BMS INSTITUTE OF TECHNOLOGY AND MANAGEMENT

(Autonomous Institution Affiliated to VTU, Belagavi)

Scheme of Teaching and Examinations – 2024 Scheme

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

(Effective from the academic year 2024 - 25 onwards)

I Semester M Tech Cyber Security

Sl. No.	Course Category	Course Code	Course Name	Teaching Department	Credits Distribution				Examination				Contact Hours/week
					L	T	P	Total	CIE Marks	SEE Marks	Total Marks	SEE Duration (H)	
1	PCC	24MCR11	Foundation of Mathematics for Cyber Security	Math's	3	0	0	3	50	50	100	3	3
2	IPCC	24MCR12	Advanced Data Structures and Algorithms	ISE	3	0	2	4	50	50	100	3	4
3	PCC	24MCR13	Cryptography and Network Security	ISE	3	2	0	4	50	50	100	3	4
4	IPCC	24MCR14	Cyber Security Essentials	ISE	3	0	2	4	50	50	100	3	4
5	PCC	24MCR15	Ethics and Privacy in Social Networks	ISE	3	0	0	3	50	50	100	3	3
6	PCCL	24MCRL16	LINUX Essentials for Cyber Security Lab	ISE	0	2	2	2	50	50	100	3	4
7	NCMC	24AUD17	Research Methodology and IPR (MOOCs – Online)	ISE	Classes and evaluation procedures are as per the policy of the online course providers						PP	---	---
TOTAL					**15**	**2**	**6**	**20**	**300**	**300**	**600**		

- **Non Credit Mandatory Courses Suggested by BOS (ONLINE courses):** Audit Courses: These are prerequisite courses suggested by the Interim Board of Studies – M.Tech Cyber Security. All activities should enhance student's abilities to employment and/or self-employment opportunities, management skills, Statistical analysis, fiscal expertise, etc. Students and the course instructor/s are to be involved either individually or in groups to interact together to enhance the learning and application skills of the study they have undertaken. The students with the help of the course teacher can take up relevant technical –activities that will enhance their skills. The prepared report shall be evaluated for CIE marks.
  Research Methodology and IPR (MRMI19) None Credit Mandatory Course (NCMC) if students have not studied this course in their undergraduate program then he /she has to take this course at **http://online.vtu.ac.in** and to qualify for this course is compulsory before Semester End Examination.

SEMESTER – I

M.TECH Cyber Security

Choice Based Credit System (CBCS)

SEMESTER - I

Foundation of Mathematics for Cyber Security (3:0:0) 3

(Effective from the academic year 2024 - 25)

Course Code	24MCR11	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:0:0	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Course Objectives:

This course will enable students to:

1. Provide the mathematical background required for cyber security.
2. Familiarize the basic building blocks of important cyber security applications
3. Discuss the theoretical aspects of number theory
4. Study the security model and analyze them before being used in many commercial, industrial as well as web applications.

Module – 1

Preamble: Significance and Scope of the course, Importance of the course in the societal, political, and economic growth of the nation, Impact of the course on societal and ethical issues, and career perspective.

Algebraic Structures: Groups – Cyclic groups, Cosets, Modulo groups - Primitive roots - Discrete logarithms. Rings – Sub rings, ideals, and quotient rings, Integral domains. Fields – Finite fields – GF (pn), GF(2n) - Classification - Structure of finite fields. Lattice, Lattice as Algebraic system, sub lattices, some special lattices. (8 hours)

(RBT Levels: L1, L2 and L3)

Module – 2

Introduction: Understanding of Vector spaces, graph theory, Statistical models & their applications in Engineering, Economics and Statistics.

Linear Algebra-I: Vector Spaces: Vector spaces; subspaces Linearly independent and dependent vectors, Basis and dimension, coordinate vectors-Illustrative examples. Linear transformations, Representation of transformations by matrices (8 hours)

(RBT Levels: L1, L2 and L3)

Module – 3

Linear Algebra-II: Computation of Eigen values and Eigen vectors of real symmetric matrices-Jacobi and Given's method. Orthogonal vectors and orthogonal basis. Gram-Schmidt orthogonalization process. QR decomposition, singular value decomposition**.** (8 hours)

(RBT Levels: L1, L2 and L3)

Module – 4

Number Theory and Algebraic Geometry: Elliptic curves, basic facts, elliptic curve cryptosystems, elliptic curve primality test – elliptic curve factorization. (8 hours)

(RBT Levels: L1, L2 and L3)

Module – 5

Coding Theory: Introduction - Basic concepts: codes, minimum distance, the equivalence of codes, Linear codes - Linear codes - Generator matrices and parity-check matrices - Syndrome decoding – Hamming codes – Hadamard codes - Goppa codes**.** (8 hours)

(RBT Levels: L1, L2 and L3)

Course outcomes:

The students will be able to

CO1: Understand basic concepts of various algebraic structures and theorems which are used for designing security algorithms.

CO2: Linearly transform the system from one dimension to another and represent the pertinent linear transformation in matrix form.

CO3: Apply techniques of constrained optimization and singular value decomposition to problems arising in power/control system analysis, signals, and systems.

CO4: Identify the approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.

CO5: Understand coding theory which will be useful for data compression and maintaining confidentiality.

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks:

1. David C.Lay, Steven R.Lay and J.J.McDonald, “Linear Algebra and its Applications”, 5th Edition, Pearson Education Ltd., 2015.
2. Neal Coblitz, “A Course in Number Theory and Cryptography”, Springer Verlag, Second edition.

References:

1. C.L. Liu, ‘Elements of Discrete Mathematics’, McGraw Hill, 2008.
2. Douglas Stinson, ‘Cryptography – Theory and Practice’, CRC Press, 2006.
3. Joseph A. Gallian, ‘’Contemporary Abstract Algebra’, Narosa, 1998.
4. D. S. Malik, J. Mordeson, M. K. Sen, “Fundamentals of Abstract Algebra, Tata McGraw Hill.
5. P. K. Saikia, “Linear Algebra”, Pearson Education.
6. Niven, H.S. Zuckerman and H. L. Montgomery, “An Introduction to the Theory of Numbers”, John Wiley and Sons,.
7. Leigh Metcalf, William Casey, “Cybersecurity and Applied Mathematics”, Syngress Publisher.

M.Tech CYBER SECURITY

Choice Based Credit System (CBCS)

SEMESTER – I

Advanced Data Structures and Algorithms (3:0:2) 4

(Effective from the academic year 2024 - 25)

Course Code	24MCR12	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:0:2	SEE Marks	50
Total Number of Contact Hours	50	Exam Hours	3

Course Objectives:

This course will enable students to:

1. Explain fundamentals of advanced data structures and their applications essential for programming/problem Solving.
2. Utilize an appropriate data structure like Stack, Queues, Lists, Trees and Graphs to solve a given
3. Demonstrate sorting and searching algorithms.

Module-1: Introduction

The Role of Algorithms in Computing, Overview and Importance of Data Structures in Cybersecurity, Relationship between Data Structures and Security, Analyzing algorithms, designing algorithms, Asymptotic notation, Standard notations and common functions, Elementary Data Structures, Stacks and queues, Linked lists, Implementing pointers and objects.

T1: Chapter 1-3, 10 R1:Chapter 1.1 ,1.2 **(8Hours)**

Module-2: Trees

Binary Search Trees, What is a binary search tree, Querying a binary search tree, Insertion and deletion, Randomly built binary search trees, Red-Black Trees, Properties of red-black trees, Rotations, Insertion, Deletion, Balanced Trees, Definition of B-trees, Basic operations on B-trees, Deleting a key from a B-tree-AVL Trees-single rotation and double rotation.

Chapters 12,13, 18 R2: Chap 4.4 **(8 Hours)**

Module-3 Hashing and Heaps

Hash Tables, Direct-address tables, Hash functions, Open addressing, Perfect hashing. Heaps, Maintaining the heap property, building a heap, the heapsort algorithm, Priority queues, Merkle Tree-creation -Merkle Tree for Data Verification-Role of Merkle Trees in Blockchains and Bitcoin, Trie -operations on Trie

Chapters 11, 6,19, R4, R7 **(8 Hours)**

Module-4 Graph Algorithms

Representations of graphs, Breadth-first search, Depth-first search, Minimum Spanning Trees algorithms,, The Bellman-Ford algorithm, All Pairs Shortest Paths, Floyd-Warshall algorithm, Johnson's algorithm for sparse graphs, Maximum Flow, Flow networks, The Ford-Fulkerson method.Attack Graphs-use Attack graphs- How Enterprises Use Attack Graphs to Protect Critical Assets

Chapters, 22.1 – 22.3, 23.1 – 23.2, 24.1 – 24.3, 25, 26.1 – 26.2 , R5 **(8 Hours)**

Module-5 Number-Theoretic Algorithms and case studies

Number-Theoretic Algorithms, Elementary number-theoretic notions, Greatest common divisor, Modular arithmetic, Solving modular linear equations, The Chinese remainder theorem, Powers of an element,

The RSA public-key cryptosystem,
Case Studies and Practical Applications - Binary Search Trees for Encryption Key Management using Binary Trees, Network topology using Graphs, Trie data structure for IP Lookup.

Chapters 31.1 – 31.7, R6, R7, R8 **(8 Hours)**

Course Outcomes:

The students will be able to:

1. **CO1:** Illustrate different types of linear data structures, its operations and algorithms to solve a given problem.
2. **CO2:** Illustrate different types of nonlinear data structures, its operations and algorithms to solve a given problem**.**
3. **CO3:** Examine any given problem, recommend and implement solutions using suitable data structures.
4. **CO4:** Design and implement applications using suitable data structures.

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for the test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks:

1.Thomas H. Cormen, Charles, E. Leiserson, Ronal L. Rivest, Clifford Stein, Introduction to Algorithms, The MIT PRess, 4th Edition, 2022.

References:

1. S.R.Jena, Dr.Dileep kumar Cyber security using Data structures,Notion Press, First Edition , 2024.
2. Mark Allen Weiss, Data structures and Algorithm Analysis, Pearson, 4th Edition, 2014
3. Gilberg & Forouzan, Data Structures: A Pseudo code approach with C, Cengage Learning, 2nd edition, 2014.
4. https://www.techopedia.com/definition/32919/merkle-tree.
5. https://xmcyber.com/glossary/what-are-attack-graphs/
6. https://developer.okta.com/blog/2019/07/29/hashing-techniques-for-password-storage
7. https://www.ijraset.com/best-journal/study-of-various-network-topologies-using-graph-theory
8. https://www.geeksforgeeks.org/trie-insert-and-search/

List of Experiments - Part A

1) Design and develop a menu driven Program for implementing multiple stacks using arrays. Include the conditions to check for stack overflow, stack underflow and stack empty conditions in the program.
2) Design and develop a menu driven Program to implement insert, delete and traverse operations in a red-black tree. Ensure that the properties of the red-black tree are not violated after insert and delete operation.
3) Design and Develop a program to implement AVL Trees i) single Rotation ii) Double Rotation
4) Implement a function that takes a password and a salt as input and returns the hashed password

using a secure hash function . Ensure that you use proper hashing techniques to enhance password security.

5) Implement IP Address Lookup and Routing using Trie Data structure.

1. 6)Design and Develop a program to find the shortest path between all pairs of vertices in an edge weighted directed graph using johnson's algorithm

2. AAT: Literature Review on Advanced Data structures

M.TECH CYBER SECURITY

Choice Based Credit System (CBCS)

SEMESTER – I

Cryptography and Network Security (4:0:0) 4

(Effective from the academic year 2024-25)

Course Code	24MCR13	CIE Marks	50
Teaching Hours/Week (L: T:P)	4:0:0	SEE Marks	50
Total Number of Contact Hours	50	Exam Hours	3

Course Objectives:

This course will enable students to:

1. Explain standard algorithms used to provide confidentiality, integrity and authenticity.
2. Distinguish key distribution and management schemes.
3. Apply encryption techniques to secure data in transit across data networks
4. Implement security applications in the field of Information technology.

Preamble: Embarking on the study of "Cryptography and Network Security" delves into the intricate world of securing digital communication and information. This field explores advanced cryptographic algorithms and protocols, essential for safeguarding sensitive data in an increasingly interconnected world. Its significance lies in thwarting cyber threats and ensuring privacy and integrity in digital transactions and communications. As cybersecurity concerns escalate, expertise in advanced cryptography becomes pivotal for protecting critical infrastructure and preserving digital trust. Pursuing this specialization promises a deep dive into the forefront of cryptographic techniques, offering opportunities to innovate and defend against evolving cyber threats.

Module – 1

Computer and Network Security: Computer Security Concepts, The OSI Security Architecture, Security Attacks, Security Services, Security Mechanisms, Fundamental Security Design Principles, Attack Surfaces and Attack Trees, A Model for Network Security, and Standards.**Symmetric Ciphers -Classical encryption techniques** : Symmetric Cipher Model , Substitution Techniques , Transposition Techniques, Rotor Machines, Stenography.

(Chapter 1 & 3) (8 Hours)

Module – 2

Block Ciphers and the Data Encryption Standard: Traditional Block Cipher Structure, The Data Encryption Standard, A DES Example, The Strength of DES, Block cipher design principles and modes of operation. **Advanced Encryption Standard**: Finite Field Arithmetic, AES Structure, AES Transformation Functions, AES Key Expansion, An AES Example and AES Implementation. **Asymmetric Ciphers: Public-Key Cryptography and RSA:** Principles of Public-Key Cryptosystems, The RSA Algorithm and Diffie-Hellman Key Exchange, Elliptic Curve Arithmetic, Elliptic Curve Cryptography.

(Topics from Chapter 4, 6, 9 & 10.1 - 10.4) (8 Hours)

Module – 3

Cryptographic Data Integrity Algorithms- Cryptographic Hash Functions : Applications of Cryptographic Hash Functions Two Simple Hash Functions, Requirements and Security, Hash Functions Based on Cipher Block Chaining, Secure Hash Algorithm (SHA) , & SHA-3. **Message Authentication Codes**: Message Authentication Requirements, Message Authentication Functions, Requirements for Message Authentication Codes, Security of MACs, MACs Based on Hash Functions: HMAC,Digital Signatures.

(Topics from Chapter 11, 12, & 13.1) (8 Hours)

Module – 4

Mutual Trust: Key Management and Distribution: Symmetric Key Distribution Using Symmetric Encryption, Symmetric Key Distribution Using Asymmetric Encryption, Distribution of Public Keys, X.509 Certificates, public-Key Infrastructure. **User Authentication:** Remote User-Authentication Principles, Remote User-authentication Using Symmetric Encryption, Kerberos.

Network Access Control and Cloud Security : Network Access Control, Extensible Authentication Protocol, IEEE 802.1X Port-Based Network Access Control, Cloud Computing , Cloud Security Risks and Countermeasures , Data Protection in the Cloud, Cloud Security as a Service, Addressing Cloud Computing Security Concerns.

(Topics from Chapter 14, 15.1-15.3, & 16) (8 Hours)

Module – 5

Transport Layer Security: HTTPS, Secure Shell (SSH), Wireless Security, Mobile Device Security, IEEE 802.11 Wireless LAN Overview, IEEE 802.11i Wireless LAN Security. **Electronic Mail Security**: internet Mail Architecture, Email Formats, Email Threats and Comprehensive Email Security , S/MIME, Pretty Good Privacy, DNSSEC, DNS-Based Authentication of Named Entities.

IP Security Overview: IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange, Cryptographic Suite.

Recap/Summary of the course.

(Topics from Chapter 17, 18, & 19) (8 Hours)

Course Outcomes: The students will be able to:

CO1: Apply the OSI security architecture, number theory and cipher techniques for the given problem.

CO2: Compare the performance of various cryptographic data integrity techniques for the identified problem.

CO3: Analyze the vulnerabilities in any computing system and design a cryptographic solution for the given problem/ case study

CO4: Examine the working of the techniques used for Mutual trust and security on internet and compare their performance.

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks:

1. William Stallings, Cryptography and Network Security Principles and Practice, 7 th edition, Pearson, 2019.

References:

1. Damien Vergnaud and Michel Abdalla, Applied Cryptography and Network Security, 7th International Conference, ACNS 2009, Paris-Rocquencourt, France, June 2-5, 2009, Proceedings.
2. B. Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, 2nd Edition, John Wiley & Sons, 1995.
3. Mihir Bellare and Phillip Rogaway, “Introduction to Modern Cryptography”, 2005.
4. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, “Handbook of Applied Cryptography” CRC Press.
5. Neal Koblitz, A Course in Number Theory and Cryptology, Springer 1987.

Web Resources:

1. “Cryptography" by Stanford University: Stanford University. “Cryptography.” Coursera, www.coursera.org/learn/crypto.
2. "Applied Cryptography" by the University of Colorado System: University of Colorado System. “Applied Cryptography.” Coursera, www.coursera.org/learn/applied-cryptography.
3. "Introduction to Cryptography" by the University of London: University of London. “Introduction to Cryptography.” Coursera, www.coursera.org/learn/crypto-introduction.

M.Tech. CYBER SECURITY
Choice Based Credit System (CBCS)
SEMESTER – I

Cyber Security Essentials(3:0:2) 4
(Effective from the academic year 2024-25)

Course Code	24MCR14	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:0:2	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Course Objectives:

This course will enable students to:

1. To summarize the concepts of cyber security, forensics and its applications in different context.
2. To investigate incident and areas affected due to cybercrime.
3. To illustrate tools used in cyber security,forensic
4. To infer legal perspectives in cyber security
5. To apply the policies, security standards, and IPR issues on a cybercrime incident.

Preamble:

The course aims to provide an overview of cyber law, security, tools, and approaches to secure resources and manage intellectual property for enhancing the competitiveness for organizations. Upon completion of this course, students should be able to accomplish the course outcomes defined. The cyber security and forensics have direct impact on the security systems, society, financial models and affecting the GDP.

Module – 1

Legacy cybersecurity systems, Transformations in cybersecurity, Advancements in security technology to security 2.0, How ML and Al will play a larger role in cybersecurity, Learning cybersecurity Technologies Mobile security ,advanced data security, cloud security ,Modern day regulations, Incidence response and forensic ,Enterprise security at scale ,penetration testing ,DevSecOps, LoT Security, User behavior analytics(UBA),Endpoint detection and response (EDR).

(8 Hours)

Module – 2

Attacker Mindset ,The category of hackers, The traits of hackers, Social Characteristics of hackers, How hackers think(Motivators),What can be learned from the psychology of hackers ?Understanding Reactive ,Proactive and Operational Security Proactive cyber defense ,Reactive cybersecurity ,Overview of operational security , The significance of the three security pillars ,Security operations and continuous monitoring, Digital forensics and real-time incident response with SIEM.

(8 Hours)

Module – 3

Understanding Access-Control and Monitoring Systems: A Quick Primer on Infrastructure Security, Access Control, Authentication Systems, Remote-Access Monitoring, Understanding Intrusion Detection and Reporting Systems: Intrusion-Detection.

(Chapter 2 & 4 from Book2) (8 Hours)

Module – 4

Understanding Reactive, Proactive, and Operational Security: Proactive cyber defense, Implementing proactive security, Reactive cybersecurity, Overview of operational security, Security operations and continuous monitoring, Digital forensics and real-time incident response with SIEM

. (Chapters 6 from Book1) (8 Hours)

Module – 5

Web Application Security: This Site Is Secure, The Core Security Problem: Users Can Submit Arbitrary Input, Key Problem Factors, The New Security Perimeter, Core Defense Mechanisms: Handling User Access, Handling User Input, Handling Attackers.

(Chapters 1 & 2 from Book3) (8 Hours)

Course Outcomes:

The students will be able to:

CO1: Identify and analyse the cyber security risks due to different cyber-crimes and examine in the legal perspective

CO2: Illustrate the use of Cyber security and of cyber-forensics tools in investigating the given cybercrime.

CO3: Analyse legal issues and socio-economic impact due to cybercrime and forensics investigation approach

CO4: Examine relevant network defense / web application tool to solve given cyber security problem/ case study

CO5: Design the security policy for an organization in line with IT ACT 2000 and based on ISO standard,

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks:

1. Cybersecurity: The Beginner's Guide by Dr. Erdal Ozkaya 1st Edition 2019
2. Cybersecurity Essentials by Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short 2018.
3. The Web Application Hacker’s Handbook Finding and Exploiting Security Flaws by Dafydd Stuttard Marcus Pinto 2nd Edition 2011

References:

1. Sunit Belapure, Nina Godbole, Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives Wiley India Pvt Ltd 2013
2. Surya Prakash Tripathi, Ritendra Goyal, Praveen Kumar Shukla, Introduction to information security and cyber laws, Dreamtech Press 2015
3. Thomas J. Mowbray, Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions John Wiley & Sons 2013
4. James Graham, Ryan Olson, Rick Howard , Cyber Security Essentials CRC Press 2010

Experiments and Tools:

1. Configuring Firewalls and VPNs : Hands-on with firewall configurations and setting up secure VPN connections.
   https://www.pfsense.org/getting-started/
   https://openvpn.net/community-resources/how-to/

2. Penetration Testing of Web Applications: Using tools like BURFSuit and OWASP ZAP to find vulnerabilities in a web application.
   https://portswigger.net/burp
   https://owasp.org/

3. Cryptographic Algorithms: Implementing symmetric and asymmetric encryption algorithms in a coding environment (e.g. Java or C++ or Python)
   https://www.pycryptodome.org/
https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html

4. Cloud Security Hands-on : Securing a cloud based application using IAM, Encryption, and security groups.
   https://aws.amazon.com/iam/
   https://cloud.google.com/security/products/iam
   https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/security-top-10

5. Incident Response Simulation: Conducting a mock incident response exercise from detection to remediation.
   https://docs.splunk.com/Documentation/Splunk
   https://www.elastic.co/guide/en/siem/guide/current/index.html

M. Tech CYBER SECURITY

Choice Based Credit System (CBCS)

SEMESTER – I

Ethics and Privacy in Social Networks (3:0:0)3

(Effective from the academic year 2024-25)

Course Code	24MCR15	CIE Marks	50
Teaching Hours/Week (L:T:P)	3:2:0	SEE Marks	50
Total Number of Contact Hours	40	Exam Hours	3

Course Objectives:

This course will enable students to:

1. Identify and describe common ethical concepts and theories.
2. Analyze ethical dilemmas and articulate a clear, descriptive account prior to forming a normative course of action.
3. Demonstrate one or more processes of philosophical analysis.
4. Identify common ethical issues facing professionals in the field of information technology.
5. Apply ethical concepts and an analytical process to common dilemmas found in the information technology field.

Module – 1

Ethics and the Professions - Introduction, Codes of Ethics, Evolution of Professions, Origins of Professions, Requirements of a Professional, Pillars of Professionalism, The Making of an Ethical Professional: Education, and Licensing , Formal Education, Licensing Authorities, Professional Codes of Conduct, Professional Decision Making and Ethics, Professional Dilemma in Decision Making, Guilt and Making Ethical Decisions, Professionalism and Ethical Responsibilities, Whistle-Blowing, Harassment and Discrimination, Ethical and Moral Implications (8 Hours)

Module – 2

New Frontiers for Computer Ethics: Cyberspace - Introduction, Cyberspace and the Concepts of Telepresence and Immersion, Securing Cyberspace, Detecting Attacks in Cyberspace, Cyberspace Systems Survivability, Personal Identity, Regulating and Censoring Cyberspace, The Social Value of Cyberspace, Privacy in Cyberspace, Privacy Protection, Global Cybernetics, Cyberspace Lingua Franca, Global Cyber Culture. (8 Hours)

Module – 3

Ethical, Privacy, and Security Issues in the Online -Social Network Ecosystems, Introduction, Introduction to Computer Networks, Computer Network Models, Computer Network Types, Social Networks, Online Social Networks(OSNs), Types of Online Social Networks , Online Social Networking Services, The Growth of Online Social Networks , Ethical and Privacy Issues in Online Social Networks, Privacy Issues in OSNs, Strengthening Privacy in OSNs, Ethical Issues in Online Social Networks, Security and Crimes in Online Social Networks, Beware of Ways to Perpetuate Crimes in Online, Social Networks, Defense Against Crimes in Online Social Networks , Proven Security Protocols and Best Practices in Online, Social Networks, Authentication, Access Control, Legislation, Self-Regulation Detection, Recovery. (8 Hours)

Module – 4

Phishing in OSM & Identifying fraudulent entities in online social networks. Profile Linking on Online Social Media, Anonymous Networks, Gephi Network Visualization tool. (8 Hours)

Module – 5

Case Study: Beware of What You Share Inferring Home Location in Social Networks, On the dynamics of username change behavior on Twitter, Boston Marathon Analyzing Fake Content on Twitter. Location-based Privacy: Privacy in Location Based Social Networks, Visualization – Highcharts.
Recap/Summary of the course. (8 Hours)

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

CO1: Identify common ethical issues faced by professionals in the field of information technology.
CO2: Apply ethical and privacy concepts to resolve issues in the information technology field.
CO3: Analyze dilemmas and articulate a clear, descriptive account prior to forming a normative course of action.

Question paper pattern:

- **SEE** will be conducted for 100 marks.
- Each full question is for 20 marks. (Answer five full questions out of 10 questions with intra modular choice). In every question, there will be a maximum of three sub-questions.
- **CIE** will be announced prior to the commencement of the course.
- 25 marks for test. Average of three tests will be taken.
- 25 marks for Flexible Assessment Method.

Textbooks

1. Joseph Migga Kizza, Ethical and Social Issues in the Information Age, Fifth Edition, Springer London, 2013.

References:

1. Quinn, M. J. (2012). Ethics for the information age. Upper Saddle River, NJ: Addison-Wesley. 5th Ed. ISBN 978-0-13-285553-2
2. Adelson, H., Ledeen, K., & Lewis, H. (2008). Blown to bits: Your life, liberty, and happiness after the digital explosion. (1st ed.). Addison-Wesley. ISBN 978-0-13-285553-2. Download PDF Format through Creative Commons Licensing: http://www.bitsbook.com/excerpts/ .
3. https://onlinecourses.nptel.ac.in/noc23_cs13/preview

M.TECH CYBER SECURITY

Choice Based Credit System (CBCS)

SEMESTER – I

LINUX ESSENTIALS FOR CYBER SECURITY Lab (0:0:2) 1

(Effective from the academic year 2024-25)

Course Code	24MCRL16	CIE Marks	50
Teaching Hours/Week (L: T:P)	0:0:2	SEE Marks	50
Total Number of Contact Hours	26	Exam Hours	3

Course Objectives: This course will enable students to:

1. Understand the linux Operating System and basic commands
2. Gain proficiency in essential Linux commands for file, user,group management
3. Apply system administration tools.
4. Explore cyber security tools on OSINT framework.

List of Experiments

PART A

1. Installation of KALI linux/ubuntu. Execute BASIC COMMANDS on it. The 'cat' command (Creating Files, Displaying Files, Concatenating Files), Managing Files (Copying Files, Renaming / Moving of Files and Directories Removing Files and Directories), IO Redirection, Filters : wc, sort, head, tail etc.

2. MANAGING FILE PERMISSIONS - Perform following operations on files
   a. Display the file permissions, owner and group to which the file belongs
   b. Change the user ownership/group ownership
   c. change the permissions using octal notation/symbolic notation
   d. Change the default mask value
   e. Make/remove the files immutable attributes to a file

3. MANAGING USER ACCOUNTS - Create a user account named sue with the following restrictions:
   a. The account should have a strong, randomly generated password (consider using https://passwordsgenerator.net or a similar site to create the password).
   b. The user should be forced to change her password every 60 days.
   c. The user should not be allowed to change her password for 2 days after it has been set.
   d. The password warning field should be set to 10.
   e. The password inactivity period should be set to 60.
   f. The account should be set to expire on January 1, 2025.
   g. This user (and all others) should have a minimum password length of 12 characters.

4. Create five user accounts, with a different password for each account. Make some of the passwords very simple, such as simple words, and some of the passwords more complex. Then run the johnny password attack tool (in Kali Linux) on these new accounts and see which passwords were compromised by the tool.

5. MANAGING GROUP ADMINISTRATORS - Create a new group named eng and add the student user to this group. Make the student user a group administrator. To test this, add the bin user to the eng group while logged in as the student user and then verify this new group membership.

6. ENABLING ACCESS CONTROL LISTS
   a. Set an access control list (ACL) for the games group that allows read and write permissions for

that group on the hosts file.

b. Change the ACL mask value to read-only.
c. Verify the default ACLs by viewing the ACLs.

PART B

Investigating cyber security tools using OSINT Framework/Kali Linux (tools other than covered in Part-A). Open-Source Intelligence (OSINT) plays a crucial role in identifying, monitoring, and mitigating cyber security threats. In this case study, you will use OSINT framework/Kali Linux to address a cybersecurity challenge of your chosen area. You are expected to define your own problem statement, investigate, and provide a solution using available tools and techniques. As AAT students can do mini project by using explored tools.

Course Outcomes: The students will be able to:

CO1. Acquire knowledge about Operating System installation
CO2. Apply Unix/Linux commands to manage files
CO3. Analyze user account policies by creating users with specific restrictions
CO4. Design and implement Access Control Lists (ACLs) for specific groups to manage file access permissions effectively
CO5. Investigate cybersecurity threats using OSINT tools / KALI linux

Text Book References:

1. Linux Essentials for Cyber Security, William Rothwell, Denise Kinsey, Pearson IT Certification; 1st edition (July 20, 2018), ISBN : 978-0-7897-5935-1
2. Trent Jaeger, Operating Systems Security, Morgan & Claypool Publisher, 2008.
3. William Stalling, Operating System: Internals and Design Principles, Prentic Hall, 7th Edition, 2012.

For every lab scenario based questions should be designed and executed. As an example for Lab01 programs designed are as follows.

Scenario Details Q1 :

Question1 :

(1) Create Lab01 directory
(2) Create BOOKS directory under Lab01 directory.
(3) Create GK, TECHNICAL and SELFHELP directories under BOOKS directory.
(4) Change directory to GK directory using relative path.
(5) From current directory create RHONDA directory under SELFHELP directory using absolute path.
(6) Change directory to RHONDA directory using relative path.

Question2 :

(1) Create a file named TheSecret with following contents
Everything that's coming in your life you are attracting into your life.
And it's attracted to you by virtue of images you are holding in your mind.
It's what you are thinking.
Whatever is going on in your mind you are attracting to you.
(2) Display contents of the file TheSecret
(3) Find the number of lines in the file TheSecret
(4) Display sorted contents of file TheSecret in reverse order
(5) Extract the last line from the file TheSecret and store the extracted line in file named TheSecret_ABSTRACT
(6) Display the count of number of words in the file TheSecret_ABSTRACT

Scenario Details Q2 :

You are working as a junior Linux administrator and are required to set up a web development environment for your team. The environment needs to have the following:

1. A directory structure for storing HTML files, CSS files, and JavaScript files.
2. Some basic text files to store configuration details, like project name, version, and developers' contact information.
3. Perform tasks like copying, renaming, moving, removing files and directories, and ensuring the correct permissions are set.
4. You will also create some sample data files and practice using Linux filters (wc, sort, head, tail).