M.TECH IN COMPUTER SCIENCE AND ENGINEERING (INFORMATION SECURITY)

CURRICULUM AND SYLLABUS

(Effect from the Academic Year 2007 – 08)

PONDICHERRY UNIVERSITY
PUDUCHERRY – 605014.
M.TECH IN COMPUTER SCIENCE AND ENGINEERING (INFORMATION SECURITY)

COURSE CURRICULUM AND SCHEME OF EXAMINATION

(Minimum Credit Requirement for the completion of the Programme: 72)

M.Tech. in Computer Science and Engineering (Information Security): Candidates for admission to the first semester of four semester M.Tech. Course in Computer Science and Engineering with specialization in Information Security should have passed B.E./B.Tech. in Computer Science and Engineering / Information Technology / Electronics & Communication Engineering / Electrical & Electronics Engineering / Electronics & Instrumentation Engineering / Instrumentation and Control Engineering (or) an examination of any University or Authority accepted by the Pondicherry University as equivalent thereto, with at least 55% marks in the degree examination or equivalent CGPA

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credits</th>
<th>Evaluation (marks)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>L  T  P</td>
<td></td>
<td>Internal  External  Total</td>
</tr>
<tr>
<td>1.</td>
<td>CS 911</td>
<td>Mathematical Foundations of Information Security</td>
<td>3  1  0</td>
<td>4</td>
<td>40       60       100</td>
</tr>
<tr>
<td>2.</td>
<td>CS 912</td>
<td>Data Structures</td>
<td>3  1  0</td>
<td>4</td>
<td>40       60       100</td>
</tr>
<tr>
<td>3.</td>
<td>CS 913</td>
<td>Internals of Operating Systems</td>
<td>3  1  0</td>
<td>4</td>
<td>40       60       100</td>
</tr>
<tr>
<td>4.</td>
<td></td>
<td>Elective – I</td>
<td>3  0  0</td>
<td>3</td>
<td>40       60       100</td>
</tr>
<tr>
<td>5.</td>
<td></td>
<td>Elective – II</td>
<td>3  0  0</td>
<td>3</td>
<td>40       60       100</td>
</tr>
<tr>
<td>6.</td>
<td>CS 917</td>
<td>Laboratory – I</td>
<td>1  0  3</td>
<td>2</td>
<td>50       50       100</td>
</tr>
</tbody>
</table>

Total: 20 250 350 600
### SEMESTER – II

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credits</th>
<th>Evaluation (marks)</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>CS914</td>
<td>Network Security</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2.</td>
<td>CS915</td>
<td>Cyber Law and Security Policies</td>
<td>3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3.</td>
<td>CS916</td>
<td>Information Theory and Coding</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4.</td>
<td></td>
<td>Elective – III</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5.</td>
<td></td>
<td>Elective – IV</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6.</td>
<td></td>
<td>Elective – V</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7.</td>
<td>CS918</td>
<td>Laboratory - II</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
</tbody>
</table>

| Total   |        |                                  | 23 | 290 | 410 | 700 |

### SEMESTER – III

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credits</th>
<th>Evaluation (marks)</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></td>
<td>Elective – VI</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2.</td>
<td></td>
<td>Elective – VII</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3.</td>
<td>CS971</td>
<td>Directed Study</td>
<td>0</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>4.</td>
<td>CS919</td>
<td>Dissertation Project (Phase I)</td>
<td>0</td>
<td>0</td>
<td>24</td>
</tr>
</tbody>
</table>

<p>| Total   |        |                                  | 17 | 430 | 270 | 700 |</p>
<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Code</th>
<th>Subject</th>
<th>Hours / Week</th>
<th>Credits</th>
<th>Evaluation (marks)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>L  T  P</td>
<td></td>
<td>Internal</td>
</tr>
<tr>
<td>1.</td>
<td>CS 920</td>
<td>Dissertation Project (Phase II)</td>
<td>0  0  36</td>
<td>12</td>
<td>250</td>
</tr>
</tbody>
</table>

<p>|        |       |                                   |             |         | 12        | 250       | 150   | 400   |</p>
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS941</td>
<td>Advanced Databases</td>
</tr>
<tr>
<td>CS942</td>
<td>Agent Technology</td>
</tr>
<tr>
<td>CS943</td>
<td>Biometric Security</td>
</tr>
<tr>
<td>CS944</td>
<td>Computer Security, Audit Assurance and Risk Management</td>
</tr>
<tr>
<td>CS945</td>
<td>Cryptography</td>
</tr>
<tr>
<td>CS946</td>
<td>Data and Knowledge Security</td>
</tr>
<tr>
<td>CS947</td>
<td>Dependable Distributed Systems</td>
</tr>
<tr>
<td>CS948</td>
<td>Embedded Systems</td>
</tr>
<tr>
<td>CS949</td>
<td>Fundamentals of Financial Management</td>
</tr>
<tr>
<td>CS950</td>
<td>Information Security Policies in Industries</td>
</tr>
<tr>
<td>CS951</td>
<td>Mobile Wireless Security</td>
</tr>
<tr>
<td>CS952</td>
<td>Security Assessment and Verification</td>
</tr>
<tr>
<td>CS953</td>
<td>Secure Software Engineering</td>
</tr>
<tr>
<td>CS954</td>
<td>Secured Network Protocols</td>
</tr>
<tr>
<td>CS955</td>
<td>Security Threats</td>
</tr>
<tr>
<td>CS956</td>
<td>Steganography and Digital Watermarking</td>
</tr>
<tr>
<td>CS957</td>
<td>Trust Management in E-Commerce</td>
</tr>
<tr>
<td>CS958</td>
<td>Trusted Internet</td>
</tr>
</tbody>
</table>
CS912 DATA STRUCTURES

UNIT I
Problem solving techniques – Space and Time complexity of algorithms-2 Growth of Functions, Asymptotic notation, Standard notations and common functions, Summations
Summation formulas and properties, Bounding summations, Recurrences-substitution method- iteration method- The master method

UNIT II
Linear data structures-array of structures-stack-queue-priority queues, pointers and linked allocation
Linked list –singly, doubly, circular -polynomial addition-sparse matrices-equivalence relations-garbage collection and compaction

UNIT III
Non linear data structures – Trees- Binary Search Tree, terminology-representation-insertion-deletion-querying
Graphs –terminology-representation-traversals-spanning trees-shortest path-topological sort

UNIT IV
Red black trees, AVL trees , B –trees –building –operations-analysis

UNIT V

Reference Books
2. Thomas H. Cormen (Author), Stein Clifford (Author), Charles E. Leiserson (Author), Robert L. Rivest (Author ) “Introduction to Algorithms (Paperback)”
5. Ellis Horowitz and sartaj sahni"Fundamentals of Data Structures",Galgotia Booksource,1995
CS952 SECURITY ASSESSMENT AND VERIFICATION

Unit I

Evolution of information security, information assets, security standards, organizational impacts, security certifications, elements of information security program, need for security assessment, security assessment process.

Unit II

Security assessment planning – Business drivers, scope definition, consultant’s perspective, Client’s perspective, Development of project plan.
Initial information gathering – Initial preparation, analysis of gathered information.

Unit III

Business process evaluation, Technology evaluation, Risk analysis, Risk mitigation.

Unit IV


Unit V

Information security standards, information security Legislation, formal security verification, security verification with SSL.

Text Book:

CS952 SECURITY ASSESSMENT AND VERIFICATION

Unit I
Evolution of information security, information assets, security standards, organizational impacts, security certifications, elements of information security program, need for security assessment, security assessment process.

Unit II
Security assessment planning – Business drivers, scope definition, consultant’s perspective, Client’s perspective, Development of project plan.
Initial information gathering – Initial preparation, analysis of gathered information.

Unit III
Business process evaluation, Technology evaluation, Risk analysis, Risk mitigation.

Unit IV

Unit V
Information security standards, information security Legislation, formal security verification, security verification with SSL.
Text Book:

CS911-MATHEMATICAL FOUNDATIONS OF INFORMATION SECURITY

UNIT I

Some topics in elementary number theory: O and Ω notations – time estimates for doing arithmetic – divisibility and the Euclidean algorithm – Congruences – some applications to factoring – finite fields – quadratic residues and reciprocity.

UNIT II


UNIT III


UNIT IV

Primality and Factoring: Pseudoprimes – the rho (γ) method – Format factorization and factor bases – the continued fraction method – the quadratic sieve method.

UNIT V


REFERENCE BOOKS

CS916 - INFORMATION THEORY AND CODING

UNIT 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.

UNIT 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.

UNIT 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.

UNIT 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.

UNIT V

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.

REFERENCE BOOKS:

CS913 - INTERNALS OF OPERATING SYSTEMS

UNIT I

Introduction to Kernel: Architecture of the UNIX operating system, System concepts, Data structures. Buffer Cache: Buffer header, Structure of Buffer pool, Reading and writing disk blocks. Files: INODES, Structure of a regular file, Directories, Super block, Inode assignment.

UNIT II


UNIT III


UNIT IV


UNIT V


REFERENCE BOOKS:


CS914 - NETWORK SECURITY

UNIT I

Introduction to Security in Networks – Characteristics of Networks – Intrusion – Kinds of security breaches – Plan of attack - Points of vulnerability – Methods of defence – Control measures – Effectiveness of controls

UNIT II


UNIT III


UNIT IV


UNIT V


REFERENCE BOOKS:

3. Charles P. Pleeger, Security in Computing, Person Education Asia
UNIT I
Data Security: Database systems- architectures- storage structures- storage issues in in Database Management Systems- Security of data at various levels of Database Management Systems

UNIT II
Distributed Databases: Distributed Data Processing- Distributed Database system- Distributed Database Management System Architecture: Architectural models for Distributed Database Management System – Global directory issues – Distributed database design – distributed design issues – fragmentation – Allocation

UNIT III

UNIT IV
Knowledge base systems - Knowledge base system design – storage of knowledge – various formats – Levels of security issues in Knowledge base system design – conceptual level – implementation level

UNIT V

REFERENCE BOOKS:
CS953- SECURE SOFTWARE ENGINEERING

UNIT I

UNIT 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

UNIT III

UNIT IV

UNIT V

REFERENCE BOOKS:
2. Jan Jürjens, Secure Systems Development with UML, Springer; 2004 (Covers Unit IV and V)
CS915 - CYBER LAW AND SECURITY POLICIES

UNIT I

Security and computing: characteristics of computer intrusion - attacks-security goals-criminals-methods of defense control- cryptography- digital signatures-program security - Protection in operating system - design of trusted operating systems.

UNIT II

Database security- security in networks- network controls-firewalls-Intrusion detection systems-secure Email-Administrating security-organization security policies-legal privacy ethical issues in computer security.

UNIT III

Information security policies and procedures: corporate policies-legal requirements-business requirements- process management-planning and preparation-developing policies-asset classification policy-developing standards.

UNIT IV

Information security: fundamentals-Employee responsibilities-information classification-Information handling-Tools of information security-Information processing-secure program administration

UNIT V


TEXT BOOKS


REFERENCE BOOKS

UNIT-I


UNIT – II


UNIT-III


UNIT – IV


UNIT-V


REFERENCE BOOKS

CS948 - EMBEDDED SYSTEMS

UNIT I


UNIT II


UNIT III

Interrupt synchronization: General features of interrupts on 6805, 6808, 6811, 6812, Interrupt Vectors and priority, External interrupts, Interrupt Polling, Round Robin Polling. Threads: Multithreaded preemptive scheduler, Semaphores, Applications of Semaphores, Timing Generation and Measurements: Input-output capture, frequency measurement, conversion between frequency and period

UNIT IV

Serial I/O devices: RS-232C specifications, RS-422 / AppleTalk / RS-423 / RS-485 balanced differential lines, other communication protocols, Serial Communication Interface SCI Applications, Parallel Port Interfaces: Input Switches and Keyboards, Output LEDs, LCDs, Transistors used or computer Controlled Relay Keys, DC Motors, Stepper Motors, Memory Interfacing: Address decoding, Timing Syntax, Bus-Timings, Memory interface examples. High-Speed I/O interfacing: High speed I/O applications, High-Speed interfaces, Examples.

UNIT V


REFERENCE BOOKS:

CS945 - CRYPTOGRAPHY

UNIT I
Introduction – Beginning with a simple communication game – Wrestling between safeguard and attack – Encryption symmetric techniques.

UNIT II
Encryption – Asymmetric techniques – Bit security of the basic public key cryptographic functions

UNIT III
Data Integrity Techniques – Authentication framework for public key cryptography.

UNIT IV
Formal and strong security definitions for public-key crypto systems – Provably secure and efficient public-key cryptosystems – Introduction – The optimal asymmetric encryption padding.

UNIT V
The Cramer–Shoup Public-key crypto systems – An overview of provably secure hybrid cryptosystems – Literature notes on practical and provably secure public-key cryptosystems – Strong and provable security for digital signatures.

REFERENCE BOOKS:
UNIT I

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

UNIT II


UNIT III


UNIT IV


UNIT V


TEXT BOOKS :

REFERENCE BOOKS :
CS957 - TRUST MANAGEMENT IN E-COMMERCE

UNIT I


UNIT II


UNIT III


UNIT IV

Introduction to trusted computing platform: Overview – Usage Scenarios – Key components of trusted platform – Trust mechanisms in a trusted platform

UNIT V

Trusted platforms for organizations and individuals – Trust models and the E-Commerce domain.

REFERENCE BOOKS:

CS956 - STEGANOGRAPHY AND DIGITAL WATERMARKING

UNIT I


UNIT II


UNIT III


UNIT IV

Survey of current watermarking techniques – Cryptographic and psycho visual aspects – Choice of a workspace – Formatting the watermark bets – Merging the watermark and the cover – Optimization of the watermark receiver – Extension from still images to video – Robustness of copyright making systems

UNIT V


REFERENCE BOOK:
CS950 - INFORMATION SECURITY POLICIES IN INDUSTRIES

UNIT I


UNIT II


UNIT III


UNIT IV


UNIT V


REFERENCE BOOKS :

CS942 - AGENT TECHNOLOGY

UNIT I
Agent Definition - History - Intelligent Agents- Agent Programming Paradigms - Agent Vs Object - Aglet - Mobile Agents – Agent Frameworks - Agent Reasoning.

UNIT II

UNIT III

Interface Agents - Agent Communication Languages - Agent Knowledge representation - Agent adaptability -Belief Desire Intension - Mobile Agent Applications.

UNIT IV
Situational Calculus - Representation of Planning - Partial order Planning- Practical Planners – Conditional Planning - Replanning Agents.

UNIT V

REFERENCE BOOKS :
CS949 - FUNDAMENTALS OF FINANCIAL MANAGEMENT

UNIT I

UNIT II

UNIT III

UNIT IV
Intermediate and Long-Term Financing - The Capital Market - Long-Term Debt, preferred Stock, and Common Stock - Term Loans and Leases

UNIT V
Special Areas of Financial Management - Convertibles, Exchangeables, and Warrants - Mergers and Other Forms of Corporate Restructuring - International Financial Management

TEXT BOOK:
CS941 - ADVANCED DATABASES

UNIT I


UNIT II


UNIT III


UNIT IV


UNIT V


REFERENCE BOOKS:

CS943 - BIOMETRIC SECURITY

UNIT 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-how biometric matching works- Accuracy in biometric systems

UNIT II:

UNIT III:

UNIT IV:
Multi biometrics: Multi biometrics and multi factor biometrics- two-factor authentication with passwords, tickets and tokens –executive decision- implementation plan

UNIT V:
Case studies on Physiological, Behavioral and multifactor biometrics in identification systems.

REFERENCE BOOKS :
CS958 - TRUSTED INTERNET

UNIT I
INTERNET: Understanding the Internet, Hardware Requirements to connect to the internet, Software requirements and Internet Service Providers (ISP), Internet Addressing, Internet Protocol: Routing Information Protocol (RIP); User Datagram Protocol (UDP); Transmission Control Protocol (TCP), Domain Name Service (DNS), Basic Connectivity: Telnet; FTP, Internet Relay Chat (IRC).

UNIT II
ATTACKS: Access Attacks – Snooping; Eavesdropping; interception, Hacker Techniques – Hacker’s motivation; Historical Hacking Techniques; Advance Techniques; Targeted Hacker, Information Security Services – Confidentiality, Integrity; Availability; Accountability.

UNIT III
FIREWALL: Firewall Concepts, Types of Firewalls, Firewall Configuration, Design a Firewall Rule set, Purpose of Firewall, Security role of a Firewall, Advantages and disadvantages of firewall, Firewall Components, Procuring a Firewall, Administrating a firewall, firewall toolkits.

UNIT IV
E-Commerce Security: E-Commerce Services, Importance of Availability, Security Implementation – Client Side; Server side; Application; Database Server.

UNIT V
SECURITY: Security Environment, User Authentication, Attacks form inside the system, Attacks from outside the system, Protection Mechanism, Trusted Systems, Trusted Computing Base, Formal Models of Secure system, Multilevel security, Designing trusted Operating System.

TEXT BOOKS:

REFERENCE BOOKS:
CS951 - MOBILE WIRELESS SECURITY

UNIT I


UNIT II


UNIT III


UNIT IV


UNIT V


TEXT BOOKS


REFERENCES

CS954 - SECURED NETWORK PROTOCOLS

UNIT I


UNIT II


UNIT III


UNIT IV


UNIT V


TEXT BOOKS

REFERENCE BOOKS
CS947 - DEPENDABLE DISTRIBUTED SYSTEMS

UNIT I

UNIT II

UNIT III

UNIT IV

UNIT V

REFERENCE BOOKS