Kerala Technological University

Cluster 4: Kottayam

# M. Tech Program in Computer Science & Engineering (Cyber Security)

Scheme of Instruction & Syllabus: 2015 Admissions


Compiled By

**Rajiv Gandhi Institute of Technology, Kottayam**

July 2015

**Kerala Technological University**

**(Kottayam Cluster)**

**M. Tech Program in Computer Science and Engineering (Cyber Security)**

**Scheme**

**Credit requirements** **:** 66
Normal Duration : Regular: 4 semesters; External Registration: 6 semesters
Maximum duration : Regular: 6 semesters; External Registration: 7 semesters
Courses: Core Courses: Either 4 or 3 credit courses; Elective courses: All of 3 credits
**Allotment of credits and examination scheme:-**

**Semester 1** (Credits: 22)

| Exam Slot | Course No: | Name | L- T - P | Internal Marks | End Semester Exam | | Credits |
|---|---|---|---|---|---|---|---|
| | | | | | Marks | Duration (hrs) | |
| A | 04 CS 6301 | Mathematical Foundations For Computer Science | 3-1-0 | 50 | 50 | 3 | 4 |
| B | 04 CS 6303 | Advanced Data Structures and Algorithms | 3-1-0 | 50 | 50 | 3 | 4 |
| C | 04 CS 6305 | Operating Systems And Security | 3-0-0 | 50 | 50 | 3 | 3 |
| D | 04 CS 6307 | Cryptographic Protocols and Standards | 3-0-0 | 50 | 50 | 3 | 3 |
| E | 04 CS 6XXX* | Elective - I | 3-0-0 | 50 | 50 | 3 | 3 |
| | 04 GN 6001 | Research Methodology | 0-2-0 | 100 | 0 | 0 | 2 |
| | 04 CS 6391 | Seminar - I | 0-0-2 | 100 | 0 | 0 | 2 |
| | 04 CS 6393 | Information Security Lab | 0-0-2 | 100 | 0 | 0 | 1 |
| | | Total | 23 | | | | 22 |

**See List of Electives-I for slot E*

**List of Elective - I Courses**

| Exam Slot | Course No. | Course Name |
|---|---|---|
| E | 04 CS 6304 | Mobile Network Security |
| E | 04 CS 6311 | Information Risk Management |
| E | 04 CS 6313 | Cryptography and Network Security |
| E | 04 CS 6315 | Secure Coding |

**Semester 2** (Credits: 18)

| Exam Slot | Course No: | Name | L- T - P | Internal Marks | End Semester Exam | | Credits |
|---|---|---|---|---|---|---|---|
| | | | | | Marks | Duration (hrs) | |
| A | 04 CS 6302 | Cyber Crime Investigations And Digital Forensics | 3-0-0 | 50 | 50 | 3 | 3 |
| B | 04 CS 6304 | Security Threats | 3-0-0 | 50 | 50 | 3 | 3 |
| C | 04 CS 6306 | Ethical Hacking | 3-0-0 | 50 | 50 | 3 | 3 |
| D | 04 CS 6XXX* | Elective 2 | 3-0-0 | 50 | 50 | 3 | 3 |
| E | 04 CS 6XXX^ | Elective 3 | 3-0-0 | 50 | 50 | 3 | 3 |
| | 04 CS 6392 | Mini Project | 0-0-4 | 100 | 0 | 0 | 2 |
| | 04 CS 6394 | Ethical Hacking Lab | 0-0-2 | 100 | 0 | 0 | 1 |
| | | Total | 21 | | | | 18 |

**See List of Electives -II for slot D* *^See List of Electives -III for slot E*

**List of Elective - II Courses**

| Exam Slot | Course Code | Course Name |
|---|---|---|
| D | 04 CS 6308 | Storage Management And Security |
| D | 04 CS 6312 | Digital Watermarking |
| D | 04 CS 6314 | Design of Secured Architectures |
| D | 04 CS 6316 | Biometric Security |

**List of Elective - III Courses**

| Exam Slot | Course Code | Course Name |
|---|---|---|
| E | 04 CS 6318 | Penetration Testing and Vulnerability Assessment |
| E | 04 CS 6322 | Internet Information And Application Security |
| E | 04 CS 6324 | Database Security |
| E | 04 CS 6326 | Cryptanalysis |

**Summer Break**

| Exam Slot | Course No: | Name | L- T - P | Internal Marks | End Semester Exam | | Credits |
|---|---|---|---|---|---|---|---|
| | | | | | Marks | Duration (hrs) | |
| NA | 04 CS 7390 | Industrial Training | 0-0-4 | NA | NA | NA | Pass /Fail |
| | | Total | 4 | | | | 0 |

**Semester 3** (Credits: 14)

| Exam Slot | Course No: | Name | L- T - P | Internal Marks | End Semester Exam | | Credits |
|---|---|---|---|---|---|---|---|
| | | | | | Marks | Duration (hrs) | |
| A | 04 CS 7XXX* | Elective - IV | 3-0-0 | 50 | 50 | 3 | 3 |
| B | 04 CS 7XXX^ | Elective - V | 3-0-0 | 50 | 50 | 3 | 3 |
| | 04 CS 7391 | Seminar - II | 0-0-2 | 100 | 0 | 0 | 2 |
| | 04 CS 7393 | Project (Phase - I) | 0-0-12 | 50 | 0 | 0 | 6 |
| | | Total | 20 | | | | 14 |

**See List of Electives-IV for slot A* *^See List of Electives-V for slot B*

**List of Elective - IV Courses**

| Exam Slot | Course Code | Course Name |
|---|---|---|
| A | 04 CS 7301 | Distributed And Cloud Computing |
| A | 04 CS 7303 | Web Security |
| A | 04 CS 7305 | Intrusion Detection And Prevention System |
| A | 04 CS 7307 | Cloud Architectures And Security |

**List of Elective - V Courses**

| Exam Slot | Course Code | Course Name |
|---|---|---|
| B | 04 CS 7304 | Malware Analysis |
| B | 04 CS 7311 | File System Forensic Analysis |
| B | 04 CS 7313 | Cloud And Utility Computing |
| B | 04 CS 7315 | Interactive Programming With Python |

**Semester 4** (Credits: 12)

| Exam Slot | Course No: | Name | L- T - P | Internal Marks | External Evaluation Marks | | Credits |
|---|---|---|---|---|---|---|---|
| NA | 04 CS 7394 | Project (Phase -II) | 0-0-21 | 50 | 50 | NA | 12 |
| | | Total | 21 | | | | 12 |

Total: 66

| COURSE CODE | COURSE NAME | L-T-P:C | YEAR OF INTRODUCTION |
|---|---|---|---|
| 04 CS 6301 | MATHEMATICAL FOUNDATIONS FOR COMPUTER SCIENCE | 4-0-0: 4 | 2015 |

**Pre-requisites:**

**Course Objectives**:

To give the Student:-

- A foundation in the fundamentals of information theory;
- Applications of probability distributions and fuzzy sets.
- An introduction to algebraic foundations for cryptography.

**Syllabus**

The syllabus includes basics of information theory, probability theory and algebra.

**Course Outcome:**

Understand mathematical concepts for cryptographic algorithms.

**References**:


1. R Bose, “Information Theory, Coding and Cryptography”, TMH 2007
2. Sheldon M. Ross, “A First Course in Probability”, Eighth Edition, Pearson Education, 2004.
3. Anirban Das Gupta, “Fundamentals of Probability: A First Course”, Springer, 2010.
4. George J Klir and Bo Yuan, ”Fuzzy sets and Fuzzy logic” Prentice-Hall of India,1995
5. William Stallings, “Cryptography and network security-principles and practice”, 3rdEdition, Pearson Prentice Hall.
6. Douglas Comer, “Internetworking with TCP IP Vol.1: Principles, Protocols, and Architecture”, Prentice Hall
7. George Varghese, “Network Algorithmics: An Interdisciplinary Approach to Designing Fast Networked Devices”, Elsevier, 2004
8. Michael Welzl, “Network Congestion Control –managing internet traffic”, John Wiley& Sons
9. RobertazziT.G,”Computer Networks and systems-Queuing Theory and Performance Evaluation”-Springer third edition.
10. Robert Love,“Linux System Programming:Talking directly to the Kernel and C library”, Oreilly media

**COURSE PLAN**

| COURSE CODE: | COURSE TITLE | CREDITS |
|---|---|---|
| 04 CS 6301 | **Mathematical Foundations For Computer Science** | **4-0-0:4** |

| MODULES | Contact Hours | Sem. Exam Marks (%) |
|---|---|---|
| MODULE 1: **Introduction to Information Theory:** Concept of amount of information-Entropy-Joint and Conditional Entropy-Relative Entropy.Mutual information-Relationship between Entropy and Mutual information-Rate of information**,** Channel capacity-Redundancy and efficiency of channels –Huffman Codes –Hidden Markovian Models | 8 | 15 |
| MODULE 2: **Fundamentals of probability:** Random Variables: Discrete random variables Expectation, Variance, Bernoulli and Binomial random variables, Geometric Random variable, Poisson random variable | 8 | 15 |
| INTERNAL TEST 1 (MODULE 1 & 2) | | |
| MODULE 3: **Probability distributions**: Cumulative distribution function, Continuous random variables: Expectation andVariance of a Continuous random variable ,Normal variable, The Normal approximation to Binomial Distribution, Gamma and Beta Distributions. | 8 | 15 |
| MODULE 4: **Algebraic Foundations**: Groups, Rings and Fields. **Queuing and Scheduling Models** :General concepts, Arrival pattern, service pattern. Queue Disciplines: Queues in Wireless nodes –DropTail, RED, SFQ queuing models, Case Study : Completely Fair Scheduler in Linux. | 8 | 15 |
| INTERNAL TEST 2 (MODULE 3 & 4) | | |
| MODULE 5: **Mathematics in Networking and Security:** Mathematical Foundations of Cryptography : Modulo arithmetic –Additive and multiplicative inverses of natural numbers under modulo arithmetic -Euler's theorem & Fermat's theorem Chinese Remainder theorem –Linear and affine ciphers –Fiestel cipher structure –Integer factorization & Discrete Logarithm problems Elliptic curve cryptography. | 12 | 20 |
| MODULE 6: **Fuzzy Sets:**Crisp sets and Fuzzy sets-, α-cuts, Convex fuzzy sets, Fuzzy cardinality, Algebra of fuzzy sets<br><br>Standard fuzzy set operations-(complement, union and intersection), Yager and Sugeno classes. Crisp relations and Fuzzy relations. Operations on Fuzzy relations.Fuzzy Cartesian product.Fuzzy Equivalence relations and similarity relations | 12 | 20 |
| END SEMESTER EXAM | | |

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 6303 | ADVANCED DATA STRUCTURES AND ALGORITHMS | 4-0-0: 4 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Understand advanced algorithmic strategies.

**Syllabus**

The syllabus includes analysis of algorithms, trees, queues etc.

**Course Outcome:**

Understand the advanced concepts in algorithms analysis.

**References**:


1. Ellis Horowitz, SartajSahni, Susan Anderson Freed, Fundamentals of Data Structures in C, Second Edition, University Press, 2008
2. YedidyahLangsam, Moshe J. Augenstein, Aaron M. Tenenbaum, Data Structures using C and C++, Second Edition, PHI Learning Private Limited, 2010
3. Thomas Cormen, Charles, Ronald Rives, Introduction to algorithm,3rd edition, PHI Learning
4. Ellis Horowitz and SartajSahni, SanguthevarRajasekaran, Fundamentals of Computer Algorithms,Universities Press, 2nd Edition, Hyderabad .
5. Sara Baase& Allen Van Gelder , Computer Algorithms – Introduction to Design and Analysis, Pearson Education..
6. AnanyLevitin, Introduction to The Design & Analysis of Algorithms, Pearson Education, 2nd Edition, New Delhi, 2008.
7. Berman and Paul, Algorithms, Cenage Learning India Edition, New Delhi, 2008.
8. S.K.Basu , Design Methods And Analysis Of Algorithms ,PHI Learning Private Limited, New Delhi,2008.
9. Jon Kleinberg and Eva Tardos, Algorithm Design, Pearson Education, NewDelhi, 2006.
10. Hari Mohan Pandey, Design Analysis And Algorithms, University Science Press, 2008.
11. R. Panneerselvam, Design and Analysis of Algorithms, PHI Learning Private Limited, New Delhi, 2004.
12. UditAgarwal, Algorithms Design And Analysis, DhanapatRai& Co, New Delhi, 2004.
13. Aho, Hopcroft and ullman, The Design And Analysis of Computer Algorithms, Pearson Education, New Delhi, 2007.
14. S.E.Goodman and S. T. Hedetmiemi, Introduction To The Design And Analysis Of Algorithms, McGraw-Hill International Editions, Singapore 2000.
15. Richard Neapolitan, Kumarss N, Foundations of Algorithms, DC Hearth &company.
16. Sanjay Dasgupta, Christos Papadimitriou, UmeshVazirani, Algorithms, Tata McGraw-Hill Edition.

**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS | |
|---|---|---|---|
| 04 CS 6303 | ADVANCED DATA STRUCTURES AND ALGORITHMS | 4-0-0:4 | |
| **MODULES** | | **Contact hours** | **Sem. Exam Marks; %** |
| **MODULE : 1 -**<br><br>Analysis of Algorithms-review of algorithmic strategies, asymptotic analysis, solving recurrence relations through Substitution Method Recursion Tree, and Master Method | | 6 | 15 |
| **MODULE : 2 –**<br><br>Dynamic Programming- Rod cutting-top down and bottom up approach, matrix chain multiplication-recursive solution, Longest common subsequence problem | | 6 | 15 |
| **FIRST INTERNAL TEST** | | | |
| **MODULE : 3**<br><br>Maximum Flow-Flow Networks, Ford-Fulkerson method analysis of Ford-Fulkerson, Edmonds-Karp algorithm, Maximum bipartite matching | | 6 | 15 |
| **MODULE : 4**<br><br>Computational Geometry- Line segment properties Finding the convex hull , Finding the closest pair of points | | 6 | 15 |
| **SECOND INTERNAL TEST** | | | |
| **MODULE : 5 -**<br><br>Trees - Threaded Binary Trees, Selection Trees, Forests and binary search trees. Counting Binary Trees, Red-Black Trees, Splay Trees Suffix Trees, Digital Search Trees, Tries- Binary Tries, Multiway Tries. | | 12 | 20 |
| **MODULE : 6** -<br><br>Priority Queues - Single and Double Ended Priority Queues, Leftist Trees. Binomial Heaps, Fibonacci Heaps, Pairing Heaps Symmetric Min-Max Heaps, Interval Heaps. | | 12 | 20 |
| END SEMESTER EXAM | | | |

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 6305 | OPERATING SYSTEMS AND SECURITY | 4-0-0: 4 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Familiarize OS concepts, process and memory management and OS security.

**Syllabus**

The syllabus includes malware analysis and protection, virtualization technique for security.

**Course Outcome:**

Understand security concepts in OS

**References**:


1. Andrew S. Tanenbaum, —Modern Operating Systems‖, 2nd edition, Addison Wesley, 2001.
2. Gary Nutt, —Operating Systems a Modern Perspective —, 2nd edition, Pearson Edition, 2001.
3. Trent Jaeger, —Operating System Security‖, Volume 1 of SynThesis Lectures on Information Security, Privacy and Trust, Morgan & Claypool Publishers, 2008.
4. Wolfgang Mauerer, —Professional Linux Kernel Architecture‖, John Wiley and Sons, New York, 2008
5. Reading: J.H. Saltzer and M.D. Schroeder, the Protection of Information in Computer Systems. Setuid Demystified, by Chen, Wagner.
6. Reading: Kerberos Authentication. Refer Website.
7. Reading: Nachenberg, Computer Virus-Antivirus Coevolution. Comm. ACM, 40(1), pp. 46-51, January 1997.
8. Paxson, *Bro:* A System for Detecting Network Intruders in Real-Time. Proc. 7th USENIX Security Symposium, San Antonio, TX, January 1998
9. Charles P. Pfleeger, “Security in Computing”, Pearson Education, Third Edition, 2005.

**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS | |
|---|---|---|---|
| 04 CS 6305 | OPERATING SYSTEMS AND SECURITY | 4-0-0:4 | |
| **MODULES** | | **Contact hours** | **Sem. Exam Marks; %** |
| **MODULE : 1 -**<br><br>Introduction Operating Systems Concepts – System Calls – OS Organization<br><br>Factors in OS Design – Basic Implementation Considerations – Time Sharing and Multi Programming.<br><br>Real Time Systems. | | 6 | 15 |
| **MODULE : 2**<br><br>Process Management: Process Concepts, Model – Process Synchronization. Process Scheduling, Threads. Dead Lock: Detection &Recovery, Avoidance, and Prevention- Two Phase Locking Issues | | 6 | 15 |
| **FIRST INTERNAL TEST** | | | |
| **MODULE : 3**<br><br>Memory Management Basic Memory Management – Swapping Virtual Memory and demand Paging– Paging with segmentation Page Replacement Algorithms-Segmentation | | 6 | 15 |
| **MODULE : 4**<br><br>File System and I/O Management Files – Low Level File Implementations – File system security .<br><br>Remote file system security NFS, SMB., SFS | | 6 | 15 |
| **SECOND INTERNAL TEST** | | | |
| **MODULE : 5**<br><br>User authentication, Passwords, Biometrics, and Smartcards .Memory Mapped Files – Directories, Implementation – Principles of I/O Hardware & Software<br><br>Device Drivers – Disks Hardware, Formatting & Arm Scheduling Algorithms | | 12 | 20 |

| | | |
|---|---|---|
| **MODULE : 6**<br><br>Security and protection in operating systems Secure Operating Systems – access control, auditing, trusted computing base, buffer overflows.<br><br>Malware analysis and protection: rootkits and their defenses, polymorphic malware, malware capture and analysis such as honeypots.<br><br>Virtualization technique for security. Intrusion Detection and Virus Protection, TCPA and NGSCB, Digital Rights Management.<br><br>Models of Security – Bell-La Padula Confidentiality Model and Biba Integrity Mode | 12 | 20 |
| END SEMESTER EXAM | | |

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 6307 | CRYPTOGRAPHIC PROTOCOLS AND STANDARDS | 3-0-0: 3 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Understand protocol goals.
- Familiarize protocols for key establishment, authentication etc.

**Syllabus**

The syllabus includes protocol goals, protocols using public key cryptography, shared key cryptography.

**Course Outcome:**

Understand various protocols for key establishment, authentication etc.

**References**:

1. Collin Boyd and AnishMathuria, "Protocols for Authentication and Key Establishment", Springer; 2010.

2. Abhijith Das and C.E. VeniMadhavan, "Public-key Cryptography, Theory and Practice", Pearson Education, 2004.

3. Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996

| COURSE NO: | COURSE TITLE: | CREDITS | |
|---|---|---|---|
| 04 CS 6307 | CRYPTOGRAPHIC PROTOCOLS AND STANDARDS | 3-0-0:3 | |
| MODULES | | Contact hours | Sem. Exam Marks; % |
| **MODULE : 1 -**<br><br>Goals for authentication and Key Establishment: Basic Goals , Enhanced Goals, Goals concerning compromised Keys, Formal Verification of Protocols, Complexity Theoretic Proofs of Security. | | 6 | 15 |
| **MODULE : 2 –**<br><br>Protocols Using Shared Key Cryptography: Entity Authentication Protocols-Bellare-Rogaway,Woo-Lam. Authentication Protocol.Server-Less Key Establishment, Andrew Secure RPC Protocol, Boyd Two-Pass. | | 6 | 15 |
| **FIRST INTERNAL TEST** | | | |
| **MODULE : 3**<br><br>Server-Based Key Establishment-Needham-Schroeder Shared Key Protocol, Otway-Rees ,Kerberos, Key Establishment Using Multiple Servers-Gong's Multiple Server, Zero Knowledge interactive proofs. | | 6 | 15 |
| **MODULE : 4**<br><br>Protocols Using Public Key Cryptography: Key Transport Protocols: Needham-Schroeder Public Key Protocol, TLS Protocol. Key Agreement Protocols: Key Control, Unknown Key-Share Attacks. | | 6 | 15 |
| **SECOND INTERNAL TEST** | | | |
| **MODULE : 5 -**<br><br>Classes of Key Agreement: Diffie-Hellman Key Agreement, MTI Protocols, Diffie-Hellman-Based Protocols with Basic Message Format: (MQV, Yacobi's) with Enhanced Message Format(Oakley, SKEME,IKE). ID based encryption schemes: Shamir's encryption and signature schemes, Okamoto's scheme, Gunther's scheme, Girault'sscheme.Secret Sharing: Threshold Secret Sharing Schemes, secret sharing based on access structures. | | 12 | 20 |

| | | |
|---|---|---|
| **MODULE : 6** -<br><br>Conference Key Protocols: Generalizing Diffie-Hellman Key Agreement: Ingemarsson<br><br>Tang-Wong Key Agreement, Perrig's Generalised Diffie- Hellman, Becker and Wille's Octopus Protocol.<br><br>Conference Key Agreement Protocols: Authenticated GDH Protocols,<br><br>Conference Key Transport Protocols: Burmester-Desmedt Star and Tree Protocols, Key Broadcasting Protocols. | 12 | 20 |
| END SEMESTER EXAM | | |

| COURSE CODE | COURSE NAME | L-T-P:C | YEAR OF INTRODUCTION |
|---|---|---|---|
| 04 CS 6304 | MOBILE NETWORK SECURITY | 3-0-0:3 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Understand signal encoding techniques, satellite networks, wireless networks security.

**Syllabus**

The syllabus includes signal encoding techniques, satellite networks, vulnerabilities of wireless and wired networks.

**Course Outcome:**

Understand mobile, wireless and satellite networks and security.

**Text Books:**

**References**:


1. KavehPahlavan and PrashantKrishnamurthy,"Principles of Wireless Networks", Prentice -Hall, 2006.
2. Cyrus Peikari and Seth Fogie, "Maximum Wireless Security" Sams, 2002.
3. Hideki lmai, Mohammad GhulamRahman and KazukuniKobari "Wireless Communications Security", Universal Personal Communications of Artech House, 2006.
4. Stallings William, "Wireless Communications and Networks‖ Second Edition, Pearson Education Ltd, 2004.
5. Jon Edney and William A. Arbaugh, " Real 802.11 Security: Wi-Fi Protected Access and 802.11i" , Addison-Wesley Professional, 2003.
6. Wireless and Mobile Network Security: Security Basics, Security in On-the-shelf and Emerging Technologies, HakimaChaouchi, Maryline Laurent-Maknavicius

**COURSE PLAN**

| COURSE CODE: | COURSE TITLE | CREDITS | |
|---|---|---|---|
| 04 CS 6311 | Mobile Network Security | 3-0-0:3 | |
| **MODULES** | | **Contact Hours** | **Sem. Exam Marks (%)** |
| **MODULE 1:**<br>Transmission Fundamentals: Antennas and Wave Propagation. Cellular Wireless networks. Third Generation Systems, 4G Long Term Evolutions | | 6 | 15 |
| **MODULE 2:**<br>Signal Encoding Techniques. Spread Spectrum, Coding and Error Control, Multiple Access in Wireless Systems | | 6 | 15 |
| **INTERNAL TEST 1 (MODULE 1 & 2)** | | | |
| **MODULE 3:**<br>Satellite Networks, Wireless System Operations and Standards, Wi-Max an Ultra Wide Band technologies. | | 6 | 15 |
| **MODULE 4:**<br>Mobile IP and Wireless Access Protocol. Wireless LAN Technology. Wi-Fi and IEEE 802.11 Wireless LAN Standard, Bluetooth and IEEE 802.15 standard. | | 6 | 15 |
| **INTERNAL TEST 2 (MODULE 3 & 4)** | | | |
| **MODULE 5:**<br>Vulnerabilities of wired and wireless Networks, Wireless Attacks, Surveillance, War Driving, Client-to-Client Hacking, Rogue Access Points, Jamming and Denial of Service.<br>Authentication, Encryption/Decryption in GSM, Securing the WLAN, WEP Introduction, RC4 Encryption, Data Analysis, IV Collision, Key Extraction. | | 12 | 20 |
| **MODULE 6:**<br>WEP Cracking, WPA/ WPA2, AES, Access Point-Based Security Measures, Third- Party Security Methods, Funk's Steel-Belted Radius, WLAN Protection Enhancements, Blue-tooth Security Implementation, Security in WiMAX, UWB security, Satellite network security. | | 12 | 20 |
| **END SEMESTER EXAM** | | | |

| COURSE CODE | COURSE NAME | L-T-P:C | YEAR OF INTRODUCTION |
|---|---|---|---|
| 04 CS 6311 | INFORMATION RISK MANAGEMENT | 3-0-0:3 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Understand risk management, security models

**Syllabus**

The syllabus includes risk analysis and management, security models, business continuity management concepts.

**Course Outcome:**

Understand risk management, governance models such as COSO and COBIT ISO 27000

**Text Books:**

**References**:


1. Alan Calder and Steve G. Watkins, "Information Security Risk Management for IS027001 /IS027002", IT Governance Ltd, 2010.
2. Susan Snedaker, "Business Continuity and Disaster Recovery Planning for IT Professionals", Elsevier Science & Technology Books, 2007.
3. Harold F Tipton and Micki Krause, "Information Security Management Handbook", Volume 1, Sixth Edition, Auerbach Publications, 2003.
4. Andreas Von Grebmer, "Information and IT Risk Management in a Nutshell: A Pragmatic Approach to Information Security" Books on Demand, 2008.
5. Evan Wheeler, " Security Risk Management" ,Elsevier, 2011.
6. Ian Tibble,"Security De-Engineering: Solving the Problems in Information Risk Management", CRC Press, 2012.

**COURSE PLAN**

| COURSE CODE: | COURSE TITLE | CREDITS | |
|---|---|---|---|
| 04 CS 6311 | Information Risk Management | 3-0-0:3 | |
| **MODULES** | | **Contact Hours** | **Sem. Exam Marks (%)** |
| **MODULE 1:**<br>Information Risk Management: Definitions and relationships among different security components, threat agent, threat, vulnerability risk, asset, exposure and safeguards | | 6 | 15 |
| **MODULE 2:**<br>Governance models such as COSO and COBIT ISO 27000 series of standards for setting up security programs. | | 6 | 15 |
| **INTERNAL TEST 1 (MODULE 1 & 2)** | | | |
| **MODULE 3:**<br>Risk analysis and management, policies, standards, baselines guidelines and procedures as applied to Security Management program, Information strategy objectives. | | 6 | 15 |
| **MODULE 4:**<br>Security awareness and training. Security Architecture and Design: review of architectural frameworks (such as Zachman and SABSA) | | 6 | 15 |
| **INTERNAL TEST 2 (MODULE 3 & 4)** | | | |
| **MODULE 5:**<br>Concepts of Security Models (such as Bell-LaPadula, Biba and Brewer-Nash) vulnerabilities and threats to information systems (such as traditional on-premise systems, web based multi-tiered applications, distributed systems and cloud based services ) application of countermeasures to mitigate against those threats and security products evaluation | | 12 | 20 |
| **MODULE 6:**<br>Business Continuity and Disaster Recovery: Business Continuity Management (BCM) concepts, Business Impact Analysis, BC/DR Strategy development backup and offsite facilities and types of drills and tests..<br><br>An introduction to Operational Security and Physical security aspects. | | 12 | 20 |
| **END SEMESTER EXAM** | | | |

| COURSE CODE | COURSE NAME | L-T-P:C | YEAR OF INTRODUCTION |
|---|---|---|---|
| 04 CS 6313 | CRYPTOGRAPHY AND NETWORK SECURITY | 3-0-0:3 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Understand attacks, encryption algorithms.
- System and network security.

**Syllabus**

The syllabus includes security attacks, encryption algorithms and network practices, network attacks, intrusion detection systems.

**Course Outcome:**

Familiarize with network security practices and intrusion detection systems.

**Text Books:**

**References**:


1. Cryptography and Network Security - Principles and Practices, William Stallings Prentice-Hall, Fourth edition, Nov 2005.
2. Introduction to cryptography, Johannes A, Buchanan, Springer-Verlag, Second Edition, 2004.
3. Eric Rescorla, —SSL and TLS: Designing and Building Secure Systems‖, Addision-Wesley Professional, 2000.
4. Thomas H. Ptacek and Timothy N. Newsham,‖Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection‖, Secure Networks, Inc., 1988.
5. Proctor Paul, —The practical intrusion detection Handbook‖, Third Edition, Prentice-Hall, Englewood Cliffs, 2001.

**COURSE PLAN**

| COURSE CODE: | COURSE TITLE | CREDITS | |
|---|---|---|---|
| 04 CS 6313 | Cryptography And Network Security | 3-0-0:3 | |
| **MODULES** | | **Contact Hours** | **Sem. Exam Marks (%)** |
| **MODULE 1:**<br>Overview: OSI security architecture - Security Attacks- Security Services. Security Mechanisms. Symmetric Ciphers: Classical Encryption Techniques. | | 6 | 15 |
| **MODULE 2:**<br>Block ciphers and Data Encryption Standards. Public-key Encryption and Hash Functions: Public-Key Cryptography and RSA. | | 6 | 15 |
| **INTERNAL TEST 1 (MODULE 1 & 2)** | | | |
| **MODULE 3:**<br>Network Security Practices: Authentication applications: Kerberos – X.504 Authentication Service – public-key Infrastructure<br><br>Electronic Mail Security: Pretty Good Privacy – S/MIME. | | 6 | 15 |
| **MODULE 4:**<br>Network Security Practices: IP Security: Overview – IP Security Architecture –Authentication Header, Encapsulating Security Payload – Combining Security Associations – Key Management – Web security: Web security considerations SSL and Transport Layer Security | | 6 | 15 |
| **INTERNAL TEST 2 (MODULE 3 & 4)** | | | |
| **MODULE 5:**<br>Intruders: Intrusion Detection – Techniques for network intrusion detection: signature-based and anomaly-based detection, Snort,<br>Password Management –Malicious Software: Virus and related threats – Denial of Service attacks – Firewalls: Firewall design principles Firewalls-packet filters and stateful firewalls, application-aware firewalls - Trusted systems<br>Common Criteria for IT security evaluation System Security: proxies, NAT, Virtual Private Network tunneling, IPSEC VPNs, L2TP, PPP, PPTP, denial of service and distributed denial-of-service | | 12 | 20 |
| **MODULE 6:**<br>(DDoS) attacks, detection and worm and virus propagation, tracing the source of attacks, analysis techniques for hiding the source or destination of network traffic, secure routing protocols, protocol scrubbing and advanced techniques for reacting to network attacks.HTTP authentication, secure DNS, Email spam and its broadcast security, secure multicasting. | | 12 | 20 |
| **END SEMESTER EXAM** | | | |

| COURSE CODE | COURSE NAME | L-T-P:C | YEAR OF INTRODUCTION |
|---|---|---|---|
| 04 CS 6315 | SECURE CODING | 3-0-0:3 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Understand secure coding in java and web applications.
- Threat modeling.

**Syllabus**

The syllabus includes overview of application security and secures programming concepts.

**Course Outcome:**

Understand web application vulnerabilities, threat modeling, software testing methodologies.

**Text Books:**

**References**:


1. Robert C. Seaford, "Secure Coding in C and C++", Addison-Wesley Professional, 2005.
2. James A. Whittaker and Herbert H. Thompson, "How to Break Software Security", Addison Wesley, 2003.
3. John C. Mitchell and Krzysztof Apt, "Concepts in Programming Languages", Cambridge University Press, 2001.

**COURSE PLAN**

| COURSE CODE: | COURSE TITLE | CREDITS | |
|---|---|---|---|
| 04 CS 6315 | Secure Coding | 3-0-0:3 | |
| **MODULES** | | **Contact Hours** | **Sem. Exam Marks (%)** |
| **MODULE 1:**<br>A brief overview of Application Security and Secure Programming concepts. Secure Coding in C and C++. | | 6 | 15 |
| **MODULE 2:**<br>Stack overflow, Strings, Integers, Arrays, File I/O, Race conditions, Signal handling, Recommended Practice. | | 6 | 15 |
| **INTERNAL TEST 1 (MODULE 1 & 2)** | | | |
| **MODULE 3:**<br>Secure Coding in Java and Web Applications-Web as a primary vector for Cyber-attacks, Anatomy of stacks, data breach case studies, Threat modelling. | | 6 | 15 |
| **MODULE 4:**<br>Cross Site Scripting (XSS) vulnerabilities, Injection flaws (SQL, process, path, etc.), Buffer overflows, Resource leaks and resource lifetime management. | | 6 | 15 |
| **INTERNAL TEST 2 (MODULE 3 & 4)** | | | |
| **MODULE 5:**<br>Threat modeling and Security design review, Software Assurance and Testing**,** Software Assurance overview, Testing threat categories, Assessing Risk. | | 12 | 20 |
| **MODULE 6:**<br>Secure Testing Methodologies - Attacking Dependencies<br>Attacking through the User Interface, Attacking Design<br>Attacking implementation, Software engineering practices for development of high assurance code Model Checking, Static Analysis techniques for analyzing software. | | 12 | 20 |
| **END SEMESTER EXAM** | | | |

| COURSE CODE | COURSE NAME | L-T-P-C | YEAR |
|---|---|---|---|
| 04 GN 6001 | RESEARCH METHODOLOGY | 0-2-0:2 | 2015 |

**Pre-requisites:**

**Course Objectives**:

To enable the students:

- To get introduced to research philosophy and processes in general.
- To formulate the research problem and prepare research plan
- To apply various numerical /quantitative techniques for data analysis
- To communicate the research findings effectively

**Syllabus**

Introduction to the Concepts of Research Methodology, Research Proposals, Research Design, Data Collection and Analysis, Quantitative Techniques and Mathematical Modeling, Report Writing.

**Course Outcome:**

Students who successfully complete this course would learn the fundamental concepts of Research Methodology, apply the basic aspects of the Research methodology to formulate a research problem and its plan. They would also be able to deploy numerical/quantitative techniques for data analysis. They would be equipped with good technical writing and presentation skills.

**Text Books:**

1. Research Methodology: Methods and Techniques', by Dr. C. R. Kothari, New Age International Publisher, 2004
2. Research Methodology: A Step by Step Guide for Beginners' by Ranjit Kumar, SAGE Publications Ltd; Third Edition

**References**:

1. Research Methodology: An Introduction for Science & Engineering Students', by Stuart Melville and Wayne Goddard, Juta and Company Ltd, 2004
2. Research Methodology: An Introduction' by Wayne Goddard and Stuart Melville, Juta and Company Ltd, 2004
3. Research Methodology, G.C. Ramamurthy, Dream Tech Press, New Delhi
4. Management Research Methodology' by K. N. Krishnaswamy et al, Pearson Education

| COURSE CODE: | COURSE TITLE | CREDITS | |
|---|---|---|---|
| 04 GN 6001 | RESEARCH METHODOLOGY | 0-2-0: 2 | |
| MODULES | | Contact Hours | |
| MODULE : 1<br>Introduction to Research Methodology: Concepts of Research, Meaning and 2 Objectives of Research, Research Process, Types of Research, Type of research: Descriptive vs. Analytical, Applied vs. Fundamental, Quantitative vs. Qualitative, and Conceptual vs. Empirical | | 5 | |
| MODULE :2<br>Criteria of Good Research, Research Problem, Selection of a problem, Techniques involved in definition of a problem, Research Proposals – Types, contents, Ethical aspects, IPR issues like patenting, copyrights. | | 4 | |
| INTERNAL TEST 1 (MODULE 1 & 2) | | | |
| MODULE: 3<br>**Research Design :** Meaning, Need and Types of research design, Literature Survey and Review, Identifying gap areas from literature review, Research Design Process, Sampling fundamentals, Measurement and scaling techniques, Data Collection – concept, types and methods, Design of Experiments. | | 5 | |
| MODULE 4:<br>**Quantitative Techniques:** Probability distributions, Fundamentals of Statistical analysis, Data Analysis with Statistical Packages, Multivariate methods, Concepts of correlation and regression - Fundamentals of time series analysis and spectral analysis. | | 5 | |
| INTERNAL TEST 2 (MODULE 3 & 4) | | | |
| MODULE: 5<br>**Report Writing:** Principles of Thesis Writing, Guidelines for writing reports & papers, Methods of giving references and appendices, Reproduction of published material, Plagiarism, Citation and acknowledgement. | | 5 | |
| MODULE: 6<br>Documentation and presentation tools – LaTeX, Office with basic presentations skills, Use of Internet and advanced search techniques. | | 4 | |
| | | | |

| COURSE CODE | COURSE NAME | L-T-P:C | YEAR OF INTRODUCTION |
|---|---|---|---|
| 04 CS 6391 | SEMINAR - I | 0-2-2:2 | 2015 |

**Syllabus**

**Course Outcome:**

Each student shall present a seminar on any topic of interest related to the core / elective courses offered in the first semester of the M. Tech. Programme. He / she shall select the topic based on the References: from international journals of repute, preferably IEEE journals. They should get the paper approved by the Programme Co-ordinator / Faculty member in charge of the seminar and shall present it in the class. Every student shall participate in the seminar. The students should undertake a detailed study on the topic and submit a report at the end of the semester. Marks will be awarded based on the topic, presentation, participation in the seminar and the report submitted.

| COURSE CODE | COURSE NAME | L-T-P:C | YEAR OF INTRODUCTION |
|---|---|---|---|
| 04 CS 6393 | INFORMATION SECURITY LAB | 0-0-2:1 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- 

**Syllabus**

**Course Outcome:**

1. Working with Sniffers for monitoring network communication (Ethereal)
2. Understanding of cryptographic algorithms and implementation of the same in C or C++ .
3. Using open ssl for web server - browser communication
4. Using GNU PGP
5. Performance evaluation of various cryptographic algorithms
6. Using IP TABLES on Linux and setting the filtering rules

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 6302 | CYBER CRIME INVESTIGATIONS AND DIGITAL FORENSICS | 3-0-0:3 | 2015 |

**Pre-requisites:** Nil

**Course Objectives**:

- Understand cybercrime.
- Familiarize crime investigation.

**Syllabus**

The syllabus includes overview of cyber crime, its types, investigation and forensics.

**Course Outcome:**

Understand cyber crime issues, recovering digital evidences and forensics.

**Text Books:**

**References**:


1. Nelson Phillips and EnfingerSteuart, “Computer Forensics and Investigations”, Cengage Learning, New Delhi, 2004.
2. Kevin Mandia, Chris Prosise, Matt Pepe, “Incident Response and Computer Forensics “, Tata McGraw -Hill, New Delhi, 2006
3. Robert M Slade,” Software Forensics”, Tata McGraw - Hill, New Delhi, 2005.
4. Bernadette H Schell, Clemens Martin, “Cybercrime”, ABC – CLIO Inc, California, 2004.
5. ”Understanding Forensics in IT “, NIIT Ltd, 2005.

**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS |
|---|---|---|
| 04 CS 6302 | Crime Investigations And Digital Forensics | 3-0-0:3 |

| MODULES | Contact hours | Sem. Exam Marks; % |
|---|---|---|
| **MODULE : 1 –**<br><br>Introduction: Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime Social Engineering, Categories of Cyber Crime, Property Cyber Crime. | 6 | 15 |
| **MODULE : 2 –**<br><br>Cyber Crime Issues: Unauthorized Access to Computers, Computer Intrusions, white collar Crimes, Viruses and Malicious Code Internet Hacking and Cracking, Virus Attacks. | 6 | 15 |
| **FIRST INTERNAL TEST** | | |
| **MODULE : 3 –**<br><br>SoftwarePiracy, Pornography, Intellectual Property, Mail Bombs, Exploitation, Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses. | 6 | 15 |
| **MODULE : 4 –**<br><br>Introduction to Cyber Crime Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation. | 6 | 15 |
| **SECOND INTERNAL TEST** | | |
| **MODULE : 5 –**<br><br>Investigation: E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies. Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking. | 9 | 20 |

| | | |
|---|---|---|
| **MODULE : 6 –**<br><br>Digital Forensics**:** Introduction to Digital Forensics, Forensic Software and Hardware Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition**,** Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics. | 9 | 20 |
| END SEMESTER EXAM | | |

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 6304 | SECURITY THREATS | 3-0-0: 3 | 2015 |

**Pre-requisites:** Nil

**Course Objectives**:

- Familiarize security threats
- Understand threat management.

**Syllabus**

The syllabus includes security threats, types of malware and threat management

**Course Outcome:**

Understand threat modelling, security policies, firewalls, IDS etc.

**Text Books:**

**References**:


6. Joseph M Kizza, —Computer Network Security‖, Springer Verlag, 2005.
7. Swiderski, Frank and Syndex, —Threat Modeling‖, Microsoft Press, 2004.
8. William Stallings and Lawrie Brown, —Computer Security: Principles and Practice‖, Prentice Hall, 2008.
9. Thomas Calabres and Tom Calabrese, —Information Security Intelligence: Cryptographic Principles & Application‖, Thomson Delmar Learning, 2004.

**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS | |
|---|---|---|---|
| 04 CS 6304 | Security Threats | 3-0-0 :3 | |
| **MODULES** | | **Contact hours** | **Sem. Exam Marks; %** |
| **MODULE : 1 - Introduction:**<br><br>Security threats - Sources of security threats- Motives<br>Target Assets and vulnerabilities – Consequences of threats | | 6 | 15 |
| **MODULE : 2 –**<br><br>E-mail threats - Web-threats - Intruders and Hackers, Insider threats, Cyber crimes | | 6 | 15 |
| **FIRST INTERNAL TEST** | | | |
| **MODULE : 3 – Network Threats:**<br><br>Active/ Passive – Interference – Interception Impersonation – Worms – Virus – Spam's – Ad ware - Spy ware – Trojans and covert channels | | 6 | 15 |
| **MODULE : 4–**<br><br>Backdoors – Bots – IP Spoofing - ARP spoofing - Session Hijacking – Sabotage, Internal treats- Environmental threats - Threats to Server security | | 6 | 15 |
| **SECOND INTERNAL TEST** | | | |
| **MODULE : 5– Security Threat Management**:<br><br>Risk Assessment - Forensic Analysis - Security threat correlation – Threat awareness -Vulnerability sources and assessment- Vulnerability assessment tools Threat identification - Threat Analysis - Threat Modeling - Model for Information Security Planning. | | 12 | 20 |
| **MODULE : 6– Security Elements:**<br><br>Authorization and Authentication - types, policies and techniques – Security certification - Security monitoring and Auditing Security Requirements Specifications - Security Policies and Procedures, Firewalls, IDS, Log Files, Honey Pots. Access control, Trusted Computing and multilevel security - Security models, Trusted Systems Software security issues, Physical and infrastructure security, Human factors – Security awareness, training , Email and Internet use policies | | 12 | 20 |
| END SEMESTER EXAM | | | |

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 6306 | ETHICAL HACKING | 3-0-0: 3 | 2015 |

**Pre-requisites:** Nil

**Course Objectives**:

- Introduction to steps in ethical hacking
- Familiarize wireless hacking and remote control insecurities.

**Syllabus**

The syllabus includes detailed description of ethical hacking steps, tools and countermeasures for attacks.

**Course Outcome:**

Students get familiarized with various tools for information gathering, scanning etc. They learn various hacking tools.

**Text Books:**

**References**:


10. Stuart McClure, Joel Scambray and Goerge Kurtz, —Hacking Exposed Network Security Secrets & Solutions‖, Tata Mcgrawhill Publishers, 2010.
11. Bensmith, and Brian Komer, —Microsoft Windows Security Resource Kit‖, Prentice Hall of India, 2010.

**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS |
|---|---|---|
| 04 CS 6306 | Ethical Hacking | 3-0-0:3 |

| MODULES | Contact hours | Sem. Exam Marks; % |
|---|---|---|
| **MODULE : 1 –**<br><br>Casing the Establishment - What is footprinting- Internet Footprinting. - Scanning-Enumeration - basic banner grabbing Enumerating Common Network services. Case study- Network Security Monitoring Securing permission. Securing file and folder permission. Using the encrypting file system. | 6 | 15 |
| **MODULE : 2 –**<br><br>Securing registry permissions. Securing service- Managing service permission. Default services in windows 2000 and windows XP. Unix - The Quest for Root. Remote Access vs Local access. Remote access. Local access. After hacking root. | 6 | 15 |
| **FIRST INTERNAL TEST** | | |
| **MODULE : 3–**<br><br>Dial-up, PBX, Voicemail, and VPN hacking - Preparing to dial up. War-Dialing. Brude-Force Scripting PBX hacking. Voice mail hacking. VPN hacking. | 6 | 15 |
| **MODULE : 4–**<br><br>Network Devices – Discovery, Autonomous System Lookup. Public Newsgroups. Service Detection. Network Vulnerability. Detecting Layer 2 Media | 6 | 15 |
| **SECOND INTERNAL TEST** | | |
| **MODULE : 5–**<br><br>Wireless Hacking - Wireless Foot printing. Wireless Scanning and Enumeration. Gaining Access. Tools that exploiting WEP Weakness. Denial of Services Attacks. Firewalls- Firewalls landscape- Firewall Identification- Scanning Through firewalls- packet Filtering- Application Proxy Vulnerabilities.<br>Denial of Service Attacks - Motivation of Dos Attackers. Types of DoS attacks. Generic Dos Attacks. Unix and Windows DoS. | 9 | 20 |

| | | |
|---|---|---|
| **MODULE : 6–**<br><br>Remote Control Insecurities - Discovering Remote Control Software. Connection. Weakness. VNC. Microsoft Terminal Server and Citrix ICA. Advanced Techniques Session Hijacking. Back Doors. Trojans.<br><br>Cryptography. Subverting the systems Environment. Social Engineering. Web Hacking. Web server hacking web application hacking. Hacking the internet User - Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global Counter measures to Internet User Hacking. | 9 | 20 |
| END SEMESTER EXAM | | |

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 6308 | STORAGE MANAGEMENT AND SECURITY | 3-0-0:3 | 2015 |

**Pre-requisites:** Nil

**Course Objectives**:

- Introduction to distributed storage systems, error management.
- Basics of RAID systems, error management, archival systems

**Syllabus**

The syllabus includes storage networking, storage components, error management, securing the storage Infrastructure.

**Course Outcome:**

Familiarize large storage systems, storage management and security.

**Text Books:**

**References**:


12. EMC Education Services —Information Storage and Management: Storing, Managing, and Protecting Digital Information , John Wiley & Sons, 2010.
13. John Chirillo, ScottBlaul — Storage Security: Protecting SANs, NAS and DAS‖, Wiley, 2003.
14. David Alexander, Amanda French, Dave Sutton —Information Security Management Principles, BCS, The Chartered Institute, 2008.
15. Gerald J. Kowalski, Mark T. Maybury — Information Storage and Retrieval Systems: Theory and Implementation, Springer, 2000.
16. Foster Stockwell, —A history of information storage and retrieval‖ McFarland, 2001.
17. R. Kelly Rainer, Casey G. Cegielski , —Introduction to Information Systems: Enabling and Transforming Business, John Wiley & Sons, 2010.

**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS | |
|---|---|---|---|
| 04 CS 6308 | Storage Management And Security | 3-0-0:3 | |
| **MODULES** | | **Contact hours** | **Sem. Exam Marks; %** |
| **MODULE : 1 –**<br><br>Introduction, History: computing, networking, storage, Need for storage networking SAN, NAS, SAN/NAS Convergence, Distributed Storage Systems. | | 6 | 15 |
| **MODULE : 2 –**<br><br>Mainframe/proprietary vs. open storage, Storage Industry Organizations and Major Vendors Market, Storage networking strategy (SAN/NAS) Technology. | | 6 | 15 |
| **FIRST INTERNAL TEST** | | | |
| **MODULE : 3 –**<br><br>Storage components, Data organization: File vs. Block, Object; Data store; Searchable models; Storage Devices (including fixed content storage devices), File Systems, Volume Managers. | | 6 | 15 |
| **MODULE : 4 –**<br><br>RAID systems, Caches, Prefetching. Error management: Disk Error Management, RAID Error Management, Distributed Systems Error Management. | | 6 | 15 |
| **SECOND INTERNAL TEST** | | | |
| **MODULE : 5 –**<br><br>Large Storage Systems: Google FS/Big Table, Cloud/Web - based systems (Amazon S3), FS+DB convergence, Programming models: Hadoop. *Archival Systems*: Content addressable storage, Backup: server less, LAN free, LAN Replication issues, Storage Security, Storage Management, Device Management, NAS Management<br>Virtualization, Virtualization solutions, SAN Management: Storage Provisioning, Storage Migration. | | 9 | 20 |

| | | |
|---|---|---|
| **MODULE : 6 –**<br><br>Securing the storage Infrastructure, Storage Security Framework, Risk Triad, Storage Security Domains, Security. Implementation in Storage Networking. Managing the Storage Infrastructure. Monitoring the Storage Infrastructure, Storage Management Activities, Developing an Ideal Solution, Concepts in Practice. | 9 | 20 |
| END SEMESTER EXAM | | |

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 6312 | DIGITAL WATERMARKING | 3-0-0:3 | 2015 |

**Pre-requisites:** Nil

**Course Objectives**:

- Introduction to models of watermarking.
- Detecting watermarks.
- Watermark security.

**Syllabus**

The syllabus includes watermarking models, types of watermarking and its security.

**Course Outcome:**

Understanding watermarking models, detection, watermark security and cryptography.

**Text Books:**

**References**:


18. Cox I., M. Miller, J. Bloom, J. Fridrich and T Kalker, "Digit Watermarking and Steganography", Second Edition, Morg Kaufmann Publishers, 2008.
19. E. Cole, R. Krutz, and J. Conley, Network Security Bible, Wiley-Dreamtech, 2005.
20. W. Stallings, Cryptography and Network Security Principles and practice, 3/e, Pearson Education Asia, 2003.
21. C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 3/e, Pearson Education, 2003.
22. M. Bishop, Computer Security: Art and Science, Pearson Education, 2003.

**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS | |
|---|---|---|---|
| 04 CS 6312 | Digital Watermarking | 3-0-0:3 | |
| **MODULES** | | **Contact hours** | **Sem. Exam Marks; %** |
| **MODULE : 1–**<br><br>Watermarking host signals: Image, Video, and Audio. Multimedia compression and decompression, Lossless compression, Models watermarking. | | 6 | 15 |
| **MODULE : 2–**<br><br>Communication-based models of watermarking. Geometric models of watermarking, modelling, watermark detection by correlation. | | 6 | 15 |
| **FIRST INTERNAL TEST** | | | |
| **MODULE : 3–**<br><br>Basic message coding, Mapping message in message vectors, Error correction coding. | | 6 | 15 |
| **MODULE : 4–**<br><br>Detecting multi-symbol watermarks, Watermarking with side information, Inform (embedding, Informed coding). | | 6 | 15 |
| **SECOND INTERNAL TEST** | | | |
| **MODULE : 5–**<br><br>Structured dirty-paper codes, analyzing errors, Message errors, ROC curves The effect of whitening on error rates, Analysis of normalized correlation, Using perceptual mode, Evaluating perceptual impact of watermarks. | | 9 | 20 |
| **MODULE : 6–**<br><br>General forms of perceptual model, Perceptual adaptive watermarking, Robust watermarking, Watermark security, Watermark security and cryptography, Content authentication, Exact authentication, Selective, authentication Localization, Restoration. | | 9 | 20 |
| END SEMESTER EXAM | | | |

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 6314 | DESIGN OF SECURED ARCHITECTURES | 3-0-0:3 | 2015 |

**Pre-requisites:** Nil

**Course Objectives**:

- Introduction to software development cycle
- Learn good coding practices, security architectures.

**Syllabus**

The syllabus covers software architecture and security, various exploits.

**Course Outcome:**

Understand software process and security and familiarize distributed sandbox security, enterprise Security Architecture.

**Text Books:**

**References**:


23. Jay Ramachandran, *"*Designing Security Architecture Solutions*"*, Wiley Computer Publishing, 2010.
24. Markus Schumacher, *"*Security Patterns: Integrating Security and Systems Engineering*"*, Wiley Software Pattern Series, 2010.

**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS | |
|---|---|---|---|
| 04 CS 6314 | Design of Secured Architectures | 3-0-0:3 | |
| **MODULES** | | **Contact hours** | **Sem. Exam Marks; %** |
| **MODULE : 1–**<br><br>Architecture and Security - Architecture Reviews-Software Process-Reviews and the Software Development Cycle-Software Process and Architecture Models-Software Process and Security | | 6 | 15 |
| **MODULE : 2–**<br><br>Architecture Review of System-Security Assessments-Security Architecture Basics- Architecture Patterns in Security Low-Level Architecture - Code Review-importance of code review. | | 6 | 15 |
| **FIRST INTERNAL TEST** | | | |
| **MODULE : 3–**<br><br>Buffer Overflow Exploits- Countermeasures against Buffer Overflow Attacks-patterns applicable- Security and Perl- Byte code Verification in Java-Good Coding Practices Lead to Secure Code- Cryptography- Trusted Code - Secure Communications. | | 6 | 15 |
| **MODULE : 4–**<br><br>Mid-Level Architecture - Middleware Security- Middleware and Security-The Assumption of Infallibility. High-Level Architecture - Security Components- Secure Single Sign-On. | | 6 | 15 |
| **SECOND INTERNAL TEST** | | | |
| **MODULE : 5–**<br><br>Public-Key Infrastructures- Firewalls- Intrusion Detection Systems-LDAP and X.500 Directories- Kerberos- Distributed Computing Environment-The Secure Shell, or SSH-The Distributed Sandbox- Security and Other Architectural Goals- Metrics for Non-Functional Goals-Force Diagrams around Security- High Availability- Robustness- Reconstruction of Events- | | 9 | 20 |

| | | |
|---|---|---|
| Ease of Use- Maintainability, Adaptability, and Evolution- Scalability- Interoperability- Performance- Portability. | | |
| **MODULE : 6–**<br><br>Enterprise Security Architecture **-** Security as a Process-Security Data- Enterprise Security as a Data Management Problem- Tools for Data Management- David Isenberg and the —Stupid Network-Extensible Markup Language- The XML Security Services Signaling Layer-XML and Security Standards- The Security Pattern Catalog Revisited-XML-Enabled Security Data-HGP: A Case Study in Data Management. Business Cases and Security: Building Business Cases for Security. | 9 | 20 |
| END SEMESTER EXAM | | |

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 6316 | BIOMETRIC SECURITY | 3-0-0:3 | 2015 |

**Pre-requisites:** Nil

**Course Objectives**:

- Understand biometric systems, matching methods.
- Familiarize physiological, behavioral and multifactor biometrics.

**Syllabus**

The syllabus includes introduction to biometric systems, various types, strength and weaknesses.

**Course Outcome:**

Understand types of biometric systems and its implementation

**Text Books:**

**References**:


25. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, —Biometrics -Identity verification in a network, Wiley Eastern, 2002.
26. John Chirillo and Scott Blaul,Implementing Biometric Security, Wiley Eastern Publications, 2005.
27. John Berger,Biometrics for Network Security, Prentice Hall, 2004.

**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS |
|---|---|---|
| 04 CS 6316 | Biometric Security | 3-0-0:3 |

| MODULES | Contact hours | Sem. Exam Marks; % |
|---|---|---|
| **MODULE : 1–**<br><br>Biometrics- Introduction- benefits of biometrics over traditional authentication systems benefits of biometrics in identification systems. | 6 | 15 |
| **MODULE : 2 –**<br><br>Selecting a biometric for a system–Applications Key biometric terms and processes biometric matching methods -Accuracy in biometric systems. | 6 | 15 |
| **FIRST INTERNAL TEST** | | |
| **MODULE : 3–**<br><br>Physiological Biometric Technologies: Fingerprints - Technical description – characteristics - Competing technologies - strengths – weaknesses deployment - Facial scan – Technical description - characteristics - weaknesses-deployment. | 6 | 15 |
| **MODULE : 4–**<br><br>Iris scan - Technical description – characteristics - strengths – weaknesses – deployment - Retina vascular pattern – Technical description – characteristics - strengths – weaknesses – deployment - Hand scan – Technical description-characteristics - strengths – weaknesses deployment – DNA biometrics. | 6 | 15 |
| **SECOND INTERNAL TEST** | | |
| **MODULE : 5–**<br><br>Behavioral Biometric Technologies: Handprint Biometrics - DNA Biometrics - signature and handwriting technology - Technical description – classification - keyboard / keystroke dynamics - Voice – data acquisition - feature extraction - characteristics - strengths – weaknesses- deployment. | 9 | 20 |

| | | |
|---|---|---|
| **MODULE : 6–**<br><br>Multi biometrics: Multi biometrics and multi factor biometrics - two- factor authentication with passwords tickets and tokens – executive decision - implementation plan. Case studies on Physiological, Behavioral and multifactor biometrics in identification systems. | 9 | 20 |
| END SEMESTER EXAM | | |

| COURSE CODE | COURSE NAME | L-T-P:C | YEAR OF INTRODUCTION |
|---|---|---|---|
| 04 CS 6318 | PENETRATION TESTING AND VULNERABILITY ASSESSMENT | 3-0-0: 3 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Introduction to ethical hacking.
- Basics of social engineering and network attacks.

**Syllabus**

The syllabus includes hacking stages, information gathering methodologies, scanning and sniffing tools

**Course Outcome:**

Familiarize with hacking methods and its tools.

**References**:

1. Kimberly Graves, "*CEH: Official Certified Ethical Hacker Review Guide*", Wiley Publishing Inc., ISBN: 978-0-7821-4437-6, 2007.
2. Shakeel Ali &TediHeriyanto, "*Backtrack -4: Assuring security by penetration testing*", PACKT Publishing., ISBN: 978-1-849513-94-4, 2011.

**COURSE PLAN**

| COURSE CODE: | COURSE TITLE | CREDITS | |
|---|---|---|---|
| 04 CS 6318 | Penetration Testing And Vulnerability Assessment | 3-0-0: 3 | |
| MODULES | | Contact Hours | Sem. Exam Marks (%) |
| MODULE 1:<br>Introduction :Ethical Hacking terminology- Five stages of hacking | | 6 | 15 |
| MODULE 2:<br>Vulnerability Research , Legal implication of hacking- Impact of hacking | | 6 | 15 |
| INTERNAL TEST 1 (MODULE 1 & 2) | | | |
| MODULE 3:<br>Foot Printing & Social Engineering**:** Information gathering methodologies | | 6 | 15 |
| MODULE 4:<br>Competitive Intelligence, DNS Enumerations- Social Engineering attacks | | 6 | 15 |
| INTERNAL TEST 2 (MODULE 3 & 4) | | | |

| | | |
|---|---|---|
| MODULE 5:<br>Scanning & Enumeration: Port Scanning-Network Scanning Vulnerability Scanning- NMAP scanning tool- OS Fingerprinting- Enumeration | 9 | 20 |
| MODULE 6:<br>Sniffers & Sql Injection: Active and passive sniffing- ARP Poisoning- Session Hijacking- DNS Spoofing Conduct SQL -Injection attack - Countermeasures. | 9 | 20 |
| END SEMESTER EXAM | | |

| COURSE CODE | COURSE NAME | L-T-P:C | YEAR OF INTRODUCTION |
|---|---|---|---|
| **04 CS 6322** | **INTERNET INFORMATION AND APPLICATION SECURITY** | **3-0-0: 3** | **2015** |

**Pre-requisites:**

**Course Objectives**:

- Familiarize web application security
- Understand types of web attack

**Syllabus**

The syllabus includes attacks like SQL injection on web applications and its prevention.

**Course Outcome:**

Secure web applications to prevent attacks and configure firewall to block attacks.

**References**:

1. DafyddStuttard, Marcus Pinto, The Web Application Hacker's Handbook, 2nd Edition, Wiley Publishing, Inc.
2. Justin Clarke, SQL Injection Attacks and Defense, 2004, Syngress Publication Inc.
3. Magnus Mischel ,ModSecurity 2.5, Packt Publishing
4. Stuart McClure Joel, ScambRay, George Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, Seventh Edition, 2012, The McGraw-Hill Companies

**COURSE PLAN**

| COURSE CODE: | COURSE TITLE | CREDITS | |
|---|---|---|---|
| 04 CS 6322 | Internet Information And Application Security | 3-0-0: 3 | |
| MODULES | | Contact Hours | Sem. Exam Marks (%) |
| MODULE 1:<br>Web application security- Key Problem factors – Core defense mechanisms- Handling user access- handling user input<br>Handling attackers – web spidering – Discovering hidden content. Transmitting data via the client – Hidden form fields | | 6 | 15 |
| MODULE 2:<br>HTTP cookies – URL parameters – Handling client-side data securely – Attacking authentication – design flaws in authentication mechanisms<br>securing authentication Attacking access controls – Common vulnerabilities – Securing access controls | | 6 | 15 |
| INTERNAL TEST 1 (MODULE 1 & 2) | | | |
| MODULE 3:<br>SQL Injection - How it happens - Dynamic string building - Insecure Database Configuration - finding SQL injection<br>Exploiting SQL injection – Common techniques – identifying the database – UNION statements – Preventing SQL injection Platform level defenses | | 6 | 15 |
| MODULE 4:<br>Using run time protection - web application Firewalls – Using ModSecurity - Intercepting filters-<br>Web server filters application filters – securing the database – Locking down the application data – Locking down the Database server | | 6 | 15 |
| INTERNAL TEST 2 (MODULE 3 & 4) | | | |
| MODULE 5:<br>Mod Security - Blocking common attacks – HTTP finger printing – Blocking proxies requests – Cross-site scripting<br>Cross-site request forgeries – Shell command execution attempts – Null byte attacks – Source code revelation – Directory traversal attacks<br>Blog spam – Website defacement – Brute force attack – Directory indexing – Detecting the real IP address of an attacker | | 9 | 20 |

| | | |
|---|---|---|
| MODULE 6:<br>Web server Hacking - Source code disclosure – Canonicalization attacks<br>Denial of service Web application hacking – Web crawling Database Hacking<br>Database discovery – Database vulnerabilities | 9 | 20 |
| END SEMESTER EXAM | | |

| COURSE CODE | COURSE NAME | L-T-P:C | YEAR OF INTRODUCTION |
|---|---|---|---|
| 04 CS 6324 | DATABASE SECURITY | 3-0-0: 3 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Understand database concepts, access control and authentication mechanisms.
- Securing databases and information retrieval.

**Syllabus**

The syllabus includes access control mechanisms and different types of authentications.

**Course Outcome:**

Securing database, perform auditing and provide privacy in data publishing.

**References**:


1. Ron Ben Natan, "Implementing Database Security and Auditing", Elsevier, 2005.
2. Hassan A. Afyouni, "Database Security and Auditing: Protecting Data Integrity and Accessibility", Course Technology, 2005.
3. Michael Gertz and SushilJajodia, "Handbook of Database Security-Applications and Trends", Springer, 2008.
4. Database Security, Cengage Learning; 1 edition (July 12, 2011),AlfredBasta . Melissa Zgola
5. Data warehousing and data mining techniques for cyber security, Springer's By AnoopSingha.
6. Carlos Coronel, Steven A. Morris, Peter Rob, "Database Systems: Design, Implementation, and Management", Cengage Learning, 2011.
7. Vijay Atluri, John Hale, "Research Advances in Database and Information Systems Security", Springer, 2000.
8. PierangelaSamarati, Ravi Sandhu," Database Security X: Status and prospects, Volume 10",Springer, 1997

**COURSE PLAN**

| COURSE CODE: | COURSE TITLE | CREDITS | |
|---|---|---|---|
| 04 CS 6324 | Database Security | 3-0-0: 3 | |
| **MODULES** | | **Contact Hours** | **Sem. Exam Marks (%)** |
| MODULE 1:<br>Introduction to databases: database modeling, conceptual database design, overview of SQL and relational algebra. | | 6 | 15 |
| MODULE 2:<br>Access control mechanisms in general computing systems. Lampson's access control matrix. Mandatory access control | | 6 | 15 |
| INTERNAL TEST 1 (MODULE 1 & 2) | | | |
| MODULE 3:<br>Authentication mechanisms in databases, DAC in databases: Griffiths and Wade,MAC mechanisms in databases: SeaView. RBAC in databases | | 6 | 15 |
| MODULE 4:<br>Authentication and password security, Weak authentication options Implementation options, Strong password selection method, Implement account lockout, Password profile. | | 6 | 15 |
| INTERNAL TEST 2 (MODULE 3 & 4) | | | |
| MODULE 5:<br>SQL Injection, Auditing in databases, Statistical inference in databases, Private information retrieval viewed as a database access problem. Privacy in data publishing, Virtual Private Databases, Security of outsourced databases | | 9 | 20 |
| MODULE 6:<br>Securing database to database communication – Monitor and limit outbound communication, Protect link usernames and passwords – Secure replication mechanisms. Trojans- Types of DB Trojans, Monitor for changes to run as privileges, Traces and event monitors.<br>Encrypting data- in transit, Encrypt data-at-rest. Database security auditing categories. | | 9 | 20 |
| END SEMESTER EXAM | | | |

| COURSE CODE | COURSE NAME | L-T-P:C | YEAR OF INTRODUCTION |
|---|---|---|---|
| 04 CS 6326 | CRYPTANALYSIS | 3-0-0: 3 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Various types of cryptanalysis
- Attacks on ciphers.

**Syllabus**

The syllabus includes cryptanalysis of stream ciphers, block ciphers and algorithms for DLP.

**Course Outcome:**

Understand concepts in number theory and perform attacks on various ciphers.

**References**:

1. Antoine Joux, "Algorithmic Cryptanalysis", Chapman & Hall/CRC Cryptography and Series, 2004.

2. Song Y Yang, "Number Theory for Computing", Second Edition,SpringerVerlag, 2010.

3. Gregory V. Bard, "Algebraic Cryptanalysis", Springer, 2004.

4. Hffstein, Jeffray, Pipher, Jill and Silverman, "An Introduction to Mathematical Cryptography", Springer, 2010.

**COURSE PLAN**

| COURSE CODE: | COURSE TITLE | CREDITS | |
|---|---|---|---|
| 04 CS 6326 | Cryptanalysis | 3-0-0:3 | |
| **MODULES** | | **Contact Hours** | **Sem. Exam Marks (%)** |
| MODULE 1:<br>Cryptanalysis of classical ciphers: Vigenere cipher, Affine cipher, Hill-cipher Linear Shift Register Random Bit Generator | | 6 | 15 |
| MODULE 2:<br>Berlekamp- Massey algorithm for the cryptanalysis of LFSR<br>Correlation attack on LFSR based stream ciphers, Cryptanalysis of ORYX, Fast algebraic attack. | | 6 | 15 |
| INTERNAL TEST 1 (MODULE 1 & 2) | | | |
| MODULE 3:<br>Cryptanalysis of Block Ciphers: Man in the middle attack double DES, Linear and Differential cryptanalysis. | | 6 | 15 |
| MODULE 4:<br>Algorithmic Number Theory: Stein's binary greatest common divisor algorithm, Shanks Tonelli algorithm for square roots in Fp, Stein's greatest common divisor algorithm for polynomials | | 6 | 15 |
| INTERNAL TEST 2 (MODULE 3 & 4) | | | |
| MODULE 5:<br>Algorithms for DLP: Pollard Rho method for DLP, Shank's baby step Giant step algorithm for DLP Silver-Pohling-, Hellman algorithm for DLP Index calculus for DLP algorithms: Trial division, Fermat method, Legendre- congruence, Continued fraction method, Pollard Rho method, Elliptic curve method, Quadratic sieve. | | 9 | 20 |
| MODULE 6:<br>Lattice based Cryptanalysis. Direct attacks using lattice reduction, Coppersmith's attacks. Attacks on cryptographic hash functions: Birth day paradox, Birthday for paradox for multi collisions<br>Birthday paradox in two groups, Application of Birthday paradox in Hash functions, Multicollisions attack on hash functions | | 9 | 20 |
| END SEMESTER EXAM | | | |

| COURSE CODE | COURSE NAME | L-T-P:C | YEAR OF INTRODUCTION |
|---|---|---|---|
| 04 CS 6392 | MINI PROJECT | 0-0-4: 2 | 2015 |

**Pre-requisites:**

**Course Objectives**:

The mini project is designed to develop practical ability and knowledge about practical tools/techniques in order to solve the actual problems related to the industry, academic institutions or similar area. Students can take up any application level/system level project pertaining to a relevant domain. Projects can be chosen either from the list provided by the faculty or in the field of interest of the student. For external projects, students should obtain prior permission after submitting the details to the guide and synopsis of the work. The project guide should have a minimum qualification of ME/M.Tech in relevant field of work. At the end of each phase, presentation and demonstration of the project should be conducted, which will be evaluated by a panel of examiners.

**Course Outcome:**

A detailed project report duly approved by the guide in the prescribed format should be submitted by the student for final evaluation. Publishing the work in Conference Proceedings/ Journals with National/ International status with the consent of the guide will carry an additional weightage in the review process.

| COURSE CODE | COURSE NAME | L-T-P:C | YEAR OF INTRODUCTION |
|---|---|---|---|
| 04 CS 6394 | ETHICAL HACKING LAB | 0-0-2:1 | 2015 |

**Pre-requisites:**

**Syllabus:**

Ethical hacking lab includes familiarization of security tools, hacking tools, firewall configuration.

**Course Outcome:**

Familiarize with various types of malware, attacks and its detection and prevention.

1. Working with Trojans, Backdoors and sniffer for monitoring network communication

2. Denial of Service and Session Hijacking using Tear Drop, DDOS attack.

3. Penetration Testing and justification of penetration testing through risk analysis

4. Password guessing and Password Cracking.

5. Wireless Network attacks , Bluetooth attacks

6. Firewalls , Intrusion Detection and Honeypots

7. Malware – Keylogger, Trojans, Keylogger countermeasures

8. Understanding Data Packet Sniffers

9. Windows Hacking – NT LAN Manager, Secure 1 password recovery

10. Implementing Web Data Extractor and Web site watcher.

11. Email Tracking.

12. Configuring Software and Hardware firewall.

13. Firewalls, Packet Analyzers, Filtering methods

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 7301 | DISTRIBUTED AND CLOUD COMPUTING | 3-0-0:3 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Introduction to clustering and virtualization.
- Cloud computing environments

**Syllabus**

The syllabus includes introduction to distributed systems, virtualization and cloud computing environments.

**Course Outcome:**

Understanding applications of cloud environments. Monitoring, management and securing data of cloud.

**References**:


1. Cloud Computing: Principles and Paradigms by RajkumarBuyya, James Broberg and Andrzej M. Goscinski, Wiley, 2011.
2. Distributed and Cloud Computing, Kai Hwang, GeofferyC.Fox, Jack J.Dongarra, Elsevier, 2012.
3. Cloud Computing : A Practical Approach, Anthony T.Velte, Toby J.Velte, Robert Elsenpeter, Tata McGraw Hill, rp2011.
4. Enterprise Cloud Computing, GautamShroff, Cambridge University Press, 2010.
5. Cloud Computing: Implementation, Management and Security, John W. Rittinghouse, James F.Ransome, CRC Press, rp2012.
6. Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, GeorgeReese, O'Reilly, SPD, rp2011.
7. Cloud Security and Privacy: An Enterprise Perspective on Ri Risks and Compliance, Tim Mather,SubraKumaraswamy, ShahedLatif, O'Reilly, SPD, rp2011.

**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS | |
|---|---|---|---|
| 04 CS 7301 | Distributed And Cloud Computing | 3-0-0:3 | |
| MODULES | | Contact hours | Sem. Exam Marks; % |
| **MODULE : 1**<br><br>Systems Modeling, Clustering and Virtualization, Distributed System Models and Enabling Technologies, Computer Clusters for Scalable Parallel Computing, Virtual Machines and Virtualization of Clusters and Data centers | | 6 | 15 |
| **MODULE : 2**<br><br>Introduction to Cloud Computing, Migrating into a Cloud, Enriching the 'Integration as a Service' Paradigm for the Cloud Era , The Enterprise Cloud Computing Paradigm. | | 6 | 15 |
| **FIRST INTERNAL TEST** | | | |
| **MODULE : 3**<br><br>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 | | 6 | 15 |
| **MODULE : 4**<br><br>Enhancing Cloud Computing Environments using a cluster as a Service, Secure Distributed Data Storage in Cloud Computing. Aneka, Comet Cloud, T-Systems | | 6 | 15 |
| **SECOND INTERNAL TEST** | | | |
| **MODULE : 5**<br><br>Workflow Engine for Clouds, Understanding Scientific Applications for Cloud Environments, Monitoring, Management and Applications An Architecture for Federated Cloud Computing, SLA Management in Cloud Computing. | | 9 | 20 |

| | | |
|---|---|---|
| **MODULE : 6**<br><br>Performance Prediction for HPC on Clouds, Best Practices in Architecting Cloud Applications in the AWS cloud, Building Content Delivery networks using Clouds, Resource Cloud Mashups, Data Security in the Cloud. | 9 | 20 |
| END SEMESTER EXAM | | |

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 7303 | WEB SECURITY | 3-0-0:3 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Introduction to web attacks
- Cryptography and web hacking basics

**Syllabus**

The syllabus includes overview of web attacks, web servers and cryptography basics.

**Course Outcome:**

Enable students to design secure web applications, database.

**References**:


1. McClure, Stuart, Saumil Shah, and Shreeraj Shah. Web Hacking:attacks and defense. Addison Wesley. 2003.
2. Garms, Jess and Daniel Somerfield. Professional Java Security.Wrox. 2001.
3. Collection of Cryptography Web Sites, Publications, FAQs, and References: http://world.std.com/~franl/crypto.html
4. FAQ: What is TLS/SSL? http://www.mail.nih.gov/user/faq/tlsssl.htm
5. The Open SSL Project (SDKs for free download): http://www.openssl.org/
6. Windows & .NET security updates Web site: http://www.ntsecurity.net/

**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS | |
|---|---|---|---|
| 04 CS 7303 | Web Security | 3-0-0:3 | |
| **MODULES** | | **Contact hours** | **Sem. Exam Marks; %** |
| **MODULE : 1**<br><br>Introduction- A web security forensic lesson, Web languages Introduction to different web attacks. | | 6 | 15 |
| **MODULE : 2**<br><br>Overview of N-tier web applications, Web Servers: Apache, IIS, Database Servers | | 6 | 15 |
| **FIRST INTERNAL TEST** | | | |
| **MODULE : 3**<br><br>Review of computer security,Public Key cryptography, RSA. | | 6 | 15 |
| **MODULE : 4**<br><br>Review of Cryptography Basics, On-lineShopping, Payment Gateways | | 6 | 15 |
| **SECOND INTERNAL TEST** | | | |
| **MODULE : 5**<br><br>Web Hacking Basics HTTP &HTTPS URL, Web Under the Cover<br><br>Overview of Java security Reading the HTML source, | | 12 | 20 |
| **MODULE : 6**<br><br>Digital Certificates, Hashing, Message Digest, & Digital Signatures<br><br>Basics, Securing databases, Secure JDBC<br><br>Securing Large Applications, Cyber Graffiti | | 12 | 20 |
| END SEMESTER EXAM | | | |

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 7305 | INTRUSION DETECTION AND PREVENTION SYSTEM | 3-0-0:3 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Understanding Intrusion Detection
- Foundations of anomaly detection systems

**Syllabus**

The syllabus includes intrusion detection and prevention basics and architecture and implementation of detection systems.

**Course Outcome:**

Enable students to understand IDS and IPS analysis. To familiarize with the applications and tools.

**References**:


1. Ali A. Ghorbani, Wei Lu, "Network Intrusion Detection and Prevention: Concepts and Techniques", Springer, 2010.
2. Carl Enrolf, Eugene Schultz, Jim Mellander, "Intrusion detection and Prevention", McGraw Hill, 2004
3. Paul E. Proctor, "The Practical Intrusion Detection Handbook ",Prentice Hall , 2001.
4. AnkitFadia and MnuZacharia, "Intrusiion Alert", Vikas Publishing house Pvt., Ltd, 2007.
5. Earl Carter, Jonathan Hogue, "Intrusion Prevention Fundamentals", Pearson Education, 2006.

**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS | |
|---|---|---|---|
| 04 CS 7305 | Intrusion Detection And Prevention System | 3-0-0:3 | |
| **MODULES** | | **Contact hours** | **Sem. Exam Marks; %** |
| **MODULE : 1**<br><br>INTRODUCTION: Understanding Intrusion Detection – Intrusion detection and prevention basics , IDSand IPS analysis schemes | | 6 | 15 |
| **MODULE : 2**<br><br>Attacks, Detection approaches –Misuse detection – anamoly detection – specification based detection – hybrid detection | | 6 | 15 |
| **FIRST INTERNAL TEST** | | | |
| **MODULE : 3**<br><br>Theoretical Foundations Of Detection: Taxonomy of anomaly detection system – fuzzy logic Bayes theory – Artificial Neural networks – Support vector machine – Evolutionary computation –Association rules – Clustering | | 6 | 15 |
| **MODULE : 4**<br><br>Architecture And Implementation: Centralized – Distributed<br><br>Cooperative Intrusion Detection, Tiered architecture | | 6 | 15 |
| **SECOND INTERNAL TEST** | | | |
| **MODULE : 5**<br><br>Justifying Intrusion Detection:Intrusion detection in security – Threat | | 9 | 20 |
| **MODULE : 6**<br><br>Applications And Tools:Tool Selection and Acquisition Process, Bro Intrusion Detection –Prelude Intrusion Detection - Cisco Security IDS - | | 9 | 20 |
| END SEMESTER EXAM | | | |

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 7307 | CLOUD ARCHITECTURES AND SECURITY | 3-0-0:3 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Introduction to cloud computing and types of cloud
- Familiarize developing environments like Amazon.

**Syllabus**

The syllabus includes introduction to cloud computing, cloud and virtualization security.

**Course Outcome:**

Enable students to learn cloud types, deploy web services from cloud.

**References**:


1. GautamShroff, "*Enterprise Cloud Computing Technology ArchitectureApplications",* Cambridge University Press; 1 edition [ISBN: 978-0521137355], 2010.
2. Toby Velte, Anthony Velte, Robert Elsenpeter, "*Cloud Computing, A Practical Approach",* Tata McGraw-Hill Osborne Media; 1 edition 22, [ISBN:0071626948], 2004.
3. Tim Mather, SubraKumaraswamy, ShahedLatif, "*Cloud Security andPrivacy: An Enterprise Perspective on Risks and Compliance",* O'ReillyMedia; 1 edition, [ISBN: 0596802765], 2004.
4. Ronald L. Krutz, Russell Dean Vines, "*Cloud Security",* Wiley [ISBN:0470589876], , 2010

**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS | |
|---|---|---|---|
| 04 CS 7307 | Cloud Architectures And Security | 3-0-0:3 | |
| **MODULES** | | **Contact hours** | **Sem. Exam Marks; %** |
| **MODULE : 1**<br><br>Cloud Computing definition, private, public and hybrid cloud. Cloud types; IaaS, PaaS, SaaS. Benefits and challenges of cloud computing. | | 6 | 15 |
| **MODULE : 2**<br><br>Public vs private cloudsrole of virtualization in enabling the cloud; Business Agility: Benefits and challenges to Cloud architecture | | 6 | 15 |
| **FIRST INTERNAL TEST** | | | |
| **MODULE : 3**<br><br>Technologies and the processes required when deploying web services. Deploying a web service from inside and outside a cloud architecture, advantages and disadvantages | | 6 | 15 |
| **MODULE : 4**<br><br>Development environments for service development; Amazon, Azure, Google App. | | 6 | 15 |
| **SECOND INTERNAL TEST** | | | |
| **MODULE : 5**<br><br>Securing The Cloud, Security Concepts - Confidentiality, privacy, integrity, authentication, nonrepudiation, availability , access control, defence in depth, least privilege- how these concepts apply in the cloud and their importance in PaaS, IaaS and SaaS. e.g. User authentication in the cloud | | 9 | 20 |
| **MODULE : 6**<br><br>Virtualization Security**,**Multi-tenancy Issues: Isolation of users/VMs from each other- How the cloudprovider can provide this**.** Virtualization System Security Issues: e.g. ESX andESXi Security, ESX file system security- storage | | 9 | 20 |

| | | |
|---|---|---|
| considerations<br><br>backup and recovery- Virtualization System Vulnerabilities. Security management in the cloud – security management standards- SaaS, PaaS, IaaS availability management | | |
| END SEMESTER EXAM | | |

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 7304 | MALWARE ANALYSIS | 3-0-0:3 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- To provide an introduction to computer infection programs.
- Basics of virus design and trigger mechanisms

**Syllabus**

The syllabus includes malware fundamentals : life cycle and working principle of certain types of malware.

**Course Outcome:**

Enable students to understand working principle of virus and design shell bash virus under linux

**References**:

1. ErciFiliol, "*Computer Viruses: from theory to applications*", Springer, 1st edition, ISBN 10: 2-287-23939-1, 2005.
2. Mark. A .Ludwig, "*The Giant black book of computer viruses,* Create Space Independent Publishing Platform, 2 nd edition, ISBN 10**:** 144140712X, 2004

**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS | |
|---|---|---|---|
| 04 CS 7304 | Malware Analysis | 3-0-0:3 | |
| **MODULES** | | **Contact hours** | **Sem. Exam Marks; %** |
| **MODULE : 1**<br><br>Introduction:Computer Infection Program- Life cycle of malware Virus nomenclature- Worm nomenclature | | 6 | 15 |
| **MODULE : 2**<br><br>Implementationof Covert Channel:Non self-reproducing Malware- Working | | 6 | 15 |
| **FIRST INTERNAL TEST** | | | |
| **MODULE : 3**<br><br>Implementation of Remote access and file transfer- Working principle of | | 6 | 15 |
| **MODULE : 4**<br><br>Virus Design And Its Implications : Virus components- Function of | | 6 | 15 |
| **SECOND INTERNAL TEST** | | | |
| **MODULE : 5**<br><br>Trigger Mechanisms- Testing virus codes- Case Study: Brute force logical bomb, Malware Design Using Open SourceComputer Virus in Interpreted | | 9 | 20 |
| **MODULE : 6**<br><br>Designing -Shell bash virus under Linux, Fighting over infection- Anti – antiviral fighting, Polymorphism- Case study: Companion virus | | 9 | 20 |
| END SEMESTER EXAM | | | |

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 7311 | FILE SYSTEM FORENSIC ANALYSIS | 3-0-0:3 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Provides introduction to digital investigation process
- Provide the steps in file systems forensics

**Syllabus**

The syllabus includes the fundamentals of digital investigation process, volume analysis and partitions. Also includes FAT 32 and NTFS file systems concepts and analysis.

**Course Outcome:**

Enable students to understand hard disk technology and data recovery for forensic analysis.

**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. Fabry , ACM Transactions on Computer Systems , August 1984, pp 181-197. **http://docs.freebsd.org/44doc/smm/05.fastfs/paper.pdf**
8. The Common Vulnerabilities and Exposures database, entry CVE-2000-0666. **http://cve.mitre.org/**

**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS |
|---|---|---|
| 04 CS 7311 | File System Forensic Analysis | 3-0-0:3 |

| MODULES | Contact hours | Sem. Exam Marks; % |
|---|---|---|
| **MODULE : 1**<br><br>Digital investigation foundation- Digital investigations and evidence, Digital crime scene investigation process, Data analysis, overview of toolkits | 6 | 15 |
| **MODULE : 2**<br><br>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. | 6 | 15 |
| **FIRST INTERNAL TEST** | | |
| **MODULE : 3**<br><br>Volume Analysis- introduction, background, analysis basics, PC based partitions- DOS partitions, Analysis considerations, Apple partitions, | 6 | 15 |
| **MODULE : 4**<br><br>Server based partitions- BSD partitions, Sun Solaris slices, GPT partitions, Multiple disk volumes- RAID, Disk Spanning | 6 | 15 |
| **SECOND INTERNAL TEST** | | |
| **MODULE : 5**<br><br>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 the type Consistency check. FAT data structure- Boot sector, FAT 32 FS info, FAT, Directory entries, Long file name directory entries | 9 | 20 |

| | | |
|---|---|---|
| **MODULE : 6**<br><br>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 | 9 | 20 |
| END SEMESTER EXAM | | |

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 7313 | CLOUD AND UTILITY COMPUTING | 3-0-0:3 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Provide introduction to cloud computing
- Cloud based information systems

**Syllabus**

The syllabus includes introduction to cloud computing, virtualization, software utility applications and architecture.

**Course Outcome:**

Enable students to learn cloud computing technology and its design considerations.

**References**:


1. John W. Rittinghouse and ames F. Ransome, "Cloud Computing Implementation, Management and Security", CRC Press, Taylor & Francis Group, Boca Raton London New York. 2010 [Unit - 11and Unit II]
2. Alfredo Mendoza, "Utility Computing Technologies, Standards, and Strategies", Artech House INC, 2007. [Unit -11I to Unit V]
3. Guy Bunker and Darren Thomson, "Delivering Utility Computing", John Wiley & Sons Ltd, 2006.


**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS | |
|---|---|---|---|
| 04 CS 7313 | CLOUD AND UTILITY COMPUTING | 3-0-0: 3 | |
| MODULES | | Contact hours | Sem. Exam Marks;% |
| **MODULE : 1**<br><br>Introduction to Cloud Computing- The Evolution of Cloud Computing – Hardware Evolution – Internet Software Evolution – Server Virtualization - Web Services Deliver from the Cloud<br><br>Communication-as-a-Service,Infrastructure-as-a-Service,Monitoring as a Service –Platform-as-a-Service – Software-as-a-Service | | 6 | 15 |

| | | |
|---|---|---|
| **MODULE : 2**<br><br>Building Cloud its Relation to Cloud-Based Information Systems Network. Federation in the Cloud- Presence in the Cloud - Privacy and Security in the Cloud - Common Standards in the Cloud – End-User Access to the Cloud Computing | 6 | 15 |
| **FIRST INTERNAL TEST** | | |
| **MODULE : 3**<br><br>Introduction - Advancing towards a Utility Model – Evolving IT infrastructure – Evolving Software Applications – Continuum of Utilities- Standards and Working Groups – Standards Bodies and Working Groups – Service Oriented Architecture – Business Process Execution Language – Interoperability Standards for Data Center Management - Utility Computing Technology | 6 | 15 |
| **MODULE : 4**<br><br>Virtualization – Hyper Threading – Blade Servers - Automated Provisioning - Policy Based Automation – Application Management – Evaluating Utility Management Technology – Virtual Test and development Environment - Data Center Challenges and Solutions - Automating the Data Center | 6 | 15 |
| **SECOND INTERNAL TEST** | | |
| **MODULE : 5**<br><br>Software Utility Application Architecture - Characteristics of an SaaS - Software Utility Applications - Cost Versus Value - Software Application Services Framework Common Enablers – Conceptual view to Reality – Business Profits - Implementing Database Systems for Multitenant Architecture | 9 | 20 |
| **MODULE : 6**<br><br>Other Design Considerations - Design of a Web Services Metering Interface – Application, Monitoring Implementation - A Design for<br><br>an Update and Notification Policy - Transforming to Software as a Service, Application Transformation Program – Business Model Scenarios – Virtual Services for Organizations - The Future | 9 | 20 |
| END SEMESTER EXAM | | |

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 7315 | INTERACTIVE PROGRAMMING WITH PYTHON | 3-0-0:3 | 2015 |

**Pre-requisites:**

**Course Objectives**:

- Enable students to familiarize python
- Basics of python programming and its security applications.

**Syllabus**

The syllabus includes introduction to python language and programming ideas for system security network etc.

**Course Outcome:**

Students should be capable of coding python scripts for web application security, network security etc.

**References**:


1. Mike Dawson,"*More Python programming for Absolute Beginner*", CengageLearning PTR; 3rd edition, ISBN-10: 1435455002, ISBN-13: 978-14354550042, 2010.
2. Mark Lutz," *Python Pocket reference",* O'Reilly Media; 4 thedition ,ISBN-10:0596158084, ISBN-13: 978-0596158088, 2004.


**COURSE PLAN**

| COURSE NO: | COURSE TITLE: | CREDITS | |
|---|---|---|---|
| 04 CS 7315 | Interactive Programming With Python | 3-0-0: 3 | |
| MODULES | | Contact hours | Sem. Exam Marks;% |
| **MODULE : 1**<br><br>Introduction To Python **:** Introduction to Interpreted Languages and Python - Data Types and variables Operators and Expressions - Program Structure and Control | | 6 | 15 |
| **MODULE : 2**<br><br>Functions and Functional Programming - Classes, Objects and other OOPS concepts, System Programming And SecurityI/O in Python<br>File and Directory Access | | 6 | 15 |

| | | |
|---|---|---|
| **FIRST INTERNAL TEST** | | |
| **MODULE : 3**<br><br>System Programming And Security,I/O in Python, File and Directory Access - Multithreading and Concurrency – Inter Process Communication (IPC) - Permissions and Controls | 6 | 15 |
| **MODULE : 4**<br><br>Network Security Programming,Raw Socket basics - Socket Libraries and Functionality, Programming Servers and Clients | 6 | 15 |
| **SECOND INTERNAL TEST** | | |
| **MODULE : 5**<br><br>Programming Wired and Wireless Sniffers, Programming arbitrary packet injectors - PCAP file parsing and analysis, Web Servers and Client scripting - Web Application Fuzzers | 9 | 20 |
| **MODULE : 6**<br><br>Web Application Security **:**Scraping Web Applications<br><br>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. | 9 | 20 |
| END SEMESTER EXAM | | |

| COURSE CODE | COURSE NAME | L-T-P:C | YEAR OF INTRODUCTION |
|---|---|---|---|
| **04 CS 7391** | **SEMINAR 2** | **0-0-2:2** | **2015** |

**Pre-requisites:**

**Course Objectives**:

Each student shall present a seminar on any topic of interest related to the core / elective courses offered in the second semester of the M. Tech. Programme. He / she shall select the topic based on the References: from international journals of repute. They should get the paper approved by the Programme Co-ordinator/ Faculty member in charge of the seminar and shall present it in the class. Every student shall participate in the seminar.

**Course Outcome:**

The students should undertake a detailed study on the topic and submit a report at the end of the semester. Marks will be awarded based on the topic, presentation, participation in the seminar and the report submitted.

| COURSE CODE | COURSE NAME | L-T-P:C | YEAR OF INTRODUCTION |
|---|---|---|---|
| 04 CS 7393 | PROJECT (PHASE 1) | 0-0-8:6 | 2015 |

**Pre-requisites:**

**Course Objectives**:

In Master's Project Phase-I, the students are expected to select an emerging research area in the field of specialization. After conducting a detailed literature survey, they should compare and analyze research work done and review recent developments in the area and prepare an initial design of the work to be carried out as Master's Project. It is mandatory that the students should refer National and International Journals and conference proceedings while selecting a topic for their Project. He/She should select a recent topic from a reputed International Journal, preferably IEEE/ACM. Emphasis should be given for introduction to the topic, literature survey, and scope of the proposed work along with some preliminary work carried out on the Project topic.

**Course Outcome:**

Students should submit a copy of Phase-I Project report covering the content discussed above and highlighting the features of work to be carried out in Phase-II of the Project. The candidate should present the current status of the Project work and the assessment will be made on the basis of the work and the presentation, by a panel of internal examiners in which one will be the internal guide. The examiners should give their suggestions in writing to the students so that it should be incorporated in the Phase–II of the Project.

| COURSE NO. | COURSE TITLE | CREDITS | YEAR |
|---|---|---|---|
| 04 CS 7394 | PROJECT (PHASE 2) | 0-0-21:12 | 2015 |

**Pre-requisites:**

**Course Objectives**:

In the fourth semester, the student has to continue the Project work and after successfully finishing the work, he / she has to submit a detailed bounded Project report. The evaluation of M Tech Project will be carried out by a panel of examiners including at least one external examiner appointed by university and internal examiner

**Course Outcome:**

The work carried out should lead to a publication in a National / International Conference or Journal. The papers received acceptance before the M.Tech evaluation will carry specific weightage.