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

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

L – Lecture, T – Tutorial, P – Practical

### Elective – I (MCSCY 105)
- MCSCB 105 - 1 Mobile Network Security
- MCSCB 105 - 2 Cryptography and Network Security
- MCSCB 105 - 3 Biometric Security
- MCSCB 105 - 4 Cyber Law and Legislation

### Elective – II (MCSCY 106)
- MCSCB 106 - 1 Information security policies in industries
- MCSCB 106 – 2 Information Risk Management
- MCSCB 106 – 3 Secure Software Engineering
- 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

<table>
<thead>
<tr>
<th>SI NO.</th>
<th>Course No.</th>
<th>Subject</th>
<th>Hrs/Week</th>
<th>Evaluation Scheme(marks)</th>
<th>Credits (C)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>L  T  P</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>MCSCB 201</td>
<td>Cyber Forensics</td>
<td>3  1   0</td>
<td>25 25 50</td>
<td>150</td>
</tr>
<tr>
<td>2</td>
<td>MCSCB 202</td>
<td>Security Threats</td>
<td>3  1   0</td>
<td>25 25 50</td>
<td>150</td>
</tr>
<tr>
<td>3</td>
<td>MCSCB 203</td>
<td>Ethical Hacking</td>
<td>3  1   0</td>
<td>25 25 50</td>
<td>150</td>
</tr>
<tr>
<td>4</td>
<td>MCSCB 204</td>
<td>Design of Secured Architectures</td>
<td>3  1   0</td>
<td>25 25 50</td>
<td>150</td>
</tr>
<tr>
<td>5</td>
<td>MCSCB 205</td>
<td>Elective – III</td>
<td>3  1   0</td>
<td>25 25 50</td>
<td>150</td>
</tr>
<tr>
<td>6</td>
<td>MCSCB 206</td>
<td>Elective – IV</td>
<td>3  1   0</td>
<td>25 25 50</td>
<td>150</td>
</tr>
<tr>
<td>7</td>
<td>MCSCB 207</td>
<td>Ethical Hacking Lab</td>
<td>-  -  3</td>
<td>25 25 50</td>
<td>150</td>
</tr>
<tr>
<td>8</td>
<td>MCSCB 208</td>
<td>Seminar- II</td>
<td>-  -  2</td>
<td>50  -    50</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td>18  4  5</td>
<td>400 700 1100</td>
<td>25</td>
</tr>
</tbody>
</table>

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

**Elective – III (MCSCY 205)**
- MCSCB 205 -1 Coding and Information Theory
- MCSCB 205 -2 Storage Management And Security
- MCSCB 205 -3 Game Theory
- MCSCB 205 -4 Digital Watermarking

**Elective – IV (MCSCY 206)**
- MCSCB 206 –1 Cryptanalysis
- MCSCB 206 -2 Logical Foundations for Access Control
- MCSCB 206 -3 Internet Information and Application Security
- 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

<table>
<thead>
<tr>
<th>Sl. No</th>
<th>Course No.</th>
<th>Subjects</th>
<th>Hrs/ Week</th>
<th>Evaluation Scheme (Marks)</th>
<th>Credits (C)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>L</td>
<td>T</td>
<td>P</td>
</tr>
<tr>
<td>1</td>
<td>MCSCB 301</td>
<td>Research Methodology</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>MCSCB 302</td>
<td>Elective - V</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>MCSCB 303</td>
<td>Global Elective</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>MCSCB 304</td>
<td>Master’s Thesis Phase - I</td>
<td>0</td>
<td>0</td>
<td>20</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td>7</td>
<td>3</td>
<td>20</td>
</tr>
</tbody>
</table>

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

#### Global Elective (MCSCY 303)
- MCSCB 303

### SEMESTER – IV

<table>
<thead>
<tr>
<th>Sl. No</th>
<th>Course No.</th>
<th>Subject</th>
<th>Hrs / Week</th>
<th>Evaluation Scheme (Marks)</th>
<th>Credits (C)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>L</td>
<td>T</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>MCSCB 401</td>
<td>Master’s Thesis</td>
<td>0</td>
<td>0</td>
<td>30</td>
</tr>
<tr>
<td>2</td>
<td>MCSCB 402</td>
<td>Master’s Comprehensive Viva</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### 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.
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


References:

4. George J Klir and Bo Yuan, "Fuzzy sets and Fuzzy logic” Prentice-Hall of India,1995

Web References

Module 1:

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:
Computational Geometry- Line segment properties, Finding the convex hull, Finding the closest pair of points.

References:


References:

6. Reading: Kerberos Authentication. Refer Website.
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.

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:
Springer; 2010.
2. Abhijith Das and C.E. Veni Madha van, "Public-key Cryptography, Theory and Practice",
3. Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone, "Handbook of Applied
Module 1: Transmission Fundamentals:


References:


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:
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
2. John Chirillo and Scott Blaul,” Implementing Biometric Security”, Wiley Eastern Publications,
2005.


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.


REFERENCES


REFERENCES

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.


References:


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.


References:
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 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. 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://www.openssl.org/docs/apps/openssl.html
- https://netfiles.uiuc.edu/ehowes/www/gpg/gpg-com-0.htm
- http://www.ethereal.com/docs/user-guide/
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.
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


References:
1 Understanding Cryptography: A Textbook for Students and Practitioners: Christof paar, Jan Pelzl.
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


REFERENCES


REFERENCES:


REFERENCES
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:

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.


References:


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.


REFERENCES

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 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:


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.


References:

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 –PKIn first order logic, security of distributed systems using Datalog with constraints,

Module 4: Executonal 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:


References:
3. Magnus Mischel, ModSecurity 2.5, Packt Publishing
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.


References:

5. Data warehousing and data mining techniques for cyber security, Springer's By Anoop Singha.
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.
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)
### Semester – II

<table>
<thead>
<tr>
<th>SI NO.</th>
<th>Course No.</th>
<th>Subject</th>
<th>Hrs/Week</th>
<th>Evaluation Scheme(marks)</th>
<th>Credits (C)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>L  T    P</td>
<td>Sessional</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TA</td>
<td>CT</td>
</tr>
<tr>
<td>1</td>
<td>MCSCB 201</td>
<td>Cyber Forensics</td>
<td>3 1 0</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>2</td>
<td>MCSCB 202</td>
<td>Security Threats</td>
<td>3 1 0</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>3</td>
<td>MCSCB 203</td>
<td>Ethical Hacking</td>
<td>3 1 0</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>4</td>
<td>MCSCB 204</td>
<td>Design of Secured Architectures</td>
<td>3 1 0</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>5</td>
<td>MCSCB 205</td>
<td>Elective – III</td>
<td>3 0 0</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>6</td>
<td>MCSCB 206</td>
<td>Elective – IV</td>
<td>3 0 0</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>7</td>
<td>MCSCB 207</td>
<td>Ethical Hacking Lab</td>
<td>- - 3</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>8</td>
<td>MCSCB 208</td>
<td>Seminar- II</td>
<td>- - 2</td>
<td>50</td>
<td>- 50</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>TA</td>
<td>CT</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>18 4 5</td>
<td>225</td>
<td>175</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Elective – III (MCSCB 205)</th>
<th>Elective – IV (MCSCB 206)</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCSCB 205 -1</td>
<td>Coding and Information Theory</td>
</tr>
<tr>
<td>MCSCB 205 -2</td>
<td>Storage Management And Security</td>
</tr>
<tr>
<td>MCSCB 205- 3</td>
<td>Internet Information and Application Security</td>
</tr>
<tr>
<td>MCSCB 205 -4</td>
<td>Digital Watermarking</td>
</tr>
</tbody>
</table>

- **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
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


References:
1 Understanding Cryptography: A Textbook for Students and Practitioners: Christof paar, Jan Pelzl.
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


REFERENCES


REFERENCES:


REFERENCES
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:

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.


References:

1. EMC Education Services “Information Storage and Management: Storing, Managing, and Protecting Digital Information” , John Wiley & Sons, 2010


References:
3. Magnus Mischel, ModSecurity 2.5, Packt Publishing
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 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:


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.


References:

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:


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.


REFERENCES
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.


References:

5. Data warehousing and data mining techniques for cyber security, Springer's By Anoop Singha.
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.
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.