COURSE STRUCTURE

and

DETAILED SYLLABI

for

Two Year PG Programme

M.Tech

Cyber Security

(Applicable for batches admitted from 2025-26)

Department of Computer Science & Engineering
University College of Engineering Kakinada (A)
JNTUK, Kakinada - 533003

M.Tech Cyber Security I - Semester

S.No	Course Title	L	T	P	C	Assessment	
						Int	Ext
1	**Program Core-1** Mathematical Foundations for Cyber Security	3	1	0	4	40	60
2	**Program Core-2** Incident Response and Threat Intelligence	3	1	0	4	40	60
3	**Program Core-3** Applied Cryptography	3	1	0	4	40	60
4	**Program Elective-1**	3	0	0	3	40	60
5	**Program Elective-2**	3	0	0	3	40	60
6	**Laboratory-1** Incident Response and Threat Intelligence Lab	0	0	4	2	40	60
7	**Laboartory-2** Applied Cryptography Lab	0	0	4	2	40	60
8	**Seminar-1**	0	0	2	1	100	-
	Total Credits	15	3	10	23		

List of Program Elective Courses in I Semester (Electives – I & II)

S.No.	Course Title
1	Firewall and VPN Security
2	Malware Analysis and Detection
3	Internet of Things Security
4	Design of Secure Operating Systems
5	Web Application security
6	Hardware Security
7	Any minimum12 weeks MOOCS/NPTEL courses with prior approval of BoS

M.Tech Cyber Security II - Semester

S.No	Course Title	L	T	P	C	Assessment	
						Int	Ext
1	**Program Core-4** Digital Forensics	3	1	0	4	40	60
2	**Program Core-5** Secure System Development	3	1	0	4	40	60
3	**Program Core-6** Penetration Testing & Vulnerability Analysis	3	1	0	4	40	60
4	**Program Elective-3**	3	0	0	3	40	60
5	**Program Elective-4**	3	0	0	3	40	60
6	**Laboratory-3** Digital Forensics Lab	0	0	4	2	40	60
7	**Laboartory-4** Penetration Testing & Vulnerability Analysis Lab	0	0	4	2	40	60
8	**Seminar-2**	0	0	2	1	100	-
	Total Credits	15	3	10	23		

List of Program Elective Courses in II Semester (Electives - III & IV)

S.No.	Course Title
1	Blockchain Application Security and Investigation
2	Post Quantum Cryptography
3	Artificial Intelligence & Machine Learning in Cyber security
4	Secure Database Application Development
5	Cloud Security
6	Cyber Laws and Security Policies
7	Any minimum12 weeks MOOCS/NPTEL courses with prior approval of BoS

Note: Summer Internship/ Industrial Training will be done during *Year break(II sem to III Sem)* and evaluated in III Sem.

M.Tech Cyber Security -III Semester

S.No	Course Title	L	T	P	C	Assessment	
						Int	Ext
1	Research Methodology and IPR / Swayam 12-week MOOC course – RM&IPR	3	0	0	3	40	60
2	Summer Internship/ Industrial Training (8-10 weeks)*	-	-	-	3	100	-
3	Comprehensive Viva#	-	-	-	2	100	-
4	Dissertation Part – A$			20	10	100	-
Total Credits		3		20	18		

** Student attended during summer/year break, and assessment will be done in the third semester.*
 # Comprehensive viva can be conducted for courses completed up to the second semester.
$ Dissertation – Part A, internal assessment

IV Semester

S.No	Courses	L	T	P	C	Assessment	
						Int	Ext
1	Dissertation Part – B%	-	-	32	16	-	100
Total Credits					16		

% External Assessment

I Semester	MATHEMATICAL FOUNDATIONS FOR CYBER SECURITY	L	T	P	C
		3	1	0	4

Course Objectives:

The main objective of this course to

- Develop a strong foundation in number theory, algebraic structures, probability theory, coding theory, and pseudorandom number generation,
- Apply mathematical concepts and computational techniques for problem-solving, cryptography, and secure communication systems.

UNIT	CONTENTS
UNIT – 1	Number Theory: Introduction, Divisibility, Greatest common divisor, Prime numbers, Fundamental theorem of arithmetic, Mersenne primes, Fermat numbers, Euclidean algorithm, Fermat's theorem, Euler totient function, Euler's theorem. Congruences: Definition, Basic properties of congruences, Residue classes, Chinese remainder theorem.
UNIT – 2	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 (p^n),GF(2^n), Classification, Structure of finite fields. Lattice, Lattice as Algebraic system, sub lattices, some special lattices.
UNIT – 3	Probability Theory: Introduction, Concepts of Probability, Conditional Probability, Baye's Theorem, Random Variables, discrete and continuous, central Limit Theorem, Stochastic Process, Markov Chain.
UNIT – 4	Coding Theory: Introduction, Basic concepts: codes, minimum distance, equivalence of codes, Linear codes, Generator matrices and parity-check matrices, Syndrome decoding, Hamming codes, Hadamard Code, Goppa codes.
UNIT – 5	Pseudorandom Number Generation: Introduction and examples, Indistinguishability of Probability Distributions, Next Bit Predictors, The Blum-Blum-Shub(BBS) Generator, Security of the BBS Generator.

Text Books:

1. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, 'An introduction to the theory of numbers', John Wiley and Sons.
2. Douglas Stinson, 'Cryptography – Theory and Practice', CRC Press.
3. Sheldon M Ross, "Introduction to Probability Models", Academic Press.

Reference Books:

1. C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill.
2. Fraleigh J. B., 'A first course in abstract algebra', Narosa.
3. Joseph A. Gallian, ''Contemporary Abstract Algebra', Narosa.

I Semester	INCIDENT RESPONSE AND THREAT INTELLIGENCE	L	T	P	C
		3	1	0	4

Course Objectives:

The main objectives of this course is to

- Provide a thorough understanding of incident response and threat intelligence processes.
- Equip students with practical skills for managing and handling cybersecurity incidents.
- Develop expertise in leveraging threat intelligence for risk management and vulnerability assessment.
- Learn the incident handling process, incident prioritization, and the impact of virtualization on response techniques.

UNIT	CONTENTS
UNIT – 1	**Introduction to Incident Response:** Cyber Incident Statistics, Computer Security Incidents, Information Warfare: Key concepts of Information Security,Types of Computer Security Incidents, Examples of Computer Security Incidents, Identifying an incident, Need for Incident Response,Goals and Purpose of Incident Response,Signs of an Incident- Precursors &Indicators, Incident Categories.
UNIT – 2	Incident Management and Handling: Incident Handling Process,Incident Prioritization, Impact of Virtualization on Incident Response & Handling,Estimating Cost of an Incident,Incident Reporting & Reporting Standards, Incident Reporting Organizations, Vulnerability Resources, Introduction to Security Operations Center (SOC), Working on SOC: Introduction to Logs, Types and Sources of Logs, Need for Log Management, Challenges of Log Management,Incident Response Tools and Techniques.
UNIT – 3	Threat Intelligence in Incident Handling,Threat Intelligence introduction, Data versus Intelligence, Need for Threat Intelligence, Threat Intelligence Process Model, Threat Intelligence Life Cycle, Levels of Threat Intelligence, Threat Intelligence Challenges
UNIT – 4	Threat Intelligence for Vulnerability and Risk Management, Risk Management, Assess Risk based on Exploitability, Exploitability versus Exploitatincident response lab ion,Sources of Intelligence , Cross-Referencing Intelligence, The Fair Play Model, The Lockheed Martin Cyber Killing Chain, The Diamond Model, The MITRE ATT&CK Framework, Cyber security framework 2.0, NIST framework
UNIT – 5	Threat Hunting Using PowerShell: Introduction to Threat Hunting, Threat Hunting Tools & Techniques, Introduction to PowerShell, Environment, Working with PowerShell Scripts, cmdlets, files & folders, dates and times, File I/O , Advanced Cmdlets , PowerShell Scripting, special variables, operators, looping, conditions, array, hash tables, regex, PowerShell Advanced Functions, Objects in Windows PowerShell; Error Handling Concepts, terminating

	&nonterminating errors, Using PowerShell to Formulate the Hunt – List & Identify the Processes, use of CIM, , PowerShell remoting capabilities: remoting concepts, invoking remote commands, processing outputs.

Textbooks:

1. Leighton Johnson, "Computer Incident Response and Forensics Team Management: Conducting Successful Incident Response", First Edition, Syngres.
2. JithinAbey Alex, "Incident Handling and Response: A Holistic Approach for an Efficient Security Incident Management", First Edition, 2020

Reference Books:

1. Murdoch, D. W, "Blue Team Handbook: Incident response", First Edition, CreateSpace Independent Publishing, 2016.
2. Steve Anson, "Applied Incident Response" First Edition, Wiley, 2020

I Semester	APPLIED CRYPTOGRAPHY	L	T	P	C
		3	1	0	4

Course Objectives:
The main objectives of this course are to

- Equip students with the knowledge and skills.
- Design, analyze and implement cryptographic techniques for ensuring confidentiality, integrity, authentication and secure communication in real-world applications.

UNIT	CONTENTS
UNIT – 1	Protocol Building Blocks, Basic Protocols, Advanced Protocols- Zero-Knowledge Proofs, Zero-Knowledge Proofs of Identity, Blind Signatures, Identity-Based Public-Key Cryptography, Key Length, Key Management..
UNIT – 2	Electronic Codebook Mode, Block Replay, Cipher Block Chaining Mode, Stream Ciphers, Self-Synchronizing Stream Ciphers, Cipher- Feedback Mode, Synchronous Stream Ciphers, Output-Feedback Mode, Counter Mode, Other Block-Cipher Modes, Choosing a Cipher Mode.Factoring, Prime Number Generation, Discrete Logarithms in a Finite Field, AES (with GCM mode) (Text book 2), ChaCha20-Poly1305, Ascon (lightweight crypto).
UNIT – 3	Pseudo-Random-Sequence Generators and Stream Ciphers- Linear Congruential Generators, Linear Feedback Shift Registers, Stream Ciphers using LFSRs, RC4, Feedback with Carry Shift Registers, Stream Ciphers Using FCSRs, Nonlinear-Feedback Shift Registers, Other Stream Ciphers, One-Way Hash Functions- MD5, Secure Hash Algorithm (SHA), One Way Hash Functions Using Symmetric Block, Using Public Key Algorithms, Message AuthenticationCodes.
UNIT – 4	Public-Key Algorithms, RSA, ElGamal, Elliptic Curve Cryptosystems, Digital Signature Algorithm (DSA), DSA Variants, Discrete Logarithm Signature Schemes, Schnorr, Converting Identification Schemes to Signature Schemes.
UNIT – 5	Diffie- Hellman, Station-to-Station Protocol, Multiple-Key Public-Key Cryptography, Subliminal Channel, Undeniable Digital Signatures, Designated Confirmer Signatures, Kerberos, Message Security Protocol (MSP), Pretty Good Privacy (PGP), Smart Cards, Public-Key Cryptography Standards (PKCS).

Text Books:

1. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, Bruce Schneier, John Wiley& Sons Inc.
2. Serious Cryptography: A Practical Introduction to Modern Encryption, Jean-Philippe Aumasson, No Starch Press, 2018

Reference Books:

1. ChaCha20 and Poly1305 for IETF Protocols, RFC 7539

2. Ascon-Based Lightweight Cryptography Standards for Constrained Devices, NIST Special Publication 800 NIST SP 800-232
3. Modern Cryptography Theory and Practicel, Wenbo Mao, Pearson Education.
4. Cryptography and network security, Behrouz A. Forouzan, McGraw-Hill, Inc.

I Semester	FIREWALL AND VPN SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

The main objectives of this course are toprovide students with the knowledge and skillsto design, configure, and manage firewalls and VPN solutions for protecting network infrastructure, ensuring secure remote access, and mitigating security threats.

UNIT	CONTENTS
UNIT – 1	**Fundamentals of Network Security:** Introduction, network Security, Seven Domains of a Typical IT Infrastructure, Goals of Network Security, Measure the Success of Network Security, Network Security Policies, Important, Internal and External Network Issues, Common Network Security Components Used to Mitigate Threats, TCP/IP Basics. **Network Security Threats:** Hackers and Their Motivation, Favorite Targets of Hackers, Threats from Internal Personnel and External Entities, The Hacking Process, Common IT Infrastructure, Threats Malicious Code (Malware), Advanced Persistent Threat, Session Hijacking, Spoofing, and Man-in-the-Middle Attacks, Covert Channels, Hacker Tools, Social Engineering.
UNIT – 2	Common Network Topologies and Infrastructures, Network Design Considerations, Firewall Fundamentals, Firewall Implementation, Firewall Deployment Considerations, Configuring Firewalls.
UNIT – 3	**Packet Filtering:** Introduction, Understanding Packets and Packet Filtering, Packet-Filtering Methods, Setting Specific Packet Filter Rules. **Working with Proxy Servers and Application-Level Firewalls:** Proxy Servers, Benefits of Proxy Servers, Configuring Proxy Servers, Choosing a Proxy Server, Proxy Server-Based Firewalls Compared.
UNIT – 4	VPN Fundamentals, VPN Management, VPN Technologies, VPN Implementation, Firewall Security Management, Best Practices for Network Security Management, EmergingTechnology and Regulatory Considerations.
UNIT – 5	**IDS infrastructure**: IDS Architecture, IDS/IPS Management and Architecture Issues with regard to deploying IDS/IPS systems, end point approach to security, system approach to security, IDS Interoperability models: CIDF, IDMEF, IODEF, CVE, OVAL. **IDS tools:** Snort and Bro IDS tools, NIDS Evasion, Insertion, and Checksums to confuse NID systems, Snort Fundamentals and Configuration, Snort GUIs & Sensor Management, Snort Performance, Active Response & Tagging, Snort Rules, Stimulus Response, hosts response to both normal and abnormal traffic, Advanced Snort Concepts as rule ordering and reduction of false negatives and positives. Evaluation and tuning of IDS, Cross over Rate (CER) of IDS.

Text Books:

1. Network Security, Firewall and VPNs, Third Edition. J. Michael Stewart, Denise Kinsey, 2020.
2. Guide to Firewalls and VPNs, Michael E. Whitman, Herbert J. Mattord, Andrew Green.

Reference Books:

1. Network Intrusion Detection, Stephen Narthcutt.
2. CCNP Security: Intrusion Prevention and Intrusion Detection Systems, David Burns, Odunayo Adesina, Keith Barker, Cisco Press.

I Semester	MALWARE ANALYSIS AND DETECTION	L	T	P	C
		3	0	0	3

Course Objectives:

The main objectives of this course are toenable students to understand, analyze, and detect malicious software by applying static and dynamic analysis techniques, Reverse engineering, and security tools for effective threat mitigation

UNIT	CONTENTS
UNIT – 1	**Introduction:** Types of Malware, Malware attack Life Cycle, Malware Business model, Malware Analysis setup, Operating Systems Files and File formats.
UNIT – 2	**System Fundamentals:** Virtual memory and Portable Executable Files, Windows Internals – Win32 API, Registry, Directories, Processes and services
UNIT – 3	**Malware Components**: Malware Components , Distribution mechanisms, Malware Packers, Persistence mechanism, Network Communication, Detecting Network Communication, Code Injection, Process Hollowing, API Hooking, Stealth techniques and Rootkits
UNIT – 4	**Malware Analysis and Classification:** Static Analysis, Dynamic Analysis , Memory Forensics with Volatility, Malware Payload dissection and Classification.
UNIT – 5	**Malware Reverse Engineering:** Debuggers and disassembly, Debugging for unpacking malware and code injections, Armoring Techniques Detection Engineering : Device Analysis, Anti-Virus Engines, IDS/IPS and Snort /Suricata rule writing, Malware Sandbox Internals, DBI for Malware analysis

Text Book

1. Ahijit Mohanta, Anoop Saldanha, Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware, Apress Berkeley, CA, 2020.
2. Michael Sikorski, Andrew Honig, “Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software”, No Starch Press, 2012.

I Semester	INTERNET OF THINGS SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

The main objectives of this courseare to

- Provide learners with a comprehensive understanding of IoT security principles
- Enabling students to identify vulnerabilities, design robust security architectures.
- Implement effective protection mechanisms to safeguard IoT devices, networks, and applications against potential threats.

UNIT	CONTENTS
UNIT – 1	**IoT-Security Overview:** IoT, Architecture of IoTs, IoT Security Requirements (Privacy preservation, Device security, authentication, confidentiality and integrity), Benefits & Applications of IoT, IoT Attack Surface, Industrial Standards and Evolution. Device security, Gateway security, IoT Privacy Concerns, Privacy by Design, Conducting a PrivacyImpact Assessment, Case Study: The Connected Barbie.
UNIT – 2	**IoT- Security & Vulnerability Issues:** IoT Vulnerabilities -Secret-Key, Authentication/Authorization for Smart Devices, Constrained, System Resources, DeviceHeterogeneity, Fixed Firmware. Attack Models - Layer-wise Attack model, Attacks to Sensors in IoTs, Attacks to RFIDs in IoTs, Attacks to Network Functions in IoTs, Attacks to Back-end Systems, Security in Front-end Sensors and Equipment. IoT Attacks - Side-channel Attacks, Spoofing Attack, Sniffing Attack, Rogue Devices Attack, Man-in-Middle Attack, DDoS Attack, Sensor base Attack. IoT Security Industry standards-ETSIEN 300645, ISOIEC 27400, Inductrial IoT IEC62443
UNIT – 3	**Securing Internet of Things Environments:** Networking Function Security - IoT Networking Protocols, Layering Architecture, Secure IoT Lower Layers, Secure IoT Higher Layers, Secure Communication Links in IoTs, Back-end Security- Secure Resource Management, Secure IoT Databases.
UNIT – 4	IoT Hardware -Test Device Range, Latency and Capacity, Manufacturability Test, Secure from Physical Attacks. IoT Software -Trusted IoT Application Platforms, Secure Firmware Updating, Network Enforced Policy, Secure Analytics Visibility and Control.
UNIT – 5	IoT attacks- case study: MIRAI Botnet Attack, Iran's Nuclear Facility, Stuxnet Attack, Tesla Crypto jacking Attack, The Spam-haus attack, Traffic Light Hacks, DDoS spoofing attack against American health insurance provider.

Text Books:

1. Fei HU, Security and Privacy in Internet of Things (IoTs): Models, Algorithms and Implementations, CRC Press, 2016.
2. Ollie Whitehouse, Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond ,NCC Group, 2014.

3. Russell, Brian and Drew Van Duren, Practical Internet of Things Security, Packet Publishing,2016.

I Semester	DESIGN OF SECURE OPERATING SYSTEMS	L	T	P	C
		3	0	0	3

Course Objectives:

The main objective of this course to

- Develop a comprehensive understanding of operating system security architectures and their implications for overall system security.
- Master the techniques for identifying, analyzing, and mitigating common and advanced security vulnerabilities in operating systems.
- Design and implement robust security mechanisms for critical OS components, including access control systems, memory management, and process isolation.
- Evaluate and critique existing operating system security measures, and propose improvements based on current best practices and emerging threats.
- Gain practical experience in secure OS development through hands-on projects, fostering skills in secure coding, testing, and debugging of OS-level security features.

UNIT	CONTENTS
UNIT – 1	Introduction: Secure Operating Systems, Security Goals, Trust Model, Threat Model. Access Control, Fundamentals of Protection System, Lampon's Access Matrix, Mandatory Protection System, Reference Monitor, Secure Operating System Definition, Assessment Criteria.
UNIT – 2	Multics: Multics,Multics History, The Multics System, Multics Fundamentals, Multics Security Fundamentals, Multics Protection System Models, Multics Protection System, Multics Reference Monitor, Multics Security- Multics Vulnerability Analysis.,Security in Ordinary Operating Systems, System Histories
UNIT – 3	Verifiable Security Goals, Information Flow, Information Flow Secrecy Models, Denning's Lattice Model, Bell-LaPadula Model, Information Flow Integrity Models, Biba Integrity Model, Low-Water Mark Integrity, Clark-Wilson Integrity, The Challenge of Trusted Processes, Covert Channels, Channel Types-Noninterference.
UNIT – 4	Secure Capability Systems: Secure Capability Systems, Capability System Fundamentals, Capability Security-Challenges in Secure Capability Systems, Capabilities and the ٨-Property, Capabilities and Confinement, Capabilities and Policy Changes-Building Secure Capability Systems, Enforcing the ٨-Property , Enforcing Confinement-Revoking Capabilities
UNIT – 5	Secure Virtual Machine Systems: Secure Virtual Machine Systems, Separation Kernels, VAX VMM Security Kernel,VAX VMM Design,VAX VMM Evaluation, VAX VMM Result, Security in Other Virtual Machine Systems.

Text Books:

1. Operating System Security, Trent Jaeger, Morgan & Claypool Publishers.
2. Operating System Internal and Design Principles: William Stallings.
3. The Design of the Unix Operating System, Maurice J Bach, PHI.

Reference Books:

1. Stallings, Operating Systems, Internals and Design Principles, 5th edition, Pearson Education, India.
2. Andrew S. Tanenbaum, Modern Operating Systems, 2nd edition, Prentice Hall of India.
3. Deitel & Deitel, Operating systems, 3rd edition, Pearson Education, India.

I Semester	WEB APPLICATION SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

The main objective of this course is to

- provide learners with an in-depth understanding of web application security principles
- enable them to identify vulnerabilities, assess risks, and implement secure coding practices

UNIT	CONTENTS
UNIT – 1	**Introduction:** Introduction to Web Application Security, OWASP list, Security Fundamentals: Input Validation, Attack Surface Reduction, Classifying and Prioritizing Threats. **Web Application Security Principles:** Authentication- Fundamentals, Two-factor and threefactor Authentication, Web Application Authentication, Securing password-based Authentication.
UNIT – 2	**Authorization:** Access control methods, Session Management Fundamentals. Database Security Principles: SQL Injection, Setting Database Permissions, Stored Procedure Security, Insecure Direct Object References.
UNIT – 3	**File Security Principles:** Keeping Your Secure Code Secret, Security Through Obscurity, Forceful Browsing, Directory Traversal **Secure Development Methodologies:** Holistic Approach, Industry Standard Secure Development Methodologies and Maturity Models.
UNIT – 4	Web Application Reconnaissance, Structure of a Modern Web Application: REST APIs, SPA Frameworks, Finding Sub domains, API Analysis, Identifying third party dependencies and weak points in Application Architecture, Web Application Firewall.
UNIT – 5	Vulnerability Discovery and Management, Defending Against XSS Attacks, CSRF Attacks,Defending Against XXE, Defending Against Injection and DoS, Securing Third-Party Dependencies.

Text Book

1. Bryan Sullivan, Vincent Liu, “Web Application Security”, McGraw Hill.
2. Dafydd Stuttard Marcus Pinto, “The Web Application Hacker’s Handbook”, Wiley Publishing Inc.

I Semester	HARDWARE SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

The main objective of this course is to

- Impart a comprehensive understanding of hardware security principles
- Enabling learners to identify potential threats, analyze vulnerabilities in hardware systems.
- Design robust protection mechanisms to ensure the confidentiality, integrity, and reliability of hardware-based components and architectures.

UNIT	CONTENTS
UNIT – 1	**Introduction to Hardware Security:** Overview of a Computing System, Layers of a Computing System, What Is Hardware Security, Hardware Security vs. Hardware Trust, Attacks, Vulnerabilities, and Countermeasures, Conflict Between Security and Test/Debug, Evolution of Hardware Security **A Quick Overview of Electronic Hardware**: Introduction, Nanoscale Technologies, Digital Logic, Circuit Theory, ASICs and FPGAs, Printed Circuit Board, Embedded Systems, Hardware-Firmware-Software Interaction. System on Chip (SoC) Design and Test: Introduction, The IP-Based SoC Life-Cycle, SoC Design Flow, SoC Verification Flow, SoC Test Flow, Design-for-Debug, Structured DFT Techniques Overview, At-Speed Delay Test. Printed Circuit Board (PCB): Design and Test: Introduction, Evolution of PCB and Components, PCB Life Cycle, PCB Assembly Process, PCB Design Verification
UNIT – 2	**Hardware Attacks:** Analysis, Examples, And Threat Models, Hardware Trojans: Introduction, Hardware Trojans, Hardware Trojans in FPGADesigns, Hardware Trojans Taxonomy, Trust Benchmarks Countermeasures Against Hardware Trojans. **Electronics Supply Chain:** Introduction, Modern Electronic Supply Chain, Electronic Components Supply Chain Issues, Security Concerns, Trust Issues, Potential Countermeasures. Hardware IP Piracy and Reverse Engineering: Introduction, Hardware Intellectual Property (IP), Security Issues in IP-Based SoC Design, Security Issues in FPGA.
UNIT – 3	**Side-Channel Attacks:** Introduction Background on Side-Channel Attacks Power Analysis Attacks, Electromagnetic (EM) Side-Channel Attacks Fault Injection Attacks, Timing Attacks **Test-Oriented Attacks:** Introduction, Scan-Based Attacks JTAG-Based Attacks, Hands-on Experiment: JTAG Attack. **Physical Attacks and Countermeasures:** Introduction Reverse Engineering, Probing Attack, Invasive Fault Injection Attack.

	Attacks on PCB: Security Challenges and Vulnerabilities: Introduction, PCB Security Challenges: Attacks on PCB, Attack Models. Secure Element.
UNIT – 4	**Counter Measures against Hardware Attacks** **Hardware Security Primitives:** Introduction, Preliminaries, Physical Unclonable Function, True Random Number Generator, Design for Anti-Counterfeit Existing Challenges and Attacks, Primitive Designs With Emerging Nano devices. Security and Trust Assessment, and Design for Security: Introduction, Security Assets and Attack Models, Pre-silicon Security and Trust Assessment for SoCs, Post-silicon Security and Trust Assessment for ICs, Design for Security **Hardware Obfuscation**: Introduction Overview of Obfuscation Techniques, Hardware Obfuscation Methods, Emerging Obfuscation Approaches, Use of Obfuscation AgainstTrojan Attacks.
UNIT – 5	**PCB Authentication and Integrity Validation** : PCB Authentication , Sources of PCB Signature, Signature Procurement and Authentication Methods, Signature Assessment Metric, Emerging Solutions, PCB Integrity Validation Emerging Trends In Hardware Attacks And Protections: System Level Attacks & Countermeasures, Introduction, Background on SoC Design, SoC Security Requirements, Security Policy Enforcement, Secure SoC Design Process, Threat Modeling, Hands-on Experiment: SoC Security Policy. STQC Specifications.

Text Book

1. Hardware Security: A Hands-On Learning Approach, Mark Tehranipoor and Swarup Bhunia, 2018.
2. Hardware Security: Design, Threats, and Safeguards, Debdeep Mukhopaday, Rajat Subhra Chakaraborthy, 2014

I Semester	INCIDENT RESPONSE AND THREAT INTELLIGENCE LAB	L	T	P	C
		0	0	4	2

Course Objectives:

The main objectives of this course is to

- analyze and respond to cybersecurity incidents effectively
- Understand incident response frameworks and best practices

List of Experiments	CONTENTS
EXP–1	Analyze a real-world cybercrime case and prepare a report. Include details such as the type of attack,forensics methods used, legal implications, and recommendations for preventing a similar incident
EXP–2	Develop an incident response plan for a simulated cyber incident. Outline steps for detection,containment, eradication, recovery, and lessons learned
EXP–3	Recovering deleted files and analyzing event logs from a compromised system.
EXP–4	Research and compile a threat intelligence report on a specific cyber threat. Include information onthe threat actor, tactics, techniques, and procedures (TTPs), and propose countermeasures.
EXP–5	Analyzing Indicators of Compromise (IoC) from a simulated ransomware attack.
EXP–6	Analyze a provided set of network traffic logs. Identify patterns of suspicious behavior, potentialsecurity incidents, and propose measures to enhance network security
EXP–7	PowerShell :File exercises: Get current directory, list files and folders, change directory, create a new directory
EXP–8	PowerShell: Working with services: List all services, get a specific service, start a service, stop service, change startup type.
EXP–9	PowerShell: working with variables and user input: Create a variable, display the variable name, get user input, use the variable in command

I Semester	APPLIED CRYPTOGRAPHY LAB	L	T	P	C
		0	0	4	2

Course Objectives:
The main objective of this course is to

- Defend the security attacks on information systems with secure algorithms.
- Implement advanced concepts of cryptography

UNIT	CONTENTS
Experiment-1	Write a Java program to perform addition and multiplication in a finite field with a given prime modulus. Test your program with different inputs.
Experiment-2	Write a Java program to find the greatest common divisor (GCD) of two numbers using Euclid's algorithm. Test your program with various pairs of numbers.
Experiment-3	Implement a Java program that performs arithmetic operations (addition, subtraction, multiplication, and division) within a finite field GF(p), where "p" is a prime number provided by the user. The program should prompt the user to input two elements of the finite field and then perform the specified operations. Ensure that division by zero is handled appropriately, and the results are displayed modulo the prime modulus.
Experiment-4	Write a Java program to determine whether a given number is a probable prime using Fermat's Little Theorem. Allow the user to input the number and the desired number of iterations for the test.
Experiment-5	Implement a Java program to solve a system of linear congruence's using the Chinese Remainder Theorem.
Experiment-6	Write a Java program to find the modular inverse of a number using the Extended Euclidean Algorithm.
Experiment-7	Write a Java program to calculate Euler's Totient Function (phi) for a given positive integer.
Experiment-8	Develop a Java program to generate RSA public and private key pairs.
Experiment-9	Develop a Java program to generate Elliptic Curve Cryptography (ECC) key pairs. Support different elliptic curves and key lengths
Experiment-10	Write a Java program to create and verify digital signatures using the RSA.
Experiment-11	Write a Java program to perform digital signatures using the Elliptic Curve Digital Signature Algorithm
Experiment-12	Implement a MAC algorithm that uses a cryptographic hash function (e.g., SHA256) to generate the code. Ensure that the MAC provides both message integrity and authenticity.
Experiment-13	Create a Java program that verifies the integrity of a message using a MAC.Demonstrate how an attacker attempting to modify the message would be detected.

Experiment-14	Write a Java program to demonstrate a basic timing attack on RSA decryption.
Experiment-15	Design and implement a Java program that combines digital signatures with biometric authentication for enhanced security.
Experiment-16	Write aJava program that verifies the digital signature of a given message using a public key.

Text Books:

1. Bruce Schneier, Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C.
2. Atul Kahate, ”Cryptography and Network Security”, 3rd Edition, Mc. Graw Hill.
3. Johannes A. Buchmann, “Introduction to Cryptography”, Springer-Verlag.
4. Bruce Schiener, “Applied Cryptography”, Second Edition, Wiley.

Reference Books:

1. Oded Goldreich ,”Foundations of Cryptography”, Cambridge University Press.
2. Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, “A Handbook of Applied Cryptography”, CRC Press.
3. Wembo Mao, “Modern Cryptography: Theory and Practice”, Pearson Education.

II Semester	DIGITAL FORENSICS	L	T	P	C
		3	1	0	4

Course Objectives:

The main objectives of this course are to

- Provide learners with a comprehensive understanding of digital forensics principles
- Equip them with the skills to collect, preserve, analyze, and present digital evidence in accordance with legal and ethical standards for investigating cyber incidents.

UNIT	CONTENTS
UNIT – 1	**File Systems:** FAT/NTFS file systems, Parsing FAT/NTFS file systems, Pre fetch and Super fetch, Shortcuts and Jumplists **Adversary and Malware hunting**: Malware detection, Malware analysis **Memory Forensics:** Memory acquisition, Memory analysis, memory analysis tools, Advanced Recycle bin, Server Logs, Google forensics. **Anti-Forensics Detection**: detection methodologies, Volume shadow copy, ESE databases,Advanced Registry, Thumbnail cache
UNIT – 2	**Computer Crime and legal issues:** Privacy issues, Intellectual property **Incident Response:** Threat and Adversary Intelligence, Financial crime analysis **Live/Online Forensics:** Live Digital Forensics Investigation.Tools: BitTorrent, Sleuthkit toolset, Windows Forensics. Tool chest Moot court: Moot court Case
UNIT – 3	**Networking overview:** Windows Networks, Users and Groups, Introduction to NetworkInvestigations **Windows and Linux servers:** Server roles, Server analysis, Windows Registry, Event logs **Linux Forensics:** Linux File systems, Linux server configurations, Linux artifacts, Apache server forensics, LAMP forensics, SMB and Linux file shares.
UNIT – 4	**IIS and Microsoft Exchange server:** IIS server, Mail server, Windows rootkits, Compromised server analysis. **SQL server and Data bases:** Microsoft SQL server, SQL server permission and encryption,SQL server Forensics Acquisition and analysis: SQL server forensics and traditional windows forensics, SQL server artifacts, Resident and non-resident artifact‟s Collecting SQL data bases, Creating an analysis database, Importing evidence, Activity Reconstruction, Data recovery, SQL server rootkits.
UNIT – 5	**Network Traffic Analysis:** Network addressing, DNS poisoning, ARP table analysis, DHCPanalysis, Wire shark analysis. **Network Device Forensics:** management of switches and routers, Diagramming physicalnetworks, Securing and isolating physical devices, Collecting Volatile/Non-volatile evidences from the routers, Volatile/Non-volatile.

Text Book:

1. H. Carvey, “Windows Forensics Analysis DVD Toolkit”, Syngress publishers.
2. S. Anson, S. Bunting, R. Johnson, S. Perason, “Mastering Windows Network Forensics and Investigations”, Sybex publishers
3. K. Fowler, “SQL Server Forensic Analysis”, Addison Wesley.
4. K. Mandia, M. Pepe , J. Luttgens, “Incident Response & Computer Forensics”, 3rd Edition.

Reference Books:

1. M.H. Ligh, A. Case, J. Levy, A. waters, “The art of memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory”, Wiley.
2. S. Davidoff, J. Ham, “Network Forensics: Tracking Hackers through Cyberspace”, Prentice Hall.

II Semester	SECURE SYSTEM DEVELOPMENT	L	T	P	C
		3	1	0	4

Course Objectives:

The main objectives of this courseare to

- Provide learners with a thorough understanding of secure software and system development principles.
- Enabling learners to design, implement, and maintain systems that incorporate security controls throughout the development lifecycle to protect against vulnerabilities and threats.

UNIT	CONTENTS
UNIT – 1	**Introduction:** Intersection of Security and Reliability, Understanding adversaries. **Designing Systems:** Case Study Safe Proxies, Design Tradeoffs, Design for Least Privilege.
UNIT – 2	Design for Understandability, Design for Changing Landscape, Design for Resilience, Design for recovery, Mitigating Denial-of-service Attacks.
UNIT – 3	**Implementing Systems:** Designing, Implementing and Maintaining a publicly Trusted CA, Writing Code and Testing Code
UNIT – 4	Deploying Code and Investigating Systems. Maintaining Systems: Disaster Planning, Crisis Management , Recovery and Aftermath.
UNIT – 5	**Organization and Culture:** Case study: Chrome Security Team, Understanding Roles and Responsibilities, Building a Culture of Security and Reliability.

Text Book:

1. Ana Oprea, Betsy Beyer, Paul Blankinship Heather Adkins, Piotr Lewandowski, Adam Stubblefield, “Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems”, O′Reilly; Edition, 2020.
2. Julia H Allen, Sean J Barnum, Robert J Ellison, Gary McGraw, Nancy R Mead,
3. “Software Security Engineering: A Guide for Project Managers”, Addison Wesley.

IISemester	PENETRATION TESTING AND VULNERABILITY ANALYSIS	L	T	P	C
		3	1	0	4

Course Objectives:
The course is taught with the objectives of enabling the student to:

- Learn the theoretical basis for cyber threats and penetration testing phases and vulnerabilities
- Perform protocol analysis using packet captures and analysis data using a sniffer
- Apply testing methodologies using tools such as Wireshark, Nmap, Snort, Metasploit and related applications and platforms.

UNIT	CONTENTS
UNIT – 1	Introduction, Terminologies, Categories of Penetration Testing, Phases of Penetration Test, Penetration Testing Reports, Information Gathering Techniques, Active, Passive and Sources of Information Gathering, Approaches and Tools, Traceroutes, Neotrace, Whatweb, Netcraft, Xcode Exploit Scanner and NSlookup. Target Enumeration and Port scanning techniques, Host discovery, Scanning for open ports and services, Port scanning.
UNIT – 2	Vulnerability Scanner Function, pros and cons, Vulnerability Assessment with NMAP, Testing SCADA environment with NMAP, Nessus, Vulnerability Scanner, Safe check, Silent dependencies, Port Range Vulnerability Data Resources, Network Sniffing, Shodan
UNIT – 3	Network Sniffing, Remote Exploitation, Capturing traffic: Networking for Capturing Traffic, Using Wireshark, ARP Cache Poisoning, DNS Cache Poisoning, SSL Attacks, SSL Stripping, Exploitation
UNIT – 4	Password Attacks: Password Management, Online Password Attacks, Offline Password Attacks. Client Side Exploitation and Post Exploitation
UNIT – 5	Windows Exploit Development Basics, Wireless Hacking and Attacks, Web hacking,Mobile Hacking

Text Books:

1. Rafay Baloch, “Ethical Hacking and Penetration Testing Guide”, CRC Press, 2015.
2. Georgia Weidman, “Penetration Testing: A Hands-On Introduction to Hacking”, 2014.
3. Wil Allsopp, “Advanced Penetration Testing, Wiley, 2017.

IISemester	BLOCKCHAIN APPLICATION SECURITY AND INVESTIGATION	L	T	P	C
		3	0	0	3

Course Objectives:
The main objectives of this course are to

- Explain the fundamental concepts of cryptography and crypto currencies
- Understand and apply enterprise blockchain solutions
- Explore distributed consensus mechanisms
- Develop skills in blockchain transaction analysis

UNIT	CONTENTS
UNIT – 1	Cryptography & Crypto Currency Fundamentals,Decentralized Systems (Block chain and derivatives) Fundamentals and Challenges,Introduction to Enterprise Block chain Solutions. Ethereum & Quorum Basics, Introduction toDeterministic Programming (Solidity Truffle).
UNIT – 2	Ethereum Mechanics & Solidity, Team Project Proposal Presentations, Security and Issues,Cryptographic Tokens & Token Economy.
UNIT – 3	Security Philosophy & Block chain usage in Cyber Security,Distributed consensus, distributed ledgers, P2P Networking Foundations, Gossip and decentralized, collaboration.
UNIT – 4	Emerging Decentralized solutions for the Data Science, Decentralized storage, content distribution,Decentralized identity, Trust and reputation. Anonymous Communication.Understanding the cybersecurity aspects of blockchain, including potential vulnerabilities, attacks, and defense strategies.
UNIT – 5	Using data analysis techniques to track transactions, identify patterns, and detect suspicious activity on the blockchain, Learning about specialized tools and techniques for investigating blockchain-related crimes, including tracing transactions and identifying malicious actors.

Text Books:

1. Karaarslan, E., Konacaklı, E. "Data Storage in the Decentralized World: Blockchain and Derivatives".
2. Kitap Bölümü. "Who Run The World: DATA" Kitabı. Istanbul University Press, 2020
3. Karaarslan E, Konacaklı E. "Decentralized solutions for data collection and privacy in healthcare",
4. Karaarslan, E., Aydin, D, "An AI Based Decision Support and Resource Management System for COVID-19 Pandemic", "DS for COVID-19" kitabı, Elsevier, 2021.

Reference Books:

1. Karaarslan E., "Use of Blockchain Technology in the Health Sector" (Turkish), "Advanced Technology Applications in Health" Book, Nobel Publishing House, 2019
2. Kravchenko P., Skriabin B., Kurbatov O., Dubinina O. (2020). Blockchain And Decentralized Systems. Volume 1-3.

IISemester	POST QUANTUM CRYPTOGRAPHY	L	T	P	C
		3	0	0	3

Course Objectives:
The main objectives of this course are to

- Provide learners with an in-depth understanding of cryptographic techniques resistant to quantum computing attacks.
- Enable them to analyze post-quantum algorithms.
- Evaluate security and performance, and implement suitable solutions for future-proof secure communication systems.

UNIT	CONTENTS
UNIT – 1	Introduction to post-quantum cryptography: Introduction and challenges, Quantum computing: Classical and quantum Computing, Computation model, The quantum Fourier transform, The hidden subgroup problem, Search algorithms
UNIT – 2	Hash-based Digital Signature Schemes: Hash based one-time signature schemes, Merkle‟ tree authentication scheme, One-time key-pair generation using an PRNG, Authentication path computation, Tree chaining, Distributed signature generation, Security of the Merkle Signature Scheme
UNIT – 3	Code-based cryptography: Introduction, Cryptosystems, The security of computing syndromes as one-way function, Codes and structures, Practical aspects
UNIT – 4	Lattice-based Cryptography: Introduction, Preliminaries, Finding Short Vectors in Random q-ary Lattices, Hash Functions, Public Key Encryption Schemes, Digital Signature Schemes, Other Cryptographic Primitives.
UNIT – 5	Multivariate Public Key Cryptography: Introduction, The Basics of Multivariate PKCs, Examples of Multivariate PKCs, Basic Constructions and Variations, Standard Attacks. Isogeney based Cryptography: Super sigular Isogeny based Key Exchange (SIKE), Digital Signature Algorithm based on Isogeny

Text Book

1. Daniel J. Bernstein · Johannes Buchmann Erik Dahmen, “Post-Quantum Cryptography”, Springer Verilag, 2009.
2. NIST Post Quantum Standardization- Specification document of the post-quantum secure Algorithms
3. https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions

II Semester	ARTIFICIAL INTELLIGENCE & MACHINE LEARNING IN CYBER SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:
The main objectives of this courseare to

- Provide learners with a comprehensive understanding of AI and ML techniques in the context of cyber security.
- Enable them to design, develop, and apply intelligent models for threat detection, anomaly analysis, malware classification, and automated incident response.

UNIT	CONTENTS
UNIT – 1	Introduction to AI for Cyber security, Applying AI in cyber security, The evolution from expert systems to data mining and AI, The different forms of automated learning, The characteristics of algorithm training and optimization, Introducing AI in the context of cyber security
UNIT – 2	AI for Cyber security, Arsenal Classification, Regression, Dimensionality reduction, Clustering, Speech recognition, Video anomaly detection, Natural language processing (NLP), Large-scale image processing, Social media analysis, Detecting Cyber security Threats with AI, How to detect spam with Perceptrons, Image spam detection with Support Vector Machines (SVMs), Phishing detection with logistic regression and decision trees, Spam detection with Naive Bayes, Spam detection adopting NLP.
UNIT – 3	Basics of Machine Learning in Cyber security, Delving into machine learning in the cyber security world, Different types of machine learning systems, Different data preparationtechniques, Machine learning architecture, statistical models and machine learning models, Model tuning to ensure model performance and accuracy, Machine learning tools, Time Series Analysis and Ensemble Modeling, Time series and its different classes, Timeseries decomposition, Analysis of time series in cyber security, Prediction of DDoS attack, Ensemble learning methods and voting ensemble methods to detect cyber-attacks.
UNIT – 4	Segregating Legitimate and Lousy URLs, Understanding URLs and how they fit in the internet address scheme, Introducing malicious URLs, Looking at the different waysmalicious URLs propagate, Using heuristics to detect malicious URLs, Using machinelearning to detect malicious URLs Knocking Down CAPTCHAs Characteristics of CAPTCHAs, Using artificial intelligence to crack CAPTCHAs, Types of CAPTCHA, Solving CAPTCHAs with neural networks.
UNIT – 5	Fraud Prevention with Cloud AI Solutions, How to leverage machine learning (ML) algorithms for fraud detection, How bagging and boosting techniques can improve an algorithm's effectiveness, How to analyze data with IBM Watson and Jupyter Notebook, Using Data Science to Catch Email Fraud and Spam, Efficient Network Anomaly Detection Using k-means, Fraudulent

	emails and spoofs, Types of email fraud, Spamdetection using the Naive Bayes algorithm, Featurization techniques that convert text-based emails into numeric values, Spam detection with logistic regression

Text Books:

1. Alessandro Parisi, Hands-On Artificial Intelligence for Cyber security: Implementsmart AI systems for preventing cyber-attacks and detecting threats and network anomalies, Packt Publication, 2019.
2. Clarence Chio and David Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms O‟REILLY Publications, 2018.
3. McKinney, W Brij B. Gupta and Quan Z. Sheng, Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices (Cyber Ecosystem and Security), CRC Press Publication, 2019.

II Semester	SECURE DATABASE APPLICATION DEVELOPMENT	L	T	P	C
		3	0	0	3

Course Objectives:
The main objectives of this course are to

- Provide learners with a comprehensive understanding of database security principles
- Enable them to design and implement mechanisms for protecting data confidentiality, integrity, and availability, while mitigating threats, vulnerabilities, and unauthorized access.

UNIT	CONTENTS
UNIT – 1	**Security Architecture:** Introduction, Security, Information Systems, Database management systems, Information security, Information security Architecture, database security, Asset types and their value, Security methods. **Operating System Security Fundamentals:** Introduction, operating systems overview, security environment, components, Authentication methods, user administration, password policies, Vulnerabilities of operating systems, E-Mail security.
UNIT – 2	**Administration of Users:** Introduction, user authentication, operating system authentication, creating/removing/modifying users, default/remote users, Database links, Linked servers, remote servers. **Profiles, Password Policies, Privileges, and Roles:** Introduction, Defining and using profiles, Designing and implementing password policies, Granting and revoking user privileges, creating, Assigning and revoking user roles.
UNIT – 3	**Database Application Security Models:**Introduction, Types of users, security models, application types, application security models and Data encryption.
UNIT – 4	**Virtual Private Databases (VPD):** Introduction, Overview, implementing a VPD using views and application context. Implementing oracle VPD, Viewing VPD policies and application context using: data dictionary, policy manager, implementing row and column level security with SQL server.
UNIT – 5	**Database Auditing Models, Application Data Auditing:** Database Auditing Models: Introduction, Auditing overview, environment, process, objectives, classification and types, benefits and side effects of auditing. **Application Data Auditing:** Introduction, DML auction auditing architecture. Triggers, fine grained auditing, DML statement audit trail and auditing application errors with Oracle.

Text Book:

1. Database Security and Auditing, Hassan Afyouni, Cengage Learning.
2. Database Security, S. Castano, M. Fugini, G. Martella, P. Samarati, Addison-Wesley.
3. Implementing Database Security and Auditing, Ron Ben Natan: Elsevier, Indian reprint.

Reference Books:

1. Database Security, Castano, Fugini, Addison Wesley

2. The security Audit and control of Databases, Clark, Holloway, List, UK:Ashgate.
3. Security and Audit of Database System, Douglas, Blackwell(UK)

IISemester	CLOUD SECURITY	L	T	P	C
		3	0	0	3

Course Objectives:

The course is taught with the objectives of enabling the student to:

1. Learn the concepts of distributed systems, algorithms and protocols
2. Understand the security in the cloud-infrastructure and analyze various attacks on cloud computing
3. Learn various cloud services and key management problems in cloud storage

UNIT	CONTENTS
UNIT – 1	**Cloud Computing Architectural Framework:** Cloud Benefits, Business scenarios, Cloud Computing Evolution, cloud vocabulary, Essential Characteristics of Cloud Computing, Cloud deployment models, Cloud Service Models, Multi- Tenancy, Approaches to create a barrier between the Tenants, cloud computing vendors, Cloud Computing threats, Cloud Reference Model, The Cloud Cube Model, Security for Cloud Computing, How Security Gets Integrated
UNIT – 2	**Compliance and Audit:** Cloud customer responsibilities, Compliance and Audit Security Recommendations. Portability and Interoperability: Changing providers reasons, Changingproviders expectations, Recommendations all cloud solutions, IaaS Cloud Solutions, PaaS Cloud Solutions, SaaS Cloud Solutions.
UNIT – 3	Traditional Security, Business Continuity, Disaster Recovery, Risk of insider abuse, Security baseline, Customers actions, Contract, Documentation, Recovery Time Objectives (RTOs), Customers responsibility, Vendor Security Process (VSP).
UNIT – 4	Data Center Operations, Security challenge, Implement Five Principal Characteristics of Cloud Computing, Data center Security Recommendations. Encryption and Key Management: Encryption for Confidentiality and Integrity, Encrypting data at rest, Key Management Lifecycle, Cloud Encryption Standards, Recommendations
UNIT – 5	Identity and Access Management in the cloud, Identity and Access Management functions, Identity and Access Management (IAM) Model, Identity Federation, Identity Provisioning Recommendations, Authentication for SaaS and Paas customers, Authentication for IaaS customers, Introducing Identity Services, Enterprise Architecture with IDaaS, IDaaS Security Recommendations. **Virtualization:** Hardware Virtualization, Software Virtualization, Memory Virtualization, Storage Virtualization, Data Virtualization, Network Virtualization, Virtualization Security Recommendations.

Text Books:

1. Practical Cloud Security: A Guide for Secure Design and Deployment, O'reilley Chris Dotson.
2. Cloud Computing Security: Foundations and Challenges, 2nd Edition

3. Securing The Cloud: Cloud Computing Security Techniques and Tactics by Vic (J.R.) Winkler, 2019

Reference Books:

1. Ronald L. Krutz, Russell Dean Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing.

IISemester	CYBER LAWS AND SECURITY POLICIES	L	T	P	C
		3	0	0	3

Course Objectives:

The main objectives of this courseare to

- Understand the purpose of computer infection program.
- Test and exploit various malware in open source environment.
- Understand the Reverse Engineering (RE) Methodology
- Disassemble products and specify the interactions between its subsystems and their functionality.

UNIT	CONTENTS
UNIT – 1	**Introduction to Computer Security-** Definition, Threats to security, Government requirements, Information Protection and Access Controls, Computer security efforts, Standards, Computer Security mandates and legislation, Privacy considerations, International security activity.
UNIT – 2	**Secure System Planning and administration-** Introduction to the orange book, Security policy requirements, accountability, assurance and documentation requirements, and Network Security, The Redbook and Government network evaluations.
UNIT – 3	**Information security policies and procedures**: Corporate policies, Tier 1, Tier2 and Tier3 policies, process management, planning and preparation, developing policies, asset classification policy, developing standards.
UNIT – 4	**Information security**-fundamentals, Employee responsibilities, information classification, Information handling, Tools of information security, Information processing, secure program administration
UNIT – 5	**Organizational and Human Security**-Adoption of Information Security Management Standards, Human Factors in Security, Role of information security professionals, IT Act- Structure of IT Act, Common cyber crime scenarios and Applicability of Legal sections, Case studies as per selected IT Act sections.

Text Books:

1. Computer Security Basics (Paperback), 2nd Edition, Debby Russell and Sr. G.T Gangemi, O'Reilly Media.
2. Information Security policies and procedures: A Practitioner's Reference‖, 2nd Edition, Thomas R. Peltier Prentice Hall.

Reference Books:

1. Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions‖, Kenneth J. Knapp, IGI Global.

IISemester	DIGITAL FORENSICS LAB	L	T	P	C
		0	0	4	2

Course Objectives:
The main objectives of this course are to

- Make familiarize students with various forensic tools and techniques used for the collection, preservation, analysis, and presentation of digital evidence.
- Develop students' practical skills in conducting forensic investigations through hands-on experience with leading forensic software and hardware tools.
- Provide an understanding of legal, ethical, and procedural aspects associated with forensic investigations and digital evidence handling.

List of Experiments	CONTENTS
EXP– 1	Study of Computer Forensics and different tools used for forensic investigation
EXP –2	How to Recover Deleted Files using Forensics Tools
EXP –3	How to make the forensic image of the hard drive using EnCase Forensics
EXP –4	How to Collect Email Evidence in Victim PC
EXP –5	How to Extracting Browser Artifacts
EXP –6	Find Last Connected USB on your system (USB Forensics)
EXP –7	Live Forensics Case Investigation using Autopsy
EXP –8	Capturing and analyzing network packets using Wireshark
EXP –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.
EXP –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
EXP –11	Email Forensics • Mail Service Providers • Email protocols • Recovering emails • Analyzing email header
EXP –12	Analyzing data of android mobile using MOBILedit

IISemester	PENETRATION TESTING & VULNERABILITY ANALYSIS LAB	L	T	P	C
		0	0	4	2

Course Objectives:
The main objectives of this course are to

- Provide practical knowledge of penetration testing methodologies and vulnerability assessment techniques.
- Develop skills in identifying, exploiting, and analyzing security weaknesses in systems, networks, and applications.
- Enable learners to recommend effective remediation strategies to enhance overall security posture.

List of Experiments	CONTENTS
EXP–1	Implement penetration testing and phases of penetrationtesting
EXP–2	Make use of different types of tools available in kali and parrotO.S
EXP–3	Practice different SQL injection attacks
EXP–4	Implement and use GHDBC and Microsoft Vulnerabilities (Common CVE)
EXP–5	Implement Exploit insecure file handling, upload web shells, deface using upload filemechanism
EXP–6	Perform XSS attacks on client side application
EXP–7	Implement a case on actions on-behalf users by CSRF, Test websites for Clickjacking
EXP–8	Implement port scanning by using NMAP and other tools to find the openports
EXP–9	Text for wireshark and tcp dumps to analyze various types of packets
EXP–10	Implement Password attacks with methods like Dictionary Files - Key-space Brute Force - Pwdump and Fgdump - Windows Credential Editor (WCE- Exercises - Password Profiling - Password Mutating
EXP–11	Implement metasploit frameworks
EXP–12	Implement Trojan horse root kits backdoors
EXP–13	Practice ARP spoofing and buffer overflow exploitation with ETERCAP ANDSHELL'S
EXP–14	Perform Port Redirection, SSL Encapsulation - Stunnel, HTTP CONNECT Tunneling, Proxy Tunnel, SSH Tunneling.

List of open Source software/learning Websites:

1. https://www.hackthebox.eu/
2. https://practicalpentestlabs.com/
3. https://pentesterlab.com

IIISemester	RESEARCH METHODOLOGY AND IPR	L	T	P	C
		3	0	0	3

Course Objectives:
The main objectives of the course are to make students to

- Understand the concept of a research problem
- Develop skills in the research process and learn effective literature review techniques
- Explore the nature and significance of intellectual property (IP)

UNIT	CONTENTS
UNIT – 1	Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem. Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations
UNIT – 2	Effective literature studies approaches, analysis Plagiarism, Research ethics, Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee
UNIT – 3	Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT
UNIT – 4	Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications.
UNIT – 5	New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs

Reference Books:

1. Stuart Melville, Wayne Goddard, “Research methodology: an introduction for science & engineering students’”
2. Wayne Goddard, Stuart Melville, “Research Methodology: An Introduction”
3. Ranjit Kumar, 2nd Edition, “Research Methodology: A Step by Step Guide for beginners”
4. Halbert, “Resisting Intellectual Property”, Taylor & Francis Ltd.
5. Mayall, “Industrial Design”, McGraw Hill.
6. Niebel, “Product Design”, McGraw Hill.
7. Asimov, “Introduction to Design”, Prentice Hall.