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 – 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</td>
<td>T</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>TA</td>
<td>CT</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>MCSCB 201</td>
<td>Cyber Forensics</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>MCSCB 202</td>
<td>Security Threats</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>MCSCB 203</td>
<td>Ethical Hacking</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>MCSCB 204</td>
<td>Design of Secured Architectures</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>MCSCB 205</td>
<td>Elective – III</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>MCSCB 206</td>
<td>Elective – IV</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>MCSCB 207</td>
<td>Ethical Hacking Lab</td>
<td>-</td>
<td>-</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>MCSCB 208</td>
<td>Seminar- II</td>
<td>-</td>
<td>-</td>
<td>2</td>
</tr>
</tbody>
</table>

|        | Total       | 18 | 4 | 5 | 225 | 175 | 400 | 700 | 1100 | 25 |

L – Lecture, T – Tutorial, P – Practical

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

**Elective – IV (MCSCB 206)**
- MCSCB 206 – 1 Cryptanalysis
- MCSCB 206 - 2 Logical Foundations for Access Control
- MCSCB 206 - 3 Game Theory
- 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
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.
Computer Forensics Evidence and Capture- Data Recovery-Evidence collection and Data Seizure-Duplication and preservation of Digital Evidence-Computer image verification and Authentication

Computer Forensics Analysis- Discovery of Electronic Evidence- Identification of data-Reconstructing Past events- networks


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 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

Module 3: 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
3. Magnus Mischel, ModSecurity 2.5, Packt Publishing
   Companies
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 $F_p$, 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 –PKI in 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.