## INDEX

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Title</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Marks Distribution</td>
<td>2</td>
</tr>
<tr>
<td>2.</td>
<td>Semester I</td>
<td>3</td>
</tr>
<tr>
<td>3.</td>
<td>Semester II</td>
<td>6</td>
</tr>
<tr>
<td>4.</td>
<td>Semester III</td>
<td>14</td>
</tr>
<tr>
<td>5.</td>
<td>Semester IV</td>
<td>17</td>
</tr>
</tbody>
</table>

Syllabus for

M.Tech - Computer Science and Engineering (CSE)  
With Specialization in - Cyber Security (CyS)  
& Information and Communication Technologies (ICT)
## MARKS DISTRIBUTION

Following is Marks Distribution for courses depending upon the credit of the courses:

(1 credit = 50 marks)

<table>
<thead>
<tr>
<th>Credit</th>
<th>Type of Course</th>
<th>Max. Marks</th>
<th>Major (End Semester examination)</th>
<th>Performance Evaluation</th>
<th>Lab Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Theory course</td>
<td>150</td>
<td>75</td>
<td>40 (20 each)</td>
<td>35</td>
</tr>
<tr>
<td>4</td>
<td>Theory course (with lab)</td>
<td>200</td>
<td>75</td>
<td>40 (20 each)</td>
<td>35</td>
</tr>
<tr>
<td>4</td>
<td>Thesis / dissertation -I</td>
<td>200</td>
<td>100</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Thesis / dissertation -I</td>
<td>700</td>
<td>300</td>
<td>400</td>
<td></td>
</tr>
</tbody>
</table>

Note: Maximum Marks is fixed for all the courses. Only internal assessments and lab evaluation marks distribution may vary as per the instructions communicated by the assigned Faculty. Refer to M.Tech Ordinance & Regulation for Assessment Procedures and Performance Evaluation.
SEMESTER-I

1. Course Code: MCSC-101,
Course Name: ADVANCE DESIGN AND ANALYSIS OF ALGORITHMS,
Credit: 4

Syllabus: Network flows (max flow and min-cost flow/circulation), Data structures (Fibonacci heaps, splay trees, dynamic trees), Linear programming (structural results, algorithms) and SDP based, Dealing with intractability: approximation algorithms (techniques for design and analysis), Dealing with large data sets (compression, streaming algorithms, compressed sensing), Computational geometry, Hardness of approximation - Approximation Algorithms based on Algorithmic Game Theory, Randomized Algorithms, complexity theory, Parallel Algorithms.


2. Course Code: MCSC-102,
Course Name: MOBILE AND WIRELESS SENSOR NETWORKS,
Credit: 4


Lab: Programming routing protocol an sensor network using ns-3, practicing theories in simulator.

3. Course Code: MCSC-103,
Course Name: ADVANCED COMPUTER NETWORKS AND COMMUNICATION,
Credit: 4

Syllabus: Includes: 1) telecommunications history; 2) telecommunications media (conducted and radiated); 3) transmission characteristics (including an introduction to coding and modulation techniques); 4) error characteristics, detection, and correction; 5) local and wide
area networking applications, hardware, and software; 6) the OSI model; 7) industry standards; 8) topologies; 9) protocols; 10) internetworking devices; 11) communications management; 12) security and recovery; 13) information system applications; and 14) the selection of telecommunications and networking systems communication security, Digital signatures, authentication protocols. WLAN, Mobile IP. SNMP(V1 and V2)-Organizational model-System Overview, The information model, communication model-Functional model, SNMP proxy server. Broadband networks and services, ATM Technology, Configuration management, Fault management, performance management. Network Management Tools, Network Statistics Measurement Systems – Web Based Management, XML Based Network Management

**Lab:** Programming protocol USING C/C++ and MATLAB and practicing theory.

4. **Course Code:** MCSC-104,  
**Course Name:** CLOUD COMPUTING,  
**Credit:** 3


5. **A. (For CyS)**  
**Course Code:** MCySC-101,  
**Course Name:** FUNDAMENTAL OF INFORMATION SECURITY & PRACTICES,  
**Credit:** 3

**Syllabus:** Introduction to information security, need, scope, basic principles- CIAA, policies, procedures, Guidelines, Standards Administrative Measures and Technical Measures info sec culture, interpretation of info sec culture, dynamic organizational model, modeling the

5. B. (For ICT)
Course Code: MICTC-101,
Course Name: MATHEMATICAL FOUNDATIONS FOR COMPUTING IN ICT,
Credit: 3

SEMESTER-II

1. Course Code: MCSC-201,  
   Course Name: RESEARCH METHODOLOGY,  
   Credit: 3


2. Course Code: MCSC-202,  
   Course Name: PROBABILITY AND STATISTICS,  
   Credit: 3


3. (For CyS)

Course Code: MCySC-201,

Course Name: CRYPTOGRAPHY,

Credit: 4

Syllabus: History and overview of cryptography, identification protocols. Password protocols, salts, PBKDF2; one time passwords (S/Key and SecurID); challenge response authentication, One time pad and stream ciphers; perfect secrecy and the one time pad, semantic security and stream ciphers, Block ciphers. Case studies: Feistel networks, DES, 3DES, and DES basic modes of operation: CBC and counter mode. Block cipher abstractions: PRPs and PRFs. Pseudo Random Permutations (PRP); Pseudo Random Functions (PRF); security against chosen plaintext attacks (CPA); nonce-based CBC encryption and nonce-based counter mode. Attacks on block ciphers: exhaustive search, time-space tradeoffs, differential & linear cryptanalysis, meet in the middle, side channels. Message integrity: definition and applications CBC-MAC and PMAC. Collision resistant hashing; Merkle-Damgard and Davies-Meyer. MACs from collision resistance. Elliptic key cryptography. Case studies: SHA and HMAC. Authenticated encryption: security against active attacks, intro to session setup using a key distribution center (KDC). Cryptography using arithmetic modulo primes, vanilla key exchange (Diffie-Hellman); the CDH and discrete-log assumptions. Public key encryption: semantically secure El Gamal encryption; CCA security. Arithmetic modulo composites. RSA and Rabin functions, how to encrypt with trapdoor permutations. Digital signatures: definitions and applications. How to sign using RSA. More signature schemes Lamport and Merkle schemes. Overview of signatures based on discrete-log; certificates and trust management. Identification protocols: Password protocols, salts; one time passwords (S/Key and SecurID); challenge response authentication. Authenticated key exchange and SSL/TLS session setup. Zero knowledge protocols.

Lab: Programming and implementation of cipher, cryptographic algo and digital signatures in C/java and practicing theory.
4. (For CyS)  
Course Code: MCySC -202,  
Course Name: SECURE SOFTWARE DESIGN AND OPERATING SYSTEM SECURITY,  
Credit: 4  

**Syllabus:** Security principles and secure coding practices using Java Security Platform, Class loading, Byte code verifier, Security Manager, security policies, and Security Framework Secure SDLC, threat modeling, software security frameworks, and secure software architectures • Best practices and standards and guidelines for secure file input/output and serialization • input validation techniques, validation errors, and best practices • exceptions, erroneous behaviors, and the best practices to handle or avoid them • Secure authentication and authorization processes, Core security coding practices of Java Cryptography that includes Encryption, Key Generator and implementation of Cipher Class, • Digital signatures, secret keys, and key management • Various Java application vulnerabilities. 
Theoretical foundation for designing trusted OS, Version of OS, Patches and Service Packs, Checking for hot fixes and service packs, Software Inventory, Alternative OS Support, Drives and file systems; NTFS, FAT, Linux. User right agreement: Security Options, Account Lockout Policy, Password Policy, BIOS Password, Password protected screen saver, Number of Windows platforms on a machine. Introduction to Access Control and authentication methods, Shares and Share Security, File/Folder permissions and Encryption, active directory security, Virtualization and its effect on secure OS, IIS Sec: ODBC connections security, IIS installation location, IIS components, Services required for IIS, FPSE (Front Page Server Extensions) Security, ACLs on virtual directories, Sample files and websites, Script mappings, Reverse Code Engineering, Registry Security, Event Log configuration, Backup procedures, Virus Protection, Case studies of secure OS, System administration.  

**Lab:** Practical implementation of theory classes as assigned by Faculty on java input validation techniques, validation errors, exceptions, erroneous behaviours, Encryption, Key Generator.

3. (For ICT)  
Course Code: MICTC- 201,  
Course Name: DIGITAL SIGNAL PROCESSING & SIGNAL THEORY,  
Credit: 4  


4. **(For ICT)**

**Course Code: MICTC-202,**

**Course Name: SPEECH COMMUNICATION AND BIOMEDICAL SIGNAL PROCESSING,**

**Credit: 4**


Biomedical Signals and Images
- ECG: Cardiac electrophysiology, relation of electrocardiogram (ECG) components to cardiac events, clinical applications. Guest lecture.
- Speech Signals: The source-filter model of speech production, spectrographic analysis of speech.
- Speech Coding: Analysis-synthesis systems, channel vocoders, linear prediction of speech, linear prediction vocoders.
- Imaging Modalities: Survey of major modalities for medical imaging: ultrasound, X-ray, CT, MRI, PET, and SPECT.
- Data Acquisition: Sampling in time, aliasing, interpolation, and quantization.
- Digital Filtering: Difference equations, FIR and IIR filters, basic properties of discrete-time systems, convolution.
- DTFT: The discrete-time Fourier transform and its properties. FIR filter design using windows.
- DFT: The discrete Fourier transform and its properties, the fast Fourier transform (FFT), the overlap-save algorithm, digital filtering of continuous-time signals.
- Sampling Revisited: Sampling and aliasing in time and frequency, spectral analysis.
- Image processing I: Extension of filtering and Fourier methods to 2-D signals and systems.
- Image processing II: Interpolation, noise reduction methods, edge detection, homomorphic filtering.
- Probability and Random Signals PDFs: Introduction to random variables and probability density functions (PDFs).
- Classification: Bayes’ rule, detection, statistical classification.
- Random signals I: Time averages, ensemble averages, autocorrelation functions, crosscorrelation functions.
- Random signals II: Random signals and linear systems, power spectra, cross spectra, Wiener filters.
- Blind source separation: Use of principal component analysis (PCA) and independent component analysis (ICA) for filtering.

Lab: Programming and practicing theory.

5. A. Course Code: MCSC-203,
Course Name: INTRODUCTION TO FORMAL METHODS AND VERIFICATION OF LARGE SYSTEMS,
Credit: 3

Syllabus: Process algebras and concurrent systems: Reactive systems, Formal methods for reactive systems, Labelled transition systems, Operational semantics for concurrent processes, Operators for process modelling, Pi-calculus. Behavioural equivalences and proof techniques: Bisimulation, Induction and co-induction proofs, Induction as a fixed point technique, Weak bisimulation, Weak bisimulations “upto”, Bisimulation in concurrency, Other equivalences such as failure equivalence, testing, testing equivalence.
- Type systems: Revisit to Pi-calculus, Simply typed Pi-calculus, Input output types, Linear types, Session types.
- Model checking: Finite state model checking, Symbolic model checking, Probabilistic model checking, Real time model checking, Optimal scheduling using model checking.
- Stochastic modelling: Foundation, Quantitative modelling, Markovian methods, PEPA as case study.
- Tools:
Experimental practice on mobility workbench (MBW), concurrency workbench (CWB-NC), CTMC.

5. B. (For CyS)
Course Code: MCySE-201
Course Name: SECURITY STANDARDS & PROJECT MANAGEMENT
Credit: 3

Syllabus: Introduction, design goals, role and security architecture relationship to information security, incident management and IT auditing processes; security risk management; legal and ethical issues of security and privacy. Trusted computing base, protection measures of trusted computing base, system security assurance concepts, confidentiality and integrity models, security risk management process, data classification, regulatory requirements, web services. What is information security management (ISM), Why ISM is important to an organization, What are the benefits of ISM, What is the background of ISM, What are the key concepts and principles in ISO/IEC 27001:2013, The terms and definitions used, The main requirements of ISO/IEC 27001:2013, COBIT, ITIL, PCI DSS, HIPPA.

5. C. (For CyS)
Course Code: MCySE-202
Course Name: SYSTEM SECURITY
Credit: 3


Database vulnerability and attack: SQL Injection, and security mechanisms: Advanced Encryption Standards, Public Key Encryption, Digital Signatures, Database auditing: Data Control Language (DCL) activities, Data Definition Language (DDL) activities, and Data
Manipulation Language (DML). Smart card operating system-fundamentals, design and implantation principles, memory organization, smart card files, file management, atomic operation, smart card data transmission ATR, PPS Security techniques- user identification, smart card security, quality assurance and testing, smart card life cycle-5 phases, smart card terminals.

5.D. (For CyS)

Course Code: MCySE- 203,
Course Name: IDENTITY AND ACCESS MANAGEMENT & TRUSTED COMPUTING,
Credit: 3

Syllabus: Identity and access management (IAM) overview, Attributes of information security, Symmetric and asymmetric cryptography, Hashing and digital signature, Key management, Public Key Infrastructure (PKI) Architecture: certification and registration authority, Life cycle management, Types of certificates and usage patterns – Encryption, Digital signature, Client certificate, SSL server certificate, Attribute based certificate, Case studies (e.g. email protection, mobile banking, and document signing), Identification verification and authentication overview, Mechanisms of identification and authentication - One time password, Biometric, Digital signature, Smartcard, Soft/hard tokens, Mobile device, Risk based authentication, Step-up authentication, Single-sign on and federated single-sign-on, OATH, OpenID, BrowserID, and SAML, Architecture framework and industrial tools, Trusted computing role in identity assurance, Security risks associated with the discussed mechanisms Access control, Principles of authorization, Access control schemes, OAuth protocol, Enterprise rights management and digital rights management, Privileged account management, Governance and compliance. IAM framework and use cases, IAM architecture framework, IAM echo system, IAM and cloud computing, Illustrative use cases - Border control, E-passport, National ID, E-banking, E-health system and EMV scheme

5.B. (For ICT)

Course Code: MICTE-201,
Course Name: SOFTWARE DESIGN AND ENGINEERING,
Credit: 3

5.C. (For ICT)
Course Code: MICTE-202,
Course Name: INFORMATION THEORY AND CODING,
Credit: 3

Syllabus: Entropy, mutual information, channel capacity, information rate, Shannon’s noiseless coding theorem and Shannon’s fundamental coding theorem; modelling of information sources—zero memory and Markov models; modelling of information channels--BSC and BEC channels, additivity of information and cascaded channels; construction of compact source codes--Kraft inequality, compact codes, Huffman and Shannon Fano compression codes; and analysis and design of error-control channel codes--Hamming distance, binary linear codes and the parity-check matrix, Hamming codes, checksum codes, cyclic codes and the generator polynomial and CRC codes, convolutional codes, Viterbi and other decoding algorithms.

5.D. (For ICT)
Course Code: MICTC-301,
Course Name: INTELLIGENT SYSTEM & GREEN ICT,
Credit: 3


Understand the overall need for an organisation to adopt a Green IT strategy, Provide an understanding of the historic development and context of the Kyoto Protocol. The key elements of Green IT, Commonly accepted definitions, IT as an energy consumer, IT as a green 'enabler', The concept and dangers of 'Green Wash', Identify and understand an organisation’s external drivers and opportunities for greening its IT, identify and understand the internal drivers, opportunities and benefits of adopting a Green IT strategy for both an organisation and its IT service provider(s) -Cost, Operations, Marketing/PR, Culture. The role of a Green IT policy, The importance of a Green IT policy, Definition of carbon footprints: direct and indirect emissions - Examples of an organisation’s footprints: direct and indirect emissions, An understanding of carbon emissions across a product/service lifecycle including: 1. Concept & design 2. Material extraction 3. Transport 4. Manufacture 5. Usage 6. Disposal, Carbon Footprint Calculators, Carbon Offsetting and Carbon Neutrality, Carbon trading. Establishing a continuous improvement framework for Green ICT including use of the ITIL Continual Service
Improvement Model. Understand the importance and risks, issues and opportunities around improving efficiency. Understand how best to re-use, recycle and dispose of IT assets.

**SEMESTER-III**

1. **Course Code: MCSC- 301,  
   Course Name: PATTERN RECOGNITION AND DATA MINING  
   Credit: 4**

   **Syllabus:** Introduction, Algorithmic models of learning, Learning classifiers, functions, relations, grammars, probabilistic models, value functions, behaviors and programs from experience. Bayesian, maximum a posteriori, and minimum description length frameworks. Parameter estimation, sufficient statistics, decision trees, neural networks, support vector machines, Bayesian networks, bag of words classifiers, N-gram models; Markov and Hidden Markov models, probabilistic relational models, association rules, nearest neighbor classifiers, locally weighted regression, ensemble classifiers. Computational learning theory, mistake bound analysis, sample complexity analysis, VC dimension, Occam learning, accuracy and confidence boosting. Dimensionality reduction, feature selection and visualization. Clustering, mixture models, k-means clustering, hierarchical clustering, distributional clustering. Reinforcement learning; Learning from heterogeneous, distributed, data and knowledge. Selected applications in data mining, automated knowledge acquisition, pattern recognition, program synthesis, text and language processing, internet-based information systems, human-computer interaction, semantic web, and bioinformatics and computational biology.

   Data Science : Statistical Thinking ,Examples ,Numerical Data, Summary Statistics ,From Population to Sampled Data, Different Types of Biases , Probability, Statistical Inference , Association and Dependence , Association and Causation ,Conditional Probability and Bayes Rule, Simpsons Paradox, Confounding ,Introduction to Linear Regression, Special Regression Models ,Exploratory Data Analysis and Visualization-Goals ,Graphs of Data, Graphs of Fitted Models, Graphs to Check Fitted Models, Principles of graphics. Apply basic machine learning algorithms (Linear Regression, k-Nearest Neighbors (k-NN), k-means, Naive Bayes) for predictive modeling. Bayesian Modeling- Bayesian inference: combining models and data in a forecasting problem, Bayesian hierarchical modeling for studying public opinion, Bayesian modeling for Big Data.


   **Lab:** Programming and implementation using R and HADOOP.
2. Course Code: MCSC-302,  
Course Name: THESIS/DISSERTATION - I,  
Credit: 4  
**Syllabus:** Students are expected to formulate a problem relevant to their area of specialisation, study the relevant literature and come out with an algorithm/software/implementation plan related to the problem formulated. Research Progress Seminar will be held twice a month for continuous evaluation.

3. **(For CyS)**  
Course Code: MCySC-301,  
Course Name: ETHICAL HACKING AND DIGITAL FORENSICS,  
Credit: 3  
**Syllabus:** Computer network and defense fundamentals • Network security threats, vulnerabilities, and attacks. **Overview of the Top 20 OWASP Security vulnerabilities. CVSS Scoring system including VAPT techniques** • Network security controls, protocols, and devices • Network security policy design and implementation • Physical security • Host security • Secure firewall configuration and management • Secure IDS configuration and management • Secure VPN configuration and management • Wireless network defense • Network traffic monitoring and analysis • Network risk and vulnerability management • Data backup and recovery • Network incident response and management, ethical hacking • Foot printing and reconnaissance • Scanning networks • Enumeration • Sniffing • System hacking • Malware threats • Social engineering • Denial of service • Session hijacking • Hacking web applications • SQL injection • Hacking wireless networks • Hacking web servers • Hacking mobile platforms • Evading IDS, Firewalls, and Honeypot.  
Computer forensics in today’s world • Computer forensics investigation process, Data Acquisition and Duplication • Understanding hard disks and file systems • Defeating anti-forensics techniques • Operating system forensics • Network forensics • Investigating web attacks • Database forensics • Cloud forensics • Malware forensics • Investigating email crimes • Mobile forensics process, Mobile OS architecture, boot process, and file systems, Mobile threats and security • Forensics report writing and presentation, encryption and stenography analysis. Investigation process: legal process of investigation, jurisdiction and agencies, internet investigation, ip address and domain names, investigation method, evidence collection. Legal Issues: Constitutional law, search and seizure guidelines, ECPA, challenges in process, international computer crime law.  
**Lab:** Practical implementation of theory classes on Introduction to Application Security: Injection Attacks, Broken Authentication and Session Management, Cross Site Scripting (XSS), Insecure Direct Object References, Security Misconfiguration, Sensitive Data Exposure, Missing Function Level Access Control, Cross Site Request Forgery, Using
Components with Known Vulnerabilities, Unvalidated Redirects and Forwards, LDAP attack, XML, HTTP attack using DVWA, METASPLOIT, WIRESHARK and other security tools.

Data Acquisition and Duplication in forensics --Understanding hard disks and file systems • Defeating anti-forensics techniques • Operating system forensics • Network forensics • Investigating web attacks • Database forensics using FDK, ENCASE, PASSWORD RECOVERY TOOLS.

3. **(For ICT)**

Course Code: MICTC-301,

Course Name: EMBEDDED SYSTEMS AND VLSI ALGORITHM DESIGN,

Credit: 3


**Lab:** 1. Design Entry and simulation of combinational logic circuits (8 bit adders, 4 bit multipliers, address decoders, multiplexers), Test bench creation, functional verification, and concepts of concurrent and sequential execution to be highlighted. 2. Design Entry and simulation of sequential logic circuits (counters, PRBS generators, accumulators). Test bench creation, functional verification, and concepts of concurrent and sequential execution to be highlighted. 3. Synthesis, P&R and Post P&R simulation for all the blocks. Concepts of FPGA
floor plan, critical path, design gate count, I/O configuration and pin assignment 4. Generation of configuration/fuse files for all the blocks/codes developed as part of Expt.1. and Expt. 2. FPGA devices must be configured and hardware tested for the blocks/codes. The correctness of the inputs and outputs for each of the blocks must be demonstrated at least on oscilloscopes (logic analyzer preferred). 5. Schematic Entry and SPICE simulation of MOS differential amplifier. Determination of gain, bandwidth, output impedance and CMRR. 6. Layout of a simple CMOS inverter, parasitic extraction and simulation. 7. Design of a 10 bit number controlled oscillator using standard cell approach, simulation followed by study of synthesis reports. 8. Automatic layout generation followed by post layout extraction and simulation of the circuit.

SEMESTER-IV

1. **Course Code:** MCSC-401,  
   **Course Name:** THESIS /DISSERTATION - II,  
   **Credit:** 14

   **Syllabus:** The students will continue to work on the problem identified in “Minor Project” (in Semester III) as per the work plan. The work is continued until all stated objectives and deliverables are met. Student will prepare a comprehensive report containing introduction to the problem, literature review, methodology, results and discussion and conclusion. Research Progress Seminar will be held twice a month for continuous evaluation. The result will be declared only after acceptance or publication of full length paper at least in peer reviewed Journal, International Conference or National Conference. The thesis grading shall be done as –

<table>
<thead>
<tr>
<th>S.No.</th>
<th>Grade</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>A+</td>
<td>Publication from thesis in SCI indexed journal.</td>
</tr>
<tr>
<td>3.</td>
<td>B+</td>
<td>Publication from thesis in proceeding of International conference which is SCI indexed.</td>
</tr>
</tbody>
</table>