Principles of Cyber Security

Code: R19MCY1151

Course Outcomes		Knowledge Level (K)#
CO1	Apply cyber security architecture principles.	K3
CO2	Demonstrate the risk management processes and practices.	K2
CO3	Appraise cyber security incidents to apply appropriate response	K5
CO4	Distinguish system and application security threats and vulnerabilities.	K4
CO5	Identify security tools and hardening techniques	K3

Applied Cryptography

Code: R19MCY1152

Course Outcomes		Knowledge Level (K)#
CO1	Demonstrate the basics of Cryptographic protocols and Stream Ciphers	K2
CO2	Explain the concepts of Public Key Encryption and Block Ciphers	K5
CO3	Demonstrate Number Theory for Symmetric and Asymmetric Ciphers and discuss various Ciphers	K2
CO4	Discuss Hashing Algorithms and Message Authentication Codes	K6
CO5	Elaborate Key-Exchange algorithms and Real world Implementations	K6

Operating Systems Administration and Security

Code: R19MCY1153

Course Outcomes		Knowledge Level (K)#
CO1	Explain the important computer system resources and the role of operating system in their management policies and algorithms.	K2
CO2	Describe the concepts of Access control Fundamentals, Multics.	K4
CO3	Identify and assess current and anticipated security risks and vulnerabilities.	K3
CO4	Identify the security Techniques and apply the real time applications.	K3
CO5	Explain the role and responsibilities of a system administrator and Create and administer user accounts on both a Linux and Windows platform.	K5

Cyber Laws and Security Policies

Code: R19MCY1153

Course Outcomes		Knowledge Level (K)#
CO1	Design the Social And Intellectual Property Issues Emerging From Cyberspace.	K6
CO2	Explain The Legal And Policy Developments In Various Countries To Regulate Cyberspace	K2
CO3	Develop The Understanding Of Relationship Between Commerce And Cyberspace.	K3
CO4	Determine in Depth Knowledge Of Information Technology Act And Legal Frame Work Of Right To Privacy, Data Security And Data Protection.	K5
CO5	Apply various Case Studies On Real Time Crimes.	K3

Cloud and IoT Security

Code: R19MCY1153

Course Outcomes		Knowledge Level (K)#
CO1	Analyze the Cloud Computing and the different Cloud services and deployment models	K4
CO2	Assessing the financial, technological, and organizational capacity of employer's for actively initiating and installing cloud-based applications.	K5
CO3	Explain how IOT can be used in different Industries.	K2
CO4	Identify how companies can plan for the future of technologies.	K3
CO5	Apply smart applications in real world.	K3

Wireless Networks Security

Code: R19MCY1154

Course Outcomes		Knowledge Level (K)#
CO1	Explain the Threats in networks and provide Authentication to real time problems.	K2
CO2	Identify and investigate in-depth both early and contemporary threats to wireless networks security	K3
CO3	Analyze and determine for any organization the database security requirements and appropriate solutions	K4
CO4	Explain IP Security Issues and solve real time problems.	K5
CO5	Build the Basic specifications in Bluetooth Security.	K6

Cyberspace Operations and Design

Code: R19MCY1154

Course Outcomes		Knowledge Level (K)#
CO1	Explain the Concept of Cyberspace Environment and Design.	K2
CO2	Explain the Cyberspace Operational Approaches.	K2
CO3	Outline the cyberspace operation and integrate it with a Joint Operations plan.	K2
CO4	Build Cyber Warriors and Warrior Corps	K3
CO5	Designing Cyber Related Commands and Organizational structures.	K6

Database and Web Applications Security

Code: R19MCY1154

Course Outcomes		Knowledge Level (K)#
CO1	Explain threats, vulnerabilities and breaches to design database	K2
CO2	Discuss Relational Data Model and concurrency controls and locking, SQL extensions to security.	K6
CO3	Demonstrate the Browser security principles.	K2
CO4	Analyze the software centric security and mobile web browser security in real time applications	K4
CO5	Construct the penetrating testing workflows with examples.	K3

Research Methodology and IPR

Code: R19MCY1155

Course Outcomes		Knowledge Level (K)#
CO1	Demonstrate the research and its types	K2
CO2	Reviewing literature. Identifying and defining research problem.	K3
CO3	Explaining research design methods, sampling techniques	K5
CO4	Designing and development of measuring instruments, data collection and analysis methods	K6
CO5	Show the IPR protection provides an incentive to inventors for further research work and Investment in R & D, which leads to creation of new and better products, and in turn brings about, Economic growth and social benefits.	K1
CO6	Identify Research proposal, research report and evaluating research	K3

Cyber Security Lab

Code: R19MCY1157

Course Outcomes		Knowledge Level (K)#
CO1	Illustrate the knowledge of in-bound and out-bound rules in a client system.	K2
CO2	Identify security tools and hardening techniques.	K3
CO3	Design a backdoor on the target machine	K6

Cryptography Lab

Code: R19MCY1156

Course Outcomes		Knowledge Level (K)#
CO1	Apply the knowledge of symmetric cryptography to implement encryption and decryption using Ceaser Cipher, Substitution Cipher, Hill Cipher	K3
CO2	Demonstrate the different algorithms like DES, BlowFish, and Rijndael, encrypt the text "Hello world" using Blowfish Algorithm.	K2
CO3	Analyze and implement public key algorithms like RSA, Diffie-Hellman Key Exchange mechanism, the message digest of a text using the SHA-1 algorithm	K4

English for Research Paper Writing

Code: R19MCY1158

Course Outcomes		Knowledge Level (K)#
CO1	How to improve your writing skills and level of readability	K1
CO2	Explain about what to write in each section	K3
CO3	Classify the skills needed when writing a Title	K2

Disaster Management

Code: R19MCY1158

Course Outcomes		Knowledge Level (K)#
CO1	Demonstrate the critical understanding of key concepts in disaster risk reduction and humanitarian response.	K2
CO2	Evaluate disaster risk reduction and humanitarian response policy and practice from multiple perspectives.	K5
CO3	Develop an understanding of standards of humanitarian response and practical relevance in specific types of disasters and conflict situations.	K6
CO4	Analyze the strengths and weaknesses of disaster management approaches, planning and programming in different countries, particularly their home country or the countries they work in	K4
CO5	Describe disaster risk reduction and humanitarian response.	K2
CO6	Outline the disaster risk reduction and humanitarian response policy and practice from multiple perspectives.	K3

Sanskrit for Technical Knowledge

Code: R19MCY1158

Course Outcomes		Knowledge Level (K)#
CO1	Demonstrate basic Sanskrit language	K2
CO2	Illustrate Ancient Sanskrit literature about science & technology	K2
CO3	Build a logical language will help to develop logic in students	K6

Value Education

Code: R19MCY1158

Course Outcomes		Knowledge Level (K)#
CO1	Infer the knowledge of self-development	K2
CO2	Describe the importance of Human values	K2
CO3	Developing the overall personality	K6

Cyber Crime Investigation and Digital Forensics

Code: R19MCY1251

	Course Outcomes	Knowledge Level (K)#
CO1	Explain the computer forensics fundamentals.	K2
CO2	Describe the types of computer forensics technology	K3
CO3	Analyze various computer forensics systems.	K4
CO4	Illustrate the methods for data recovery, evidence collection and data seizure.	K2
CO5	Identify the Role of CERT-In Security	K3

Ethical Hacking

Code: R19MCY1252

	Course Outcomes	Knowledge Level (K)#
CO1	Explain the concepts related to malware, hardware and software vulnerabilities and their causes	K2
CO2	Determine the applicable laws, legal issues and ethical issues regarding computer crime.	K4
CO3	Explain the business need for security, threats, attacks, top ten security vulnerabilities, and secure software development.	K2
CO4	Demonstrate systematic understanding of the concepts of security at the level of policy and strategy in a computer system	K2
CO5	Evaluate security techniques used to protect system and user data	K5

Software Vulnerability Analysis

Code: R19MCY1253

	Course Outcomes	Knowledge Level (K)#
CO1	Contrast the basic concepts of security & Authentication	K2
CO2	Illustrate the Malicious Code in software applications	K2
CO3	Analyze and apply Access Control & Physical Protection to the UNIX and Windows operating system	K4
CO4	Explain the concepts of OSI Model, Sockets	K2
CO5	Explain the concepts of Counter Measures	K5

Malware Analysis and Reverse Engineering

Code: R19MCY1253

	Course Outcomes	Knowledge Level (K)#
CO1	Explain the characteristics of Malware and its effects on Computing systems.	K2
CO2	Predict the given system scenario using the appropriate tools to Identify the vulnerabilities and to perform Malware analysis.	K6
CO3	Analyze the given Portable Executable and Non-Portable Executable files using Static and dynamic analysis techniques.	K4
CO4	Demonstrate the Malware functionalities.	K2
CO5	Apply anti-reverse engineering in different Applications.	K3

Application Threat Detection

Code: R19MCY1253

Course Outcomes		Knowledge Level (K)#
CO1	Explain Hacking Web Apps and Profiling	K5
CO2	Illustrate to provide Authentication to the web application.	K2
CO3	Develop Penetration Testing and implement Input Injection Attacks.	K3
CO4	Identify the basic fundamentals of Metasploit	K3
CO5	Apply knowledge on Capturing User Input and Abusing UI Expectations	K3

Biometric Security

Code: R19MCY1254

	Course Outcomes	Knowledge Level (K)#
CO1	Demonstrate knowledge of the basic physical and biological science and engineering principles underlying biometric systems	K2
CO2	Analyze biometric systems at the component level and be able to analyze and design basic biometric system applications	K4
CO3	Illustrate to work effectively in teams and express their work and ideas orally and in writing	K2
CO4	Identify the sociological and acceptance issues associated with the design and implementation of biometric systems	K3
CO5	Elaborate various Biometric security issues in real world applications	K6

Web Security

Code: R19MCY1254

	Course Outcomes	Knowledge Level (K)#
CO1	Demonstrate security concepts, security professional roles, and security resources in the context of systems and security development life cycle	K2
CO2	Justify applicable laws, legal issues and ethical issues regarding computer crime	K5
CO3	Explain the business need for security, threats, attacks, top ten security vulnerabilities, and secure software development	K2
CO4	Apply information security policies, standards and practices, the information security blueprint	K3
CO5	Analyze and describe security requirements for typical web application scenario	K4

Firewall and VPN Security

Code: R19MCY1254

	Course Outcomes	Knowledge Level (K)#
CO1	To show the fundamental knowledge of Firewalls and it types	K2
CO2	Construct a VPN to allow Remote Access, Hashing, connections with Cryptography and VPN Authorization	K3
CO3	Elaborate the knowledge of depths of Firewalls, Interpreting firewall logs, alerts, Intrusion and Detection	K6
CO4	Infer the design of Control Systems of SCAD, DCS, PLC's and ICS's	K2
CO5	Evaluate the SCADA protocols like RTU, TCP/IP, DNP3, OPC,DA/HAD	K5

Cyber Crime Investigation and Digital Forensics Lab

Code: R19MCY1255

	Course Outcomes	Knowledge Level (K)#
CO1	Identify the importance of a systematic procedure for investigation of data found on digital storage media that might provide evidence of wrong-doing.	K3
CO2	Construct the file system storage mechanisms of two common desktop opera ting systems and forensics tools used in data analysis.	K6
CO3	List and Implement all running processes, network connections from a memory image and find whether a firewall is set by analyzing a memory image.	K4
CO4	Design and develop live incident response on a system, View all browser history and List out all established network connections in a computer (Hint: Triage Incident Response).	K6

Ethical Hacking Lab

Code: R19MCY1256

	Course Outcomes	Knowledge Level (K)#
CO1	Build the knowledge on Nmap, hping2 and hping3, Xmas scanning networks on targeted IP's.	K3
CO2	Make up the ideas in service enumeration tools like SuperScan and Softperfect.	K6
CO3	Apply knowledge on vulnerabilities scanning using Nessus tool and the system hacking tools like winrtgen .	K3
CO4	Determine the knowledge on Capture network packets using whireshark, Social Engineering Attack using Kali Linux	K5
CO5	Apply the idea on malware threats using HTTP RAT Torjan, TCP/IP Connections using currport tool.	K3
CO6	Infer the exposure on DOS attacks using Metasploit and Hping3	K2

Constitution of India

Code: R19MCY1258

	Course Outcomes	Knowledge Level (K)#
CO1	Discuss the growth of the demand for civil rights in India for the bulk of Indians before the arrival of Gandhi in Indian politics.	K6
CO2	Discuss the intellectual origins of the framework of argument that informed the conceptualization of social reforms leading to revolution in India.	K6
CO3	Discuss the circumstances surrounding the foundation of the Congress Socialist Party [CSP] under the leadership of Jawaharlal Nehru and the eventual failure of the proposal of direct elections through adult suffrage in the Indian Constitution.	K6
CO4	Discuss the passage of the Hindu Code Bill of 1956.	K6
CO5	Discuss the growth of the demand for civil rights in India for the bulk of Indians before the arrival of Gandhi in Indian politics.	K6

Pedagogy Studies

Code: R19MCY1258

	Course Outcomes	Knowledge Level (K)#
CO1	What pedagogical practices are being used by teachers in formal and informal classrooms in developing countries?	K1
CO2	What is the evidence on the effectiveness of these pedagogical practices, in what conditions, and with what population of learners?	K1
CO3	How can teacher education (curriculum and practicum) and the school curriculum and guidance materials best support effective pedagogy?	K1

Stress Management by Yoga

Code: R19MCY1258

	Course Outcomes	Knowledge Level (K)#
CO1	Develop healthy mind in a healthy body thus improving social health also	K2
CO2	Improve efficiency	K6

Personality Development through Life Enlightenment Skills

Code: R19MCY1258

	Course Outcomes	Knowledge Level (K)#
CO1	Study of Shrimad-Bhagwad-Geeta will help the student in developing his personality and achieve the highest goal in life	K2
CO2	The person who has studied Geeta will lead the nation and mankind to peace and prosperity	K3
CO3	Study of Neetishatakam will help in developing versatile personality of students.	K5

Cyber Security Governance

Code: R19MCY2351

	Course Outcomes	Knowledge Level (K)#
CO1	Explain the fundamental concepts and principles of the cyber Security Governance and theories of governance.	K2
CO2	Demonstrate the metrics of Cyber Security Governance.	K2
CO3	Explain the principal driving force for Cyber security governance is risk management, which involves mitigating risks and reducing or preventing potential impact on information resources.	K5
CO4	Model the enterprise needs metric against which to judge Cyber security policy to ensure that organizational objectives are achieved.	K3
CO5	Explore the Threat Intelligence Governance and Industrial Governance.	K6

Principles of Secure Coding

Code: R19MCY2352

	Course Outcomes	Knowledge Level (K)#
CO1	Outline the secure systems and various security attacks	K2
CO2	Demonstrate the development of process of software leads to secure coding practices	K2
CO3	Apply Secure programs and various risk in the software's	K3
CO4	Classify various errors that lead to vulnerabilities	K4
CO5	Design Real time software and vulnerabilities	K6

Information System Audit

Code: R19MCY2353

	Course Outcomes	Knowledge Level (K)#
CO1	Illustrate the fundamental concepts of information security and systems auditing	K2
CO2	Analyze the latest trend of computer security threats and defense	K4
CO3	Identify security weaknesses in information systems, and rectify them with appropriate security mechanisms	K3
CO4	Explain the security controls in the aspects of physical, logical and operational security control and case studies	K5
CO5	Evaluate the security of information systems	K6

Python Programming

Code: R19MCY2352

	Course Outcomes	Knowledge Level (K)#
CO1	Demonstrate and comprehend the basics of python programming.	K2
CO2	Demonstrate the principles of structured programming and be able to describe, design, implement, and test structured programs using currently accepted methodology.	K3
CO3	Explain the use of the built-in data structures list, sets, tuples and dictionary.	K5
CO4	Make use of functions and its applications.	K3
CO5	Identify real-world applications using oops, files and exception handling provided by python.	K3

Principles of Cyber Security

Code: R19MCY2352

Course Outcomes		Knowledge Level (K)#
CO1	Apply cyber security architecture principles.	K3
CO2	Demonstrate the risk management processes and practices.	K2
CO3	Appraise cyber security incidents to apply appropriate response	K5
CO4	Distinguish system and application security threats and vulnerabilities.	K4
CO5	Identify security tools and hardening techniques	K3

Internet of Things

Code: R19MCY2352

Course Outcomes		Knowledge Level (K)#
CO1	Explain the definition and usage of the term 'the internet of things' in different contexts	K5
CO2	Discover the various network protocols used in IoT	K3
CO3	Be familiar with the key wireless technologies used in IoT systems, such as Wi-Fi, 6LoWPAN, Bluetooth and ZigBee	K4
CO4	Illustrate the role data analytics in a typical IoT system	K2
CO5	Design a simple IoT system made up of sensors, wireless network connection, data analytics and display/actuators, and write the necessary control software	K6

Artificial Intelligence and Machine Learning

Code: R19MCY2352

Course Outcomes		Knowledge Level (K)#
CO1	Explain the fundamentals of AI and machine learning	K2
CO2	Identify an appropriate AI problem solving method and knowledge representation technique	K3
CO3	Identify appropriate machine learning models for problem solving	K3
CO4	Design and develop the AI applications in real world scenario	K6
CO5	Compare the relationship between AI, ML, and Deep Learning	K2