MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL - 462003

Name of Program M.Tech (IS) **Semester** 1st **Year I**

Name of Course MATHEMATICAL FOUNDATION OF INFORMATION SECURITY

Course Code IS 101

Core / Elective / Other Core

Prerequisite:

1. Set Theory, Basic Number Theory
2. Algebra, Permutation and Combination
3. Probability

Course Outcomes:

1. Understand the notion of mathematical thinking, mathematical proofs, and algorithmic thinking, and be able to apply them in problem solving related to information security.
2. Understand underlying Mathematical concepts required for cryptology.
   Be able to use effectively algebraic techniques for computer security.
3. Understand some basic properties of graphs and related discrete structures, and be able to relate these to information security.
   Be able to use Decision and Game Theory for improvising system's security.

Description of Contents in brief:

Number Theory and Algebra: Integer Arithmetic, Integers set Z, Z_n, Z_n*, Greatest common divisors in Z, Euclidean algorithm, Extended Euclidean Algorithm, Additive and Multiplicative inverses in Z_n, Modular Arithmetic, Linear Diophantine equations, Linear Congruence, Groups, Ring, Field, Lattice, Galois Field over prime numbers and power of 2, Lattice reduction, Sieve algorithms; Euler's Phi-function, Fermat's little theorem, Euler's theorem, primality testing, factorization, Chinese remainder theorem, Quadratic congruence, Discrete logarithm problem, Index calculus algorithms; Matrices, Graph Theory in Network Security, Decision and Game Theory for Security.

List of Text Books:

1. No text book is recommended, subject will be taught using the material available on internet and research papers.

List of Reference Books:

1. Cryptography and Network Security, Behrouz A. Forouzan, The McGraw-Hill.
2. Introduction to Linear Algebra 5th Edition, Gilbert Strang, Wellesley Cambridge Press.
3. Decision and Game Theory for Security, 6th International Conference,

GameSec 201.

URLs

1. https://hyperelliptic.org/tanja/teaching/cryptoI13/nt.pdf
2. http://www.cs.columbia.edu/~rjaiswal/factoring-survey.pdf
3. https://arxiv.org/ftp/arxiv/papers/1511/1511.04785.pdf

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY
BHOPAL - 462003

Name of Program **M Tech** **Semester -I** **Year 1st**

Name of Course **Computer & network security**

Course Code CN-102

Core / Elective / Other Core

Prerequisite:

1. knowledge of computer networks, operating systems, data structures and algorithms
2. knowledge of advanced programming in C

Course Outcomes:

1. Students will be able toAcquire professional/academic knowledge and skills.
2. Students will be able toDescribe some common problems or attacks on network security. And alsoDescribe some network security services and mechanisms
3. Students will be able toStudy and analyze some cryptographic algorithms with their relation with real life.

Description of Contents in brief:

1. Introduction to computer and network security. Basic concepts, threat models, common security goals.
2. Cryptography and cryptographic protocols, including encryption, authentication, message authentication codes, hash functions, one way functions, public key cryptography, secure channels, zero knowledge in practice, models and methods for security protocol analysis.
3. Malicious code analysis and defense. Viruses, Worms, spyware, rootkits, botnets, etc. and defenses against them, Detecting Attackers.
4. Software security. Secure software engineering, defensive programming, buffer overruns and other implementation flaws.
5. Language based security: analysis of code for security errors, safe languages, and sandboxing techniques. Operating system security. Memory protection, access control, authorization, authenticating users, enforcement of security, security evaluation, trusted devices, digital rights management.
6. Network security. Network based attacks, Kerberos,X.509, firewalls, intrusion detection systems, DoS attacks and defense. Case studies: DNS, IPSec.
7. Web security. Securing Internet Communication, XSS attacks and defenses, etc. Advanced topics. Security monitoring, surreptitious communication, data remanence, trusted devices, privacy and security of low powered devices (RFID) electronic voting, quantum cryptography, penetration analysis, digital rights management and copy protection, security and the law.

List of Text Books:

1. Cryptography and Network Security: Principles and Practice, 6th Edition, William Stallings, 2014, Pearson, ISBN13:9780133354690.
2. Computer Security: A Hands-on Approach, Wenliang Du, CreateSpace Independent Publishing Platform; 1-st edition (2017)
3. Cryptography: Theory and Practice, Third Edition, Douglas R. Stinson, CRC (2005)

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY
BHOPAL - 462003

List of Reference Books:

1. Network Security: Private Communications in a Public World, M. Speciner, R. Perlman, C. Kaufman, Prentice Hall, 2002.
2. Network Security, Firewalls And VPNs, J. Michael Stewart, Jones & Bartlett Learning, 2013, ISBN-10: 1284031675, ISBN-13: 978-1284031676.
3. The Network Security Test Lab: A Step-By-Step Guide, Michael Gregg, Dreamtech Press, 2015, ISBN-10:8126558148, ISBN-13: 978-8126558148.

URLs:

1. https://nptel.ac.in/courses/106105031/

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY,
BHOPAL - 462003

Name of Program	**M.Tech**	**Semester I**	**Year I**
Name of Course	Cybercrime & Information Warfare		
Course Code	IS 103		
Core / Elective / Other	Core		

Prerequisite:	
1.	This Course doesn't require any prerequisites, but the basic knowledge of computers security is desired.
2.	General awareness of how information is shared in cyber space.
Course Outcomes:	
1.	Understand and identify the features and typologies of various challenges to crime and cyberspace patterns.
2.	Analyze how national and non-national actors utilize the Internet as a medium of attacks in cyber warfare to penetrate automated networks and seize control of critical infrastructure by case studies
3.	Identify the role of the Web as a medium for hiring, communicating and funding extremism and Analyze the technological, social and political dynamics of cyber terrorism and the war against intelligence.
4.	Grow the ability to perform integrated and autonomous research through theoretical and practical presentations
Description of Contents in brief:	
1.	A brief Introduction of cybercrime, the evolution of cybercrime, challenges of cyber Crime, categorizing cybercrime, cyber terrorism, virtual crimes, and perception of Cyber criminals, their motives, type, and organization.
2.	Cyber Crime Cases: Money Laundering, Bank Fraud, Advance Fee Fraud, Malicious Agents, Stock Robot Manipulation, Identity Theft, Digital Piracy, Intellectual Property Crime, Internet Gambling.Tools used to implement attacks, System Protection against attack.
3.	Perception of cyber criminals: hackers, insurgents and extremist groups, Interception of data, surveillance and protection, criminal copy right infringement, cyber stalking. Hiding crimes in cyberspace and methods of Concealment.
4.	Privacy in cyber space: web defacements and semantic attacks, DNS attacks, code injection attacks. The challenges of fighting cybercrime: Opportunities, General challenges, Legal Challenges
5.	Information Warfare concept: information as an intelligence weapon, attacks and retaliation, attack and defense. Information Warfare Strategies and Tactics from a Military Perspective, Information Warfare Strategies and Tactics from a Corporate Perspective, Strategies and Tactics from a Terrorist and Criminal Perspective An I-War risk analysis model, implication of I-WAR for information managers, Perceptual Intelligence and I-WAR, Handling Cyber Terrorism and information warfare, Jurisdiction
6	Development of Capability to analyze and prognosis the potential of Socioeconomic, sociopolitical impact that can be exerted by a rumor.
List of Reference Books:	
1.	Principles of cybercrime, Jonathan Clough Cambridge University Pres
2.	Information Warfare: Corporate attack and defence in digital world, William Hutchinson, Mathew Warren, Elsevier.
3.	Cyber security and cyber warp. W. Singer and Allan Friedma

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY,
BHOPAL - 462003

URLs:	
1.	https://swayam.gov.in/nd2_nou19_cs08/

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL - 462003

Name of Program M.Tech. (IS) **Semester** I[st] **Year I**

Name of Course MALWARE ANALYSIS AND REVERSE ENGINEERING

Course Code IS-1104

Core / Elective / Other Core

Prerequisite:

1. Operating System Design
2. Programming
3. Software Engineering
4. Computer and Network Security

Course Outcomes:

1. To understand the concept of malware and reverse engineering.
2. Implement tools and techniques of malware analysis.

Description of Contents in brief:

Fundamentals of Malware Analysis (MA), Reverse Engineering Malware (REM) Methodology, Introduction to key MA tools and techniques, Behavioral Analysis vs. Code Analysis, Resources for Reverse-Engineering Malware (REM) Understanding Malware Threats, Malware indicators, Malware Classification, Examining ClamAV Signatures, Creating Custom ClamAV Databases, Using YARA to Detect Malware Capabilities, Creating a Controlled and Isolated Laboratory, Introduction to MA Sandboxes, Ubuntu, Zeltser'sREMnux, SANS SIFT , Sandbox Setup and Configuration New Course Form, Routing TCP/IP Connections, Capturing and Analyzing Network Traffic, Internet simulation using INetSim, Using Deep Freeze to Preserve Physical Systems, Using FOG for Cloning and Imaging Disks ,Using MySQL Database to Automate FOG Tasks, Introduction to Python ,Introduction to x86 Intel assembly language, Scanners, Analysis Automation Tools. Malware Forensics: Using TSK, Microsoft Offline API to Registry Discoveries, Packers, Registry Forensics, Locked Files, Conficker's File System, ACL Restrictions, Rogue PKI Certificates. Malware and Kernel Debugging: Opening and Attaching to Processes, Shellcode Analysis, Controlling Program Execution, Breakpoints**,** DLL Export Enumeration, Execution, and Debugging**,** Introduction to WinDbg Commands and Controls, Detecting Rootkits with WinDbgScripts**,** Kernel Debugging with IDA Pro. Memory Forensics and Volatility: Memory Dumping, Windows Memory Toolkit**,** Accessing VM Memory Files, Investigating Processes in Memory Dumps**,** Code Injection and Extraction**,** Detecting and Capturing Suspicious Loaded DLLs**,** Finding Artifacts in Process Memory**,** Identifying Injected Code with Malfind and YARA. Researching and Mapping Source Domains/IPs: Using WHOIS to Research Domains**,** DNS Hostname Resolution**,** Querying Passive DNS**,** Checking DNS Records**,** Reverse IP Search New Course Form**,** Creating Static Maps**,** Creating Interactive Maps.

List of Text Books:

1. No text book is recommended, subject will be taught using the material available

on internet and research papers.

List of Reference Books:

1. Michael Sikorski, Andrew Honig “Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software” publisher Williampollock
2. “The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System” Second Edition by Reverend Bill Blunden
3. “Practical Reverse Engineering” by Dang, Gazet, Bachaalany
4. “Rootkits: Subverting the Windows Kernel” by Jamie Butler and Greg Hoglund

URLs

1. https://people.sgu.ac.id/charleslim/mlw-tutorial/
2. https://cybersecurity.att.com/blogs/labs-research/reverse-engineering-malware
3. https://www.sciencedirect.com/book/9781597492683/malware-forensics
4. https://www.sciencedirect.com/topics/computer-science/malware-forensics
5. https://bugs.python.org/file47781/Tutorial_EDIT.pdf
6. https://www.cs.virginia.edu/~evans/cs216/guides/x86.html
7. https://www.digitalocean.com/community/tutorials/an-introduction-to-dns-terminology-components-and-concepts

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL - 462003

Name of Program M.Tech.(IS) **Semester** 2nd **Year I**

Name of Course APPLIED CRYPTOGRAPHY

Course Code IS-201

Core / Elective / Other Core

Prerequisite:

1. Algorithms
2. Mathematical Foundation Of Information Security
3. Computer and Network Security

Course Outcomes:

1. Describe how various cryptography algorithms and protocols work.
2. Study the mathematical foundations of cryptographic schemes.
3. Understand the design philosophy of encryption schemes.
4. Evaluate the security of the ciphers using rigorous approaches.
5. Understand various cryptographic applications.

Description of Contents in brief:

Introduction to cryptography, Classical cipher and cryptanalysis: Shift, Substitution, Affine, Vigenere, Hill, Permutation, Playfair cipher. Perfect secrecy, one-time pad cipher, Spurious keys and unicity distance. Classes of cryptanalysis attacks: Ciphertext-only, Known-Plaintext attack, Chosen-Ciphertext attack and Chosen-plaintext attack. Symmetric Cryptography and cryptanalysis: DES, AES, Differential and Linear cryptanalysis, modes of operation. Cryptographic hash functions: design properties, data integrity, security, SHA, CBC-MAC. Mathematics and Hardness assumptions of asymmetric cryptography such as Factorization, Discrete Logarithm, Primality testing, and Factoring algorithms. Asymmetric cryptography: RSA, ElGamal cryptosystem, Elliptic curve cryptosystems. Protocols and concepts: Key-Distribution - Diffie-Hellman, Digital signatures, Homomorphic encryption, Zero-Knowledge Proofs, Bit-commitment, Oblivious Transfer, Dual-Receiver encryption, Broadcast encryption, Public-Key Infrastructure (PKI), Kerberos, Bitcoin and Blockchain.

List of Text Books:

1. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd edition, by Bruce Schneier, John Wiley & Sons Publication

List of Reference Books:

1. Cryptography Theory and Practice, Douglas R. Stinson
2. Introduction to Modern Cryptography, Jonathan Katz, Yehuda Lindell, Chapman & Hall/CRC
3. Cryptography and Network Security: Principles and Practice, William Stallings

SMAULANA AZAD NATIONAL INATITUTE OF TECHNOLOGY, BHOPAL - 462003

Name of Program	**M.tech (Information Security)**	**Semester II**	**Year I**
Name of Course	Database Security and Access Control		
Course Code	IS 202		
Core / Elective / Other	Core		

Prerequisite:

1. Fundamental knowledge of database
2. Familiarity with SQL and Oracle

Course Outcomes:

1. Students will be enabled to understand and implement classical models and algorithms.
2. students will be enabled to understand database access control methods for secure database application development.
3. students will learn how to analyze the data, identify the problems, design secure database, assess the weaknesses of various access control models and to analyze their behavior.

Description of Contents in brief:

1. Introduction to Access Control, Purpose and fundamentals of access control,Policies of Access Control, Models of Access Control, and Mechanisms, Discretionary Access Control(DAC), Non-Discretionary Access Control, Mandatory Access Control (MAC).
2. Capabilities and Limitations ofAccess Control Mechanisms: Access Control List (ACL) and Limitations, Capability List and Limitations, Role-Based Access Control (RBAC) and Limitations, Core RBAC, Hierarchical RBAC, Statically Constrained RBAC, Dynamically Constrained RBAC, Limitations of RBAC.
3. Comparing RBAC to DAC and MAC Access control policy, Biba's intrigity model, Clark-Wilson model, Domain type enforcement model, mapping the enterprise view to the system view, Role hierarchies-inheritance schemes, hierarchy structures and inheritance forms, using SoD in real system, Temporal Constraints in RBAC, MAC AND DAC.
4. Integrating RBAC with enterprise IT infrastructures: RBAC for WFMSs, RBAC for UNIX and JAVA environments Case study: Multiline Insurance Company.
5. Smart Card based Information Security, Smart card operating system-fundamentals, design and implantation principles, memory organization, smart card files, file management, atomic operation, smart card data transmission ATR,PPS Security techniques-user identification, smart card security, quality assurance and testing, smart card life cycle-5 phases, smart card terminals.

List of Text Books:

1. Database Security by Silvano Castano, Fugini, Martella, Samarati – Addison Wesley

2. Implementing Database Security and Auditing: Includes Examples for Oracle, SQL Server,Db2 Udb, Sybase. Ben-Natan, R. B. 2005, Digital Press

List of Reference Books:

1. Role Based Access Control: David F. Ferraiolo, D. Richard Kuhn, Ramaswamy Chandramouli.

2. Michael J. Hernandez, Database Design for Mere Mortals: A Hands-On Guide to Relational Database Design 3rd Edition

URLs:

1. http://www.fit.vutbr.cz/~cvrcek/confers98/datasem/datasem.html.cz

2. http://www.smartcard.co.uk/tutorials/sct-itsc.pdf: Smart Card Tutorial.

3.

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL - 462003

Name of Program **M.Tech.** **Semester - II** **Year 1st**

Name of Course **Digital Forensics**

Course Code **IS 203**

Core / Elective / Other **Core**

Prerequisite:

1. Good skills and concept of programming.
2. Sound knowledge of Windows and UNIX operating systems.
3. Knowledge of Networking.

Course Outcomes: (After completion of course, students would be able to:)

1. Build a solid foundation for computer forensics and digital investigation and its processes, policies and procedures.
2. Understand relevant legislation and codes of ethics.
3. Collection of evidence, understand guidelines and standard of tools and environment.

Description of Contents in brief:

1. Introduction to Digital Forensics and Digital Evidences, Acquisition and Handling of Digital Evidences, and Analysis of Digital Evidences
   - This covers the definition, scope, goals and various framework of digital forensics
   - This includes definition and importance of digital evidence, working with autospy
2. Incident Response Methodology, Live Data Collection: Windows System and UNIX systems
   - This provides the response strategy on occurring of an incidence and its proper solutions, and the path to collection of data such as host-based data, file system data and creation of response toolkit.
3. Network Forensics: requirement for preservation of network data, Email Forensics: email forensics steps, Mobile Device Forensics: mobile forensics procedures, Cloud Forensics: challenges to cloud forensics, specialized tools related to forensics
   - This describes how to perform network monitoring, email forensics, mobile phone forensics and cloud forensics and obtain evidence by interviewing system administrators, managers and other personnel,
4. Intrusion Detection and Intrusion Forensics
   - This explains analyzing computer intrusions and analysis of an attack using intrusion forensics
5. Validation of Digital Forensics Tools, Log Correlation: Tools and Techniques, Crime Text Mining Approach
   - This describes verification of tools that is truly “forensic” i.e. capable of meeting the requirements of the ‘trier of fact’ and how to avoid points of failure on auditing and investigating of logs with special emphasis on the tools and techniques for managing these logs.

List of Text Books:

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY,
BHOPAL - 462003

1. Digital Forensic- The Fascinating World of Digital Evidences, Nilakshi Jain and Dr. Dhananjay R. Kalbande, Wiley Publication,2017. (1-3)
2. Computer and Intrusion Forensics, G.Mohay,A.Anderson,B.Collie,O.D.Vel, R.McKemmish, ISBN 1-58053-369-8 (4)
3. Digital Crime and Forensic Science in Cyberspace, P.Kanellis, E.Kiountouzis,N.Kolokotronics, D.Matakos, IDEA group publishing, ISBN 1-59140-873-3 (5)

List of Reference Books:

1. Cyber Forensics, Dejey and Murugan, Oxford University Press, 2018
2. Digital Forensics and Incident Response- an intelligent way to respond to attacks, Gerard Johansen, Packt Publication, 2017

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY,
BHOPAL - 462003

Name of Program **M. Tech**

Name of Course Biometrics

Course Code IS 501

Core / Elective / Other **Group A: Program Electives**

Prerequisite:

1. Good Knowledge of digital Image Processing / computer Graphics /
2. Linear algebra
3. Probabilities and Statistics
4. Matlab

Course Outcomes:

1. To understand the state-of-the-art in biometric technologies
2. To survey the currently available biometric systems
3. To enable design of biometric system
3. To explore ways to improve some of the current and new techniques
4. To learn and implement some of the biometrics authentication
6. Perform R&D on biometrics methods and systems.
7. A good understanding of the various modules constituting a biometric system.
8. Familiarity with different biometric traits and to appreciate their relative significance.
9. A good knowledge of the feature sets used to represent some of the popular biometric traits.
10. Evaluate and design security systems incorporating biometrics.
11. Recognize the challenges and limitations associated with biometrics.

Description of Contents in brief:

1. **Biometrics-Introduction :** benefits of biometrics over traditional authentication systems -benefits of biometrics in identification systems-selecting a biometric for a system.

2. **History of Biometrics :** Evolution of biometric system with respect to time

3. **Types of Biometric :**

   Physical : Fingerprints, Hand Geometry, Retina Scanning, Iris scanning , Facial Recognition, DNA, Behavioral : Signature, Voice, Key stroke pattern, Gait Body dynamics

4. **Technical description:** strengths, weaknesses, Hand scan DNA biometrics. Handprint Biometrics DNA Biometrics.

5. **Multi biometrics and multi factor biometrics:** Limitations of unimodal systems, Multibiometric scenarios, Levels of fusion, user-specific parameters, and soft biometrics

6. **Biometric System Security:** Standards, Databases, Patient Records, Biometrics in Credit Cards, Identification Forensic Odontology, Case Study Presentations

List of Text Books:

Digital Image Processing using MATLAB, By: Rafael C. Gonzalez, Richard Eugene Woods, 2nd Edition, Tata McGraw-Hill Education 2010

Biometrics for network security,Paul Reid, Hand book of Pearson

A. Jain, R. Bolle, S. Pankanti, (Ed.), BIOMETRICS: Personal Identification in Networked Society , KluwerAcademic Publishers, 1999. ISBN 0-7923-8345-1. TK7882.P3 B36

J. Ashbourn, Biometrics: Advanced Identity Verification, Springer-Verlag, 2000. ISBN 1-85233-243-3. TK7882.P3 A84

Guide to Biometrics, By: Ruud M. Bolle, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, Jonathan H. Connell, Springer 2009

Pattern Classification, By: Richard O. Duda, David G.Stork, Peter E. Hart, Wiley 2007

List of Reference Books:

1. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition,
Springer Verlag, 2003.

2. A. K. Jain, R. Bolle, S. Pankanti (Eds.), BIOMETRICS: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999.

3. J. Wayman, A.K. Jain, D. Maltoni, and D. Maio (Eds.), Biometric Systems: Technology, Design and Performance Evaluation, Springer, 2004.

4. Anil Jain, Arun A. Ross, Karthik Nandakumar, Introduction to biometric, Springer,2011.

URLs:

1. https://nptel.ac.in/courses/106104119/
2. https://www.tutorialspoint.com/biometrics/index.htm

3. https://www.mathworks.com/products/matlab.html

4. https://www.coursera.org/lecture/usable-security/biometric-authentication-RXVog

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY,
BHOPAL - 462003

Name of Program **M.Tech**

Name of Course Privacy: Data & User Protection

Course Code IS 502

Core / Elective / Other **Group A: Program Electives**

Prerequisite:

1. Basic knowledge of privacy and data protection legislation
2. Knowledge of General Data Protection Regulation is required.

Course Outcomes:

1. The general theme of this course is to provide students an overview for the security and privacy with a set of techniques, Which enable them to address the security & privacy challenges.
2. This course is intended for students and professionals in information policy, public policy, computer science, and information science who have an interest in work or research in security and privacy fields, or in support of those fields
3. The course will include individual reading and writing assignments, class discussion, case studies, and a group assignment. Students will have some latitude to tailor the assignments to their skills and interests.

Description of Contents in brief:

1. Introduction:-The increasing vulnerabilities of networks, Privacy issues, Privacy cost assessments in cyber attack, privacy-enhancing technologies
2. VPN, Privacy in RFID, Privacy in cyber physical systems and Internet of Things (IoT), Privacy measurement, Privacy policies and Enforcement, P3PPolicy, Policy Enforcement Techniques, Issues,
3. Models of Privacy: Machine Readable Policy. Internet Privacy:- Internet Privacy, Importance of good password, Minimizing your Online Digital Fingerprints, Preventing Identity Theft and Fraud, Risk, Privacy concerns in big data
4. Web Privacy:-Dangers of Wireless Networks and "Hotspots", Securing Devices, Using Encryption to Hide and Keep Safe your Personal Digital Items, Information and Data, Torrent File Sharing and Anonymous on the web, Secure
5. Private and Anonymous Usenet. Social Networks Privacy and security on Social Media. Threats to privacy in OSNs Threats regarding awareness, control, trustworthiness. Children's Privacy, Online Advertising, Digital Afterlife, Health and Genetic Privacy.

List of Text Books:

1. International Guide to Privacy – American Bar Association (Privacy)
2. International Guide to Cyber Security – American Bar Association (Cyber Security)
3. Roadmap to an Enterprise Security Program - American Bar Association (Roadmap)

List of Reference Books:

1. Complete guide to Internet Privacy, Anonymity and Security (Matthew Bailey)
2. Internet Privacy: Options for adequate realization edited (Johannes Buchman)
3. Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things Aurelia Tamò-Larrieux

URLs:

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL - 462003

1. Case studies from the Harvard Business School. These materials are available from http://cb.hbsp.harvard.edu/cb/access/5263390
2. Big data privacy: a technological perspective and review : https://journalofbigdata.springeropen.com/articles/10.1186/s40537-016-0059-y
3. Privacy and Its Importants: **https://iapp.org/about/what-is-privacy/**

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY,
BHOPAL - 462003

Name of Program **M.Tech**

Name of Course Secure Software Engineering

Course Code IS 503

Core / Elective / Other **Group A: Program Electives**

Prerequisite:

1. The basic knowledge about the principles of software engineering.
2. The software lifecycle.
3. Sufficient programming skills for the team development project.

Course Outcomes:

1. Students will author a software requirements document.
2. Students will demonstrate an understanding of the proper contents of a software requirements document.
3. Students will author a formal specification for a software system.
4. Students will demonstrate an understanding of distributed system architectures and application architectures..
5. Students will demonstrate an understanding of the differences between real-time and non-real time systems.
6. Students will demonstrate proficiency in rapid software development techniques

Description of Contents in brief:

1. Security a software Issue: introduction, the problem, Software Assurance and Software Security, Threats to software security, Sources of software insecurity, Benefits of Detecting Software Security What Makes Software Secure: Properties of Secure Software, Influencing the security properties of software, Asserting and specifying the desired security properties?
2. Requirements Engineering for secure software : Introduction, the SQUARE process Model, Requirements elicitation and prioritization
3. Secure Software Architecture and Design: Introduction, software security practices for architecture and design: architectural risk analysis, software security knowledge for architecture and design: security principles, security guidelines and attack patterns Secure coding and Testing: Code analysis, Software Security testing, Security testing considerations throughput the SDLC
4. Security and Complexity: System Assembly Challenges: introduction, security failures, functional and attacker perspectives for security analysis, system complexity drivers and security
5. Governance and Managing for More Secure Software: Governance and security, Adopting an enterprise software security framework, How much security is enough?, Security and project management, Maturity of Practice

List of Text Books:

1. Software Security Engineering: Julia H. Allen, Pearson Education

2. Developing Secure Software: Jason Grembi, Cengage Learning

List of Reference Books:

1. Software Security : Richard Sinn, Cengage Learning

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL - 462003

Name of Program **M-Tech (IS)**

Name of Course **STEGANOGRAPHY AND DIGITAL WATERMARKING**

Course Code **IS504**

Core / Elective / Other **Group A: Program Electives**

Prerequisite:

1. Digital Image Processing, Image Analysis

Course Outcomes:

1. Learn the concept of information hiding.
2. Survey of current techniques of steganography and learn how to detect and extract hidden information.
3. Learn watermarking techniques and through examples understand the concept.

Description of Contents in brief:

Steganography: Overview, History, Methods for hiding (text, images, audio, video, speech etc.), Issues: Security, Capacity and Imperceptibility, Frameworks for secret communication (pure Steganography, secret key, public key steganography), Steganography algorithms (adaptive and non-adaptive), Steganography techniques: Substitution systems, Spatial Domain, Transform domain techniques, Spread spectrum, Statistical steganography, Cover Generation and cover selection, Tools :EzStego, FFEncode, Hide 4 PGP, Hide and Seek, S Tools etc.)

Steganalysis: Active and Malicious Attackers, Active and passive steganalysis, Detection, Distortion, Techniques: LSB Embedding, LSB Steganalysis using primary sets, Texture based

Digital Watermarking: Introduction, Difference between Watermarking and Steganography, History, Classification (Characteristics and Applications),

Types and techniques (Spatial-domain, Frequency-domain, and Vector quantization based watermarking), Attacks and Tools (Attacks by Filtering, Re-modulation, Distortion, Geometric Compression, Linear Compression etc.), Watermark security & authentication.

List of Text Books: No text book is recommended, subject will be taught using the material available on internet and research papers.

List of Reference Books:

1. Peter Wayner, "Disappearing Cryptography – Information Hiding: Steganography & Watermarking", Morgan Kaufmann Publishers, New York, 2002.

2. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, TonKalker, "Digital Watermarking and Steganography", Margan Kaufmann Publishers, New York, 2008.
3. Information Hiding: Steganography and Watermarking-Attacks and Countermeasures by Neil F. Johnson, Zoran Duric, SushilJajodia
4. Information Hiding Techniques for Steganography and Digital Watermarking by Stefan Katzenbeisser, Fabien A. P. Petitcolas

URLs

1. https://www.garykessler.net/library/steganography.html
2. https://www.hindawi.com/journals/jcnc/2018/9475142/
3. https://www.matec-conferences.org/articles/matecconf/pdf/2016/20/matecconf_icaet2016_02003.pdf
4. https://www.commonlounge.com/discussion/4bc16dbc2c7145ff87ad0f0d5401a242
5. https://www.cl.cam.ac.uk/teaching/0910/R08/work/essay-ma485-watermarking.pdf
6. https://arxiv.org/ftp/arxiv/papers/1407/1407.4735.pdf

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY,
BHOPAL - 462003

Name of Program **MTech**

Name of Course **Security Threats and Modelling**

Course Code **IS 505**

Core / Elective / Other **Group A: Program Electives**

Prerequisite:

1. Understanding of the general principles of information technology security,
2. Awareness of the issues involved with security control activity would be advantageous.
3. Basic knowledge of IT

Course Outcomes:

1. After completing this course, the student would be having a deep understanding of variety of threats and would be well versed with Threat Modelling Methodologies.
2. Would be able to Find, Address and mitigate Threats
3. Would know about the state-of-the -art Modelling tools

Description of Contents in brief:

1. Threats and Basics of Threat Modelling: Vulnerabilities and Malicious Software--Types of Malicious Software and counter measures-- Definition and necessity of Threat modelling.- Strategies for Threat Modelling -- Structured approaches to threat modelling -- Focusing on assets. -- Software, attackers, Software models to Threats.

2. Finding Threats: STRIDE Model:- Spoofing Threats—Tampering Threats--Repudiation Threats--Information Disclosure Threats-- Denial-of-Service Threats and Elevation Threats. Working with Attack Trees--Representing a Tree--Example Attack Tree OWASP .

3. Processing and managing threats: Defensive tactics and technologies -- Authentication, Integrity, --Non-Repudiation—Confidentiality—Availability--Authorization. -- Addressing threats with patterns--Standard Deployments and Addressing CAPEC Threats --Mitigating Privacy Threats
4. Trade-offs Associated with Addressing Threats: Classic Strategies for Risk –Management-Selecting Mitigations for Risk Management -- Threat-Specific Prioritization Approaches--Mitigation via Risk Acceptance-- Threat Modelling Tools-- Microsoft Threat Modelling tool--TRIKE, OWASP.
5. Thread Modelling in Technologies: Web and Cloud threats— Mobile Threats –Cloud Provider Threats. Accounts and Identity – Account life cycle-Authentication - Recovery.
   Human Factor and Usability: Models of Software scenarios—Threat elicitation techniques – Tools and techniques for addressing Human Factor—User Interface tools and Techniques, Perspective on Usability and Ceremonies.

List of Text Books:

1. Threat Modelling: Designing for Security: Adam Schostak, WILEY. {Ch 1,2,3,4,5}

2. Cryptography and Network Security Principles and Practices: William Stallings, PRENTICE HALL. {Ch 1,2}

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL - 462003

Name of Program **M Tech**

Name of Course **Penetration Testing and Vulnerability Assessment**

Course Code IS 106

Core / Elective / Other **Group A: Program Electives**

Prerequisite:

1. Initial Assessment: Identify the assets and define the risk and critical value for each device (based on the client input), such as a security assessment
2. Vulnerability scanner: It's important to identify at least the importance of the device that you have on your network or at least the devices that you'll test.
3. Understand the strategic factors and have a clear understanding of details.

Course Outcomes:

1. penetration testing and security auditing platform with advanced tools to identify, detect, and exploit any vulnerability uncovered in the target network environment
2. Applying appropriate testing methodology with defined business objectives and a scheduled test plan will result in robust penetration testing of your network
3. Penetration Testing/Security Analysts is a procedure of analyzing the security of a computer system or network which makes impermeable for an attacker

Description of Contents in brief:

1. Introduction to Penetration Testing and Methodologies, software installation, Information gathering, Concept of ethical hacking and essential Terminologies, Threat, Attack, Vulnerabilities, Target of Evaluation, Exploit. Phases involved in hacking
2. Vulnerabilities Scan : introduction to vulnerability exploit, threat and risk ,Ethical requirements and legal issuesPenetration Testing Scoping and Engagement Methodology
   Port scanning and OS fingerprinting. Man in the middle attacks, Spoofing and Sniffing attacks, Wireshark.
3. Scanning and exploits: Scanning and Service Enumeration Vulnerability detection methods, configure Vulnerability toolTypes of scanners, Scanning using nmap, Scanning using Nessus, Nexpose, Penetration test 1report structure and components.
   DNS,TCP, UDP, connections Client-Side Attacks with Metasploit Exploiting Network Services and Leveraging the Meterpreter.
4. Analyzing Vulnerabilities and Exploits:Types of exploits: worm, spyware, backdoor, rootkits, Denial of Service (DoS),Deploying exploit frameworks, Vulnerabilities in infrastructure support servers Network management tool attacks, Identifying Snort IDS bypass attacks Choosing credentials, ports and dangerous tests.
5. Social Engineering Penetration Testing Methodology, Information gathering toolsNetwork Penetration Testing methedology - External Module, Network Penetration Testing Methodology-Internal Module, Network Penetration Testing- Parameter Devices Module
6. Vulnerability mapping Target exploitation. Web Application Penetration Testing, :introduction to web application penetration testing.
7. Burp suit tool. Browser proxies and non-rendered content, Cross-site scripting and cross-site request forgery,Web authentication and session management, Session Hijacking, Web Application Security.
8. Metasploit exploitation framework, Database Penetration Testing:, Databases, SQL, SQL Injection,Database security, Hijacking windows with using RAT and Trojan.Wireless Penetration Testing Methodology ModuleCloud Penetration Testing Methodology Module

Report Writing and Post Test Actions.

List of Text Books:

1. Penetration Testing - A hands-on introduction to Hackingby Georgia Weidman (1,2,3,4,5,8)
2. Network Vulnerability Assessment by Sagar Rahalkar(1,3,4,6,7,8)
3. Metasploit - The Penetration Tester's Guide by David Kennedy , Jim O'gorman , Devon Kearns and Mati Aharoni – NoStarch Press Publication
4. Hacking Exposed Web Application, 3rd Edition by Joel Scambray, Vincent Liu, Caleb Sima

List of Reference Books:

1. The Browser Hacker’s Handbook by Wade Alcorn, Christian Frichot and Michele Orru – Wiley Publication
2. Web Penetration Testing with Kali Linux by Joseph Muniz, Aamir Lakhan – Packt Publication
3. The Web Application Hecker’s Handbook 2 – Dafydd Stuttard , Marcus Pinto

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL - 462003

Name of Program **M.Tech.**

Name of Course **Ethical Hacking**

Course Code **IS-107/202**

Core / Elective / Other **Group A: Program Electives**

Prerequisite:

1. Basic Concept of Web programming, Operating System and Networking
2. Good problem-solving skills and analytical skills

Course Outcomes: (Students will be able to:)

1. Understand the core concepts related to vulnerabilities and their causes
2. Understand ethics behind hacking and vulnerabilities disclosure
3. Appreciate the impact of hacking
4. Exploit the vulnerabilities related to computer system and networks using state of the art tools and technologies

Description of Contents in brief:

1. Ethical hacking Overview
   - This covers the definition of ethical hacking and describes what is legal and what is not legal
2. TCP/IP Concepts Review, Network and Computer Attacks, Network enumeration and Foot printing- DNS query, Whois query, OS finger printing, Banner grabbing
   - This provides overview of TCP/IP and numbering system along with IP Addressing and intruder attacks.
3. Programming for security professionals- Web application vulnerabilities, Buffer overflow attack, Session hijacking, Code injection attacks- Cross Site Scripting attack, SQL injection attack
   - This cover understanding of practical extraction of programming vulnerabilities
4. Password hacking, windows hacking, network hacking, anonymity and email hacking
   - This covers practical exposures to password hacking related to windows and email and also explains anonymity and network vulnerabilities.
5. Web servers hacking, session hijacking, Surveillance, desktop and server OS Vulnerabilities, Database attacks, cryptography, Hacking wireless networks network protection systems, Trojan and backdoor applications, legal resources, virtualization.
   - This describes wireless network standards, authentication and wardriving, firewalls, snort rules, honeypots and intrusion detection systems (IDS), methods of surveillance, various vulnerabilities related to OS and various web based and DB attacks, and explains different types of malware and its applications

List of Text Books:

1. Ethical Hacking and Network Defense. Michael T. Simpson, Kent Backman, James Corley (1-3, 5)
2. Hacking Exposed6 – Network Security secrets and solutions, S.McClure, J.Scambray,

G.Kurtz, McGrawHill (4)

List of Reference Books:

1. CEH, Review Guide, Kimberly Graves, Wiley Publication

2. Network Security Hacks, Andrew Lockhart, O'Reilly Publication

URLs:

https://nptel.ac.in/courses/106105217/

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL - 462003

Name of Program **M. Tech Information Seurity**

Name of Course Security Operations and Incidence Response

Course Code IS 508

Core / Elective / Other **Group A: Program Electives**

Course Outcomes:

1. Students will learn about Security policies and Industrial best practices
2. Security standards and audit, Cyber Laws and Legal system
3. Computer emergency readiness, Computer security incident response, Computer Emergency Response Team (CERT)

Description of Contents in brief:

1. Security Governance Control Framework, Strategy, Security policies, Security audits, Standards and Best practices
2. Evaluating Incident Management Capabilities: incident handling lifecycle, code of conduct, detecting and analyzing incidents, identifying the cause of vulnerabilities, performing triage, data loss prevention techniques
3. Risk Diagnostic for Incident: artifact and malware analysis categories and techniques, Machine learning for risk identification
4. Incidence Response: Analyzing and coordinating response to major computer security events and incidents, Incident response procedure, developing and delivering effective communications, Machine learning for incident response
5. Operating system security threats and hardening of the OS
6. Cyber Laws: Legal and RegulatoryFramework, Indian and International Laws

List of Text Books:

1. Information SecurityGovernance: Framework and Toolset forCISOs and Decision Makers by Andrej Volchkov

List of Reference Books:

1. CISO Desk Reference Guide by Bill Bonney, Gary Hayslip,MattStampe
2. CISO Compass: Navigating Cybersecurity LeadershipChallenges with Insights from PioneersbyTodd Fitzgerald

URLs:

1. https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P139
2. https://www.sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P23B

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY,
BHOPAL - 462003

Name of Program	**M.Tech**
Name of Course	**Internet Security Tools and Techniques**
Course Code	**IS-509**
Core / Elective / Other	**Group A: Program Electives**

Prerequisites:

1. Understanding of computer networks, OSI Model, TCP/IP Model.
2. Knowledge of information security and network security.
3. Basic understanding of vulnerabilities in the internet.

Course Outcomes:

1. Understanding of cyber-attacks and cyber threats.
2. Knowing various cyber security tools and their applications on various security problems.
3. Usage of different cyber security techniques.

Description of Contents in brief:

1. Introduction to Internet Security: Introduction to internet security, understanding the importance of internet security, goals of internet security.
2. Types of Cyber-attacks: Understanding the types of cyber-attacks, different types of cyber attackers.
3. Cyber Security Technologies: Understanding the technologies like VPNs, intrusion detection, digital signature, and access control.
4. Cyber Security tools: Knowing different types of security tools like firewalls, antivirus software, penetration testing, and PKI services.
5. Cyber security challenges: Knowing different types of security challenges with real-life scenarios like ransom ware evolution, block chain revolution, IOT threats, AI expansion.

List of Textbooks:

1. Firewalls and Internet Security: Repelling the Wily Hacker by William R. Cheswick and Steve Bellovin.

2. Metasploit - The Penetration Tester's Guide by David Kennedy, Jim O'gorman , Devon Kearns and Mati Aharoni.

List of Reference Books:

1. Digital Signatures by Jonathan Katz.

2. Cyber Security: Threats and Responses for Government and Business.

URLs:

1. https://www.cs.tau.ac.il/~tromer/courses/infosec11/lecture11.pdf
2. https://www.javatpoint.com/cyber-security-tools
3. https://www.techrepublic.com/article/a-beginners-guide-to-public-key-infrastructure/

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL - 462003

Name of Program **M.tech(Information Security)**

Name of Course Information Risk Management and Compliance

Course Code IS 510

Core / Elective / Other **Group A: Program Electives**

Prerequisite:

1. Fundamental knowledge of computer network
2. Fundamental knowledge of internet security
3. Familiarity with of C/C++

Course Outcomes:

1. To develop skills of high order so as to provide thorough knowledge and insight into the spectrum of risks faced by an organization.
2. Understand the concept of risk management as well as processes and techniques that can ensure the effectiveassessment, monitoring and control of risk at all levels.
3. To develop the ability to devise and implement adequate and effective systems to ensure compliance of all applicable laws.

Description of Contents in brief:

1. An introduction to risk management: introduction to the theories of risk management, the changing environment, the art of managing risks.
2. Threat assessment process: threat assessment and its input to risk assessment, threat assessment method, example threat assessment.
3. Vulnerability issues: operating system vulnerabilities, application vulnerabilities, public domain or commercial off-the-shelf software, connectivity and dependence, vulnerability assessment for natural disaster, vulnerability of critical infrastructures.
4. Risk process, analysis, tools and types of risk assessment: qualitative and quantitative risk assessment, policies, proceduresand processes of risk management; integrated risk management, future of the risk management.
5. compliance management: compliance program, compliance and risk management, ensuring adequacy and effectiveness of compliance system, internal compliance reporting mechanisms, internal control, reporting, website management.

List of Text Books:

1. Malcolm Harkins, Managing Risk and Information Security, Apress, 2012.
2. Daniel Minoli, Information Technology Risk Management in Enterprise Environments, Wiley, 2009.
3.

List of Reference Books:

1. Andy Jones, Debi Ashenden,Risk Management for Computer Security: Protecting Your Network & Information Assets, 1st Edition, Butterworth-heinemann, Elsevier, 2005.
2. Andreas Von Grebmer, Information and IT Risk Management in a Nutshell: A pragmatic approach to Information Security, 2008, Books On Demand Gmbh.
3.

URLs:

1. https://ocw.mit.edu/courses/sloan-school-of-management/15-997-practice-of-finance-advanced-corporate-risk-management-spring-2009/
2. https://nptel.ac.in/courses/110107128/

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY,
BHOPAL - 462003

Name of Program **M.Tech**
Name of Course **Intellectual Property and Espionage**
Course Code **IS-511**

Core / Elective / Other **Group A: Program Electives**

Prerequisite:

1. Understanding Copyright and Related Rights.
2. Understanding knowledge and application of laws governing copyrights, patents, trademarks and trade secrets.
3. Understanding fundamentals underpinning copyright law and practice, and describe the different types of rights which copyright and related rights law protects

Course Outcomes:

1. The students once complete this course, shall get an adequate knowledge on patent and copyright for their innovative research works
2. During their research career, information in patent documents provide useful insight on novelty of their idea from state-of-the art search. This provide further way for developing their idea or innovations

Description of Contents in brief:

1. History and International Regime: Pre- TRIPs and post TRIPs, Balancing Rights of the IPR Holder and the Society, PR and Human Rights, Concept of Intellectual Property Law Patents, Trademark, Geographical Indications, Copyright, Industrial Designs, Integrated Circuits Layout Designs, Trade Secrets or Undisclosed Information, Introduction to Competition Law Anti-Competitive Practices.
2. Introduction to Copyright, Meaning, Nature of Copyright - Subject matter of copyright: original literary, Justification, dramatic, musical, artistic works; cinematograph films and sound recordings - Registration Procedure, Term of protection, Ownership of copyright, Assignment and license of copyright - Infringement, Remedies & Penalties – Related Rights - Distinction between related Rights and copyrights.
   Industrial Design and Layout Designs of Integrated Circuit: Meaning, Scope and Registration, History, International Developments. Designs v/s Copyright and Trademark, Infringement and Remedies
3. Patent: Scope, Objectives and Justification, History and International Treaties, Patentability Criteria, Patentable and Non- patentable inventions, Registration, Ownership, Rights of Patentee, Transfer of technology, Working of Patents and Compulsory licensing, Infringement, Impact of TRIPs and TRIPs Flexibilities, Pharm patents via a Public Health Issues, Utility Patent
4. Trademark: Justification, History, and International Treaties, Different kinds of marks (brand names, logos, signatures, symbols, well known marks, certification marks and service marks) ,- Non Registrable Trademarks - Registration of Trademarks and Scope of Protection, Kinds : Conventional and Non-conventional, Rights of holder and assignment and licensing of marks, Infringement, Remedies & Penalties - Trademarks registry and appellate board
5. Other forms of IP: Design, Geographical Indication (GI), Plant Variety Protection, Layout Design Protection, Current Contour.

List of Text Books:

1. Nithyananda, K V. (2019). Intellectual Property Rights: Protection and Management. India, IN: Cengage Learning India Private Limited.(Ch:1,2,3,4,5)

2. Neeraj, P., & Khusdeep, D. (2014). Intellectual Property Rights.India, IN: PHI learning Private Limited.(Ch:1,2,3)

3.

List of Reference Books:

1. Ahuja, V K. (2017). Law relating to Intellectual Property Rights.India, IN: Lexis Nexis..

2. World Intellectual Property Organisation. (2004). WIPO Intellectual property Handbook. Retrieved from https://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo_pub_489.pdf

URLs:

1. https://nptel.ac.in/courses/110105139/

2. http://www.bdu.ac.in/cells/ipr/docs/syllabus.pdf

3. http://ili.ac.in/4_Intellectual%20Property%20Rights.pdf

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL - 462003

Name of Program **M-Tech (IS)**

Name of Course **STEGANOGRAPHY AND DIGITAL WATERMARKING**

Course Code **IS-601**

Core / Elective / Other **Group B:Department Electives**

Prerequisite:

1. Digital Image Processing, Image Analysis

Course Outcomes:

1. Learn the concept of information hiding.
2. Survey of current techniques of steganography and learn how to detect and extract hidden information.
3. Learn watermarking techniques and through examples understand the concept.

Description of Contents in brief:

Steganography: Overview, History, Methods for hiding (text, images, audio, video, speech etc.), Issues: Security, Capacity and Imperceptibility, Frameworks for secret communication (pure Steganography, secret key, public key steganography), Steganography algorithms (adaptive and non-adaptive), Steganography techniques: Substitution systems, Spatial Domain, Transform domain techniques, Spread spectrum, Statistical steganography, Cover Generation and cover selection, Tools :EzStego, FFEncode, Hide 4 PGP, Hide and Seek, S Tools etc.)

Steganalysis: Active and Malicious Attackers, Active and passive steganalysis, Detection, Distortion, Techniques: LSB Embedding, LSB Steganalysis using primary sets, Texture based

Digital Watermarking: Introduction, Difference between Watermarking and Steganography, History, Classification (Characteristics and Applications),

Types and techniques (Spatial-domain, Frequency-domain, and Vector quantization based watermarking), Attacks and Tools (Attacks by Filtering, Re-modulation, Distortion, Geometric Compression, Linear Compression etc.), Watermark security & authentication.

List of Text Books: No text book is recommended, subject will be taught using the material available on internet and research papers.

List of Reference Books:

1. Peter Wayner, "Disappearing Cryptography – Information Hiding: Steganography & Watermarking", Morgan Kaufmann Publishers, New York, 2002.

2. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, TonKalker, "Digital Watermarking and Steganography", Margan Kaufmann Publishers, New York, 2008.
3. Information Hiding: Steganography and Watermarking-Attacks and Countermeasures by Neil F. Johnson, Zoran Duric, SushilJajodia
4. Information Hiding Techniques for Steganography and Digital Watermarking by Stefan Katzenbeisser, Fabien A. P. Petitcolas

URLs

1. https://www.garykessler.net/library/steganography.html
2. https://www.hindawi.com/journals/jcnc/2018/9475142/
3. https://www.matec-conferences.org/articles/matecconf/pdf/2016/20/matecconf_icaet2016_02003.pdf
4. https://www.commonlounge.com/discussion/4bc16dbc2c7145ff87ad0f0d5401a242
5. https://www.cl.cam.ac.uk/teaching/0910/R08/work/essay-ma485-watermarking.pdf
6. https://arxiv.org/ftp/arxiv/papers/1407/1407.4735.pdf

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL - 462003

Name of Program **M.Tech.**

Name of Course **Ethical Hacking**

Course Code **IS-602**

Core / Elective / Other **Group B:Department Electives**

Prerequisite:

1. Basic Concept of Web programming, Operating System and Networking
2. Good problem-solving skills and analytical skills

Course Outcomes: (Students will be able to:)

1. Understand the core concepts related to vulnerabilities and their causes
2. Understand ethics behind hacking and vulnerabilities disclosure
3. Appreciate the impact of hacking
4. Exploit the vulnerabilities related to computer system and networks using state of the art tools and technologies

Description of Contents in brief:

1. Ethical hacking Overview
   - This covers the definition of ethical hacking and describes what is legal and what is not legal
2. TCP/IP Concepts Review, Network and Computer Attacks, Network enumeration and Foot printing- DNS query, Whois query, OS finger printing, Banner grabbing
   - This provides overview of TCP/IP and numbering system along with IP Addressing and intruder attacks.
3. Programming for security professionals- Web application vulnerabilities, Buffer overflow attack, Session hijacking, Code injection attacks- Cross Site Scripting attack, SQL injection attack
   - This cover understanding of practical extraction of programming vulnerabilities
4. Password hacking, windows hacking, network hacking, anonymity and email hacking
   - This covers practical exposures to password hacking related to windows and email and also explains anonymity and network vulnerabilities.
5. Web servers hacking, session hijacking, Surveillance, desktop and server OS Vulnerabilities, Database attacks, cryptography, Hacking wireless networks network protection systems, Trojan and backdoor applications, legal resources, virtualization.
   - This describes wireless network standards, authentication and wardriving, firewalls, snort rules, honeypots and intrusion detection systems (IDS), methods of surveillance, various vulnerabilities related to OS and various web based and DB attacks, and explains different types of malware and

its applications

List of Text Books:

1. Ethical Hacking and Network Defense. Michael T. Simpson, Kent Backman, James Corley (1-3, 5)
2. Hacking Exposed6 – Network Security secrets and solutions, S.McClure, J.Scambray, G.Kurtz, McGrawHill (4)

List of Reference Books:

1. CEH, Review Guide, Kimberly Graves, Wiley Publication
2. Network Security Hacks, Andrew Lockhart, O'Reilly Publication

URLs:

https://nptel.ac.in/courses/106105217/

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY,
BHOPAL - 462003

Name of Program	**M.Tech**
Name of Course	**Internet Security Tools and Techniques**
Course Code	**IS -603**
Core / Elective / Other	**Group B:Department Electives**

Prerequisites:

1. Understanding of computer networks, OSI Model, TCP/IP Model.
2. Knowledge of information security and network security.
3. Basic understanding of vulnerabilities in the internet.

Course Outcomes:

1. Understanding of cyber-attacks and cyber threats.
2. Knowing various cyber security tools and their applications on various security problems.
3. Usage of different cyber security techniques.

Description of Contents in brief:

1. Introduction to Internet Security: Introduction to internet security, understanding the importance of internet security, goals of internet security.
2. Types of Cyber-attacks: Understanding the types of cyber-attacks, different types of cyber attackers.
3. Cyber Security Technologies: Understanding the technologies like VPNs, intrusion detection, digital signature, and access control.
4. Cyber Security tools: Knowing different types of security tools like firewalls, antivirus software, penetration testing, and PKI services.
5. Cyber security challenges: Knowing different types of security challenges with real-life scenarios like ransom ware evolution, block chain revolution, IOT threats, AI expansion.

List of Textbooks:

1. Firewalls and Internet Security: Repelling the Wily Hacker by William R. Cheswick and Steve Bellovin.

2. Metasploit - The Penetration Tester's Guide by David Kennedy, Jim O'gorman , Devon Kearns and Mati Aharoni.

List of Reference Books:

1. Digital Signatures by Jonathan Katz.

2. Cyber Security: Threats and Responses for Government and Business.

URLs:

1. https://www.cs.tau.ac.il/~tromer/courses/infosec11/lecture11.pdf
2. https://www.javatpoint.com/cyber-security-tools
3. https://www.techrepublic.com/article/a-beginners-guide-to-public-key-infrastructure/

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY,
BHOPAL - 462003

Name of Program **M.Tech**
Name of Course **Intellectual Property and Espionage**
Course Code **IS -604**

Core / Elective / Other **Group B:Department Electives**

Prerequisite:

1. Understanding Copyright and Related Rights.
2. Understanding knowledge and application of laws governing copyrights, patents, trademarks and trade secrets.
3. Understanding fundamentals underpinning copyright law and practice, and describe the different types of rights which copyright and related rights law protects

Course Outcomes:

1. The students once complete this course, shall get an adequate knowledge on patent and copyright for their innovative research works
2. During their research career, information in patent documents provide useful insight on novelty of their idea from state-of-the art search. This provide further way for developing their idea or innovations

Description of Contents in brief:

1. History and International Regime: Pre- TRIPs and post TRIPs, Balancing Rights of the IPR Holder and the Society, PR and Human Rights, Concept of Intellectual Property Law Patents, Trademark, Geographical Indications, Copyright, Industrial Designs, Integrated Circuits Layout Designs, Trade Secrets or Undisclosed Information, Introduction to Competition Law Anti-Competitive Practices.
2. Introduction to Copyright, Meaning, Nature of Copyright - Subject matter of copyright: original literary, Justification, dramatic, musical, artistic works; cinematograph films and sound recordings - Registration Procedure, Term of protection, Ownership of copyright, Assignment and license of copyright - Infringement, Remedies & Penalties – Related Rights - Distinction between related Rights and copyrights.
   Industrial Design and Layout Designs of Integrated Circuit: Meaning, Scope and Registration, History, International Developments. Designs v/s Copyright and Trademark, Infringement and Remedies
3. Patent: Scope, Objectives and Justification, History and International Treaties, Patentability Criteria, Patentable and Non- patentable inventions, Registration, Ownership, Rights of Patentee, Transfer of technology, Working of Patents and Compulsory licensing, Infringement, Impact of TRIPs and TRIPs Flexibilities, Pharm patents via a Public Health Issues, Utility Patent
4. Trademark: Justification, History, and International Treaties, Different kinds of marks (brand names, logos, signatures, symbols, well known marks, certification marks and service marks) ,- Non Registrable Trademarks - Registration of Trademarks and Scope of Protection, Kinds : Conventional and Non-conventional, Rights of holder and assignment and licensing of marks, Infringement, Remedies & Penalties - Trademarks registry and appellate board
5. Other forms of IP: Design, Geographical Indication (GI), Plant Variety Protection, Layout Design Protection, Current Contour.

List of Text Books:

1. Nithyananda, K V. (2019). Intellectual Property Rights: Protection and Management. India, IN: Cengage Learning India Private Limited.(Ch:1,2,3,4,5)

2. Neeraj, P., & Khusdeep, D. (2014). Intellectual Property Rights.India, IN: PHI learning Private Limited.(Ch:1,2,3)
3.

List of Reference Books:

1. Ahuja, V K. (2017). Law relating to Intellectual Property Rights.India, IN: Lexis Nexis..
2. World Intellectual Property Organisation. (2004). WIPO Intellectual property Handbook. Retrieved from https://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo_pub_489.pdf
3.

URLs:

1. https://nptel.ac.in/courses/110105139/
2. http://www.bdu.ac.in/cells/ipr/docs/syllabus.pdf
3. http://ili.ac.in/4_Intellectual%20Property%20Rights.pdf

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY,
BHOPAL - 462003

Name of Program **M.Tech**

Name of Course **Internet Security Tools and Techniques**

Course Code **IS701**

Core / Elective / Other **Group C: Institute Electives**

Prerequisites:

1. Understanding of computer networks, OSI Model, TCP/IP Model.
2. Knowledge of information security and network security.
3. Basic understanding of vulnerabilities in the internet.

Course Outcomes:

1. Understanding of cyber-attacks and cyber threats.
2. Knowing various cyber security tools and their applications on various security problems.
3. Usage of different cyber security techniques.

Description of Contents in brief:

1. Introduction to Internet Security: Introduction to internet security, understanding the importance of internet security, goals of internet security.
2. Types of Cyber-attacks: Understanding the types of cyber-attacks, different types of cyber attackers.
3. Cyber Security Technologies: Understanding the technologies like VPNs, intrusion detection, digital signature, and access control.
4. Cyber Security tools: Knowing different types of security tools like firewalls, antivirus software, penetration testing, and PKI services.
5. Cyber security challenges: Knowing different types of security challenges with real-life scenarios like ransom ware evolution, block chain revolution, IOT threats, AI expansion.

List of Textbooks:

1. Firewalls and Internet Security: Repelling the Wily Hacker by William R. Cheswick and Steve Bellovin.

2. Metasploit - The Penetration Tester's Guide by David Kennedy, Jim O'gorman , Devon Kearns and Mati Aharoni.

List of Reference Books:

1. Digital Signatures by Jonathan Katz.

2. Cyber Security: Threats and Responses for Government and Business.

URLs:

1. https://www.cs.tau.ac.il/~tromer/courses/infosec11/lecture11.pdf
2. https://www.javatpoint.com/cyber-security-tools
3. https://www.techrepublic.com/article/a-beginners-guide-to-public-key-infrastructure/

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY,
BHOPAL - 462003

Name of Program **M.Tech**
Name of Course **Intellectual Property and Espionage**
Course Code **IS 702**

Core / Elective / Other **Group C: Institute Electives**

Prerequisite:

1. Understanding Copyright and Related Rights.
2. Understanding knowledge and application of laws governing copyrights, patents, trademarks and trade secrets.
3. Understanding fundamentals underpinning copyright law and practice, and describe the different types of rights which copyright and related rights law protects

Course Outcomes:

1. The students once complete this course, shall get an adequate knowledge on patent and copyright for their innovative research works
2. During their research career, information in patent documents provide useful insight on novelty of their idea from state-of-the art search. This provide further way for developing their idea or innovations

Description of Contents in brief:

1. History and International Regime: Pre- TRIPs and post TRIPs, Balancing Rights of the IPR Holder and the Society, PR and Human Rights, Concept of Intellectual Property Law Patents, Trademark, Geographical Indications, Copyright, Industrial Designs, Integrated Circuits Layout Designs, Trade Secrets or Undisclosed Information, Introduction to Competition Law Anti-Competitive Practices.
2. Introduction to Copyright, Meaning, Nature of Copyright - Subject matter of copyright: original literary, Justification, dramatic, musical, artistic works; cinematograph films and sound recordings - Registration Procedure, Term of protection, Ownership of copyright, Assignment and license of copyright - Infringement, Remedies & Penalties – Related Rights - Distinction between related Rights and copyrights.
   Industrial Design and Layout Designs of Integrated Circuit: Meaning, Scope and Registration, History, International Developments. Designs v/s Copyright and Trademark, Infringement and Remedies
3. Patent: Scope, Objectives and Justification, History and International Treaties, Patentability Criteria, Patentable and Non- patentable inventions, Registration, Ownership, Rights of Patentee, Transfer of technology, Working of Patents and Compulsory licensing, Infringement, Impact of TRIPs and TRIPs Flexibilities, Pharm patents via a Public Health Issues, Utility Patent
4. Trademark: Justification, History, and International Treaties, Different kinds of marks (brand names, logos, signatures, symbols, well known marks, certification marks and service marks) ,- Non Registrable Trademarks - Registration of Trademarks and Scope of Protection, Kinds : Conventional and Non-conventional, Rights of holder and assignment and licensing of marks, Infringement, Remedies & Penalties - Trademarks registry and appellate board
5. Other forms of IP: Design, Geographical Indication (GI), Plant Variety Protection, Layout Design Protection, Current Contour.

List of Text Books:

1. Nithyananda, K V. (2019). Intellectual Property Rights: Protection and Management. India, IN: Cengage Learning India Private Limited.(Ch:1,2,3,4,5)

2. Neeraj, P., & Khusdeep, D. (2014). Intellectual Property Rights.India, IN: PHI learning Private Limited.(Ch:1,2,3)

3.

List of Reference Books:

1. Ahuja, V K. (2017). Law relating to Intellectual Property Rights.India, IN: Lexis Nexis..

2. World Intellectual Property Organisation. (2004). WIPO Intellectual property Handbook. Retrieved from https://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo_pub_489.pdf

3.

URLs:

1. https://nptel.ac.in/courses/110105139/

2. http://www.bdu.ac.in/cells/ipr/docs/syllabus.pdf

3. http://ili.ac.in/4_Intellectual%20Property%20Rights.pdf