GANGA INSTITUTE OF TECHNOLOGY AND MANAGEMENT, KABLANA (JHAJJAR)
An Autonomous Institute

'A' GRADE ACCREDITED BY NAAC

Evaluation Scheme & Syllabus For

Master of Technology (Cyber Forensics and Information Security)

(Effective from the Session: 2024-25)

APPROVED BY AICTE, NEW DELHI AND AFFILIATED TO MDU, ROHTAK

1. DEFINITION OF CREDIT

1	1 Lecture (L) per week	1 Credit
2	2 Practical (P) per week	1 Credit
3	2 Seminar per Week	2 Credit
4	4 Project Per Week	2 Credit

2. RANGE OF CREDIT

A credit of 86 is required for a student to be eligible for a postgraduate degree in Cyber Forensics and Information Security

3. STRUCTURE OF POSTGRADUATE ENGINEERING PROGRAM (M.TECH)

Sr. No.	Category	Breakup of Credits
1	Professional Core Courses	32*
2	Professional Elective Courses (Relevant to chosen specialization/branch)	8*
3	Mandatory Learning Course	3*
4	Multidisciplinary Open Elective Courses	6*
5	Foundation Elective Courses	3*
6	Seminar	6*
7	Lab Courses	4*
8	Project	2*
9	Dissertation	22*
	Total Credits	**86***

**Minor variation is allowed as per need of the respective disciplines.*

4. COURSE CODE AND DEFINITIONS

Sr. No.	Category	Course Code
1	Professional Core Courses	PCC
2	Professional Elective Courses (Relevant to chosen specialization/branch)	PEC
3	Mandatory Learning Course	MLC
4	Multidisciplinary Open Elective Courses	OEC
5	Foundation Elective Courses	FEC
6	Seminar	SM
7	Lab Courses	LC
8	Project	PROJ
9	Dissertation	DISS

GANGA INSTITUTE OF TECHNOLOGY AND MANAGEMENT, KABLANA, JHAJJAR (HR.)

Scheme of Studies and Examination

M. Tech (Cyber Forensics and Information Security) –1st Semester

w.e.f. 2024-25

Sr. No.	Category	Course Code	Course Title	Lectures per week			Total Load Per Week	Credits	Examination Scheme (Marks)				Exam Duration in Hours
				Lecture (L)	Tutorial (T)	Practical (P)			Assessment	End Semester Examination		Total	
										Theory	Practical		
1	Professional Core Courses	PCC-MTCFIS-101A	Mathematical Foundations of Information Security	4	0	0	4	4	40	60		100	3
2	Professional Core Courses	PCC-MTCFIS-103A	Networks and Information Security	4	0	0	4	4	40	60		100	3
3	Professional Core Courses	PCC-MTCFIS-105A	Operating Systems and Security	4	0	0	4	4	40	60		100	3
4	Professional Core Courses	PCC-MTCFIS-107A	Cyber Forensics	4	0	0	4	4	40	60		100	3
5	Professional Core Courses	PCC-MTCFIS-109A	Database Security	4	0	0	4	4	40	60		100	3
6	Lab Course	LC-MTCFIS-111A	Information Security Lab	0	0	2	2	1	25		25	50	3
7	Lab Course	LC-MTCFIS-113A	OS Security Lab	0	0	2	2	1	25		25	50	3
8	Seminar	SM-MT-115A	Seminar-I	0	0	2	2	2	50			50	
Total Credits								**24**				**650**	

GANGA INSTITUTE OF TECHNOLOGY AND MANAGEMENT, KABLANA, JHAJJAR (HR.)

Scheme of Studies and Examination

M. Tech (Cyber Forensics and Information Security) –2nd Semester

w.e.f. 2024-25

Sr. No.	Category	Course Code	Course Title	Hours per week			Total Load Per Week	Credits	Examination Scheme (Marks)				Exam Duration in H
				Lecture (L)	Tutorial (T)	Practical (P)			Assessment	End Semester Examination		Total	
										Theory	Practical		
1	Professional Core Courses	PCC-MTCFIS-102A	Ethical Hacking and Digital Forensics	4	0	0	4	4	40	60		100	3
2	Professional Core Courses	PCC- MTCFIS-104A	Steganography and Digital Watermarking	4	0	0	4	4	40	60		100	3
3	Professional Elective Courses	Refer Table-I	.....	4	0	0	4	4	40	60		100	3
4	Multidisciplinary Open Elective Courses	Refer Table-II	.....	3	0	0	3	3	40	60		100	3
5	Foundation Elective Courses	Refer Table-III	.....	3	0	0	3	3	40	60		100	3
6	Lab Course	LC-MTCFIS-106A	Ethical Hacking Lab	0	0	2	2	1	25		25	50	3
7	Lab Course	LCMTCFIS-108A	Steganography Lab	0	0	2	2	1	25		25	50	3
8	Seminar	SM-MT-110A	Seminar-II	0	0	2	2	2	50			50	
Total Credits								**22**				**650**	

Table I: Professional Elective Courses

Sr. No.	Course Code	Course Name
1	PEC- MTCFIS-112A	Advanced Computer Networks
2	PEC- MTCFIS-114A	Security Threats
3	PEC- MTCFIS-116A	Multimedia Security
4	PEC- MTCFIS-118A	Mobile & Wireless Security

Table II: Multidisciplinary Open Elective-I Courses

Students of all M. Tech programmes are required to study one Multidisciplinary open elective course in each of the 2nd and 3rd Semesters and one foundation elective course in 2nd Semester for 2-Years Programmes. They may choose any one of the following courses (excluding the courses offered by the departments of their own subjects, if not stated otherwise).

Sr. No	Course Code	Course Name	Offered by Department
1	OEC-130A	Basic of Economics	Management Department
2	OEC-132A	Fundamentals of Management	Management Department
3	OEC-134A	Disaster Management	Civil Engineering
4	OEC-136A	Industrial Safety	Fire Technology and Safety
5	OEC-138A	Indian Literature in Translation-I	Applied Sc. & Humanities (English)
6	OEC-140A	Environmental Issues	Applied Sc. & Humanities (Chemistry)
7	OEC-142A	Quantitative Techniques	Applied Sc. & Humanities (Mathematics)
8	OEC-144A	Sources of Energy-I	Electrical Engineering
9	OEC-146A	Operation Research	Mechanical Engineering
10	OEC-148A	Multimedia Communication	Electronics and Communication Engineering
11	OEC-150A	Introduction to Information Technology	Computer Sc. & Applications
12	OEC-152A	Cyber Forensics and Security	Computer Sc. & Engineering
13	OEC-154A	Computer Science and Principles	Computer Sc. & Engineering
14	OEC-156A	Software Engineering Practice	Computer Sc. & Engineering

Table III: Foundation Elective Courses

Sr. No	Course Code	Course Name	Offered by Department
1	FEC-158A	Basics of Accounting	Management Department
2	FEC-160A	Basics of E-commerce	Management Department
3	FEC-162A	Element of Banking	Management Department
4	FEC-164A	Computer Fundamentals	Computer Sc. & Applications
5	FEC-166A	Communication and Soft Skills	Applied Sc. & Humanities (English)
6	FEC-168A	Entrepreneurship Development	Management Department
7	FEC-170A	Electronics Engineering	Electronics and Communication Engineering

Course Code	**PCC-MTCFIS-101A**				
Category	Professional Core Courses				
Course Title	**Mathematical Foundations of Information Security**				
Scheme and Credits	L	T	P	**Credits**	**Semester-I**
	4	0	0	**4**	
Course Objectives	The objectives of this course are • To understand the principles of number theory and their applications in cryptography. • To explore classical and modern encryption techniques for secure communication. • To study public key cryptography and advanced cryptographic protocols. • To analyze primality testing and factorization methods for cryptographic applications.				
Assessment	40 Marks				
End Semester Examination	60 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	Skill Demonstrated	RBT Level
CO1	Define the fundamental concepts of number theory and cryptosystems.	Level 1: Remember
CO2	Understand the basic concepts of number theory, algebra and cryptography.	Level 2: Understand
CO3	Apply the concepts of encryption schemes and number theory to solve computational problems.	Level 3: Apply
CO4	Analyze the principles, theorems and algorithms in number theory and cryptography to enhance efficiency and security in information Systems.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Topics in elementary number theory: O and notations, time estimates for doing arithmetic, divisibility and the Euclidean algorithm, Congruences: Definitions and properties, linear congruences, residue classes, Euler's phi function, Fermat's Little Theorem, Chinese Remainder Theorem, Applications to factoring, finite fields, quadratic residues and reciprocity: Quadratic residues, Legendre symbol, Jacobi symbol.

Unit-II

Simple Cryptosystems: Enciphering Matrices, Encryption Schemes, Symmetric and Asymmetric Cryptosystems, Cryptanalysis, Block ciphers–Use of Block Ciphers, Multiple Encryption, Stream Ciphers–Affine cipher, Vigenere, Hill, and Permutation Cipher, Secure Cryptosystem.

Unit-III

Public Key Cryptosystems: The idea of public key cryptography, The Diffie–Hellman Key Agreement Protocol - RSA Cryptosystem, Bit security of RSA, ElGamal Encryption - Discrete Logarithm ,Knapsack problem, Zero-Knowledge Protocols, From Cryptography to Communication Security-Oblivious Transfer.

Unit-IV

Primality and Factoring: Pseudo primes, the rho (γ) method, Format factorization and factor bases, the continued fraction method, the quadratic seieve method. Number Theory and Algebraic Geometry: Elliptic curves, basic facts, elliptic curve cryptosystems, elliptic curve primality test, and elliptic curve factorization.

Suggested Readings:

1. A Computational Introduction to Number Theory and Algebra by Victor Shoup, Cambridge University Press, 2005.
2. Hand Book of Applied Cryptography by A. Manezes, P. Van Oorschot and S. Vanstone, CRC Press, 1996.
3. Classical Introduction to Cryptography, Applications for Communication Security by Serge Vaudenay, Springer, 2006.
4. A Course in Number Theory and Cryptography by Neal Koblitz, 2nd Edition, Springer, 2002.
5. Introduction to Cryptography by Johannes A. Buchman, 2nd Edition, Springer, 2004.
6. The Mathematics of Ciphers, Number Theory and RSA Cryptography by S.C. Coutinho, A.K. Peters, Natick, Massachusetts, 1998.

Useful Video links:

Unit No.	Topics	Links
Unit-I	Fundamental theorem of arithmetic	https://youtu.be/FpEI8yh7Ls8?si=U7vVHU9a7egq6on1
	Chinese remainder theorem	https://youtu.be/qs1nop_YEmc?si=IomQX0vcLBwrw3fZ
	Fermat's theorem	https://youtu.be/FT_NqVQI-Hs?si=ulA7aQQnmFF3HtP0
Unit-II	Symmetric key Encryption	https://youtu.be/eIJzIUhks6E?si=TXlqkrnTuPfY5eSc
	Modes of operation of block cipher	https://youtu.be/3ujQWgW41-M?si=VBO7Jb3xedvHlAvw
	Symmetric key encryption	https://youtu.be/eIJzIUhks6E?si=ynr5SKbP4ItXS4i4
Unit-III	Public key encryption	https://youtu.be/tBRP0aSeHyE?si=WMOKnis6eieK4Asq
	RSA public key cryptosystem	https://youtu.be/gVPyTRbBc70?si=W5MTXCEqNpYnGIkg
	Diffie-Hellman Problem and Security of ElGamal Systems	https://youtu.be/2kfAga111ls?si=zJJFJmZv2Y7lLLDR
Unit-IV	Pseudo random functions	https://youtu.be/_iPVd87B_zc?si=Auv4Ojp0LyunhI08
	Primality testing	https://youtu.be/_7F8tVeOgZE?si=h3SSQkUQ98QyuVkA

Course Code	**PCC-MTCFIS-103A**				
Category	Professional Core Courses				
Course Title	**Networks and Information Security**				
Scheme and Credits	L	T	P	**Credits**	**Semester-I**
	4	0	0	**4**	
Course Objectives	The objectives of this course are • To understand the fundamental concepts of network security. • To explore various access control mechanisms and models • To gain a comprehensive understanding of cryptographic techniques and encryption methods • To analyze the role of security protocols and services				
Assessment	40 Marks				
End Semester Examination	60 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	Skill Demonstrated	RBT Level
CO1	Define the concepts of network security, protocols, and cryptographic techniques used to protect data and ensure secure communications.	Level 1: Remember
CO2	Explain various security services, such as confidentiality, integrity, authentication, and non-repudiation, and their role in network security.	Level 2: Understand
CO3	Apply appropriate access control mechanisms, encryption methods, and security protocols to secure communication and prevent cyber threats.	Level 3: Apply
CO4	Analyze different security models, access control mechanisms, and cryptographic systems to assess their effectiveness in mitigating network risks.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Introduction: Characteristics of Networks, Security Concepts, Kinds of security breaches, Threats and Risks, Points of vulnerability, Attacks, Passive and Active, Security Services, Confidentiality, Authentication, Non-Repudiation, Integrity, Access Control, Availability, Methods of defence, Control measures, Effectiveness of controls, Model for Internetwork Security, Internet Standards and RFCs Access Control Mechanisms, Access Matrix, HRU, TAM, ACL and capabilities.

Unit-II

Access Control Models: Chinese wall, Clark-Wilson, Bell-LaPadula, Non Interference and Role Base Model. Cryptography, Encryption techniques, Characteristics of good encryption systems, Secret Key and Public Key Cryptosystems, Symmetric Ciphers, Block Ciphers and Stream Ciphers, DES, IDEA and Key Escrow, RSA and ElGamal, Secure Hash and Key management, Non-repudiation, cryptanalysis.

Unit-III

Secure sockets, IPsec overview, IP security architecture–IPsec-Internet Key Exchanging (IKE)–IKE phases, encoding, Internet security, Threats to privacy, Packet sniffing, Spoofing - Web security requirements, Real Time communication security, Security standards–Kerberos.X.509 Authentication Service. Security protocols, Transport layer protocols, SSL, Electronic mail security, PEM and S/MIME security protocol, Pretty Good Privacy, Web Security-Firewalls design principles, trusted systems, Electronic payment protocols. Intrusion detection, password management, Viruses and related Threats, Virus Counter measures, Virtual Private Networks.

Unit-IV

Network Security Applications, Authentication Mechanisms: Passwords, Cryptographic authentication protocol, Smart Card, Biometrics, Digital Signatures and seals, Kerberos, X.509 LDAP Directory. Web Security: SSL Encryption, TLS, SET, Email Security, Pretty Good Privacy (PGPs)/MIME, IP Security, Access and System Security, Intruders, Intrusion Detection and Prevention, Firewall, Hardware Firewall, Software Firewall, Application Firewall, Packet Filtering, Packet Analysis, Proxy Servers, Firewall setting in Proxy, ACL in Proxy.

Suggested Readings:

1. Network Security Essentials by William Stallings, 3rd Edition, Pearson Education, 2006.
2. Fundamentals of Computer Security Technology by Edward Amoroso, Prentice-Hall, 1999.
3. Security in Computing by Charles P. Pleeger, Pearson Education, 5th Edition, 2001.
4. Cryptography and Network Security: Principles and Standards by William Stallings, Prentice Hall India, 3rd Edition, 2003.

Useful Video links:

Unit No.	Topics	Links
Unit-I	Security Concepts, Kinds of security breaches, Threats and Risks, Points of vulnerability	https://youtu.be/eCqYztA7iXc?list=PLFe9iOZ1HkC5V4gwbV8H8buJZhgo4cb_z
	Attacks, Passive and Active	https://youtu.be/i9j2tw_RhQU?si=vbxYax1xc90rvbS8
	Identification and Authentication	https://youtu.be/tDQvHzfS4X0?si=4aBisRd6YSbLnmjm
Unit-II	Cryptography, Cryptology, Cryptoanalysis	https://youtu.be/Svb9rNB3feU?si=BHALT3juTXQqAJdp
	Encryption techniques, Secret Key and Public Key Cryptosystems,	https://youtu.be/uzGzSHGip_o?t=446
	Symmetric Ciphers, Block Ciphers and Stream Ciphers	https://youtu.be/j53iXhTSi_s?list=PLBlnK6fEyqRgJU3EsOYDTW7m6SUmW6kII&t=391
Unit-III	IPsec overview, Internet Key Exchanging (IKE)	https://youtu.be/XsgVqrcP32U
	Packet sniffing, Spoofing	https://youtu.be/Y6jLOqD9WzI?t=192
	Security protocols, Transport layer protocols	https://youtu.be/lnU-Zw3NEEQ?si=ElnLBRNE4t_833As
	Virus Counter measures	https://youtu.be/AXk_3avEAlM?t=464
	Firewalls design principles	https://youtu.be/BK6nxKDKijc?t=1
Unit-IV	Authentication Mechanisms: Passwords, Cryptographic authentication protocol	https://youtu.be/n17OOlXsUaU?t=240
	Web Security: SSL Encryption, TLS, SET	https://youtu.be/FmflaVEZRPo?t=645
	Email Security, PGPs / MIME	https://youtu.be/Ta8r_I7-wrw?t=489

Course Code	**PCC-MTCFIS-105A**				
Category	Professional Core Courses				
Course Title	**Operating System and Security**				
Scheme and Credits	L	T	P	**Credits**	**Semester-I**
	4	0	0	**4**	
Course Objectives	The objectives of this course are • To understand the core concepts of Operating Systems, including process management, synchronization, scheduling, and deadlock handling for efficient execution. • To evaluate memory management techniques like swapping, virtual memory, and page replacement to optimize system resources. • Learn the principles of file system and I/O management, including file structures, device drivers, and disk scheduling. • To explore Windows OS internals and tools like the registry, process/thread management, and WMI to manage system resources and automate tasks.				
Assessment	40 Marks				
End Semester Examination	60 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	Skill Demonstrated	RBT Level
CO1	Define the basic concepts of operating system and security.	Level 1: Remember
CO2	Understand the fundamentals of operating systems, process & memory management, threads, access control and file system security.	Level 2: Understand
CO3	Apply different scheduling, page replacement algorithms and principles of system security to solve the real world problems.	Level 3: Apply
CO4	Analyze process, memory & windows management techniques and security mechanisms for securing operating systems.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Introduction: Operating Systems Concepts, System Calls, OS Organization, Factors in OS Design, Basic Implementation Considerations, Time Sharing and Multi Programming, Real Time Systems.
Process Management: Process Concepts, Model, Process Synchronization, Process Scheduling, Threads.
Deadlock: Detection & Recovery, Avoidance, Prevention- Two Phase Locking Issues.

Unit-II

Memory Management: Basic Memory Management, Swapping, Virtual Memory, Page Replacement Algorithms, Segmentation, File System and I/O Management: Files, Low Level File Implementations, Memory Mapped Files, Directories, Implementation, Principles of I/O Hardware & Software, Device Drivers, Disks Hardware, Formatting & Arm Scheduling Algorithms.

Unit-III

Windows Management Mechanisms: The registry, Registry usage, Registry data types, Local structure, Troubleshooting Registry problems, Registry Internals, Services, Applications, Accounts, Service control Manager, Windows Management Instrumentation, Processes, Threads, and Jobs: Process Internals, Flow of create process, Thread Internals, Examining Thread creation, Thread Scheduling, Job Objects.

Unit-IV

Secure Operating Systems: Access control and file system security, Remote file system security, NFS, SMB, SFS, User authentication, Passwords, Biometrics, Smartcards, Intrusion Detection and Virus Protection: Trusted Computing, TCPA and NGSCB, Digital Rights Management.

Suggested Readings:

1. Modern Operating Systems by Andrew S. Tanenbaum, 2nd edition, Addison Wesley, 2001.
2. Operating Systems A Modern Perspective by Gary Nutt, 2nd edition, Pearson Education, 2001.
3. The Design of the Unix Operating System by Maurice J. Bach, Prentice Hall of India, 1991.
4. Microsoft® Windows® Internals by Mark E. Russinovich and David A. Solomon, 4th Edition, Microsoft Press, 2004.
5. Operating Systems: Internals and Design Principles by William Stallings, 5th Edition, Prentice Hall, 2005.

Useful Video links:

Unit No.	Topics	Links
Unit-I	Introduction to Operating System	https://archive.nptel.ac.in/noc/courses/noc21/SEM2/noc21-cs72/
	Introduction to Computer	https://archive.nptel.ac.in/courses/106/105/106105214/
	Deadlock	https://onlinecourses.swayam2.ac.in/cec22_cs23/preview
Unit-II	Introduction to Memory management	https://youtu.be/_pKbqFyG03s?si=3xUICKHljgRMR-_I
	Virtual Memory	https://youtu.be/kQKpJ4bD8TA?si=qtLN6B735HAFe9KE
	Arm Scheduling Algorithm	https://www.youtube.com/watch?v=9uoa_p8q47Y
Unit-III	Windows Registry & its Types	https://www.youtube.com/watch?v=jXaGtWy_5is
	Multi-Threading	https://www.youtube.com/watch?v=6rYOyIGfy3w
Unit-IV	Secure Operating System	https://www.youtube.com/playlist?list=PL0ABbZ9l6XI5y8yym50mVVP_m1WrDghff
	Intrusion Detection and Prevention Systems	https://www.youtube.com/watch?v=G_oJ2OtD9ys

Course Code	**PCC-MTCFIS-107A**				
Category	Professional Core Courses				
Course Title	**Cyber Forensics**				
Scheme and Credits	L	T	P	**Credits**	**Semester-I**
	4	0	0	**4**	
Course Objectives	The objectives of this course are • To develop a Comprehensive Understanding of Cyber Forensics. • To explore Forensic Technologies across Different Sectors. • To gain Proficiency in Evidence Collection and Analysis. • To master Network Forensics and Digital Crime Scene Investigation.				
Assessment	40 Marks				
End Semester Examination	60 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	Skill Demonstrated	RBT Level
CO1	Define the fundamental concepts, terminology, methods, and tools in cyber forensics and ethical hacking.	Level 1: Remember
CO2	Explain the concepts, technologies, and methods of cyber forensics and ethical hacking.	Level 2: Understand
CO3	Apply techniques, tools, and methodologies of cyber forensics and ethical hacking to resolve network intrusions, investigate cybercrimes cases and ensure data security to mitigate cyber threats across various domains.	Level 3: Apply
CO4	Analyze case studies, previous attacks and cyber forensic methodologies to detect, collect, investigate security breaches and identify vulnerabilities across digital systems.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Introduction to Cyber forensics: Information Security Investigations, Corporate Cyber Forensics, Scientific method in forensic analysis, investigating large scale Data breach cases, Analyzing Malicious software, Types of Computer Forensics Technology, Types of Military Computer Forensic Technology, Types of Law Enforcement: Computer Forensic Technology, Types of Business Computer Forensic Technology, Specialized Forensics Techniques, Hidden Data and How to Find It, Spyware and Adware, Encryption Methods and Vulnerabilities, Protecting Data from Being Compromised Internet Tracing Methods, Security and Wireless Technologies, Avoiding Pitfalls with Firewalls Biometric Security Systems.

Unit-II

Types of Computer Forensics Systems: Internet Security Systems, Intrusion Detection Systems, Firewall Security Systems, Storage Area Network Security Systems, Network Disaster Recovery Systems, Public Key Infrastructure

Systems, Wireless Network Security Systems, Satellite Encryption Security Systems, Instant Messaging (IM) Security Systems, Net Privacy Systems, Identity Management Security Systems, Identity Theft, Biometric Security Systems

Unit-III

Ethical Hacking: Essential Terminology, Windows Hacking, Malware, Scanning, Cracking. Digital Evidence in Criminal Investigations: The Analog and Digital World, Training and Education in digital evidence, Evidence Collection and Data Seizure: Why Collect Evidence, Collection Options Obstacles, Types of Evidence, The Rules of Evidence, Volatile Evidence, General Procedure, Collection and Archiving, Methods of Collection, Artifacts, Collection Steps, Controlling Contamination: The Chain of Custody, Reconstructing the Attack, The digital crime scene, Investigating Cybercrime, Duties Support Functions and Competencies.

Unit-IV

Identification of Data: Timekeeping, Forensic Identification and Analysis of Technical Surveillance Devices, Reconstructing Past Events: How to Become a Digital Detective, Useable File Formats, Unusable File Formats, Converting Files, Investigating Network Intrusions and Cyber Crime, Network Forensics and Investigating logs, Investigating network Traffic, Investigating Web attacks, Router Forensics, Cyber forensic tools and case studies.

Suggested Readings:

1. Computer Forensics: Computer Crime Scene Investigation by John R. Vacca, 2nd Edition, Charles River Media, 2005.
2. Understanding Cryptography: A Text book for Students and Practitioners by Christof Paar, Jan Pelzl, 2nd Edition, Springer's, 2010.
3. Ali Jahangiri, Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts, Ali Jahangiri, 2009.
4. Computer Forensics: Investigating Network Intrusions and Cyber Crime (Ec-Council Press Series: Computer Forensics), 2010.

Useful Video links:

Unit No.	Topics	Links
Unit-I	Introduction to Cyber forensics	https://www.youtube.com/watch?v=crmA2rzwHE
	Types of Computer Forensics Technology	https://www.youtube.com/watch?v=pKqyz0ckdK0
	Biometric Security Systems	https://youtu.be/GMDggxifxqk?si=PMvooWp607rFXDcJ
	Encryption Methods and Vulnerabilities	https://www.youtube.com/watch?v=HvZ-05RssYw
Unit-II	Intrusion Detection Systems	https://nptel.ac.in/courses/106106178
	Firewall Security Systems	https://www.youtube.com/watch?v=2YGUvopGkQc
	Satellite Encryption Security Systems	https://youtu.be/dt4Ce8gQPns?si=8om6_9gudSD_rdVe
Unit-III	Types of Evidence	https://www.youtube.com/watch?v=4mQ7fvJOkck
	Reconstructing the Attack	https://youtu.be/usOYloLB2SU?t=1
Unit-IV	Forensic Identification and Analysis of Technical Surveillance Devices	https://youtu.be/giv0DQDSsjQ?list=PLJu2iQtpGvv-2LtysuTTka7dHt9GKUbxD&t=1
	Network Forensics and Investigating logs	https://www.youtube.com/watch?v=bCFJcY8ifJw
	Cyber forensic tools and case studies.	https://youtu.be/JfvHzsexnmc?list=PLa2xctTiNSCiTGuejkc05zsr-G5t9AuH8&t=1

Course Code	**PCC-MTCFIS-109A**				
Category	Professional Core Courses				
Course Title	**Database Security**				
Scheme and Credits	L	T	P	**Credits**	**Semester-I**
	4	0	0	**4**	
Course Objectives	The objectives of this course are • To understand the fundamental problems and challenges in database security • To gain knowledge of security mechanisms used in databases • To explore the principles of statistical database protection and intrusion detection systems • To study models for the protection of new generation database systems				
Assessment	40 Marks				
End Semester Examination	60 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	Skill Demonstrated	RBT Level
CO1	Define the basic concepts of database security and security measures.	Level 1: Remember
CO2	Explain the principles of database security models, security mechanisms, and protection techniques in distributed, object-oriented, and new-generation database systems.	Level 2: Understand
CO3	Apply database security mechanisms, such as access control, encryption, and intrusion detection, to ensure secure database management systems.	Level 3: Apply
CO4	Analyze the strengths and weaknesses of various database security models and assess their applicability to real-world database security problems.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Introduction to Database Security Problems in Databases Security Controls, Security Models–1: Introduction Access Matrix Model Take-Grant Model, Aclcn Model, PN Model, Hartsor and Hsiao's Model, Fernandez's Model, Bussolati and Martella's Model for Distributed databases, Security Models 2: Bell and LaPadula's Model, Biba's Model, Dion's Model, Sea View Model, Jajodia and Sandhu's Model, the Lattice Model for the Flow Control conclusion.

Unit-II

Security Mechanisms: Introduction User Identification/Authentication Memory Protection Resource Protection Control Flow Mechanisms Isolation Security Functionalities in Some Operating Systems Trusted Computer System Evaluation Criteria - Security Software Design: Introduction, A Methodological Approach to Security Software Design Secure Operating System Design Secure DBMS Design Security Packages Database Security Design.

Unit-III

Statistical Database Protection & Intrusion Detection Systems: Introduction Statistics Concepts and Definitions Types of Attacks Inference Controls Evaluation Criteria for Control Comparison, Introduction IDES System, RETISS System, ASES System Discovery.

Unit-IV

Models For the Protection Of New Generation Database Systems -1: Introduction, A Model for the Protection of Frame Based Systems, Model for the Protection of Object: Oriented Systems SORION Model for the Protection of Object-Oriented Databases Models For The Protection Of New Generation Database Systems -2: A Model for the Protection of New Generation Database Systems: the Orion Model Jajodia anc Kenan's Model A Model for the Protection of Active Databases Conclusions.

Suggested Readings:

1. Database Security by Castano, Silvana; Fugini, Maria Grazia, Martella, Giancarlo, Pearson Edition, 1994.
2. Database Security and Auditing: Protecting Data Integrity and Accessibility by 1st Edition, Hassan Afyouni Thomos Edison, 2006.

Useful Video links:

Unit No.	Topics	Links
Unit-I	Database Security Problems in Databases Security Controls	https://www.youtube.com/watch?v=_2JLaovsRnk&list=PLyp-1WQY32mPzFy0oPS8VOsg9Z47glxbB
	LaPadula's Model Biba's Model	https://www.youtube.com/watch?v=9Co0OwXopyM
	Security Models in data base security	https://youtu.be/_2JLaovsRnk?si=8u1pqzS1nS5T9ivk
Unit-II	Security Mechanisms	https://www.youtube.com/watch?v=KOv4csT0W1s
	Operating system security	https://www.youtube.com/watch?v=3kKkOBClw1Q
	DBMS security design	https://www.youtube.com/watch?v=Nl-Sb1RZpew
Unit-III	Intrusion Detection Systems	https://www.youtube.com/watch?v=3xfLPBjs5BU&t=303s
	Inference Controls	https://www.youtube.com/watch?v=Z9ZjtvcgOcs
	Data base security	https://youtu.be/_2JLaovsRnk?si=DFXWAkT79kFg0f0x
	Database security and attacks	https://www.youtube.com/watch?v=xCL_amRLw7o
Unit-IV	New Generation Database System	https://www.youtube.com/watch?v=pyGj9AvHiJg
	Concept of object-oriented system	https://youtu.be/JUL1yhFrXkg?si=P4LMzwCld1xhdzSF

Course code	**LC-MTCFIS-111A**				
Category	Lab Course				
Course title	**Information Security Lab**				
Scheme and Credits	L	T	P	**Credits**	**Semester-I**
	0	0	2	1	
Course Objectives	The objectives of this course are • To understand and apply network monitoring and analysis tools. • To implement and evaluate cryptographic algorithms and protocols. • To develop secure communication systems. • To identify and mitigate common security vulnerabilities.				
Assessment	25 Marks				
End Semester Practical Examination	25 Marks				
Total	50 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	Skill Demonstrated	RBT Level
CO1	Understand basic network security concepts and threats.	Level 2: Understand
CO2	Implement access control mechanisms and models in real-world scenarios.	Level 3: Apply
CO3	Apply encryption techniques for secure communication.	Level 3: Apply
CO4	Analyze network protocols for security vulnerabilities, evaluate network security applications such as firewalls and intrusion detection systems, and propose effective mitigation techniques.	Level 4: Analyze

List of Experiments:

Sr. No.	Content
1	Study basic network security concepts and threats.
2	Implement a basic Access Control List (ACL) for a simulated network.
3	Implement the Bell-LaPadula security model for ensuring data confidentiality.
4	Demonstrate confidentiality and integrity using hashing algorithms (e.g., MD5 or SHA).
5	Encrypt and decrypt a message using symmetric key encryption (e.g., DES, AES).
6	Encrypt and decrypt a message using RSA (asymmetric key encryption).
7	Perform cryptanalysis on a simple substitution cipher.
8	Configure and demonstrate a secure communication using Secure Sockets Layer (SSL).

9	Simulate a basic Kerberos authentication process.
10	Implement and analyze the Internet Key Exchange (IKE) protocol for IPsec.
11	Simulate a simple intrusion detection system (IDS) to detect abnormal activities.
12	Design and configure a firewall using software tools (e.g., IP tables or pfSense).

Note: At least 10 experiments are to be performed by the students. Faculty member can add 2-3 extra experiment under topic beyond syllabus.

Course Code	**LC-MTCFIS-113A**				
Category	**Lab Course**				
Course title	**OS Security Lab**				
Scheme and Credits	L	T	P	**Credits**	**Semester-I**
	0	0	2	1	
Course Objectives	The objectives of this course are ● To teach the fundamentals of core operating system concepts like process management, memory allocation, and file systems through practical experiments. ● To give exposure and training to handle OS security mechanisms including access control, user authentication, and secure file systems.				
Assessment	25 Marks				
End Semester Practical Examination	25 Marks				
Total	50 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	Skill Demonstrated	RBT Level
CO1	Understand basic concepts of operating system security.	Level 2: Understand
CO2	Implement the fundamental concepts of operating systems and secure operating system mechanisms.	Level 3: Apply
CO3	Implement algorithms and system calls to manage processes, memory, and files effectively in an operating system.	Level 3: Apply
CO4	Analyze and simulate deadlock scenarios, page replacement algorithms, and disk scheduling strategies.	Level 4: Analyze

List of Experiments:

Sr. No.	Content
1	Study basic concepts of operating system security.
2	Write a program to demonstrate the use of system calls for file operations.
3	Write a script to read, write, and modify Windows registry keys using a high-level programming language.
4	Implement file access control lists (ACLs) to simulate secure file access.
5	Write a program to simulate user authentication using password-based security.
6	Implement a producer-consumer problem using semaphores or mutexes.
7	Develop a program to examine thread creation and scheduling using Windows APIs.
8	Simulate virtual memory management using paging and segmentation
9	Write a program to detect a deadlock using a resource allocation graph.

10	Implement disk arm scheduling algorithms like FCFS, SSTF, or C-SCAN.
11	Implement page replacement algorithms.

Note: At least 10 experiments are to be performed by the students. Faculty member can add 2-3 extra experiment under topic beyond syllabus.

Course Code	**SM-MT-115A**				
Category	Seminar				
Course Title	**Seminar-I**				
Scheme and Credits	L	T	P	**Credits**	**Semester-I**
	0	0	2	**2**	
Course Objectives	The objectives of this course are • To develop students' ability to effectively present research topics and findings by effective communication. • To improve problem-solving and critical thinking skills of the students. • To expose students to the latest trends and advancements by reviewing and discussing contemporary research.				
Assessment	50 Marks				
End Semester Examination	-				
Total	50 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	**Skill Demonstrated**
CO1	Identify the trends and advancements in the related field.
CO2	Analyze and synthesize research literature with in-depth reviews of key studies and methodologies.
CO3	Undertake problem identification, formulation, proposing solution and analyze the impact on society, economy and environment.
CO4	Prepare a well-organized report employing elements of effective communication and critical thinking.
CO5	Demonstrate a sound technical knowledge of their research field.

Overview:

This is a course designed to help M. Tech students develop research presentation skills. The focus is on selecting a topic or research paper relevant to their specialization, conducting an in-depth review, and effectively presenting the research findings.

General Guidelines:

Topic Selection	Each student is required to choose the research topic based on published review paper(s) or literature related to their relevant field. The same topic cannot be selected by multiple students.
Approval Process	The selected paper or topic must be approved by the faculty members/committee appointed by the Head of Department.
Presentation Guidelines	Each student will have 30-40 minutes for their presentation, followed by 5 minutes for Q &A.
Evaluation	The presentation will be evaluated by a committee constituted by the Head of Department. The evaluation will be based on:

Parameters for the Evaluation of Seminar:

Sr. No.	Parameters	Marks Allotted	Relevant COs
1	Clarity of the topic	10	CO1
2	Literature Survey	10	CO2
3	Content Relevancy	10	CO3
4	Presentation Skills	10	CO4
5	Q &A Response	10	CO5

GANGA INSTITUTE OF TECHNOLOGY AND MANAGEMENT, KABLANA, JHAJJAR (HR.)

Scheme of Studies and Examination

M. Tech (Cyber Forensics and Information Security)–2nd Semester

w.e.f. 2024-25

Sr. No.	Category	Course Code	Course Title	Hours per week			Total Load Per Week	Credits	Examination Scheme (Marks)				Exam Duration in H
				Lecture (L)	Tutorial (T)	Practical (P)			Assessment	End Semester Examination		Total	
										Theory	Practical		
1	Professional Core Courses	PCC-MTCFIS-102A	Ethical Hacking and Digital Forensics	4	0	0	4	4	40	60		100	3
2	Professional Core Courses	PCC- MTCFIS-104A	Steganography and Digital Watermarking	4	0	0	4	4	40	60		100	3
3	Professional Elective Courses	Refer Table-I	.....	4	0	0	4	4	40	60		100	3
4	Multidisciplinary Open Elective Courses	Refer Table-II	.....	3	0	0	3	3	40	60		100	3
5	Foundation Elective Courses	Refer Table-III	.....	3	0	0	3	3	40	60		100	3
6	Lab Course	LC-MTCFIS-106A	Ethical Hacking Lab	0	0	2	2	1	25		25	50	3
7	Lab Course	LCMTCFIS-108A	Steganography Lab	0	0	2	2	1	25		25	50	3
8	Seminar	SM-MT-110A	Seminar-II	0	0	2	2	2	50			50	
Total Credits								**22**				**650**	

Course Code	**PCC-MTCFIS-102A**				
Category	Professional Core Courses				
Course Title	**Ethical Hacking and Digital Forensics**				
Scheme and Credits	L	T	P	**Credits**	**Semester-II**
	4	0	0	**4**	
Course Objectives	The objectives of this course are • To understand and analyze various hacking techniques • To explore networking security protocols and vulnerabilities • To examine strategies for fraud detection and prevention • To develop expertise in fraud analysis and forensic techniques.				
Assessment	40 Marks				
End Semester Examination	60 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	Skill Demonstrated	RBT Level
CO1	Define the basic concepts of ethical hacking and cyber forensics.	Level 1: Remember
CO2	Understand the fundamental concepts and techniques in cyber security, threat identification, attack prevention, fraud detection, and system protection.	Level 2: Understand
CO3	Apply cyber security concepts and techniques to identify threats, prevent attacks, detect fraud, and secure digital systems.	Level 3: Apply
CO4	Analyze cyber security threats, attack methods, network vulnerabilities, fraud detection techniques to enhance the security and integrity of digital systems.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Hacking windows, Network hacking, Web hacking, Password hacking. A study on various attacks, Input validation attacks, SQL injection attacks, Buffer overflow attacks, Privacy attacks.

Unit-II

TCP / IP, Checksums, IP Spoofing port scanning, DNS Spoofing, DOS attacks, SYN attacks, Smurf attacks, UDP flooding, DDOS, Models. Firewalls, Packet filter firewalls, Packet Inspection firewalls, Application Proxy Firewalls, Batch file programming.

Unit-III

Fundamentals of Computer Fraud, Threat concepts, Framework for predicting inside attacks, managing the threat, Strategic Planning Process, Architecture strategies for computer fraud prevention, Protection of Websites, Intrusion detection system, NIDS, HIDS, Penetration Testing process, Web Services, Reducing transaction risks.

Unit-IV

Key Fraud Indicator selection process customized taxonomies, Key fraud signature selection process, Accounting Forensics, Computer Forensics, Journaling and its requirements, Standardized Logging criteria, Journal Risk And control matrix, Neural Networks, Misuse Detection and Novelty detection.

Suggested Readings:

1. Insider Computer Fraud by Kenneth C. Brancik, Auerbach Publications Taylor & Francis Group, 2008.
2. Ethical Hacking by Ankit Fadia, 2nd Edition, Macmillan India Ltd, 2006.

Useful Video links:

Unit No.	Topics	Links
Unit-I	Introduction to Ethical Hacking	https://youtu.be/qswOrF2WPaw?si=aChTJPlb1byA7AJi
	SQL injection attacks	https://www.youtube.com/watch?v=lwqACxcFOO0
	Buffer overflow attacks	https://www.youtube.com/watch?v=7nFUdrAZib4&t=75s
Unit-II	TCP / IP, Checksums	https://www.youtube.com/watch?v=EO4B_ykP8f8
	Firewalls	https://www.youtube.com/watch?v=2YGUvopGkQc
	DDOS, Models	https://www.youtube.com/watch?v=Wan1S9RJacU
Unit-III	Fundamentals of Computer Fraud	https://www.youtube.com/watch?v=weWbKxN5qIE
	Penetration Testing process	https://www.youtube.com/watch?v=C44oY7safys
	Advanced Fraud Prevention Technologies	https://www.youtube.com/watch?v=uCDe72jtarA
Unit-IV	Key fraud signature selection process	https://www.youtube.com/watch?v=3J23S9VJQBs
	Novelty Detection through Model-Based Characterization of Neural Networks	https://www.youtube.com/watch?v=CkPC-vGR7Dk

Course Code	**PCC- MTCFIS-104A**				
Category	Professional Core Courses				
Course Title	**Steganography And Digital Watermarking**				
Scheme and Credits	L	T	P	**Credits**	**Semester-II**
	4	0	0	**4**	
Course Objectives	The objectives of this course are • To understand the principles and historical context of information hiding in steganography and watermarking. • To evaluate various steganographic techniques. • To investigate the techniques used for detecting, extracting, and disabling hidden information. • To assess the principles, algorithmic design issues, and current techniques in watermarking.				
Assessment	40 Marks				
End Semester Examination	60 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	Skill Demonstrated	RBT Level
CO1	Define the basic concepts of information hiding, steganography, and watermarking in digital media and communication systems.	Level 1: Remember
CO2	Explain the principles and applications of steganography and watermarking.	Level 2: Understand
CO3	Apply steganographic techniques to hide information in digital media, ensuring robustness against common attacks and distortions.	Level 3: Apply
CO4	Analyze various information hiding methods based on detection, security, and robustness against attacks.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Introduction to Information hiding, Brief history and applications of information hiding, Principles of Steganography, Frameworks for secret communication, Security of Steganography systems, Information hiding in noisy data, Adaptive versus non adaptive algorithms, Laplace filtering, Using cover models, Active and malicious attackers, Information hiding in written text, Examples of invisible communications.

Unit-II

Survey of steganographic techniques, Substitution system and bitplane tools, Transform domain techniques, Spread spectrum and information hiding, Statistical Steganography, Distortion and code generation techniques, Automated generation of English text.

Unit-III

Steganalysis, Detecting hidden information, Extracting hidden information, Disabling hidden information, Watermarking techniques, History, Basic Principles, applications, Requirements of algorithmic design issues, Evaluation and benchmarking of watermarking system.

Unit-IV

Survey of current watermarking techniques, Cryptographic and psycho visual aspects, Choice of a workspace, Formatting the watermark bets, Merging the watermark and the cover, Optimization of the watermark receiver, Extension from still images to video, Robustness of copyright making systems, Fingerprints, Examples, Classification, Research history, Schemes, Digital copyright and watermarking, Conflict of copyright laws on the internet.

Suggested Readings:

1. Information hiding techniques for Steganography and Digital Watermarking by Stefan Katzenbelsser and Fabien A. P. Petitcolas, ARTECH House Publishers, 2004.
2. Steganography in Digital Media: Principles, Algorithms, and Applications by Jessica Fridrich, Cambridge university press, 2010.
3. Digital Image Steganography by Abbas Cheddad, VDM Verlag Dr. Müller Aktiengesellschaft & Co. KG, Dec 2009.
4. Digital Watermarking And Steganography by Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich and Ton Kalker, Morgan Kaufmann Publishers, Nov 2007.

Useful Video links:

Unit No.	Topics	Links
Unit-I	Introduction to Information hiding	https://youtu.be/t4GPGkLh4Vg?feature=shared
	Security of Steganography systems	https://www.youtube.com/watch?v=CWQfbYrommk
	Cyber Security: Steganography, Introduction	https://youtu.be/wLRb9zhhqIk?feature=shared
Unit-II	Steganographic techniques	https://www.youtube.com/live/u_luy52v7z4?feature=shared
	Transform domain techniques	https://youtu.be/ODf76oPiPWQ?feature=shared
Unit-III	Ste analysis	https://www.youtube.com/watch?v=xtZPe4RWe4s
	Introduction of digital watermarking	https://youtu.be/WvRBKn8-JJA?feature=shared
Unit-IV	Cryptographic and psycho visual aspects	https://youtu.be/iTVyKbDCJrA?feature=shared
	Fingerprints	https://youtu.be/45uJAOs22jE?feature=shared

Course code	**LC-MTCFIS-106A**				
Category	Lab Course				
Course title	**Ethical Hacking Lab**				
Scheme and Credits	L	T	P	**Credits**	**Semester-II**
	0	0	2	1	
Course Objectives	The objectives of this course are • To implement firewall rules to control network traffic and enhance security. • To deploy and configure firewall IDS to detect and alert on suspicious network activities • To set up honeypots to attract and analyze cyber attackers. • To configure and apply ethical hacking tools to enhance system security				
Assessment	25 Marks				
End Semester Practical Examination	25 Marks				
Total	50 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	Skill Demonstrated	RBT Level
CO1	Understand the fundamental concepts of network security, ethical hacking techniques, and the identification of vulnerabilities in network systems.	Level 2: Understand
CO2	Apply security tools and techniques to monitor network traffic, detect unauthorized access, and implement protective measures to defend systems from attacks.	Level 3: Apply
CO3	Implement security protocols, configure firewalls, and deploy intrusion detection systems to enhance the defense mechanisms of network infrastructure.	Level 3: Apply
CO4	Analyze security measures to prevent attacks, and determine areas for improvement in strengthening an organization's network security.	Level 4: Analyze

List of Experiments:

Sr. No.	Content
1	Study Trojan, backdoor tool for monitoring network communication on a test network.
2	Write a program to apply Data Packet Sniffers tools to monitor network communication and assess security risks.
3	Write a program to apply any Keylogger to steal data and suggest countermeasures against keyloggers.
4	Write a program to apply Password guessing to identify vulnerabilities and implement.
5	Write a program to apply Penetration Testing using proper tools.
6	Write a program to implement countermeasures to defend against Denial of Service in the controlled lab environment.

7	Write a program to implement security tools to identify and mitigate vulnerabilities in wireless networks.
8	Write a program to appl**y** Firewalls and Intrusion Detection systems to protect the network against unauthorized access and enhance network security.
9	Write a program to implement Password Cracking script ethically in a controlled lab environment.
10	Write a program to implement honeypots to enhance system integrity and mitigate the risk of malicious activities.

Note: At least 10 experiments are to be performed by the students. Faculty member can add 2-3 extra experiment under topic beyond syllabus.

Course code	**LC-MTCFIS-108A**				
Category	Engineering Science Courses				
Course title	**Steganography Lab**				
Scheme and Credits	L	T	P	**Credits**	**Semester-II**
	0	0	2	1	
Course Objectives	The objectives of this course are • To develop Expertise in Steganography and Information Hiding Techniques. • To gain practical knowledge of digital watermarking systems. • To understand and apply cryptographic methods for data security. • To analyze the advanced security techniques and protocols in Information Hiding.				
Assessment	25 Marks				
End Semester Practical Examination	25 Marks				
Total	50 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	Skill Demonstrated	RBT Level
CO1	Understand the basic concepts of steganography and watermarking.	Level 2: Understand
CO2	Implement digital certificates for authorization.	Level 3: Apply
CO3	Apply the concepts of information hiding and encryption for privacy and security.	Level 3: Apply
CO4	Analyze steganography and watermarking techniques to enhance performance and security.	Level 4: Analyze

List of Experiments:

Sr. No.	Content
1	Study common steganography methods used.
2	Study basic principles of digital watermarking.
3	Write a program to implement a digital certificate for authorization.
4	Write a program to implement encryption and decryption techniques.
5	Write a program to implement Information hiding in binary files.
6	Write a program to implement Information hiding in text.
7	Write a program to implement Information hiding in images.
8	Write a program to implement Information hiding in audio/video.

9	Write a program to implement Information hiding using DNA techniques.
10	Write a program to analyze different steganography methods.
11	Write a program to analyze performance of LSB and DCT Watermarking.

Note: At least 10 experiments are to be performed by the students. Faculty member can add 2-3 extra experiment under topic beyond syllabus.

Course Code	**SM-MT-110A**				
Category	Seminar				
Course Title	**Seminar-II**				
Scheme and Credits	L	T	P	**Credits**	**Semester-II**
	0	0	2	**2**	
Course Objectives	The objectives of this course are • To develop students' ability to effectively present research topics and findings by effective communication. • To improve problem-solving and critical thinking skills of the students. • To expose students to the latest trends and advancements by reviewing and discussing contemporary research.				
Assessment	50 Marks				
End Semester Examination	-				
Total	50 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	Skill Demonstrated
CO1	Identify the trends and advancements in the related field.
CO2	Analyze and synthesize research literature with in-depth reviews of key studies and methodologies.
CO3	Undertake problem identification, formulation, proposing solution and analyze the impact on society, economy and environment.
CO4	Prepare a well-organized report employing elements of effective communication and critical thinking.
CO5	Demonstrate a sound technical knowledge of their research field.

Overview:

This is a course designed to help M. Tech students develop research presentation skills. The focus is on selecting a topic or research paper relevant to their specialization, conducting an in-depth review, and effectively presenting the research findings.

General Guidelines:

Topic Selection	Each student is required to choose the research topic based on published review paper(s) or literature related to their relevant field. The same topic cannot be selected by multiple students.
Approval Process	The selected paper or topic must be approved by the faculty members/committee appointed by the Head of Department.
Presentation Guidelines	Each student will have 30-40 minutes for their presentation, followed by 5 minutes for Q&A.
Evaluation	The presentation will be evaluated by a committee constituted by the Head of Department. The evaluation will be based on:

Parameters for the Evaluation of Seminar:

Sr. No.	Parameters	Marks Allotted	Relevant COs
1	Clarity of the topic	10	CO1
2	Literature Survey	10	CO2
3	Content Relevancy	10	CO3
4	Presentation Skills	10	CO4
5	Q&A Response	10	CO5

Course Code	**PEC- MTCFIS-112A**				
Category	Professional Elective Courses				
Course Title	**Advanced Computer Networks**				
Scheme and Credits	L	T	P	**Credits**	**Semester-II**
	4	0	0	**4**	
Course Objectives	The objectives of this course are • To learn the structure and functions of the TCP/IP and OSI models. • To master IP addressing and routing: Understand IPv4/IPv6 addressing and network-layer routing protocols. • To explore transport and application protocols: Gain proficiency in TCP, UDP, and common application-layer protocols. • To learn about Wi-Fi, Mobile IP, and multimedia networking technologies.				
Assessment	40 Marks				
End Semester Examination	60 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	Skill Demonstrated	RBT Level
CO1	Define the fundamental concepts of computer networks.	Level 1: Remember
CO2	Understand the advanced concepts of computer networks.	Level 2: Understand
CO3	Apply the concepts of networking to solve computational challenges in computer networks.	Level 3: Apply
CO4	Analyze advanced networking concepts, protocols and addressing to improve network performance and enhance security.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Foundation of Networking Protocols: 5-layer TCP/IP Model, 7-layer OSI Model, Internet Protocols and Addressing, Equal-Sized Packets Model: ATM -Networking Devices: Multiplexers, Modems and Internet Access Devices, Switching and Routing Devices, Router Structure.

The Link Layer and Local Area Networks: Link Layer: Introduction and Services, Error-Detection and Error-Correction techniques,- Multiple Access Protocols, Link Layer Addressing, Ethernet, Interconnections: Hubs and Switches, PPP: The Point-lo-Point Protocol, Link Visualization - Routing and Internetworking: Network-Layer Routing, Least-Cost-Path algorithms, Non-Least-Cost-Path algorithms, Intradomain Routing Protocols, Interdomain Routing Protocols, Congestion Control at Network Layer.

Unit-II

Logical Addressing: IPv4 Addresses, IPv6 Addresses - Internet Protocol: Internetworking, IPv4, IPv6, Transition from IPv4 to IPv6 - Multicasting Techniques and Protocols: Basic Definitions and Techniques, Intradomain Multicast Protocols, Interdomain Multicast Protocols, Node-Level Multicast algorithms - Transport and End-to-End

Protocols: Transport Layer, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Mobile Transport Protocols, TCP Congestion Control - Application Layer: Principles of Network Applications, The Web and HTTP, File Transfer: FTP, Electronic Mail in the Internet, Domain Name System (DNS), P2P File Sharing, Socket Programming with TCP and UDP, Building a Simple Web Server.

Unit-III

Wireless Networks and Mobile IP: Infrastructure of Wireless Networks, Wireless LAN Technologies. IEEE: 802.11 Wireless Standard, Cellular Networks, Mobile IP, Wireless Mesh Networks (WMNs) - Optical Networks and WDM Systems: Overview of Optical Networks, Basic Optical Networking Devices, Large-Scale Optical Switches, Optical Routers, Wavelength Allocation in Networks, Case Study: An All-Optical Switch.

Unit-IV

VPNs, Tunneling and Overlay Networks: Virtual Private Networks (VPNs), Multiprotocol Label Switching (MPLS), Overlay Networks-VoIP and Multimedia Networking: Overview of IP Telephony, VoIP Signaling Protocols, Real-Time Media Transport Protocols, Distributed Multimedia Networking, Stream Control Transmission Protocol.
Mobile A-Hoc Networks: Overview of Wireless Ad-Hoc Networks, Routing in Ad-Hoc Networks, Routing Protocols for Ad-Hoc Networks - Wireless Sensor Networks: Sensor Networks and Protocol Structures, Communication Energy Model, Clustering Protocols, Routing Protocols

Suggested Readings:

1. Computer Networking: A Top-Down Approach Featuring the Internet by James E Kurose, Keith W. Ross, Third Edition, Pearson Education, 2007.
2. Computer and Communication Networks by Nader F. Mir, Pearson Education. 2007.
3. Data Communications and Networking by Behrouz A. Forouzan, Fourth Edition, TMH, 2007.
4. An Engineering Approach to Computer Networking by S. Keshav. Pearson Education, 4th Edition, 1997.
5. Computer Networks by Andrew S. Tanenbaum, Fourth Edition, Prentice Hall, 4th Edition, 2002.

Useful Video links:

Unit No.	Topics	Links
Unit-I	Network model	https://youtu.be/b6f9vh3cd6w
	Link layer	https://youtu.be/rGWPOm3ectk
Unit-II	IP V4	https://youtu.be/5vbPS-KnhvI
	IP V6	https://youtu.be/FkaFr3cpg6U
Unit-III	IEEE 802.11	https://youtu.be/6SWBxiPeSqk
	Mobile IP	https://youtu.be/0QLRULNfbFg
Unit-IV	Multiprotocol Label Switching (MPLS)	https://youtu.be/t2WpMsk18yU?feature=shared
	Mobile Ad-Hoc Networks	https://youtu.be/ycaz99NogS4

Course Code	**PEC- MTCFIS-114A**				
Category	Professional Elective Courses				
Course Title	**Security Threats**				
Scheme and Credits	L	T	P	**Credits**	**Semester-II**
	4	0	0	**4**	
Course Objectives	The objectives of this course are • To understand and Identify Security Threats • To implement Effective Risk and Threat Management • To master Security Elements and Protocols • To apply Access Control and Trusted Computing Practices.				
Assessment	40 Marks				
End Semester Examination	60 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	Skill Demonstrated	RBT Level
CO1	Define the basic concepts of security threats, vulnerabilities, and common attack techniques in network and information security.	Level 1: Remember
CO2	Explain the concepts of security threats, risk management, and threat identification methods to enhance understanding of cybersecurity practices.	Level 2: Understand
CO3	Apply appropriate security measures and techniques to safeguard systems and networks.	Level 3: Apply
CO4	Analyze potential security risks and vulnerabilities using threat modeling, forensic analysis, and vulnerability assessment tools.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Introduction: Security threats, Sources of security threats, Motives, Target Assets and vulnerabilities, Consequences of threats, E-mail threats, Web-threats - Intruders and Hackers, Insider threats, Cybercrimes. Network Threats: Active/ Passive, Interference, Interception, Impersonation, Worms, Virus, Spam's, Adware, Spyware, Trojans and covert channels, Backdoors, Bots, IP, Spoofing: ARP spoofing, Session Hijacking, Sabotage, Internal treats, Environmental threats, Threats to Server security.

Unit-II

Security Threat Management: Risk Assessment, Forensic Analysis, Security threat correlation, Threat awareness, Vulnerability sources and assessment, Vulnerability assessment tools, Threat identification, Threat Analysis, Threat Modeling, Model for Information Security Planning.

Unit-III

Security Elements: Authorization and Authentication - types, policies and techniques - Security certification - Security monitoring and Auditing - Security Requirements Specifications - Security Policies and Procedures, Firewalls, IDS, Log Files, Honey Pots.

Unit-IV

Access control, Trusted Computing and multilevel security - Security models, Trusted Systems, Software security issues, Physical and infrastructure security, Human factors ,Security awareness, training, Email and Internet use policies.

Suggested Readings:

1. Threat Modeling by Swiderski, Frank and Syndex, Microsoft Press, 2004.
2. Computer Security: Principles and Practice by William Stallings and Lawrie Brown, Prentice Hall, 2008.
3. Computer Network Security by Joseph M Kizza, Springer Verlag, 2005.
4. Information Security Intelligence: Cryptographic Principles & Application by Thomas Calabres and Tom Calabrese, Thomson Delmar Learning, 2004.

Course Code	**PEC- MTCFIS-116A**				
Category	Professional Elective Courses				
Course Title	**Multimedia Security**				
Scheme and Credits	L	T	P	**Credits**	**Semester-II**
	4	0	0	**4**	
Course Objectives	The objectives of this course are • To understand the Fundamentals of Digital Watermarking. • To explore Media-Specific Watermarking Techniques. • To analyze and Develop Secure Watermarking Protocols. • To integrate Cryptography with Multimedia Security.				
Assessment	40 Marks				
End Semester Examination	60 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	Skill Demonstrated	RBT Level
CO1	Define the fundamental concepts of digital watermarking, protocols and basic cryptographic principles used in multimedia encryption.	Level 1: Remember
CO2	Understanding the concepts of digital watermarking, models, media-specific applications and the application of cryptographic protocols for secure watermarking and multimedia encryption.	Level 2: Understand
CO3	Apply digital watermarking techniques to various media formats and implement cryptographic methods and secure watermarking protocols to protect and encrypt multimedia data.	Level 3: Apply
CO4	Analyze the effectiveness of digital watermarking techniques and cryptographic protocols in securing multimedia content and preventing forgeries across various media formats.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Digital Watermarking Basics: Models of Watermarking, Basic Message Coding, Error Correction Coding. Digital Watermarking and Digital Communications: Mutual Information and Channel Capacity, How to Design a Good Digital Watermark, Spread Spectrum Watermarking, Block DC domain Watermarking, Watermarking with Side-Information (Dirty-paper Coding), Improved Spread Spectrum Watermarking, Affine-Resistant Watermarking.

Unit-II

Media Specific Digital Watermarking: Image Watermarking, Video Watermarking, Audio Watermarking, Watermarking for CG-models, Watermarking for Binary Images, Watermarking for 3D Contents, Data Hiding through watermarking techniques.

Unit-III

Digital Watermarking Protocols: A Buyer-Seller Watermarking Protocol, An Efficient and Anonymous Buyer-Seller, Watermarking Protocol, Extensions of Watermarking Protocols, Protocols for Secure Computation.

Unit-IV

Cryptography and Multimedia Encryption: Introduction to Cryptography, Multimedia Processing in the Encryption Domain, Privacy preserving Information Processing, Information Theory and Digital Forensics, Forgeries Detection, New ways for making Forgeries.

Suggested Readings:

1. Digital Watermarking and Steganography, 2nd Edition, by Cox, Miller, Bloom, Fredric, and Kalker, 2008.
2. Multimedia Security Handbook by Borko Furth, Darko Kirov ski, CRC Press, 2004.
3. Multimedia Security Technologies for Digital Rights Management by Wenjun Zeng, Heather Yu, Ching-Yung Lin, Elsevier, 2006.

Useful Video links:

Unit No.	Topics	Links
Unit-I	Digital Watermarking	https://youtu.be/gd2W0vaKTxA?t=395
	Models of Watermarking	https://youtu.be/2Kx9jbSMZqA?t=1
Unit-II	Image Watermarking, Video Watermarking	https://youtu.be/2AoD5pDMjXQ?t=99
	Audio Watermarking	https://youtu.be/Xv7hay6w_Uc?t=489
	Data Hiding through watermarking techniques.	https://youtu.be/FuqVbw1jJ_s?t=17
Unit-III	A Buyer-Seller Watermarking Protocol	https://youtu.be/tf9zVbL9Kvg?t=697
	Protocols for Secure Computation	https://youtu.be/mhEz8DoueXg?t=4
Unit-IV	Cryptography and Multimedia Encryption	https://youtu.be/xHlSWqJT8lc?t=2434
	Digital Forensics	https://youtu.be/giv0DQDSsjQ?list=PLJu2iQtpGvv-2LtysuTTka7dHt9GKUbxD&t=1233
	Information Theory	https://youtu.be/TlzTNjD_t8I?si=nwM-LF4daopUMZeU

Course Code	**PEC- MTCFIS-118A**				
Category	Professional Elective Courses				
Course Title	**Mobile & Wireless Security**				
Scheme and Credits	L	T	P	**Credits**	**Semester-II**
	4	0	0	**4**	
Course Objectives	The objectives of this course are • To understand and analyze the key components of wireless network hardware, protocols, and security mechanisms • To explore the implementation of standards and policy solutions for wireless network security • To examine the core principles of security in wireless networks • To investigate the role of global mobile satellite systems and enterprise wireless networks				
Assessment	40 Marks				
End Semester Examination	60 Marks				
Total	100 Marks				
Duration of Exam	03 Hours				

Course Outcomes: After studying this course, the students will be able to

CO	Skill Demonstrated	RBT Level
CO1	Define the fundamental concepts of mobile and wireless networks.	Level 1: Remember
CO2	Understand the basic concepts of mobile and wireless networks.	Level 2: Understand
CO3	Apply security solutions and configure wireless networks to ensure protection against common security threats.	Level 3: Apply
CO4	Analyze wireless network protocols, security mechanisms, vulnerabilities and global mobile satellite systems for enhanced security of wireless communication systems.	Level 4: Analyze

Note: Examiner will set nine questions in total. Question one will be compulsory. Question one will have 8 parts (2 from each unit/section) of 1.5 marks each and remaining eight questions of 12 marks each to be set by taking two questions from each unit. The students have to attempt five questions in total, first being compulsory and selecting one from each unit.

Unit-I

Wireless Fundamentals: Wireless Hardware, Wireless Network Protocols, Wireless Programming, WEP Security. Wireless Cellular Technologies: concepts, Wireless reality, Security essentials, Information classification standards, Wireless Threats: Cracking WEP, Hacking Techniques, Wireless Attacks, Airborne Viruses**.**

Unit-II

Standards and Policy Solutions: Network Solutions, Software Solutions. Physical Hardware Security, Wireless Security: Securing WLAN, Virtual Private Networks, Intrusion Detection System, Wireless Public Key infrastructure. Tools: Auditing tools, Pocket PC hacking, wireless hack walkthrough.

Unit-III

Security Principles: Authentication, Access control and Authorization, Non-repudiation, privacy and Confidentiality, Integrity and Auditing, Security analysis process, Privacy in Wireless World, Legislation and Policy, Identify targets and roles analysis, Attacks and vulnerabilities, Analyze mitigations and protection.
WLAN Configuration: IEEE 802.11, Physical layer, media access frame format, systematic exploitation of 802.11b WLAN, WEP, WEP Decryption script, overview of WEP attack, Implementation, Analysis of WEP attacks.

Unit-IV

Global Mobile Satellite Systems, case studies of the IRIDIUM and GLOBALSTAR systems, Wireless Enterprise Networks: Introduction to Virtual Networks, Bluetooth technology, Bluetooth Protocols. Server-side programming in Java, Pervasive web application architecture, Device independent example application.

Suggested Readings:

1. Wireless Security Essentials: Defending Mobile from Data Piracy by Russel Dean Vines, John Wiley & Sons, 1st Edition, 2002.
2. Maximum Wireless Security by Cyrus, Peikari and Seth Fogie, SAMS Publishing, 2002.
3. Neural Networks by Simon Haykin, Pearson Education.
4. Mobile and Personal Communication systems and services by Raj Pandya, Prentice Hall of India, 2001.

Useful Video links:

Unit No.	Topics	Links
Unit-I	Types of Wireless communication	https://youtu.be/QHDxbbc1GWs?si=e1NbtFic9v7q0Nyd
	The cellular concept - System Design issues	https://youtu.be/whYljse4Abc?si=Zgd0q8lvjyuHfs2Y
	5G and other Wireless Technologies	https://www.youtube.com/watch?v=MONjGfn0Sjk
Unit-II	Intruders - Types, Intrusion Detection Systems	https://www.youtube.com/watch?v=Q0eLuRLKiCE
	Internet Key Exchange - Phases, Modes, Methods	https://www.youtube.com/watch?v=BNr9JP76ZSQ
Unit-III	Intruders - Types, Intrusion Detection Systems	https://www.youtube.com/watch?v=Q0eLuRLKiCE
	Internet Key Exchange - Phases, Modes, Methods	https://www.youtube.com/watch?v=BNr9JP76ZSQ
Unit-IV	Bluetooth Architecture, Protocol Stack	https://www.youtube.com/watch?v=XDwz1XNOkhY
	Global Navigation Satellite System	https://www.youtube.com/watch?v=kHOsM9dGTEA