# MAHATMA GANDHI UNIVERSITY


## SCHEME AND SYLLABI

**FOR**

## M.TECH DEGREE PROGRAMME

**IN**

## COMPUTER SCIENCE AND ENGINEERING

## WITH

## SPECIALIZATION

## IN

## CYBER SECURITY

**(2013 ADMISSION ONWARDS)**

# SCHEME AND SYLLABI FOR M .Tech DEGREE PROGRAMME IN COMPUTER SCIENCE AND ENGINEERING WITH SPECIALIZATION IN CYBER SECURITY

## SEMESTER - I

| SI NO. | Course No. | Subject | Hrs/Week | | | Evaluation Scheme(marks) | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Sessional | | | ESE | Total | Credits ( C ) |
| | | | L | T | P | TA | CT | Sub Total | | | |
| 1 | MCSCB 101# | Mathematical Foundations For Computer Science | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 4 |
| 2 | MCSCB 102* | Advanced Data Structures and Algorithms | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 4 |
| 3 | MCSCB 103 | Operating Systems And Security | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 4 |
| 4 | MCSCB 104 | Cryptographic Protocols and Standards | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 4 |
| 5 | MCSCB 105 | Elective - I | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 3 |
| 6 | MCSCB 106 | Elective - II | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 3 |
| 7 | MCSCB 107 | Information Security Lab | - | - | 3 | 25 | 25 | 50 | 100 | 150 | 2 |
| 8 | MCSCB 108 | Seminar-I | - | - | 2 | 50 | - | 50 | 0 | 50 | 1 |
| | | **Total** | 18 | 4 | 5 | | | 400 | 700 | 1100 | 25 |

**L** – Lecture, **T** – Tutorial, **P** – Practical

| Elective – I (MCSCY 105) | | Elective – II (MCSCY 106) | |
|---|---|---|---|
| MCSCB 105 - 1 | Mobile Network Security | MCSCB 106 - 1 | Information security policies in industries |
| MCSCB 105 - 2 | Cryptography and Network Security | MCSCB 106 – 2 | Information Risk Management |
| MCSCB 105 - 3 | Biometric Security | MCSCB 106 – 3 | Secure Software Engineering |
| MCSCB 105 - 4 | Cyber Law and Legislation | MCSCB 106 – 4 | Secure Coding |

**TA** – Teacher's Assessment (Assignments, attendance, group discussion, Quiz, tutorials, seminars, etc.)
**CT** – Class Test (Minimum of two tests to be conducted by the Institute)
**ESE** – End Semester Examination to be conducted by the University

* – common for MCSCB & MCSCS
# – common for MCSCB & MCSIS

**SEMESTER – II**

| SI NO. | Course No. | Subject | Hrs/Week | | | Evaluation Scheme(marks) | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | Sessional | | | ESE | Total | Credits ( C ) |
| | | | L | T | P | TA | CT | Sub Total | | | |
| 1 | MCSCB 201 | Cyber Forensics | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 4 |
| 2 | MCSCB 202 | Security Threats | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 4 |
| 3 | MCSCB 203 | Ethical Hacking | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 4 |
| 4 | MCSCB 204 | Design of Secured Architectures | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 4 |
| 5 | MCSCB 205 | Elective – III | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 3 |
| 6 | MCSCB 206 | Elective – IV | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 3 |
| 7 | MCSCB 207 | Ethical Hacking Lab | - | - | 3 | 25 | 25 | 50 | 100 | 150 | 2 |
| 8 | MCSCB 208 | Seminar- II | - | - | 2 | 50 | - | 50 | 0 | 50 | 1 |
| | | **Total** | **18** | **4** | **5** | | | **400** | **700** | **1100** | **25** |

**L** – Lecture, **T** – Tutorial, **P** – Practical

| Elective – III (MCSCY 205) | | Elective – IV (MCSCY 206) | |
|---|---|---|---|
| MCSCB 205 -1 | Coding and Information Theory | MCSCB 206 – 1 | Cryptanalysis |
| MCSCB 205 -2 | Storage Management And Security | MCSCB 206 - 2 | Logical Foundations for Access Control |
| MCSCB 205- 3 | Game Theory | MCSCB 206 - 3 | Internet Information and Application Security |
| MCSCB 205 -4 | Digital Watermarking | MCSCB 206 - 4 | Database Security |

**TA** – Teacher's Assessment (Assignments, attendance, group discussion, quiz, tutorials, Seminars, etc.)
**CT –** Class Test (Minimum of two tests to be conducted by the Institute)
**ESE –** End Semester Examination to be conducted by the University

**SEMESTER – III**

| Sl. No | Course No. | Subjects | Hrs/ Week | | | Evaluation Scheme(Marks) | | | | | Credits (C ) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | L | T | P | Sessional | | | ESE | Total | |
| | | | | | | TA | CT | Sub Total | | | |
| 1 | MCSCB 301 | Research Methodology | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 4 |
| 2 | MCSCB 302 | Elective - V | 2 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 3 |
| 3 | MCSCB 303 | Global Elective | 2 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 3 |
| 4 | MCSCB 304 | Master's Thesis Phase - I | 0 | 0 | 20 | 50 | 0 | 50 | 0 | 50 | 5 |
| | | Total | **7** | **3** | **20** | **125** | **75** | **200** | **300** | **500** | **15** |

| **Elective – V (** MCSCY **302)** | |
|---|---|
| MCSCB 302 - 1 | |
| MCSCB 302 - 2 | |
| MCSCB 302 - 3 | |
| MCSCB 302 - 4 | |

| **Global Elective (** MCSCY **303)** | |
|---|---|
| MCSCB 303 | |

# SEMESTER - IV

| Sl. No. | Course No. | Subject | Hrs / Week | | | Evaluation Scheme (Marks) | | | | | Credits (C) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | L | T | P | Sessional Exam (internal) | | | Thesis Evaluation and viva**** | Total | |
| | | | | | | TA*** | CT | Sub Total | | | |
| 1 | MCSCB 401 | Master's Thesis | 0 | 0 | 30 | 100 | 0 | 100 | 100 | 200 | 15 |
| 2 | MCSCB 402 | Master's Comprehensive Viva | | | | | | | 100 | 100 | |
| **Total** | | | | | | | | | | **300** | **15** |
| **Grand Total of four Semesters** | | | | | | | | | | **2750** | Total credits =**80** |

*** 50% of the marks to be awarded by the project guide and the remaining 50% to be awarded by a panel of examiners, including project guide, constituted by the department.

**** Thesis evaluation and Viva-voce will be conducted at end of the fourth semester by a panel of examiners, with at least one external examiner, constituted by the university.

**MCSCB 101#** **MATHEMATICAL FOUNDATIONS FOR COMPUTER SCIENCE**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**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

**Module 2 : Mathematical Preliminaries of Neural Networks:** Linear Algebra – Linear transformation – matrices & operations – eigenvalues and eigenvectors – expectation – covariance matrices – Vector Algebra – Vector spaces – vector products & orthogonality – Cauchy Schwarz Inequality – Cosine similarity – Function continuity and monotonic functions

**Module 3 : Fuzzy Sets:** Crisp sets and Fuzzy sets-, α-cuts, Convex fuzzy sets, Fuzzy cardinality, Algebra of fuzzy sets, 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.

**Module 4 : 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 – Extension Fields - Kronecker's theorem – Galois field
Queuing and Scheduling Models : General concepts, Arrival pattern, service pattern, Queue Disciplines - Queues in Wireless nodes – DropTail, RED, SFQ queuing models[6,7,8,11,12], Case Study : Completely Fair Scheduler in Linux [10,13,14]

**References:**


1. R Bose, “Information Theory, Coding and Cryptography”, TMH 2007
2. Satish Kumar “Neural Networks: A classroom Approach”, The McGraw-Hill Companies.
3. J Gilbert, L Gilbert, “Linear Algebra and Matrix Theory”, Academic Press, Elsevier
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”, 3rd Edition, 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. Robertazzi T.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


**Web References**


11. http://www.isi.edu/nsnam/ns/doc/node69.html
12. https://sites.google.com/a/seecs.edu.pk/network-technologies-tcp-ip-suite/home/performance-analysis-of-impact-of-various-queuing-mechanisms-on-mpeg-traffic/working-mechanism-of-fq-red-sfq-drr-and-drop-tail-queues
13. https://www.kernel.org/doc/Documentation/scheduler/sched-design-CFS.txt
14. http://www.ibm.com/developerworks/library/l-completely-fair-scheduler/

**MCSCB 102*  ADVANCED DATA STRUCTURES AND ALGORITHMS**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module 1:**
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

**Module 2:**
Priority Queues - Single and Double Ended Priority Queues, Leftist Trees, Binomial Heaps, Fibonacci Heaps, Pairing Heaps, Symmetric Min-Max Heaps, Interval Heaps

**Module 3:**
Analysis of Algorithms-review of algorithmic strategies, asymptotic analysis, solving recurrence relations through Substitution Method, Recursion Tree, and Master Method
Dynamic Programming- Rod cutting-top down and bottom up approach, matrix chain multiplication-recursive solution, Longest common subsequence problem

**Module 4:**
Maximum Flow-Flow Networks, Ford-Fulkerson method-analysis of Ford-Fulkerson, Edmonds-Karp algorithm, Maximum bipartite matching
Computational Geometry- Line segment properties, Finding the convex hull **,** Finding the closest pair of points.

**References:**


1. Ellis Horowitz, Sartaj Sahni, Susan Anderson Freed, Fundamentals of Data Structures in C, Second Edition, University Press, 2008
2. Yedidyah Langsam, 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 Sartaj Sahni, Sanguthevar Rajasekaran, 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. Anany Levitin, 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, 2009.
12. Udit Agarwal, Algorithms Design And Analysis, Dhanapat Rai & Co, New Delhi, 2009.
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, Umesh Vazirani, Algorithms, Tata McGraw-Hill Edition.

**MCSCB 103** **OPERATING SYSTEM AND SECURITY**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module 1:** Introduction Operating Systems Concepts – System Calls – OS Organization – Factors in OS Design – Basic Implementation Considerations – Time Sharing and Multi Programming – Real Time Systems. Process Management: Process Concepts, Model – Process Synchronization – Process Scheduling, Threads. Dead Lock: Detection & Recovery, Avoidance, and Prevention- Two Phase Locking Issues.

**Module 2:** Memory Management Basic Memory Management – Swapping – Virtual Memory and demand Paging– Page Replacement Algorithms-Segmentation.

**Module 3:** File System and I/O Management Files – Low Level File Implementations – File system security .Remote file system security.NFS, SMB, SFS, User authentication, Passwords, Biometrics, and Smartcards .Memory Mapped Files – Directories, Implementation – Principles of I/O Hardware & Software – Device Drivers – Disks Hardware, Formatting & Arm Scheduling Algorithms.

**Module 4**: Security and protection in operating systems Secure Operating Systems – access control, auditing, trusted computing base, buffer overflows. Malware analysis and protection: rootkits and their defenses, polymorphic malware, malware capture and analysis such as honeypots. Virtualization technique for security. Intrusion Detection and Virus Protection, TCPA and NGSCB, Digital Rights Management.

**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

**MCSCB 104 CRYPTOGRAPHIC PROTOCOLS AND STANDARDS**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module 1:** Goals for authentication and Key Establishment:
Basic Goals, Enhanced Goals, Goals concerning compromised Keys, Formal Verification of Protocols, Complexity Theoretic Proofs of Security.

**Module 2:** Protocols Using Shared Key Cryptography: Entity Authentication Protocols, Server-Less Key Establishment, Server-Based Key Establishment, Key Establishment Using Multiple Servers, Zero Knowledge interactive proofs.

**Module 3:** Authentication and Key Transport Using Public Key Cryptography: Design Principles for Public Key Protocols, Entity Authentication Protocol, Key Transport Protocols. Key Agreement Protocols: Key Control, Unknown Key-Share Attacks, Classes of Key Agreement: Diffie-Hellman Key Agreement, MTI Protocols, Diffie-Hellman-Based Protocols with Basic Message Format and with Enhanced Message Format. ID based encryption schemes: Boneh and Franklin's Scheme, Shamir's encryption and signature schemes, Okamoto's scheme, Gunther's scheme, Girault's scheme Protocols not Based on Diffie Hellman: SKEME protocol Secret Sharing: Threshold Secret Sharing Schemes, secret sharing based on access structures.

**Module 4:** Conference Key Protocols: Generalizing Diffie-Hellman Key Agreement, Conference Key Agreement Protocols, Identity-Based Conference Key Protocols, Conference Key Agreement without Diffie-Hellman, Conference Key Transport Protocols, Key Broadcasting Protocols

.

**References:**


1. Collin Boyd and Anish Mathuria, "Protocols for Authentication and Key Establishment", Springer; 2010.
2. Abhijith Das and C.E. Veni Madha van, "Public-key Cryptography, Theory and Practice", Pearson Education, 2009.
3. Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996.

**MCSCB 105 - 1** **MOBILE NETWORK SECURITY**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module 1:** Transmission Fundamentals:
Antennas and Wave Propagation. Cellular Wireless networks, Third Generation Systems, 4G Long Term Evolutions, Signal Encoding Techniques, Spread Spectrum, Coding and Error Control, Multiple Access in Wireless Systems.

**Module 2:** Satellite Networks, Wireless System Operations and Standards, Wi-Max an Ultra Wide Band technologies, Mobile IP and Wireless Access Protocol. Wireless LAN Technology, Wi-Fi and IEEE 802.11 Wireless LAN Standard, Blue-tooth and IEEE 802.15 standard.

**Module 3:** Threats to Wireless networks, ESM, ECM and ECCM, Proliferation of device and technologies, Practical aspects, Wireless availability, Privacy Challenges, Risks: Denial of Service, Insertion Attacks, Interception and monitoring wireless traffic, MIS configuration, Wireless Attacks, Surveillance, War Driving, Client-to-Client Hacking, Rogue Access Points, Jamming and Denial of Service.

**Module 4:** Authentication, Encryption/Decryption in GSM, Securing the WLAN, WEP Introduction, RC4 Encryption, Data Analysis, IV Collision, Key Extraction, 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 Wi- MAX, UWB security, Satellite network security.

**References:**


1 Kaveh Pahlavan and Prashant Krishnamurthy,"Principles of Wireless Networks", Prentice - Hall, 2006.
2 Cyrus Peikari and Seth Fogie, "Maximum Wireless Security" Sams, 2002.
3 Hideki lmai, Mohammad Ghulam Rahman and Kazukuni Kobari "Wireless Communications Security", Universal Personal Communications of Artech House, 2006.
4 Stallings William, "Wireless Communications and Networks" Second Edition, Pearson Education Ltd, 2009.
5 Jon Edney and William A. Arbaugh, " Real 802.11 Security: Wi-Fi Protected Access and 802.11i" , Addison-Wesley Professional, 2003.

**MCSCB 105 - 2** **CRYPTOGRAPHY AND NETWORK SECURITY**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module 1:** Overview: OSI security architecture - Security Attacks- Security Services Security Mechanisms. Symmetric Ciphers: Classical Encryption Techniques - Block ciphers and Data Encryption Standards. Public-key Encryption and Hash Functions: Public-Key Cryptography and RSA.

**Module 2:** Network Security Practices: Authentication applications: Kerberos – X.509 Authentication Service – public-key Infrastructure - Electronic Mail Security: Pretty Good Privacy – S/MIME. 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.

**Module 3:** Intruders: Intrusion Detection – Techniques for network intrusion detection: signature-based and anomaly-based detection, Snort, - 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 – Common Criteria for IT security evaluation.

**Module 4:** System Security: proxies, NAT, Virtual Private Network tunneling, IPSEC VPNs, L2TP, PPP, PPTP, denial of service and distributed denial-of-service (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.

**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.

**MCSCB 105 - 3** **BIOMETRIC SECURITY**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module I:** Biometrics- Introduction- benefits of biometrics over traditional authentication systems benefits of biometrics in identification systems-selecting a biometric for a system –Applications – Key biometric terms and processes - biometric matching methods -Accuracy in biometric systems.

**Module II:** Physiological Biometric Technologies: Fingerprints - Technical description – characteristics - Competing technologies - strengths – weaknesses – deployment - Facial scan – Technical description - characteristics - weaknesses-deployment - 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.

**Module III:** 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.

**Module IV:** 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.

**References:**


1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, “Biometrics -Identity verification in a network”, Wiley Eastern, 2002.
2. John Chirillo and Scott Blaul,” Implementing Biometric Security”, Wiley Eastern Publications, 2005.
3. John Berger,” Biometrics for Network Security”, Prentice Hall, 2004.

**MCSCB 105 - 4** **CYBER LAW AND LEGISLATION**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module I:** Introduction to Computer Security: Definition, Threats to security, Government requirements, Information Protection and Access Controls, Computer security efforts, Standards, Computer Security mandates and legislation, Privacy considerations, International security activity.

**Module II:** Secure System Planning and administration, Introduction to the orange book, Security policy requirements, accountability, assurance and documentation requirements, Network Security, The Red book and Government network evaluations.

**Module III:** Information security policies and procedures: Corporate policies- Tier 1, Tier 2 and Tier3 policies - process management-planning and preparation-developing policies-asset classification policy-developing standards.

**Module IV:** Information security: fundamentals-Employee responsibilities- information classification-Information handling- Tools of information security- Information processing-secure program administration. Organizational and Human Security: Adoption of Information Security Management Standards, Human Factors in Security- Role of information security professionals.

**REFERENCES**


1. Debby Russell and Sr. G.T Gangemi, "Computer Security Basics (Paperback)", 2nd Edition, O' Reilly Media, 2006.
2. Thomas R. Peltier, "Information Security policies and procedures: A Practitioner's Reference", 2nd Edition Prentice Hall, 2004.
3. Kenneth J. Knapp, "Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions", IGI Global, 2009.
4. Thomas R Peltier, Justin Peltier and John blackley, "Information Security Fundamentals", 2nd Edition, Prentice Hall, 1996
5. Jonathan Rosenoer, "Cyber law: the Law of the Internet", Springer-verlag, 1997.

**MCSCB 106 - 1 INFORMATION SECURITY POLICIES IN INDUSTRIES**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module I:** Introduction to Information Security Policies – About Policies – why Policies are Important – When policies should be developed – How Policy should be developed - Policy needs – Identify what and from whom it is being protected – Data security consideration – Backups, Archival storage and disposal of data - Intellectual Property rights and Policies – Incident Response and Forensics - Management Responsibilities – Role of Information Security Department – Security Management and Law Enforcement – Security awareness training and support .

**Module II:** Policy Definitions – Standards – Guidelines - Procedures with examples - Policy Key elements - Policy format and Basic Policy Components - Policy content considerations - Program Policy Examples - Business Goal Vs Security Goals - Computer Security Objectives – Mission statement Format – Examples - Key roles in Organization - Business Objectives - Standards – International Standards.

**Module III:** Writing The Security Policies - Computer location and Facility construction – Contingency Planning - Periodic System and Network Configuration Audits - Authentication and Network Security – Addressing and Architecture – Access Control – Login Security – Passwords – User Interface – Telecommuting and Remote Access – Internet Security Policies – Administrative and User Responsibilities – WWW Policies – Application Responsibilities – E-mail Security Policies.

**Module IV:** Establishing Type of Viruses Protection - Rules for handling Third Party Software – User Involvement with Viruses - Legal Issues- Managing Encryption and Encrypted data – Key Generation considerations and Management - Software Development policies -Processes - Testing and Documentation- Revision control and Configuration management - Third Party Development - Intellectual Property Issues

**REFERENCES**


1. Scott Barman, “Writing Information Security Policies”, Sams Publishing, 2002.
2. Thomas.R.Peltier, “Information Policies, Procedures and Standards”, CRC Press, 2004.

**MCSCB 106 - 2** **INFORMATION RISK MANAGEMENT**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module 1:** Information Risk Management: Definitions and relationships among different security components - threat agent, threat, vulnerability, risk, asset, exposure and safeguards; Governance models such as COSO and COBIT, ISO 27000 series of standards for setting up security programs.

**Module 2:** Risk analysis and management, policies, standards, baselines, guidelines and procedures as applied to Security Management program, Information strategy objectives.

**Module 3:** Security awareness and training. Security Architecture and Design: review of architectural frameworks (such as Zachman and SABSA), 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.

**Module 4:** 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. An introduction to Operational Security and Physical security aspects.

**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.

**MCSCB 106 - 3** **SECURE SOFTWARE ENGINEERING**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module I:** Problem, Process, and Product - Problems of software practitioners – approach through software reliability engineering- experience with SRE – SRE process – defining the product – Testing acquired software – reliability concepts- software and hardware reliability. Implementing Operational Profiles - Developing, identifying, crating, reviewing the operation – concurrence rate – occurrence probabilities- applying operation profiles

**Module II:** Engineering "Just Right" Reliability - Defining "failure" for the product - Choosing a common measure for all associated systems. - Setting system failure intensity objectives- Determining user needs for reliability and availability, overall reliability and availability objectives, common failure intensity objective., developed software failure intensity objectives. – Engineering software reliability strategies. Preparing for Test - Preparing test cases. - Planning number of new test cases for current release. -Allocating new test cases. - Distributing new test cases among new operations - Detailing test cases. - Preparing test procedures.

**Module III:** Executing Test - Planning and allocating test time for the current release. - Invoking test-identifying failures - Analyzing test output for deviations. – Determining which deviations are failures. Establishing when failures occurred. Guiding Test - Tracking reliability growth - Estimating failure intensity. - Using failure intensity patterns to guide test – Certifying reliability. Deploying SRE - Core material - Persuading your boss, your coworkers, and stakeholders - Executing the deployment - Using a consultant.

**Module IV:** Using UML for Security - UML diagrams for security requirement -security business process physical security - security critical interaction - security state. Analyzing Model - Notation - formal semantics - security analysis - important security opportunities. Model based security engineering with UML - UML sec profile- Design principles for secure systems – Applying security patterns. Applications - Developing Secure Java program- Tools support for UML Sec - Extending UML CASE TOOLS with analysis tools - Automated tools for UML SEC.

**References:**


1. John Musa D, "Software Reliability Engineering", 2nd Edition, Tata McGraw-Hill, 2005 (Units I, II and III)
2. Jan Jürjens, "Secure Systems Development with UML", Springer; 2004 (Unit IV )

**MCSCB 106 - 4** **SECURE CODING**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module 1:** A brief overview of Application Security and Secure Programming 'concepts. Secure Coding in C and C++, Stack overflow, Strings, 'Integers, Arrays, File I/O, Race conditions, Signal handling, Recommended Practice,

**Module 2:** Secure Coding in Java and Web Applications-Web as a primary vector for Cyber-attacks, Anatomy of stacks, data breach case studies, Threat modeling, Cross Site Scripting (XSS) vulnerabilities, Injection flaws (SQL, process, path, etc.), Buffer overflows, Resource leaks and resource lifetime management, Threat modeling and Security design review,

**Module 3:** Software Assurance and Testing-Software Assurance overview, Testing threat categories, Assessing Risk.

**Module 4:** Secure Testing Methodologies - Attacking Dependencies, Attacking through the User Interface, Attacking Design, Attacking Implementation, Software engineering practices for development of high assurance code, Model Checking, Static Analysis techniques for analyzing software.

**References:**


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

**MCSCB 107** **INFORMATION SECURITY LAB**

| L | T | P | C |
|---|---|---|---|
| 0 | 0 | 3 | 2 |

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

7 Configuring S/MIME for e-mail communication

8 Understanding the buffer overflow and format string attacks

9 Using NMAP for ports monitoring

10 Implementation of proxy based security protocols in C or C++ with features like confidentiality, integrity and authentication

**FOLLOWING ARE SOME OF THE WEB LINKS, WHICH HELP TO SOLVE THE ABOVE ASSIGNMENTS:**

- http://linuxcommand.org/man_pages/openssl1.html
- http://www.openssl.org/docs/apps/openssl.html
- http://www.queen.clara.net/pgp/art3.html
- http://www.ccs.ornl.gov/~hongo/main/resources/contrib/gpg-howto/gpg-howto.html
- https://netfiles.uiuc.edu/ehowes/www/gpg/gpg-com-0.htm
- http://www.ethereal.com/docs/user-guide/

**MCSCB 108** **SEMINAR – I**

| L | T | P | C |
|---|---|---|---|
| 0 | 0 | 2 | 1 |

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.

| MCSCB 201 | CYBER FORENSICS | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 1 | 0 | 4 |

**Module 1:** Cyber forensics
Introduction to Cyber forensics, Type of Computer Forensics Technology- Type of Vendor and Computer Forensics Services. Information Security Investigations, Corporate Cyber Forensics, Scientific method in forensic analysis, investigating large scale Data breach cases, Analyzing Malicious software.

**Module 2:** Ethical Hacking
Essential Terminology, Windows Hacking, Malware, Scanning, Cracking.
Digital Evidence in Criminal Investigations. The Analog and Digital World, Training and Education in digital evidence, the digital crime scene, Investigating Cybercrime, Duties Support Functions and Competencies.
Computer Forensics Evidence and Capture- Data Recovery-Evidence collection and Data Seizure-Duplication and preservation of Digital Evidence-Computer image verification and Authentication

**Module 3:**Investigating Network Intrusions and Cyber Crime, Network Forensics and Investigating logs, Investigating network Traffic, Investigating Web attacks, Router Forensics.
Computer Forensics Analysis- Discovery of Electronic Evidence- Identification of data-Reconstructing Past events- networks

**Module 4:** Countermeasure: Information warfare- Surveillance tool for Information warfare of the future-Advanced Computer Forensics. Cyber forensics tools and case studies.

**References:**


1 Understanding Cryptography: A Textbook for Students and Practitioners: Christof paar, Jan Pelzl.
2 Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts Ali Jahangiri
3 Handbook of Digital and Multimedia Forensic Evidence [Paperback] John J. Barbara
4 Computer Forensics: Investigating Network Intrusions and Cyber Crime (Ec-Council Press Series: Computer Forensics)
5 Cyber Forensics: Understanding Information Security Investigations (Springer's Forensic Laboratory Science Series) by Jennifer Bayuk
6 Information warfare : Information warfare and security: (ACM Press) by Dorothy Elizabeth Robling Denning
7 Cyberwar and Information Warfare : Springer's by Daniel Ventre
8 Computer forensics: computer crime scene investigation, Volume 1 ( Charles River Media, 2008) By John R. Vacca

| MCSCB 202 | SECURITY THREATS | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 1 | 0 | 4 |

**Module I:** Introduction: Security threats - Sources of security threats- Motives - Target Assets and vulnerabilities – Consequences of threats- E-mail threats - Web-threats - Intruders and Hackers, Insider threats, Cyber crimes.

**Module II:** Network Threats: Active/ Passive – Interference – Interception – Impersonation – Worms – Virus – Spam's – Ad ware - Spy ware – Trojans and covert channels – Backdoors – Bots – IP Spoofing - ARP spoofing - Session Hijacking - Sabotage-Internal treats- Environmental threats - Threats to Server security.

**Module III:** Security Threat Management: 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.

**Module IV:** Security Elements: 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.

**REFERENCES**


1. Joseph M Kizza, "Computer Network Security", Springer Verlag, 2005.
2. Swiderski, Frank and Syndex, "Threat Modeling", Microsoft Press, 2004.
3. William Stallings and Lawrie Brown, "Computer Security: Principles and Practice", Prentice Hall, 2008.
4. Thomas Calabres and Tom Calabrese, "Information Security Intelligence: Cryptographic Principles & Application", Thomson Delmar Learning, 2004.

**MCSCB 203** **ETHICAL HACKING**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module I:** 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. 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.

**Module II:** Dial-up ,PBX, Voicemail, and VPN hacking - Preparing to dial up. War-Dialing. Brude-Force Scripting PBX hacking. Voice mail hacking . VPN hacking. Network Devices – Discovery, Autonomous System Lookup. Public Newsgroups. Service Detection. Network Vulnerability. Detecting Layer 2 Media.

**Module III:** 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 . Denial of Service Attacks - Motivation of Dos Attackers. Types of DoS attacks. Generic Dos Attacks. Unix and Windows DoS

**Module IV:** Remote Control Insecurities - Discovering Remote Control Software. Connection. Weakness.VNC . Microsoft Terminal Server and Citrix ICA .Advanced Techniques Session Hijacking. Back Doors. Trojans. 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.

**REFERENCES**:


1. Stuart McClure, Joel Scambray and Goerge Kurtz, “Hacking Exposed Network Security Secrets & Solutions”, Tata Mcgrawhill Publishers, 2010.
2. Bensmith, and Brian Komer, “Microsoft Windows Security Resource Kit”, Prentice Hall of India, 2010.

**MCSCB 204** **DESIGN OF SECURED ARCHITECTURES**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module I:** Architecture and Security - Architecture Reviews-Software Process-Reviews and the Software Development Cycle-Software Process and Architecture Models-Software Process and Security- Architecture Review of System-Security Assessments-Security Architecture Basics-Architecture Patterns in Security.

**Module II:** Low-Level Architecture - Code Review-importance of code review- 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

**Module III:** Mid-Level Architecture - Middleware Security- Middleware and Security- The Assumption of Infallibility. High-Level Architecture - Security Components- Secure Single Sign-On-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- Ease of Use- Maintainability, Adaptability, and Evolution- Scalability- Interoperability- Performance- Portability.

**Module IV:** 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

**REFERENCES**


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

**MCSCB 205-1** **CODING AND INFORMATION THEORY**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module I:** Source Coding - Introduction to information theory, uncertainty and information, average mutual information and entropy, source coding theorem, Shannon-fano coding, Huffman coding, Arithmetic coding, Lempel-Ziv algorithm, run-length encoding and rate distortion function.

**Module II:** Channel capacity and coding - channel models, channel capacity, channel coding, information capacity theorem, random selection of codes. Error control coding: linear block codes and their properties, decoding of linear block code, perfect codes, hamming codes, optimal linear codes and MDS codes.

**Module III:** Cyclic codes - polynomials, division algorithm for polynomials, a method for generating cyclic codes, matrix description of cyclic codes, burst error correction, fire codes,
golay codes, CRC codes, circuit implementation of cyclic codes. BCH codes: minimal polynomials, generator polynomial for BCH codes, decoding of BCH codes, Reed-Solomon codes and nested codes.

**Module IV:** Convolutional codes - tree codes and trellis codes, polynomial description of convolutional codes, distance notions for convolutional codes, generation function, matrix description of convolutional codes, viterbi decoding of convolutional codes, distance bounds for convolutional codes, turbo codes and turbo decoding. Trellis Coded Modulation - concept of coded modulation, mapping by set partitioning, ungerboeck's TCM design rules, TCM decoder, Performance evaluation for Additive White Gaussian Noise (AWGN) channel, TCM for fading channels.

**References:**


1. Lin S. and D. J. Costello, "Error Control Coding — Fundamentals and Applications", Second Edition, Pearson Education Inc., NJ., USA, 2004
2. Shu Lin and Daniel J. Costello, "Error Control Coding", Second Edition, Prentice Hall, 1983.
3. Ranjan Bose, "Information Theory, Coding and Cryptography", Tata McGraw-Hill, 2003.
4. E. R. Berlekamp, "Algebraic Coding Theory", McGraw-Hill, New York, 1968.
5. R. E. Blahut, "Algebraic Codes for Data Transmission", Cambridge University Press Cambridge, UK, 2003.
6. Ranjan Bose, "Information theory, coding and cryptography", Tata McGraw Hill, 2002.
7. Viterbi, "Information theory and coding", McGraw Hill, 1982.
8. John G. Proakis, "Digital Communications", 2nd Edition, McGraw Hill, 1989.

**MCSCB 205-2** **STORAGE MANAGEMENT AND SECURITY**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module 1:** Introduction, History: computing, networking, storage, Need for storage networking , SAN, NAS, SAN/NAS Convergence, Distributed Storage Systems, Mainframe/proprietary vs. open storage, Storage Industry Organizations and Major Vendors Market, Storage networking strategy (SAN/NAS) Technology

**Module 2:** Storage components, Data organization: File vs. Block, Object; Data store; Searchable models; Storage Devices (including fixed content storage devices), File Systems, Volume Managers, RAID systems, Caches, Prefetching. Error management: Disk Error Management, RAID Error Management, Distributed Systems Error Management.

**Module 3:** 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, Virtualization, Virtualization solutions, SAN Management: Storage Provisioning, Storage Migration

**Module 4:** 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.

**References:**


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

**MCSCB 205-3** **GAME THEORY**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module I:** Fundamentals: Conflict, Strategy and Games, Game theory, The Prisoner's Dilemma, Scientific metaphor, Business case, Games in normal and extensive forms – Representation, Examination, Examples.

**Module II:** Non Cooperative Equilibrium in Normal Games: Dominant Strategies and Social Dilemmas, Nash Equilibrium, Classical Cases in Game theory, Three person games, Introduction to Probability and Game theory, N-Person games.

**Module III:** Cooperative Solutions: Elements of Cooperative Games- Credible commitment, A Real Estate Development, Solution Set, Some Political Coalitions, Applications of the Core to Economics – The Market Game, The Core of a Two Person Exchange Game, The Core with More than Two Pairs of Traders, The core of Public Goods Contribution Game, Monopoly and Regulation .

**Module IV:** Sequential Games: Strategic Investment to Deter Entry, The Spanish Rebellion, Again, Imbedded Games – Planning Doctoral Study, Centipede Solved, Repeated play- Campers Dilemma, Pressing the shirts, Indefinitely Repeated Play – A Repeated Effort Dilemma, The Discount Factor. Applications: Voting Games, Games and Experiments, Auctions, Evolution and Boundary Rational Learning.

**REFERENCES**


1. Roger A. McCain, "Game Theory – A Non-Technical Introduction to the Analysis of Strategy", Thomson South-Western, 2005.
2. Tirole, "Game Theory", Mit press 2005.
3. Osborne, "An Introduction to Game Theory", Oxford Press 2006.
4. E. N. Barron, "Game Theory: An Introduction", Wiley India Pvt Ltd, 2009.

**MCSCB 205-4** **DIGITAL WATERMARKING**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module 1:** Watermarking host signals: Image, Video, and Audio. Multimedia compression and decompression, Lossless compression, Models watermarking, Communication-based models of watermarking, Geometric models of watermarking, modeling watermark detection by correlation

**Module 2:** Basic message coding, Mapping message in message vectors, Error correction coding, Detecting multi-symbol watermarks, Watermarking with side information, Inform( embedding, Informed coding.

**Module 3:** 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.

**Module 4:** General forms of perceptual model, Perceptual adaptive watermarking, Robust watermarking, Watermark security, Watermark security and cryptography, Content authentication, Exact authentication, Selective, authentication, Localization, Restoration.

**References:**


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

**MCSCB 206-1** **CRYPTANALYSIS**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module 1:** Cryptanalysis of classical ciphers: Vigenere cipher, Affine cipher, Hill-cipher Linear Shift Register Random Bit Generator: Berlekamp- Massey algorithm for the cryptanalysis of LFSR, Correlation attack on LFSR based stream ciphers, Cryptanalysis of ORYX, Fast algebraic attack.

**Module 2:** Cryptanalysis of Block Ciphers: Man in the middle attack double DES, Linear and Differential cryptanalysis. 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.

**Module 3:** 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.

**Module 4:** 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, Birthday paradox in two groups, Application of Birthday paradox in Hash functions, Multicollisions attack on hash functions.

**References:**


1. Antoine Joux, "Algorithmic Cryptanalysis", Chapman & Hall/CRC Cryptography and Series, 2009.
2. Song Y Yang, "Number Theory for Computing", Second Edition,SpringerVerlag, 2010.
3. Gregory V. Bard, "Algebraic Cryptanalysis", Springer, 2009.
4. Hffstein, Jeffray, Pipher, Jill and Silverman, "An Introduction to Mathematical Cryptography", Springer, 2010.

**MCSCB 206-2 LOGICAL FOUNDATIONS FOR ACCESS CONTROL**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module 1:** Mathematical Logic: Mathematical systems, Propositions and connectives, Statement formulae and truth tables, Logic variables, Logic Functions, Logic expressions, Equivalences of Logic functions, complete sets of logic functions.

**Module 2:** Propositional & Predicate Calculus: Propositional and Predicate Calculus: Language of Propositional and Predicate Logic - Logic Programming, Formulas, Models,

**Module 3:** Normal Forms— CNF, DNF, SNF, PNF, Satisfiability, consequences and Interpretations, Tableaux, Resolution, Soundness and completeness of Tableaux and Resolution, Semantic Tableaux complete Systematic Tableaux, Decision Methods, Security Models:Biba, Bell LaPadula, Chinese wall, Lattice model, SPKI/SDSI –PKIin first order logic, security of distributed systems using Datalog with constraints,

**Module 4:** Executional specification of security policies in a logic programming framework, Delegation logic, trust management systems, Case studies of specific logic programming models for distributed systems security such as SD3, SecPAL, RT etc.

**References:**


1. John W Lloyd, "Foundations of Logic Programming (Symbolic E Artificial Intelligence)", Springer, 1993
2. J. W Lloyd and John Lloyd, 'Logic and Learning: Knowledge -tation, Computation and Learning in Higher-order Logic", ES—L'11 Heidelberg, 2003.
3. Mordechai Ben-Ad, "Mathematical Logic for Computer Science", B". on, Springer International Edition, 2008.
4. George Matakides and Anil Nerode, "Principles of Logic and Logic — North Holland, 1996.
5. Alessandro Aldini, Gilles Barthe, Roberto Gorrieri, " Foundations of Security Analysis and Design V, Volume 5,Springer, 2009.

**MCSCB 206-3** **Internet Information and Application Security**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module 1:** Web application security- Key Problem factors – Core defense mechanisms- Handling user access- handling user input- Handling attackers – web spidering – Discovering hidden content. Transmitting data via the client – Hidden form fields – HTTP cookies – URL parameters – Handling client-side data securely – Attacking authentication – design flaws in authentication mechanisms –securing authentication Attacking access controls – Common vulnerabilities – Securing access controls

**Module 2:** SQL Injection - How it happens - Dynamic string building - Insecure Database Configuration - finding SQL injection – Exploiting SQL injection – Common techniques – identifying the database – UNION statements – Preventing SQL injection Platform level defenses - Using run time protection - web application Firewalls – Using ModSecurity - Intercepting filters- Web server filters - application filters – securing the database – Locking down the application data – Locking down the Database server

**Module3:** Mod Security - Blocking common attacks – HTTP finger printing – Blocking proxies requests – Cross-site scripting – Cross-site request forgeries – Shell command execution attempts – Null byte attacks – Source code revelation – Directory traversal attacks – Blog spam – Website defacement – Brute force attack – Directory indexing – Detecting the real IP address of an attacker

**Module 4:** Web server Hacking - Source code disclosure – Canonicalization attacks – Denial of service – Web application hacking – Web crawling Database Hacking – Database discovery – Database vulnerabilities

**References:**


1. Dafydd Stuttard, Marcus Pinto, The Web Application Hacker's Handbook, 2nd Edition, Wiley Publishing, Inc.
2. Justin Clarke, SQL Injection Attacks and Defense, 2009, 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

**MCSCB 206-4** **DATABASE SECURITY**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module 1:** Introduction to databases: database modeling, conceptual database design, overview of SQL and relational algebra, Access control mechanisms in general computing systems: Lampson's access control matrix. Mandatory access control.

**Module 2:** Authentication mechanisms in databases, DAC in databases: Griffiths and Wade, MAC mechanisms in databases: SeaView. RBAC in databases. Authentication and password security – Weak authentication options, Implementation options, Strong password selection method, Implement account lockout, Password profile.

**Module 3:** 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.

**Module 4:** 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. Encrypting data- in transit, Encrypt data-at-rest. Database security auditing categories.

**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 Sushil Jajodia, "Handbook of Database Security-Applications and Trends", Springer, 2008.
4. Database Security, Cengage Learning; 1 edition (July 12, 2011),Alfred Basta . Melissa Zgola
5. Data warehousing and data mining techniques for cyber security, Springer's By Anoop Singha.
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. Pierangela Samarati, Ravi Sandhu," Database Security X: Status and prospects, Volume 10",Springer, 1997.

**MCSCB 207** **ETHICAL HACKING LAB**

| L | T | P | C |
|---|---|---|---|
| 0 | 0 | 3 | 2 |

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.

**MCSCB 208** **SEMINAR - II**

| L | T | P | C |
|---|---|---|---|
| 0 | 0 | 2 | 1 |

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, 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.

# MAHATMA GANDHI UNIVERSITY

## SCHEME AND SYLLABI

**FOR**

## M.TECH DEGREE PROGRAMME

**IN**

## COMPUTER SCIENCE AND ENGINEERING

## WITH SPECIALIZATION

## IN

## CYBER SECURITY

**(2013 ADMISSION ONWARDS)**

# SCHEME AND SYLLABI FOR M .Tech DEGREE PROGRAMME IN COMPUTER SCIENCE AND ENGINEERING WITHSPECIALIZATION IN CYBER SECURITY

## SEMESTER – II

| SI NO. | Course No. | Subject | Hrs/Week | | | Evaluation Scheme(marks) | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | L | T | P | Sessional | | | ESE | Total | Credits ( C ) |
| | | | | | | TA | CT | Sub Total | | | |
| 1 | MCSCB 201 | Cyber Forensics | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 4 |
| 2 | MCSCB 202 | Security Threats | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 4 |
| 3 | MCSCB 203 | Ethical Hacking | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 4 |
| 4 | MCSCB 204 | Design of Secured Architectures | 3 | 1 | 0 | 25 | 25 | 50 | 100 | 150 | 4 |
| 5 | MCSCB 205 | Elective – III | 3 | 0 | 0 | 25 | 25 | 50 | 100 | 150 | 3 |
| 6 | MCSCB 206 | Elective – IV | 3 | 0 | 0 | 25 | 25 | 50 | 100 | 150 | 3 |
| 7 | MCSCB 207 | Ethical Hacking Lab | - | - | 3 | 25 | 25 | 50 | 100 | 150 | 2 |
| 8 | MCSCB 208 | Seminar- II | - | - | 2 | 50 | - | 50 | 0 | 50 | 1 |
| **Total** | | | **18** | **4** | **5** | **225** | **175** | **400** | **700** | **1100** | **25** |

**L** – Lecture, **T** – Tutorial, **P** – Practical

| Elective – III (MCSCB 205) | | Elective – IV (MCSCB 206) | |
|---|---|---|---|
| MCSCB 205 -1 | Coding and Information Theory | MCSCB 206 – 1 | Cryptanalysis |
| MCSCB 205 -2 | Storage Management And Security | MCSCB 206 - 2 | Logical Foundations for Access Control |
| MCSCB 205- 3 | Internet Information and Application Security | MCSCB 206 - 3 | Game Theory |
| MCSCB 205 -4 | Digital Watermarking | MCSCB 206 - 4 | Database Security |

**TA** – Teacher's Assessment (Assignments, attendance, group discussion, quiz, tutorials, Seminars, etc.)
**CT** – Class Test (Minimum of two tests to be conducted by the Institute)
**ESE** – End Semester Examination to be conducted by the University

**MCSCB 201** **CYBER FORENSICS**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module 1:** Cyber forensics
Introduction to Cyber forensics, Type of Computer Forensics Technology- Type of Vendor and Computer Forensics Services. Information Security Investigations, Corporate Cyber Forensics, Scientific method in forensic analysis, investigating large scale Data breach cases, Analyzing Malicious software.

**Module 2:** Ethical Hacking
Essential Terminology, Windows Hacking, Malware, Scanning, Cracking.
Digital Evidence in Criminal Investigations. The Analog and Digital World, Training and Education in digital evidence, the digital crime scene, Investigating Cybercrime, Duties Support Functions and Competencies.
Computer Forensics Evidence and Capture- Data Recovery-Evidence collection and Data Seizure-Duplication and preservation of Digital Evidence-Computer image verification and Authentication

**Module 3:**Investigating Network Intrusions and Cyber Crime, Network Forensics and Investigating logs, Investigating network Traffic, Investigating Web attacks, Router Forensics.
Computer Forensics Analysis- Discovery of Electronic Evidence- Identification of data- Reconstructing Past events- networks

**Module 4:** Countermeasure: Information warfare- Surveillance tool for Information warfare of the future-Advanced Computer Forensics. Cyber forensics tools and case studies.

**References:**


1 Understanding Cryptography: A Textbook for Students and Practitioners: Christof paar, Jan Pelzl.
2 Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts Ali Jahangiri
3 Handbook of Digital and Multimedia Forensic Evidence [Paperback] John J. Barbara
4 Computer Forensics: Investigating Network Intrusions and Cyber Crime (Ec-Council Press Series: Computer Forensics)
5 Cyber Forensics: Understanding Information Security Investigations (Springer's Forensic Laboratory Science Series) by Jennifer Bayuk
6 Information warfare : Information warfare and security: (ACM Press) by Dorothy
Elizabeth Robling Denning
7 Cyberwar and Information Warfare : Springer's by Daniel Ventre
8 Computer forensics: computer crime scene investigation, Volume 1 ( Charles River Media, 2008) By John R. Vacca

**MCSCB 202** **SECURITY THREATS**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module I:** Introduction: Security threats - Sources of security threats- Motives - Target Assets and vulnerabilities – Consequences of threats- E-mail threats - Web-threats - Intruders and Hackers, Insider threats, Cyber crimes.

**Module II:** Network Threats: Active/ Passive – Interference – Interception – Impersonation – Worms – Virus – Spam's – Ad ware - Spy ware – Trojans and covert channels – Backdoors – Bots – IP Spoofing - ARP spoofing - Session Hijacking - Sabotage-Internal treats- Environmental threats - Threats to Server security.

**Module III:** Security Threat Management: 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.

**Module IV:** Security Elements: 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.

**REFERENCES**


1. Joseph M Kizza, "Computer Network Security", Springer Verlag, 2005.
2. Swiderski, Frank and Syndex, "Threat Modeling", Microsoft Press, 2004.
3. William Stallings and Lawrie Brown, "Computer Security: Principles and Practice", Prentice Hall, 2008.
4. Thomas Calabres and Tom Calabrese, "Information Security Intelligence: Cryptographic Principles & Application", Thomson Delmar Learning, 2004.

**MCSCB 203** **ETHICAL HACKING**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module I:** 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. 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.

**Module II:** Dial-up ,PBX, Voicemail, and VPN hacking - Preparing to dial up. War-Dialing. Brude-Force Scripting PBX hacking. Voice mail hacking . VPN hacking. Network Devices – Discovery, Autonomous System Lookup. Public Newsgroups. Service Detection. Network Vulnerability. Detecting Layer 2 Media.

**Module III:** 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 . Denial of Service Attacks - Motivation of Dos Attackers. Types of DoS attacks. Generic Dos Attacks. Unix and Windows DoS

**Module IV:** Remote Control Insecurities - Discovering Remote Control Software. Connection. Weakness.VNC . Microsoft Terminal Server and Citrix ICA .Advanced Techniques Session Hijacking. Back Doors. Trojans. 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.

**REFERENCES**:


1. Stuart McClure, Joel Scambray and Goerge Kurtz, “Hacking Exposed Network Security Secrets & Solutions”, Tata Mcgrawhill Publishers, 2010.
2. Bensmith, and Brian Komer, “Microsoft Windows Security Resource Kit”, Prentice Hall of India, 2010.

**MCSCB 204** **DESIGN OF SECURED ARCHITECTURES**

| L | T | P | C |
|---|---|---|---|
| 3 | 1 | 0 | 4 |

**Module I:** Architecture and Security - Architecture Reviews-Software Process-Reviews and the Software Development Cycle-Software Process and Architecture Models-Software Process and Security- Architecture Review of System-Security Assessments-Security Architecture Basics- Architecture Patterns in Security.

**Module II:** Low-Level Architecture - Code Review-importance of code review- 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

**Module III:** Mid-Level Architecture - Middleware Security- Middleware and Security- The Assumption of Infallibility. High-Level Architecture - Security Components- Secure Single Sign-On- 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- Ease of Use- Maintainability, Adaptability, and Evolution-Scalability- Interoperability- Performance- Portability.

**Module IV:** 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

**REFERENCES**


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

**MCSCB 205-1** **CODING AND INFORMATION THEORY**

| L | T | P | C |
|---|---|---|---|
| 3 | 0 | 0 | 3 |

**Module I:** Source Coding - Introduction to information theory, uncertainty and information, average mutual information and entropy, source coding theorem, Shannon-fano coding, Huffman coding, Arithmetic coding, Lempel-Ziv algorithm, run-length encoding and rate distortion function.

**Module II:** Channel capacity and coding - channel models, channel capacity, channel coding, information capacity theorem, random selection of codes. Error control coding: linear block codes and their properties, decoding of linear block code, perfect codes, hamming codes, optimal linear codes and MDS codes.

**Module III:** Cyclic codes - polynomials, division algorithm for polynomials, a method for generating cyclic codes, matrix description of cyclic codes, burst error correction, fire codes, golay codes, CRC codes, circuit implementation of cyclic codes. BCH codes: minimal polynomials, generator polynomial for BCH codes, decoding of BCH codes, Reed-Solomon codes and nested codes.

**Module IV:** Convolutional codes - tree codes and trellis codes, polynomial description of convolutional codes, distance notions for convolutional codes, generation function, matrix description of convolutional codes, viterbi decoding of convolutional codes, distance bounds for convolutional codes, turbo codes and turbo decoding. Trellis Coded Modulation - concept of coded modulation, mapping by set partitioning, ungerboeck's TCM design rules, TCM decoder, Performance evaluation for Additive White Gaussian Noise (AWGN) channel, TCM for fading channels.

**References:**


1. Lin S. and D. J. Costello, "Error Control Coding — Fundamentals and Applications", Second Edition, Pearson Education Inc., NJ., USA, 2004
2. Shu Lin and Daniel J. Costello, "Error Control Coding", Second Edition, Prentice Hall, 1983.
3. Ranjan Bose, "Information Theory, Coding and Cryptography", Tata McGraw-Hill, 2003.
4. E. R. Berlekamp, "Algebraic Coding Theory", McGraw-Hill, New York, 1968.
5. R. E. Blahut, "Algebraic Codes for Data Transmission", Cambridge University Press Cambridge, UK, 2003.
6. Ranjan Bose, "Information theory, coding and cryptography", Tata McGraw Hill, 2002.
7. Viterbi, "Information theory and coding", McGraw Hill, 1982.
8. John G. Proakis, "Digital Communications", 2nd Edition, McGraw Hill, 1989.

**MCSCB 205-2** **STORAGE MANAGEMENT AND SECURITY**

| L | T | P | C |
|---|---|---|---|
| 3 | 0 | 0 | 3 |

**Module 1:** Introduction, History: computing, networking, storage, Need for storage networking , SAN, NAS, SAN/NAS Convergence, Distributed Storage Systems, Mainframe/proprietary vs. open storage, Storage Industry Organizations and Major Vendors Market, Storage networking strategy (SAN/NAS) Technology

**Module 2:** Storage components, Data organization: File vs. Block, Object; Data store; Searchable models; Storage Devices (including fixed content storage devices), File Systems, Volume Managers, RAID systems, Caches, Prefetching. Error management: Disk Error Management, RAID Error Management, Distributed Systems Error Management.

**Module 3:** 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, Virtualization, Virtualization solutions, SAN Management: Storage Provisioning, Storage Migration

**Module 4:** 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.

**References:**


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

**MCSCB 205-3** **Internet Information and Application Security**

| L | T | P | C |
|---|---|---|---|
| 3 | 0 | 0 | 4 |

**Module 1:** Web application security- Key Problem factors – Core defense mechanisms- Handling user access- handling user input- Handling attackers – web spidering – Discovering hidden content. Transmitting data via the client – Hidden form fields – HTTP cookies – URL parameters – Handling client-side data securely – Attacking authentication – design flaws in authentication mechanisms –securing authentication Attacking access controls – Common vulnerabilities – Securing access controls

**Module 2:** SQL Injection - How it happens - Dynamic string building - Insecure Database Configuration - finding SQL injection – Exploiting SQL injection – Common techniques – identifying the database – UNION statements – Preventing SQL injection Platform level defenses - Using run time protection - web application Firewalls – Using ModSecurity - Intercepting filters- Web server filters - application filters – securing the database – Locking down the application data – Locking down the Database server

**Module3:** Mod Security - Blocking common attacks – HTTP finger printing – Blocking proxies requests – Cross-site scripting – Cross-site request forgeries – Shell command execution attempts – Null byte attacks – Source code revelation – Directory traversal attacks – Blog spam – Website defacement – Brute force attack – Directory indexing – Detecting the real IP address of an attacker

**Module 4:** Web server Hacking - Source code disclosure – Canonicalization attacks – Denial of service – Web application hacking – Web crawling Database Hacking – Database discovery – Database vulnerabilities

**References:**


1. Dafydd Stuttard, Marcus Pinto, The Web Application Hacker’s Handbook, 2nd Edition, Wiley Publishing, Inc.
2. Justin Clarke, SQL Injection Attacks and Defense, 2009, 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

**MCSCB 205-4** **DIGITAL WATERMARKING**

| L | T | P | C |
|---|---|---|---|
| 3 | 0 | 0 | 3 |

**Module 1:** Watermarking host signals: Image, Video, and Audio. Multimedia compression and decompression, Lossless compression, Models watermarking, Communication-based models of watermarking, Geometric models of watermarking, modeling watermark detection by correlation

**Module 2:** Basic message coding, Mapping message in message vectors, Error correction coding, Detecting multi-symbol watermarks, Watermarking with side information, Inform( embedding, Informed coding.

**Module 3:** 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.

**Module 4:** General forms of perceptual model, Perceptual adaptive watermarking, Robust watermarking, Watermark security, Watermark security and cryptography, Content authentication, Exact authentication, Selective, authentication, Localization, Restoration.

**References:**


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

**MCSCB 206-1** **CRYPTANALYSIS**

| L | T | P | C |
|---|---|---|---|
| 3 | 0 | 0 | 3 |

**Module 1:** Cryptanalysis of classical ciphers: Vigenere cipher, Affine cipher, Hill-cipher Linear Shift Register Random Bit Generator: Berlekamp- Massey algorithm for the cryptanalysis of LFSR, Correlation attack on LFSR based stream ciphers, Cryptanalysis of ORYX, Fast algebraic attack.

**Module 2:** Cryptanalysis of Block Ciphers: Man in the middle attack double DES, Linear and Differential cryptanalysis. 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.

**Module 3:** 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.

**Module 4:** 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, Birthday paradox in two groups, Application of Birthday paradox in Hash functions, Multicollisions attack on hash functions.

**References:**


1. Antoine Joux, "Algorithmic Cryptanalysis", Chapman & Hall/CRC Cryptography and Series, 2009.
2. Song Y Yang, "Number Theory for Computing", Second Edition,SpringerVerlag, 2010.
3. Gregory V. Bard, "Algebraic Cryptanalysis", Springer, 2009.
4. Hffstein, Jeffray, Pipher, Jill and Silverman, "An Introduction to Mathematical Cryptography", Springer, 2010.

| MCSCB 206-2 | LOGICAL FOUNDATIONS FOR ACCESS CONTROL | L | T | P | C |
|---|---|---|---|---|---|
| | | 3 | 0 | 0 | 3 |

**Module 1:** Mathematical Logic: Mathematical systems, Propositions and connectives, Statement formulae and truth tables, Logic variables, Logic Functions, Logic expressions, Equivalences of Logic functions, complete sets of logic functions.

**Module 2:** Propositional & Predicate Calculus: Propositional and Predicate Calculus: Language of Propositional and Predicate Logic - Logic Programming, Formulas, Models,

**Module 3:** Normal Forms— CNF, DNF, SNF, PNF, Satisfiability, consequences and Interpretations, Tableaux, Resolution, Soundness and completeness of Tableaux and Resolution, Semantic Tableaux complete Systematic Tableaux, Decision Methods, Security Models:Biba, Bell LaPadula, Chinese wall, Lattice model, SPKI/SDSI –PKIin first order logic, security of distributed systems using Datalog with constraints,

**Module 4:** Executional specification of security policies in a logic programming framework, Delegation logic, trust management systems, Case studies of specific logic programming models for distributed systems security such as SD3, SecPAL, RT etc.

**References:**


1. John W Lloyd, "Foundations of Logic Programming (Symbolic E Artificial Intelligence)", Springer, 1993
2. J. W Lloyd and John Lloyd, 'Logic and Learning: Knowledge -tation, Computation and Learning in Higher-order Logic", ES—L'11 Heidelberg, 2003.
3. Mordechai Ben-Ad, "Mathematical Logic for Computer Science", B". on, Springer International Edition, 2008.
4. George Matakides and Anil Nerode, "Principles of Logic and Logic — North Holland, 1996.
5. Alessandro Aldini, Gilles Barthe, Roberto Gorrieri, " Foundations of Security Analysis and Design V, Volume 5,Springer, 2009.

**MCSCB 206-3** **GAME THEORY**

| L | T | P | C |
|---|---|---|---|
| 3 | 0 | 0 | 3 |

**Module I:** Fundamentals: Conflict, Strategy and Games, Game theory, The Prisoner's Dilemma, Scientific metaphor, Business case, Games in normal and extensive forms – Representation, Examination, Examples.

**Module II:** Non Cooperative Equilibrium in Normal Games: Dominant Strategies and Social Dilemmas, Nash Equilibrium, Classical Cases in Game theory, Three person games, Introduction to Probability and Game theory, N-Person games.

**Module III:** Cooperative Solutions: Elements of Cooperative Games- Credible commitment, A Real Estate Development, Solution Set, Some Political Coalitions, Applications of the Core to Economics – The Market Game, The Core of a Two Person Exchange Game, The Core with More than Two Pairs of Traders, The core of Public Goods Contribution Game, Monopoly and Regulation .

**Module IV:** Sequential Games: Strategic Investment to Deter Entry, The Spanish Rebellion, Again, Imbedded Games – Planning Doctoral Study, Centipede Solved, Repeated play-Campers Dilemma, Pressing the shirts, Indefinitely Repeated Play – A Repeated Effort Dilemma, The Discount Factor. Applications: Voting Games, Games and Experiments, Auctions, Evolution and Boundary Rational Learning.

**REFERENCES**


1. Roger A. McCain, "Game Theory – A Non-Technical Introduction to the Analysis of Strategy", Thomson South-Western, 2005.
2. Tirole, "Game Theory", Mit press 2005.
3. Osborne, "An Introduction to Game Theory", Oxford Press 2006.
4. E. N. Barron, "Game Theory: An Introduction", Wiley India Pvt Ltd, 2009.

**MCSCB 206-4** **DATABASE SECURITY**

| L | T | P | C |
|---|---|---|---|
| 3 | 0 | 0 | 3 |

**Module 1:** Introduction to databases: database modeling, conceptual database design, overview of SQL and relational algebra, Access control mechanisms in general computing systems: Lampson's access control matrix. Mandatory access control.

**Module 2:** Authentication mechanisms in databases, DAC in databases: Griffiths and Wade, MAC mechanisms in databases: SeaView. RBAC in databases. Authentication and password security – Weak authentication options, Implementation options, Strong password selection method, Implement account lockout, Password profile.

**Module 3:** 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.

**Module 4:** 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. Encrypting data- in transit, Encrypt data-at-rest. Database security auditing categories.

**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 Sushil Jajodia, "Handbook of Database Security-Applications and Trends", Springer, 2008.
4. Database Security, Cengage Learning; 1 edition (July 12, 2011),Alfred Basta . Melissa Zgola
5. Data warehousing and data mining techniques for cyber security, Springer's By Anoop Singha.
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. Pierangela Samarati, Ravi Sandhu," Database Security X: Status and prospects, Volume 10",Springer, 1997.

**MCSCB 207** **ETHICAL HACKING LAB**

| L | T | P | C |
|---|---|---|---|
| 0 | 0 | 3 | 2 |

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.

**MCSCB 208** **SEMINAR - II**

| L | T | P | C |
|---|---|---|---|
| 0 | 0 | 2 | 1 |

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, 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.