**Course Name:** M.Sc (Information and Cyber Security)

**Duration:** 2 years (Full Time)

**Eligibility:** Bachelor In Engineering/Science from any University recognised by UGC.

**Course Objective:** The goal of this course is for students to maintain an appropriate level of awareness, knowledge and skill on the disciplines of technology, business and law to allow them to minimize the occurrence and severity of information security incidents. The students will learn techniques used to detect, respond to, and prevent network intrusions. The duration of the course is two years and its syllabus is divided into four semesters that would provide the students with an in-depth understanding of core concepts with major thrust on functional competencies related to real life situations. The course bear a strong adherence to computer based technological skills and capabilities, and thereby resulting in efficiency to handle a variety of issues related to Information and Cyber Security in any organization.

**Course Structure:**

Summary:

<table>
<thead>
<tr>
<th>Semester No</th>
<th>Total Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>24</td>
</tr>
<tr>
<td>2</td>
<td>24</td>
</tr>
<tr>
<td>3</td>
<td>24</td>
</tr>
<tr>
<td>4</td>
<td>24</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>96</strong></td>
</tr>
</tbody>
</table>

**Theory**

<table>
<thead>
<tr>
<th>SI No</th>
<th>Course Code</th>
<th>Topic</th>
<th>Contact hrs/wk</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MAM105</td>
<td>C Programming and Data Structure</td>
<td>3 1 -</td>
<td>4 4</td>
</tr>
<tr>
<td>2</td>
<td>MCS103</td>
<td>Information Systems &amp; Software Engineering</td>
<td>3 1 -</td>
<td>4 4</td>
</tr>
<tr>
<td>3</td>
<td>MCL101</td>
<td>Fundamentals of Information Security and Legal Framework</td>
<td>3 1 -</td>
<td>4 4</td>
</tr>
<tr>
<td>4</td>
<td>MCL102</td>
<td>Introduction to Hardware, Network, the Internet</td>
<td>3 1 -</td>
<td>4 4</td>
</tr>
<tr>
<td>5</td>
<td>MCL 103</td>
<td>Cyber Threat and Modelling</td>
<td>3 1 -</td>
<td>4 4</td>
</tr>
</tbody>
</table>

**Total of Theory:** 20 20
### Practical

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Course Code</th>
<th>Topic</th>
<th>Contact hrs/wk</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>MCL191</td>
<td>Computer LAB (MATLAB, Excel, Linux Server- Apache)</td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

**Total number of Practical**

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Course Code</th>
<th>Topic</th>
<th>Contact hrs/wk</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

**Total**

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Course Code</th>
<th>Topic</th>
<th>Contact hrs/wk</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>24</td>
<td>24</td>
</tr>
</tbody>
</table>

### Semester 2

#### Theory

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Course Code</th>
<th>Topic</th>
<th>Contact hrs/wk</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MCL201</td>
<td>Cyber Crimes &amp; Investigation</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>MCL202</td>
<td>Network Security(Ref: WBUT MCSE 401C)</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>MCL203</td>
<td>Application and System Security</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>MCL204</td>
<td>Operating System, Database and Infrastructure Security</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>MCL205</td>
<td>Cyber Forensics</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

**Total of Theory**

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Course Code</th>
<th>Topic</th>
<th>Contact hrs/wk</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>20</td>
<td>20</td>
</tr>
</tbody>
</table>

### Practical

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Course Code</th>
<th>Topic</th>
<th>Contact hrs/wk</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>MCL 291</td>
<td>Cyber Forensics Lab</td>
<td>-</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

**Total number of Practical**

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Course Code</th>
<th>Topic</th>
<th>Contact hrs/wk</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

**Total**

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Course Code</th>
<th>Topic</th>
<th>Contact hrs/wk</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>24</td>
<td>24</td>
</tr>
</tbody>
</table>
### Semester 3

#### Theory

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Course Code</th>
<th>Topic</th>
<th>Contact hrs/wk</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>L  T  P  Total</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>MCL301</td>
<td>Information Security &amp; Cryptography</td>
<td>3 1 - 4</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>MCL302</td>
<td>Mobile, Wireless and VoIP Security</td>
<td>3 1 - 4</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>MCL303</td>
<td>Malware Analysis</td>
<td>3 1 - 4</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>MCL304</td>
<td>Cyber Law</td>
<td>3 1 - 4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>MCL305</td>
<td>Security Architecture and Models</td>
<td>3 1 - 4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Total of Theory</strong></td>
<td></td>
<td>20 20</td>
</tr>
</tbody>
</table>

#### Practical

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Course Code</th>
<th>Topic</th>
<th>Contact hrs/wk</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>MCL391</td>
<td>Cryptography Lab</td>
<td>- 4 4 4 4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Total of Practical</strong></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Total</strong></td>
<td></td>
<td>24 24</td>
</tr>
</tbody>
</table>

### Semester 4

#### Theory

<table>
<thead>
<tr>
<th>Sl No</th>
<th>Course Code</th>
<th>Topic</th>
<th>Contact hrs/wk</th>
<th>Credit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>L  T  P  Total</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>Elective I</td>
<td>3 1 - 4</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Elective II</td>
<td>3 1 - 4</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>MCL403</td>
<td>Security Policy &amp; Audit</td>
<td>3 1 - 4</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>MCL404</td>
<td>Block Chain</td>
<td>3 1 - 4</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Sessionals</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>MCL481</td>
<td>Sessional Project</td>
<td>9 9 6</td>
<td></td>
</tr>
</tbody>
</table>
**Elective I**
MCLPE601A/MCS E 401A Cloud Computing
MCLPE 601B Mobile & Digital Forensics
MCL E 601C Penetration Testing & Vulnerability Assessment

**Elective II**
MCLPE 602A Risk Management
MCLPE 602B Hardware Security
MCLPE 602C Biometric Security

**Semester 1**

**MAM-105: C Programming and Data Structure**


**Text Books:**
1. Data structure using c and c++ - Tanenbaum
2. Fundamentals of Data structure in c++ - E. Horwitz, Sahni, D. Mehta

**MCS103: Information Systems & Software Engineering**

Information System, IT Infrastructure and Emerging Technologies, Foundations of Business Intelligence, Telecommunications, the internet, and wireless Technology, Securing Information Systems, Enterprise Applications, Knowledge Management, Enhancing Decision Making information gathering, requirement and feasibility analysis, data flow diagrams, process specifications, input/output design, process life cycle, software planning and managing the project (single & multi variable model), design, software modularity & metrics, coding, testing, implementation, maintenance, software quality and reliability.

**Text Books:**
3. An Integrated Approach to Software Engineering by P. jalote, Springer

**MCL101: Fundamentals of Information Security and Legal Framework**

**Module I: Introduction.** [6L]

**Module II: Security Needs.** [6L]
Secure Software Development.

**Module III: Cryptography Concepts.** [8L]
Public Key Infrastructure (PKI), Different attacks on Cryptosystems.

**Module IV: Internet Standards and Authentication.** [8L]

**Module V: Risk and Disaster Management.** [6L]

**Module VI: Remote Access Protection.** [6L]
Access Control, Biometric Access Controls, Firewalls, Protecting Remote Connections in Remote Access and Virtual Private Networks (VPNs), Intrusion Detection and Prevention Systems

**Module VII: Legal Framework**
Indian legal system, federalism and constitutionalism, Legislation, Enforcement of laws and Adjudication, Judicial system in India and hierarchy of courts, Criminal and Civil legal and justice system, Concept of Jurisdiction, Regulatory tribunals and their functions, Principles of administrative law, Alternative dispute resolution mechanism.
Text Books:
3) Indian Legal System: S.P. Sharma, Mittal Publication

MCL102: Introduction to Hardware, Network, the Internet

Module I: (6L)
Definition of computer system, Block Diagram, Components of a computer system, generations of computers, storage devices, Memory Hierarchy, Software, Classification of software, Operating System and its functionalities

Module II: (6L)
Introduction to networking; Data communications: components, data representation (ASCII, ISO etc.), direction of data flow (simplex, half duplex, full duplex); network criteria, physical structure (type of connection, topology), categories of network (LAN, MAN, WAN);
Overview of data(analog & digital), signal(analog & digital), transmission (analog & digital) & transmission media (guided & unguided);

Module III: (8L)
Local Area Networks and data link protocols, point-to-point links and sliding window flow control, CSMA/CD, Ethernet, wireless LAN, cellular networks, and advanced multi-user communication (CDMA, SDMA/MIMO), mobility
Internetworking using TCP/IP: network programming using socket API, network client/server design
Packet/circuit switching and wide-area networks: store-and-forward networks, source routing, virtual/permanent, circuits and call set-up, LAN/WAN addressing, hop-by-hop vs. end-to-end control

Module IV: (10L)
Routing techniques - intra-domain routing (OSPF, RIP), inter-domain policy routing (BGP) and network connectivity
Transport protocols - TCP and UDP, Congestion control, TCP window control, multimedia streaming
High-level network services - DNS, HTTP, SMTP, network management (SNMP), network security

Module V: (10L)
Introduction and history of Internet, WWW, Markup Language: HTML, XML and tags, Scripting Languages, Client-Server Architecture, websites, Internet security and threats, Firewall, Introduction to e-commerce

Text Books:
1. Fundamental of Computers, V.Rajaraman, Prentice Hall India
3. Data Communication and Networking by B. Forouzan
4. Data and Communication by W. Stallings

MCL 103: Cyber Threat and Modelling

Understanding Intelligence: Intelligence Lexicon and Definitions, Traditional Intelligence Cycle, Sherman Kent and Intelligence Tradecraft, Structured Analytical Techniques

Understanding Cyber Threat Intelligence: Defining Threats, Understanding Risk, Cyber Threat Intelligence and Its Role, Expectation of Organizations and Analysts, Four Methods of Threat Detection

Threat Intelligence Consumption: Sliding Scale of Cybersecurity, Consuming Intelligence for Different Goals, Enabling Other Teams with Intelligence

Positioning the Team to Generate Intelligence: Building an Intelligence Team, Positioning the Team in the Organization, Prerequisites for Intelligence Generation

Planning and Direction (Developing Requirements): Intelligence Requirements, Priority Intelligence Requirements, Beginning the Intelligence Lifecycle, Threat Modeling

Case-Study: Carbanak, "The Great Bank Robbery"

MCL191: Computer LAB (MATLAB, Excel, Linux Server- Apache)

Assignment-1
Familiarization with MATLAB Control System tool Box, MATLAB- SIMULINK tool box & p SPICE

Assignment-2
Determination of step response for 1 order & 2 order system with unity feedback on CRO & calculation of control system specifications for variations of system design.

Assignment-3
Simulation of step response & impulse response for Type-I & Type-II system with unity feedback using MATLAB.

Assignment-4
Determination of root locus, Bode-plot, SyQuest Plot, using MATLAB control system toolbox for a given 2nd order transfer function & determination of different control system specifications.

Assignment-5
Electronic spreadsheet software, spreadsheet design, creating a spreadsheet, updating data & recalculations, Common spreadsheet commands.

Assignment-6
graphics capability, special features, different Formulas Related to database function, logical function, math & Accounting function.

Assignment-7
Linux Install, Network Interface configuration, Basic Linux Commands, Telnet.

Assignment-8
IP Subnet Calculation:-Public & Private IP Address, Classes of IP Address, IP sub netting.

Assignment-9
Packet Monitoring software (tcpdump, snort, ethereal).

Assignment-10
Linux File System Permission, Controlling new file permission & ownership, Trace route, Ping, Finger, Nmap.

Semester 2

MCL201: Cyber Crimes and Investigation

Introduction to cyber crime, Data diddling, Data leakage, Eavesdropping, E-mail forgery, E-mail threats, Internet misinformation, Internet terrorism, Password cracking, Round downs, Salami Techniques, Scavenging/Corporate Espionage, Social Engineering, Software Piracy, Spamming, Super zapping, Piggybacking, Trap door, Trojan Horse, Virus, Worm Impersonation, Time bomb, Logic bomb, DOS Attack


Intrusion Analysis, Intrusion Analysis as a Core Skillset, Methods to Performing Intrusion Analysis, Intrusion Kill Chain, Passively Discovering Activity in Historical Data and Logs, Detecting Future Threat Actions and Capabilities, Denying Access to Threats, Delaying and Degrading Adversary Tactics and Malware, Identifying Intrusion Patterns and Key Indicators

Text Books:
1) Cyber Law Law Of Information Technology And Internet (Lexix Nexis) Anirudh Rastogi
2) Understanding Laws– Cyber Laws And Cyber Crimes (Lexix Nexis)

3) Cyber Crime Manual by Bibhas Chatterjee, Lawman Publication

MCL202: Network Security
Concepts and Terminology:
Threats, Attacks, Services and Mechanisms, Security Attacks, Security Services, Integrity check, digital Signature, authentication, Spoofing, Sniffing, Firewall.

Cryptography:
Techniques, Mathematical foundation, Stream Ciphers, Block Ciphers, Cryptanalysis, Hash Algorithms.

Secret Key Cryptography:
Block Encryption, DES rounds, S-Boxes IDEA: Overview, comparison with DES, Key expansion, IDEA rounds, Uses of Secret key Cryptography; ECB, CBC, OFB, CFB, Multiple encryptions DES.
Hash Functions and Message Digests:
Length of hash, uses, algorithms (MD2, MD4, MD5, SHA) MD2: Algorithm (Padding, checksum, passes.) MD4 and 5: algorithm (padding, stages, digest computation.) SHA: Overview, padding, stages.

Public key Cryptography:

Authentication:

Security Policies and Security Handshake Pitfalls:
What is security policy, high and low level policy, user issues? Protocol problems, assumptions, Shared secret protocols, public key protocols, mutual authentication, reflection attacks, use of timestamps, nonce and sequence numbers, session keys, one-and two-way public key based authentication.

Network Security:
Electronic mail security, IP security, Network management security.

System Security:
Intruders and Viruses, Firewalls, Intrusion Detection.

Case Studies
Web threats, E-mail threats, Domain controller threats, Extranet and VPN threats.
Assignment and Project work.

Text Books:
MCL203: Application and System Security

Module I: Introduction. [8L]
Protocols and standards, Hypertext Transfer Protocol (HTTP), Markup languages Hypertext Markup Language (HTML), Cascading Style Sheets (CSS).

Module II: Web Application. [14L]
Extensible Hypertext Markup Language (XHTML), CGI scripts and clickable maps, JAVA applets, JAVA servlets, Perl. DHTML, XML, Client-side technologies, JavaScript, Server-side technologies, SQL, PHP.

Module III: Software and System Security. [5L]
Control hijacking attacks – buffer overflow, integer overflow, bypassing browser memory protection, Sandboxing and Isolation, Tools and techniques for writing robust application software, Security vulnerability detection tools, and techniques – program analysis, Privilege, access control, and Operating System Security, Exploitation techniques, and Fuzzing.

Module IV: Network Security & Web Security. [8L]

Module V: Security in Mobile Platforms. [3L]
Android security model, threat models, information tracking, rootkits, Threats in mobile applications, analyzer for mobile apps to discover security vulnerabilities, Viruses, spywares, and keyloggers and malware detection

Threats of Hardware Trojans and Supply Chain Security, Side Channel Analysis based Threats, and attacks.

Text Books:
MCL204: Operating System, Database and Infrastructure Security

Module I: Operating System. [18L]

Introduction to OS - Operating system functions, evaluation of O.S., Different types of O.S.: batch, multi-programmed, time-sharing, real-time, distributed, parallel. Computer system operation, I/O structure, storage structure, storage hierarchy, different types of protections, operating system structure (simple, layered, virtual machine), O/S services, system calls.

Process Management: Concept of processes, process scheduling, operations on processes, co-operating processes, inter-process communication. Process Synchronization, Deadlocks.

Memory Management: background, logical vs. physical address space, swapping, contiguous memory allocation, paging, segmentation, segmentation with paging. Virtual Memory: background, demand paging, performance, page replacement, page replacement algorithms (FCFS, LRU), allocation of frames, thrashing.

File Systems: file concept, access methods, directory structure, file system structure, allocation methods (contiguous, linked, indexed), free-space management (bit vector, linked list, grouping), directory implementation (linear list, hash table), efficiency & performance.

I/O Management: I/O hardware, polling, interrupts, DMA, application I/O interface (block and character devices, network devices, clocks and timers, blocking and nonblocking I/O), kernel I/O subsystem (scheduling, buffering, caching, spooling and device reservation, error handling), performance, Disk Management.

Protection & Security: Goals of protection, domain of protection, security problem, authentication, one time password, program threats, system threats, threat monitoring, encryption.

Module II: Database. [16L]

Introduction Concept & Overview of DBMS, Data Models, Database Languages, Database Administrator, Database Users, Three Schema architecture of DBMS.

Entity-Relationship Model. Relational Model, Relational Algebra, Relational Calculus, Extended Relational Algebra Operations, Views, Modifications Of the Database.

SQL and Integrity Constraints.

Relational Database Design: Functional Dependency, Different anamolies in designing a Database., Normalization using functional dependencies, Decomposition, Boyce-Codd Normal Form, 3NF, Nomalization using multi-valued depedencies, 4NF, 5NF.

Transaction processing, Concurrency control and Recovery Management: transaction model properties, state serializability, lock base protocols, two phase locking.

File Organization & Index Structures.

Module III: Infrastructure Security. [6L]

IT Infrastructure Management Services, Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement

Text Books:

MCL205: Cyber Forensics


Unix/Linux fundamentals: Unix/Linux incident response tools, Unix/Linux file systems (Ext2/Ext3)

Unix/Linux Forensic Investigation: Unix/Linux forensics investigation steps and technologies, Unix/Linux forensics case studies

Windows Incident Response: Memory forensics, Windows incident response tools

Windows fundamentals: Windows file systems, Windows forensics tools

Windows Forensic Investigation: Windows acquisition, Windows forensics analysis – registry and other artifacts

Advanced artifacts: Loadable kernel module rootkits, Steganography hiding, detection and analysis

Text Books:

MCL291: Cyber Forensics Lab

Software Tools: CyberCheck 4.0 - Academic Version CyberCheckSuite MobileCheck Network Session Analyser Win-LiFT TrueImager TrueTraveller Photo Examiner Ver 1.1, CDRAnalyzer

Network Forensics: • Intrusion detection • Logging (the best way to track down a hacker is to keep vast records of activity on a network with the help of an intrusion detection system) • Correlating intrusion detection and logging


**Semester 3**

**MCL301: Information Security & Cryptography**


**Cryptography:** Concepts and Techniques, symmetric and asymmetric key cryptography, steganography, Symmetric key Ciphers: DES structure, DES Analysis, Security of DES, variants of DES, Block cipher modes of operation, AES structure, Analysis of AES, Key distribution Asymmetric key Ciphers: Principles of public key cryptosystems, RSA algorithm, Analysis of RSA, Diffie-Hellman Key exchange


**Intruders, Virus and Firewalls:** Intruders, Intrusion detection, password management, Virus and related threats, Countermeasures, Firewall design principles, Types of firewalls

**Introduction to Cryptoanalysis:** Linear Cryptanalysis, Differential Cryptanalysis, Cryptanalysis of DLP

MCL302: Mobile, Wireless and VoIP Security

Module I: Introduction. [6L]

Module II: Mobile Networks. [6L]

Module III: Wireless Systems. [8L]

Module IV: Security in Wireless Communication. [8L]

Module V: VoIP. [5L]
Streaming in 3rd generation mobile architecture, Voice and Video over IP (Media over IP), Session Initiation Protocol (SIP) and its use in Media Over IP, Skype as a case study.

Module VI: Security in VoIP. [6L]
Attacks against the VOIP network, Challenges against implementing VOIP network, WEP (Wired Equivalent Privacy), Effects of using WEP in VOIP networks, Concepts of WPA and WPA2.

Text Books:

MCL 303: Malware Analysis

Implementation of Covert Channel Non self-reproducing Malware - Working principle of Trojan Horse - Implementation of Remote access and file transfer - Working principle of Logical Bomb - Case Study: Conflicker C worm.

Virus Design And Its Implications: Virus components - Function of replicator, concealer and dispatcher - Trigger Mechanisms - Testing virus codes - Case Study: Brute force logical bomb.

Malware Design Using Open Source: Computer Virus in Interpreted programming language - Designing Shell bash virus under Linux - Fighting over infection - Anti-antiviral fighting – Polymorphism - Case study: Companion virus.

Virus And Worm Analyses: Klez Virus - Clone Virus - Doom Virus - Black wolf worm - Sassar worm - Happy worm 99.

TEXT BOOKS:


MCL 304 : Cyber Law


Module III: Constitutional & Human Rights Issues in Cyberspace - Freedom of Speech and Expression in Cyberspace - Right to Access Cyberspace – Access to Internet - Right to Privacy - Right to Data Protection


Module V: Cyber Torts - Cyber Defamation - Different Types of Civil Wrongs under the IT Act, 2000, Electronic Evidence.


Text Books:
4. S. R. Bhansali, Information Technology Act, 2000, University Book House Pvt. Ltd

MCL305: Security Architecture and Models

Module I: Security Architecture And Information. [7L]

Module II: Logical design and physical design. [7L]

Module III: Low-level architecture. [6L]

Module IV: Mid-level architecture. [6L]

Module V: High-level architecture. [6L]

Module VI: Business cases and security. [2L]

MCL391: Cryptography Lab

1) Perform Basic Encryption/Decryption (Text only).
2) Diffie-Hellman key exchange and symmetric key cryptography.
3) Public key cryptography using RSA.
4) Implementing Private key cryptography.
5) Perform Basic Encryption/Decryption
6) Perform Basic Hash Functions (Like MD4, MD5 etc.).
7) Perform Basic Fractal functions (Like Julia set etc.)
8) Generate Asymmetric Key Pair.
9) Generate Web Certificate from Key Pair.

**Semester 4**

**MCL 403 Security Policy and Audit**

**Module I: Introduction.**
Basics of Audit, IT Auditing: What Is It? The Situation and the Problem, Audit Standards, Importance of Audit Independence, Need for IT Audit Function, Auditor: Knowledge, Skills, and Abilities, Role of the IT Auditor, Types of Auditors and Their Duties, Functions, and Responsibilities

**Module II: Audit Process in an Information Technology Environment.**
Audit Universe, Risk Assessment, Audit Plan, Developing an Audit Schedule, Audit Budget, Objective and Context, Using the Plan to Identify Problems, Audit Process, Design Audit Procedures, Fieldwork and Implementing Audit Methodology.

**Module III: IT Auditing in Modern Era.**
IT Auditing Trends, New Dimension: Information Assurance, IT Audit: The Profession, A Common Body of Knowledge, Certification, Role of the IT Auditor in IT Governance, IT Auditor as Counselor, IT Auditor as Partner of Senior Management.

**Module IV: Audit using Computer Assisted Audit Tools.**

**Module V: Managing IT Audit.**
Evaluating IT Audit, IT Audit Quality, Terms of Assessment, IT Audit and Auditor Assessment Form, Criteria for Assessing the Audit, Criteria for Assessing the Auditor, Applying the Concept, Evaluation of IT Audit Performance.

**Module VI: Security Audit Process.**
Pre-planning audit, Audit Risk Assessment, Performing Audit, Internal Controls, Audit Evidence, Audit Testing, Audit Finding, Follow-up activities.

**Text Books:**

**MCL 404 Block Chain & Cryptocurrency**

Intro to Blockchain and Cryptocurrency
Internet of money, Public vs. private blockchain technology, Proof of work, consensus verification, Data blocks, Bitcoin and valuation, Ethereum and Blockchain Platforms Clearing and , Introduction to Blockchain API

Open source tools, Algorithms,,Assets and Tokenization and the Value of the Blockchain Credits versus tokens Community currency

Smart Contracts Distributed ledger technology, Regulation and legal frameworks, Consensus Protocols and Byzantine Fault Tolerance (BFT), Scalability and distributed ledgers, ethereum, Regulatory Environment

Use Cases Finance, Security, Social Good, Other alternative uses,

Security: Attacks and Trustless Networks

MCSE401A/MCLE601A: Cloud Computing


Concurrent Computing, High-throughput Computing and Data-Intensive Computing: Programming applications with Threads, Thread API, Parallel computation with Threads, Task computing, Frameworks for Task computing, Task-based application model, Data-intensive computing, characteristics, technology Cloud Platforms and Applications: Overview on Amazon Web Services, Google AppEngine and Microsoft Azure, Cloud applications in scientific, business and consumer Domain

Text Books:

MCLE401B Mobile & Digital Forensics

CIA triad in mobile phones-Voice, SMS and Identification data interception in GSM: Introduction, practical setup and tools, implementation- Software and Hardware Mobile phone tricks: Netmonitor, GSM network service codes, mobile phone codes, catalog tricks and AT command set- SMS security issues

Mobile phone forensics: crime and mobile phones, evidences, forensic procedures, files present in SIM card, device data, external memory dump, evidences in memory card, operators systems-Android forensics: Procedures for handling an android device, imaging android USB mass storage devices, logical and physical techniques

Digital forensics: Introduction – Evidential potential of digital devices: closed vs. open systems, evaluating digital evidence potential- Device handling: seizure issues, device identification, networked devices and contaminationUnit V (8 hours) Digital forensics examination principles: Previewing, imaging, continuity, hashing and evidence locationsSeven element security model-developmental model of digital systems- audit and logs- Evidence interpretation: Data content and context

Text Books:

MCLE401C Penetration Testing & Vulnerability Assessment

Introduction Ethical Hacking terminology- Five stages of hacking- Vulnerability Research-Legal implication of hackingImpact of hacking.

Foot printing & Social engineering Information gathering methodologies- Competitive Intelligence- DNS Enumerations- Social Engineering attacks.

System Hacking Password cracking techniques- Key loggers- Escalating privileges- Hiding Files- Steganography technologies- Countermeasures.

Sniffers & SQL Injection Active and passive sniffing- ARP Poisoning- Session Hijacking- DNS Spoofing- Conduct SQL Injection attack - Countermeasures.

TEXT BOOKS:

MCLE402A Risk Management

Module I: Introduction to Information Risk Management. [9L]

Module II: Introduction to Risk Assessments and Risk Semantics. [7L]

Module III: Risk Issues in IT and Telecommunication. [9L]

Module IV: Security Management. [6L]

Module V: Incident Analysis. [4L]
Introduction, Log analysis, Event criticality, General log configuration and maintenance, Live Incident Response, Timelines, Other forensics topics.

Text Books:

MCLPE 402B Hardware Security
Overview of Different Issues of Hardware Security

Preliminaries: Algebra of Finite Fields, Basics of the Mathematical Theory of Public Key Cryptography, Basics of Digital Design on Field-programmable Gate Array (FPGA), Classification using Support Vector Machines (SVMs)

Useful Hardware Security Primitives: Cryptographic Hardware and their Implementation, Optimization of Cryptographic Hardware on FPGA, Physically Unclonable Functions (PUFs), PUF Implementations, PUF Quality Evaluation, Design Techniques to Increase PUF Response Quality

Side-channel Attacks on Cryptographic Hardware: Basic Idea, Current-measurement based Side-channel Attacks (Case Study: Kocher’s Attack on DES), Design Techniques to Prevent Side-channel Attacks, Improved Side-channel Attack Algorithms (Template Attack, etc.), Cache Attacks

Testability and Verification of Cryptographic Hardware: Fault-tolerance of Cryptographic Hardware, Fault Attacks, Verification of Finite-field Arithmetic Circuits

Modern IC Design and Manufacturing Practices and Their Implications: Hardware Intellectual Property (IP) Piracy and IC Piracy, Design Techniques to Prevent IP and IC Piracy, Using PUFs to prevent Hardware Piracy, Model Building Attacks on PUFs (Case Study: SVM Modeling of Arbiter PUFs, Genetic Programming based Modeling of Ring Oscillator PUF)

Hardware Trojans: Hardware Trojan Nomenclature and Operating Modes, Countermeasures Such as Design and Manufacturing Techniques to Prevent/Detect Hardware Trojans, Logic Testing and Side-channel Analysis based Techniques for Trojan Detection, Techniques to Increase Testing Sensitivity
Infrastructure Security: Impact of Hardware Security Compromise on Public Infrastructure, Defense Techniques (Case Study: Smart-Grid Security)

Text Books:


MCLE 402C  BIOMETRIC SECURITY

Introduction to Biometrics, Fingerprint Recognition, Face Recognition, Iris Recognition, Hand Geometry Recognition

Gait Recognition, The Ear as a Biometric, Voice Biometrics, A Palm print Authentication System, and OnLine Signature Verification
3D Face Recognition, Automatic Forensic Dental Identification, Hand Vascular Pattern Technology, Introduction to Multi biometrics, Multispectral Face Recognition


Linkages between Biometrics and Forensic Science, Biometrics in the Government Sector, Biometrics in the Commercial Sector, Biometrics Standards, Biometrics databases

Text Books: