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

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

1. Comprehend the various security threats and vulnerabilities of the cyber world keeping in line with the 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 lines 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</th>
<th>LTP</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>MA619</td>
<td>FC</td>
<td>Advanced Discrete Mathematics</td>
<td>4 0 0</td>
<td>4</td>
</tr>
<tr>
<td>SN620</td>
<td>SC</td>
<td>Operating System and Security</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td>SN629</td>
<td>FC</td>
<td>Algorithmic Fundamentals for Security</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td>SN624</td>
<td>FC</td>
<td>Advanced Computer Networks and Internet Architectures</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td>SN627</td>
<td>SC</td>
<td>Principles of Cryptography</td>
<td>3 0 0</td>
<td>3</td>
</tr>
<tr>
<td>WN605</td>
<td>SC</td>
<td>Advanced Computer Programming</td>
<td>0 0 1</td>
<td>1</td>
</tr>
<tr>
<td>HU601</td>
<td>HU</td>
<td>Cultural Education*</td>
<td></td>
<td>P/F</td>
</tr>
</tbody>
</table>

Credits: 20

*Non-credit course

### Second Semester

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>LTP</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>MA609</td>
<td>FC</td>
<td>Linear Algebra and Random Process</td>
<td>4 0 0</td>
<td>4</td>
</tr>
<tr>
<td>CS622</td>
<td>FC</td>
<td>Parallel and Distributed Systems</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td>SN623</td>
<td>SC</td>
<td>Advanced Security of Networked Systems</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>Elective–I</td>
<td>3 0 0</td>
<td>3</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>Elective–II</td>
<td>3 0 0</td>
<td>3</td>
</tr>
<tr>
<td>EN600</td>
<td>HU</td>
<td>Technical Writing*</td>
<td></td>
<td>P/F</td>
</tr>
</tbody>
</table>

Credits: 18

*Non-credit course

### Third Semester

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>LTP</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>SN621</td>
<td>SC</td>
<td>Database and Application Security</td>
<td>2 0 1</td>
<td>3</td>
</tr>
<tr>
<td>E</td>
<td></td>
<td>Elective –III</td>
<td>3 0 0</td>
<td>3</td>
</tr>
<tr>
<td>SN796</td>
<td>P</td>
<td>Live-in-Labs</td>
<td></td>
<td>P/F</td>
</tr>
<tr>
<td>SN797</td>
<td>P</td>
<td>Practical Capture the Flag Exercises</td>
<td></td>
<td>P/F</td>
</tr>
<tr>
<td>SN799</td>
<td>P</td>
<td>Dissertation</td>
<td></td>
<td>10</td>
</tr>
</tbody>
</table>

Credits: 16

### Fourth Semester

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Type</th>
<th>Course</th>
<th>LTP</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>SN799</td>
<td>P</td>
<td>Dissertation</td>
<td></td>
<td>12</td>
</tr>
</tbody>
</table>

Credits: 12

Total Credits: 66
## List of Courses

### Foundation Core

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course</th>
<th>LTP</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>MA619</td>
<td>Advanced Discrete Mathematics</td>
<td>4 0 0</td>
<td>4</td>
</tr>
<tr>
<td>MA609</td>
<td>Linear Algebra and Random Process</td>
<td>4 0 0</td>
<td>4</td>
</tr>
<tr>
<td>SN629</td>
<td>Algorithmic Fundamentals for Security</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td>SN624</td>
<td>Advanced Computer Networks and Internet Architectures</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td>CS622</td>
<td>Parallel and Distributed Systems</td>
<td>3 0 1</td>
<td>4</td>
</tr>
</tbody>
</table>

### Subject Core

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course</th>
<th>LTP</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>SN620</td>
<td>Operating System and Security</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td>SN621</td>
<td>Database and Application Security</td>
<td>2 0 1</td>
<td>3</td>
</tr>
<tr>
<td>SN623</td>
<td>Advanced Security of Networked Systems</td>
<td>3 0 1</td>
<td>4</td>
</tr>
<tr>
<td>WN605</td>
<td>Advanced Computer Programming</td>
<td>0 0 1</td>
<td>1</td>
</tr>
<tr>
<td>SN627</td>
<td>Principles of Cryptography</td>
<td>3 0 0</td>
<td>3</td>
</tr>
</tbody>
</table>

### Electives

#### Elective-I

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course</th>
<th>LTP</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>SN701</td>
<td>Security in the Cloud</td>
<td>3 0 0</td>
<td>3</td>
</tr>
<tr>
<td>SN702</td>
<td>Formal Methods</td>
<td>3 0 0</td>
<td>3</td>
</tr>
<tr>
<td>SN717</td>
<td>Fundamentals of Data Science and Applications</td>
<td>2 0 1</td>
<td>3</td>
</tr>
</tbody>
</table>

#### Elective-II

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course</th>
<th>LTP</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>SN705</td>
<td>Security of Cyber Physical Systems</td>
<td>3 0 0</td>
<td>3</td>
</tr>
<tr>
<td>SN706</td>
<td>Wireless Security</td>
<td>3 0 0</td>
<td>3</td>
</tr>
<tr>
<td>SN710</td>
<td>Principles of Machine Learning</td>
<td>3 0 0</td>
<td>3</td>
</tr>
<tr>
<td>SN716</td>
<td>Mobile Computing Security</td>
<td>3 0 0</td>
<td>3</td>
</tr>
</tbody>
</table>

#### Elective-III

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course</th>
<th>LTP</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>SN709</td>
<td>Cyber Crimes, Cyber Laws and Cyber Forensics</td>
<td>3 0 0</td>
<td>3</td>
</tr>
<tr>
<td>SN713</td>
<td>Software Protection</td>
<td>3 0 0</td>
<td>3</td>
</tr>
<tr>
<td>SN718</td>
<td>Advanced Data Science for Security Analysis</td>
<td>2 0 1</td>
<td>3</td>
</tr>
</tbody>
</table>

### Project Work

<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course</th>
<th>LTP</th>
<th>Cr</th>
</tr>
</thead>
<tbody>
<tr>
<td>SN796</td>
<td>Live-in-Labs</td>
<td>P/F</td>
<td></td>
</tr>
<tr>
<td>SN797</td>
<td>Practical Capture the Flag Exercises</td>
<td>P/F</td>
<td></td>
</tr>
<tr>
<td>SN799</td>
<td>Dissertation</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>SN799</td>
<td>Dissertation</td>
<td>12</td>
<td></td>
</tr>
</tbody>
</table>
DETAILED SYLLABUS

MA619  ADVANCED DISCRETE MATHEMATICS    4-0-0- 4

Logic, Mathematical reasoning, Sets, Basics of counting, Relations
Graph Theory: Euler graphs, Hamiltonian Paths and circuits, Planar graphs, Trees, Shortest path algorithms, Rooted and binary trees, Distance and centres in a tree, Fundamental circuits and cut sets, Connectivity and separability, Network flows, dominating sets, domination number, 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, Reduced residue systems and the Euler –Fermat theorem, simultaneous linear congruences, Lagrange’s theorem and its applications, Wilson’s theorem, Chinese remainder theorem, applications of the Chinese remainder theorem, primitive roots and reduced residue systems.
Algebra: Groups, subgroups, cyclic groups, abelian groups, permutation groups, group homomorphism, normal subgroups, rings, ideal, ring homomorphism, Fields, Finite fields and their applications to cryptography.

TEXTBOOKS/REFERENCES:

5. N. Deo, Graph Theory with Applications to Engineering and Computer Science, Prentice Hall of India, New Delhi, 1974.

SN620  OPERATING SYSTEM AND SECURITY    3-0-1- 4

OS Processes, Synchronization, Memory Management, File Systems
Multics – Multics system, Multics security, Multics vulnerability analysis
Security in Ordinary OS – Unix, Windows,
Verifiable security goals – Information flow, Denning's Lattice model, Bell-Lapadula model, Biba integrity model, Covert channels.
Security Kernels – Secure Communications processor, Securing Commercial OS
Secure Capability Systems – Fundamentals, Security, Challenges
Secure Virtual Machine Systems
Case study - Linux kernel, Android, DVL, Solaris Trusted Extensions
TEXTBOOKS/REFERENCES:


SN629 ALGORITHMIC FUNDAMENTALS FOR SECURITY 3-0-1-4

Asymptotic Notation and Recurrences: Asymptotic Notation, Recurrences and their solutions, Master’s theorem, amortized analysis. Review of combinatorics. Introduction to amortized analysis.
Sorting and searching with corresponding analyses: Bubble sort, Insertion sort, merge sort, quick sort and binary search.
Graph algorithms: BFS, DFS, topological sort, SCC, MST (greedy), SSSP: Dijkstra’s and Bellman Ford, APSP (DP). Data structures for disjoint sets.
Greedy technique: Fractional Knapsack, activity selection. Divide-and-Conquer technique: Strassen’s algorithm for matrix multiplication, maximum sub-array problem, linear time median. Dynamic programming technique. LC subsequence/substring, 0-1 knapsack, Floyd’s APSP, matrix chain multiplication, maximum sub-array problem, rod cutting, party planning, bitonic TSP.
Number Theory: Preliminaries, Euclid’s algorithm and extended Euclid’s algorithm. Introduction to string matching algorithms.
Introduction to NP-Completeness. P, NP, NP-hard, NP-complete, polynomial time reductions. Approximation algorithms: Vertex cover, TSP with triangle inequality etc..

TEXTBOOKS/REFERENCES:


SN624 ADVANCED COMPUTER NETWORKS AND INTERNET ARCHITECTURES 3-0-1-4

OSI Layer introduction, Switching topologies
Introduction to Wireless Networks – Wireless LAN technology, Network layer – Internet Addresses, ARP, RARP, IP, Routing algorithm – Interior and Exterior routing. ICMP, Classless and Subnet Address Extensions (CIDR), Internet Multicasting. NAT Routing protocol design and architectures for RIP, OSPF, BGP, RIP- Algorithm of routing, Split horizon, Poison reverse etc., OSPF- OSPF neighbor establishment, database creations,
multiple network types, NBMA, Virtual link scenarios, ABR, ASBR, LSA, Stubby networks etc. BGP-EBGP, IBGP, Mandatory BGP attributes, Next-hop self interactions across ASes, routing loop avoidance, best path selection algorithm TCP and Congestion Control Mechanisms. Quality of service: Quality of Service models, IPP, DiffServ models, dot1p bits, scheduling of traffic. Traffic distribution models and benefits. Internet Architectures- Flow of traffic and routing behavior within Internet, Application of Qos models, application of new resilient designs. Understanding of control and data planes in high end Internet core routers, CEF, hardware packet flows. MPLS, labels, label stacking, packet analysis, RSVP, label allocation, distribution models. MPLS-VPNs- Detailed understanding of MPLS L3 VPNS, routing model employed, forwarding of mplsvpn packets, VRF tables, application scenarios. Implementation in global service provider networks. SocketLevelprogramming,RPC,HighlevelnetworkingusingJava/Python

TEXTBOOKS/REFERENCES:


SN627 PRINCIPLES OF CRYPTOGRAPHY 3-0-0-3


TEXTBOOKS/REFERENCES:


**WN605 ADVANCED COMPUTER PROGRAMMING 0-0-1-1**

Programming in C, Basic Computer Organization and Architecture, Build and Compilation process, Debugging concepts, Data Types and Variables, Input/Output implementation and usage, Control flow, Modular Programming with functions, Stack Frames and Activation Records, Arrays, Pointers, Strings, Structures, Implementation of Structures, Memory, Stacks, Recursion, Dynamic Memory Allocation, Heap, Program Runtime Analysis, Big-Oh Notation.

Significant labs, e.g., Spell Checker with a real dictionary, complicated data structure such as a Vector/Set, Customer Relationship Management system, custom string Abstract Data Type, Maze, etc.

**TEXT BOOKS/REFERENCES:**

**MA609 LINEAR ALGEBRA AND RANDOM PROCESS 4-0-0-4**

Linear Algebra: Review of Matrices, Geometry of linear equations, Vectors and subspaces, Linear independence, basis and dimensions, Linear transformations, Applications of linear transformations, inner product space, orthogonality, Gram Schmidt orthogonalization process, projections and least squares 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, twodimensional random variables and joint probability distributions, stochastic independence of random variables.

Theory of estimation, Bayesian methods of estimation, construction of test statistics, critical region, p-value.

Random Processes: general concepts, definitions, systems with stochastic inputs, power spectrum, discrete-time processes, random walks and other applications, ergodicity, Markov chains, transition probabilities, classification of states, transient and absorption probabilities.

**TEXTBOOKS/REFERENCES:**

**CS622 PARALLEL AND DISTRIBUTED SYSTEMS 3-0-1-4**

Introduction: Basics of parallelization and parallelization strategies. Parallel/distributed programming models and interfaces - shared memory vs. message passing vs. remote procedure call (RPC) vs. global address space languages: e.g., pthreads, MPI, MapReduce, OpenMP, HPF, UPC, language-level threads (e.g., Java). Parallel machine architectures - shared and distributed memory machines, multicore and multithreaded chips, interconnection networks. Parallel program optimization techniques - synchronization granularity, dependences, scheduling, load balancing. Synchronization - hardware primitives, logical and physical clocks, mutual exclusion, distributed transactions, transactional memory. Consistency and coherence - data-centric versus client-centric consistency models, cache coherence protocols. Fault tolerance and reliability - fail-stop versus byzantine failure models, two- and three-phase commits, reliable group communication, check pointing, message logging.

**TEXTBOOKS/REFERENCES:**


**SN623 ADVANCED SECURITY OF NETWORKED SYSTEMS 3-0-1-4**


TEXT BOOKS/REFERENCES:


EN600 TECHNICAL WRITING P/F


TEXTBOOKS/REFERENCES:


SN621 DATABASE AND APPLICATION SECURITY 2-0-1-3

Database security – Introduction includes threats, vulnerabilities and breaches
Application security – Concepts, CIA Triad, Hexad, types of cyber attacks. Discretionary and Mandatory access control – Principles and applications
Basics of database design: ACID, transaction management and query processing, basic querying tools, data types, integrity constraints and fault tolerance. Database inference problem, distributed database, security levels.
Software development vulnerabilities, code analyzers – Static and dynamic analyzers.
Security in relational data model, concurrency controls and locking.
DB authorization policies, RBAC – concepts and applications, biometric DB authorization, concepts of DB audit. SQL extensions to security with Oracle as an example. MAC Concepts and multi-level secure data base concepts, Polyninstantiation
System R concepts, Context and control based access control, Oracle VPD
Privacy preservation, anonymization and Hippocratic databases: Principles and architecture.
Inference – An in-depth treatment, types of inference attacks
Biometric security concepts. XML security, Multi-level object DB security.
Security in data warehouses and OLAP systems. Database watermarking – Concepts and copyright protection. Managing and querying encrypted data
DB issues in trust management and trust negotiation

TEXTBOOKS/ REFERENCES:


SN701 SECURITY IN THE CLOUD 3-0-0- 3

Introduction to cloud computing- Evolution of cloud computing, Definition of cloud computing, SPI framework, Service delivery model, Deployment models, Key drivers to adopting the cloud, Barriers to cloud computing adoption in the cloud, Modular arithmetic background, concepts of security, how to assess security of a system, information theoretic security v/s computational security, Data security and storage in cloud, data dispersal techniques, High-availability and integrity layer for cloud storage, Encryption and key management in the cloud, Cloud forensics, Data location and availability, Data security tools and techniques for the cloud, Data distribution and information dispersal techniques, Data encryption/decryption methodologies and algorithms for a client-server setup such as SSL, IPSec, etc., Introduction to Homomorphic encryption. Approximate string searching over encrypted data stored in the cloud, Trustworthy cloud infrastructures, Secure computations, Cloud related regulatory and compliance issues.

TEXTBOOKS/REFERENCES:

SN702  
FORMAL METHODS  
3-0-0- 3

Background: Computability and Complexity  
Decidability, Semi-decidability, Undecidability, Halting problem, Rice's theorem  
Overview of complexity classes: P, NP, NP-completeness.  
Propositional and First-Order Logic: Syntax, Semantics, Proof methods  
Program Verification: Floyd-Hoare logic, Weakest Pre-conditions; Partial Correctness and Termination  
Structural induction and Fixed-point induction for recursive procedures  
Data refinement in Z abstract data types: Forward and backward simulation, Concurrent  
Programs and Correctness Properties: Owick-Gries, Assume-Guarantee  
Reactive Systems: Transformational vs Reactive systems, Temporal Logic: Linear (LTL) and Branching Time (CTL), Temporal specification of reactive systems: Safety, Liveness, Fairness, Buchi automata, LTL-to-Buchi automata, Properties: containment, emptiness  
Model Checking: LTL and CTL model-checking. Analysis of model-checking algorithms  
Symbolic model checking; overview of state-space reduction methods, Case study and practical verification of properties  
Process Algebra: CCS and Pi-calculus, Reductions and labelled transitions, Harmony lemma, Bisimulations

TEXTBOOKS/REFERENCES:


SN705  
SECURITY OF CYBER PHYSICAL SYSTEMS  
3-0-0- 3


TEXTBOOKS/REFERENCES:


TEXT BOOKS/REFERENCES:


SN709  CYBER CRIMES, CYBER LAWS AND CYBER FORENSICS  3-0-0- 3

Introduction to IT laws & Cyber Crimes – India and International perspectives, Governance and Legal Issues.

TEXTBOOKS/REFERENCES:

Role of learning in intelligent behavior, designing a learning system; learning from example; concept learning, Bayesian decision theory, Bayesian Learning, Decision tree learning; Univariate Trees, Classification Trees, Regression Trees, Rule Extraction from Trees, Learning Rules from Data, linear discrimination, SVMs: linear SVMs, introduction to kernel methods, multilayer perceptrons, Local models, Competitive Learning, Incorporating Rule-Based Knowledge, Computational Learning Theory, Instance-based Learning, Learning sets of Rules, Analytical Learning, Boosting algorithms, Combining multiple learners, Reinforcement Learning.

TEXTBOOKS/REFERENCES:


SN 713 SOFTWARE PROTECTION 3-0-0-3

Offensive and Defensive strategies - Offense – Motivation, Methods of attacking software protection. Defense: Methods for hiding information, purpose, algorithms in software.
Program Analysis Static analysis: Control flow analysis, data flow analysis, dependence analysis.
Dynamic analysis: Debugging, tracing, profiling, emulation.
Static Code obfuscation - In-depth Semantics preserving obfuscating transformations, complicating control flow, opaque predicates, data encoding, breaking abstractions.
Obfuscation - Theoretical Bounds Various impossibility results.
Tamper roofing and Watermarking Definitions, Algorithms for Tamperproofing, Remote Tamperproofing.
Software Similarity Analysis: Alternate methods for defeating obfuscations. K-gra bounding analysis, API-Based analysis, Tree-based Analysis, Graph-Based analysis, Metrics-Based Analysis.

TEXTBOOKS/REFERENCES:


SN 716 MOBILE COMPUTING AND SECURITY 3-0-0-3

Introduction to Mobile Computing: Mobile Computing Models, Design and Implementation, Mobile Architecture, Service Discovery protocol, Mobile P2P systems,

TEXTBOOKS / REFERENCES:


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.

SN 717 FUNDAMENTALS OF DATA SCIENCE AND APPLICATIONS 2-0-1-3

Data Stores - Introduction to Structured Data, DBMS Concepts, RDBMS (Oracle/MySQL), NoSQL Concepts, Mongo, Cassandra, Basic to complex Querying in SQL. (Lab Element), Query tuning., Introduction to Unstructured Data, Taming Unstructured Data. Understanding Data - Understanding data formats (XML, JSON, YAML, PMML), Data feeds (RSS, Atom, RDF), Preparing Data - Data Analysis/Profiling, Data Cleansing.
Introduction to Streaming Data Analytics, Introduction to Spark, Introduction to Storm, Introduction to Scala.

TEXTBOOKS/REFERENCES:


SN 718 ADVANCED DATA SCIENCE FOR SECURITY ANALYSIS 2-0-1-3

Big Data Warehouse - Hadoop Ecosystem, HBase, Pig & Pig Latin, Sqoop, ZooKeeper, Hue, Hive, Flume, Oozie
Security Concerns in Big data, Visualization techniques in Big Data Analytics, Case Study & Implementation

TEXTBOOKS/REFERENCES: