Shri Rawatpura Sarkar University, Raipur

Examination Scheme & Syllabus

For

Master of Technology

In

Computer Science & Engineering

Specialization : Cyber Forensics

Semester-I

(Effective from the session: 2022-23)

**Faculty of Engineering,
Shri Rawatpura Sarkar University, Raipur**

SHRI RAWATPURA SARKAR UNIVERSITY, RAIPUR, CHHATTISGARH
FACULTY OF ENGINEERING

Three Years M.Tech(Cyber Forensics) Programme

Scheme of Teaching and Examination
Master of Technology – Ist Semester
Computer Science & Engineering

Outcome Based Education (OBE) and Choice Based Credit System (CBCS)

(**Effective from the Academic Year 2022-2023**)

Sr. No.	Course Code	Course Title	Hours / Week			Credits	Maximum Marks			Sem End Exam Duration (Hrs)
			L	T	P		Continuous Evaluation	Sem End Exam	Total	
1	**EMT06101**	Cyber Security Fundamentals	3	1	-	4	30	70	100	3 Hr.
2	**EMT06102**	Research Methodology for Engineers	3	1	-	4	30	70	100	3 Hr.
3	**EMT06103**	Digital Forensics	3	1	-	4	30	70	100	3 Hr.
4	**EMT06104**	Cryptography & Network Security	3	1	-	4	30	70	100	3 Hr.
5	**EMT06105**	Operating System & Security	3	1	-	4	30	70	100	3 Hr.
6	**EMT06106**	Digital Forensics Lab	-	-	4	2	15	35	50	3 Hr.
7	**EMT06107**	Operating System & Security Lab	-	-	4	2	15	35	50	3 Hr.
Total Contact hr. per week: 28			**Total Credit**			**24**	**180**	**420**	**600**	

Course Title	CYBER SECURITY FUNDAMENTALS				
Course Code	EMT06101				
Course Credits	**L**	**T**	**P**	**TC**	
	3	**1**	**-**	**4**	
Prerequisites	Basic knowledge about Cyber security fundamental.				
Course Objectives	1. Interpret and analyze operating system and machine level structures. 2. Assess trends in computer criminology and social behaviors related to technology use including physical security. 3. Engage in ethical decision-making and apply ethical principles to cyber security. 4. Identify and assess attacks through forensics.				
Course Contents	**Unit I** Topics in Data Structures: Various Trees, Linked List, Heap, Stack, Queues. Abstract Data Typesusing Python and C Language. **Unit II** Topics in Data Base Management Systems: Entity–Relationship model (E-R model) – E-RDiagrams, Functional Dependencies – Non-loss Decomposition, First, Second, Third Normal Forms, Dependency Preservation – Boyce/Codd Normal Form- Multi-Valued Dependencies and FourthNormal Form – Join Dependencies and Fifth Normal Form, Two Phase Commit, ACIDProperty, TwoPhase Locking –Intent Locking – Deadlock- Serializability, Magnetic Disks – RAID– Tertiarystorage – File Organization **Unit III** Topics in Algorithms: Algorithm Development, Complexity analysis, Sorting, Searching, BFS, DFS, Minimum Spanning Tree, Prim's and Kruskal';s algorithms, Greedy algorithms – Divide and conquer – Dynamic programming – backtracking– algorithm analysis **Unit IV** Topics in Operating System: Overview of operating systems, functionalities and characteristics of OS, concept of a process, operations on processes, process states, concurrent processes, process control block, process context, Job and processor scheduling, scheduling algorithms, Deadlock: prevention, detection, avoidance, banker';s algorithm, Memory organization and management, storage allocationAndroid OS, iOS, Linux OS file structure and security features **Unit V** Topics in Computer networks: OSI Model and each layer working, properties and related protocols insecurity areas.				

Course Outcomes	1. Identify and define key knowledge areas of cyber security. 2. Explain what to protect, why to protect, and create a plan to protect in the cyber world. 3. Describe cyber security in the real-world and apply their knowledge to scenarios to reflect technology's latest capabilities and trends 4. Interpret legal implications of security incidents and conduct investigations using industry best practices.
Text Books	1. Introduction to Algorithms by Thomas H. Cormen 2. The Practice of Programming by Kernighan♣
Reference Books	1. A. V. Aho, J. E. Hopcroft, and J. D. Ullman, "Data Structures and Algorithms", 2. PearsonEducation♣Ramez Elmasri, Shamkant B. Navathe, "Fundamentals of Database Systems"

Course Title	**Research Methodology for Engineers**				
Course Code	**EMT06102**				
Course Credits	**L**	**T**	**P**	**TC**	
	4	**1**	**-**	**5**	
Prerequisites	To learn and apply appropriate research methodology in a particular research area.				
Course Objectives	To identify and apply appropriate research methodology in order to plan, conduct and evaluate basic research.				
Course Contents	**UNIT I:** BASICS OF RESEARCH Basics of Research, Types and Methods of Research, Research problem, Hypothesis, Research plan, Research design, Significance of Research, Sampling techniques, Data collection, Quantitative and Qualitative Data, Tools for Data Collection; Research Problem, Hypothesis- Meaning & Characteristics, Research Design. **UNIT II:** REPORT AND MANUSCRIPT WRITING Interpretation and Report writing: Meaning of Interpretation, Significance of Report writing, Different steps in writing report, Layout of the Research Report, Types of Reports, Mechanics of writing a Research report; Preparation of Manuscript for Publication of Research Paper, Reference writing styles, Bibliography, Writing a Review of Paper, Writing Synopsis & Thesis. **UNIT III:** STATISTICAL ANALYSIS Statistical Analysis - Measures of Central Tendency, Measures of Dispersion, Measures of Association/Relationship - Regression and Correlation Analysis, Hypothesis testing, significance testing, Student's 't' test, ANOVA, Parametric and Non-parametric test; Introduction to Statistical Software: SPSS, Features for Statistical Data Analysis. **UNIT IV:** BASICS OF COMPUTER Introduction to MS Excel, Using Formulas and Functions, , Generating Charts/Graphs, Introduction to MS Word, Features and Functions, Writing Report in MS Word, Introduction to Open Office or Latex, Creating Presentation in MS Power Point, Use of Advanced Research Techniques; Basics of Internet, FTP, email, worldwide web (www), navigating the www, search engines. **UNIT V:** IPR Introduction to Intellectual Property; Types of Intellectual Property; Importance of IPR; Patents, Trademarks, Copyright and Related rights, Industrial Design; Traditional knowledge; Geographical indications; History of Indian Patent System and Law; Types of Patent; Patentable and Non-Patentable items.				
Course Outcomes	Enable scholars to distinguish between the scientific method and common sense knowledge while laying the foundation for research skills at higher levels.				

Text Books	1. Research Methodology: An Introduction by CR Kothari, New Age publication. 2. Research Methodology: Methods and Techniques by C. R. Kothari, New Age International Publishers, ISBN:81-224-1522-9.
Reference Books	1. Research Methodology for Business: A Skill Based Approach by Kumar, Shekaran (2009), New York, John Wiley Publishers. 2. Statistical Methods for Research Workers by Fisher R. A., Cosmo Publications, New Delhi ISBN:81-307-0128-6.

Course Title	Digital Forensics				
Course Code	EMT06103				
Course Credits	**L**	**T**	**P**	**TC**	
	3	**1**	**-**	**4**	
Prerequisites	Basic knowledge about Digital Forensic.				
Course Objectives	• To differentiate and understand the challenges of cyber fraud. • To understand modular cyber forensic concepts.				
Course Contents	**Unit I** File system: CHS, LBA, HPA, write blockers, Extracting & recovering partitions, MBR, DOSpartition table, Extended partition table, RAID; FAT file system: Architecture, File creation, Filedeletion; NTFS file system: Architecture, File creation, File deletion, Compression, encryptionandindexing; **Unit II** Extended file systems: EXT2, EXT3 and EXT4, Architecture, File creation, File deletionandJournaling; Apple File System (APFS); Other Disk structures; Windows and Linux boot process; Filesystem acquisition and recovery **Unit III** Windows Forensic Analysis: Window artifacts, Evidence volatility, System time, Logged on user(s), Open files, MRUs, Network information, Process information, Service information, WindowsRegistry, Start up tasks, Memory dumping; Document Forensics: PDF structure, PDF analysis, MSOffice Document structure and analysis, Macros, Windows thumbnails, Android Thumbnails **Unit IV** Mobile Forensics: SIM Card, Android architecture, Android File System, Android application, Android SDK,Android Debug Bridge, Memory & SIM acquisition; Virtual Machines, NetworkForensics; Cyber crime investigation: Pre investigation, SOP for Investigation; Case scenarios: social media crime, Online defacement crime, Email investigation; CDR Analysis **Unit V** Auditing: Internal Audit and IT Audit Function, IT Governance, Frameworks, Standards, andRegulations, Identifying information assets, Risk assessment, Risk management, TypesofAuditing, ISO 27001, PCIDSS				

Course Outcomes	After completion of the course study, students will be able to- 1. Use and differentiate between basic concepts of cyber forensic and digital forensic.
Text Books	1. Computer Evidence - Collection and Preservation.Brown, C.L.T. Course Technology Guide to Computer Forensics And Investigations Nelson, Bill ; Phillips, 2. Amelia; Enfinger, Frank; Steuat, Christopher Thomson Course Technology. ♣Cengage Learning.
Reference Books	1. Computer Forensics – Computer Crime Scene Investigation.Vacca, John R. Charles Bunting, Steve and William Wei. 2. EnCase Computer Forensics: The Official EnCE: ♣RiverMedia EnCaseCertifed Examiner Study Guide. Sybex, 2006.

Course Title	Cryptography & Network Security				
Course Code	EMT06104				
Course Credits	**L**	**T**	**P**	**TC**	
	3	**1**	**-**	**4**	
Prerequisites	Basic knowledge about cryptography & network security.				
Course Objectives	• To learn the Computer cryptography & network security concepts.				
Course Contents	**Unit I** Foundations – Protocol Building Blocks - Basic Protocols - Intermediate Protocols - AdvancedProtocols - Zero-Knowledge Proofs - Zero-Knowledge Proofs of Identity -Blind Signatures - Identity- Based Public-Key Cryptography - Oblivious Transfer - Oblivious Signatures - Esoteric Protocols **Unit II** Key Length - Key Management - Electronic Codebook Mode - Block Replay - Cipher Block ChainingMode - Stream Ciphers - Self-Synchronizing Stream Ciphers - Cipher-Feedback Mode - SynchronousStream Ciphers - Output-Feedback Mode - Counter Mode - Choosing a Cipher Mode - Interleaving- Block Ciphers versus Stream Ciphers - Choosing an Algorithm - PublicKey CryptographyversusSymmetric Cryptography - Encrypting Communications Channels - Encrypting Data for Storage- Hardware Encryption versus Software Encryption - Compression, Encoding, and Encryption- Detecting Encryption – Hiding and Destroying Information **Unit III** Live malware analysis, dead malware analysis, analyzing traces of malware, systemcalls, api calls, registries, network activities. Anti-dynamic analysis techniques, VM detection techniques, Evasiontechniques, , Malware Sandbox, Monitoring with Process Monitor, Packet Sniffing with Wireshark, Kernel vs. User-Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching **Unit IV** Downloaders and Launchers, Backdoors, Credential Stealers, Persistence Mechanisms, Handles, Mutexes, Privilege Escalation, Covert malware launching- Launchers, Process Injection, ProcessReplacement, Hook Injection, Detours, APC injection, YARA rule based detection **Unit V** Android Malware Analysis: Android architecture, App development cycle, APKTool, APKInspector, Dex2Jar, JD-GUI, Static and Dynamic Analysis, Case studies.				

Course Outcomes	After completion of the course study, students will be able to- 1. To familiar with security of networks. 2. To know about cyber threat.
Text Books	1. "Practical Malware Analysis" by Michael Sikorski and Andrew Honig 2. "The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System" Second Edition by Reverend Bill Blunden
Reference Books	1. "Rootkits: Subverting the Windows Kernel" by Jamie Butler and Greg Hoglund 2. "Practical Reverse Engineering" by Dang, Gazet, Bachaalany

Course Title	Operating System & Security				
Course Code	EMT06105				
Course Credits	**L**	**T**	**P**	**TC**	
	3	1	-	4	
Prerequisites	To understand about the basic concepts relating to operating systems and its security parameters.				
Course Objectives	Introduce students to the field of threads and vulnerabilities in OS and how to provide security in different OS.				
Course Contents	**UNIT – I** Introduction: Secure Os, Security Goals, Trust Model, Threat Model, Access Control. Fundamentals: Protection system, Lampson's Access Matrix, Mandatory protection system. **UNIT – II** Multics: Fundamentals, multics protection system models, multics reference model, multics security, multics vulnerability analysis. **UNIT – III** Security in ordinary operating system: UNIX security, windows security Verifiable security goals: Information flow, information flow secrecy, models, information flow integrity model, the challenges of trusted, process, covert channels. **UNIT – IV** Security Kernels: The Security Kernels, secure communications, processor Scomp, Gemini secure OS, Securing commercial OS, Retrofitting security into a commercial OS, History Retrofitting commercial OS, Commercial era, microkernel era, UNIX eraIX, domainand type enforcement. **UNIT – V** Case study: Solaris Extensions Trusted extensions, access control, Solaris compatibility, trusted extensions, mediations process rights management, role based access control, trusted extensions, networking trusted extensions, multilevel services, trusted extensions administration. Case study: Building secure OS for Linux: Linux security modules, security enhanced Linux.				
Course Outcomes	• Understands the different services provided by Operating System at different level. • They learn real life applications of Operating System in every field.				

Text Books	Trent Jaeger, Operating system security, Morgan & Claypool Publishers, 2008
	Operating System Design & Implementation by Tanenbaum, A.S., PHI.
	Operating system concepts Galvin by Silberscatz, John Weiley& Sons
Reference Books	1. Paxson, Bro: A System for Detecting Network Intruders in Real-Time. Proc. 7th USENIX Security Symposium, San Antonio, TX, January 1998
	2. Operating System Concept & Design, Milenkovic M, McGraw Hill.
	3. Operation System, Stalling William, Maxwell MCMillan International Editions

Course Title	Digital Forensics Lab				
Course Code	EMT06106				
Course Credits	**L**	**T**	**P**	**TC**	
	-	**-**	**4**	**2**	
Prerequisites	Basic knowledge about Cyber forensic.				
Course Objectives	• Explain various computer forensic techniques/phases. • Demonstrate the knowledge of forensic examination related to Microsoft Windows and Linux artifacts.				
Course Contents	**List of Experiments:** 1. Install, Configure and study a Intrusion detection system (IDS). 2. Implementation of different message digest/hashing techniques such as MD5, SHA 3. Implementation of email security using PGP(create yourself a 1024 bit PGP key. Use your name and email address for your key label. Use PGP to verify the signature on this assignment.) 4. Demonstrate the use of honey pots for the implementation of IDS 5. Use the OpenSSL commands to create a CA root certificate, a server certificate, and two or more client certificates 6. Write a client-server package for file transfer. The server will listen on some network port. When it accepts a connection, it immediately starts up SSL. The server verifies that the client's certificate came from the proper CA; that's the authentication used.				
Course Outcomes	• Understand security issues related to networking vulnerabilities, firewalls, intrusion detection systems. • Identify infrastructure components including devices, systems software, management and security.				
Text Books	Bill Nelson Amelia Phillips Christopher Steuart, "Guide to Computer Forensics and Investigations", 4th Edition, Course Technology, Cengage Learning, ISBN-13: 978-1-435-49883.				
Reference Books	Brian Carrier, "File System Forensic Analysis", Pearson education, 1st Edition, ISBN13:978-0321268174.				

SHRI RAWATPURA SARKAR UNIVERSITY, RAIPUR, CHHATTISGARH

FACULTY OF COMPUTER SCIENCE & ENGINEERING

M.Tech(Cyber Forensics) First Semester

Course Title	Operating System & Security Lab				
Course Code	EMT06107				
Course Credits	**L**	**T**	**P**	**TC**	
	-	-	4	2	
Prerequisites	Basic knowledge of operating system & security.				
Course Objectives	Implement different distributed cocepts like RPC, RMI.				
Course Contents	**List of Experiments:** 1. A program to execute RPC/ gRPC concept on different hosts 2. A program to execute RMI concept on different hosts 3. Message Passing Interface study and cluster setup on LAN 4. Case Study on Intel VT enable architecture 5. Hadoop-MapReduce cluster setup 6. Mini Project on operating system design				
Course Outcomes	After completion of this course the students will be able to • Learn basics of MPI and its implementation • Demonstrate the need of virtualization.				
Text Books	Coulouris George, Dollimore Jean, Kindberg Tim, Blair Gordon, Distributed Systems: Concepts and Design, Fifth Edition, Pearson, 2017.				
Reference Books	Coulouris George, Dollimore Jean, Kindberg Tim, Blair Gordon, Distributed Systems: Concepts and Design, Fifth Edition, Pearson, 2017.				