This M.Tech programme aims to train the students in the cyber security discipline through a well-designed combination of courseware and its application on real-world scenarios. The programme has a strong emphasis on foundational course such mathematics for security application, advanced algorithms, networks etc., in addition to diverse subject core areas such as cryptography, operating systems and security, cloud security, security of cyber physical systems etc.

Students will be exposed to real-world problems, open-end problems and simulated real-life scenarios with active guidance from domain experts in this field. The programme will help the students to:

1. Comprehend the various security threats and vulnerabilities of the cyber world keeping in line with industrial trends.
2. Scale up to the demand from multiple industrial sectors on the cyber world to promote effective methods, practices and tools to counter the cyber crimes.
3. To be able to architect, design and implement fool-proof product line in the field of cyber security.

Ultimately this programme will yield next generation cyber security leaders who can be successfully employed in various sectors of industries, business firms, Government departments, financial bodies, educational institutions, etc, and these sectors generate huge demand for well-trained, professional people to be employed on cyber security front and they are always on the look-out for professionally trained people in the area of cyber security.
## CURRICULUM

### First Semester

<table>
<thead>
<tr>
<th>Course code</th>
<th>Type</th>
<th>Course title</th>
<th>L-T-P</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>18SN611</td>
<td>SC</td>
<td>Essentials of Cyber Security</td>
<td>0 0 3</td>
<td>3</td>
</tr>
<tr>
<td>18SN612</td>
<td>SC</td>
<td>Operating System and Security</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td>18SN601</td>
<td>FC</td>
<td>Practical Algorithms for Programmers</td>
<td>1 0 3</td>
<td>4</td>
</tr>
<tr>
<td>18SN613</td>
<td>SC</td>
<td>Network Security</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Elective -I</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>18HU601</td>
<td>HU</td>
<td>Amrita Values Program*</td>
<td></td>
<td>P/F</td>
</tr>
<tr>
<td>18HU602</td>
<td>HU</td>
<td>Career Competency I*</td>
<td></td>
<td>P/F</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Credits</strong></td>
<td></td>
<td><strong>18</strong></td>
</tr>
</tbody>
</table>

* Non-credit Course

### Second semester

<table>
<thead>
<tr>
<th>Course code</th>
<th>Type</th>
<th>Course title</th>
<th>L-T-P</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>18SN614</td>
<td>SC</td>
<td>Cryptography and Applications</td>
<td>4 0 0</td>
<td>4</td>
</tr>
<tr>
<td>18SN615</td>
<td>SC</td>
<td>Systems Security</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td>18SN616</td>
<td>SC</td>
<td>Cyber Forensics and Incident Response</td>
<td>2 0 1</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>E</td>
<td>Elective II</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>E</td>
<td>Elective III</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>18HU603</td>
<td>HU</td>
<td>Career Competency II</td>
<td>0 0 2</td>
<td>1</td>
</tr>
<tr>
<td>18RM600</td>
<td>SC</td>
<td>Research Methodology</td>
<td>2 0 0</td>
<td>2</td>
</tr>
<tr>
<td>18SN797</td>
<td>P</td>
<td>Live-in-Labs*</td>
<td></td>
<td>P/F</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Credits</strong></td>
<td></td>
<td><strong>20</strong></td>
</tr>
</tbody>
</table>

* Non-credit Course

### Third semester

<table>
<thead>
<tr>
<th>Course code</th>
<th>Type</th>
<th>Course title</th>
<th>L-T-P</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td></td>
<td>Elective IV</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>Elective V</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Course code</td>
<td>Type</td>
<td>Course title</td>
<td>L-T-P</td>
<td>Credits</td>
</tr>
<tr>
<td>-------------</td>
<td>------</td>
<td>--------------------------------------------------</td>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td>18SN798</td>
<td>P</td>
<td>Dissertation</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>16</td>
</tr>
</tbody>
</table>

**Fourth semester**

<table>
<thead>
<tr>
<th>Course code</th>
<th>Type</th>
<th>Course title</th>
<th>L-T-P</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>18SN799</td>
<td>P</td>
<td>Dissertation</td>
<td></td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>10</td>
</tr>
</tbody>
</table>

**Total credits: 64**

**List of courses**

**Foundation core**

<table>
<thead>
<tr>
<th>Course code</th>
<th>Type</th>
<th>Course title</th>
<th>L-T-P</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>18SN601</td>
<td>FC</td>
<td>Practical Algorithms for Programmers</td>
<td>1 0 3</td>
<td>4</td>
</tr>
</tbody>
</table>

**Subject Core**

<table>
<thead>
<tr>
<th>Course code</th>
<th>Type</th>
<th>Course title</th>
<th>L-T-P</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>18SN611</td>
<td>SC</td>
<td>Essentials of Cybersecurity</td>
<td>0 0 3</td>
<td>3</td>
</tr>
<tr>
<td>18SN612</td>
<td>SC</td>
<td>Operating System and Security</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td>18SN613</td>
<td>SC</td>
<td>Network Security</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td>18SN614</td>
<td>SC</td>
<td>Cryptography and Applications</td>
<td>3 0 0</td>
<td>3</td>
</tr>
<tr>
<td>18SN615</td>
<td>SC</td>
<td>Systems Security</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td>18SN616</td>
<td>SC</td>
<td>Cyber Forensics and Incident Response</td>
<td>2 0 1</td>
<td>3</td>
</tr>
</tbody>
</table>

**Electives**

<table>
<thead>
<tr>
<th>Course code</th>
<th>Course title</th>
<th>L-T-P</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>18MA612</td>
<td>Mathematical Foundations for Cyber Security</td>
<td>3 0 0</td>
<td>3</td>
</tr>
<tr>
<td>18SN701</td>
<td>Distributed Systems and Security</td>
<td>3 0 0</td>
<td>3</td>
</tr>
<tr>
<td>Course Code</td>
<td>Course title</td>
<td>L</td>
<td>T</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------------------------------------</td>
<td>----</td>
<td>----</td>
</tr>
<tr>
<td>18SN702</td>
<td>Security in the Cloud</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>18SN703</td>
<td>Formal Methods</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>18SN704</td>
<td>Security of Cyber Physical Systems</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>18SN705</td>
<td>Android Internal Security</td>
<td>201</td>
<td></td>
</tr>
<tr>
<td>18SN706</td>
<td>Advanced Network Security</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>18SN707</td>
<td>Mobile Computing and Security</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>18SN708</td>
<td>Malware Analysis</td>
<td>201</td>
<td></td>
</tr>
<tr>
<td>18SN709</td>
<td>SCADA Network Security</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>18SN710</td>
<td>Software Protection</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>18SN711</td>
<td>Security of Internet of Things</td>
<td>102</td>
<td></td>
</tr>
<tr>
<td>18SN712</td>
<td>Digital Systems Security</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>18SN713</td>
<td>Introduction to Software Reverse Engineering</td>
<td>201</td>
<td></td>
</tr>
<tr>
<td>18SN714</td>
<td>Wireless Security</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>18SN715</td>
<td>Database and Web Application Security</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>18SN716</td>
<td>Data Analytics for Security</td>
<td>201</td>
<td></td>
</tr>
<tr>
<td>18SN717</td>
<td>Blockchains and Cryptocurrencies</td>
<td>201</td>
<td></td>
</tr>
<tr>
<td>18SN718</td>
<td>Cybersecurity Governance</td>
<td>300</td>
<td></td>
</tr>
<tr>
<td>18SN719</td>
<td>Software Defined Networking and Security</td>
<td>1-0-2</td>
<td></td>
</tr>
</tbody>
</table>

Project Work

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course title</th>
<th>L</th>
<th>T</th>
<th>P</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>18SN798</td>
<td>Dissertation</td>
<td></td>
<td></td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>18SN799</td>
<td>Dissertation</td>
<td></td>
<td></td>
<td></td>
<td>12</td>
</tr>
</tbody>
</table>
Linux: Install Linux using a VM. Installing softwares in linux using apt, Using the shell, changing passwords, resetting password from GRUB, password protecting GRUB, installing mysql on docker, connecting to other linux machines using SSH, configuring passwordless login using SSH, verifying file integrity
IPtables: Configuring iptables, exercises using iptables (blocking a particular service, blocking a particular port, whitelisting, blocking IP from a certain country)
Cookie Stealing Lab: Locating cookies in file system, Install firebug plugin to export cookie and importing it in another machine, automating cookie stealing using python.
Secure Email using gpg: Setting up gpg keys, securing email using gpg
Openssl Lab: Encryption and decryption using openssl
Information Gathering: Enumerating Ports, SMB, SMTP, SNMP; Using Shodan.io to scan IoT devices; Vulnerability scanning using OpenVAS
Metasploit: Installing and setting up, MSF, Payloads, Exploiting using Metasploit
Password Cracking: Dictionary attack, Keyspacebruteforce, using online tools (Ncrack, Hydra), Password hash attacks
Capture the Flag exercises: Basic exercises in Crypto, Reverse Engineering, forensics and exploitation using InCTFj


Knapsack problem - Coin Change problem. Greedy algorithms: Fractional knapsack, job
scheduling, matroids. Graph Algorithms - Graph Traversal, Single-Source Shortest Paths,
All pairs Shortest Paths, Depth First Search, Breadth First Search and their applications,
Flow– Cuts - Maximum Bipartite Matching - Graph partitioning via multi-commodity flow,
Karger'r Min Cut Algorithm. Amortized Analysis - Aggregate Method - Accounting Method

TEXT BOOKS/ REFERENCES:

   and Internet Examples”, John Wiley and Sons, 2002
2. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest and Clifford Stein,
   McGraw-Hill, 2009

18SN613       NETWORK SECURITY       3-0-1-4

Introduction - Overview of computer networks and network security
Application layer - Overview of HTTP, FTP, SMTP and DNS and socket programming.
Weaknesses, vulnerabilities and attacks against above protocols - hijacking, spoofing and
Application layer security - Goals, cryptography primitives and principles, TLS - Objectives,
protocol, working and features, PGP: Overview, objective, working, features and limitations.
Transport layer - Introduction, objectives, unreliable data transfer and UDP, general
principles of reliable data transfer, TCP: Overview, reliable data transfer, flow control,
congestion control. Attacks against transport layer protocols: UDP flooding, TCP spoofing,
TCP connection hijacking, TCP SYN flood.
Network layer – Addressing schemes(IPv4 and IPv6), Forwarding and routing in Internet,
Routing algorithms, Routing protocols in Internet(OSPF, RIP and BGP), BGP security,
ICMP, NAT, IPSec – Introduction, Tunnel and Transfer Modes, IPSec Authentication
Header, Encapsulating Security Header and Payload, IPSec Key Exchange and VPNs.
Link layer - Introduction and services, Link layer addressing, Multiple Access Protocols,
Ethernet, ARP, Attacks against and vulnerabilities in ARP.

TEXTBOOKS/ REFERENCES:

   Asia, 2002.
   Hall, 2011.

18SN614 CRYPTOGRAPHY AND APPLICATIONS 4-0-0-4

Unit 1: Concepts of Number Theory: Number Theory, GCD, Euclidean algorithm, Extended Euclidean algorithm, prime numbers, congruence’s, how to solve congruence equations, Chinese remainder theorem, residue classes and complete residue systems, Euler Fermat theorem, primitive roots.

Unit 2: Symmetric Key Cryptographic Systems: Caesar and affine ciphers, mono-alphabetic substitutions, transposition, homomorphic, Vigenere and Beaufort ciphers, one-time pad, product/iterated/block ciphers, DES and AES. Heavy discussion is given to the security of these ciphers, not only are they studied in an algorithm sense but their attacks and defences are also discussed.

Unit 3: Cryptanalysis of symmetric keys- Attack Models, Linear, Differential and various others such as meet-in-the-middle attack.

PKCS- Concepts of PKCS, Diffie Hellman key-exchange protocol, RSA, Rabin and ElGamal cryptosystems, primarily testing, pollard rho factorisation, man-in-the-middle attack.


Unit 5: Hash Functions and MACs- Hash functions: the Merkle-Damgard construction, Message Authentication Codes, security of Hash functions, security weakness of MD4, MD5, SHA1,SHA2 and construction of SHA3, identification protocols, authenticated key exchange and SSL/TLS session setup, Zero knowledge protocols.

Unit 6: Basic elliptic curve cryptography: definition, mathematical formulation of them, elliptic curve cryptography and pairings, introduction to quantum computers and the future of cryptography.

TEXTBOOKS/REFERENCES:

18SN615 SYSTEMS SECURITY 3-0-1-4


**TEXT BOOKS/ REFERENCES:**

2. James C. Foster and Vincent T. Liu, “*Writing Security Tools and Exploits*”, Syngress Publishing

**18SN616 CYBER FORENSICS AND INCIDENT RESPONSE 2-0-1-3**


**TEXTBOOKS/ REFERENCES:**


**18MA612 MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY SYSTEMS 3-0-0-3**

Logic, Mathematical reasoning, Sets, Basics of counting, Relations.

Graph Theory: Euler graphs, Hamiltonian paths and circuits, planar graphs, trees, rooted and binary trees, distance and centres in a tree, fundamental circuits and cut sets, graph
colorings and applications, chromatic number, chromatic partitioning, chromatic polynomial, matching, vector spaces of a graph.

Analytic Number Theory: Euclid’s lemma, Euclidean algorithm, basic properties of congruences, residue classes and complete residue systems, Euler-Fermat theorem, Lagrange’s theorem and its applications, Chinese remainder theorem, primitive roots. Algebra: groups, cyclic groups, rings, fields, finite fields and their applications to cryptography.

Linear Algebra: vector spaces and subspaces, linear independence, basis and dimensions, linear transformations and applications.

Probability and Statistics: introduction to probability concepts, random variables, probability distributions (continuous and discrete), Bayesian approach to distributions, mean and variance of a distribution, joint probability distributions, theory of estimation.


TEXTBOOKS / REFERENCES:
4. N. Deo, “Graph theory with applications to Engineering and Computer Science”, Prentice Hall of India, New Delhi, 1974.

18RM600 RESEARCH METHODOLOGY 2-0-0-2

Unit I:

Unit II:
Problem Formulation, Understanding Modeling & Simulation, Conducting Literature Review, Referencing, Information Sources, Information Retrieval, Role of libraries in Information Retrieval, Tools for identifying literatures, Indexing and abstracting services, Citation indexes
Unit III:
Experimental Research: Cause effect relationship, Development of Hypothesis, Measurement Systems Analysis, Error Propagation, Validity of experiments, Statistical Design of Experiments, Field Experiments, Data/Variable Types & Classification, Data collection, Numerical and Graphical Data Analysis: Sampling, Observation, Surveys, Inferential Statistics, and Interpretation of Results

Unit IV:
Preparation of Dissertation and Research Papers, Tables and illustrations, Guidelines for writing the abstract, introduction, methodology, results and discussion, conclusion sections of a manuscript. References, Citation and listing system of documents

Unit V:

TEXTBOOKS/ REFERENCES:


18SN701 DISTRIBUTED SYSTEMS AND SECURITY 3-0-0-3


TEXTBOOKS/ REFERENCES:

18SN702 SECURITY IN THE CLOUD 3-0-0-3

Introduction to cloud computing:- Evolution of cloud computing, Definition of cloud computing, NIST reference model, Service delivery model, Deployment models, Benefits and challenges of cloud adoption, Introduction to popular cloud platforms, Virtualization, Containers


Advanced Security Concepts:- Trustworthy cloud infrastructures, Differential privacy, Secure computations, High-availability and integrity layer for cloud storage, Homomorphic encryption, Malware and cloud, Cloud forensics.

Cloud-centric regulatory compliance issues and mechanisms

TEXT BOOKS / REFERENCES:

18SN703 FORMAL METHODS 3-0-0-3


properties, Process Algebra: CCS and Pi-calculus, Reductions and labelled transitions, Harmony lemma, Bisimulations.

**TEXTBOOKS / REFERENCES:**


**18SN704 SECURITY OF CYBERPHYSICAL SYSTEMS 3-0-0-3**


**TEXTBOOKS / REFERENCES:**


**18SN705 ANDROID INTERNALS AND SECURITY 2-0-1-3**


TEXT BOOKS/REFERENCES:
4. Adapted Materials from Android development sites.

18SN706 ADVANCED NETWORK SECURITY 3-0-0-3

Application Security – Introduction – Overview of Attacks Against Applications, AttackingSUID Programs, Environment Attacks, Input Argument Attacks, File Access Attacks, Smashing the Stack for Fun and Profit, Format String Attacks, Assembly Primer, ELF File Format, PLT and GOT, Data and BSS Overflow, Array Overflow, Non-terminated String Overflow, Heap Overflow, Tools and Defenses


TEXT BOOKS/REFERENCES:
4. Larry L. Peterson, Bruce S. Davie, Computer Networks: A Systems Approach

18SN707 MOBILE COMPUTING AND SECURITY 3-0-0-3


TEXTBOOK AND REFERENCES:
2. This will be a research paper based course. Students are expected to read, summarize and discuss assigned research papers in the field for each class.

18SN708 MALWARE ANALYSIS 2-0-1-3


TEXTBOOKS/REFERENCES:

TEXT BOOKS / REFERENCES:


TEXTBOOKS/ REFERENCES:

**TEXT BOOKS / REFERENCES:**


**18SN712 DIGITAL SYSTEMS SECURITY 3-0-0-3**


**TEXT BOOKS / REFERENCES:**


**18SN713 INTRODUCTION TO SOFTWARE REVERSE ENGINEERING 2-0-1-3**
Introduction, ethical and legal aspects of reverse engineering, low level assembly programming, identify common techniques and approaches for basic reverse engineering, disassembler and debugger aided debugging, reverse engineering high level languages, identifying and defeating anti-disassembly techniques, anti-debugging techniques, anti-VM techniques and code obfuscation, introduction to techniques used by malware, analysing and reversing windows executables, reverse engineering higher level languages (Python, Java and .Net bytecode).

**TEXT BOOKS / REFERENCES:**


**18SN714 WIRELESS SECURITY 3-0-0-3**


**TEXT BOOKS/REFERENCES:**


**18SN715 DATABASE AND WEB APPLICATION SECURITY 3-0-0-3**

Database security – Introduction includes threats, vulnerabilities and breaches, Basics of database design, DB security – concepts, approaches and challenges, types of access controls, Oracle VPD, Discretionary and Mandatory access control – Principles, applications and poly-instantiation, Database inference problem, types of inference attacks, distributed database, security levels, SQL-injection: types and advanced concepts. Security in relational data model, concurrency controls and locking, SQL extensions to security (oracle as an example), System R concepts, Context and control based access control, Hippocratic databases, Database watermarking, Database intrusion, Secure data outsourcing, Web application security, Basic principles and concepts, Authentication, Authorization, Browser security principles;
XSS and CSRF, same origin policies, File security principles, Secure development and deployment methodologies, Web DB principles, OWASP – Top 10 - Detailed treatment, IoT security – OWASP Top 10 – Detailed treatment, Mobile device security – Introduction, attack vector and models, hardware centric security aspects, SMS / MMS vulnerabilities, software centric security aspects, mobile web browser security, Application security – Concepts, CIA Triad, Hexad, types of cyber attacks, Introduction to software development vulnerabilities, code analyzers – Static and dynamic analyzers, Security testing / Penetration testing – Principles and concepts, PT work flows and examples, blind tests, ethical hacking techniques, synthetic transactions, interface testing and fuzzing, SDLC phases and security mandates

**TEXTBOOKS/ REFERENCES:**


**18SN716 DATA ANALYTICS FOR SECURITY 2-0-1-3**

Introduction: Introduction to Information Security, Introduction to Data Mining for Information Security


**TEXTBOOKS / REFERENCES:**


18SN717 BLOCKCHAINS AND CRYPTOCURRENCIES 3-0-0-3


TEXTBOOKS / REFERENCES:
1. Bitcoin and Cryptocurrency Technologies by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder
2. Mastering Bitcoin by Andreas Antonopoulos

18SN718 CYBERSECURITY GOVERNANCE 3-0-0-3


TEXTBOOKS / REFERENCES:

18SN719 SOFTWARE DEFINED NETWORKING AND SECURITY 1-0-2-3


TEXTBOOKS / REFERENCES:

2. SDN: Software Defined Networks, An Authoritative Review of Network Programmability Technologies, By Thomas D. Nadeau, Ken Gray Publisher: O'Reilly Media, August 2013,