# M. TECH. (CYBER FORENSIC & INFORMATION SECURITY/CYBER SECURITY)

## COURSE STRUCTURE AND SYLLABUS

### I Year I Semester

<table>
<thead>
<tr>
<th>Code</th>
<th>Group</th>
<th>Subject</th>
<th>L</th>
<th>T/P/D</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Mathematical Foundation for Cyber Security</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Applied Cryptography</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network and Wireless Security</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Biometric Systems and Biometric Image Processing</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Elective -I</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Distributed and Cloud Computing</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information Storage Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information Systems Audit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Elective -II</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>IT Security Metrics</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Web Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Distributed Systems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lab</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Seminar</td>
<td>-</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total</td>
<td>18</td>
<td>3</td>
<td>22</td>
</tr>
</tbody>
</table>

### I Year II Semester

<table>
<thead>
<tr>
<th>Code</th>
<th>Group</th>
<th>Subject</th>
<th>L</th>
<th>T/P/D</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Software Vulnerability Analysis</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intrusion Detection and Prevention Systems</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber Crime Investigations and Digital Forensics</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cyber Laws and Security Policies</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Elective -III</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information Theory and Coding Security Threats</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Digital Watermarking and Steganography</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Elective -IV</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network Programming</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Distributed Systems Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intellectual Property Rights</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lab</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Seminar</td>
<td>-</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total</td>
<td>18</td>
<td>3</td>
<td>22</td>
</tr>
</tbody>
</table>

### II Year I Semester

<table>
<thead>
<tr>
<th>Code</th>
<th>Group</th>
<th>Subject</th>
<th>L</th>
<th>T/P/D</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Comprehensive Viva</td>
<td>-</td>
<td>-</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Project Seminar</td>
<td>0</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Project Work</td>
<td>-</td>
<td>-</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total</td>
<td>-</td>
<td>3</td>
<td>22</td>
</tr>
</tbody>
</table>

### II Year II Semester

<table>
<thead>
<tr>
<th>Code</th>
<th>Group</th>
<th>Subject</th>
<th>L</th>
<th>T/P/D</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Project Work and Seminar</td>
<td>-</td>
<td>-</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Total</td>
<td>-</td>
<td>-</td>
<td>22</td>
</tr>
</tbody>
</table>
MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY

Unit- I

Unit- II
ALGEBRAIC STRUCTURES: Groups – Cyclic groups, Cosets, Modulo groups - Primitive roots - Discrete logarithms. Rings – Sub rings, ideals and quotient rings, Integral domains. Fields – Finite fields – GF (p^n), GF(2^n) - Classification - Structure of finite fields. Lattice, Lattice as Algebraic system, sub lattices, some special lattices.

Unit- III

Unit- IV

Unit -V

REFERENCES:
JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – I Sem. (CF&IS/Cyber Security)

APPLIED CRYPTOGRAPHY

Unit-I

Unit-II

Unit- III

Unit- IV

Unit- V
(subject may be taught with implementation through JAVA)

REFERENCES
JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – I Sem. (CF&IS/Cyber Security)

NETWORK AND WIRELESS SECURITY

Unit- I


ELECTRONIC MAIL SECURITY: Store and forward – Security services for e-mail – Establishing keys – Privacy – Authentication of the Source – Message Integrity – Non-repudiation – Proof of submission and delivery - Pretty Good Privacy – Secure/Multipurpose Internet Mail Extension.

Unit- II


Unit- III
SECURITY IN DATA NETWORKS: Wireless Device security issues - CDPD security (Cellular Digital Packet Data)-GPRS security (General Packet Radio Service) - GSM (Global System for Mobile Communication) security – IP security.

Unit -IV

Unit -V

REFERENCES:
Learning Objectives:
This course introduces the basic biometric system, classification and applications. The student will be introduced the fundamentals of biometric technologies, basic techniques in image processing for fingerprint and iris based identification.

Unit -I:


Unit- II:


Unit- III:

Unit -IV:

Unit- V:
Iris Biometrics: Iris System Architecture, Definitions and Notations - Iris Recognition: Iris location, Doubly Dimensionless Projection, Iris code, Comparison - Coordinate System: Head Tilting Problem, Basic Eye Model, Searching Algorithm, Texture Energy Feature

References for Biometric systems:

References for Biometric Image processing:
Learning Objectives:
After the completion of the course, the student should be able to Understand different biometric technologies, applications and classification, Security issues etc. Understand image processing techniques for fingerprint and iris based identification.
DISTRIBUTED AND CLOUD COMPUTING
(Elective-I)

Unit-I
Systems Modeling, Clustering and Virtualization
Distributed System Models and Enabling Technologies, Computer Clusters for Scalable Parallel Computing, Virtual Machines and Virtualization of Clusters and Data centers.

Unit-II

Unit-III
Infrastructure as a Service (IAAS) & Platform and Software as a Service (PAAS / SAAS)

Unit-IV
Monitoring, Management and Applications

Unit-V

TEXT BOOKS:

REFERENCE BOOKS:
JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – I Sem. (CF&IS/Cyber Security)

INFORMATION STORAGE AND MANAGEMENT
(Elective-I)

Unit-I
INTRODUCTION TO STORAGE TECHNOLOGY: Data proliferation and the varying value of data with time & usage, Sources of data and states of data creation, Data center requirements and evolution to accommodate storage needs, Overview of basic storage management skills and activities, The five pillars of technology, Overview of storage infrastructure components, Evolution of storage, Information Lifecycle Management concept, Data categorization within an enterprise, Storage and Regulations.

Unit-II
STORAGE SYSTEMS ARCHITECTURE: Intelligent disk subsystems overview, Contrast of integrated vs. modular arrays, Component architecture of intelligent disk subsystems, Disk physical structure-components, properties, performance, and specifications, Logical partitioning of disks, RAID & parity algorithms, hot sparing, Physical vs. logical disk organization, protection, and back end management, Array caching properties and algorithms, Front end connectivity and queuing properties, Front end to host storage provisioning, mapping, and operation, Interaction of file systems with storage, Storage system connectivity protocols

Unit-III

Unit-IV
INTRODUCTIONS TO INFORMATION AVAILABILITY: Business Continuity and Disaster Recovery Basics, Local business continuity techniques, Remote business continuity techniques, Disaster Recovery principles & techniques
MANAGING & MONITORING: Management philosophies (holistic vs. system & component), Industry management standards (SNMP, SMI-S, CIM), Standard framework applications, Key management metrics (thresholds, availability, capacity, security, performance), Metric analysis methodologies & trend analysis, Reactive and pro-active management best practices, Provisioning & configuration change planning, Problem reporting, prioritization, and handling techniques, Management tools overview

Unit-V
SECURING STORAGE AND STORAGE VIRTUALIZATION: Define storage security. , List the critical security attributes for information systems, describe the elements of a shared storage model and security extensions, Define storage security domains, List and analyze the common threats in each domain, Identify different virtualization technologies, describe block-level and file level virtualization technologies and processes.

REFERENCES
INFORMATION SYSTEMS AUDIT
(Elective-I)

Unit- I

Unit- II
The Application Control Framework-I: Boundary Controls, Input Controls, Communication Controls.

Unit-III
The Application Control Framework-II: Processing Controls, Database Controls, output Controls.

Unit- IV

Unit -V

References
3. Jalote : Software Project Management in Practice, Pearson Education
4. Royce : Software Project Management, Pearson Education.
IT SECURITY METRICS
(Elective-II)

Unit-I:

Unit-II:

Unit-III:

Unit-IV:

Unit-V:

Text Books:
1. IT SECURITY METRICS, Lance Hayden, TATA McGraw-HILL.
2. SECURITY METRICS, CAROLINE WONG, TATA McGraw-HILL.
WEB SECURITY
(Elective-II)

Unit-I

Unit-II
Review of computer security, Public Key cryptography, RSA. Review of Cryptography Basics, On-line Shopping, Payment Gateways

Unit-III
Web Hacking Basics HTTP & HTTPS URL, Web Under the Cover Overview of Java security Reading the HTML source, Applet Security Servlets Security Symmetric and Asymmetric Encryptions, Network security Basics, Firewalls & IDS

Unit-IV
Digital Certificates, Hashing, Message Digest, & Digital Signatures

Unit-V
Basics, Securing databases, Secure JDBC, Securing Large Applications, Cyber Graffiti

Text Books:

Related Web Sites:
3. The Open SSL Project (SDKs for free download): http://www.openssl.org/
JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – I Sem. (CF&IS/Cyber Security)

DISTRIBUTED SYSTEMS
(Elective-II)

Unit-I

Unit-II
Distributed OS, Its kernel, Processes and Threads, Naming and Protection, Communication and Invocation, Virtual Memory, File Service components, Design issues, Interfaces, implementation techniques, SUN network file systems

Unit-III
SNS – a name service model, its design issues, Synchronizing physical clocks, Logical time and logical clocks, Distributed coordination. Replication and its architectural model, Consistency and request ordering, Conversation between a client and a server, Transactions, Nested Transactions.

Unit-IV
Concurrency control Locks, Optimistic concurrency control, Timestamp ordering, Comparison of methods for concurrency control.
Distributed Transactions and Nested Transactions, Atomic commit protocols, Concurrency control in distributed transactions, distributed Deadlocks, Transactions with replicated data, Transaction recovery, Fault tolerance, Hierarchical and group masking of faults.

Unit-V
Cryptography, Authentication and key distribution, Logics of Authentication, Digital signatures.
Distributed shared memory, Design and Implementation issues, Sequential consistency and ivy, Release consistency and Munin, Overview of Distributed Operating systems Mach, Chorus.

Text Book:

Reference Books:
JAWAHarlAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – I Sem. (CF&IS/Cyber Security)

APPLIED CRYPTOGRAPHY LAB

(will be uploaded shortly)
SOFTWARE VULNERABILITY ANALYSIS

Unit-I:

Unit-II:

Unit-III:

Unit-IV:

Unit-V:
Counter Measures: Detection of System Daemons, Crash Course in Signals, Tinyweb Daemon, Tools of the Trade, tinywebd Exploit Tool, Log Files, Blend In with the Crowd, Overlooking the Obvious, One Step at a time, Putting Things Back Together Again, Child Laborers, Advanced Camouflage, Spoofing the Logged IP Address, Logless Exploitation, The Whole Infrastructure, Socket Reuse, Payload Smuggling, String Encoding, How to Hide a Sled, Buffer Restrictions, Polymorphic Printable ASCII Shellcode. Hardening Countermesures - Nonexecutable Stack, ret2libc, Returning into system(). Randomized Stack Space - Investigations with BASH and GDB, Bouncing Off linux-gate. Applied Knowledge, First Attempts, Paying the Odds

Textbooks:
INTRUSION DETECTION AND PREVENTION SYSTEM

Unit-I
THEORETICAL FOUNDATIONS OF DETECTION: Taxonomy of anomaly detection system – fuzzy logic – Bayes theory – Artificial Neural networks – Support vector machine – Evolutionary computation – Association rules – Clustering

Unit-II
ARCHITECTURE AND IMPLEMENTATION: Centralized – Distributed – Cooperative Intrusion Detection - Tiered architecture

Unit-III
JUSTIFYING INTRUSION DETECTION: Intrusion detection in security – Threat Briefing – Quantifying risk – Return on Investment (ROI)

Unit-IV

Unit-V

REFERENCES:
JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

CYBER CRIME INVESTIGATIONS AND DIGITAL FORENSICS

Unit -I

Unit -II

Unit -III

Unit -IV

Unit -V

REFERENCES:
JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

CYBER LAWS AND SECURITY POLICIES

Unit-I

Unit-II

Unit-III
Information security policies and procedures: Corporate policies- Tier 1, Tier 2 and Tier3 policies - 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

REFERENCES

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

INFORMATION THEORY AND CODING
(Elective-III)

Unit-I
RANDOM VARIABLES AND PROCESSES: Events - Random variables - Distribution and density functions - Operations on random variables - Covariance - Correlation functions - Random process - Stationarity - Spectral decomposition - Response of linear system to random inputs, Relation between information and probability

Unit-II

Unit-III
ERROR CONTROL CODING: Backward error correction linear block codes, BCH codes, Golay codes, efficiency of LBC, forward correction codes-Convolution coding decoding algorithms, Viterbi decoding optimum decoding performance measures

Unit-IV
DATA AND VOICE CODING: Context dependent coding, arithmetic codes, overall efficiency consideration. Voice coding, Delta Modulation and adaptive delta modulation, linear predictive coding, silence coding, sub-band coding

Unit-V

REFERENCES:
SECURITY THREATS
(Elective-III)

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, Insider threats, Cyber crimes.

Unit-II

Unit-III

Unit-IV

Unit-V

REFERENCES
M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

DIGITAL WATERMARKING AND STEGANOGRAPHY
(Elective-III)

Unit I

Unit II

Unit III
PERCEPTUAL MODELS: Evaluating perceptual impact – General form of a perceptual model – Examples of perceptual models – Robust watermarking approaches - Redundant Embedding, Spread Spectrum Coding, Embedding in Perceptually significant coefficients

Unit IV

Unit V
STEGANOGRAPHY: Steganography communication – Notation and terminology – Information-theoretic foundations of steganography – Practical steganographic methods – Minimizing the embedding impact – Steganalysis

REFERENCES:
JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

NETWORK PROGRAMMING
(Elective-IV)

Unit-I
Introduction to Network Programming: OSI model, Unix standards, TCP and UDP & TCP connection establishment and Format, Buffer sizes and limitation, standard internet services, Protocol usage by common internet application.

Sockets: Address structures, value – result arguments, Byte ordering and manipulation function and related functions Elementary TCP sockets – Socket, connect, bind, listen, accept, fork and exec function, concurrent servers. Close function and related function.

Unit-II
TCP client server: Introduction, TCP Echo server functions, Normal startup, terminate and signal handling server process termination, Crashing and Rebooting of server host shutdown of server host.

Elementary UDP sockets: Introduction UDP Echo server function, lost datagram, summary of UDP example, Lack of flow control with UDP, determining outgoing interface with UDP.

I/O Multiplexing: I/O Models, select function, Batch input, shutdown function, poll function, TCP Echo server,

Unit-III
socket options getsockopt and setsockopt functions. Socket states, Generic socket option IPV6 socket option ICMPV6 socket option IPV6 socket option and TCP socket options.

Advanced I/O Functions-Introduction, Socket Timeouts, recv and send Functions, readv and writev Functions, recvmsg and sendmsg Functions, Ancillary Data, How Much Data Is Queued?, Sockets and Standard I/O, T/TCP: TCP for Transactions

Unit-IV
Elementary name and Address conversions: DNS, gethost by Name function, Resolver option, Function and IPV6 support, uname function, other networking information.

Daemon Processes and inetd Superserver – Introduction, syslogd Daemon, syslog Function, daemon_init Function, inetd Daemon, daemon_inetd Function

Broadcasting- Introduction, Broadcast Addresses, Unicast versus Broadcast, dg_cli Function Using Broadcasting, Race Conditions

Multicasting- Introduction, Multicast Addresses, Multicasting versus Broadcasting on A LAN, Multicasting on a WAN, Multicast Socket Options, mcast_join and Related Functions, dg_cli Function Using Multicasting, Receiving MBone Session Announcements, Sending and Receiving, SNTP: Simple Network Time Protocol, SNTP (Continued)

Unit-V
Raw Sockets-Introduction, Raw Socket Creation, Raw Socket Output, Raw Socket Input, Ping Program, Traceroute Program, An ICMP Message Daemon,

Datalink Access- Introduction, BPF: BSD Packet Filter, DLPI: Data Link Provider Interface, Linux: SOCK_PACKET, libpcap: Packet Capture Library, Examining the UDP Checksum Field

Remote Login: Terminal line disciplines, Pseudo-Terminals, Terminal modes, Control Terminals, rlogin Overview, RPC Transparency Issues.

Text Books:
1. UNIX Network Programming, by W. Richard Stevens, Bill Fenner, Andrew M. Rudoff, Pearson Education
DISTRIBUTED SYSTEMS SECURITY
(Elective-IV)

Unit-I

Unit-II

Unit-III

Unit-IV

Unit-V

REFERENCES
JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

INTELLECTUAL PROPERTY RIGHTS
(Elective-IV)

Unit-I

Unit-II

Unit-III
Introduction to Copyrights – – Principles of Copyright Principles -The subjects Matter of Copy right – The Rights Afforded by Copyright Law – Copy right Ownership, Transfer and duration – Right to prepare Derivative works – Rights of Distribution – Rights of Perform the work Publicity Copyright Formalities and Registrations - Limitations - Copyright disputes and International Copyright Law – Semiconductor Chip Protection Act

Unit -IV
The law of patents-patent searches –Patent owner ship and transfer-Patent infringement-International Patent Law

Unit-V

BOOKS:
1. Debirag E.Bouchoux: "Intellectual Property". Cengage learning, New Delhi
3. Cyber Law. Texts & Cases, South-Western’s Special Topics Collections
JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

M. Tech – I Year – II Sem. (CF&IS/Cyber Security)

ETHICAL HACKING LAB

(will be uploaded shortly)