DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

LIST OF COURSES OFFERED FOR HONOR PROGRAM (R23)

(Cyber Security)

Course code	Course Title	Contact hours/week				Credits
		L	T	P	Total	
23CSH1	Mathematical Foundations for Security	3	0	0	3	3
23CSH2	Principles of Cyber Security	3	0	0	3	3
20CSH3	Vulnerability Assessment and Penetration Testing	3	0	0	3	3
20CSH4	Cyber Crime Investigation & Digital Forensics	3	0	0	3	3
23CSH5	Malware Analysis & Reverse Engineering	3	0	0	3	3
23CSH6	Cyber Security Lab	0	0	3	3	1.5
23CSH7	Digital Forensics Lab	0	0	3	3	1.5

List of MOOCs Courses:

1. **Cyber Security and Privacy**
2. **Privacy and security in online social media**
3. **Safety and Risk Analytics**
4. **Practical Cyber Security for Cyber Security Practitioners**
5. **Secure Computation: Part II**

B.Tech.CSE (HONOR) **23CSH1- Mathematical Foundations for Security**

L	T	P	Cr.
3	0	0	3

Course Objectives:

- To understand the mathematical fundamentals in probabilistic and statistical concepts
- To develop the understanding of the mathematical and logical basis of various modern techniques in information technology like machine learning, programming language design, and concurrency.
- To study various Graph Theory problems.

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

CO1: Understand the basic notions of discrete and continuous probability **(Understand-L2)**
CO2: Apply the methods of statistical inference, and learn application of sampling distributions in Data mining and Machine Learning**.(Apply-L3)**
CO3: Apply statistical analysis to algorithmic problems of simple to moderate complexity in different domains **(Apply-L3)**
CO4: Model different applications of Computer science as graph theory problems **(Apply-L3)**
CO5: Evaluate modular exponentiation for cryptographic applications. **(Evaluate-L5)**

UNIT I

Density, and cumulative distribution functions, Expected value, conditional expectation, Applications of the univariate and multivariate Central Limit Theorem, Probabilistic inequalities, Markov chains.

UNIT II

Random samples, sampling distributions of estimators, and Maximum Likelihood.

UNIT III

Statistical inference, Introduction to multivariate statistical models: classification problems, principal component analysis, The problem of over fitting model assessment

UNIT IV

Graph Theory: Isomorphism, Planar graphs, graph coloring, Hamilton circuits and Euler cycles. Permutations and Combinations with and without repetition. Specialized techniques to solve combinatorial enumeration problems **.**

UNIT V

Number Theory: Elementary number theory, unique factorization, Euler's function, modular arithmetic, Fermat's little theorem, Chinese remainder theorem, modular exponentiation, RSA public key encryption.

Text Books:

1. John Vince, Foundation Mathematics for Computer Science, Springer, 2015.
2. K. Trivedi, Probability and Statistics with Reliability, Queuing, and Computer Science Applications, Wiley, 2001.

Reference Books:

1. M. Mitzenmacher and E. Upfal, Probability and Computing: Randomized Algorithms and Probabilistic Analysis, 2005.
2. Alan Tucker, Applied Combinatorics, Wiley, 2012.

B.Tech.CSE (HONOR)

23CSH2- Principles of Cyber Security

L	T	P	Cr.
3	0	0	3

Course Objectives: The main objectives of the course is to

- To learn threats and risks within context of the cyber security architecture..
- Student should learn and Identify security tools and hardening techniques.
- To learn types of incidents including categories, responses and timelines for response.

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

CO1: Apply cyber security architecture principles. **(Apply- L3)**
CO2: Describe risk management processes and practices.**(Understand- L2)**
CO3: Appraise cyber security incidents to apply appropriate response. **(Analyze- L4)**
CO4: Distinguish system and application security threats and vulnerabilities. **(Analyze- L4)**
CO5: Identify security tools and hardening techniques. **(Remember-L1)**

UNIT – I:

Introduction to Cyber security- Cyber security objectives, Cyber security roles, Differences between Information Security & Cyber security, Cyber security Principles-Confidentiality, integrity, &availability Authentication & non- repudiation.

UNIT – II:

Information Security (IS) within Lifecycle Management-Lifecycle management landscape, Security architecture processes, Security architecture tools, Intermediate lifecycle management concepts, Risks & Vulnerabilities-Basics of risk management, Operational threat environments, Classes of attacks.

UNIT – III:

Incident Response- Incident categories, Incident responseIncident recovery, and Operational security protection: Digital and data assets, ports and protocols, Protection technologies, Identity and access Management, configuration management.

UNIT – IV:

Threat Detection and Evaluation (DE):Monitoring- Vulnerability Management, Security Logs and Alerts, Monitoring Tools and Appliances. Analysis- Network traffic Analysis, packet capture and analysis .

UNIT – V:

Introduction to backdoor System and security-Introduction to metasploit, Backdoor, demilitarized zone(DMZ),Digital Signature, Brief study on Harding of operating system.

Textbooks:

1. NASSCOM: Security Analyst Student Hand Book Dec 2015.
2. Information Security Management Principles Updated Edition by David Alexander, Amanda Finch, David Sutton ,Published by BCS, June 2013.

Reference Books:

1.CSX- cyber security fundamentals 2 nd edition, Published by ISACA, Cyber security, Network Security, Data Governance Security

B.Tech.CSE (HONOR)

20CSH3- Vulnerability Assessment and Penetration Testing

L	T	P	Cr.
3	0	0	3

Course Objectives: The main objectives of the course is to

- To identify security vulnerabilities and weaknesses in the target applications.
- To identify how security controls can be improved to prevent hackers gaining access to operating systems and networked environments.
- To test and exploit systems using various tools.
- To understand the impact of hacking in real time machines.

Course Outcomes: After successful completion of the course the students are able to

CO1: Explain Penetration testing phases. **(Understand-L2)**
CO2: Illustrate information gathering methodologies. **(Understand-L2)**
CO3: Apply System Hacking Techniques in real time applications **. (Apply - L3)**
CO4: Describe Bypassing WLAN Authentication **(Understand-L2)**
CO5: Analyze and test wireless network security using authentication bypass,attack simulation, and traffic analysis techniques. **(Analyze-L4)**

UNIT – I:

Introduction-Penetration Testing phases/Testing Process, types and Techniques, Blue/Red Teaming, Strategies of Testing, Non Disclosure Agreement Checklist, Phases of hacking, Open-source/proprietary Pentest Methodologies .

UNIT – II:

Information Gathering and Scanning-Information gathering methodologies- Foot printing, Competitive Intelligence- DNS Enumerations- Social Engineering attacks, Port Scanning-Network Scanning- Vulnerability Scanning- NMAP scanning tool- OS Fingerprinting- Enumeration.

UNIT – III:

System Hacking Password cracking techniques- Key loggers- Escalating privileges- Hiding Files, Double Encoding, Steganography technologies and its Countermeasures. Active and passive sniffing- ARP Poisoning, MAC Flooding- SQL Injection - Error- based, Union based, Time-based, Blind SQL, Out-of-band. Injection Prevention Techniques.

UNIT – IV:

Advanced System Hacking: Broken Authentication, Sensitive Data Exposure, XML External Entities, Broken Access Code, XSS - Stored, Reflected, DOM Based

UNIT – V:

Wireless Pentest: Wi-Fi Authentication Modes, Bypassing WLAN Authentication, Types of Wireless Encryption, WLAN Encryption Flaws, AP Attack, Attacks on the WLAN Infrastructure, DoS-Layer1, Layer2, Layer 3, DDoS Attack, Client Misassociation, Wireless Hacking Methodology, Wireless Traffic Analysis .

Text Books:

1. Kali Linux
2. Windows Penetration Testing, 1st Edition, By Wolf Halton, Bo Weaver, June 2016 ,Packt Publishing.

Reference Books:

1. Mastering Modern Web Penetration Testing By Prakhar Prasad, October 2016 Packt Publishing.
2. SQL Injection Attacks and Defense 1st Edition, by Justin Clarke-Salt, Syngress Publication.

B.Tech. CSE (HONOR)

20CSH4- Cyber Crime Investigation & Digital Forensics

L	T	P	Cr.
3	0	0	3

Course Objectives: The learning objectives of this course are to:

- Able to identify security risks and take preventive steps
- To understand the forensics fundamentals.
- To understand the evidence capturing process.
- To understand the preservation of digital evidence

Course Outcomes: After successful completion of the course the students are able to

CO1: Acquire the definition of computer forensics fundamentals.**(Remember-L1)**

CO2: Describe the types of computer forensics technology. **(Understand-L2)**

CO3: Analyze various computer forensics systems**. (Analyze-L4)**

CO4: Illustrate the methods for data recovery, evidence collection and data seizure. **(Understand-L2)**

CO5: Summarize duplication and preservation of digital evidence.**(Understand-L2)**

UNIT I

Introduction: Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime: Social Engineering, Categories of Cyber Crime, Property Cyber Crime. Style.

UNIT II

Cyber Crime Issues: Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation ,Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses.

UNIT III

Investigation: Investigation Introduction to Cyber Tools, Crime Investigation, e-Discovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies. Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.

UNIT IV

Digital Forensics: Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics.

UNIT V

Laws And Acts: Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC , Electronic Communication Privacy ACT, Legal Policies.

Reference Books:

1. Nelson Phillips and Enfinger Steuart, "Computer Forensics and Investigations", Cengage Learning, New Delhi, 2009.
2. Kevin Mandia, Chris Prosise, Matt Pepe, "Incident Response and Computer Forensics", Tata McGraw-Hill, New Delhi, 2006.
Robert M Slade," Software Forensics", Tata McGraw - Hill, New Delhi, 2005.

B.Tech.CSE (HONOR)

23CSH5- Malware Analysis & Reverse Engineering

L	T	P	Cr.
3	0	0	3

Course Objectives: The main objectives of the course is to

- To understand the purpose of computer infection program.
- To implement the covert channel and mechanisms.
- To test and exploit various malware in open source environment.
- To analyze and design the famous virus and worms.
- Understand the Reverse Engineering (RE) Methodology
- Disassemble products and specify the interactions between its subsystems and their functionality.

Course Outcomes: After successful completion of the course the students are able to

CO1: Explain the characteristics of Malware and its effects on Computing systems. **(Understand-L2)**
CO2: Predict the given system scenario using the appropriate tools to Identify the vulnerabilities and to perform Malware analysis. **(Apply-L3)**
CO3: Analyze the given Portable Executable and Non-Portable Executable files using Static and dynamic analysis techniques.**(Analyze – L4)**
CO4: Demonstrate the Malware functionalities.**(Apply - L3)**
CO5: How to apply anti-reverse engineering in different Applications .**(Apply - L3)**

UNIT – I:

Malware Basics- General Aspect of Computer infection program, Non Self Reproducing Malware, How does Virus Operate, Virus Nomenclature, Worm Nomenclature, Recent Malware Case Studies.

UNIT – II:

Basic Analysis- Antivirus Scanning, x86 Disassembly, Hashing, Finding Strings, Packed Malware, PE File Format, Linked Libraries & Functions, PE Header File &Section.

UNIT – III:

Advanced Static & Dynamic Analysis-IDA Pro, Recognizing C code constructs, Analyzing malicious windows program, Debugging, OllyDbg, Kernel Debugging with WinDbg, Malware Focused Network Signatures.

UNIT – IV:

AMalware Functionalities-Malware Behavior, Covert Malware Launch, Data Encoding, Shell code Analysis.

UNIT – V:

Reverse Engineering Malware (REM): REM Methodology, Resources for Reverse-Engineering Malware (REM) Understanding Malware Threats, Malware indicators, Malware Classification, Examining Clam AV-Signatures.

Text Books:

1. Michael Sikorski, Andrew Honig “Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software” publisher Williampollock.

Reference Books:

1. ErciFiliol, “Computer Viruses: from theory to applications”, Springer, 1st edition, 2005.

B.Tech.CSE (HONOR)

23CSH6- Cyber Security Lab

L	T	P	Cr.
0	0	3	1.5

Course Objectives: The main objectives of the course is to

- Student to get the knowledge about audit and information security management, which makes the student to get the real world experience.
- To learn and implement Data leakage in a website database.

Course Outcomes: After successful completion of the course the students are able to

CO1: Analyze and implement Audit security policy in windows environment, create a Demilitarized zone creation in Network environment **(Analyze-L4)**
CO2: Illustrate the Resource harvesting attack and mitigation, Window Patch management policy, Trojans and mitigation strategies. **(Understand-L2)**
CO3: Apply the knowledge of metasploit, Access control list creation and content filtering limiting the traffic **(Apply - L3)**
CO4: Explain the Data leakage in a website database, Password policy and verification, Patch management using MBSA tool on windows machine .**(Understand-L2)**
CO5: Build an Audit Policy management, Media handling policy and event log analysis and Installation of Trojan, Network DOS attack and proof of bandwidth utilization **(Create-L6)**

List of Experiments:

Exercise 1: Audit security policy implementation in windows environment.
Exercise 2: Create a Demilitarized zone creation in Network environment for information security.
Exercise 3: Implement Resource harvesting attack and mitigation.
Exercise 4: Implement Window Patch management policy.
Exercise 5: Knowing the Behaviour of Trojans and mitigation strategies.
Exercise 6: Create a metasploit and make it to implement.
Exercise 7: Access control list creation and content filtering limiting the traffic.
Exercise 8: Data leakage in a website database and preventive measures.
Exercise 9: Password policy implementations and verification.
Exercise 10: Patch management implementation using MBSA tool on windows machine
Exercise 11: Audit Policy management for users and computers log analysis.
Exercise 12: Media handling policy implementation and event log analysis.
Exercise 13: Installation of Trojan and study of different options.
Exercise 14: Network DOS attack and proof of bandwidth utilization and preventive steps.

B.Tech.CSE (HONOR)	23CSH7- Digital Forensics Lab	L	T	P	Cr.
		0	0	3	1.5

Course Objectives: The main objectives of the course is to

- Identify the potential sources of digital evidence.
- Preserve the evidence by storing it securely and protecting it from alteration.
- Analyze the collected data to extract relevant information.

Course Outcomes: After successful completion of the course the students are able to

CO1: Apply forensic tools and techniques to recover deleted files and create forensic disk images. **(Apply-L3)**
CO2: Collect, preserve, and analyze digital evidence from emails, browsers, and USB devices. **(Apply-L3)**
CO3: Perform live forensic investigations using specialized tools to capture and analyze system activity **(Apply - L3)**
CO4: Analyze network traffic and packet data using Wireshark to extract forensic evidence. **(Analyze – L4)**
CO5: Use system monitoring tools to track processes, network activity, and memory usage for forensic purposes. **(Apply - L3)**

List of Experiments:

Exercise 1: Study of Computer Forensics and different tools used for forensic investigation.
Exercise 2: How to Recover Deleted Files using Forensics Tools
Exercise 3: How to make the forensic image of the hard drive using EnCase Forensics.
Exercise 4: How to Collect Email Evidence in Victim PC.
Exercise 5: How to Extracting Browser Artifacts
Exercise 6: Find Last Connected USB on your system (USB Forensics)
Exercise 7: Live Forensics Case Investigation using Autopsy
Exercise 8: Capturing and analyzing network packets using Wireshark
Exercise 9: Analyze the packets provided in lab and solve the questions using Wireshark
a) What web server software is used by www.uceou.com
b) About what cell phone problem is the client concerned?
c) How many webservers are running in Apache webserver.
Exercise 10: Using Sysinternals tools for Network Tracking and Process Monitoring
- Check Sysinternals tools
- Monitor Live Processes
- Capture RAM
- Capture TCP/UDP packets
- Monitor Hard Disk
- Monitor Virtual Memory
- Monitor Cache Memory

Exercise 11: Email Forensics
- Mail Service Providers
- Email protocols
- Recovering emails
- Analyzing email header

Exercise 12: Analyzing data of android mobile using MOBILedit.