3	4
B	03 CS 6011	Cyber Forensics Basics	4-0-0	40	60	3	4
C	03 CS 6021	Information Security Basics	4-0-0	40	60	3	4
D	03 CS 6031	Operating Systems Security	3-0-0	40	60	3	3
E		Elective I	3-0-0	40	60	3	3
S	03 RM 6001	Research Methodology	1-1-0	100			2
T	03 CS 6901	Seminar I	0-0-2	100			2
U	03 CS 6801	Cyber Forensics Laboratory	0-0-2	100			1
		TOTAL	**19-1-4**	**500**	**300**	**-**	**23**

TOTAL CONTACT HOURS : 24
TOTAL CREDITS : 23

Elective I

03 CS 6041 Computer Algorithms
03 CS 6051 Virtual Forensics
03 CS 6061 Applied Cryptography

SEMESTER 2

Examination Slot	Course Number	Name	L-T-P	Internal Marks	End Semester Examination		Credits
					Marks	Duration (hours)	
A	03 CS 6002	File System Forensic Analysis	4-0-0	40	60	3	4
B	03 CS 6012	Windows and Linux Forensics Analysis	3-0-0	40	60	3	3
C	03 CS 6022	Network Security	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	03 CS 6902	Mini Project	0-0-4	100			2
U	03 CS 6802	Network Security and Ethical Hacking Lab	0-0-2	100			1
		TOTAL	**16-0-6**	**400**	**300**	**-**	**19**

TOTAL CONTACT HOURS : 22
TOTAL CREDITS : 19

Elective II

03 CS 6032 Malware Forensics
03 CS 6042 Image Forensics and Biometric Security
03 CS 6052 Information Security Governance

Elective III

03 CS 6062 Ethical Hacking
03 CS 6072 Software Forensics and Vulnerability Analysis
03 CS 6082 Wireless Security and Mobile Devices Forensics

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
	03 CS 7903	Seminar II	0-0-2	100			2
	03 CS 7913	Project (Phase 1)	0-0-8	50			6
		TOTAL	**6-0-10**	**230**	**120**	**-**	**14**

TOTAL CONTACT HOURS : 16
TOTAL CREDITS : 14

Elective IV

03 CS 7003	Cloud Forensics and Big Data Analysis
03 CS 7013	Advanced Data Mining Concepts
03 CS 7023	Information Storage and Security

Elective V

03 CS 7033	Cyber Crime, Legal issues and Ethics
03 CS 7043	Intellectual Property Rights
03 CS 7053	Programming with Python and Perl

SEMESTER 4

Examination Slot	Course Number	Name	L-T-P	Internal Marks	End Semester Examination		Credit
					Marks	Duration (hours)	
	03 CS 7914	Project (Phase 2)	0-0-21	70	30		12
		TOTAL	**0-0-21**	**70**	**30**	**-**	**12**

TOTAL CONTACT HOURS : 21
TOTAL CREDITS : 12

TOTAL NUMBER OF CREDITS : 68

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6001	Mathematical Foundations for Cyber Forensics	4-0-0	4	2015

Course Objectives

1. To understand and apply the fundamental concepts in
   a. Counting
   b. Recursion and Recurrence relations
   c. Graphs and Multigraphs
   d. Information Theory
   e. Probability
   f. Probability distributions

Syllabus

Fundamental principles of counting, Counting Lists, Permutations and Subsets, Lists and functions Binomial coefficients, Recursion, Mathematical Induction ,Graphs , Representation, Multigraphs, Graphs algorithms, Trees, representation of directed graphs ,Matching Theory- The idea of a matching ,Information Theory ,conditional and joint entropies, Error detection: correction and decoding,. Hamming codes, cyclic codes – polynomial and matrix descriptions ,Source Coding , Properties of Probability, Complementary probabilities, Probability and Hashing, The probability of a union of events, Principle of inclusion and exclusion for probability, Conditional Probability

Expected Outcome

1. Conceptual understanding of the above topics and ability to apply them in practical situations.

Text books and 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. Information Theory, Coding and Cryptography, R Bose, 2/e ,TMH 2007, New Delhi
4. Concepts of Information Theory & Coding , P.S.SathyaNarayana: Dynaram Publications,2005
5. Miguel A. Lerma, Notes on Discrete Mathematics
6. Keneth H. Rosen: Discrete Mathematics and Its Applications, Vth Edition, 2003, McGraw Hill
7. Discrete Mathematics for Computer Science-Gary Haggard, John Schliff, Sue whitesides, Indian Edition-2007,Thomson Learning

8. Information theory,Coding and Cryptography-Arjith Saha & Nilotpal Manna

03 CS 6001-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	7	25
	Counting subsets of a set, Binomial coefficients-Pascal's Triangle , A proof using the Sum Principle, The Binomial Theorem, Labeling and trinomial coefficients, Multisets, The bookcase arrangement problem, The number of k-element multisets of an n-element set.	8	
FIRST INTERNAL EXAM			
II	Recursion, First order linear recurrences, Iterating a recurrence, Geometric series,Recursively defined functions, Cardinality, , Mathematical Induction, Strong Induction, Induction in general, Graphs- The degree of a vertex, Paths, Connectivity, Cycles, Trees, Other Properties of Trees, Multigraphs, Planar graphs, Representing graphs in computer memory, Graph algorithms,	8	25
	Directed graphs, Basic definitions, Spanning trees, Rooted Trees, Warshall's algorithm: 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.	7	
III	Introduction to Information Theory. Concept of amount of information, units – entropy, marginal,conditional and joint entropies – relation among entropies – mutual information, information rate, classification of codes.	7	25
	Error detection: correction and decoding: Communication channels, Maximum likelihood decoding, Hamming distance, Nearest neighbor/ minimum distance decoding, Distance of a code. Hamming codes –	8	

	encoding and decoding, cyclic codes – polynomial and matrix descriptions. Linear codes, Hamming weight, Bases of linear codes . Source Coding: Adaptive Huffman Coding, Arithmetic Coding, LZW algorithm .		
SECOND INTERNAL EXAM			
IV	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, The principle of inclusion and exclusion for counting, Conditional Probability.	12	25
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6011	Cyber Forensics Basics	4-0-0	4	2015

Course objectives

1. To understand about Computer Forensics and the procedures for investigations.
2. To study about data acquisition and to have an understanding of different forensic acquisition tools
3. To explore the Windows and DOS system structures and UNIX /LINUX disk structures
4. To understand the different hiding techniques
5. The theory behind Network Forensics, Mobile Forensics and various types of Forensics.

Syllabus

Computer Forensics: history of computer forensics,Understanding Computer Investigations,procedures for corporate high tech investigations,determining the physical requirements for a CF lab,Data Acquisition - storage formats for digital evidence,using remote network acquisition tools, using other forensic acquisition tools,. Seizing digital evidence at the scene, storing digital evidence, obtaining a digital hash,Working with windows and DOS systems,Examining UNIX and LINUX disk structures,examining IDE/EIDE and SATA devices,Analysis and validation,data -hiding techniques,Working with Graphics Files,Recovering Graphics Files,Network Forensics,Email Investigations-role of E-mail in investigations,Cell Phone and Mobile Device forensics,Expert Testimony in High Tech Investigations

Expected Outcome

Upon successful completion of this course, the student will:

1. have deep conceptual and basic understanding of Computer Forensics and the forensic investigations
2. how to acquire data from devices and the theory behind various types of data acquisitions
3. how to work with Windows/DOS/Unix/Linux systems
4. know the theory behind various types of Forensics

Text Books and References

1. Computer Forensics and Investigations- Bill Nelson, Amelia Phillips, Frank Enfinger, ChristoferSteuart , Second Indian Reprint 2009, Cengage Learning India Private Ltd.
2. Digital Evidence and Computer Crime – Eoghan Casey, Edition 3, Academic Press,2011
3. Computer Forensics and Cyber Crime : An Introduction – MarjieBritz, Edition 2, Prentice Hall, 2008
4. Practical guide to Computer Forensics- David Benton and Frank Grindstaff , Book Surge

Publishing,2006
5. Computer Evidence: Collection & Preservation- Christopher L.T Brown Charles River Media publishing, Edition 1, 2005
6. Computer Investigation (Forensics, the Science of crime-solving) – Elizabeth Bauchner, Mason Crest Publishers, 2005
7. Real Digital Forensics- Keith J. Jones, Richard Bejtlich and Curtis W. Rose, Addison-Wesley publishers, 2005
8. Forensic Computer Crime Investigation (International Forensic Science and Investigation)- Thomas A. Johnson, CRC Press, 2005 Publishing Co. Beijing, 1999.
9. S. K. Basu, "Design Methods and Analysis of Algorithms", Prentice Hall India, 2005.

03 CS 6011 - COURSE PLAN

Module	Contents	Hours Allotted	% of Marks in End-Semester Examination
I	Computer Forensics: history of computer forensics, understanding case law, developing computer forensics resources, preparing for computer investigations, understanding law enforcement agency investigations and corporate investigations, maintaining professional conduct	7	25
	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 CF lab, selecting a basic forensic workstation, building a business case for developing a forensic lab	8	
FIRST INTERNAL EXAM			
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, Processing Crime and Incident Scene	7	25
	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.	6	
III	Working with windows and DOS systems- file systems, exploring Microsoft file structures, examining NTFS disks, whole disk encryption, the windows registry, Microsoft and MS-DOS start up tasks, virtual machines, Evaluating Computer Forensic s Tool needs, computer forensics software and hardware tools, validating and testing forensics software.Examining UNIX and LINUX disk structures and boot processes, examining CD data structures, examining SCSI Disk, examining IDE/EIDE and SATA devices.	11	25
SECOND INTERNAL EXAM			
IV	Analysis and validation -determining what data to collect and analyze, validating forensic data, addressing data -hiding techniques, performing	7	25

	remote acquisitions. 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.Network Forensics-overview, performing live acquisitions, developing standard procedures for network forensics, using network tools.		
	Email Investigations-role of E-mail in investigations, exploring the roles of the client and server, investigating e-mail crimes and violations, understanding E-mail servers, specialized E-mail forensic tools.	5	
	Cell Phone and Mobile Device forensics- Mobile device forensics, acquisition procedures for cell phones and mobile devices. Report writing for high tech investigations, Expert Testimony in High Tech Investigations.	5	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6021	Information Security Basics	4-0-0	4	2015

Course objectives

1. To understand the basics and fundamentals of Information Security.
2. To understand the need of security.
3. To understand laws and ethics in information security.
4. To understand the fundamentals of cryptology and cryptography.

Syllabus

The history of Information security, Components of an Information system ,the need for security, threats, theft ,attacks,Laws and ethics in Information security,Information security planning and governance,Information security governance, Information security policy, standards and practices,Security technology,Firewalls and VPNs,Intrusion detection and prevention systems,Foundations of Cryptology, Cipher methods,Cryptographic algorithms,Modular Arithmetic-Chinese Remainder Theorem –Introduction to Finite Fields,Digital signatures, Digital certificates, Steganography,Securing wireless networks with WEP and WPA, Securing TCP/IP with IPSec

Expected Outcome

Upon successful completion of this course, the student will:

1. have deep conceptual understanding of Information Security
2. have understanding about the need for security in systems
3. acquire ability to distinguish between various types of threats and security issues
4. have understanding of Cryptology and the various cryptographic algorithms
5. know the theory behind finite fields and how to secure wireless networks and TCP/IP

Text Books and 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. Absolute beginner's guide to Security, Spam, Spyware & Viruses- Andy Walker, Que publishers, 2005
4. Information Security Management Principles- Andy Taylor, David Alexander, Amanda Finch, David Sutton, BCS publishers, 2008
5. Guide to Computer forensics and Investigations- B. Nelson, A. Phillips, F. Enfinger, C. Steuart, Cengage Learning, 4th edition, 2010
6. Applied Information security: A Hands-On guide to Information security- R. Boyle, Prentice Hall, 2010
7. Fundamentals of Network Security- E. Maiwald, McGraw- Hill, 2004
8. Managing Information Security- John R. Vacca, Elsevier Inc, 2010
9. Cryptography and Network Security-William Stallings

03 CS 6021 - COURSE PLAN

Module	Contents	Hours Allotted	% of Marks in End-Semester Examination
I	The history of Information security, Components of an Information system. The need for security- Threats-Compromises to individual property, Deliberate software attacks, Deviations in quality of service, Espionage, Sabotage, Theft, 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. Social Engineering, Pharming, Timing attack, Secure software development.	10	25
INTERNAL TEST I			
II	Laws and ethics in Information security. An overview of risk management, Risk identification, Risk assessment, Risk control strategies, Selecting a risk control strategy, Quantitative versus qualitative risk control practices, Risk appetite, Residual risks, Documenting results. Information security planning and governance- Planning levels, Planning and the CISO, Information security governance, Information security policy, standards and practices, Policy management, Designing of security architecture, Security education training and awareness program, Continuity strategies.	12	25

III	Security technology-Firewalls and VPNs, Access control-Identification, Authentication, Authorization , Accountability, Firewall processing modes, Firewalls categorized by generation, Firewalls categorized by structure, Firewall architectures. Configuring and managing firewalls, Content filters, Protecting remote connections-Remote access, VPNs. Intrusion detection and prevention systems-Types, detection models, response behavior ,strengths and limitations, deployment and implementation, measuring the effectiveness. Honeypots, Honeynets and padded cell systems	16	25
INTERNAL TEST II			
IV	Foundations of Cryptology, Cipher methods- Substitution cipher, Transposition cipher, Crytographic algorithms- Symmetric encryption-Modular Arithmetic-Chinese Remainder Theorem –Introduction to Finite Fields- DES Algorithm -Analysis, AES Algorithm -Components-Analysis, Asymmetric encryption- The RSA system-The knapsack system ,Public key systems based on elliptic curves. Digital signatures, Digital certificates, Steganography, Securing web transactions with SET, SSL and S-HTTP, Securing wireless networks with WEP and WPA, Securing TCP/IP with IPSec.	20	25
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6031	Operating Systems Security	3-0-0	3	2015

Course objectives

- To study the concepts and principles in Operating Systems.
- To have an deeper understanding of distributed processing and distributed systems
- To study the goals and principles of Secure Operating systems
- To study how security is provided in Windows and UNIX.

Syllabus

Basic Concepts in Operating Systems,Memory management,Process and Disk Scheduling, File Management,Distributed processing-Types of distributed systems and Architectures,Virtualization,Distributed operating systems - Architecture, theoretical foundation,clock synchronization,Election algorithms - Traditional algorithms,Distributed Mutual Exclusion,Secure operating systems,Security Goals, Trust Model Threat Model, Access Control fundamentals, Multics- Security and Vulnerability Analysis, Security in Windows and UNIX Protection system,security kernels, Secure communications Processor,Secure Virtual Machine Systems,Mobile Operating systems-Security in Mobile OS

Expected Outcome

Upon successful completion of this course, students will be able to:

- Understand the basic principles and concepts of Operating Systems
- Understand distributed processing
- Study about distributed Operating systems and the various election algorithms
- Study how security is provided in Windows/Unix/Mobile Operating systems

References

1. Advanced Concepts in Operating Systems- MukeshSinghal , NiranjanShivarathri, TataMcGrawHill , Edition 1, 2001
2. Trent Jaeger, Operating Systems Security, Morgan & Claypool Publishers, 2008
3. Distributed systems, Principles and Paradigms- Tannenbaum, Maarten Van Steen, Prentice Hall, Edition 2, 2007
4. Distributed Computing, Fundamentals, Simulations and Advanced Topics – HagitAttiya,Jennifer Welch, McGraw-Hill, 1997
5. Modern Operating systems – Andrew S. Tannenbaum, PH, Edition 2, 2001
6. Michael J.Palmer, Guide to Operating Systems Security, Thomson/Course Technology, 2004
7. Operating Systems: Internals and Design Principles- Stallings , PH,2011
8. Distributed Operating System: Concepts and Design- Sinha, Wiley- IEEE Press, 1996
9. Distributed Operating Systems: Concepts and Practice- Doreen L. Galli, PHI, 1999
10. Microsoft Windows OS essentials-Tom Carpenter-Sybex1.Tom Adelstein and Bill Lubanovic, "Linux System Administration", O'Reilly Media, Inc., 1st Edition, 2007
11. Microsoft Windows Security Essentials-Darnl Gibson-Wiley Publishers

03 CS 6031 - COURSE PLAN

Module	Contents	Hours Allotted	% of Marks in End-Semester Examination
I	Processes and threads, Symmetric multiprocessing, Microkernels, Concurrency, Mutual Exclusion, Semaphores, Deadlocks, Concurrency mechanism, Memory management, Virtual Memory-Hardware and Control structures, Process and Disk Scheduling, File Management-Organization, Access, Sharing, File system security-case studies in Linux and Windows	15	25
	FIRST INTERNAL EXAM		
II	Distributed processing-Types of distributed systems and Architectures Virtualization- role in distributed systems, architecture of virtual machines, clients, servers, code migration, communication- layered protocols, types, RPC, types of Communication	4	25
	Distributed operating systems - Architecture, theoretical foundation,	5	

	clock synchronization- Physical clocks, The Berkeley algorithm, The Happened-Before Relationship, Logical clocks, Vector Timestamps, Global states, Election algorithms - Traditional algorithms, elections in wireless environments, elections in large scale systems,		
	Distributed Mutual Exclusion- Requirements, Centralised, Decentralised algorithms, Ricart and Agrawala's Algorithm, Maekawa's Algorithm, Token Based Dist ME.	4	
III	Secure operating systems-Introduction-Security Goals, Trust Model Threat Model. Access Control fundamentals –Lampson's Access Matrix, Mandatory Protection Systems, Reference Monitor, Secure OS Definition, Assessment Criteria. Multics – History, Multics System, Security, vulnerability Analysis	5	25
SECOND INTERNAL EXAM			
IV	Security in Windows and UNIX Protection system, authorization, security analysis and vulnerabilities- The security kernel- Secure communications processor – Retrofitting security into operating systems	6	25
	Security kernels, Secure communications Processor, Case Study, Secure Virtual Machine Systems Separation Kernels, VAX VMM Security Kernel, Security in Other Virtual Machine Systems	7	
	Mobile Operating systems-Security in Mobile OS	2	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6041	Computer Algorithms	3-0-0	3	2015

Course Objectives

1. To understand how to analyze and establish correctness of algorithms
2. To understand the theory behind various classes of algorithms
3. To understand the Flow Networks and the algorithms and Problems associated with it

Syllabus

The role of algorithms in computing,Designing algorithms,Growth of functions,recurrences andsolving recurrences, Sorting Algorithms, Tree, Graph algorithms,Growing a minimum spanning tree, Shortest path Algorithms, Flow Networks and Algorithms ,String matching with finite automata,Polynomial-time verification, NP-completeness and reducibility

Expected Outcome

1. Ability to analyzeand establish correctness of algorithms
2. Study various algorithms and their complexities and area of applications
3. Ability to explain flow networks
4. Ability to find the shortest path and minimum cost in trees and graphs

Text books and References

1. Computer Algorithms- Horowitz, Sahni, Rajasekharan, Silicon Press, 2nd edition, 2008
2. Cormen, Thomas H, Leiserson, Charles E &Rivest, Ronald L, 'Introduction to Algorithms',Prentice Hall of India Private Limited, New Delhi, Third Edition, 2009
3. Algorithms- Robert Sedgewick, Kevin Wayne, Pearson Education, 2011
4. Sahni, 'Data Structures, Algorithms and Applications in C++', Silicon Press, 2nd edition, 2004
5. Algorithm Design: Jon Kleinberg and Eva Tardos, AW (2005)
6. Anany V. Levitin. Introduction to the Design & Analysis of Algorithms (2nd Ed): A W (2006)
7. TheAlgorithm Design Manual(2nd Ed): Steven S. Skiena, Springer(2008)
8. Computer Algorithms: Introduction to Design and Analysis (3rd Ed): Sara Baase and AllenVan Gelder. AW (1999)

03 CS 6041 - COURSE PLAN

Module	Contents	Hours Allotted	% Marks in End of 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-sub array problem, Strassen's algorithm for matrix multiplication, The substitution method for solving recurrences, The recursion-tree method for solving recurrences, Probabilistic analysis and randomized algorithms- The Hiring problem, Indicator random variables, Randomized algorithms, Probabilistic analysis and further uses of indicator random variables	15	25
FIRST INTERNAL EXAM			
II	Heap sort- Heaps, Maintaining the Heap property, Building a heap, The heap sort algorithm, Quicksort- Description of quick sort, Performance of quick sort, A randomized version of quicksort, Analysis of quicksort, Counting sort, Radix sort, Bucket sort, Hash tables- Direct-address tables, Hash tables, Hash functions, Open addressing, Perfect hashing, Binary search trees, Randomly built binary search trees	9	25
III	Red-black tree- Properties, Insertion, Deletion, Rotations, Dynamic programming- , Matrix chain multiplication, Longest common subsequence, Optimal binary search trees, Greedy Algorithms- An activity selection problem, Huffman codes, Graph Algorithms –BFS, DFS, Topological sort, strongly connected components, Growing a minimum spanning tree, The algorithms of Kruskal and Prim, The Bellman-Ford algorithm, Single-source shortest paths in directed acyclic graphs, Dijkstra's algorithm, The Floyd-Warshall algorithm.	9	25
SECOND INTERNAL EXAM			
IV	Flow networks- The Ford-Fulkerson method, 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, Polynomial-time verification, NP-completeness and reducibility, NP completeness proofs, The vertex-cover problem, The travelling-salesman problem, The set-covering problem, The subset-sum problem	15	25
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6051	Virtual Forensics	3-0-0	3	2015

Course Objectives

1. Develop theoretical Foundations of virtualization, concepts and different categories of virtualization ,fundamentals of investigating live virtual environments and the different challenges faced in virtualization

Syllabus

Requirement of virtualization, How virtualization works,virtualizing operating systems,categories of virtualization,benefits of virtualization,desktop virtualization,preconfigured virtual Environments, virtual appliance providers,Fundamentals of investigating live virtual environments,, system and methods for enforcing software license compliance with virtual machine,Detecting Rogue virtual machines,Virtual environment and compliance-standards,compliance, regulatory requirements,Virtualization challenges,Malware and virtualization

Expected Outcome

1. Awareness about virtualization, the various categories of virtualization and their practical significance.
2. Ability to apply virtualization in practical scenarios
3. Study the challenges and security concerns in virtualization

Text books and References

1. Virtualization and Forensics: A Digital Forensic Investigator's Guide to Virtua Environments, Diane Barrett, Greg Kipper, Elsevier Science & Technology, 2010
2. Introduction to Virtualization e-book
3. Cloud Computing: Automating the Virtualized Data Center-VenkataJosyula, Malcolm Orr & Greg Page, Cisco Press, 2011
4. Cloud Computing : Insights into new- era infra structure-Dr Kumar Saurabh, Wiley Publishers, April 2011
5. Hacking Exposed: Virtualization & Cloud Computing: Secrets& Solutions- Hoff Christofer, Mogull Rich & Balding Craig, McGraw Hill,

03 CS 6051 – 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, categories of virtualization- full virtualization, para virtualization, hardware-assisted virtualization , operating system virtualization, application server virtualization , application virtualization , network virtualization , storage virtualization , service virtualization , benefits of virtualization, cost of virtualization, Purpose of server virtualization, server virtualization the bigger picture, differences between desktop and server virtualization, common virtual servers.	15	25
FIRST INTERNAL EXAM			
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. Investigating dead Virtual environments – Install files, Remnants, registry , Microsoft disk image format, data to look for	10	25
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, 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. 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	10	25
SECOND INTERNAL EXAM			

03 CS 6051 – COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
IV	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 datarecovery. 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, 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	15	25
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6061	Applied Cryptography	3-0-0	3	2015

Course Objectives

1. To impart deeper understanding in
   a. Principles of cryptography and the Cryptographic protocols
   b. Different cryptographic techniques
   c. Cryptographic algorithms

Syllabus

Preliminaries of Cryptography, Cryptographic protocols,Digital signatures with encryption,cryptographic protection of databases,Intermediate protocols,Advanced protocols,Esoteric protocols,Cryptographic techniques,Key Management,Cryptographic algorithms- Information theory, Complexity theory, Number theory, Data Encryption and Standard,Block Ciphers,Using symmetric key algorithms, Using public key algorithms, Secret-sharing algorithms

Expected Outcome

1. The student gains insight into conceptual and practical aspects of cryptographic algorithms.
2. The student gains a complete understanding of the usage of cryptographic techniques.

Text books and References

1. Applied Cryptography: Protocols, Algorithms and Source code in C- Bruce Schneieir, John Wiley & Sons, Edition, 1996
2. Cryptography A Primer- Alan G Konhein, John Wiley & sons, 1981
3. Handbook of Applied Cryptography- Alfred Menezes, Paul van Oorschot, Scott Vanstone, CRC Press, Edition 1, 1996
4. Introduction to Modern Cryptography- Jonathan Katz, Yehuda Lindell, Chapman and Hall/CRC; Edition 1, 2007
5. Understanding Cryptography- ChritofPaar, Jan Pelzl, Bart Preneel, Springer; Edition 2, 2010
6. Cryptography: A New Dimension in Computer Data Security- Carl Meyer, SM Matyas, John Wiley & Sons, 1982

03 CS 6061 – 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	8	25
	Digital signatures with encryption, Random and pseudo-random sequence generation, 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	7	
FIRST INTERNAL EXAM			
II	Intermediate protocols - Time stamping services, Subliminal channel, Undeniable digital signatures, Designated Confirmer signatures, Proxy signatures, Group signatures, Fail-stop digital signatures, Computing with encrypted data, Bit Commitment, Fair coin flips, Mental Poker, One-way accumulators, All-or-nothing disclosure of secrets, Key escrow, 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. Esoteric protocols- Secure elections, Secure multiparty computation, Anonymous message broadcast, Digital cash	10	25
III	Cryptographic techniques- Key Length- Symmetric key length, Public-key key length, Birthday attacks against One-Way Hash functions, Caveat Emptor, Key Management- Generating keys, Nonlinear keyspaces, Transferring ,Verifying, Using, Updating and Storing keys, Backup Keys, Compromised keys, Lifetime of keys, Destroying keys, Public-key management. Algorithms types and Modes, Choosing a cipher mode,Choosing an algorithm,Encrypting communication channels, Encrypting data for storage, Hardware versus software encryption.	10	25
SECOND INTERNAL EXAM			

03 CS 6061 – COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
IV	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, 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	15	25
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 RM 6001	Research Methodology	0-2-0	2	2015

Course Objectives

1. This course is designed to familiarize the student with the research process, problem identification strategies and formulation of a research plan by doing case studies

Syllabus

Introduction to Research Methodologies - Objectives -motivation in research- Significance of research - interaction between industries and research units –research and innovation

Research Formulation- - literature review– Ethics in research: – copy right – plagiarism – citation – acknowledgement Research Design – and Report writing

Case Studies : Department / stream specific case study and preparation of a research plan or a review paper

Expected Outcome

1. Students will be able to write a review paper after critically evaluating the state of the art development in a topic of interest
2. Students will acquire capability to write a research proposal in the form of a technical paper which could lead the student towards his / her final thesis topic
3. No formal end semester examination is intended – Evaluation is based on internal oral presentations and a Technical Report or a Research Plan or a Review Paper

References

1. R. Paneersalvam, "Research Methodology",Prentice Hall of India Pvt. Ltd.,2011
2. Mike Martin, Roland Schinzinger, "Ethics in Engineering" ,McGraw Hill Education, Fourth Edition,.2014
3. Vinod V Sople," Managing Intellectual Property-The Strategic Imperative, EDA", Prentice of Hall Pvt. Ltd.,2014
4. Kothari C R &Gaurav Garg – "Research Methodology- Methods and Techniques",New Age International(P) Ltd Publications,2006
5. Day A Robert,"How to write and publish a scientific paper",Cambridge University,UK,2012
6. Leedy P D,"Practical Research-Planning and Design", Prentice Hall of India Pvt. Ltd.

03 RM 6001 – COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Introduction –Need for research- objectives and motivations in research. Significance of research - -need for interaction between academic institutions, industrial and research establishments – research and innovation. Research Formulation- Identifying a research problem- - literature review– confirming to a research problem based on literature review.	4	25%
FIRST ASSESSMENT			
II	Research Ethics – Environmental impacts – Ethical issues - Intellectual Property Rights – Patents – legal formalities in filing patent in India – Copy right– plagiarism – citation and acknowledgement.	3	25%
III	Research design –Prepare research plan. Report writing – types of report – research report, research proposal, funding agencies for research concerned to the specialization, significance of peer reviewed articles and technical paper- - simple exercises - oral presentation	3	
SECOND ASSESSMENT			
IV	Case Studies The student is expected to prepare a research plan relating to a topic of current interest in the concerned specialization, which has appeared in a recent journal. A minimum of 20 related referred articles should be critically studied. On the basis of this, the student is expected to prepare a review report/paper of publishable quality. **This paper has to be presented for open defence before the departmental committee. (This would carry 50% marks)**	6	50%

END SEMESTER ASSESSMENT			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6901	Seminar I	0-0-2	1	2015

Course Objectives

To make students,

- identify a domain of interest
- identify sufficient number of latest good quality research papers on a particular problem or allied problems
- do extensive study and analysis of the problem and solution(s)
- Prepare a comprehensive report
- make a presentation (20-25 minutes) based on the report

Syllabus

.

No specific Syllabus

Expected Outcome

To student

- gets good exposure to a domain of interest and the research problems in the domain
- gets practice in the art doing literature survey
- improves his/her writing and presentation skills
- expectation- gets a good domain and problem to pursue his/her thesis work.

Seminar Guidelines

- Each student shall individually prepare and present a seminar and the topic should be relevant to the stream of study with content suitable for M.Tech level Presentation.
- For selection of topics refer internationally reputed transactions/journals. The primary reference should be published during the last two or three years.
- A detailed write-up /synopsis should be prepared in the prescribed format given by the Department and get the topic approved by the PG Coordinator well in advance.
- The seminar shall be of 30 minutes duration and a committee, with the PG Co-ordinator as the chairman and two faculty members from the department as members shall evaluate the seminar based on the technical content, presentation, depth of knowledge and ability to answer the questions put forward by the committee.

After the completion of the Seminar work the students would be required to submit two

copies of the seminar reports prepared by them in the prescribed format.

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6801	Cyber Forensics Laboratory	0-0-2	1	2015

Syllabus

Experiments are based on but not limited to the topics covered in 0*3 CS 6011: Cyber Forensics Basics*

03 CS 6701 – EXPERIMENTS

Experiment No	Description	Hours Allotted
I	Survey of Latest developments in Cyber Forensics	2
II	Registry Editing and Viewing using native tools of OS	4
III	Hex analysis using Hex Editors	4
IV	Bit level Forensic Analysis of evidential image using FTK, Encase and ProDiscover Tools	6
V	Hash code generation, comparison of files using tools like HashCalcetc	4
VI	File analysis using Sleuthkitetc	4
VII	Graphical File analysis and Image Analysis	4
VIII	Email Analysis involving Header check, tracing route, performing a check on Spam mail and Non- Spam mail	4

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6002	File System Forensic Analysis	4-0-0	4	2015

Course Objectives

1. To understand foundation of digital investigation and methods of data analysis
2. To understand the file system and how to analyze a file system
3. To familiarize the NTFS,ext2 and ext3 file systems
4. To familiarize the UFS1 and UFS2 concepts
5. To understand the different file system structures-Windows/Linux

Syllabus

Digital investigation foundation,Data analysis, Hard disk data acquisition ,Volume Analysis , File system analysis, File system category ,Application-level search techniques ,NTFS concepts , NTFS Analysis, NTFS data structure, Ext2 and Ext3 concepts , UFS1 and UFS2 concepts and analysis

Expected Outcome

In-depth knowledge in

1. Data and File analysis
2. NTFS,ext2,ext3 file systems
3. UFS1 and UFS2 concepts
4. Windows and Linux File system structures

Text books and References

1. File System Forensic Analysis – Brian Carrier, Addison Wesley, 2005
2. Digital Evidence and Computer Crime- Casey, Eoghan , edition 2, Academic Press, 2004.
3. Computer Forensics- Kruse, Warren and Jay Heiser, Addison Wesley, 2002.
4. Guide to Computer Forensics and Investigations- Bill Nelson, Amelia Phillips, Frank Enfinger, Chris Steuart, Thomson Course Technology, 2004
5. Forensic Discovery – Dan Farmer &WietseVenema, Addison Wesley, 2005
6. Incident Response and Computer Forensics- Mandia, Kevin, Chris Prosise, Matt Pepe, McGraw Hill/Osborne, 2003.
7. A Fast File System for UNIX-McKusick, William N. Joy, Samuel J. Leffler, Robert S.
8. Fabry , ACM Transactions on Computer Systems , August 1984, pp 181-197. http://docs.freebsd.org/44doc/smm/05.fastfs/paper.pdf
9. The Common Vulnerabilities and Exposures database, entry CVE-2000-0666.http://cve.mitre.org/

03 CS 6002 – 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, 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.	9	25
	Volume Analysis- introduction, background, analysis basics, PC based partitions- DOS partitions, Analysis considerations, Apple partitions, removable media, Server based partitions- BSD partitions, Sun Solaris slices, GPT partitions, Multiple disk volumes- RAID, Disk Spanning,	9	
FIRST INTERNAL EXAM			
II	File system analysis- What is a file system, File system category, Content category, Metadata category, File name category, Application category, Application-level search techniques, Specific file systems, FAT concepts and analysis- Introduction, File system category, Content category, Metadata category, File name category, The big picture, File recovery, determining type, Consistency check. FAT data structure-Boot sector, FAT 32 FS info, directory entries, Long file name directory entries.	11	25
III	NTFS concepts- Introduction, Everything is a file, MFT concepts, MFT entry attribute concepts, Other attribute concepts, Indexes, Analysis tools, 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	12	25
SECOND INTERNAL EXAM			
IV	Ext2 & Ext3 concepts- File system category, Content, Metadata category, File name category, The big picture, File recovery, determining the type, Consistency check. Ext2 and Ext3 data structures-Super block, group descriptor tables, Block bitmap, Inodes, Extended attributes, Directory Entry, Symbolic Link, Hash trees, Journal data structures	9	25
	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, 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,	9	

03 CS 6002 – COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
	UFS2 Extended attributes, Directory entries.		
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6012	Windows and Linux Forensic Analysis	3-0-0	3	2015

Course Objectives

1. To understand how data acquisition is done from a Windows and Linux System
2. To understand what is inside a windows registry
3. To analyze windows memory and files including executable files
4. To have an overview on concepts implemented in modern operating systems.

Syllabus

Windows Forensic Analysis,Data Collection,, Live Response,What Data to Collect,Live-Response Methodologies,Windows Memory Analysis,Analyzing a Physical Memory Dump,Registry Analysis,File Analysis,Executable File Analysis,Rootkits, Rootkit Detection,Image Analysis,Data Analysis,Reconnaissance Tools,The /Proc File System,The Linux Boot Process,Malware-Introduction, Viruses, Storms on the Horizon, Scanning the Target Directory

Expected Outcome

1. In-depth knowledge in acquisition of data from Windows and Linux System.
2. An understanding on how to analyze registry, file and physical Memory dump

References

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

4. File System Forensic Analysis- Brian Carrier, Addison Wesley, Edition 1, 2005
5. Handbook of Digital Forensics and Investigation- Eoghan Casey, Academic Press, 2009
6. Digital Forensics with Open Source Tools- Cory Altheide, Harlan Carvey, SyngressInc, Edition 1,April 2011

03 CS 6012 - COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Windows Forensic Analysis- Live Response: Data Collection- Introduction , 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 Info, Live-Response Methodologies: Data Analysis- Data Analysis, Agile Analysis, Windows Memory Analysis-Collecting Process Memory, Dumping Physical Memory, Alternative Approaches for Dumping Physical Memory, Analyzing a Physical Memory Dump.	15	25
FIRST INTERNAL EXAM			
II	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, File Analysis-Log Files, Event Logs, Other Log files, Recycle Bin, XP System Restore Points, Vista Volume Shadow Copy Service, Prefetch and Shortcut files, File Metadata, File Signature Analysis, NTFS Alternate Data Streams, Alternative Methods of Analysis, Exe File Analysis- Static Analysis, Dynamic Analysis.	9	25
III	Rootkits, Rootkit Detection-Live Detection, GMER, Helios, MS Strider GhostBuster, F-Secure BlackLight, Sophos Anti-Rootkit, Postmortem Detection, Prevention, Case studies, Performing Analysis on a Budget-Documenting Your Analysis, Tools-Acquiring Images, Image Analysis, File Analysis, Network Tools, Search Utilities. Linux Forensic Analysis- Live Response Data Collection- Prepare the Target Media, Format the Drive, Gather Volatile Information, Acquiring the Image, 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	11	25
SECOND INTERNAL EXAM			
IV	The /Proc File System- Introduction , Process IDs, File Analysis- The Linux Boot Process, System and Security Configuration Files- Users, Groups, and Privileges, Cron Jobs , Log Files, 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	13	25

03 CS 6012 - COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
	Target Directory.		
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6022	Network Security	3-0-0	3	2015

Course Objectives

To impart a deeper understanding of

1. network security,cyber security and information security principles and policies
2. wireless networking security issues and approaches.

Syllabus

Basics of Computer Networks: Internet Addressing,State of Network Security, Cyber Security, New approaches to cyber security,Key principles of network security,Information System Security Management- Security policies, Security awareness, Windows Security, Attacks against the Windows workstation, Linux Security, Web Browser and Client risk, How a web browser works, Web browser attacks, Web security, E-mail security, Security Issues with DNS, VoIP, Wireless Security, Wi-Fi Security recommendations, Bluetooth, WAP, Cryptography- Principles, Steganography- overview, history, Core areas of network security and their relation to steganography, penetration testing, Formal penetration testing methodology, general tips for protecting a site, security best practices.

Expected Outcome

1. Deeper understanding of and ability to use the advanced theoretical and practical aspects of network security, cyber security and information security

Text Books and References

1. Network Security Bible- Eric Cole, Ronald Krutz, James W. Conley, Edition 2, Wiley India Pvt Ltd, 2010
2. Network Security Essentials – William Stallings, Edition 4, Pearson Education, 2011
3. Cryptography and Network Security: Principles and Practice-William Stallings, Edition 3,

Pearson education, 2003
4. Data Communications and Networking ,Behrouz A. Forouzan, McGraw Hill, Edition 4
5. Hacking Exposed- Network Security Secrets and solutions, Joel Scambray, McGraw Hill, Edition 5,2005
6. Wireless Security : Models, Threats and Solutions- Randall K. Nichols, Panos C. Lekkas, McGraw Hill, Edition 1, 2001
7. Secrets and Lies: Digital Security in a Networked world- Bruce Schneier, Wiley publishers, Edition 1, 2004
8. Network Analysis, Architecture and Design- James D. McCabe, Morgam Kaufman, Edition 3, 2007

03 CS 6022 - COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Basics of Computer Networks: Classful Internet Addresses- The Original Classful Addressing Scheme Dotted Decimal Notation - Subnetting and Classless Extensions,VLAN. State of Network Security, Cyber Security, New approaches to cyber security, Interfacing with the organization,	8	25
	Information security principles- Key principles of network security, Formal Processes, Risk Management, Calculating and managing risk, Information System Security Management- Security policies, Security awareness, Managing the Technical effort, Configuration Management, Business Continuity and Disaster Recovery Planning, Physical Security, Legal and Liability Issues, Access Control- Control Models, Types of Access Control Implementations, Identification and Authentication, Remote access	7	
FIRST INTERNAL EXAM			
II	Windows Security at the heart of the defense, Installing applications, Putting the workstation on the network, Operating Windows safely, Upgrades and Patches, Maintain and test the security, Attacks against the Windows workstation, Linux Security- Physical security, Controlling the configuration, Operating Linux safely, Hardening Linux, Web Browser and Client risk, How a web browser works, Web browser attacks, Operating safely, Web Browser config, Web security-HTTP working, Server and Client contents, State, Attacking Web servers, Web Services, E-mail security- The e-mail risk, Protocols, Authentication, Security Issues with DNS, DNS attacks, Server security-Risks, Security by design, Operating servers safely, Multi-level security and digital rights management	10	25
III	VoIP, Wireless Security- The Cellular phone network, Wireless transmission systems, Pervasive Wireless Data Network Technologies, IEEE Wireless LAN specification, War driving, War Chalking, War Flying, Wi-Fi Security recommendations, Bluetooth, WAP, Network segments- Perimeter Defense, NAT, Basic architecture issues, Address Resolution protocol and media access control, zero configuration networks, system design and architecture against insider threats	10	25

03 CS 6022 - COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
SECOND INTERNAL EXAM			
IV	Cryptography- Principles, four cryptographic primitives, Proprietary versus open source algorithms, Attacks on Hash functions, Quantum cryptography, Steganography- overview, history, Core areas of network security and their relation to steganography, Certification and accreditation, DIACAP, Penetration testing, Auditing and Monitoring. Integrated cyber security- Validating your security- overview, Current state of penetration testing, Formal penetration testing methodology, Steps to explore a system, Data Protection, Endpoint security, Insider threats and data protection, Critical problems facing organizations,general tips for protecting a site, security best practices.	12	25
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6032	Malware Forensics	3-0-0	3	2015

Course Objectives

1. To understand the working of malware programs
2. To find the malware artifacts from a live Windows and Linux system
3. To analyze the suspect files affected by malwares
4. To learn how to extract the malware artifacts

Syllabus

Malware Incident response,Volatile Data collection methodology,Identifying Users logged into the system,Non-volatile Data collection from a live system,Memory Forensics: Analyzing Physical and Process Dumps for Malware Artifacts,Memory Forensics methodology,Discovering and Extracting Malware and Associated Artifacts from Windows Systems and Linux systems,Forensic Examinations of Compromised Windows / Linux Systems,Legal considerations,Tools for acquiring data, Acquiring data across Borders,File Identification and profiling,Working with Executable,File Obfuscation,Pre -execution preparation,Event reconstruction and artifact review

Expected Outcome

1. Students gain in-depth theoretical and practical knowledge on how to collect and analyze malware artifacts from a windows and Linux system

Text Books and References

1. Malware Forensics Investigating and Analyzing Malicious code-James M. Aquilina, EoghanCasey,Cameron H. Malin, Syngress Publishing, 2008
2. Malware Analyst's Cookbook Tools and Techniques for fighting malicious code- Michael Hale Ligh, Steven Adair, Blake Hartstein, Matthew Richard, Wiley Publishing Inc, 2011
3. Unix and Linux Forensic Analysis DVD ToolKit - Chris Pogue, Cory Altheide, Todd Haverkos, Syngress Inc. , 2008
4. Windows Forensic Analysis DVD Toolkit- Harlan Carvey, Edition 2, Syngress Inc. , 2007
5. Windows Forensic Analysis- Harlan Carvey , Dave Kleiman, Syngress Inc. , 2007
6. Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry – Harlan Carvey, SyngressInc, Feb 2011
7. File System Forensic Analysis- Brian Carrier, Addison Wesley, Edition 1, 2005
8. Handbook of Digital Forensics and Investigation- Eoghan Casey, Academic Press, 2009
9. Digital Forensics with Open Source Tools- Cory Altheide, Harlan Carvey, SyngressInc, Edition1, April 2011

03 CS 6032- 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 / Linux System-Volatile Data collection methodology-Preservation of volatile data, Collecting Subject System details, Identifying Users logged into the system, Inspect Network Connections and activity, Current and recent network connections, Collecting process information, Process to executable program mapping , Dependencies loaded by running processes, Correlate open ports with running processes and programs, Identifying servers and drivers, Determining scheduled tasks, Collecting Clipboard contents, Non-volatile Data collection from a live Windows system, Forensic duplication of storage media on a live Windows system, Forensic preservation of Select Data on a Live Windows System, Incident Response Tool Suites for Windows, Assess Security configuration, Collect Logon and System Logs.	15	25

03 CS 6032- COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
FIRST INTERNAL EXAM			
II	Memory Forensics: Analyzing Physical and Process Dumps for Malware Artifacts- Memory Forensics methodology, Old School Memory Analysis, Windows Memory Forensics Tools, Active, Inactive and Hidden Processes, How Windows Memory Forensics Tools work, Process Memory Dumping and Analysis on a Live Windows System, Capturing Process and Analyzing Memory, Linux Memory Forensics Tools, How Linux Memory Forensics Tools work, Process Memory Dumping and Analysis on a Live Linux System, Capturing and Examining Process Memory in Linux System.	10	25
III	Post-Mortem Forensics: Discovering and Extracting Malware and Associated Artifacts from Windows Systems and Linux systems- Forensic Examinations of Compromised Windows / Linux Systems, Functional Analysis Resuscitating a Windows / Linux Computer, Malware Discovery and Extraction from a Windows/ Linux system, Inspect services, Drivers Auto-starting Locations, and scheduled jobs. Legal considerations- Framing the issues, Sources of Investigative authority, Statutory limits of authority, protected data, Tools for acquiring data, Acquiring data across Borders, Involving Law Enforcement, Improve chances for admissibility.	10	25
SECOND INTERNAL EXAM			
IV	File Identification and profiling: Initial Analysis of a suspect file on a Windows / Linux system-Overview of the File Profiling process, Working with Executables-Compilation, Linking- Static, Dynamic, System details, Hash values, File similarity indexing, File signature identification and classification- File types, Tools, Embedded artifact extraction, Symbolic and Debug information, File Obfuscation: Packing and Encryption Identification-Packers, Cryptors, Wrappers, Elf File structure, Analysis of a suspect program: Windows/ Linux- Analysis Goals, Guidelines for examining a malicious executable program, establishing the environment baseline, Pre -execution preparation: system and network monitoring, Observing, File system, Embedded Artifact Extraction revisited, Exploring and verifying specimen functionality and purpose, Event reconstruction and artifact review: File system, Registry, Process and Network Activity Post-run Data	15	25

03 CS 6032- COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
	Analysis..		
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6042	Image Forensics and Biometric Security	3-0-0	3	2015

Course Objectives

1. To familiarize the fundamentals in image processing through image enhancement, image segmentation and edge detection
2. To study the biometric fundamentals and the different biometric technologies
3. To study the basics of information hiding and steganography
4. Study the latest watermarking techniques

Syllabus

Digital Image representation - Fundamental steps in Image Processing,Image Enhancement,Image Segmentation,Biometric fundamentals – Biometric technologies,Biometrics Vs traditional techniques,Key biometric processes,Physiological Biometrics: Leading technologies,Behavioral Biometrics: Leading technologies,Introduction to Information hiding,Principles of Steganography,Current watermarking techniques: History – Basic Principles – applications,Robustness of copyright making Evaluation and benchmarking of watermarking system

Expected Outcome

1. Understand basic concepts in image processing, biometrics, and image hiding
2. Able to apply biometric and watermarking techniques in image processing

References

1. Anil K Jain, Patrick Flynn, Arun A Ross, "Handbook of Biometrics", Springer, 2008
2. Anil K Jain, Arun A Ross, KarthikNandakumar, "Introduction to Biometrics", Springer, 2011
3. Samir Nanavati, Michael Thieme, Raj Nanavati, "Biometrics – Identity Verification in a Networked World", Wiley-dreamtech India Pvt Ltd, New Delhi, 2003
4. Paul Reid, "Biometrics for Network Security", Pearson Education, New Delhi, 2004
5. John R Vacca, "Biometric Technologies and Verification Systems", Elsevier Inc, 2007
6. Stefan Katzenbelsser and Fabien A. P. Petitcolas, "Information hiding techniques forSteganography and Digital Watermarking", ARTECH House Publishers, January 2004.
7. Jessica Fridrich, "Steganography in Digital Media: Principles, Algorithms, and Applications",Cambridge university press, 2010.
8. Steganography, Abbas Cheddad, VdmVerlag and Dr. Muller, "Digital Image" Aktienge sells chaft& Co. Kg, Dec 2009.9
9. Ingemar Cox, Matthew Miller,JeffreyBloom,JessicaFridrich and TonKalker, "Digital

Watermarking And Steganography", Morgan Kaufmann Publishers, Nov 2007.

03 CS 6042 – COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Digital Image representation - Fundamental steps in Image Processing Image Enhancement: The Spatial Domain Methods, The Frequency Domain Methods - Image Segmentation: Pixel Classification by Thresholding, Histogram Techniques, Smoothing and Thresholding- Gradient Based Segmentation: Gradient Image, Boundary Tracking, Laplacian Edge Detection.	8	25
	Biometric fundamentals – Biometric technologies – Biometrics Vs traditional techniques –Characteristics of a good biometric system – Benefits of biometrics – Key biometric processes: verification, identification and biometric matching – Performance measures in biometric systems, FAR, FRR, FTE rate, EER and ATV rate, Applications of Biometric Systems, Security and Privacy Issues	7	
FIRST INTERNAL EXAM			
II	Physiological Biometrics: Leading technologies : Finger-scan – Facial-scan – Iris-scan – Voice-scan –components, working principles, competing technologies, strengths and weaknesses – Other biometrics technologies : Hand-scan, Retina-scan – components, working principles, competing technologies, strengths and weaknesses – Automated fingerprint identification systems Behavioral Biometrics: Leading technologies: Signature-scan – Keystroke scan – components, working principles, strengths and weaknesses	10	25
III	Introduction to Information hiding – Brief history and applications of information hiding– Principles of Steganography – Frameworks for secret communication – Security of Steganography systems – Information hiding in noisy data – Adaptive versus non adaptive algorithms – Laplace filtering – Using cover models – Active and malicious attackers – Information hiding in written text – Examples of invisible communications. Steganalysis – Detecting hidden information – Extracting hidden information - Disabling hidden information	10	25
SECOND INTERNAL EXAM			
IV	Current watermarking techniques: History – Basic Principles – applications – Requirements of algorithmic design issues – Cryptographic and psycho visual aspects – Choice of a workspace – Formatting the watermark bets - Merging the watermark and the cover – Optimization of the watermark	12	25

03 CS 6042 – COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
	receiver – Extension from still images to video – Robustness of copyright making Evaluation and benchmarking of watermarking system		
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03CS 6052	Information Security Governance	3-0-0	3	2015

Course Objectives

1. To study the basics of governance in information security
2. To familiarize the strategic metrics used in governance
3. To learn efficient techniques for security governance and security program development

Syllabus

Governance Overview—Basics, Origins of Governance,Information Security Governance,Benefits of Good Governance,Security Governance and Regulation,Strategic Metrics,. Information Security Outcomes,Strategic Alignment,Risk Management,Business Process Assurance/Convergence,Resource Management,Security Architecture, Managing Complexity, Providing a Framework and Road Map,Gap Analysis—Unmitigated Risk,Security Program Development Metrics-Information Security Program Development Metrics, Program Development Operational Metrics,Metrics for Risk Management,Incident Management and Response Metrics-Incident Management Decision Support Metrics.

Expected Outcome

1. Capable of handling information security governance issues
2. Capable in identifying risks and learn how to manage risks
3. Capable of developing information security programs and its application in diversified fields

Text Books and References

1.Information Security Governance- A practical development and implementation approach by KragBrotby, 2009.
2. Information Security Governance byS.H. vonSolms, Rossouw von Solms, 2008

3. Information Security Governance byTodd Fitzgerald, 2011
4. Management of Information Security, by MichaelE.Whitman, Herbert J.Mattord,Cengage Learning,2010
5. Applied Information security: A Hands-On guide to Information security- R. Boyle. Prentice Hall, 2010
6. Managing Information Security- John R. Vacca, Elsevier Inc, 2010
7. Information Security Management Principles- AndyTaylor, David Alexander, Amanda Finch, David Sutton, BCS publishers, 2008

03 CS 6052 – COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Governance Overview—Basics, Origins of Governance , Governance Definition , Information Security Governance, Six Outcomes of Effective Security Governance, Defining 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, 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, Increasing Predictability and Reducing Uncertainty of Business Operations, A Management Problem. Legal and Regulatory Requirements- Security Governance and Regulation. Roles and Responsibilities- The Board of Directors, Executive Management , Security Steering Committee, The CISO.	15	25
FIRST INTERNAL EXAM			
II	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—Aligning Security Activities in Support of Organizational Objectives, Risk Management—Executing Appropriate Measures to Manage Risks and Potential Impacts to an Acceptable Level, 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—Using Organizational Resources Efficiently and Effectively, Performance Measurement— Monitoring and Reporting on Security Processes	12	25
III	Security Governance Objectives - Security Architecture, Managing Complexity, Providing a Framework and Road Map, Simplicity and Clarity through Layering and Modularization, Business Focus Beyond the Technical Domain, Objectives of Information Security Architectures, SABSA - SABSA Development Process, SABSA Life Cycle, National	12	25

03 CS 6052 – COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
	Cybersecurity Task Force, Information Security Governance: A Call to Action. Risk Management Objectives - Risk Management Responsibilities, Managing Risk Appropriately, Determining Risk Management Objectives, Recovery Time Objectives. Current State - Current State of Security, SABSA, CobiT, CMM, ISO/IEC 27001, 27002, Cyber Security Taskforce Governance Framework, Current State of Risk Management, Gap Analysis—Unmitigated Risk. Developing a Security Strategy, Using CobiT for Strategy Development, Using CMM for Strategy Development Sample Strategy Development - The Process		
SECOND INTERNAL EXAM			
IV	Security Program Development Metrics-Information Security Program Development Metrics, Program Development Operational Metrics. Information Security Management Metrics,CISO Decisions, Strategic Alignment—Aligning Security Activities in Support of Organizational Objectives, Risk Management—Executing Appropriate Measures to Manage Risks and Potential Impacts to an acceptable Level, Metrics for Risk Management, Assurance Process Integration, Value Delivery—Optimizing Investments in Support of the Organization's Objectives, Resource Management—Using Organizational Resources Efficiently and Effectively, Performance Measurement— Monitoring and Reporting on Security Processes to Ensure that Organizational Objectives are Achieved, Information Security Operational Metrics. Incident Management and Response Metrics- Incident Management Decision Support Metrics.	14	25
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6062	Ethical Hacking	3-0-0	3	2015

Course Objectives

1. To understand the basics of network and computer attacks
2. To study the various OS, Server and Desktop vulnerabilities
3. To study how to hack a windows/Linux based system and how to secure a system from external attacks

Syllabus

Ethical Hacking overview, Network and computer attacks,Desktop and server OS vulnerabilities. Embedded Operating Systems,Exploitation- techniques,Network Protection Systems,Dumpster Diving, Tailgating, Shoulder Surfing- basics,Social Engineering- basics, human nature and weakness, P2P Hacking,End point and server hacking- hacking windows, UNIX, cyber crime and advanced persistent threats. Infrastructure hacking

Expected Outcome

1. Ability to identify the vulnerabilities in asystem
2. Ability to hack a computer system
3. Ability to secure a computer system from threats.

Text books and References

1. Hands on ethical hacking and network defense by Michael T Simpson, Kent Backman, James Corley, Cengage Learning, 2 edition, 2010
2. The Basics of Hacking and Penetration Testingby Patrick Engebretson, Syngress Basics Series, edition 01, 2011
3. NoTech Hacking : A Guide to Social Engineering, Dumpster Diving and Shoulder Surfing by Johnny Long, Syngress publishers, 1st edition, 2008
4. Hacking: The Art of Exploitation, 2nd Edition byJon Erickson, William Pollock publishers, 2008
5. Hackers Beware by Eric Cole, New Riders publishing, 2002
6. An unofficial guide to ethical hacking by AnkitFadia, Macmillan publishers, 2nd edition, 2006
7. Hacking: 01 Edition by S. Pankaj, A P H Publishers, 2005
8. Hacking Exposed 7: Network Security Secrets & Solutions byStuart McClure, Joel Scambray, edition 7, McGraw-Hill publishing, 2012

03 CS 6062 – 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. Embedded Operating Systems: the hidden threat, legal resources, Virtualization and ethical hacking.	13	25
FIRST INTERNAL EXAM			
II	Exploitation- techniques, buffer overflows, BASH, Format strings. Networking- OSI Model, Sockets, network sniffing, TCP/IP Hijacking. Hacking web servers, Hacking Wireless Networks, Network Protection Systems, Shell code, Counter measures .	13	25
III	Dumpster Diving, Tailgating, Shoulder Surfing- basics, locations, electronic deduction, killer real life surfing sessions. Physical Security- Introduction, Lock bumping. Social Engineering- basics, human nature and weakness, the mind of a victim, countering social engineering attacks.	13	25
SECOND INTERNAL EXAM			
IV	Google Hacking Showcase- Introduction, greek stuff, open network devices, applications, cameras, telco gear, power, sensitive info, social security numbers. P2P Hacking, People Watching, Kiosks, Vehicle Surveillance, Badge Surveillance, Epiloque top ten ways to shut down No-Tech hackers. End point and server hacking- hacking windows, UNIX, cyber crime and advanced persistent threats. Infrastructure hacking- remote connectivity and VOIP hacking, wireless hacking, hacking hardware. Reconaissance, Web-based Exploitation, Maintaining Access with Backdoors and Rootkits.	13	25
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6072	Software Forensics and Vulnerability Analysis	3-0-0	3	2015

Course Objectives

1. To make aware the importance of security in software's.
2. To learn how to manage software security risk.
3. To understand the various testing methods.
4. To learn how to identify software vulnerabilities .
5. To understand the host level solutions for vulnerabilities.

Syllabus

Introduction to Software Security,Security Goals, Prevention, Traceability and Auditing, Monitoring, Privacy and Confidentiality,Managing Software Security Risk,- Architectural Risk Analysis - Penetration Testing,Application-Level Threats and Vulnerabilities,Service-Level Threats and Vulnerabilities,Host-Level Solutions,Infrastructure-Level Solutions,Application-Level Solutions.

Expected Outcome

1. Ability to manage software security risk.
2. Ability to identify software vulnerabilities
3. Ability to apply solutions for vulnerabilities detected

References

1. John Viega& Gary McGraw: Building Secure Software: How to Avoid Security Problem the Right Way(Addison-Wesley Professional Computing Series)
2. Gary McGraw: Software Security: Building Security In (Addison-Wesley Professional Computing Series)
3. AbhijitBelapurakar, AnirbanChakrabarti and et al., "Distributed Systems Security: Issues.Processes and solutions", Wiley, Ltd., Publication, 2009.
4. AbhijitBelapurkar, AnirbanChakrabarti, HarigopalPonnapalli, NiranjanVaradarajan, SrinivasPadmanabhuni and SrikanthSundarrajan, "Distributed Systems Security: Issues, Processes andSolutions", Wiley publications, 2009.
5. RachidGuerraoui and Franck Petit, "Stabilization, Safety, and Security of Distributed Systems",Springer, 2010

03 CS 6072 - COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Introduction to Software Security - Dealing with Widespread Security Failures, Bugtraq, CERT Advisories, RISKS Digest, Technical Trends Affecting Software Security,Penetrate and Patch, On Art and Engineering, Security Goals, Prevention, Traceability and Auditing, Monitoring, Privacy and Confidentiality, Multilevel Security, Anonimity, Authentication, Integrity, Know Your Enemy – Common Software Security Pitfalls. Software Project Goals.	12	25
FIRST INTERNAL EXAM			
II	Managing Software Security Risk: Software Risk Management For Security, The Role Of Security Personnel, Software Security Personnel in the Life Cycle, Deriving Requirements, Risk Assessment, Design For Security, Implementation and Testing, A Dose Of Reality, Getting People To Think About Security, Software Risk Management In Practice, When Development Goes Astray, Code Review (Tools) - Architectural Risk Analysis - Penetration Testing - Risk-Based Security Testing - Abuse Cases - Security Requirements – Security Operations	13	25
III	Application-Level Threats and Vulnerabilities: Application-Layer Vulnerabilities –Injection Vulnerabilities -Cross-Site Scripting (XSS) - Improper Session Management - Improper Error Handling - Improper Use of Cryptography - Insecure Configuration Issues - Denial of Service - Canonical Representation Flaws - Overflow Issues. Service-Level Threats and Vulnerabilities: SOA and Role of Standards - Service-Level Security Requirements - Service-Level Threats and Vulnerabilities - Service-Level Attacks – Services Threat Profile	13	25
SECOND INTERNAL EXAM			
IV	Host-Level Solutions: Sandboxing – Virtualization - Resource Management - Proof-Carrying Code -Memory Firewall – Antimalware. Infrastructure-Level Solutions: Network-Level Solutions - Grid-Level Solutions - Storage-Level Solutions. Application-Level Solutions: Application-Level Security Solutions	12	25
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6082	Wireless Security and Mobile Devices Forensics	3-0-0	3	2015

Course Objectives

1. To understand the different wireless technologies
2. To impart deeper understanding of mobile system architecture and the level of security they provide

Syllabus

Wireless technologies and security,Mobile system architectures, Overview of mobile cellular systems,Security Framework for mobile Systems,Mobile Forensics: Crime and mobile phones, evidences, forensic procedures, files present in SIM card,Forensic Analysis of different Mobile devices

Expected Outcome

1. A deep understanding of what the mobile systems provide in respect of security
2. Clear view of the different crimes committed using mobile phones
3. In depth understanding of the files reside inside a mobile system

References

1. Losif I. Androulidakis, " Mobile phone security and forensics: A practical approach", Springer publications, 2012.
2. Andrew Hoog, " Android Forensics: Investigation, Analysis and Mobile Security for Google Android", Elsevier publications, 2011
3. Kia Makki, Peter Reiher, "Mobile and Wireless Network Security and Privacy", Springer
4. NoureddineBoudriga, "Security of Mobile Communications", ISBN 9780849379413, 2010

03 CS 6082 - COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Overview of wireless technologies and security: Personal Area Networks, Wireless Local Area Networks, Metropolitan Area Networks, Wide Area Networks. Wireless threats, vulnerabilities and security: Wireless LANs, War Driving, War Chalking, War Flying, Common Wi-fi security recommendations, PDA Security, Cell Phones and Security, Wireless DoS attacks, GPS Jamming, Identity theft	13	25
FIRST INTERNAL EXAM			
II	Mobile system architectures, Overview of mobile cellular systems, GSM and UMTS Security & Attacks, Vulnerabilities in Cellular Services, Cellular Jamming, Attacks & Mitigation, Security in Cellular VoIP Services, Mobile application security	12	25
III	Security Framework for mobile Systems : CIA triad in mobile phones- Voice, SMS and Identification data interception in GSM: Introduction, practical setup and tools, implementation- Software and Hardware Mobile phone tricks: Netmonitor, GSM network service codes, mobile phone codes, catalog tricks and AT command set- SMS security issues.	12	25
SECOND INTERNAL EXAM			
IV	Mobile Forensics: Crime and mobile phones, evidences, forensic procedures, files present in SIM card, device data, external memory dump, evidences in memory card, operators systems- Android forensics: Procedures for handling an android device, imaging android USB mass storage devices, logical and physical techniques. Forensic Analysis of different Mobile devices	12	25
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6902	Mini Project	0-0-4	2	2015

Course Objectives

The student is expected to do implementation of a sufficiently complex tool or application that demonstrates the significance of any theoretical concept or concepts (or problem or problems) he/she learned in the first or second semester. The work will be supervised and evaluated by a faculty member.

Syllabus

.

No specific Syllabus

Expected Outcome

The student gains in-depth knowledge in the concept/problem he/she has undertaken and allied topics.

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 6802	Network Security and Ethical Hacking Laboratory	0-0-2	1	2015

Syllabus

Experiments are based on but not limited to topics covered in *03 CS 6022: Network Security* and *03 CS 6062: Ethical Hacking*.

Experiments

Experiment No	Description	Hours Allotted
I	Port Scanning using NMap, Superscan	2
II	Enumeration-SNMP, SMTP, Unix/Linux, LDAP, NTP	3
III	Monitoring Live Network capturing packets and analyzing over the live network using Wireshark	2
IV	Vulnerability Scanning	2
V	Firewall, Intrusion detection and Honey pots	3
VI	Password Guessing and Password cracking	3
VII	Buffer overflow attacks	2
VIII	Monitoring Network Communication: Working with Trojans, Backdoors and sniffer	2
IX	Client side script injection to a web application using XSS	2
X	Wireless Network attacks, Bluetooth attacks	3
XI	Website mirroring using HTTrack and hosting on a Local Network	3
XII	Penetration testing and justification of penetration testing through risk analysis, SQL injection Attacks	3
XIII	Steganographic Tools	2

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 7003	Cloud Forensics and Big Data Analysis	3-0-0	3	2015

Course Objectives

1. To understand fundamental concepts of cloud computing.
2. To understand management of virtual machines for cloud infrastructures.
3. To explore benefits, advantages, limitations, applications of cloud infrastuctures
4. To understand how to build cloud networks and to analyze big data.
5. To analyze data with Hadoop
6. To study NoSQL

Syllabus

Cloud Computing,Infrastructure as a Service (IAAS) & Platform and Software as a Service (PAAS / SAAS),Secure Distributed Data Storage in Cloud Computing,Applications for Cloud Environments. Benefits-limitations of Cloud computing,Building Cloud networks,Role of open source software and usage Cloud Analysis and Environment,Security Management in Cloud,Understanding Big data,web analytics – big data and marketing – fraud and big data,introduction to Hadoop – open source technologies – cloud and big data,analyzing data with Hadoop,Design of Hadoop distributed file system (HDFS) – HDFS concepts,Introduction to NoSQL – aggregate data models – aggregates – key-value and document data models,-- Composing Map-Reduce Calculations. MapReduce workflows,MapReduce types – input formats – output formats

Expected Outcome

1. Indepth understanding of cloud and the different Service models
2. Ability to manage cloud infrastructures.
3. Design a Hadoop system and analyze data
4. Understanding of Working with No SQL

References

1. Cloud Computing: Principles and Paradigms by RajkumarBuyya, James Broberg and Andrzej M. Goscinski, Wiley, 2011
2. Toby Velte, Anthony Velte, Robert Elsenpeter ,(2009) Cloud Computing, A Practical Approach, McGraw
3. John W. Rittinghouse, James F. Ransome (2009).Cloud Computing Implementation, Management, and Security
4. Michael Minelli, Michelle Chambers, and AmbigaDhiraj, "Big Data, Big Analytics: Emerging Business Intelligence and Analytic Trends for Today's Businesses", Wiley, 2013

5. Tom White, "Hadoop: The Definitive Guide", Third Edition, O'Reilley, 2012.

03 CS 7003 – COURSE PLAN

Module	Contents	Hours Allotted	% of Marks in End-Semester Examination
I	Introduction to Cloud Computing, Migrating into a Cloud, Enriching the 'Integration as a Service' Paradigm for the Cloud Era, The Enterprise Cloud Computing Paradigm. Infrastructure as a Service (IAAS) & Platform and Software as a Service (PAAS / SAAS) Virtual machines provisioning and Migration services, On the Management of Virtual machines for Cloud Infrastructures, Enhancing Cloud Computing Environments using a cluster as a Service, Secure Distributed Data Storage in Cloud Computing. Aneka, Comet Cloud, T-Systems', Workflow Engine for Clouds, Understanding Scientific Applications for Cloud Environments. Benefits-limitations of Cloud computing- security concerns- regulatory issues –Cloud computing services: IaaS, PaaS,SaaS Software plus services.	13	25
FIRST INTERNAL EXAM			
II	Building Cloud networks-Evolution- Cloud Data Center-Collaboration – SOA- Basic approach to data center based SOA-Role of open source software and usage Cloud Analysis and Environment: Risk Model- Risk treatment – Security Assessment – Virtual Overlays – Malware– Attacks. Cloud Security: Infrastructure Security - Cloud Data Security and storage – Security as a Service- Security Management in Cloud	12	25
III	Understanding Big data:What is big data – why big data – convergence of key trends – unstructured data – industry examples of big data – web analytics – big data and marketing – fraud and big data – risk and big data – credit risk management – big data and algorithmic trading- big data technologies – introduction to Hadoop – open source technologies – cloud and big data – mobile business intelligence – Crowd sourcing analytics – inter and trans firewall analytics Data format – analyzing data with Hadoop – scaling out – Hadoop streaming – Hadoop pipes. Design of Hadoop distributed file system (HDFS) – HDFS concepts – Java interface – data flow, Data Ingest with CFlume and Sqoop. Hadoop I/O – data integrity – compression – serialization – Avro – file-based data structures	12	25
SECOND INTERNAL EXAM			
IV	Introduction to NoSQL – aggregate data models – aggregates – key-value and document data models –relationships – graph databases – schemaless databases – materialized views – distribution models –sharding – master-slave replication – peer-peer replication – sharding and replication. Consistancy relaxing consistency --version stamps—MapReduce – partitioning and combining -- Composing Map-ReduceCalculations. MapReduce workflows – unit tests with MRUnit – test data and local tests – anatomy of MapReduce job run – classic Map-reduce – YARN – failures in classic Map-reduce and YARN – job scheduling – shuffle and sort – task	13	25

	execution – MapReduce types – input formats – output formats		
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 7013	Advanced Data Mining Concepts	3-0-0	3	2015

Course Objectives

1. To learn about the general architecture of data mining systems, as well as gain insight into the kinds of data on which mining can be performed the types of patterns that can be found, and how to tell which patterns represent useful knowledge.
2. To study data mining primitives, from which data mining query languages can be designed and how data mining systems can be classified.
3. To learn methods for mining the simplest form of frequent patterns and basic techniques for data classification

Syllabus

Data mining:-Basic Concepts and Functionalities, Classification of Data Mining Systems, Data Marts, Online Analytical Processing, Data Warehousing, Tools for Data Warehousing, Data Preprocessing. Data Mining Primitives, Data mining Query language. Classification and Prediction. Cluster Analysis. Clustering methods. Partitional Algorithm. Divisive and Agglomerative methods. GA based clustering, Large Database. Web Mining

Expected Outcome

1. This course provides a comprehensive understanding of different data mining tasks and the algorithms most appropriate for addressing them.
2. Defines knowledge discovery and data mining and helps to recognize the key areas and issues in data mining.
3. Gives a fair idea about what type of data are to be mined and present a general classification of tasks and primitives to integrate data mining system.
4. It helps to determine whether a real world problem has a data mining solution

References

1. Jiawei Han, MichelineKamber, Jian Pei, "Data Mining: Concepts and Techniques", Morgan Kaufmann, 2nd Ed., 2005.
2. G. K. Gupta "Introduction to Data Mining with Case Studies", Eastern Economy Edition, Prentice Hall of India, 2006.
3. Soumen Chakrabarti, "Mining the Web: Discovering Knowledge from Hypertext Data", Morghan Kaufmann, 1st Ed., 2005.
4. Margaret H. Dunham, "Data Mining: Introductory and Advanced Topics", Prentice Hall, 1st Ed., 2002.
5. Da Ruan, Guoqing Chen, Etienne E. Kerre, Geert Wets, "Intelligent Data Mining: Techniques and Applications (Studies in Computational Intelligence)", Springer, 1st Ed., 2010.
6. Masoud Mohammadian, "Intelligent Agents for Data Mining and Information Retrieval", Idea Group Publishing, 2004.

7. I. H. Witten and E. Frank. Data Mining: Practical Machine Learning Tools and Techniques. Morgan Kaufmann. 2000.
8. D. Hand, H. Mannila and P. Smyth. Principles of Data Mining. Prentice-Hall. 2001.

03 CS 7013 - COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Data mining:-Basic Concepts and Functionalities, KDD process, Architecture of a typical Data Mining System, Classification of Data Mining Systems, Different kinds of data used for mining, Kinds of Patterns that can be Mined, Major Issues in Data Mining. Data Preprocessing: - Data cleaning, data integration and transformation, data reduction, Discretization and concept hierarchy generation. Data Warehouse: Basic concepts, Differences between Operational Database Systems and Data Warehouses, Stars, Snowflakes, and Fact Constellations: Schemas for Multidimensional Data Models, Typical OLAP Operations.	13	25
FIRST INTERNAL EXAM			
II	Association Rules mining- Introduction, basics, Naïve Algorithm, Improved Naïve algorithm, the Apriori algorithm, Frequent, closed and maximal Item set. Mining frequent patterns without candidate generation. Classification and Prediction:-Decision Tree – tree induction algorithm, Split algorithm based on information theory, Split algorithm based on the Gini index- Naïve Bayes method- Estimating predictive accuracy of classification methods.	10	25
III	Cluster Analysis: -Desired features of cluster Analysis, Types of data in cluster analysis, Computing Distance, clustering methods: Partitional methods -MST, Squared Error, K-Means, Nearest Neighbour, PAM, Hierarchical methods-Single link, average Link, Complete Link, Dendrogram - Divisive and Agglomerative methods- GA based clustering, Categorical algorithm, Dealing with Large Databases, Quality and validity of cluster analysis methods	12	25
SECOND INTERNAL EXAM			

03 CS 7013 - COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
IV	Web Mining:-Introduction, Web data, Web Knowledge mining Web Mining:-Introduction, Web data, Web Knowledge mining Taxonomy, Web Content Mining, Web usage Mining, Ontology based web mining research, Web Mining Application.	7	25
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 7023	Information Storage and Security	3-0-0	3	2015

Course Objectives

1. To introduce storage management and information life cycle Management
2. To learn the storage system architecture and different storage system protocols
3. To study the management philosophies and the security concerns in storage

Syllabus

Basic storage management skills and activities,storage infrastructure components,Information Lifecycle Management,Storage Systems Architecture,Disk physical structure,Storage system connectivity protocols,Management philosophies,Industry management standards,Reactive and pro-active management best practices,Storage security-critical security attributes for information systems, elements of a shared storage model,Cloud level security

Expected Outcome

1. Be able to manage storage using different storage system protocols
2. Indepth knowledge of security attributes in storage

References

1. Information Storage and Management: Storing, Managing, and Protecting Digital Information in Classic, Virtualized, and Cloud Environments, (2nd ed.), EMC Education Services ISBN: 978-1-1180-9483-9, (2012)
2. Marc Farley Osborne, "Building Storage Networks", Tata Mac Graw Hill, 2001

3. Robert Spalding and Robert Spalding, "Storage Networks: The Complete Reference", Tata McGrawHill, 2003
4. Meeta Gupta, "Storage Area Network Fundamentals", Pearson Education Ltd., 2002

03 CS 7023 – COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Data proliferation and the varying value of data with time & usage, Sources of data and states of data creation, Data center requirements and evolution to accommodate storage needs, Overview of basic storage management skills and activities, The five pillars of technology, Overview of storage infrastructure components, Evolution of storage, Information Lifecycle Management concept, Data categorization within an enterprise, Storage and Regulations.	13	25
	FIRST INTERNAL EXAM		
II	Storage Systems Architecture: Intelligent disk subsystems overview, Contrast of integrated vs.modular arrays, Component architecture of intelligent disk subsystems, Disk physical structure components, properties, performance, and specifications, Logical partitioning of disks, RAID & parity algorithms, hot sparing, Physical vs. logical disk organization, protection, and back end management, Array caching properties and algorithms, Front end connectivity and queuing properties, Front end to host storage provisioning, mapping, and operation, Interaction of file systems with storage, Storage system connectivity protocols .Networked Storage: JBOD, DAS, SAN, NAS, & CAS evolution elements, connectivity, & management.	14	25
III	Management philosophies (holistic vs. system & component), Industry management standards (SNMP, SMI-S, CIM), Standard framework applications, Key management metrics (thresholds, availability, capacity, security, performance), Metric analysis methodologies & trend analysis, Reactive and pro-active management best practices, Provisioning & configuration change planning, Problem reporting, prioritization, and handling techniques, Management tools	11	25
	SECOND INTERNAL EXAM		
IV	Storage security-critical security attributes for information systems, elements of a shared storage model and security extensions, storage security domains, analyze the common threats in each domain, different virtualization technologies, describe block-level and file level virtualization technologies and processes. Cloud level security	12	25

03 CS 7023 – COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 7033	Cyber Crime, Legal Issues and Ethics	3-0-0	3	2015

Course Objectives

1. To understand the different types of cyber crimes and cyber laws in india and abroad
2. To impart sufficient knowledge on the fundamental legal issues in internet archiving.
3. To expose to ethical issues in today's computer based environment

Syllabus

Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime,cyber crime issues,Computer Ethics,Ethics and IT,Legal issues in Computer Information Systems,Legal issues in archiving internet resources-internet archiving,web archiving,understanding international security system,Evolution of Cyber law-Evolution of property rights,Legal measures to protect the integrity on the internet,, The Information Technology Act 2000,regulation of certifying authorities, duties of subscribers, penalties and adjudication, the cyber regulations Appellate

Expected Outcome

1. Awareness of rules and regulations, and of the laws applicable to computer and software related contracts.
2. Exposure to different forms of Cyber crimes and the Indian and International laws to combat Cyber crimes and facilitate e-commerce.
3. Capability to reason out different situations of ethics faced in the cyber world.

References

1. Cyber crime and Legal issues-Paul T Augastine-Crescent Publishing corporation,2007
2. Deborah G Johnson, Computer Ethics, Pearson Education Pub., ISBN : 81-7758-593-2.
3. Cyber crime and corporate liability-RohasNagpal, Kluwer publications,2008
4. Cyber crime-Prosecution and defence-rohasNagpal,asian school of Cyber laws,2008
5. Nelson Phillips and EnfingerSteuart, "Computer Forensics and Investigations", Cengage

Learning, New Delhi, 2009.
6. Bernadette H Schell, Clemens Martin, "Cybercrime", ABC – CLIO Inc, California, 2004.
7. Cyber crime investigation Manual-RohasNagpal, ASCL Academy 2008
8. Cyber crime and Law enforcement-V.D.Dudeja, Common wealth Publishers,2003
9. Digital evidence and Computer crime-Eoghan Casey, academia Press,2004

03 CS 7033 – COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime: Social Engineering, Categories of Cyber Crime, cyber crime issues: Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Child Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation ,Stalking and Obscenity in Internet Computer Ethics: Why Computer Ethics ,Ethics and IT, Ethics in IT configured Societies, activities, Domain of Life, Democracy and the Internet	13	25
FIRST INTERNAL EXAM			
II	Computer information Systems, Legal issues in Computer Information Systems, Regulation of Computer crime, Computer information system content. Legal issues in archiving internet resources-internet archiving,web archiving, crime prevention in cyber space, support of victims in reporting computer crime, understanding international security system, Criminal intelligence and investigation practices, use of gathering police information ,factors for information and non information sharing and non sharing.	12	25
III	Evolution of Cyber law-Evolution of property rights, impacts of factors ,security of property rights, assurance problems, determinants of trust, reputation and recourse, dispute resolution of thirty party, customary law, polycentric governance, institutional developments in cyber space, benefits of polycentric customary law	11	25
SECOND INTERNAL EXAM			
IV	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, problems in personal data, tolerability of computer generated evidence, harmonization of Cyber laws, The Information Technology Act 2000-Definitions,secure digital signature, Secure Electronic records, regulation of certifying authorities, duties of subscribers, penalties and adjudication, the cyber regulations Appellate	13	25
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
01 CS 7043	Intellectual Property Rights	3-0-0	4	2015

Course Objectives

1. To have a n understanding of Intellectual property rights

Syllabus

Intellectual Property Law,Legal Tasks in Intellectual Property Law,Trade mark – Trade mark Registration Process,Infringement,Copyrights – – Principles of Copyrights -The subjects Matter of Copy right,law of patents-patent searches –Patent owner ship and transfer-Patent infringement-Patent Litigation- International Patent Law,Trade Secret – Maintaining Trade Secret – Physical Security,TRIPS Agreement, Geographical Indications (GI), IPRs in Information and communication technologies (ICT)

Expected Outcome

1. The student gets a wide exposure of the Intellectual property rights

References

1. DebiragE.Bouchoux: "Intellectual Property". Cengage learning, New Delhi
2. M.Ashok Kumar and Mohd.Iqbal Ali: "Intellectual Property Right" Serials Pub.
3. Cyber Law. Texts & Cases, South-Western's Special Topics Collections
4. PrabhuddhaGanguli: ' Intellectual Property Rights" Tata Mc-Graw –Hill, New Delhi
5. J Martin and C Turner "Intellectual Property" CRC Press
6. Richard Stimm " Intellectual Property" Cengage Learning

03 CS 7043– COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Introduction to Intellectual Property Law – The Evolutionary Past - The IPR Tool Kit- Para -Legal Tasks in Intellectual Property Law – Ethical obligations in Para Legal Tasks in Intellectual Property Law - Introduction to Cyber Law – Innovations and Inventions Trade related Intellectual Property Right	12	25
FIRST INTERNAL EXAM			
II	Introduction to Trade mark – Trade mark Registration Process – Post registration Procedures – Trade mark maintenance - Transfer of Rights - Inter partes Proceeding – Infringement - Dilution Ownership of Trade mark – Likelihood of confusion - Trademarks claims – Trademarks Litigations – International Trade mark Law	12	25
III	Introduction to Copyrights – – Principles of Copyrights -The subjects Matter of Copy right – The Rights Afforded by Copyright Law – Copyrights Ownership- Transfer of ownership and duration of copyright – Right to Prepare Derivative Works – Rights of Distribution – Rights of Publicity - Copyright Formalities and Registrations - Limitations - Copyright disputes and International Copyright Law – Semiconductor Chip Protection Act	10	25
	The law of patents-patent searches –Patent owner ship and transfer-Patent infringement-Patent Litigation- International Patent Law	5	
SECOND INTERNAL EXAM			
IV	Introduction to Trade Secret – Maintaining Trade Secret – Physical Security – Employee Limitations - Employee confidentiality agreements - Trade Secret Law - Unfair Competition – Trade Secret Litigation – Breach of Contract – Applying State Law	8	25
	TRIPS Agreement, Geographical Indications (GI), IPRs in Information and communication technologies (ICT), Intellectual Property Rights in Software: Copyright and Licensing, Software Patents, Free/Open Source Software Licensing. Copyright and neighbouring rights in Internet.	7	
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 7053	Programming with Python and Perl	3-0-0	3	2015

Course Objectives

1. To understand programming with Python and Perl Language

Syllabus

Introduction to Python - Data Types and variables -Operators and Expressions,Functions and Functional Programming,Classes, Objects and other OOPS concepts. I/O in Python,Multithreading and Concurrency - Inter Process Communication (IPC),Network Security Programming,Web Application Security: Web Servers and Client scripting,Exploit Development techniques,Writing plugins in Python,Perl Programming using scripts

Expected Outcome

The students who succeeded in this course should be

1. able to write programs in Python Programming language.
2. able to write scripts using Perl Scripts

References

1. Mike Dawson,"More Python programming for Absolute Beginner", Cengage Learning PTR; 3rd edition,2010
2. Mark Lutz," Python Pocket reference", O'Reilly Media; 4 th edition,2009
3. Randal L. Schwartz,"LearningPearl",O'Reilly ,2011

03 CS 7053 – COURSE PLAN			
Module	**Contents**	**Hours Allotted**	**% of Marks in End-Semester Examination**
I	Introduction to Interpreted Languages and Python - Data Types and variables -Operators and Expressions - Program Structure and Control - Functions and Functional Programming - Classes, Objects and other OOPS concepts. I/O in Python - File and Directory Access - Multithreading and Concurrency - Inter Process Communication (IPC) - Permissions and Controls	13	25
FIRST INTERNAL EXAM			
II	Network Security Programming :Raw Socket basics -Socket Libraries and Functionality - Programming Servers and Clients - Programming Wired and Wireless Sniffers - Programming arbitrary packet injectors - PCAP file parsing and analysis.Web Application Security: Web Servers and Client scripting - Web Application Fuzzers - Scraping Web Applications – HTML and XML file analysis - Web Browser Emulation - Attacking Web Services - Application Proxies and Data Mangling - Automation of attacks such as SQL Injection, XSS etc.	10	25
III	Exploit Development techniques - Immunity Debuggers and Libs - Writing plugins in Python - Binary data analysis - Exploit analysis Automation. Sample Programs in Python	11	25
SECOND INTERNAL EXAM			
IV	Perl Programming using scripts	13	25
END SEMESTER EXAM			

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 7903	Seminar II	0-0-2	1	2015

Course Objectives

To make students,

- identify a domain of interest
- identify sufficient number of latest good quality research papers on a particular problem or allied problems
- do extensive study and analysis of the problem and solution(s)
- Prepare a comprehensive report
- make a presentation of 30 minutes based on the report

Seminar Guidelines

- Topic should be relevant to the stream of study with content suitable for M.Tech level Presentation.
- For selection of topics refer internationally reputed transactions/journals. The primary reference should be published during the last two or three years.
- A detailed write-up /synopsis should be prepared in the prescribed format given by the Department and get the topic approved by the PG Coordinator well in advance.
- The seminar shall be of 30 minutes duration and a committee, with the PG Co-ordinator as the chairman and two faculty members from the department as members shall evaluate the seminar based on the technical content, presentation, depth of knowledge and ability to answer the questions put forward by the committee.
- After the completion of the Seminar work the students would be required to submit two copies of the seminar reports prepared by them in the prescribed format.

Expected Outcome

To student

- gets good exposure to a domain of interest and the research problems in the domain
- improves his/her writing and presentation skills
- Gets practice in the art of doing literature survey

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 7913	Project (Phase I)	0-0-8	6	2015

Course Objectives

The main objective is to provide an opportunity to each student to do an independent study and research in the area of specialization under the guidance of a faculty member. The student is required to explore in depth and a topic of his/her own choice, which adds significantly to the body of knowledge existing in the relevant field. The student has to undertake and complete the preliminary work on the stream of specialization during the semester.

Syllabus

.

Each student shall identify a project related to the curriculum of study.

Expected Outcome

The student is expected to identify a domain in the area of specialization, do enough exploration by reviewing the literature. The student should also identify his problem and objectives. The progress will be assessed by two reviews. First review would highlight the topic, objectives, methodology and expected results and shall be conducted in first half of the semester. Second review comprises of the presentation of the work completed and scope of the work which is to be completed in the forthcoming semester. Progress of the project work is to be evaluated at the end of the semester. The student is also expected to submit a preliminary report at the end of the semester.

Guidelines for Project (Phase I)

- **Total Marks : 50**
- Progress evaluation by the Project Supervisor : 20 Marks
- Presentation and evaluation by the committee : 30 Marks

Course No.	Course Name	L-T-P	Credits	Year of Introduction
03 CS 7914	Project (Phase II)	0-0-21	12	2015

Course Objectives

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

Syllabus

.

Each student shall identify a project related to the curriculum of study

Expected Outcome

The student is expected to publish technical papers related to his/her research in peer reviewed journals/conferences.

Guidelines for Project (PhaseII)

- **Total Marks: 100**
- Project evaluation by the supervisor: 30 Marks
- Evaluation by the External Expert: 30 Marks
- Presentation & Evaluation by the Committee: 40 Marks