Shree Ramdeobaba College of Engineering & Management

Department of Computer Science & Engineering (Cyber Security)

HONORS & MINORS SCHEME & SYLLABUS

2023-24

Honors in B.Tech. CSE For students of branches CSE, AIML and Data Science

Sr. No.	Sem	Course Code	Course Title	Hrs/ Week			Credits	Maximum Marks			ESE Duration
				L	T	P		CA	ESE	Total	
1	III	CSTH303	Information and Cyber Security	3	0	0	3	40	60	100	3 Hrs
2	IV	CSTH403	Cyber Security Auditing	3	0	0	3	40	60	100	3 Hrs
3	V	CSTH503	Cyber Forensics: Threats, Vulnerability, Malware	4	0	0	4	40	60	100	3 Hrs
4	VI	CSTH603	Security Strategies in Windows and Linux	4	0	0	4	40	60	100	3 Hrs
5	VII	CSPH703	Project	0	0	8	4	50	50	100	-

Minor Scheme: For Departments Other than CSE & Allied Branches

Sr. No.	Semester	Course Code	Course Name	Hrs / Week			Credits	Maximum Marks			ESE Duration
				L	T	P		CA	ESE	Total	
1.	III	CCTM301	Introduction to Cyber Security	3	0	0	3	40	60	100	3 Hrs
2	IV	CCTM401	Cryptography	3	0	0	3	40	60	100	3 Hrs
3.	V	CCTM501	Network Security Fundamentals	4	0	0	4	40	60	100	3 Hrs
4.	VI	CCTM601	Basics of Ethical Hacking	4	0	0	4	40	60	100	3 Hrs
5.	VII	CCTM701	Project	0	0	8	4	50	50	100	-

Syllabus for Semester III(Honor), B. TECH CSE (Cyber Security)

Course Code: CSTH303 **Course: Information and Cyber Security**

L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week **Total Credits: 3**

Course Objectives

1. To develop an understanding Cyber Security
2. To introduce the student to the major concepts involved in Cyber Crimes
3. To understand basics of Cyber Attacks

Introduction to Computer Networks, Need of Cybersecurity, History & Impact of Internet, Introduction to Cybercrime, Reasons
for Committing Cybercrimes, Cyber-offenses Planning by Criminals, Introduction to Cyber Security, CNSS Security Model, Types of Network Attacks, Application Security, Identity and Access Management, Mobile Security, Infrastructure Security, Defense-in-Depth, Authentication, Data Loss Prevention (DLP), Data Backup, Fighting Cyber Attacks, Legal, Ethical, and Professional Issues in Information Security, Physical Security, Implementing Information Security, IS Project Management, Information Security Maintenance, Security Management Models, Balancing Information Security & Access, Security Professionals, IS Governance, Overview of Risk Management

Text Books:

1. Introduction to Cyber Security: Guide to the World of Cyber Security by Anand Shinde. Notion Press.
2. Principles of Information Security, Sixth Edition by Michael E. Whitman & Herbert J. Mattord. Cengage Publishing.

Course Outcomes:

After the successful completion of the course, students shall be able to –

1. Identify scope of modern-day cybersecurity needs.
2. Assign appropriate security controls for specific requirements.
3. Implement and maintain cybersecurity in organizations from legal and ethical perspectives.

Syllabus for Semester IV(Honor), B. TECH CSE (Cyber Security)

Course Code: CSTH403 **Course: Cyber Security Auditing**

L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week **Total Credits: 3**

Course Objectives

1. To understand concept of Auditing
2. To introduce the student to various Auditing frameworks and services
3. To gain knowledge of fraud detection and prevention

Auditing Internal Controls in an IT Environment, SOx and the COSO Internal Controls Framework, IIA and ISACA Standards for the Professional Practice of Internal Auditing, Using COBIT to Perform IT Audits, Understanding Risk Management Through COSO ERM Framework, Performing Effective IT Audits, Auditing IT General Controls, ITIL Service, CAATTs, IT Controls and the Audit Committee, Compliance with IT-Related Laws and Regulations, Cybersecurity and Privacy Controls, IT Fraud Detection and Prevention, Professional Certifications: CISA, CIA, and More, Penetration Testing Lab Setup, Information Gathering, Finding Vulnerabilities, Traffic Capture, Exploitation, Password Cracking, Social Engineering, Wireless Attacks, Buffer Overflow in Linux & Windows, Fuzzing, Porting, Mobile Hacking.

Text Books:

1. IT Audit, Control, and Security by Robert R. Moeller. Wiley Publishing.
2. Penetration Testing: A Hands-On Introduction to Hacking by Georgia Weidman. No Starch Press.

Course Outcomes:

After the successful completion of the course, students shall be able to –

1. Identify internal controls for auditing IT infrastructures.
2. Perform IT audits compliant to international standards.
3. Assess risk of cyber-attacks to organizations by using ethical hacking techniques to perform penetration tests.

Syllabus for Semester V(Honor), B. TECH CSE (Cyber Security)

Course Code: CSTH503 **Course: Cyber Forensics – Threats, Vulnerability, Malware**

L: 4 Hrs, T: 0 Hr, P: 0 Hr, Per Week **Total Credits: 4**

Course Objectives

1. To develop an understanding of digital data
2. To identify various domains of cyber attacks
3. To know the concept of forensic investigation

Introduction, Bits, Bytes & Numbering Schemes, Storage & Memory, File Extensions & Signatures, Labs & Tools, Collecting Evidence, Chain of Custody, Cloning, Live RAM Collection, Hashing, Windows System Artifacts, Anti-forensics, Legal Requirements, Expert Testimony, Internet & Email Forensics, Network Forensics, Mobile Device Forensics, Report Writing, Social Media Forensics, Social Engineering Forensics, Cloud Forensics Challenges, Malware Incident Response, Memory Forensics for Malware Artifacts, Extracting Malware: Post-Mortem, Malware File Identification & Profiling, Static & Dynamic Malware Analysis

Text Books:

1. The Basics of Digital Forensics, Second Edition by John Sammons. Syngress Publishing.
2. Digital Forensics Explained, Second Edition by Greg Gogolin. CRC Press.
3. Malware Forensics: Investigating and Analyzing Malicious Code by James M. Aquilina, Eoghan Casey & Cameron H. Malin. Syngress Publishing.

Course Outcomes:

After the successful completion of the course, students shall be able to –

1. Recognize valuable digital evidence from digital data.
2. Perform forensics investigation in multiple domains of cyber-attacks.
3. Present forensic evidence and its analysis according to acceptable reporting formats.

Syllabus for Semester VI(Honor), B. TECH CSE (Cyber Security)

Course Code: CSTH603 **Course: Security Strategies in Windows & Linux**

L: 4 Hrs, T: 0 Hr, P: 0 Hr, Per Week **Total Credits: 4**

Course Objectives

1. To understand the attacks areas of Windows and Linux
2. To identify security plan for operating systems like Windows and Linux
3. To understand how to apply security layers in Windows and Linux

Information Systems Security, Microsoft EULA, Microsoft Windows & Applications IT Infrastructure, Anatomy of Microsoft Windows Vulnerabilities, Windows Attack Surfaces and Mitigation, Managing & Maintaining Security in Microsoft Windows, Windows Security Profile & Audit Tools, Windows Security Administration, Windows OS Hardening, MS Application Security, Windows Incident Handling & Management, Linux Overview & Security Brief, Security Threats to Linux, Basic Components of Linux Security, Layered Security in Linux, AppArmor, SELinux, Kernel Security Risk Mitigation, Managing Security Alerts & Updates, Maintaining Linux Security Baseline, Detecting & Responding to Security Breaches, Best Practices & Emerging Technology

Text Books:

1. Security Strategies in Windows Platforms and Applications, Third Edition by Michael G. Solomon. Jones and Bartlett Learning.
2. Security Strategies in Linux Platforms and Applications, Second Edition by Michael Jang & Ric Messier. Jones and Bartlett Learning.

Course Outcomes:

After the successful completion of the course, students shall be able to –

1. Recognise the attack surface on different versions & flavours of Windows & Linux operating systems.
2. Design strategic security plans for operating system security in Windows & Linux.
3. Administer layered security controls in Windows & Linux operating systems..

Syllabus for Semester VII (Honor), B. Tech. Computer Science & Engineering (Cyber Security)

Course Code:	**CCPH703**	**Course:**	**Project**
L: 0 Hrs, T: 0 Hr, P: 8 Hr, Per Week		**Total Credits:**	**04**

Outcomes

These learning outcomes are intended to assist students in acquiring a comprehensive understanding of Cyber Security concepts and their practical applications. On successful completion of the project, students will be able to:

1. Identify, understand, formulate, and solve engineering problems
2. Apply knowledge of Math, Science, and Engineering
3. Participate in a hands-on project involving Cyber Security techniques, and the applications of these skills in different domains and settings.
4. Identify and employ appropriate system development tools and techniques
5. Test and deploy the system to solve the society's and industry's real life problems
6. Function in multi-disciplinary teams
7. Engage in Life-long learning.
8. Employ techniques, skills, and modern engineering tools for presentation, report / paper drafting, and product manual development.

The project will focus on the creation of Cyber Security-based products, utilizing the expertise acquired in previous semesters. This topic primarily centers on the product development cycle and its sequential execution. The acquisition of skills necessary for producing high-quality research papers, project reports, product manuals, patent documents, and presentations is facilitated by engaging in a range of educational activities like as attending technical sessions and seminars, accessing online resources like YouTube lectures, participating in courses offered by platforms like NPTEL, EDX, and Coursera, and completing associated assessments.

Syllabus for Semester III(Minor), B. TECH CSE (Cyber Security)

Course Code: CCTM301 Course: Introduction to Cyber Security

L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 3

Course Objectives

1. To understand the need of cyber security
2. To get knowledge of various types of cyber crimes
3. To understand various tools and methods to handle cyber crimes

Introduction to Computer Networks, Need of Cybersecurity, History & Impact of Internet, Introduction to Cybercrime, Reasons
for Committing Cybercrimes, Cybercrime: Mobile and Wireless Devices, Cyber-offenses Planning by Criminals, Introduction to Cyber Security, CNSS Security Model, Types of Network Attacks, Application Security, Identity and Access Management, Mobile Security, Infrastructure Security, Defense-in-Depth, Authentication, Data Loss Prevention (DLP), Data Backup, Fighting Cyber Attacks, Cybersecurity: Organizational Implications, Tools and Methods Used in Cybercrime, Cybercrime and Cyberterrorism: Social, Political, Ethical and Psychological Dimensions, Cybercrimes and Cybersecurity: The Legal Perspectives, Careers in Cybersecurity

Text Books:

1. Introduction to Cyber Security: Guide to the World of Cyber Security by Anand Shinde. Notion Press.
2. Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole & Sunit Belapure. Wiley Publishing.

Course Outcomes:

After the successful completion of the course, students shall be able to –

1. Identify scope of modern-day cybersecurity needs.
2. Assign appropriate security controls for specific requirements.
3. Implement and maintain cybersecurity in organizations from legal and ethical perspectives.

Syllabus for Semester IV(Minor), B. TECH CSE (Cyber Security)

Course Code: CCTM401 **Course: Cryptography**

L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week **Total Credits: 3**

Course Objectives

1. To understand basics of Cryptography.
2. To be able to secure a message over insecure channel by various means.
3. To learn about how to maintain the Confidentiality, Integrity and Availability of data
4. To understand various protocols to protect against the threats in the networks.

Introduction to security attacks - services and mechanism, Mathematics of Cryptography- Integer Arithmetic, Modular Arithmetic, introduction to cryptography - Conventional Encryption, Mathematics of Symmetric-key Cryptography- Algebraic Structures- Groups, ring & Finitefield, stream and block ciphers - Modern Block Ciphers: Block ciphers principals - Shannon's theory of confusion and diffusion - fiestal structure - data encryption standard (DES) - strength of DES - block cipher modes of operations - DES – AES. Confidentiality using conventional encryption - Mathematics of Asymmetric-key cryptography- random number generation - Principles of public key crypto systems - RSA algorithm - security of RSA - key management Diffie-Hellman key exchange algorithm Integrity checks and Authentication algorithms MD5 message digest algorithm Application Layer Security, IP Security and Key Management

Text Books:

1. William Stallings, "Cryptography and Network securityPrinciples and Practices", Pearson/PHI ,5th Edition
2. Wade Trappe, Lawrence C Washington, "Introduction toCryptography with coding theory", Pearson.
3. Behrouz A. Forouzan, Debdeep Mukhopadhyay, "Cryptographyand Network Security" 3rd Edition, McGrawHill.

Course Outcomes:

After the successful completion of the course, students shall be able to –

1. Understand various cryptographic Techniques.
2. Apply various public key cryptography techniques.
3. Implement hashing and digital signature techniques.
4. Apply IP security techniques.

Syllabus for Semester V(Minor), B. TECH CSE (Cyber Security)

Course Code: CCTM501 **Course: Network Security Fundamentals**

L: 4 Hrs, T: 0 Hr, P: 0 Hr, Per Week **Total Credits: 4**

Course Objectives

1. To get to know various threats on networks
2. To design security policies for network
3. To use various tools for network security

Network Security Overview, Understanding Vulnerabilities, Understanding Defenses, Malware & Social Engineering Attacks, Application & Network Attacks, Vulnerability Assessment, Host, Application & Data Security, Cryptography, Security Policies, Secure Design, Web Security, Router Security, Firewalls, IDS/IPS, Remote Access, Endpoint Security, VPNs, PKI, Key Management, SSL/TLS, Wireless Security, Logging & Auditing, Cloud and Virtualization Security, Access Control Fundamentals, RADIUS, TACACS, LDAP, Authentication & Account Management, SSO, Risk Mitigation

Text Books:

1. Network Security Fundamentals by Gert De Laet & Gert Schauwers. Cisco Press.
2. CompTIA Security+: Guide to Network Security Fundamentals, Seventh Edition by Mark Ciampa. Cengage Publishing.

Course Outcomes:

After the successful completion of the course, students shall be able to –

1. Distinguish between different cyber threats and attacks on networks.
2. Enhance network security structurally through security policies and network design.
3. Implement security tools and rules for network perimeter protection.

Syllabus for Semester VI (Minor), B. TECH CSE (Cyber Security)

Course Code: CCTM601 Course: Basics of Ethical Hacking

L: 4 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 4

Course Objectives

1. Learn about the hacker mindset and the history of hackers
2. Understand basic networking and security technologies
3. Gain a basic understanding of security policy
4. Explore various vulnerability analysis techniques.

Syllabus:

Ethical Hacking, Types of Hackers, Phases of Ethical Hacking, Fundamentals of computer networking. TCP/IP protocol stack, IP addressing and routing, Common Network Threats/Attacks, Introduction to cryptography, private-key encryption, public-key encryption, Key exchange protocols, cryptographic hash functions, applications, Digital signatures, Attacks on cryptosystems Vulnerability Analysis, Types of Vulnerability Analysis, Vulnerability Assessment Tools, System Hacking, Password Cracking, Penetration testing, Hiding Files, Clearing logs

DoS attack, DDoS attack, Common symptoms of DoS/DDoS attack Categories of DoS/DDoS Attack Vectors, session hijacking, Application and Network level session hijacking ,Malware and its propagation ways, Malware components, Types of malware, Concept of sniffing, Types of sniffing, Types of sniffing attacks Intrusion Detection System (IDS), Types of Intrusion Detection Systems, Introduction to Firewalls, Types of Firewalls, Introduction to Honeypots, Case studies: various attacks scenarios and their remedies.

Course Outcome:

At the end of the course, the students should be able to:

1. Develop the core foundations of ethics and cryptography in regards to computer security
2. Analyzing the vulnerability with respect to hacking, DDOS attack and session hijacking
3. Classify various types of malware and sniffing attacks on network
4. Analyzing various attacks scenario and remedies and detecting the attack with IDS.

Text Books:

1. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy, 2nd Edition, Patrick Engebreston, ISBN: 0124116442

Reference Books:

1. Penetration Testing: A Hands-On Introduction to Hacking, Georgia Weidman, ISBN: 1593275641
2. ETHICAL HACKING: A Comprehensive Beginner's Guide to Learn and Master Ethical Hacking, Hein Smith, Hilary Morrison

Syllabus for Semester VII (Minor), B. Tech. Computer Science & Engineering (Cyber Security)

Course Code:	**CCPM701**	**Course:**	**Project**
L: 0 Hrs, T: 0 Hr, P: 8 Hr, Per Week		**Total Credits:**	**04**

Outcomes

These learning outcomes are intended to assist students in acquiring a comprehensive understanding of Cyber Security concepts and their practical applications. On successful completion of the project, students will be able to:

9. Identify, understand, formulate, and solve engineering problems
10. Apply knowledge of Math, Science, and Engineering
11. Participate in a hands-on project involving Cyber Security techniques, and the applications of these skills in different domains and settings.
12. Identify and employ appropriate system development tools and techniques
13. Test and deploy the system to solve the society's and industry's real life problems
14. Function in multi-disciplinary teams
15. Engage in Life-long learning.
16. Employ techniques, skills, and modern engineering tools for presentation, report / paper drafting, and product manual development.

The project will focus on the creation of Cyber Security-based products, utilizing the expertise acquired in previous semesters. This topic primarily centers on the product development cycle and its sequential execution. The acquisition of skills necessary for producing high-quality research papers, project reports, product manuals, patent documents, and presentations is facilitated by engaging in a range of educational activities like as attending technical sessions and seminars, accessing online resources like YouTube lectures, participating in courses offered by platforms like NPTEL, EDX, and Coursera, and completing associated assessments.