MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

Name of Program		**M. Tech. in CSE with Specialization in Information Security**				**Semester: 1st**	
Name of Course		**Mathematical Foundation of Information Security**					
Course Code		**IS 511**					
Core / Elective / Other		**Core**					
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**

Prerequisite:	
1.	Set theory, basic number theory
2.	Algebra, permutation and combination
3.	Probability
Course Outcomes: At the end of the course, the student will be able to:	
1.	Assess the notion of mathematical thinking, mathematical proofs, and algorithmic thinking, and be able to apply them in problem solving related to information security.
2.	Practice mathematical concepts required for cryptology.
3.	Recognize effective algebraic techniques for computer security.
4.	Recognize some basic properties of graphs and related discrete structures, and relate these for information security.
5.	Formulate decision and game theory for improvising system's security.
Description of Contents in brief:	
Number Theory and Algebra: Integer Arithmetic, Integers set Z, Zn, Zn*, Greatest Common Divisors in Z, Euclidean Algorithm, Extended Euclidean Algorithm, Additive and Multiplicative Inverses in Zn, 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 5thEdition, Gilbert Strang, Wellesley Cambridge Press.
3.	Decision and Game Theory for Security, 6th International Conference, GameSec 2015.

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

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. in CSE with Specialization in Information Security**					**Semester: 1st**	
Name of Course	**Computer & Network Security**						
Course Code	**IS 512**						
Core / Elective / Other	**Core**						
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**

Prerequisite:	
1.	Knowledge of computer networks, operating systems, data structures and algorithms
2.	Knowledge of advanced programming in C
Course Outcomes: At the end of the course, the student will be able to:	
1.	Identify some of the factors driving the need for network security.
2.	Explain the terms vulnerability, threat and attack and identify physical points of vulnerability in simple networks.
3.	Compare and contrast symmetric and asymmetric encryption systems and their vulnerability to attack, and explain the characteristics of hybrid systems.
Description of Contents in brief:	
1.	Introduction to Computer and Network Security: Basic concepts, threat models, common security goals.
2.	Cryptography and Cryptographic Protocols: 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.

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

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

Name of Program	**M. Tech. in CSE with Specialization in Information Security**					**Semester: 1st**	
Name of Course	**Cybercrime & Information Warfare**						
Course Code	**IS 513**						
Core / Elective / Other	**Core**						
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**

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: At the end of the course, the student will be able to:	
1.	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 cyberterrorism 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 Text Books:	
1.	Principles of cybercrime, Jonathan Clough Cambridge University Press
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
List of Reference Books:	
1.	No reference book is needed, text books are sufficient.
URLs:	
1.	https://swayam.gov.in/nd2_nou19_cs08/

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

Name of Program	**M. Tech. in CSE with Specialization in Information Security**					**Semester: 1st**	
Name of Course	**Malware Analysis and Reverse Engineering**						
Course Code	**IS 514**						
Core / Elective / Other	**Core**						
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**

Prerequisite:

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

Course Outcomes: At the end of the course, the student will be able to:

1.	Acquire basic knowledge about the main opportunities provided by Reverse Engineering, which represents an opportunity to learn how to conduct detailed product design.
2.	Collect the large number of data/ information for the product.
3.	Depth analyze of the products and extraction of real time data.

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's REMnux, 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 William Pollock.
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. in CSE with Specialization in Information Security**					**Semester: 2nd**	
Name of Course	**Cryptography**						
Course Code	**IS 521**						
Core / Elective / Other	**Core**						
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**

Prerequisite:	
1.	Algorithms
2.	Mathematical Foundation Of Information Security
3.	Computer and Network Security
Course Outcomes: At the end of the course, the student will be able to:	
1.	Illustrate various Public key cryptographic techniques.
2.	Study the mathematical foundations of cryptographic schemes.
3.	Evaluate the authentication and hash algorithms.
4.	Evaluate the security of the ciphers using rigorous approaches.
5.	Summarize the intrusion detection and its solutions to overcome the attacks.
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, KnownPlaintext 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

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

		Security					
Name of Course		**Database Security & Access Control**					
Course Code		**IS 522**					
Core / Elective / Other		**Core**					
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**

Prerequisite:	
1.	Fundamental Knowledge of Database
2.	Familiarity with SQL and Oracle
Course Outcomes: At the end of the course, the student will be able to:	
1.	Assess about implementation of classical models and algorithms.
2.	Demonstrate database access control methods for secure database application development.
3.	Analyze the data, identify the problems, design secure database, and 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 of Access 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

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

Name of Program		**M. Tech. in CSE with Specialization in Information Security**				**Semester: 2nd**	
Name of Course		**Digital Forensics**					
Course Code		**IS 523**					
Core / Elective / Other		**Core**					
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**

Prerequisite:	
1.	Good Skills and Concept of Programming.
2.	Sound Knowledge of Windows and UNIX Operating Systems.
3.	Knowledge of Networking.
Course Outcomes: At the end of the course, the student will be able to:	
1.	Build a solid foundation for computer forensics and digital investigation and its processes, policies and procedures.
2.	Assemble the relevant legislation and codes of ethics.
3.	Recognize evidence, guidelines and standard of tools for environment of digital forensics.
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 autopsy.
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

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

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

Name of Program		**M. Tech. in CSE with Specialization in Information Security**				**Semester: -**	
Name of Course		**Biometrics**					
Course Code		**IS 551**					
Core / Elective / Other		**Group A : Program Elective**					
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**
Prerequisite:							
1.	Good knowledge of digital image processing / computer graphics						
2.	Linear algebra						
3.	Probabilities and statistics						

4.	MATLAB
Course Outcomes: At the end of the course, the student will be able to:	
1.	Assess the state-of-the-art in biometric technologies.
2.	Categorize the currently available biometric systems.
3.	Demonstrate R&D on biometrics methods and systems.
4.	Conclude various modules constituting a biometric system.
5.	Interpret different biometric traits and to appreciate their relative significance.
Description of Contents in brief:	
1.	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:	
1.	Digital Image Processing using MATLAB, By: Rafael C. Gonzalez, Richard Eugene Woods, 2nd Edition, Tata McGraw-Hill Education 2010.
2.	Biometrics for network security, Paul Reid, Hand book of Pearson A. Jain, R. Bolle, S. Pankanti.
3.	BIOMETRICS: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999. ISBN 0-7923-8345-1.TK7882.P3 B36.
4.	J. Ashbourn, Biometrics: Advanced Identity Verification, Springer-Verlag, 2000. ISBN 1-85233-243-3. TK7882.P3 A84.
5.	Guide to Biometrics, By: Ruud M. Bolle, Sharath Pankanti, Nalini K. Ratha, Andrew W. Senior, Jonathan H. Connell, Springer 2009.
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.

Name of Program		**M. Tech. in CSE with Specialization in Information Security**				**Semester: -**	
Name of Course		**Privacy: Data & User Protection**					
Course Code		**IS 552**					
Core / Elective / Other		**Group A : Program Elective**					
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**
Prerequisite:							
1.	Basic knowledge of privacy and data protection legislation.						
2.	Knowledge of general data protection regulation is required.						
Course Outcomes: At the end of the course, the student will be able to:							

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

1.	Demonstrate the security and privacy with a set of techniques, which enable to address the security & privacy challenges.
2.	Assess information policy, public policy of computer science and information science that have an interest in work or research in security and privacy fields, or in support of those fields.
3.	Assess the security and privacy level of data & user space.
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, 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:	
1.	http://cb.hbsp.harvard.edu/cb/access/5263390
2.	https://journalofbigdata.springeropen.com/articles/10.1186/s40537-016-0059-y
3.	https://iapp.org/about/what-is-privacy/

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

Name of Program		**M. Tech. in CSE with Specialization in Information Security**				**Semester: -**	
Name of Course		**Secure Software Engineering**					
Course Code		**IS 553**					
Core / Elective / Other		**Group A : Program Elective**					
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**
Prerequisite:							
1.	The basic knowledge about the principles of software engineering.						
2.	The software lifecycle.						
3.	Sufficient programming skills for the team development project.						

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

Course Outcomes: At the end of the course, the student will be able to:	
1.	Design a software requirements document.
2.	Demonstrate an understanding of the proper contents of a software requirements document.
3.	Illustrate distributed system architectures and application architectures.
4.	Differentiate real-time and non-real time systems.
5.	Assemble proficiency in rapid software development techniques.
Description of Contents in brief:	
1.	Software Security Issues: Introduction, the problem, software assurance and software security, threats to software security, sources of software insecurity, and 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. in CSE with Specialization in Information Security**				**Semester: -**	
Name of Course		**Steganography and Digital Watermarking**					
Course Code		**IS 554**					
Core / Elective / Other		**Group A : Program Elective**					
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**
Prerequisite:							
1.	Digital image processing, image analysis						
Course Outcomes: At the end of the course, the student will be able to:							
1.	Formulate the concept of information hiding.						

2.	Recognize the current techniques of steganography and practice how to detect and extract hidden information.
3.	Recognize watermarking techniques and through examples relate the concept.
Description of Contents in brief:	
1.	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.
2.	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:	
1.	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, Sushil Jajodia.
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.matecconferences.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

Name of Program	**M. Tech. in CSE with Specialization in Information Security**	**Semester: -**
Name of Course	**Security Threats and Modelling**	
Course Code	**IS 555**	
Core / Elective / Other	**Group A : Program Elective**	

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**
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: At the end of the course, the student will be able to:							
1.	Recognize of variety of threats and threat modelling methodologies.						
2.	Assess to find and mitigate threats.						
3.	Demonstrate 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. in CSE with Specialization in Information Security**	**Semester: -**
Name of Course	**Penetration Testing and Vulnerability Assessment**	
Course Code	**IS 556**	
Core / Elective / Other	**Group A : Program Elective**	

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**
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: At the end of the course, the student will be able to:							
1.	Demonstrate penetration testing and security auditing platform with advanced tools to identify, detect, and exploit any vulnerability uncovered in the target network environment.						
2.	Apply appropriate testing methodology with defined business objectives and a scheduled test plan, which will result in robust penetration testing of the network.						
3.	Examine 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 issues penetration 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 test1 report 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 tools network penetration testing methodology - 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 suite tool, browser proxies and non-rendered content, cross-site scripting and crosssite 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 module cloud penetration testing methodology module, report writing and posttest actions.
List of Text Books:	
1.	Penetration Testing - A hands-on introduction to Hackingby Georgia Weidman (Ch 1,2,3,4,5,8).
2.	Network Vulnerability Assessment by Sagar Rahalkar (Ch 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.

Name of Program	**M. Tech. in CSE with Specialization in Information Security**	**Semester: -**
Name of Course	**Ethical Hacking**	
Course Code	**IS 557**	
Core / Elective / Other	**Group A : Program Elective**	

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**

Prerequisite:	
1.	Basic concept of web programming, operating system and networking.
2.	Good problem-solving skills and analytical skills.
Course Outcomes: At the end of the course, the student will be able to:	
1.	Illustrate the core concepts related to vulnerabilities and their causes.
2.	Assess ethics behind hacking and vulnerabilities disclosure.
3.	Estimate the impact of hacking.
4.	Recognize 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 (Ch 1-3, 5).
2.	Hacking Exposed 6, Network Security secrets and solutions, S. McClure, J. Scambray, G. Kurtz, McGraw Hill (Ch 4).

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

List of Reference Books:	
1.	CEH, Review Guide, Kimberly Graves, Wiley Publication
2.	Network Security Hacks, Andrew Lockhart, O'Reilly Publication
URLs	
1.	https://nptel.ac.in/courses/106105217/

Name of Program	M. Tech. in CSE with Specialization in Information Security	Semester: -
Name of Course	Security Operations and Incidence Response	
Course Code	IS 558	

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

Core / Elective / Other		**Group A : Program Elective**					
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**
Course Outcomes: At the end of the course, the student will be able to:							
1.	Analyze about Security policies and industrial best practices.						
2.	Assess security standards and audit, cyber laws and legal system.						
3.	Interpret 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 regulatory framework, indian and international laws.						
List of Text Books:							
1.	Information Security Governance: Framework and Toolset forCISOs and Decision Makers by Andrej Volchkov.						
List of Reference Books:							
1.	CISO Desk Reference Guide by Bill Bonney, Gary Hayslip, Matt Stampe.						
2.	CISO Compass: Navigating Cybersecurity Leadership Challenges with Insights from Pioneers by Todd 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						

Name of Program	**M. Tech. in CSE with Specialization in Information Security**	**Semester: -**
Name of Course	**Internet Security, Tools and Techniques**	

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

Course Code		**IS 559**					
Core / Elective / Other		**Group A : Program Elective**					
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**

Prerequisite:	
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: At the end of the course, the student will be able to:	
1.	Evaluate cyber-attacks and cyber-threats.
2.	Demonstrate various cyber security tools and their applications on various security problems.
3.	Examine 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. (Multiple subjects)
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 Text Books:	
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

Course Code		**IS 560**					
Core / Elective / Other		**Group A : Program Elective**					
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**

Prerequisite:	
1.	Fundamental knowledge of computer network.
2.	Fundamental knowledge of internet security.
3.	Familiarity with of C/C++.
Course Outcomes: At the end of the course, the student will be able to:	
1.	Assess skills of high order to provide thorough knowledge and insight into the spectrum of risks faced by an organization.
2.	Estimate risk management as well as processes and techniques that can ensure the effective assessment, monitoring and control of risk at all levels.
3.	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, procedures and 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.
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.
URLs	
1.	https://ocw.mit.edu/courses/sloan-school-of-management/15-997-practice-of-financeadvanced-corporate-risk-management-spring-2009/
2.	https://nptel.ac.in/courses/110107128/

Name of Program	**M. Tech. in CSE with Specialization in Information Security**	**Semester: -**
Name of Course	**Intellectual Property and Espionage**	
Course Code	**IS 561**	

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

Core / Elective / Other		**Group A : Program Elective**					
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**
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: At the end of the course, the student will be able to:							
1.	Estimate patent and copyright with adequate knowledge for their innovative research works.						
2.	Assess details to use during their research career, information in patent documents provide useful insight on novelty of their idea from state-of-the art search.						
3.	Illustrate further way for developing their idea or innovations on intellectual properties.						
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)
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.
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

Course Code		**IS 554**					
Core / Elective / Other		**Group B : Department Elective**					
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**

Prerequisite:	
1.	Digital image processing, image analysis
Course Outcomes: At the end of the course, the student will be able to:	
1.	Formulate the concept of information hiding.
2.	Recognize the current techniques of steganography and practice how to detect and extract hidden information.
3.	Recognize watermarking techniques and through examples relate the concept.
Description of Contents in brief:	
1.	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.
2.	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:	
1.	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, Sushil Jajodia.
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.matecconferences.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

Name of Program	**M. Tech. in CSE with Specialization in Information Security**	**Semester: -**
Name of Course	**Ethical Hacking**	
Course Code	**IS 557**	
Core / Elective / Other	**Group B : Department Elective**	

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**
Prerequisite:							
1.	Basic concept of web programming, operating system and networking.						
2.	Good problem-solving skills and analytical skills.						
Course Outcomes: At the end of the course, the student will be able to:							
1.	Illustrate the core concepts related to vulnerabilities and their causes.						
2.	Assess ethics behind hacking and vulnerabilities disclosure.						
3.	Estimate the impact of hacking.						
4.	Recognize 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 (Ch 1-3, 5).						
2.	Hacking Exposed 6, Network Security secrets and solutions, S. McClure, J. Scambray, G. Kurtz, McGraw Hill (Ch 4).						

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

List of Reference Books:	
1.	CEH, Review Guide, Kimberly Graves, Wiley Publication
2.	Network Security Hacks, Andrew Lockhart, O'Reilly Publication
URLs	
1.	https://nptel.ac.in/courses/106105217/

Name of Program	M. Tech. in CSE with Specialization in Information Security	Semester: -
Name of Course	Internet Security Tools and Techniques	
Course Code	IS 559	

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

Core / Elective / Other		**Group B : Department Elective**					
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**

Prerequisite:	
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: At the end of the course, the student will be able to:	
1.	Evaluate cyber-attacks and cyber-threats.
2.	Demonstrate various cyber security tools and their applications on various security problems.
3.	Examine 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 Text Books:	
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

Core / Elective / Other		**Group B : Department Elective**					
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**

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: At the end of the course, the student will be able to:	
1.	Estimate patent and copyright with adequate knowledge for their innovative research works.
2.	Assess details to use during their research career, information in patent documents provide useful insight on novelty of their idea from state-of-the art search.
3.	Illustrate further way for developing their idea or innovations on intellectual properties.
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)
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.
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

Name of Program	**M. Tech. in CSE with Specialization in Information Security**	**Semester: -**
Name of Course	**Internet Security Tools and Techniques**	

MAULANA AZAD NATIONAL INSTITUTE OF TECHNOLOGY, BHOPAL – 462003

Course Code		**IS 701**					
Core / Elective / Other		**Group C : Institute Elective**					
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**

Prerequisite:	
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: At the end of the course, the student will be able to:	
1.	Evaluate cyber-attacks and cyber-threats.
2.	Demonstrate various cyber security tools and their applications on various security problems.
3.	Examine 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 Text Books:	
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 Course		**Intellectual Property and Espionage**					
Course Code		**IS 561**					
Core / Elective / Other		**Group C : Institute Elective**					
Credits	**3**	**L**	**3**	**T**	**-**	**P**	**-**

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: At the end of the course, the student will be able to:	
1.	Estimate patent and copyright with adequate knowledge for their innovative research works.
2.	Assess details to use during their research career, information in patent documents provide useful insight on novelty of their idea from state-of-the art search.
3.	Illustrate further way for developing their idea or innovations on intellectual properties.
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)
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.
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