

**ANNA UNIVERSITY, CHENNAI**  
**NON- AUTONOMOUS COLLEGES**  
**AFFILIATED TO ANNA UNIVERSITY**  
**M.E. BIOMETRICS AND CYBERSECURITY**  
**REGULATIONS 2025**

**PROGRAMME OUTCOMES (POs):**

<b>PO</b>	<b>Programme Outcomes</b>
<b>PO1</b>	An ability to independently carry out research /investigation and development work to solve practical problems
<b>PO2</b>	An ability to write and present a substantial technical report/document.
<b>PO3</b>	Students should be able to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

**PROGRAMME SPECIFIC OUTCOMES:**

- PSO1:** Advanced Biometric System Design and Implementation Design, develop, evaluate and conduct research on biometric systems such as fingerprint, iris, face, and multimodal authentication systems using advanced image processing, pattern recognition, and machine learning techniques.
- PSO2:** Cybersecurity Threat Analysis and Risk Mitigation: Analyze, detect, and prevent cybersecurity threats and attacks by applying cryptographic algorithms, secure communication protocols, and digital forensics techniques for robust security solutions.



# ANNA UNIVERSITY, CHENNAI

## POSTGRADUATE CURRICULUM (NON-AUTONOMOUS AFFILIATED INSTITUTIONS)

**Programme:** M.E. Biometrics and Cybersecurity

**Regulations:** 2025

### Abbreviations:

**BS** – Basic Science (Mathematics)

**L** – Laboratory Course

**ES** – Engineering Science (Programme Core (**PC**),  
Programme Elective (**PE**))

**T** – Theory

**SD** – Skill Development

**LIT** – Laboratory Integrated Theory

**SL** – Self Learning

**PW** – Project Work

**TCP** – Total Contact Period(s)

### Semester I

S. No.	Course Code	Course Title	Type	Periods per week			TCP	Credits	Category
				L	T	P			
1.	MA25C07	Advanced Mathematical Methods (CSIE)	T	3	1	0	4	4	BS
2.	CP25C01	Advanced Data Structures and Algorithms	LIT	3	0	4	7	5	ES (PC)
3.	BC25101	Network Design and Programming	LIT	3	0	0	3	3	ES (PC)
4.	CP25C03	Advanced Operating Systems	T	3	0	0	3	3	ES (PC)
5.	CP25C04	Advanced Compiler Design	T	3	0	0	3	3	ES (PC)
6.	BC25102	Technical Seminar	-	0	0	2	2	1	SD
<b>Total Credits</b>							<b>22</b>	<b>19</b>	

### Semester II

S. No.	Course Code	Course Title	Type	Periods per week			TCP	Credits	Category
				L	T	P			
1.	BC25201	Biometric Data Processing	LIT	3	0	4	7	5	ES (PC)
2.	BC25202	Applied Cryptography	LIT	3	0	2	5	4	ES (PC)
3.	CP25C07	Quantum Computing	T	2	0	0	2	2	ES (PC)
4.		Programme Elective I	T	3	0	0	3	3	ES (PE)
5.		Industry-Oriented Course I	-	1	0	0	1	1	SD
6.	BC25203	Industrial Training	-	-	-	-	-	2	SD
7.		Self-Learning Course	-	-	-	-	-	1	-
<b>Total Credits</b>							<b>18</b>	<b>18</b>	

### Semester III

S. No.	Course Code	Course Title	Type	Periods per week			TCP	Credits	Category
				L	T	P			
1.		Programme Elective II	T	3	0	0	3	3	ES (PE)
2.		Programme Elective III	T	3	0	0	3	3	ES (PE)
3.		Programme Elective IV	T	3	0	0	3	3	ES (PE)
4.		Programme Elective V	T	3	0	0	3	3	ES (PE)
5.		Industry-Oriented Course II	--	1	0	0	1	1	SD
6.	BC25301	Project Work I	-	0	0	12	12	6	SD
<b>Total Credits</b>							<b>25</b>	<b>19</b>	

### Semester IV

S. No.	Course Code	Course Title	Type	Periods per week			TCP	Credits	Category
				L	T	P			
1.	BC25401	Project Work II	-	0	0	24	24	12	SD
<b>Total Credits</b>							<b>24</b>	<b>12</b>	

**PROGRAMME ELECTIVE COURSES (PE)**

S. No.	Course Code	Course Title	Periods per week			TCP	Credits
			L	T	P		
1.	BC25001	Principles of Secure Coding	3	0	0	3	3
2.	BC25002	AI for Cybersecurity	3	0	0	3	3
3.	BC25003	Operating System Security	3	0	0	3	3
4.	BC25004	Security Practices	3	0	0	3	3
5.	BC25005	Cybercrime Investigations	3	0	0	3	3
6.	BC25006	Mobile and Digital Forensics	3	0	0	3	3
7.	BC25007	Firewall and VPN Security	3	0	0	3	3
8.	BC25008	Biometric Security	3	0	0	3	3
9.	BC25009	Cyber Security Managements and Cyber Laws	3	0	0	3	3
10.	CP25C12	Quantum Cryptography	3	0	0	3	3
11.	BC25010	Data Analytics and Risk monitoring	3	0	0	3	3
12.	BC25011	Cryptanalysis	3	0	0	3	3
13.	IF25C04	Block chain Technologies	3	0	0	3	3
14.	BC25012	Cyber Forensics and Investigation	3	0	0	3	3
15.	BC25013	Wireless Security	3	0	0	3	3
16.	BC25014	Malware Analysis	3	0	0	3	3
17.	BC25015	Ethical Hacking and Network defence	3	0	0	3	3
18.	BC25016	E-Commerce Security	3	0	0	3	3
19.	CP25C24	Vibe Coding	3	0	0	3	3
20.	CP25C20	Agentic AI	3	0	0	3	3

MA25C07	Advanced Mathematical Methods (CSIE)	L	T	P	C
		3	1	0	4
<b>Course Objectives:</b>					
<ul style="list-style-type: none"> <li>• Develop an in-depth understanding of advanced concepts in linear algebra, multivariate analysis, and number theory for computer science applications.</li> <li>• Apply mathematical tools such as eigenvalue decomposition, SVD, and multivariate statistical methods to real-world computing and data-driven problems.</li> <li>• Analyze and implement number-theoretic techniques for cryptography, security, and algorithmic problem-solving in computer science.</li> </ul>					
<b>Linear Algebra:</b> Vector spaces, norms, Inner Products, Eigenvalues using QR transformations, QR factorization, generalized eigenvectors, Canonical forms, singular value decomposition and applications, pseudo inverse, least square approximations.					
<b>Multivariate Analysis:</b> Random vectors and matrices, Mean vectors and covariance matrices, Multivariate normal density and its properties, Principal components, Population principal components, Principal components from standardized variables.					
<b>Elementary Number Theory:</b> The division algorithm, Divisibility and the Euclidean algorithm, The fundamental theorem of arithmetic, Modular arithmetic and basic properties of congruences; Principles of mathematical induction and well ordering principle. Primality Testing algorithms, Chinese Remainder Theorem, Quadratic Congruence.					
<b>Advanced Number Theory:</b> Advanced Number Theory, Primality Testing algorithms, Chinese Remainder Theorem, Quadratic Congruence, Discrete Logarithm, Factorization Methods, Side Channel Attacks, Shannon Theory, Perfect Secrecy, Semantic Security.					
<b>Weightage:</b> Continuous Assessment: 40%, End Semester Examinations: 60%.					
<b>Assessment Methodology:</b> Assignments (15), Quiz (10), Virtual Demo (20), Flipped Class Room (10), Review of Gate and IES Questions (25), Project (20).					
<b>References:</b>					
<ol style="list-style-type: none"> <li>1. Gilbert Strang, Linear Algebra and Its Applications, Cengage Learning.</li> <li>2. Richard A. Johnson &amp; Dean W. Wichern, Applied Multivariate Statistical Analysis, Pearson.</li> <li>3. Neal Koblitz, A Course in Number Theory and Cryptography, Springer.</li> <li>4. Victor Shoup, A Computational Introduction to Number Theory and Algebra, Cambridge University Press.</li> </ol>					
<b>E-resources:</b>					
<ol style="list-style-type: none"> <li>1. <a href="https://ocw.mit.edu/courses/18-06-linear-algebra">https://ocw.mit.edu/courses/18-06-linear-algebra</a></li> <li>2. <a href="https://nptel.ac.in/courses/111105041">https://nptel.ac.in/courses/111105041</a></li> <li>3. <a href="https://crypto.stanford.edu/pbc/notes/numbertheory">https://crypto.stanford.edu/pbc/notes/numbertheory</a></li> </ol>					

<b>CO</b>	<b>Description of CO</b>	<b>PO</b>	<b>PSO</b>
<b>CO1</b>	Describe the advanced mathematical concepts, techniques, and tools essential for problem solving in computing and information engineering.	--	--
<b>CO2</b>	<b>Analyze</b> mathematical models, transformations, and numerical methods to understand their behavior and applicability to engineering problems.	PO1 (3)	PSO1 (3)
<b>CO3</b>	<b>Evaluate</b> solutions obtained using analytical and numerical approaches to determine accuracy, stability, and efficiency.	PO3 (2)	PSO2 (2)
<b>CO4</b>	<b>Design</b> mathematical formulations and computational strategies for solving complex real-world problems in computer science and information engineering.	PO2 (1)	PSO1 (3)

CP25C01	Advanced Data Structures and Algorithms	L	T	P	C
		3	0	4	5

**Course Objectives:**

1. To explore advanced linear, tree, and graph data structures and their applications.
2. To design efficient algorithms using appropriate algorithmic paradigms.
3. To evaluate computational complexity and identify tractable vs. intractable problems.

**Linear Data Structures and Memory Optimization:** Advanced arrays: Sparse arrays, dynamic arrays, cache-aware structures, Linked lists: Skip lists, unrolled linked lists, XOR linked lists, Stacks and Queues: Priority queues, double-ended queues, circular buffers, Hashing: Perfect hashing, cuckoo hashing, extendible hashing.

**Practical:**

- Implement skip lists and measure performance compared with balanced BST.
- Experiment with cache-aware data structures and analyze memory utilization.

**Advanced Tree Data Structures:** Balanced Trees: AVL, Red-Black Trees, Splay Trees, Treaps, Multi-way Trees: B-Trees, B+ Trees, R-Trees, Segment Trees, Fenwick Trees, Suffix Trees and Tries for string processing, Applications in indexing, text retrieval, computational geometry.

**Practical:**

- Implement B+ tree for database indexing use-case.
- Design a suffix tree-based algorithm for DNA sequence matching.

**Graph Data Structures and Algorithms:** Representation: Adjacency list/matrix, incidence matrix, compressed storage, Traversals: DFS, BFS with applications, Shortest Path Algorithms: Dijkstra, Bellman-Ford, Floyd-Warshall, Johnson’s algorithm, Minimum Spanning Trees: Prim’s, Kruskal’s, Borůvka’s algorithm, Network Flow Algorithms: Ford-Fulkerson, Edmonds-Karp, Push-Relabel.

**Practical:**

- Implement Johnson’s algorithm for sparse graph shortest paths.
- Demonstration of Maximum flow in traffic or network routing simulation.

**Algorithm Design and Paradigms:** Divide and Conquer: Karatsuba’s multiplication, Strassen’s algorithm, Greedy Methods: Huffman coding, interval scheduling, set cover approximation, Dynamic Programming: Matrix chain multiplication, Floyd-Warshall, knapsack variants, Backtracking and Branch-and-Bound, Randomized Algorithms and Probabilistic Analysis.

**Practical:**

- Implement Strassen’s algorithm and compare with naive matrix multiplication.
- Develop a randomized algorithm for primality testing (Miller–Rabin).

**Computational Complexity and Approximation Algorithms:** Complexity Classes: P, NP, NP-Complete, NP-Hard, Reductions: Polynomial-time reductions, Cook-Levin theorem (overview), Approximation Algorithms: Vertex cover, set cover, TSP, k-center problem, Heuristic Algorithms: Local search, simulated annealing, genetic algorithms.

**Practical:**

- Implement approximation algorithm for vertex cover.
- Complexity analysis of a chosen NP-hard problem and implement a heuristic.

**Advanced Topics and Emerging Trends:** Randomized Algorithms – Monte Carlo Algorithms, Parallel and Distributed Algorithms – PRAM Model, Divide and Conquer in Parallel, Load Balancing, Streaming Algorithms – Data Stream Models, Sketching and Sampling, Frequency Moments, Advanced String Matching – Suffix Trees, Suffix Arrays, Pattern Matching in Linear Time.

**Practical:**

- Implement randomized and streaming algorithms on real-world datasets.
- Design of parallel and distributed algorithms.

**Weightage:** Continuous Assessment: 50%, End Semester Examinations: 50%

**Assessment Methodology:** Assignments (15), Quiz (10), Virtual Demo (20), Flipped Class Room (10), Review of Gate and IES Questions (25), Project (20)

**References:**

1. Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2009). Introduction to algorithms. MIT Press.
2. La Rocca, M. (2021). Advanced algorithms and data structures. Manning Publications.
3. Goodrich, M. T., Tamassia, R., & Mount, D. M. (2011). Data structures and algorithms in C++. John Wiley & Sons, Inc.
4. Weiss, M. A. (2014). Data structures and algorithm analysis in C++. Pearson Education.
5. Drozdek, A. (2013). Data structures and algorithms in C++. Cengage Publications.

**E-resources:**

1. <https://www.theiotacademy.co/blog/data-structures-and-algorithms-in-c/>
2. [https://github.com/afrid18/Data\\_structures\\_and\\_algorithms\\_in\\_cpp](https://github.com/afrid18/Data_structures_and_algorithms_in_cpp)
3. <https://www.udemy.com/course/introduction-to-algorithms-and-data-structures-in-c/?srsltid=AfmBOorEZlkgV7QzaEh6lqzAaKLjC-lpFU1NGgWFOHMLhOos-uDVKjCK>

	Description of CO	PO	PSO
CO1	Describe data structures and implement algorithmic solutions for complex computational problems.	--	--
CO2	Analyze the time complexity and efficiency of algorithms for various computing problems.	PO1(3)	PSO1(3)
CO3	Evaluate algorithmic techniques and data structures to determine their suitability for different applications.	PO3(2)	PSO2(2)

	<b>Description of CO</b>	<b>PO</b>	<b>PSO</b>
CO4	Design optimized solutions for real-world problems using appropriate algorithms and data structures.	PO2(1)	PSO1(3)

BC25101	Network Design and Programming	L	T	P	C
		3	0	0	3
<p><b>Course Objective:</b></p> <ul style="list-style-type: none"> <li>• To impart knowledge of network architectures and design principles for building efficient and scalable computer networks.</li> <li>• To enable students to develop programming skills for implementing and managing network functionalities.</li> <li>• To equip learners with the ability to design and evaluate network systems in real-world scenarios.</li> </ul>					
<p><b>Network Design Fundamentals:</b> Network design lifecycle, requirements analysis- capacity planning. Hierarchical network architectures, Core-Distribution-Access layers and modern data center designs. OSI/TCP-IP protocols, routing protocols (OSPF, BGP, EIGRP), switching technologies. Quality of Service (QoS) implementation strategies, cost-benefit analysis in network design.</p> <p><b>Activities:</b> Demonstrates of inter process communication.</p>					
<p><b>Socket Programming and Network Communication:</b> Berkeley Socket API and Winsock for TCP/UDP communication. I/O multiplexing (select, poll, epoll), asynchronous programming, IPv6 considerations. Multi-language network programming and implementation. Custom protocol design-HTTP client/server implementation, file transfer protocols.</p> <p><b>Activity:</b> Development of TCP and UDP client/server applications</p>					
<p><b>Distributed Systems and Network Programming Frameworks:</b> Distributed system architectures, RPC, message passing, and consensus algorithms (Raft, Paxos) with CAP theorem analysis. Event-driven programming frameworks - Node.js/Express- Python asyncio/FastAPI- RxJava/Spring WebFlux- gRPC implementation. Microservices architecture with RESTful and GraphQL API design.</p> <p><b>Activity:</b> Demonstration of message passing and Creation of Micro services.</p>					
<p><b>Software-Defined Networking and Network Virtualization:</b> SDN fundamentals with OpenFlow protocols- flow tables, and controller programming (OpenDaylight, ONOS, Ryu). SDN application development for topology management. Network Function Virtualization (NFV) with ETSI standards. Virtual networking technologies - VXLAN tunneling- container networking (Docker/Kubernetes)-cloud networking solutions.</p> <p><b>Activity:</b> Development of SDN applications.</p>					
<p><b>Network Management and Monitoring:</b> Network management protocols, SNMP programming, NETCONF implementation- YANG data modeling with REST APIs. Network monitoring, topology visualization- anomaly detection systems. Network automation using frameworks (Ansible, Puppet, Chef), intent-based networking - CI/CD pipeline implementation</p> <p><b>Activity:</b> Demonstration of Network Monitoring.</p>					
<p><b>Performance Optimization:</b> Traffic shaping, bandwidth management, CDN implementation, network algorithm optimization.</p>					

<b>Activity:</b> Design of CDN Algorithm for Network optimization.
<b>Weightage:</b> Continuous Assessment: 40%, End Semester Examinations: 60%
<b>Assessment Methodology:</b> Assignments (15), Quiz (10), Virtual Demo (20), Flipped Class Room (10), Review of Gate and IES Questions (25), Project (20).
<b>References:</b> 1. Bose, S., & Vijayakumar, P. Cryptography and network security. Pearson (2017). 2. Kurose, J. F., & Ross, K. W. (2021). Computer networks: A top-down approach. Pearson Education. 3. Newmarch, J. (2021). Network programming with Go. Apress. 4. Donahoo, M. J., & Calvert, K. L. (2009). TCP/IP sockets in C: Practical guide for programmers. Morgan Kaufmann.
<b>E- Resources:</b> 1. Prof. Soumya Kanti Ghosh Prof. Sandip Chakraborty, “Computer Networks And Internet Protocol”, IIT Kharagpur, NPTEL “ <a href="https://nptel.ac.in/courses/106105183">https://nptel.ac.in/courses/106105183</a> ” 2. Prof. Neminath Hubballi Prof. Sameer Kulkarni, “Advanced Computer Networks, IIT Indore, IIT Gandhi nagar, NPTEL “ <a href="https://nptel.ac.in/courses/106106243">https://nptel.ac.in/courses/106106243</a> ”

	Description of CO	PO	PSO
CO1	Explain complex network architectures integrating QoS strategies.	--	--
CO2	Apply SDN and NFV concepts to create programmable, virtualized network solutions.	PO1(3)	PSO1(3)
CO3	Develop robust client-server applications using socket programming.	PO3(2)	PSO2(2)
CO4	Evaluate network performance and optimize designs using monitoring tools.	PO2(1)	PSO1(3)

CP25C03	Advanced Operating Systems	L	T	P	C
		3	0	0	3
<p><b>Course Objectives:</b></p> <ul style="list-style-type: none"> <li>To analyze the architectures and design issues of advanced operating systems.</li> <li>To develop the model for process synchronization and recovery in complex environments.</li> <li>To evaluate algorithms for distributed coordination, resource management, fault tolerance, and security.</li> </ul>					
<p><b>Advanced Process and Thread Management:</b> Multithreading models, thread pools, context switching, Synchronization issues and solutions: semaphores, monitors, lock-free data structures, CPU scheduling in multi-core systems</p> <p><b>Activity:</b> CPU scheduler simulation for multicore systems.</p>					
<p><b>Memory and Resource Management in Modern OS:</b> Virtual memory, demand paging, page replacement policies-Huge pages, NUMA-aware memory management-Resource allocation in cloud-native environments</p> <p><b>Activity:</b> Simulate demand paging and page replacement algorithms.</p>					
<p><b>Virtualization and Containerization:</b> Hypervisors (Type I &amp; II), KVM, QEMU, Xen-Containers: Docker, LXC, systemd-nspawn-OS-level virtualization and namespaces</p> <p><b>Activity:</b> Deploy and configure Docker containers with various images.</p>					
<p><b>Distributed Operating Systems and File Systems:</b> Distributed scheduling, communication, and synchronization-Distributed file systems: NFS, GFS, HDFS-Transparency issues and fault tolerance</p> <p><b>Activity:</b> Simulate distributed process synchronization.</p>					
<p><b>Security and Trust in Operating Systems:</b> Access control models: DAC, MAC, RBAC-OS hardening techniques, sandboxing, SELinux, AppArmor-Secure boot, rootkit detection, trusted execution environments</p> <p><b>Activity:</b> Implement Role-Based Access Control (RBAC) using Linux user and group permissions.</p>					
<p><b>Real-Time and Embedded Operating Systems:</b> Real-time scheduling algorithms (EDF, RM)-POSIX RT extensions, RTOS architecture-TinyOS, FreeRTOS case studies</p> <p><b>Activity:</b> Analyze FreeRTOS task scheduling behavior.</p>					
<p><b>Edge and Cloud OS: Future Paradigms:</b> Serverless OS, unikernels, lightweight OS for edge computing-Mobile OS internals (Android, iOS)-OS for quantum and neuromorphic computing (intro)</p> <p><b>Activity:</b> Analyze Android's system architecture using emulator tools.</p>					
<p><b>Weightage:</b> Continuous Assessment: 40%, End Semester Examinations: 60%</p>					
<p><b>Assessment Methodology:</b> Assignments (15), Quiz (10), Virtual Demo (20), Flipped Class Room (10), Review of Gate and IES Questions (25), Project (20).</p>					

**References:**

1. Tanenbaum, A. S., & Bos, H. (2023). Modern operating systems. Pearson.
2. Buyya, R., et al. (2022). Content delivery networks and emerging operating systems. Springer.
3. Silberschatz, A., Galvin, P. B., & Gagne, G. (2022). Operating system concepts. Wiley.
4. Anderson, T., & Dahlin, M. (2021). Operating systems: Principles and practice. Recursive Books.
5. Arpaci-Dusseau, R. H., & Arpaci-Dusseau, A. C. (2020). Operating systems: Three easy pieces.

**E-Resources:**

1. Prof. Smruti Ranjan Sarangi, "Advanced Distributed Systems", IIT Delhi, NPTEL, [https://onlinecourses.nptel.ac.in/noc22\\_cs80/preview](https://onlinecourses.nptel.ac.in/noc22_cs80/preview)
2. Prof. Rajiv Misra, "Cloud Computing and Distributed Systems", IIT Patna, NPTEL, <https://nptel.ac.in/courses/106104182>

	<b>Description of CO</b>	<b>PO</b>	<b>PSO</b>
CO1	Describe operating system concepts for memory and resource management.	--	--
CO2	Analyse virtualization and distributed OS mechanisms for scalability and performance.	PO1(3)	PSO1(3)
CO3	Evaluate OS security and resource handling strategies in diverse environments.	PO3(2)	PSO2(2)
CO4	Design innovative OS solutions using modern tools and techniques.	PO2(1)	PSO1(3)

CP25C04	Advanced Compiler Design	L	T	P	C
		3	0	0	3
<p><b>Course Objective:</b></p> <ul style="list-style-type: none"> <li>• To analyze the theory and principles of modern compiler design and advanced optimization techniques.</li> <li>• To design and implement efficient front-end and back-end compiler components for programming languages.</li> <li>• To evaluate code optimization strategies and runtime environment management in contemporary architectures.</li> </ul>					
<p><b>Intermediate Representations and Control Flow Analysis:</b> Static single assignment (SSA) form-Context-Free Grammar (CFG) construction-dominance relations-Intermediate Representation (IR) design for functional and imperative languages-Static single assignment and def-use chains</p> <p><b>Activities:</b></p> <ol style="list-style-type: none"> <li>1. Convert source code to SSA form using LLVM IR.</li> <li>2. Visualize control flow graphs from SSA using LLVM tools.</li> </ol>					
<p><b>Program Analysis and Transformations:</b> Data flow analysis- live variable analysis- reaching definitions-Alias analysis and dependence analysis-Loop optimizations and transformations</p> <p><b>Activities:</b></p> <ol style="list-style-type: none"> <li>1. Perform loop unrolling and strength reduction.</li> <li>2. Conduct live variable analysis and visualize data flow graphs.</li> </ol>					
<p><b>Advanced Optimizations and Polyhedral Compilation:</b> Polyhedral model for loop nests-Tiling, skewing, fusion, and vectorization-Profile-guided and feedback-directed optimizations</p> <p><b>Activities:</b></p> <ol style="list-style-type: none"> <li>1. Implement loop tiling and loop skewing on a matrix multiplication program.</li> <li>2. Analyze the effect on loop-intensive code with LLVM optimization flags.</li> </ol>					
<p><b>Just-in-Time (JIT) and Runtime Compilation:</b> JIT compilation models: tracing, method-based-GraalVM architecture, Java HotSpot internals-LLVM JIT and dynamic language support</p> <p><b>Activities:</b></p> <ol style="list-style-type: none"> <li>1. Develop a basic JIT-enabled interpreter with LLVM or GraalVM.</li> <li>2. Implement dynamic dispatch using LLVM JIT API.</li> </ol>					

**Machine Learning in Compiler Design:** ML for phase ordering, auto-tuning, and IR prediction-Reinforcement learning for optimization passes-Dataset creation and benchmarking for compiler ML

**Activities:**

1. Train an ML model to predict optimization passes.
2. Use reinforcement learning for pass selection in toy compiler.

**Domain-Specific Languages (DSLs) and Compiler Extensions:** Designing DSLs for AI/ML, DSP, graphics-Code generation for custom accelerators-Integration with TensorFlow XLA and Halide

**Activities:**

1. Design and test a simple DSL grammar using ANTLR.
2. Integrate a DSL with TensorFlow XLA or Halide.

**Security, Verification, and Future Trends:** Secure compilation and type-safe intermediate representations-Compiler fuzzing and formal verification (e.g., CompCert)-Quantum compilers, multi-target compilers, and neuromorphic systems

**Activities:**

1. Use CompCert to verify compilation of simple programs.
2. Apply compiler fuzzing using tools like libFuzzer.

**Weightage:** Continuous Assessment: 40%, End Semester Examinations: 60%

**Assessment Methodology:** Assignments (15), Quiz (10), Virtual Demo (20), Flipped Class Room (10), Review of Gate and IES Questions (25), Project (20).

**References:**

1. Cooper, K. D., & Torczon, L. (2023). Engineering a compiler. Morgan Kaufmann.
2. Grune, D., Bal, H. E., Jacobs, C. J. H., & Langendoen, K. G. (2012). Modern compiler design (2nd ed.). Springer.
3. Aho, A. V., Lam, M. S., Sethi, R., & Ullman, J. D. (2006). Compilers: Principles, techniques, and tools (2nd ed.). Pearson.
4. Völter, M. (2013). DSL engineering: Designing, implementing and using domain-specific languages. dslbook.org.
5. Sarda, S., & Pandey, M. (2015). LLVM essentials. Packt Publishing.

**E-Resources:**

1. Prof. AmeyKarkare, IIT Kanpur, "Advanced Compiler Optimizations"  
Link: <https://www.cse.iitk.ac.in/users/karkare/Courses/cs738/>
2. Prof. Santanu Chattopadhyay, "Compiler Design", IIT Kharagpur  
Link: [https://onlinecourses.nptel.ac.in/noc21\\_cs07/preview](https://onlinecourses.nptel.ac.in/noc21_cs07/preview)

	<b>Description of CO</b>	<b>PO</b>	<b>PSO</b>
CO1	Explain intermediate control flow techniques in compiler design.	--	--
CO2	Apply program analysis techniques and advanced optimizations for design of compilers.	PO1(3)	PSO1(3)
CO3	Develop compiler features and machine learning techniques for optimization.	PO3(2)	PSO2(2)
CO4	Evaluate secure compilation strategies for quantum and multi-target compilation.	PO2(1)	PSO1(3)

BC25201	Biometric Data Processing	L	T	P	C
		3	0	4	5
<p><b>Course Objective:</b></p> <ul style="list-style-type: none"> <li>• To introduce the fundamentals of biometric systems and various biometric modalities.</li> <li>• To impart knowledge on biometric data acquisition, preprocessing, feature extraction, and matching techniques.</li> <li>• To familiarize students with biometric system architectures and their application in identity verification and authentication systems</li> <li>• To analyze and evaluate biometric system performance using standard metrics.</li> <li>• To discuss the ethical and legal concerns associated with biometric data</li> </ul>					
<p><b>Introduction to Biometrics:</b> Introduction to biometrics - Need and scope of biometric systems - Biometric system components and architecture - Characteristics of biometric traits – Types of biometrics: physiological and behavioral-Applications and challenges</p> <p><b>Activities:</b> Implementation of Image Enhancement Implementation of Image Segmentation</p>					
<p><b>Biometric Modalities Fingerprint recognition:</b> ridge structure, minutiae detection-Face recognition: geometry-based and appearance-based methods-Iris recognition: iris localization and encoding-Voice recognition: signal modelling - Other modalities: hand geometry, gait, signature</p> <p><b>Activities:</b> Implementation of Fingerprint Image Acquisition Implementation of Face Image Acquisition Implementation of Iris Image Acquisition</p>					
<p><b>Data Acquisition and Preprocessing:</b> Sensors for biometric systems - Image acquisition, enhancement, and normalization - ROI extraction and alignment - Noise reduction and filtering techniques - Case Study: How India's Aadhaar System Processes 1.2B+ Low- Quality Rural Fingerprints</p> <p><b>Activities:</b> Implementation of Fingerprint Feature Extraction Implementation of Face Feature Extraction Implementation of Iris Feature Extraction</p>					
<p><b>Feature Extraction and Matching Techniques :</b> Statistical, structural and neural feature extraction techniques- Dimensionality reduction: PCA, LDA- Template matching methods - Classification algorithms: SVM, k-NN, neural networks - Fusion techniques: score-level, decision-level, and multi-modal fusion</p>					

<b>Activities:</b> <b>9.</b> Implementation of 3D Biometric – Palmprint <b>10.</b> Implementation of Mobile Biometrics
<b>Biometric System Evaluation, Security, and Privacy:</b> Performance metrics: FAR, FRR, EER, ROC - Standard biometric datasets and evaluation protocols-Biometric template protection: watermarking, cryptosystems - System security and spoof detection. Ethical use of biometric data - Biometric data protection laws and standards

CO	Description of CO	PO	PSO
CO1	Describe the fundamental principles, modalities, and workflows involved in biometric data acquisition, representation, and processing.	--	--
CO2	<b>Analyze</b> biometric feature extraction, matching techniques, and performance metrics to understand reliability and recognition accuracy.	PO1 (3)	PSO1 (3)
CO3	<b>Evaluate</b> biometric systems, fusion strategies, and security mechanisms to assess robustness, privacy, and usability in real-world environments.	PO3 (2)	PSO2 (2)
CO4	<b>Design</b> biometric processing solutions by selecting suitable algorithms, datasets, and system architectures for specific application requirements.	PO2 (1)	PSO1 (3)
<b>Weightage:</b>	Continuous Assessment: 40% (i) Activity: 10% (ii) Internal Theory Examination: 30%	End Semester Theory Examinations: 60%	
Mandated Activities with Marks: Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)			
Internal Examinations: Two Tests			

**References:**

1. Jain, A.K., Ross, A., & Prabhakar, S. Introduction to Biometrics, Springer, 2011.
2. Bose, S., & Vijayakumar, P. Cryptography and network security. Pearson (2017).
3. Maltoni, D., Maio, D., Jain, A.K., & Prabhakar, S. Handbook of Fingerprint Recognition, Springer, 2009.
4. Li, S.Z., & Jain, A.K. (Eds.), Encyclopedia of Biometrics, Springer, 2009.
5. Wayman, J.L., Jain, A.K., Maltoni, D., & Maio, D., Biometric Systems: Technology, Design and Performance Evaluation, Springer, 2005.
6. Ratha, N.K. & Bolle, R.M., Automatic Fingerprint Recognition Systems, Springer, 2004.
7. Zhang, D., Automated Biometrics: Technologies and Systems, Springer, 2013.

BC25202	Applied Cryptography	L	T	P	C
		3	0	2	4

**Course Objectives (COs):**

- Understand and analyze cryptographic algorithms and protocols.
- Design secure cryptographic systems using both symmetric and asymmetric methods.
- Evaluate cryptographic protocols in terms of security properties and performance.
- Apply cryptographic knowledge to solve real-world privacy and security problems.
- Demonstrate knowledge of modern cryptographic applications like blockchain, MPC, and post-quantum cryptography.

**Introduction to Cryptography:** History, objectives, and applications of cryptography-Basic terminology: Plaintext, ciphertext, encryption, decryption, keys-Types of cryptographic attacks: Brute-force, cryptanalysis, side-channel-Security services: Confidentiality, integrity, authentication, non-repudiation-Mathematical foundations: Modular arithmetic, prime numbers, GCD, Euclidean algorithm-Information theory and perfect secrecy: Entropy, Shannon’s theorem-Computational complexity and security models

**Activity:**

1. Demonstration of Symmetric classic cryptographic techniques

**Classical and Symmetric Key Cryptography:** Classical ciphers: Caesar, Affine, Monoalphabetic, Polyalphabetic, Rail Fence, Columnar, Hill cipher-Vigenère cipher and variants, One-Time Pad and perfect secrecy-Cryptanalysis: Frequency analysis and statistical attacks-Symmetric key ciphers: Feistel and SP-Networks, DES, AES-Other block ciphers: Blowfish, Twofish, Serpent; stream ciphers: RC4- Cryptographic hash functions: MD5, SHA-1, SHA-2, SHA-3 (Keccak), BLAKE2-Message Authentication Codes: HMAC, CBC-MAC, GMAC

**Activities:**

1. Demonstration of Symmetric conventional cryptographic techniques
2. Demonstration of Hashing and Message Digest techniques

**Asymmetric and Post-Quantum Cryptography:** Public key algorithms: RSA, ElGamal, ECC-Key generation and digital signatures; Key exchange: Diffie-Hellman-Advanced systems: Rabin cryptosystem, Paillier cryptosystem, IBE, ABE-Post-quantum cryptography: Quantum threats, Shor’s and Grover’s algorithms-Lattice-based and code-based

cryptography-Key management and PKI: CAs, trust models, CRL, OCSP-Hybrid cryptosystems: Combining symmetric and asymmetric cryptography

**Activities:**

1. Demonstration of Hashing and Message digest techniques
2. Design and implementation of new cryptographic algorithms

**Cryptographic Protocols and Network Security:** Authentication protocols: Challenge-response, Zero-knowledge proofs (Schnorr, Fiat-Shamir), MFA-Key establishment: Needham-Schroeder, Kerberos, Station-to-Station, IKE-Digital signatures and non-repudiation: RSA, padding schemes-Secure communication: SSL/TLS, SSH protocol analysis-Wireless security: Bluetooth protocols-Email security: PGP (Web of Trust), S/MIME (X.509 certificates)-Blockchain and distributed ledger security

**Activities:**

1. Demonstration and Implementation of secure communication using standard crypto libraries (OpenSSL, NTL, GMP)
2. Implementation of smart card based server/client applications
3. Demonstration of authentication techniques

**Advanced Cryptanalysis and Emerging Applications:** Cryptanalysis techniques: Linear, differential, integral, and higher-order attacks-Side-channel attacks: Timing, power, electromagnetic, fault injection, cache-based-Homomorphic encryption: Partial and fully homomorphic schemes-Secure applications: Cloud computing, secure multi-party computation, differential privacy-Biometric cryptography: Template protection, multimodal systems-Emerging fields: Machine learning in cryptography, blockchain privacy, 5G security

**Activities:**

1. Developing cryptographic algorithms for industrial applications
2. Developing cryptographic algorithms for innovative applications

CO	Description of CO	PO	PSO
CO1	Describe the fundamental principles, algorithms, and applications of applied cryptography in securing digital communication and data.	--	--
CO2	<b>Analyze</b> symmetric and asymmetric cryptographic techniques, hashing, and authentication mechanisms to understand their strengths and limitations.	PO1 (3)	PSO1 (3)
CO3	<b>Evaluate</b> cryptographic protocols, key management schemes, and security models to assess their effectiveness against various attack scenarios.	PO3 (2)	PSO2 (2)
CO4	<b>Design</b> secure cryptographic solutions by selecting appropriate algorithms, protocols, and implementation strategies for real-world security requirements.	PO2 (1)	PSO1 (3)
Weightage:		Continuous Assessment: 60%	

	(i) Activity: 15% (ii) Internal Theory Examination: 35% (iii) Internal Laboratory Examinations: 15%	End Semester Theory Examinations: 40%
Mandated Activities with Marks: Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)		
Internal Examinations: Two Tests		

### Text books:

1. **Bose, S., & Vijayakumar, P.** Cryptography and network security. Pearson (2017).
2. **Bruce Schneier**, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed., Wiley, 1996.
3. **William Stallings**, Cryptography and Network Security: Principles and Practice, 8th ed., Pearson, 2023.
4. **Douglas Stinson**, Cryptography: Theory and Practice, 4th ed., CRC Press, 2018.
5. **Jonathan Katz and Yehuda Lindell**, Introduction to Modern Cryptography, 3rd ed., CRC Press, 2020.
6. **Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno**, Cryptography Engineering: Design Principles and Practical Applications, Wiley, 2010.

CP25C07	Quantum Computing	L	T	P	C
		2	0	0	2
<b>Course Objective:</b>					
<ol style="list-style-type: none"> <li>1. To provide a mathematical foundation for Quantum Computing and provide the basics of working</li> <li>2. To interpret the various aspects and applications of quantum computing.</li> <li>3. To examine the factors that affect Quantum computation</li> </ol>					
<b>Physical properties and mathematical foundations</b>					
Double Slit Experiment; Light: Particle Vs Wave; Heisenberg Uncertainty Principle. Vector spaces – basis; Inner product; Outer product; Tensor product; Linear operators					
<b>Activities:</b>					
<ul style="list-style-type: none"> <li>• Simulate the experiment using an interactive virtual lab</li> <li>• Construct simple operators and visualize action on vectors</li> </ul>					
<b>Quantum computing postulates and gates</b>					
Review of postulates, Bloch sphere, Single qubit states and gates, superposition; Two Qubit States and Gates - Bell States, Entanglement, CNOT gate, Phase oracles, Pauli Gates.					
<b>Activities:</b>					
<ul style="list-style-type: none"> <li>• Group quiz to match postulates to physical implications</li> <li>• Visualization with Bloch sphere simulators</li> </ul>					
<b>Quantum computing circuits</b>					
Dirac's notation for quantum computing, Computational Basis, Orthonormality, Hadamard and Phase Gates- building quantum circuits					
<b>Activities:</b>					
<ul style="list-style-type: none"> <li>• Use IBM Q Composer to build and simulate custom circuits</li> <li>• Hands-on: Apply X, H, Z gates and observe results on simulators</li> </ul>					
<b>Fundamental Quantum Algorithms</b>					
Deutsch–Josza Algorithm, Grover search algorithm: Problem definition, Amplitude amplification, Grover oracle, diffuser, multiple solutions in the search space					
<b>Activities:</b>					
<ul style="list-style-type: none"> <li>• Construct DJ circuit for a 3-bit input function</li> <li>• Simulation of Grover's algorithm with multiple marked elements</li> </ul>					
<b>Programming on a real quantum computer</b>					
Coding a real time quantum computer via IBMQ to carry out basic quantum measurement and state analysis.					

**Activities:**

- Connect Qiskit with IBMQ using personal API token
- Hands-on: Create 1- and 2-qubit circuits using Hadamard, X, Z, and measurement gates
- Compare real and simulated results and Observe impact of quantum noise

**Text Books:**

1. Chuck Easttom, "Quantum Computing Fundamentals", 1st edition, Published by Addison-Wesley Professional (June 1st 2021)
2. Qiskit TextBook - <https://qiskit.org/textbook/preface.html> (2022)

**References:**

1. Kasirajan, Venkateswaran. Fundamentals of quantum computing. Springer International Publishing, 2021.
2. Chris Bernhardt, Quantum Computing for Everyone, The MIT Press, Cambridge, 2020
3. Nielsen, Michael A., and Isaac L. Chuang, "Quantum Computation and Quantum Information" Cambridge University Press (5 April 2013)

**Weightage:** Continuous Assessment:40%, End Semester Theory Examination: 60%

**Assessment Methodology:** Assignments (30), Quiz (10), Virtual demonstration (25), Flipped Classroom (10), Review of GATE & IES questions (25).

CO	Description of CO	PO	PSO
CO1	Describe the fundamental principles, postulates, and computational models of quantum computing and their significance in next-generation computing systems.	--	--
CO2	Analyze quantum algorithms and quantum circuit models to understand their computational advantages, limitations, and performance characteristics.	PO1 (3)	PSO1 (3)
CO3	Evaluate quantum computing paradigms, error correction techniques, and hardware technologies for their suitability in solving complex computational problems.	PO3 (2)	PSO2 (2)
CO4	Design quantum circuits and algorithmic solutions by selecting appropriate quantum gates, qubit architectures, and computational models for real-world problem scenarios.	PO2 (1)	PSO1 (3)

BC25001	Principles of Secure Coding	L	T	P	C
		3	0	0	3
<p><b>Course objectives:</b></p> <ul style="list-style-type: none"> <li>• To gain knowledge about the fundamentals of secure programming.</li> <li>• To familiarize about the concepts of the programming errors and software vulnerabilities.</li> <li>• To understand the security threats in software and secure coding techniques.</li> <li>• To familiarize the database and web specific security issues.</li> <li>• To understand about the testing secure applications.</li> </ul>					
<p><b>Fundamentals of secure programming: Introduction to security:</b> security and CIA triad, exploit, threat, vulnerability, risk, and attack, malware overview: viruses, trojans, worms, rootkits, trapdoors, botnets, keyloggers, honeypots. <b>Types of security attacks:</b> active attacks: IP spoofing, tear drop, DOS, XSS, SQL injection, smurf, man-in-the-middle, format string attack, passive attacks: eavesdropping, traffic analysis.</p>					
<p><b>Principles of software security:</b> Introduction to software security, managing software security risks, selecting secure software development technologies, guiding principles for secure programming, open source vs. Closed source software security. Need for secure systems secure software development cycle (S-SDLC)-security issues in different phases: SRS (software requirement specification), design phase security, development phase security, test phase security, maintenance phase security.</p>					
<p><b>Programming Errors and software vulnerabilities:</b> Introduction to software vulnerabilities: software security fundamentals, common programming errors and their security implications. Programming errors leading to vulnerabilities: buffer overflows, format string problems, integer overflow, SQL injection, command injection, failure to handle errors properly types of security vulnerabilities: invalidated input, race conditions, access-control problems, weaknesses in authentication and authorization, cryptographic practice vulnerabilities. Access control and security best practices: role-based access control, principle of least privilege, mitigating privilege escalation.</p> <p><b>Activity:</b></p> <ul style="list-style-type: none"> <li>• Group exercise – test strategy design for risk-based scenarios</li> </ul>					

**Security threats in Software & secure coding techniques:**

Introduction to Software Security, Importance of security analysis, Overview of security techniques and best practices. Security Issues and Countermeasures: Anti-Tampering, DoS/DDoS Protection, Copy Protection Schemes, Client-Side Security, Database Security and SQL Injection Prevention.

Case Study - Create advanced test cases for a real-world case study

Threat Modelling and Risk Assessment: Threat Modelling and Attack Trees, DREAD Rating for threat evaluation, Risk Mitigation Techniques. Authentication, Authorization, and Defense Strategies: Authentication and Authorization Basics, Defense, in Depth and Least Privilege. Secure Coding Techniques: DoS Protection, Secure Java Coding, Preventing Application Failures and CPU Starvation. Network and Remote Security: ARP Spoofing, Socket Security, Securing RPC and Server Hijacking Prevention

**Database and Web-Specific Security Issues:** SQL Injection, Race Conditions, Time of Check vs Time of Use (TOC/TOU), Input Validation & Interposes Communication (IPC), Signal Handlers & File Operations, Cross-Site Scripting (XSS), Bypassing XSS Filters, Information Leakage, Poor Usability, Network Traffic Protection, Improper Use of PKI, Trusting Network Name Resolution.

**Testing Secure Applications:** Security code overview, secure software installation. The Role of the Security Tester, Building the Security Test Plan. Testing HTTP-Based Applications, Testing File-Based Applications, Testing Clients with Rogue Servers. **Secure Testing Tools:** Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST), Vulnerability assessment & Penetration testing (VAPT).

**References:**

1. M. Howard and D. LeBlanc, Writing Secure Code, 2nd ed. Microsoft Press, 2003.
2. R. McGraw, Software Security: Building Security In. Addison-Wesley, 2006.
3. J. Viega and G. McGraw, Building Secure Software: How to Avoid Security Problems the Right Way. Addison-Wesley, 2001.

4. M. Dowd, J. McDonald, and J. Schuh, The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. Addison-Wesley, 2006.
5. G. Hoglund and G. McGraw, Exploiting Software: How to Break Code. Addison-Wesley, 2004.
6. C. Anley, J. Heasman, F. Linder, and G. Richarte, The Shellcoder's Handbook: Discovering and Exploiting Security Holes, 2nd ed. Wiley, 2007.

Weightage:	Continuous Assessment: 40%	End Semester Theory Examinations: 60%
	(i) Activity: 10% (ii) Internal Theory Examination: 30%	

Mandated Activities with Marks:  
Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)

Internal Examinations: Two Tests

CO	Description of CO	PO	PSO
CO1	Describe the fundamental principles, practices, and guidelines of secure coding for building reliable and resilient software systems.	--	--
CO2	<b>Analyze</b> software vulnerabilities, threat models, and common coding flaws to understand their causes and security implications.	PO1 (3)	PSO1 (3)
CO3	<b>Evaluate</b> secure coding techniques, defensive programming strategies, and security testing methods to determine their effectiveness in mitigating risks.	PO3 (2)	PSO2 (2)
CO4	<b>Design</b> secure software components by applying secure coding standards, validation techniques, and protective mechanisms in real-world development scenarios.	PO2 (1)	PSO1 (3)

BC25002		L	T	P	C
---------	--	---	---	---	---

		<b>AI for Cybersecurity</b>			
		3	0	0	3
<p><b>Prerequisites:</b> Basic understanding of cyber security and machine learning fundamentals</p> <p><b>Course Objectives</b>            By the end of this course, students will be able to:</p> <ol style="list-style-type: none"> <li>1. To introduce the applications of Artificial Intelligence in the domain of Cyber security.</li> <li>2. To understand various machine learning techniques used for detecting cyber threats.</li> <li>3. To apply deep learning models for advanced threat detection and classification.</li> <li>4. To design intelligent systems that automates cyber security tasks such as intrusion detection and phishing prevention.</li> <li>5. To explore the ethical and privacy issues of using AI in Cyber security.</li> </ol>					
<p><b>Introduction to AI and Cyber security:</b> Overview of Cyber security and Threat Landscape - Role of AI in Cyber security - Types of Cyber Threats and Attack Vectors - Challenges in Cyber security Data and Model Development</p>					
<p><b>Machine Learning in Threat Detection:</b> Supervised Learning: Decision Trees, SVM, Logistic Regression - Unsupervised Learning: Clustering, Dimensionality Reduction - Performance Evaluation: Confusion Matrix, ROC, AUC - Use Cases: Malware Detection, Spam Filtering</p>					
<p><b>Deep Learning Approaches in Cyber Security:</b> Introduction to Neural Networks and Deep Learning - CNNs for Image- Based Threat Analysis - RNNs and LSTM for Sequence-Based Attack Detection - Case Studies in Deep Learning for Security</p>					
<p><b>AI for Security Automation:</b> Automated Intrusion Detection Systems - Security Information and Event Management (SIEM) Tools - Threat Intelligence and Prediction - Phishing Detection and Email Security using NLP</p>					
<p><b>Ethics and Future Directions:</b> Adversarial Attacks on AI Models - Bias, Fairness and Privacy Concerns in AI Security Systems - Explainable AI in Cyber security - Emerging Trends: Federated Learning, Edge AI, Real-time Analytics</p>					
<p><b>Suggested Activities common to all modules</b></p> <ul style="list-style-type: none"> <li>• Flipped Classroom: Review research videos before classes</li> <li>• Project-Based Learning: Each student submits a mini project with optimization</li> <li>• Research Paper Reproduction: Benchmark or replicate results from CGO/PLDI/LLVM papers</li> </ul> <p>Industry Interaction: Guest sessions Industry</p>					

CO	Description of CO	PO	PSO
CO1	Describe the fundamental concepts, techniques, and applications of artificial intelligence in enhancing cybersecurity systems.	--	--
CO2	<b>Analyze</b> AI-based threat detection, anomaly detection, and malware analysis techniques to understand their capabilities and limitations.	PO1 (3)	PSO1 (3)
CO3	<b>Evaluate</b> AI-driven cybersecurity frameworks, datasets, and models to assess accuracy, robustness, and resilience against adversarial attacks.	PO3 (2)	PSO2 (2)
CO4	<b>Design</b> intelligent cybersecurity solutions by integrating appropriate AI models, defensive strategies, and monitoring mechanisms for real-world environments.	PO2 (1)	PSO1 (3)
Weightage:	Continuous Assessment: 60%	End Semester Theory Examinations: 40%	
	(i) Activity: 15% (ii) Internal Theory Examination: 35% (iii) Internal Laboratory Examinations: 15%		
Mandated Activities with Marks: Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)			
Internal Examinations: Two Tests			

### Text books

1. C. Chio and D. Freeman, Machine Learning and Security: Protecting Systems with Data and Algorithms. O'Reilly Media, 2018.
2. Bose, S., & Vijayakumar, P. Cryptography and network security. Pearson (2017).
3. S. Mukkamala, AI in Cybersecurity. Wiley India, 2023.
4. S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, 4th ed. Pearson, 2020.
5. S. Shalev-Shwartz and S. Ben-David, Understanding Machine Learning: From Theory to Algorithms. Cambridge University Press, 2014.
6. C. M. Bishop, Pattern Recognition and Machine Learning. Springer, 2006.



BC25003	Operating System Security	L	T	P	C
		3	0	0	3
<p><b>Course Objectives:</b></p> <ul style="list-style-type: none"> <li>• To understand vulnerabilities, threat models, and attack surfaces in operating systems.</li> <li>• To learn protection mechanisms in modern OS kernels (Linux, Android, seL4, etc.).</li> <li>• To explore security techniques such as access control, memory protection, and virtualization.</li> <li>• To study secure system design principles and their application in real OS environments.</li> </ul>					
<p><b>Fundamentals of OS Security:</b> Introduction to operating system security: scope, challenges, and goals - Secure OS architecture and kernel concepts - Threat modeling and attacker types - Historical lessons: Multics, UNIX, and security evolution - Overview of secure kernel design and trusted computing base (TCB).</p>					
<p><b>OS Vulnerabilities and Protection Mechanisms:</b> Common vulnerabilities: buffer overflows, privilege escalation, race conditions - Authentication and authorization in OS - Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC) - File system security and access control lists - Logging, auditing, and recovery.</p>					
<p><b>Memory and Process Protection:</b> Virtual memory security, address space isolation - Stack/heap protection, ASLR, DEP - Secure process and thread management - Case study: Linux security modules (LSM), SELinux - Malware and rootkit analysis basics.</p>					
<p><b>Virtualization and OS-level Security Extensions:</b> Virtualization concepts and security implications - Hypervisor attacks and defense techniques - Containers vs VMs: security perspectives- Hardware support for OS security: Intel SGX, ARM TrustZone- Case studies: seL4, QNX microkernel security.</p>					
<p><b>Mobile, Cloud, and Emerging OS Security:</b> Android and iOS OS security architectures - App sandboxing and permission models - OS support for cloud and distributed environments - User perspective and usability in OS security - OS security trends: secure boot, integrity measurement, TPM.</p>					

**References:**

1. Bose, S., & Vijayakumar, P. Cryptography and network security. Pearson (2017).
2. Trent Jaeger, "Operating System Security (Synthesis Lectures on Information Security", Privacy, and Trust), Morgan & Claypool Publishers, 1st edition, 2008.
3. Thomas Anderson, Michael Dahlin, "Operating Systems: Principles and Practice", Recursive Books, 2nd edition, 2014.
4. Andrew S. Tanenbaum, "Modern Operating Systems", Pearson, 4th edition, 2014.
5. Brett Tjaden, "Fundamentals of Secure Computer Systems", CreateSpace Independent Publishing, 1st edition, 2012.
6. Ross Anderson, "Securit Engineering: A Guide to Building Dependable Distributed Systems", Wiley, 3rd edition, 2020.
7. Reza Azarderakhsh, "Network Security: Private Communication in a Public World", Prentice Hall, 2nd edition, 2002.

CO	Description of CO	PO	PSO
CO1	Describe the principles, mechanisms, and challenges involved in securing modern operating systems.	--	--
CO2	<b>Analyze</b> operating system vulnerabilities, access control models, and threat scenarios to understand potential security risks.	PO1 (3)	PSO1 (3)
CO3	<b>Evaluate</b> security features, hardening techniques, and monitoring tools to assess their effectiveness in protecting operating system resources.	PO3 (2)	PSO2 (2)
CO4	<b>Design</b> secure operating system environments by applying appropriate configuration strategies, protection mechanisms, and security policies.	PO2 (1)	PSO1 (3)
Weightage:	Continuous Assessment: 40%	End Semester	
	(i) Activity: 10%	Theory Examinations:	
	(ii) Internal Theory Examination: 30%	60%	
Mandated Activities with Marks: Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)			
Internal Examinations: Two Tests			

BC25004	Security Practices	L	T	P	C
		3	0	0	3

**Course Objectives:**

- To learn the core fundamentals of system and web security concepts
- To have through understanding in the security concepts related to networks
- To deploy the security essentials in IT Sector
- To be exposed to the concepts of Cyber Security and cloud security
- To perform a detailed study of Privacy and Storage security and related Issues

**System Security:** Foundational concepts, Model of network security – Threats and attacks, services and mechanisms – OSI security architecture - A Cryptography primer- Intrusion detection system- Intrusion Prevention system - Management and Compliance, Security web applications- Case study: OWASP - Top 10 Web Application Security Risks.

**Network Security:** Internet Security - Intranet security- Network segmentation-Local Area Network Security - Wireless Network Security - Wireless Sensor Network Security- Cellular Network Security - Mobile security – Cloud Network security- End point Security-IOT security – Zero Trust security- Case Study - Kali Linux.

**Security Management:** Security Information and Event Management- Information security essentials for IT Managers- Security Management System – Risk Management-cyber security Management- Security Awareness- Policy Driven System Management- IT Security - Online Identity and User Management System. Case study: Metasploit

**Cyber Security and Cloud Security:** Cyber Forensics- Disk Forensics – Network Forensics – Wireless Forensics – Database Forensics – Malware Forensics – Mobile Forensics – Email Forensics- Cyber security risk in remote work - Best security practices for automate Cloud infrastructure management –Cloud Analytics– Establishing trust in IaaS, PaaS, and SaaS Cloud types. Case study: DVWA

<b>Privacy and Storage Security:</b> Data Breaches- Data Encryption- Privacy on the Internet - Privacy Enhancing Technologies - Personal privacy Policies - Detection of Conflicts in security policies- privacy and security in environment monitoring systems-Malware Protection. Storage Area Network Security - Storage Area Network Security Devices –data Retention Policies- Risk management - Physical Security Essentials.			
CO	Description of CO	PO	PSO
CO1	Describe the fundamental concepts, policies, and best practices involved in implementing security across systems and organizations.	--	--
CO2	<b>Analyze</b> security requirements, risk factors, and compliance needs to understand how security controls are planned and applied.	PO1 (3)	PSO1 (3)
CO3	<b>Evaluate</b> security tools, frameworks, and incident management strategies to determine their effectiveness in protecting assets.	PO3 (2)	PSO2 (2)
CO4	<b>Design</b> organizational and technical security practices by selecting suitable controls, procedures, and monitoring mechanisms for real-world environments.	PO2 (1)	PSO1 (3)
Weightage:	Continuous Assessment: 40%	End Semester Theory Examinations: 60%	
	(i) Activity: 10% (ii) Internal Theory Examination: 30%		
Mandated Activities with Marks: Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)			
Internal Examinations: Two Tests			

### References:

1. Bose, S., & Vijayakumar, P. Cryptography and network security. Pearson (2017).
2. John R. Vacca, Computer and Information Security Handbook, Third Edition, Elsevier 2017
3. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, Seventh Edition, Cengage Learning, 2022
4. Richard E. Smith, Elementary Information Security, Third Edition, Jones and Bartlett Learning, 2019
5. Mayor, K.K.Mookhey, Jacopo Cervini, Fairuzan Roslan, Kevin Beaver,
7. Metasploit Toolkit for Penetration Testing, Exploit Development and Vulnerability Research, Syngress publications, Elsevier, 2007.
8. John Sammons, “The Basics of Digital Forensics- The Primer for Getting
9. Started in Digital Forensics”, Syngress, 2012

BC25005	Cybercrime Investigations	L	T	P	C
		3	0	0	3
<p><b>Course Objectives:</b></p> <ol style="list-style-type: none"> <li>1. To introduce students to the fundamentals of cybercrime and its classifications.</li> <li>2. To equip learners with methodologies and tools for digital evidence collection and analysis.</li> <li>3. To understand the legal framework and procedures governing cybercrime investigations.</li> <li>4. To explore techniques for tracing, analyzing, and preventing cybercrime activities.</li> <li>5. To gain practical insights through case studies and forensic tools.</li> </ol>					
<p><b>Fundamentals of Cybercrime:</b> Definition and types of cybercrime - Classification: financial, hacktivism, cyberterrorism, cyberstalking - Cybercriminal profiles - Threat landscape and trends - Digital evidence basics - Introduction to computer forensics and investigation process</p>					
<p><b>Investigation Methodologies &amp; Tools:</b> Stages of cybercrime investigation - Incident response and forensic readiness - Identification, preservation, and acquisition of evidence - Chain of custody - Disk imaging tools - RAM and volatile memory acquisition - File carving - Open-source forensic tools overview.</p>					
<p><b>Network &amp; Mobile Forensics:</b> Network forensics: Packet capture, session reconstruction, flow analysis - Log file analysis - SIEM overview - IP traceback and attribution - Mobile forensics: Android and iOS investigation basics - SIM and app data extraction - Anti-forensic techniques and countermeasures.</p>					
<p><b>Legal Framework &amp; International Standards:</b> Cybercrime laws in India: IT Act 2000/2008, IPC, CrPC - Admissibility of digital evidence - International laws: Budapest Convention - Privacy, ethics, and surveillance - Case law references - GDPR and cross-border data access issues.</p>					
<p><b>Case Studies and Current Trends:</b> Major case studies: Ransomware (WannaCry), Data breaches (Equifax), Insider threats - Emerging threats: Deepfakes, AI-generated fraud - Blockchain forensics - Cryptocurrency investigation challenges - Integration of threat intelligence and forensic processes.</p>					
CO	Description of CO	PO	PSO		
CO1	Describe the fundamental concepts, legal perspectives, and investigative procedures related to cybercrimes and digital offenses.	--	--		

<b>CO2</b>	<b>Analyze</b> cybercrime incidents, digital footprints, and evidence sources to understand methods used by offenders and investigators.	PO1 (3)	PSO1 (3)
<b>CO3</b>	<b>Evaluate</b> investigative tools, forensic techniques, and reporting processes to determine their reliability and admissibility in legal contexts.	PO3 (2)	PSO2 (2)
<b>CO4</b>	<b>Design</b> effective cybercrime investigation strategies by planning evidence collection, documentation, and analysis procedures for real-world scenarios.	PO2 (1)	PSO1 (3)

Weightage:	Continuous Assessment: 40%	End Semester Theory Examinations: 60%
	(i) Activity: 10% (ii) Internal Theory Examination: 30%	
Mandated Activities with Marks: Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)		
Internal Examinations: Two Tests		
<b>References:</b> <ol style="list-style-type: none"> <li>1. Bose, S., &amp; Vijayakumar, P. Cryptography and network security. Pearson (2017).</li> <li>2. Marjie T. Britz, Computer Forensics and Cyber Crime: An Introduction, 3rd Edition, Pearson, 2013.</li> <li>3. B. Nelson, A. Phillips, F. Enfinger, and C. Steuart, Guide to Computer Forensics and Investigations, 2nd ed., Cengage Learning, 2006.</li> <li>4. C. Altheide and H. Carvey, "Digital Forensics with Open Source Tools", Syngress, 2011.</li> <li>5. A. Hoog, "Android Forensics", Elsevier, 2011.</li> <li>6. J. Vacca, "Computer Forensics: Computer Crime Scene Investigation", Charles River Media, 2005</li> </ol>		

BC25006	Mobile and Digital Forensics	L	T	P	C
		3	0	0	3
<p><b>Course Objective:</b></p> <ul style="list-style-type: none"> <li>• To introduce students to the fundamentals of digital and mobile forensics.</li> <li>• To understand forensic acquisition, preservation, and analysis of digital evidence.</li> <li>• To explore forensic tools and methodologies for Android and iOS.</li> <li>• To understand legal, ethical, and procedural aspects of forensic investigation.</li> <li>• Use modern tools for forensic data acquisition, analysis, and reporting</li> </ul>					
<p><b>Introduction to Mobile and Digital Forensics:</b> Overview of digital forensics: scope, importance, and applications - Types of digital evidence, cybercrime classification -Mobile device architecture: Android &amp; iOS basics-Phases of a forensic investigation: acquisition, preservation, analysis, and reporting.</p>					
<p><b>Evidence Acquisition and Preservation:</b> Imaging and cloning (bit-stream, logical, physical) -Hashing techniques: MD5, SHA-1, SHA-256 - Chain of custody and documentation -Write blockers and anti-forensic techniques - Live vs dead forensics and volatile data handling</p>					
<p><b>Android and iOS Forensics:</b> Android OS structure: file systems (EXT, YAFFS, F2FS), rooting techniques - iOS structure: file systems, jailbreaking methods -Extraction methods: logical, physical, file-system, cloud-based -Tools: Cellebrite, MOBILedit, Oxygen Forensics, Autopsy</p>					
<p><b>Data Analysis and Reporting:</b> Analysis of system files: registry, log files, event logs -File recovery: slack space, deleted files, metadata analysis-Timeline creation, browser history, app data analysis - Report writing, documentation standards, expert witness basics</p>					
<p><b>Legal, Ethical, and Emerging Trends:</b> Cyber laws and digital evidence admissibility (Indian IT Act, GDPR, etc.) - Ethical issues in forensics - Introduction to cloud and IoT forensics - Emerging technologies: AI in forensics, encrypted messaging forensics</p>					

CO	Description of CO	PO	PSO
CO1	Describe the fundamental principles, processes, and tools used in mobile and digital forensics for evidence identification and preservation.	--	--
CO2	<b>Analyze</b> digital evidence, file systems, and mobile device artifacts to understand acquisition, extraction, and examination procedures.	PO1 (3)	PSO1 (3)
CO3	<b>Evaluate</b> forensic analysis techniques, reporting standards, and chain-of-custody practices to determine their reliability and legal validity.	PO3 (2)	PSO2 (2)
CO4	<b>Design</b> effective forensic workflows by selecting appropriate tools, methodologies, and documentation practices for real-world investigations.	PO2 (1)	PSO1 (3)
Weightage:	Continuous Assessment: 40%	End Semester Theory Examinations: 60%	
	(i) Activity: 10% (ii) Internal Theory Examination: 30%		
Mandated Activities with Marks: Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)			
Internal Examinations: Two Tests			

### References:

1. Satish Bommisetty, Rohit Tamma, Heather Mahalik, "Practical Mobile Forensics", Packt Publishing, 4th edition, 2022.
2. Bill Nelson, Amelia Phillips, Christopher Steuart, "Guide to Computer Forensics and Investigations", Cengage Learning, 6th edition, 2018.
3. Bose, S., & Vijayakumar, P. Cryptography and network security. Pearson (2017).
4. Cory Altheide, Harlan Carvey, "Digital Forensics with Open Source Tools", Syngress (Elsevier), 1st edition, 2011.
5. Eoghan Casey, "Digital Evidence and Computer Crime", Academic Press (Elsevier), 3rd edition, 2011.
6. John Sammons, "The Basics of Digital Forensics: The Primer for Getting Started", Syngress (Elsevier), 2nd edition, 2015.
7. Ayman Shaaban, Konstantin Saponov, "Practical Windows Forensics", Packt Publishing, 1st edition, 2016.
8. Sherri Davidoff, Jonathan Ham, "Network Forensics: Tracking Hackers Through Cyberspace", Prentice Hall (Pearson), 1st edition, 2012.

### Online Platforms:

- SWAYAM/NPTEL: [Digital Forensics Courses](#)
- <https://www.ifsedu.in/cell.phone.mobile.forensics.syllabus.html>

BC25007	Firewall And VPN Security	L	T	P	C
		3	0	0	3

**Course Objectives:**

- Identify and assess current and anticipated security risks and vulnerabilities.
- Develop a network security plan and policies
- Establish a VPN to allow IPSec remote access traffic
- Monitor, evaluate and test security conditions and environment
- Develop critical situation contingency plans and disaster recovery plan

**Firewall Introduction:** Types of Firewalls, Ingress and Egress Filtering, Network Address Translation (NAT), Application Proxy, Circuit Proxy, Content Filtering, Software versus Hardware Firewalls, IPv4 versus IPv6 Firewalls, Dual-Homed and Triple-Homed Firewalls, Placement of Firewalls. Cloud-based firewall solutions and AI-driven threat detection mechanisms in modern firewall implementations.

**VPN Fundamentals:** VPN Deployment Models and Architecture, Edge Router, Corporate Firewall, VPN Appliance, Remote Access, Site-to-Site, Host-to-Host, Extranet Access, Tunnel versus Transport Mode, The Relationship Between Encryption and VPNs, Establishing VPN Connections with Cryptography, Digital Certificates, VPN Authorization. Implementation of Wire Guard VPN and quantum-resistant cryptographic algorithms.

**Exploring the Depths of Firewalls:** Firewall Rules, Authentication and Authorization, Monitoring and Logging, Understanding and Interpreting Firewall Logs and Alerts, Intrusion Detection, Limitations of Firewalls, Downside of Encryption with Firewalls, Firewall Enhancements, and Management Interfaces. Integration of Security Orchestration, Automation and Response (SOAR) platforms with firewall systems.

**Overview of Industrial Control Systems:** Overview of SCADA, DCS, and PLCs, ICS Operation, Key ICS Components, Control Components, Network Components, SCADA Systems, Distributed Control Systems, Programmable Logic Controllers, Industrial Sectors and Their Interdependencies. Security considerations for Industrial IoT (IIoT) and analysis of recent ICS malware attacks

**Scada Protocols:** Modbus RTU, Modbus TCP/IP, DNP3, DNP3 TCP/IP, OPC, DA/HAD, SCADA protocol fuzzing, Finding Vulnerabilities in HMI: software- Buffer Overflows, Shell code. Previous attacks Analysis-Stuxnet, Duqu. IEC 62351 security standards for SCADA protocols and contemporary ransomware threats targeting industrial systems.

### References

1. Bose, S., & Vijayakumar, P. Cryptography and network security. Pearson (2017).
2. J. Michael Stewart and Denise Kinsey "Network Security, Firewalls, and VPNs", 3rd Edition, Jones & Bartlett Learning, October 2020, ISBN: 9781284183696
3. T. Macaulay and B. L. Singer, Cyber security for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS, Auerbach Publications, 2011.
4. J. Lopez, R. Setola, and S. Wolthusen, Critical Infrastructure Protection Information Infrastructure Models, Analysis, and Defense, Springer-Verlag Berlin Heidelberg, 2012.
5. Robert Radvanovsky and Jacob Brodsky, editors. Handbook of SCADA/Control Systems Security. Routledge, 2020, ISBN 9780367596668.
6. A.W. Colombo, T. Bangemann, S. Karnouskos, S. Delsing, P. Stiuka, R. Harrison, et al. Industrial cloud-based cyber-physical systems Springer International Publishing, 2014.

CO	Description of CO	PO	PSO
CO1	Describe the fundamental concepts, architectures, and functions of firewalls and Virtual Private Networks in securing network communications.	--	--
CO2	<b>Analyze</b> firewall policies, VPN configurations, and traffic flows to understand security enforcement, performance, and constraints.	PO1 (3)	PSO1 (3)
CO3	<b>Evaluate</b> different firewall technologies, tunneling protocols, and deployment strategies to assess their effectiveness in varied network environments.	PO3 (2)	PSO2 (2)
CO4	<b>Design</b> secure network solutions by integrating appropriate firewall configurations and VPN mechanisms for organizational requirements.	PO2 (1)	PSO1 (3)

**Weightage:** **Continuous Assessment:** 40% **End Semester Theory Examinations:** 60%

(i) Activity: 10%

(ii) Internal Theory Examination: 30%

**Mandated Activities with Marks:**

Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10),

Review of Gate and IES Questions (25)

Internal Examinations: Two Tests

BC25008	Biometric Security	L	T	P	C
		3	0	0	3
<b>Course Objectives:</b> <ul style="list-style-type: none"> <li>• To introduce the principles of biometric systems and their use in security.</li> <li>• To study physiological and behavioral biometric traits and technologies.</li> <li>• To explore multi-modal biometric systems and their applications.</li> <li>• To understand biometric standards, performance metrics, and deployment issues.</li> </ul>					
<b>Introduction to Biometrics:</b> Overview of biometrics and its advantages over traditional authentication - Biometric system components and processes - Biometric matching types: verification vs identification - Key performance metrics: FAR, FRR, EER, FTE - Biometric standards and system accuracy considerations					
<b>Physiological Biometrics I:</b> Fingerprint recognition: feature extraction, minutiae detection - Facial recognition: 2D/3D face recognition techniques - Iris recognition: texture analysis, Daugman's algorithm - Retinal scan: vascular pattern recognition.					
<b>Physiological Biometrics II:</b> Hand geometry: features and comparison techniques - Palmprint recognition: texture-based methods - DNA biometrics: encoding, matching, forensic applications - Implementation and deployment challenges					
<b>Behavioral Biometrics:</b> Signature and handwriting recognition - Voice recognition: feature extraction, MFCC - Keystroke dynamics: timing analysis, classification methods - Gait recognition: motion-based modelling.					
<b>Multimodal and Security Applications:</b> Multi-biometric systems: fusion techniques, levels of integration - Two- factor authentication: combining biometrics with passwords/tokens- Correlation-based recognition filters and digital correlation methods - Privacy, ethical issues, spoofing countermeasures - Applications in border control, banking, smartphones, and surveillance					

CO	Description of CO	PO	PSO
CO1	Describe the fundamental concepts, biometric modalities, and security challenges involved in biometric authentication systems.	--	--
CO2	<b>Analyze</b> biometric system architectures, feature matching techniques, and performance metrics to understand reliability and vulnerability aspects.	PO1 (3)	PSO1 (3)
CO3	<b>Evaluate</b> biometric attacks, spoofing countermeasures, and privacy-preserving techniques to determine their effectiveness in real-world deployments.	PO3 (2)	PSO2 (2)
CO4	<b>Design</b> secure biometric authentication solutions by integrating appropriate algorithms, system components, and protection mechanisms.	PO2 (1)	PSO1 (3)
Weightage:	Continuous Assessment: 40% (i) Activity: 10% (ii) Internal Theory Examination: 30%	End Semester Theory Examinations: 60%	
Mandated Activities with Marks: Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)			
Internal Examinations: Two Tests			

#### References:

1. Samir Nanavati, Michael Thieme, Raj Nanavati, "Biometrics: Identity verification in a networked world", Wiley Eastern, 1st edition, 2002.
2. Bose, S., & Vijayakumar, P. Cryptography and network security. Pearson (2017).
3. John Chirillo, Scott Blaul, "Implementing biometric security", Wiley Eastern, 1st edition, 2005.
4. Paul Reid, "Biometrics for network security", Pearson Education, 1st edition, 2004.
5. James L. Wayman, Anil K. Jain, Davide Maltoni, Dario Maio, "Biometric systems: Technology, design and performance evaluation", Springer, 2005.
6. Anil K. Jain, Ruud Bolle, Sharath Pankanti, "Biometrics: Personal identification in networked society", Kluwer Academic Publishers, 1st edition, 1999.

BC25009	Cyber Security Management and Cyber Laws	L	T	P	C
		3	0	0	3

**Course Objective:**

- To understand the nature of threats and cyber security management goals technology
- To understand the landscape of hacking and perimeter defense mechanisms
- To develop strategies for Intelligence and protecting critical infrastructure
- To understand policies to mitigate cyber risks and digital signature
- To understand the IT Act, scheme, amendments, IPR and emerging cyber law and desired cyber ecosystem capabilities.

**Introduction Cyber Security:** Cyber security Policy, Mission and Vision of Cyber security Program. Enterprise Security Architecture, Cyber Security Frameworks, Strategic alignment of security, perimeter defense and encryption, Cyber security management framework.

**Risk Management and Business Continuity for Hacker:** Risk Assessment & Quantification, Threat Modeling, Risk Appetite, Tolerance, and Capacity, Integrating Business Continuity Management and Disaster Recovery, Technology - Perimeter Defense, Types of Network Security Devices - Firewalls, Intrusion Detection Systems, Content Filtering, Virtual Private Networks, Encryption.

**Threat Intelligence and Secure Enterprise:** Cyber Threat Intelligence Lifecycle, Incident Detection Tools, Zero Trust Architecture (ZTA) and Identity-Centric Security, Anomaly detection, Predictive modelling, Securing E-Governance Services, Protecting Critical Information Infrastructure.

**Foundations of Cyber Law and Amendments:** Jurisprudence of Cyber Law and Legal Theories, Legal Recognition of Electronic Records & Digital Signatures, Investigation and Digital Evidence, Cyber Forensics and Admissibility in Court, Role of Law Enforcement Agencies.

**Data Protection and Privacy Laws:** Information Technology Act: Salient Features, Scheme, Application of the I.T. Act, Amendments I.T. Act, Offences, Compounding of Offences.

**Intellectual Property Rights:** Types of Intellectual Property Rights, Intellectual Property Rights in India, Intellectual Property in Cyber Space. Emerging Trends of Cyber Law. Desired Cyber Ecosystem Capabilities.

### References

1. Bose, S., & Vijayakumar, P. Cryptography and network security. Pearson (2017).
2. Charles P. Pfleeger Shari Lawrence Pfleeger Jonathan Margulies, Security in Computing, 5th Edition, Pearson Education, 2018
3. Nina Godbole, Sunit Belapure, "Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley India Pvt. Ltd., 2011
4. P. Duggal, Cyber Law: The Indian Perspective, 4th ed. New Delhi, India: Saakshar Law Publications, 2020.
5. V. Sharma, Information Technology Law and Practice, 5th ed. New Delhi, India: Universal Law Publishing, 2021.
6. Peter Trim and Yang-Im Lee, —Cyber Security Management- A Governance, Risk and Compliance Frameworkll, Gower Publishing, England 2014.

CO	Description of CO	PO	PSO
CO1	Describe the principles, frameworks, and legal perspectives governing cybersecurity management and cyber laws.	--	--
CO2	<b>Analyze</b> organizational security policies, governance structures, and compliance requirements to understand their implications on cybersecurity practices.	PO1 (3)	PSO1 (3)
CO3	<b>Evaluate</b> cybersecurity regulations, incident handling processes, and legal case studies to determine their effectiveness and applicability.	PO3 (2)	PSO2 (2)
CO4	<b>Design</b> comprehensive cybersecurity management strategies by integrating legal, technical, and organizational controls for real-world scenarios.	PO2 (1)	PSO1 (3)

Weightage:	Continuous Assessment: 40%	End Semester Theory Examinations: 60%
	(i) Activity: 10% (ii) Internal Theory Examination: 30%	
Mandated Activities with Marks: Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)		
Internal Examinations: Two Tests		

<b>CP25C12</b>	<b>Quantum Cryptography</b>	<b>L</b>	<b>T</b>	<b>P</b>	<b>C</b>
		3	0	0	3
<p><b>Course Objective:</b>  The objective of this course is to introduce the principles of quantum information and computation, along with key quantum algorithms and their practical applications. It also aims to provide a clear understanding of post-quantum and advanced quantum cryptographic techniques essential for secure communication in the quantum era.</p>					
<p><b>Quantum Information:</b> Qubit - Single and Multiple qubits – Mathematical Model for Quantum mechanics – Quantum measurements – Quantum Computation and No-cloning: Phase shift – Bit flips – Hadamard transform – Arbitrary Transforms – Entanglement - Quantum gates and circuits: CNOT gate – CCNOT gate – Reversible gates - Universal quantum gates - quantum circuit – quantum parallelism</p> <p><b>Activities</b></p> <ul style="list-style-type: none"> <li>• Build and simulate quantum circuits using Qiskit (or another quantum simulator)</li> <li>• Create a Bell state using a Hadamard gate followed by a CNOT gate.</li> </ul>					
<p><b>Quantum Algorithms:</b> Deutsch’s algorithm – Phase Kickback – Generalizing to n bits: Deutsch-Jozsa algorithm – Simon’s algorithm: Analysis - Quantum Fourier Transform, Grover's Algorithm, Shor's Algorithm.</p> <p><b>Activities</b></p> <ul style="list-style-type: none"> <li>• Simulate both Deutsch’s algorithm (1-bit) and the Deutsch-Jozsa algorithm (n-bit) using Qiskit.</li> </ul>					
<p><b>Quantum Cryptanalysis:</b> Quantum order finding – Factoring – Discrete logarithms, Hidden subgroup problems (HSP) – Key Exchange: Diffie-Hellman (DH) problems - Computational DH – Decisional DH – Indistinguishable Chosen Plaintext Attack (IND-CPA): Applications in RSA Encryption and Elgamal Encryption</p> <p><b>Activities</b></p> <ul style="list-style-type: none"> <li>• Simulate Shor’s Algorithm using Qiskit or any quantum simulator to factor small numbers</li> </ul>					
<p><b>Post-Quantum Cryptography:</b> Post Quantum Crypto: Introduction to lattices – Codes – Isogenies - Lattice Problems. Learning with Errors (LWE) and Short Integer Solution (SIS) problem. Connection to dihedral hidden subgroup problem - Public Key Encryption (PKE) from LWE - Fully Homomorphic Encryption (FHE).</p> <p><b>Activities</b></p> <ul style="list-style-type: none"> <li>• Implement a simplified version of a public-key encryption scheme based on the LWE problem using Python or SageMath</li> </ul>					

<p><b>Advanced Quantum Cryptography - I</b> : Quantum Key Distribution and bit commitment – Random Oracles - Quantum One Time Pad and Encryption - Quantum PKE – Quantum FHE - Quantum Indifferentiability - Quantum Money</p> <p><b>Activities</b></p> <ul style="list-style-type: none"> <li>• Simulate the BB84 protocol for quantum key distribution between two parties in Python using Qiskit</li> </ul>
<p><b>Advanced Quantum Cryptography – II</b> : Quantum key distribution with imperfect devices – beyond point-to-point quantum key distribution – device independent Quantum cryptography</p> <p><b>Activities:</b></p> <ul style="list-style-type: none"> <li>• Simulate Quantum key distribution between two IoT based device in python using Qiskit</li> </ul>
<p><b>Weightage:</b> Continuous Assessment: 40%, End Semester Theory Examinations: 60%</p>
<p><b>Assessment Methodology:</b> Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)</p>
<p><b>References:</b></p> <ol style="list-style-type: none"> <li>1. Quantum Computation and Quantum Information, M. A. Nielsen and I. Chuang, Cambridge University Press, 2012.</li> <li>2. Quantum Computing from the Ground Up, Riley Tipton Perry, World Scientific Publishing Ltd., 2012.</li> <li>3. Quantum algorithms via linear Algebra Primer, Richard J. Lipton Kenneth W. Regan, The MIT Press Cambridge, 2014.</li> <li>4. Quantum Computing: An Applied Approach, Jack D. Hidary, 1<sup>st</sup> Edition, Springer, 2019.</li> </ol>
<p><b>E-resources:</b></p> <ol style="list-style-type: none"> <li>1. Quantum Algorithms and Cryptography (Video) – NPTEL</li> <li>2. Introduction to Quantum Computing: Quantum Algorithms and Qiskit (Video) – NPTEL</li> <li>3. Practical Quantum Computing with IBM Qiskit for Beginners (Video) – Coursera</li> </ol>

### CO-PO-PSO Mapping

CO	Description of CO	PO	PSO
CO1	Describe the fundamental principles, protocols, and security concepts of quantum cryptography and their significance in secure communication systems.	--	--
CO2	Analyze quantum cryptographic protocols and security mechanisms to understand their robustness, vulnerabilities, and performance characteristics.	PO1 (3)	PSO1 (3)
CO3	Evaluate quantum cryptographic techniques and implementations to assess their effectiveness in ensuring confidentiality and secure key distribution.	PO3 (2)	PSO2 (2)

<b>CO4</b>	Design secure communication systems by applying appropriate quantum cryptographic protocols, architectures, and security strategies for real-world applications.	PO2 (1)	PSO1 (3)
------------	--	------------	-------------

BC25010	Data Analytics and Risk Monitoring	L	T	P	C
		3	0	0	3
<p><b>Course Objectives:</b></p> <ul style="list-style-type: none"> <li>• To understand various types and characteristics of fraud across domains like finance, e-commerce, and cybersecurity.</li> <li>• To develop the ability to preprocess, analyze, and visualize structured and unstructured data for fraud detection.</li> <li>• To apply advanced statistical and machine learning models for detecting and predicting fraudulent activities.</li> <li>• To utilize big data technologies and real-time analytics for scalable fraud monitoring and prevention.</li> <li>• To evaluate legal, ethical, and regulatory aspects related to data-driven fraud analytics in various sectors.</li> </ul>					
<p><b>Fundamentals of fraud and Analytical Frameworks:</b> Fundamentals of Fraud: Conceptual architecture of fraud detection systems, Types of fraud: financial, cyber, insurance, identity, health, Fraud triangle theory, red flags, and behavioral analytics, Role of data analytics in fraud prevention and detection, Case studies: Enron, Wirecard, credit card fraud.</p> <p><b>Data Collection, Preprocessing and Exploratory Analysis:</b> Data sources: structured, semi-structured, unstructured, Data cleaning, transformation, and handling imbalanced data, Feature selection and dimensionality reduction, detection techniques, EDA tools and visualization for fraud patterns.</p> <p><b>Machine learning techniques in Fraud Detection:</b> Logistic Regression, Decision Trees, Random Forest, Gradient Boosting, Unsupervised Learning: K-Means, Isolation Forest, Autoencoders, Deep Learning for fraud detection, Model evaluation metrics: Precision, Recall, ROC-AUC, F1-Score, Confusion Matrix, Cross-validation and hyperparameter tuning for fraud detection.</p>					

**Big data analytics and real-time fraud detection:** Big Data frameworks: Hadoop, Spark, Hive, Kafka, Streaming analytics using Apache Spark Streaming and Apache Flink, Real-time dashboards and alerts, Fraud scoring systems and risk engines, Deployment and integration with SIEM tools.

**Governance, Ethics, and Industry Applications:** Legal and regulatory frameworks: GDPR, PCI-DSS, SOX, HIPAA, Ethical challenges in automated fraud detection, Explainability in ML: LIME, SHAP, Case studies: Fraud analytics in banking, telecom, insurance, and healthcare, Emerging trends: Blockchain, federated learning, AI and adversarial attacks

**REFERENCES:**

1. D. D. Spann, Fraud Analytics: Strategies and Methods for Detection and Prevention. Wiley, 2013
2. Bose, S., & Vijayakumar, P. Cryptography and network security. Pearson (2017).
3. G. Shmueli, P. C. Bruce, and N. R. Patel, Data Mining for Business Analytics: Concepts, Techniques, and Applications, 3rd ed. Wiley, 2016
4. C. Chio and D. Freeman, Machine Learning for Fraud Management. O'Reilly Media, 2018
5. E. Mays, Credit Risk Analytics: Measurement Techniques, Applications, and Examples in SAS. Wiley, 2017.
6. F. Provost and T. Fawcett, Data Science for Business. O'Reilly Media, 2013.

CO	Description of CO	PO	PSO
CO1	Describe the fundamental concepts, processes, and tools involved in data analytics and risk monitoring across organizational systems.	--	--
CO2	<b>Analyze</b> datasets, risk indicators, and analytical models to understand patterns, anomalies, and potential risk factors.	PO1 (3)	PSO1 (3)
CO3	<b>Evaluate</b> risk assessment frameworks, visualization techniques, and decision-support systems to determine their effectiveness in monitoring and mitigation.	PO3 (2)	PSO2 (2)
CO4	<b>Design</b> data-driven risk monitoring solutions by integrating appropriate analytical methods, dashboards, and reporting mechanisms.	PO2 (1)	PSO1 (3)

Weightage:	Continuous Assessment: 40%	End Semester Theory Examinations: 60%
	(i) Activity: 10% (ii) Internal Theory Examination: 30%	
Mandated Activities with Marks: Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)		
Internal Examinations: Two Tests		

BC25011	Cryptanalysis	L	T	P	C
		3	0	0	3
<p><b>Course Objective:</b></p> <ul style="list-style-type: none"> <li>• Introduce students to the fundamental concepts of cryptography and cryptanalysis.</li> <li>• Develop a strong understanding of symmetric and asymmetric cryptographic algorithms.</li> <li>• Explore various cryptanalytic techniques, including brute-force attacks, linear cryptanalysis, and differential cryptanalysis.</li> <li>• Analyze the security of cryptographic systems and identify potential vulnerabilities.</li> <li>• Provide a foundation for further study in advanced cryptography and information security.</li> </ul>					
<p><b>Introduction:</b> Introduction to Cryptanalysis - Kerckhoffs' principle - Notions of security: confidentiality, integrity, authenticity - Models of attack-Targets of attack -Theoretical attacks vs. practical attacks-Lessons learned from classic ciphers</p>					
<p><b>Cryptanalysis of Block Ciphers:</b> Meet-in-the-Middle attack &amp; TMTO-Basic differential analysis-Basic linear analysis-Wide-trail strategy and AES -Integral cryptanalysis- Boomerang and rectangle attacks-Zero-correlation linear attack</p>					
<p><b>Cryptanalysis of Stream Ciphers:</b> Guess-and-determine attack on stream ciphers-Time-Memory-Data trade off attack-Linear distinguisher and correlation attacks- Cryptanalysis of hash functions -Birthday attacks-MD and Sponge- Differential cryptanalysis and collision attacks-</p>					

Meet-in-the-Middle Pre- image attack

**Computer-Aided Cryptanalysis:** MILP-based cryptanalysis- SAT-based cryptanalysis- Algebraic cryptanalysis -Interpolation attack-Cube attacks and Higher order differential attack-Linearization lattice based Cryptanalysis Direct attacks using lattice reduction, Coppersmith's small roots attacks. Elliptic curves and pairings: Introduction to elliptic curves, The Weil pairing, the elliptic curve factoring method.

**Algorithms:** Merkle-Hellman Knapsack - Diffie-Hellman Key Exchange and MitM - Discrete Log algorithms -Baby-step giant-step- Factoring algorithms - Dixon's Algorithm, Quadratic Sieve- Birthday- based algorithms for functions-LFSR-based key stream generators, correlation attacks

CO	Description of CO	PO	PSO
CO1	Describe the fundamental principles, goals, and techniques of cryptanalysis and their role in evaluating cryptographic systems.	--	--
CO2	<b>Analyze</b> classical and modern cryptanalytic methods to understand vulnerabilities, attack models, and system weaknesses.	PO1 (3)	PSO1 (3)
CO3	<b>Evaluate</b> the strength of cryptographic algorithms and security protocols against various cryptanalytic attacks.	PO3 (2)	PSO2 (2)
CO4	<b>Design</b> cryptanalysis strategies and testing approaches to assess and improve the resilience of real-world cryptographic systems.	PO2 (1)	PSO1 (3)
Weightage:	Continuous Assessment: 40%	End Semester Theory Examinations: 60%	
	(i) Activity: 10%		
	(ii) Internal Theory Examination: 30%		
Mandated Activities with Marks: Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)			
Internal Examinations: Two Tests			

**References:**

1. Bose, S., & Vijayakumar, P. Cryptography and network security. Pearson (2017).
2. D. R. Stinson and M. B. Paterson, *Cryptography: Theory and Practice*, 4th ed., CRC Press, 2018.
3. W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory*, 3rd ed., Pearson, 2020.
4. Algorithmic Cryptanalysis, by Antoine Joux, 1st Edition, CRC Press, 2009.
5. Algebraic Cryptanalysis, Bard Gregory, Springer, 2009
6. B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed., Wiley, 2015.
7. N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering:*

*Design Principles and Practical Applications, Wiley, 2010.*

IF25C04	Block Chain Technologies	L	T	P	C
		3	0	0	3
<p><b>Course Objectives:</b></p> <ul style="list-style-type: none"> <li>• To understand the foundational principles of blockchain technology.</li> <li>• To explore the architecture and consensus mechanisms of distributed ledgers.</li> <li>• To design and develop smart contracts and decentralized applications.</li> <li>• To evaluate real-world use cases and security issues in blockchain networks.</li> </ul>					
<p><b>Introduction to Blockchain and Distributed Ledger Technologies:</b> Centralized vs. Decentralized systems- Blockchain fundamentals: blocks, chains, hash functions, Merkle trees- Types of blockchain: Public, Private, Consortium- Consensus mechanisms: PoW, PoS, PBFT-Key challenges: scalability, privacy, interoperability.</p> <p><b>Activities:</b> Analyze and compare centralized vs decentralized systems (e.g., traditional banking vs Bitcoin).</p> <p><b>Cryptographic Foundations and Consensus:</b> Cryptographic hash functions- Digital signatures and public-key cryptography-Mining and proof-of-work in Bitcoin- Byzantine fault tolerance and proof-of-stake mechanisms-Tokenomics and incentive structures.</p> <p><b>Activities:</b> Simulate a blockchain manually with students acting as nodes. Include hash functions, blocks, and consensus.</p> <p><b>Smart Contracts and Ethereum Platform:</b> Ethereum architecture and EVM- Solidity programming language-Smart contract design and development-Gas optimization and security best practices-Deployment and interaction with contracts.</p>					

**Activities:**

- Teams debate PoW vs PoS vs PBFT – focusing on efficiency, security, and real-world applications.

**Blockchain Platforms and Applications:** Hyperledger Fabric and enterprise blockchains-Corda and permissioned networks-Decentralized Finance (DeFi) and NFTs-Blockchain in supply chain, healthcare, identity, and voting-Interoperability solutions (Polkadot, Cosmos).

**Activities:** Given a list of real-world use cases (e.g., Bitcoin, Hyperledger, Ripple), identify the type of blockchain used and justify the classification.

**Challenges, Trends, and Research Directions:** Security and privacy in blockchain systems-Legal, regulatory, and ethical considerations-Scalability solutions: Layer-1 vs Layer-2-Blockchain and IoT integration-Future trends: zk-SNARKs, DAGs, CBDCs.

**Activities:** Create a visual representation of block structure, Merkle tree, and hash chaining.

<b>Weightage:</b>	Continuous Assessment: 40%	End Semester Theory Examination: 60%
	(i). Activities: 10% (ii). Internal Theory Examinations: 30%	

**Mandated Activities with marks:**

Assignments (30), Quiz (10), Virtual demonstration (25), Flipped Classroom (10), Review of GATE & IES questions (25).

**Internal Examinations:** TWO tests

**References:**

1. Arvind Narayanan et al., Bitcoin and Cryptocurrency Technologies, Princeton University Press, 2016.
2. Bose, S., & Vijayakumar, P. Cryptography and network security. Pearson (2017).
3. Imran Bashir, Mastering Blockchain, Packt Publishing, 3<sup>rd</sup> Edition, 2020.
4. Andreas M. Antonopoulos, Mastering Bitcoin, O'Reilly Media
5. Melanie Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media

**E-resources:**

1. NPTEL – Blockchain and Its Applications (IIT Kharagpur)
2. NPTEL – Introduction to Blockchain Technology and Applications (IIT Kanpur)

<b>CO</b>	<b>Description of CO</b>	<b>PO</b>	<b>PSO</b>
<b>CO1</b>	Describe the fundamental concepts, architectures, and components of blockchain technologies and distributed ledger systems.	--	--
<b>CO2</b>	<b>Analyze</b> blockchain consensus mechanisms, transaction workflows, and cryptographic foundations to understand performance and security characteristics.	PO1 (3)	PSO1 (3)
<b>CO3</b>	<b>Evaluate</b> blockchain platforms, smart contract models, and application scenarios to assess feasibility, scalability, and trust.	PO3 (2)	PSO2 (2)
<b>CO4</b>	<b>Design</b> blockchain-based solutions by integrating appropriate architectures, protocols, and smart contracts for real-world applications.	PO2 (1)	PSO1 (3)

BC25012	Cyber forensics and Investigation	L	T	P	C
		3	0	0	3
<p><b>Course objectives:</b></p> <ul style="list-style-type: none"> <li>• To gain a comprehensive understanding of cyber forensic principles and the collection, preservation, and analysis of digital evidence.</li> <li>• To combine both the technical expertise and the knowledge required to investigate, detect, and prevent digital crimes.</li> <li>• To understand the different applications and methods for conducting network and digital forensic acquisition and analysis.</li> <li>• To learn the E-evidence collection and preservation, investigating operating systems and file systems, network, cloud, and mobile device forensics.</li> <li>• To gain knowledge on digital forensics legislations, digital crime, forensic processes, and procedures.</li> </ul>					
<p><b>Cyber Forensics Science</b></p> <p><b>Cyber Forensics Science:</b> Forensics Science, Forensics Fundamentals, Computer Forensics, and Digital Forensics. Role of AI/ML in forensic analysis (e.g., pattern recognition in large datasets), behavioral forensics.</p> <p><b>Cyber Crime:</b> Criminalistics in the Investigative Process, Analysis of Cyber Criminalistics Area, Holistic Approach to Cyber-forensics.</p> <p><b>Indian Context:</b> Computer Forensics and Law Enforcement, Forensics Services, Professional Forensics Methodology. Dark web investigations, <b>Magnet AXIOM</b> tool overview.</p>					

## **Network Security Forensics System and Services**

**Forensics on:** Internet Usage – Intrusion - Firewall and Storage Area Network. **Enhanced:** Cloud-native forensics (AWS/Azure logs), **container forensics (Docker/Kubernetes).**

**Cyber-crimes:** Occurrence, Cyber Detectives, Fighting Cyber Crimes.

**New:** Case study on **SolarWinds breach analysis**, SIEM tools (Splunk) for forensic correlation.

**Tools Section:** Open-source Security Tools for Network Forensic Analysis (updated with **Wireshark 4.0**), Requirements for Preservation of Network Data.

**Computer Forensics:** Data Backup and Recovery - Test Disk Suite.

### **Digital Forensics Preservation and Forensic Data Analysis:**

**Digital Repositories:** Evidence Collection – Data Preservation Approaches – Meta Data and Historic records – Legal aspects. Block chain forensics (tracing Bitcoin/Monero). **Forensic Analysis:** Basic Steps in Windows/Linux – Forensic Scenario – Email Analysis – File Signature Analysis – Hash Analysis. **Enhanced:** Automated triage with **KAPE (Kroll Artifact Parser)**. **Advanced Topics:** Forensic Examination of log files (updated with **SIEM integration**), Data-Recovery Solutions, Hiding and Recovering Hidden Data. Deep fake detection tools (e.g., Microsoft Video Authenticator).

### **Cloud, Network and Mobile Forensics:**

**Cloud Forensics:** Working with cloud vendors, obtaining evidence, reviewing logs and APIs. Slack/Teams forensic artifacts. **Mobile Forensics:** Techniques and Tools - Android Device Analysis (updated for **Android 14**) – iOS Forensic Analysis – SIM Forensic Analysis.

**New: eSIM investigations,** IoT device forensics (Alexa /Ring cameras). **Case Study:** Colonial Pipeline ransomware response.

### **Legal Aspects of Digital Forensics:**

**Laws and Ethics:** IT Laws, Digital Evidence Controls, Evidence Handling Procedures. **India's DPDP Act 2023,** GDPR, CCPA implications. **Acts:** Basics of Indian Evidence Act, IPC, CrPC, Electronic Communication Privacy Act, Legal Policies, IT Act 2000/2008.

**Forensic Tools:** Overview of **En Case, Autopsy 4.0, Magnet AXIOM Cloud,** Mobile Forensic Tools, SQLite. Mock courtroom trial workshop.

CO	Description of CO	PO	PSO
CO1	Describe the fundamental principles, processes, and legal considerations involved in cyber forensics and digital investigations.	--	--
CO2	<b>Analyze</b> digital evidence sources, logs, and artifacts to understand acquisition, preservation, and examination procedures.	PO1 (3)	PSO1 (3)
CO3	<b>Evaluate</b> forensic tools, reporting techniques, and incident reconstruction methods to determine accuracy and admissibility.	PO3 (2)	PSO2 (2)
CO4	<b>Design</b> structured investigation workflows by selecting appropriate forensic methodologies, documentation practices, and analysis techniques.	PO2 (1)	PSO1 (3)
Weightage:	Continuous Assessment: 40%	End Semester Theory Examinations: 60%	
	(i) Activity: 10% (ii) Internal Theory Examination: 30%		
Mandated Activities with Marks: Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)			
Internal Examinations: Two Tests			

#### References:

1. J. R. Vacca, Computer Forensics: Computer Crime Scene Investigation, 2nd ed. Charles River Media, 2005.
2. Bose, S., & Vijayakumar, P. Cryptography and network security. Pearson (2017).
3. C. Altheide, R. Carvey, et al., Digital Forensics with Open Source Tools, Syngress, 2011.
4. S. Bommisetty, R. Tamma, O. Skulkin, H. Mahalik, Practical Mobile Forensics, Packt Publishing, 2014.
5. A. Hoog and J. McCash, Android Forensics: Investigation, Analysis, and Mobile Security. Syngress, 2011.
6. C. Altheide and H. Carvey, Digital Forensics with Open Source Tools, Syngress, 2011.

BC25013	Wireless Security	L	T	P	C
		3	0	0	3
<p><b>Course Objective:</b></p> <ul style="list-style-type: none"> <li>• Understand the fundamentals of wireless technologies, WLAN standards, transmission media, and WEP protocol.</li> <li>• Identify and analyze a range of wireless security threats and countermeasures.</li> <li>• Examine security implementations in CDPD, GPRS, GSM, and IP-based wireless data networks.</li> <li>• Explore secure wireless transport protocols like SSL, WTLS, and WAP security architectures.</li> <li>• Evaluate Bluetooth security mechanisms and apply assessment through real-world case studies.</li> </ul>					
<p><b>Wireless Technologies:</b> Introduction to wireless technologies- Wireless data networks- Personal Area Networks -Transmission Media – WLAN standards - Securing WLANS - Countermeasures - WEP (Wired Equivalence Protocol).</p>					
<p><b>Wireless threats:</b> Kinds of security breaches - Eavesdropping - Communication Jamming - RF interference - Covert wireless channels - DOS attack – Spoofing - Theft of services - Traffic Analysis- Cryptographic threats - Wireless security Standards</p>					
<p><b>Security in data networks:</b>Wireless Device security issues - CDPD security (Cellular Digital Packet Data)-GPRS security (General Packet Radio Service) - GSM (Global System for Mobile Communication) security – IP security.</p>					
<p><b>Wireless Transport Layer Security:</b> Secure Socket Layer - Wireless Transport Layer Security - WAP Security Architecture – WAP Gateway.</p>					
<p><b>Bluetooth security:</b> Basic specifications – Pico nets – Bluetooth security architecture – Scatter nets – Security at the baseband layer and link layer – Frequency hopping – Security manager – Authentication – Encryption – Threats to Bluetooth security introduction to security assessment process</p>					

<b>Case studies:</b> Case study 1 – Terrestrial microwave relay systems, Case study 2 – Public safety wireless networks, Case study 3 – Military tactical radio systems, Case study 4 – Satellite communications systems , Case study 5 – Wide Area Wireless Data Services (CDPD, GPRS, etc.), Case study 6 – Wireless LANs (802.11, etc.), Case study 7 – Wireless			
CO	Description of CO	PO	PSO
CO1	Describe the fundamental concepts, vulnerabilities, and security mechanisms associated with wireless communication systems.	--	--
CO2	<b>Analyze</b> wireless threats, attack models, and protection techniques to understand risks across different wireless technologies.	PO1 (3)	PSO1 (3)
CO3	<b>Evaluate</b> wireless security protocols, authentication mechanisms, and intrusion detection techniques to determine their effectiveness.	PO3 (2)	PSO2 (2)
CO4	<b>Design</b> secure wireless network solutions by integrating appropriate encryption methods, access control strategies, and monitoring tools.	PO2 (1)	PSO1 (3)
Weightage:	Continuous Assessment: 40%	End Semester Theory Examinations: 60%	
	(i) Activity: 10%		
	(ii) Internal Examination: 30%	Theory	
Mandated Activities with Marks: Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)			
Internal Examinations: Two Tests			

### References:

1. **Bose, S., & Vijayakumar, P.** Cryptography and network security. Pearson (2017).
2. **William Stallings,** *Wireless Communications and Networks*, 2nd Edition, Pearson Education, 2005.
3. **Jonathan Katz & Yehuda Lindell,** *Introduction to Modern Cryptography*, 2nd Edition, CRC Press, 2014.

4. Mark Ciampa, Security+ Guide to Network Security Fundamentals, 6th Edition, Cengage Learning, 2018.
5. N. Nichols and L. Lekka, Wireless Security: Models, Threats and Solutions. New Delhi: Tata McGraw-Hill, 2006.
6. D. Pollino, Wireless Security. New Delhi: Osborne/McGraw-Hill, 2005.
7. W. Osterhage, Wireless Security. Boca Raton, FL: CRC Press, 2011.

### Web Resources

1. **National Institute of Standards and Technology (NIST) – Wireless Security Guidelines**  
<https://csrc.nist.gov>  
*Official security recommendations and standards for wireless networks.*
2. **IEEE Xplore Digital Library – Wireless Security Journals & Papers**  
<https://ieeexplore.ieee.org>  
*Latest research articles and conference papers on secure wireless technologies.*
3. **OWASP – Mobile Security Project**  
<https://owasp.org/www-project-mobile-security/>  
*Community-driven project focusing on mobile/wireless threats and best practice*

BC25014	Malware Analysis	L	T	P	C
		3	0	0	3
<p><b>Course Objectives:</b></p> <ul style="list-style-type: none"> <li>• To introduce the foundational concepts and methodologies in malware analysis.</li> <li>• To enable students to perform static and dynamic analysis of malware samples.</li> <li>• To explore persistence mechanisms, process injection, and command-and- control (C2) strategies used by malware.</li> <li>• To provide hands-on experience with debugging, unpacking, and memory forensics tools.</li> <li>• To understand anti-analysis techniques and investigate modern malware attack vectors.</li> </ul>					
<p><b>Foundations of Malware Analysis:</b> Introduction to malware – Types: viruses, worms, Trojans, ransomware, spyware, rootkits, botnets – Cyber threat ecosystem and malware lifecycle – Static, dynamic, and memory analysis methodologies – Legal and ethical considerations</p>					
<p><b>Lab:</b> Malware analysis lab setup using virtualization (VMware/VirtualBox), REMnux, INetSim – Host-only networking for safe simulation.</p>					
<p><b>Basic Static and Dynamic Analysis:</b> Hashing techniques (MD5, SHA256) – String analysis and obfuscation detection (FLOSS) – PE file format and analysis tools (PE-bear, PEview) – Import/export function analysis using Dependency Walker – Basic dynamic analysis using sandboxing – Behavioral monitoring with Process Monitor, Process Hacker – Network monitoring with Wireshark – Generating Indicators of Compromise (IoCs).</p>					
<p><b>Malware Functionality and Persistence:</b> Persistence techniques: registry keys, scheduled tasks, startup folders, malicious services – Process injection: DLL injection, process hollowing, thread hijacking – Information stealing methods – Encoding techniques: Base64, XOR – C2 communication techniques: beaconing, heartbeat traffic, protocols (HTTP, DNS tunneling).</p>					
<p><b>Advanced Dynamic Analysis:</b> Debugging  Debugging basics – Breakpoints and execution control – Debuggers: x64dbg, OllyDbg – Inspecting stack, memory, and registers – Runtime analysis of malware behavior – Extracting decrypted configurations – Memory forensics using Volatility Framework – Detection of injected code, rogue processes, and C2 data in RAM.</p>					

**Anti-Reverse Engineering and Modern Vectors:** Anti-analysis techniques: obfuscation, anti-debugging, anti-VM – Packers and unpacking using Detect It Easy – Manual unpacking with debugger (finding OEP) – Script-based malware: PowerShell, JavaScript – Analysis of malicious documents: VBA macros, RTF shellcode – Shellcode extraction and basic analysis.

CO	Description of CO	PO	PSO
CO1	Describe the fundamental concepts, lifecycle, and behavior characteristics of malware and malicious software.	--	--
CO2	<b>Analyze</b> malware samples, artifacts, and behavior patterns to understand infection techniques and system impact.	PO1 (3)	PSO1 (3)
CO3	<b>Evaluate</b> static and dynamic analysis tools, sandboxing techniques, and detection mechanisms to assess their effectiveness.	PO3 (2)	PSO2 (2)
CO4	<b>Design</b> malware analysis workflows by selecting appropriate tools, procedures, and reporting strategies for real-world investigations.	PO2 (1)	PSO1 (3)
Weightage:	Continuous Assessment: 40% (i) Activity: 10% (ii) Internal Theory Examination: 30%	End Semester Theory Examinations: 60%	
Mandated Activities with Marks: Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)			
Internal Examinations: Two Tests			

## References

1. M. Sikorski and A. Honig, *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*, No Starch Press, 2012.
2. M. Egele, D. Brumley, Y. Fratantonio, and C. Kruegel, *Software Security: Principles, Policies, and Protection*, Springer, 2015.
3. M. Ligh, S. Adair, B. Hartstein, and M. Richard, *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*, Wiley, 2010.
4. D. Solomon and A. Russinovich, *Windows Internals*, 6th Edition, Microsoft Press, 2012.
5. V. P. Sachdeva, *Fundamentals of Cybersecurity*, Wiley India, 2020.
6. R. A. Carbone, *The Art of Memory Forensics*, Wiley, 2014.

BC25015	<b>Ethical Hacking and Network Defence</b>	L	T	P	C
		3	0	0	3

**Course Objective:**

- A strong ethical framework and a comprehensive understanding of the legal boundaries and professional responsibilities that govern penetration testing and cybersecurity operations.
- Equip students with a systematic, phase-based methodology for identifying, analyzing, documenting, and exploiting vulnerabilities within network infrastructures, computer systems, and applications.
- Develop advanced practical skills in utilizing a broad range of industry- standard tools and techniques
- Conducting both offensive security assessments and implementing proactive network defense measures.
- Foster a deep understanding of modern defensive architectures and strategies, including the core principles of intrusion detection, prevention systems, and the operational use of Security Information and Event Management (SIEM).

**Foundations of Offensive and Defensive Security:**

Introduction to Ethical Hacking concepts - hacker classifications - Rules of Engagement (RoE) - scoping - Legal and ethical frameworks - CFAA - IT Act - PCI-DSS - HIPAA - The Cyber Kill Chain & MITRE ATT&CK framework - Review of TCP/IP - OSI model - fundamental cryptographic concepts.

**Reconnaissance, Scanning, and Vulnerability Analysis:**

Passive and Active Reconnaissance - Footprinting - Open-Source Intelligence (OSINT) - Google Hacking - theHarvester - Maltego - Shodan - Network Scanning using Nmap - Host discovery - port scanning techniques - service version detection - evasion methods - Enumeration of services - SNMP - NetBIOS - LDAP - Active Directory - Automated Vulnerability Scanning - Nessus - OpenVAS - analysis of results - false positive validation.

**System Exploitation, Persistence, and Anti-Forensics:**

Gaining Access - Exploitation using the Metasploit Framework - payloads - shells - Password Attacks - Online brute-force - offline hash cracking - Hydra - John the Ripper - Hashcat - Post-Exploitation - Privilege escalation for Windows and Linux - Maintaining Access - Persistence - backdoors - web shells - Trojans - Covering Tracks - Anti-Forensics - Log clearing - data hiding - steganography.

### **Advanced Attack Vectors: Web, Wireless, And Emerging Threats**

Web Application Hacking - OWASP Top 10 - SQL Injection (SQLi) - Cross-Site Scripting (XSS) - Burp Suite - sqlmap - Wireless Network Hacking - WPA2-PSK attacks - capturing handshakes - rogue access points - Social Engineering - Phishing - pretexting - Social-Engineer Toolkit (SET) - Emerging threats - IoT - OT - Cloud Security - misconfigurations - vulnerabilities.

### **Proactive Network Defence and Incident Response:**

Defensive Architecture - Defense-in-Depth - Firewalls - Intrusion Detection/Prevention Systems (IDS/IPS) - Security Operations and Monitoring - SOC functions - SIEM - network traffic analysis with Wireshark - Cyber Threat Intelligence (CTI) lifecycle - Indicators of Compromise (IoCs) - Incident Response - NIST framework - Preparation - Detection - Containment - Eradication - Recovery - Professional penetration test reporting - communication

### **References**

1. Bose, S., & Vijayakumar, P. *Cryptography and network security*. Pearson (2017).
2. Wilson, Michael, and Nicholas Antill. *Hands-On Ethical Hacking and Network Defense, 4th Edition*. Cengage Learning, 2024.
3. Kim, Peter. *The Hacker Playbook 3: Practical Guide to Penetration Testing*. Secure Planet LLC, 2018.
4. Stallings, William, and Lawrie Brown. *Computer Security: Principles and Practice, 4th Edition*. Pearson, 2018.
5. Weidman, Georgia. *Penetration Testing: A Hands-On Introduction to Hacking*. No Starch Press, 2014.
6. Stuttard, Dafydd, and Marcus Pinto. *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, 2nd Edition*. Wiley, 2011.
7. Sikorski, Michael, and Andrew Honig. *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. No Starch Press, 2012.
8. Erickson, Jon. *Hacking: The Art of Exploitation, 2nd Edition*. No Starch Press, 2008.

CO	Description of CO	PO	PSO	
CO1	Describe the fundamental concepts, methodologies, and ethical considerations involved in ethical hacking and network defence.	--	--	
CO2	<b>Analyze</b> network vulnerabilities, attack strategies, and penetration testing techniques to understand system weaknesses.	PO1 (3)	PSO1 (3)	
CO3	<b>Evaluate</b> security controls, defensive mechanisms, and remediation strategies to determine their effectiveness in mitigating attacks.	PO3 (2)	PSO2 (2)	
CO4	<b>Design</b> ethical hacking and defence strategies by planning assessments, implementing protections, and documenting findings for real-world environments.	PO2 (1)	PSO1 (3)	
Weightage:	Continuous Assessment: 40% (i) Activity: 10% (ii) Internal Theory Examination: 30%	End Semester Theory Examinations: 60%		
Mandated Activities with Marks: Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)				
Internal Examinations: Two Tests				

BC25016	E-Commerce Security	L	T	P	C
		3	0	0	3

**Course Objective:**

The course aims to:

1. To introduce the fundamental principles and architecture of e-commerce and its security needs.
2. To understand the key technologies and cryptographic techniques used to secure electronic transactions.
3. To explore authentication, integrity, and confidentiality mechanisms for secure e-commerce applications.
4. To examine the risks, threats, and legal frameworks affecting digital payments and e-commerce infrastructures.
5. To analyze real-world e-commerce security models and develop secure electronic commerce solutions.

**Introduction to E-Commerce and Security**

E-commerce models – E-commerce architecture – Components – Payment systems overview – Need for security in e-commerce – Security goals – Security threats – E-commerce risks and risk management.

**Cryptography for E-Commerce**

Symmetric and asymmetric cryptography – RSA, AES – Key distribution – Hash functions – Digital signatures – Public Key Infrastructure (PKI) – Secure sockets layer (SSL)/Transport Layer Security (TLS).

**Authentication and Access Control**

User authentication protocols – Two-factor and biometric authentication – Digital certificates – Access control models – Federated identity management – OAuth, SAML.

**Securing Transactions and Payment Systems**

Secure Electronic Transaction (SET) – E-cash, E-cheque – Credit card frauds – Secure Payment Gateway – Mobile payments and wallet security – Blockchain and smart contract basics.

**Legal, Ethical and Real-World Practices**

Cyber laws and IPR in e-commerce – Data privacy policies – GDPR, PCI DSS – Indian IT Act 2000 (amended) – Case studies on secure e-commerce platforms – Security best practices.

CO	Description of CO	PO	PSO
CO1	Describe the fundamental concepts, threats, and security requirements associated with e-commerce systems.	--	--
CO2	<b>Analyze</b> e-commerce architectures, payment mechanisms, and transaction models to understand potential risks and vulnerabilities.	PO1 (3)	PSO1 (3)

<b>CO3</b>	<b>Evaluate</b> security protocols, trust models, and fraud prevention techniques used in e-commerce environments.	PO3 (2)	PSO2 (2)
<b>CO4</b>	<b>Design</b> secure e-commerce solutions by integrating appropriate authentication, encryption, and risk-management mechanisms.	PO2 (1)	PSO1 (3)

Weightage:	Continuous Assessment: 40%	End Semester Theory Examinations: 60%
	(i) Activity: 10% (ii) Internal Theory Examination: 30%	
Mandated Activities with Marks: Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)		
Internal Examinations: Two Tests		

### References

1. **Bose, S., & Vijayakumar, P.** Cryptography and network security. Pearson (2017).
2. **William Stallings**, *Cryptography and Network Security: Principles and Practice*, Pearson Education, 7th Edition, 2017.
3. **Kenneth C. Laudon & Carol G. Traver**, *E-Commerce 2020: Business, Technology, and Society*, Pearson, 16th Edition, 2020.
4. **Pankaj Sharma**, *E-Commerce Security and Cyber Laws*, APH Publishing Corporation, 2019.
5. **B. Nina Godbole & Sunit Belpure**, *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*, Wiley India, 2011.

### Web Resources

1. **NIST Cybersecurity Framework for E-Commerce**  
<https://www.nist.gov/cyberframework>
2. **OWASP – Application Security Resources**  
<https://owasp.org>
3. **PCI Security Standards Council (PCI-DSS Guidelines)**  
<https://www.pcisecuritystandards.org>

CP25C24	Vibe Coding	L	T	P	C
		3	0	0	3
<p><b>Course Objective:</b>  This course introduces the basics of AI-assisted coding and Vibe Coding. Participants will learn to use AI tools, build simple applications, and understand the roles and ethics involved. By the end, they will create their own AI-powered projects.</p>					
<p><b>Introduction To Vibe Coding and Human-Ai Collaboration</b></p> <p>Introduction to Vibe Coding-Basic Prompting Techniques for Coding Tasks-Roles and -Responsibilities in Human-AI Collaboration-AI Assistant-Prompt Engineer-Developer-Designing Simple AI-Augmented Workflows-Interaction Between AI-Generated Code and Developer Feedback</p> <p><b>Activities:</b></p> <ul style="list-style-type: none"> <li>• <b>Role Play:</b> Students take on roles such as AI, prompt engineer, and developer to simulate collaborative coding.</li> <li>• <b>Flipped Classroom &amp; Quiz:</b> Students learn prompting basics at home and participate in a class quiz and discussion.</li> </ul>					
<p><b>Tools And Platforms for Ai-Assisted Coding</b></p> <p>Overview of AI-Assisted Coding Tools-Cursor, v0, Bolt, etc.-Features and Use Cases of Each Tool-Setting Up and Navigating AI-Coding Platforms-Building Simple Web Applications with AI -Integration-Workflow Prototyping Using AI Tools</p> <p><b>Activities:</b></p> <ul style="list-style-type: none"> <li>• <b>Flipped Classroom &amp; Hands-on Tutorial:</b> Students explore AI tools (e.g., Cursor or v0) at home and build a basic app in class.</li> <li>• <b>Team Activity:</b> Groups design a simple development workflow using AI tools and explain tool selection and purpose.</li> </ul>					
<p><b>AI Prompt Design, Oversight, and Ethical Coding Practices</b></p> <p>6Vibe Coder’s Toolkit: Prompts, Context, and Flow-Prompt Optimization Techniques-Human Oversight in AI Coding Systems-Ethical and Responsible AI Usage-Challenges and Best Practices in AI-Augmented Development</p> <p><b>Activities:</b></p> <ul style="list-style-type: none"> <li>• <b>Team Presentation:</b> Each group presents a complete AI workflow, including prompt design, context handling, and oversight strategy.</li> <li>• <b>Ethical Case Discussion:</b> Class discussion on accountability, code quality, and risks of over-reliance on AI in software development.</li> </ul>					
<p><b>The Unbundled Programmer and the Future of Coding Roles</b></p> <p>Evolving Developer Roles in the AI Era-The Shift from Coding to Orchestration and Strategy-AI Integration Across the Software Development Lifecycle-Human-AI</p>					

Collaboration in Debug, Design, and Deployment-Strategic Thinking and Adaptability in AI-Augmented Teams

### Activities

- **Team Presentation:** Showcase how AI transforms developer roles across the SDLC.
- **Role Play & Quiz:** Simulate a modern dev team using AI tools and complete a quiz based on workflow observations.

### Code Quality, Reliability, and Ethical Development

Long-Term Maintainability of AI-Generated Code-Refactoring AI-Assisted Code for Clarity and Standards-Documentation Strategies for Mixed Human-AI Codebases-Common Security and Reliability Issues in Vibe Code-Ethical Coding Practices in AI-Augmented Environments-Navigating Cultural Shifts in 'Vibe Coding' and Accountability

### Activities:

- **Tutorial & MCQ:** Refactor example AI-generated code and answer related questions on quality and security.
- **Flipped Classroom:** Study ethical case studies at home and present findings in class.

### Applied Projects and Real-World AI Applications

6AI-Powered Task Manager and To-Do Lists-Resume Builder with Smart AI Suggestions-Note-Taking App with Auto-Organization-Recipe Generator with Ingredient Substitution Logic-Visual Memory Game Using AI Tools-Non-diagnostic Health Symptom Checker

### Activities

- **Team Project:** Build a working prototype (e.g., to-do list, resume builder) using AI-assisted tools.
- **Presentation & Quiz:** Present the final project and complete a quiz on the design and development process.

### Advanced AI-Driven Web Application Deployment

Planning and Scoping AI-Assisted Applications-Workflow Mapping from Idea to Deployment-Integrating Front-End, Back-End, and AI Logic-Testing and Deploying AI-Augmented Applications-Human Oversight and Continuous Improvement Loops-Project Ownership and Accountability in AI Codebases

### Activities

- **Capstone Project:** Design and deploy a full AI-assisted web application as a team.
- **Demo Day & Reflection:** Teams demo their solutions and reflect on human-AI collaboration challenges.

CO	Description of CO	PO	PSO
CO1	Describe the fundamental ideas, philosophy, and collaborative practices behind vibe coding as a modern approach to software development.	--	--
CO2	<b>Analyze</b> vibe coding workflows, teamwork dynamics, and tool ecosystems to understand productivity and creativity impacts.	PO1 (3)	PSO1 (3)
CO3	<b>Evaluate</b> real-world applications, coding communities, and project outcomes developed using vibe coding principles.	PO3 (2)	PSO2 (2)
CO4	<b>Design</b> software development practices and project workflows using vibe coding concepts, tools, and collaborative strategies.	PO2 (1)	PSO1 (3)
<b>Weightage:</b>	<b>Continuous Assessment: 40%</b> <b>(i) Activity: 10%</b> <b>(ii) Internal Theory Examination: 30%</b>	<b>End Semester Theory Examinations: 60%</b>	
<b>Mandated Activities with Marks:</b> Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)			
<b>Internal Examinations: Two Tests</b>			

#### References:

1. Ted Winston, *Mastering Vibe Coding: Build, Debug, and Ship Software with AI Assistants like Cursor, Replit, and GPT*, Kindle Edition, April 25, 2025.
2. Ethan Voss, *Vibe Coding: Build & Sell Apps Without Coding Experience: How to Use AI to Create Profitable Apps Even If You've Never Written a Line of Code*, Kindle Edition, 26 March 2025.
3. Amit Iyer, *Beginner's Guide to Vibe Coding: Exploring Features, Use Cases and Understanding Vibe Coding*, Paperback, 19 March 2025.
4. Gene Kim, Steve Yegge, *Vibe Coding: Building Production-grade Software With GenAI, Chat, Agents, and Beyond*, Paperback, 21 October 2025.
5. Addy Osmani, *Beyond Vibe Coding*, O'Reilly Media, Inc., August 2025. ISBN: 9798341634756

CP25C20	Agentic AI	L	T	P	C
		3	0	0	3
<p><b>Course Objectives:</b></p> <ol style="list-style-type: none"> <li>1. Understand the foundations and architecture of intelligent agents.</li> <li>2. Design agents capable of autonomous and rational decision-making.</li> <li>3. Apply reinforcement learning for adaptive agent behavior.</li> <li>4. Explore coordination in multi-agent and human-AI systems.</li> <li>5. Analyse the ethical implications of agentic systems.</li> <li>6. Develop real-world applications using modern agent-based AI frameworks.</li> </ol>					
<p><b>Foundations of Intelligent Agents</b></p> <p>Introduction to Agentic AI: History, Motivation, Applications - Agents and Environments: Sensors, Actuators, Environment Types - Types of Agents: Simple Reflex, Goal-Based, Utility-Based, Learning Agents - Architectures: Reactive, Deliberative, Hybrid, Subsumption</p> <p><b>Activity:</b></p> <ul style="list-style-type: none"> <li>• Report preparation about types of Agents, role and architecture of each agent</li> </ul>					
<p><b>Agent Decision-Making and Planning</b></p> <p>Rationality and Utility Theory - Task Environment Analysis - AI Planning Techniques: STRIPS, Classical Planning - Decision-Making under Uncertainty: MDPs, Bayesian Models, Game Theory</p> <p><b>Activity:</b></p> <ul style="list-style-type: none"> <li>• Design a simple application for making decision using AI in python</li> </ul>					
<p><b>Learning in Agentic Systems</b></p> <p>Reinforcement Learning: Q-Learning, SARSA - Value and Policy Iteration - Deep RL: DQNs, Policy Gradient Methods, Actor-Critic - Tools: OpenAI Gym, PettingZoo, TensorFlow RL</p> <p><b>Activity:</b></p> <ul style="list-style-type: none"> <li>• Write a case study for Tools about OpenAI and TensorFlow with proper application</li> </ul>					
<p><b>Multi-Agent Systems and Collaboration</b></p> <p>Multi-Agent Coordination: Cooperation, Competition - Agent Communication and Negotiation - Human-AI Collaboration: Interactive and Mixed-Initiative Systems - Platforms: NetLogo, RoboCup Simulation</p> <p><b>Activity:</b></p> <ul style="list-style-type: none"> <li>• Create Autonomous agents using NetLogo platform</li> </ul>					

## LLM Agents and Embodied Cognition

Language-based Agents: Tool Use, Planning, and Reasoning - Memory-Augmented and Situated Agents - Agents in Robotics and Smart Environments - Unity ML-Agents, Hugging Face Tools

### Activity:

- Design a simple application based on LLM-based tool-using agents

## Ethics and Applications of Agentic AI

AI Alignment, Fairness, Explainability - Social and Environmental Implications - Case Studies: Autonomous Vehicles, Conversational Agents - Course Project Evaluation and Presentations

### Activity:

- Agent-based simulations for real-world problems

### References:

1. Artificial Intelligence: A Modern Approach, Russell & Norvig, 4th Ed., Pearson, 2021
2. Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations, Shoham & Leyton-Brown, CUP, 2009
3. Reinforcement Learning: An Introduction, Sutton & Barto, 2nd Ed., MIT Press, 2018

### Tools & Technologies:

**Languages:** Python

**Libraries:** PyTorch, TensorFlow, OpenAI Gym, LangChain

**Frameworks:** PettingZoo, Unity ML-Agents, NetLogo, Hugging Face

**Platforms:** Jupyter, VS Code, RoboCup Simulators

<b>Weightage:</b>	<b>Continuous Assessment: 40%</b>	<b>End Semester Theory Examinations: 60%</b>
	<b>(i) Activity: 10%</b> <b>(ii) Internal Theory Examination: 30%</b>	

### Mandated Activities with Marks:

Assignments (30), Quiz (10), Virtual Demo (25), Flipped Class Room (10), Review of Gate and IES Questions (25)

**Internal Examinations: Two Tests**

CO	Description of CO	PO	PSO
CO1	Describe the fundamental concepts, architectures, and principles of agentic artificial intelligence and autonomous agent systems.	--	--
CO2	Analyze agentic AI models and decision-making mechanisms to understand autonomy, goal-directed behavior, and interaction in intelligent agents.	PO1 (3)	PSO1 (3)

<b>CO3</b>	Evaluate agentic AI frameworks, learning strategies, and coordination techniques to assess their effectiveness in complex and dynamic environments.	PO3 (2)	PSO2 (2)
<b>CO4</b>	Design agentic AI solutions by selecting appropriate agent architectures, learning methods, and coordination mechanisms for real-world applications.	PO2 (1)	PSO1 (3)