Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Network Security & Cryptography
Course Code	CY-401
Semester	4
Course Category	Program Core Courses
Credits	3
Hours per Week	3L:0T:4P

1. Prerequisites

• Fundamentals of Computer Networks and Operating Systems (including OSI model basics)

• Discrete Mathematics and Number Theory (modular arithmetic, primes, GCD, basic probability)

• Programming proficiency (e.g., Python or C)

2. Course Learning Objectives

• This course introduces students to fundamental concepts and applications of the subject

• Students will learn theoretical foundations and practical skills relevant to the field

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	Class Test Full marks	Assignment Full marks	Attendance Full marks	Total Marks
CIA-1	25	10	5	40
CIA-2	25	10	5	40
End Semester Examination (ESE)	–	–	–	60
Total				100

5. Course Modules

Module	Topics	Hours
1	**Foundations of Information Security** - Objectives of information security - Confidentiality, Integrity, Authentication, Availability (CIA) model - Risk management and security governance basics - Common threat categories for computers, networks and AI-driven systems - Intrusion concepts and basic intrusion-detection approaches - Legal, regulatory and ethical issues (including data-privacy regulations) - Security principles and defense-in-depth strategy - Types of attacks (passive vs. active) and typical attack vectors - Core security services: confidentiality, integrity, non-repudiation, availability - Fundamental security mechanisms: encryption, access control, auditing, logging - OSI security architecture and a practical network-security model - Overview of cyber-crimes and emerging AI-related security concerns	6
2	**Classical Cryptography and Theoretical Foundations** - Introduction and objectives of cryptography - Classical encryption techniques: substitution and transposition - Classic ciphers (Caesar, Vigenère, Playfair, etc.) - Concept of perfect secrecy and basic information-theoretic ideas - One-way and trap-door functions (high-level view) - Cryptanalysis fundamentals and common attack models	7

	- Number-theoretic basics needed for modern crypto: * Modular arithmetic, Euclid's algorithm and GCD * Prime numbers, simple primality testing, factorisation concepts * Euler's totient, Fermat's and Euler's theorems (conceptual) - Introduction to steganography - High-level view of linear & differential cryptanalysis (conceptual only) - Relevance of classical crypto to modern AI data-protection scenarios	
3	**Symmetric-Key Cryptography** - Principles of symmetric-key encryption - Block-cipher fundamentals and design criteria - Data Encryption Standard (DES) and its variants (3DES) - Advanced Encryption Standard (AES) - structure, security evaluation - Other notable block ciphers (Blowfish, RC5, IDEA) - overview - Block-cipher modes of operation (ECB, CBC, CFB, OFB, CTR, GCM/AEAD) - Stream ciphers: RC4 and LFSR-based designs - Cryptographically secure pseudorandom number generators (CSPRNGs) - Key size, key-space considerations and basic key-management practices - Typical attacks on symmetric algorithms (brute-force, related-key, differential, linear) - Authenticated encryption for protecting AI model parameters and data	8
4	**Asymmetric Cryptography, PKI & Key Management** - Principles of public-key cryptosystems (high-level) - Core mathematical tools (modular exponentiation, discrete logarithms - conceptual) - RSA algorithm: key generation, encryption/decryption, digital signatures - Diffie-Hellman key exchange and its practical variants - ElGamal encryption and signature scheme (overview) - Digital Signature Algorithm (DSA) and Schnorr signatures - basics - Elliptic-Curve Cryptography (ECC) - high-level concepts and why it matters for lightweight AI devices - Public-Key Infrastructure (PKI): X.509 certificates, certificate authorities, trust chains - Kerberos authentication service and ticket-granting mechanisms - Secure key distribution for federated learning and AI model sharing	7
5	**Hash Functions, MACs & Authentication Protocols** - Cryptographic hash functions: MD5, SHA-1, SHA-2 family, SHA-3 overview - Desired hash properties and known practical attacks - Password-hashing best practices (bcrypt, scrypt, Argon2) - Message Authentication Codes (MAC): definition, HMAC, CMAC - Keyed hash functions and security considerations - Recap of digital signatures (RSA, DSA, ECDSA, Schnorr) - Authentication requirements and mechanisms for AI services - Entity authentication techniques: passwords, challenge-response, biometrics, token-based methods - Zero-knowledge proof protocols (high-level view)	6

	- Secure multiparty computation - conceptual overview for privacy-preserving AI - Relevant standards (IEEE, ISO/IEC 27001, NIST SP 800-63)	
6	**Security Protocols, Network & Application Security, Emerging Topics** - Network security models and firewall architectures (packet-filter, stateful, next-gen) - IP Security (IPSec) suite: AH, ESP, IKE, security associations - Transport-layer security: SSL/TLS architecture, HTTPS, secure coding guidelines - Secure Shell (SSH) and remote-access best practices - Wireless security fundamentals: IEEE 802.11, WPA3, device-level protections - Email security mechanisms: PGP and S/MIME (key management, signing, encryption) - Web-application security: XSS, SQL injection, CSRF, secure coding, web application firewalls - Cloud security basics: IAM, network access control, container security - Case studies: Single Sign-On (SSO), secure inter-branch payments, cloud-based AI service hardening - AI-specific security topics: * Adversarial machine-learning attacks and defenses * Model poisoning and data-poisoning mitigation * Secure inference and homomorphic encryption basics * Differential privacy for training data * Federated learning security considerations - Side-channel attacks and practical countermeasures - Overview of post-quantum cryptography concepts (high-level, no deep math)	8

6. References

Textbooks:

1. William Stallings, "Cryptography and Network Security - Principles and Practice", Seventh Edition, Pearson Education, 2017.

2. Cryptography and Network Security: Atul Kahate, Mc Graw Hill, 3rd Edition.

Reference Books:

1. Behrouz A. Ferouzan, Debdeep Mukhopadhyay, "Cryptography and Network Security", 3rd Edition, Tata Mc Graw Hill, 2015.

2. Charles Pfleeger, Shari Pfleeger, Jonathan Margulies, "Security in Computing", Fifth Edition, Prentice Hall, New Delhi, 2015.

3. Nina Godbole, Sunit Belapure, "Cyber Security: Understanding Cyber crimes, Computer Forensics and Legal Perspectives", First Edition, Wiley India, 2011.

4. Cryptography and Network Security: C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, 1st Edition.

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-401.1	Recall and list the fundamental concepts of information security, including the CIA triad, risk-management components, common threat categories, and core security principles such as defense-in-depth.	Recall	Remember
CY-401.2	Explain the operation and mathematical basis of classical cryptographic techniques (e.g., substitution ciphers, Caesar, Vigenère) and the foundational number-theoretic concepts needed for modern cryptography.	Explain	Understand
CY-401.3	Apply symmetric (AES, block-cipher modes) and asymmetric (RSA, ECC) encryption algorithms, together with appropriate key-management practices, to protect data confidentiality and integrity in AI model storage and transmission.	Apply	Apply
CY-401.4	Analyze given network and application configurations to identify vulnerabilities in protocols (e.g., TLS, IPSec, SSH) and recommend mitigation measures such as firewall rules, secure-coding practices, or protocol hardening.	Analyze	Analyze
CY-401.5	Evaluate the effectiveness of selected cryptographic and AI-specific security controls (e.g., homomorphic encryption, differential privacy, federated-learning safeguards) against defined adversarial threat scenarios, using criteria from standards like NIST SP 800-163.	Evaluate	Evaluate
CY-401.6	Design a comprehensive security architecture for a cloud-based AI service that integrates cryptographic primitives, secure protocols, AI-focused defenses, and governance mechanisms, and justify the design choices with risk-assessment outcomes and compliance requirements.	Design	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	-	1	-	2	-	2	-	-	-	1
CO2	3	2	1	2	1	2	-	2	-	-	-	2
CO3	3	2	3	2	3	2	2	2	2	2	2	3
CO4	2	3	2	3	2	2	-	2	2	2	2	2

CO5	2	3	2	3	2	2	2	3	2	2	2	3
CO6	3	3	3	3	3	3	3	3	3	3	3	3

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	1	2
CO2	3	1	2
CO3	3	3	2
CO4	2	3	1
CO5	2	2	3
CO6	3	3	3

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Artificial Intelligence
Course Code	CY-402
Semester	4
Course Category	Program Core Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

• Introduction to Discrete Mathematics

• Fundamentals of Computer Science (including data structures and algorithms)

• Basic Probability and Statistics

2. Course Learning Objectives

• To provide students with a comprehensive understanding of the fundamental principles of Artificial Intelligence (AI) and their application to various cybersecurity challenges.

• To equip students with the ability to model and solve cybersecurity problems using AI techniques, including search algorithms, knowledge representation and reasoning, and probabilistic methods.

• To enable students to critically evaluate and apply machine learning algorithms for addressing real-world cybersecurity threats such as malware detection, intrusion detection, and anomaly detection.

• To foster students' understanding of the ethical implications and societal impact of AI in cybersecurity, promoting responsible AI development and deployment.

• To develop students' problem-solving skills in the context of cybersecurity by applying AI techniques to analyze security scenarios, design intelligent agents, and propose effective mitigation strategies.

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	**Class Test Full Marks**	**Assignment Full Marks**	**Attendance Full Marks**	**Total Marks**
CIA-1	25	10	05	40
CIA-2	25	10	05	40
End Semester Examination (ESE)	-	-	-	60
Total				100 Marks

5. Course Modules

Module	**Topics**	**Hours**
1	**Introduction to AI and Intelligent Agents for Cybersecurity** - What is AI and its relevance to Cybersecurity? - History of AI and its impact on security threats - Foundations of AI: Symbolic vs. Subsymbolic AI - The State of the Art in AI for Cybersecurity - Intelligent Agents in Cybersecurity: Intrusion Detection, Threat Hunting - Agents and Environments: Network Security as an environment - Good Behavior: Defining rational security agents - The Nature of Cybersecurity Environments: Dynamic, adversarial	10

	- The Structure of Security Agents: Knowledge representation, reasoning - PEAS (Performance Measure, Environment, Actuators, Sensors) in a security context - Types of Cybersecurity Environments: Network, endpoint, cloud - Types of Security Agents: Reactive, proactive, learning - Agent Design Philosophies for Security: Robustness, resilience, explainability	
2	**Problem Solving and Search in Cybersecurity** - Problem-Solving Agents for Security: Vulnerability detection, incident response - Formulating Security Problems: Defining goals, constraints, metrics - Searching for Solutions: Exploring attack paths, identifying vulnerabilities - State Space Representation in Security: Network configurations, system states - SAGP (State, Action, Goal test, Path cost) in Security Scenarios - Uninformed Search Strategies (BFS, DFS) for Security: Network scanning, vulnerability analysis (complexity discussion limited) - Informed Search Strategies (Greedy best-first search, A*) for Security: Prioritized vulnerability assessment - Heuristic Functions for Security: Risk scoring, threat prioritization - Constraint Satisfaction Problems (CSPs) in Security: Access control, policy enforcement	6
3	**Knowledge Representation & Reasoning for Cybersecurity** - Knowledge-Based Agents for Security: Intrusion detection systems, threat intelligence platforms - Propositional Logic for Security Policies: Representing access control rules - First-Order Logic for Security Modeling: Representing relationships between entities and threats (simplified) - Knowledge Representation in Security: Vulnerability databases, threat intelligence feeds - Rule-Based Systems for Security: Intrusion detection rules, firewall rules - Search-Based Planning for Security: Incident response planning, vulnerability remediation planning	7
4	**Probabilistic Reasoning and Security**	6

	- Quantifying Uncertainty in Cybersecurity: Risk assessment, threat modeling - Basic Probability Notation and its application to security events - Conditional Probability in Security: Analyzing attack success probabilities - Bayes' Theorem for Security: Spam filtering, anomaly detection - Bayesian Networks for Security: Modeling dependencies between security events - Decision Theory in Security: Resource allocation, risk mitigation strategies	
5	**Machine Learning for Cybersecurity** - Introduction to Machine Learning for Security: Malware detection, intrusion detection - Supervised Learning for Security: Classification of malware, phishing detection - Decision Tree Learning for Security: Building models for threat classification - Perceptron Learning and its application to security (simplified) - Unsupervised Learning for Security: Anomaly detection, clustering of malicious activity - Reinforcement Learning for Security: Developing adaptive security systems	6
6	**Cybersecurity Applications of AI and Ethical Considerations** - Expert Systems for Security: Vulnerability assessment tools, security auditing systems - AI-driven Security Tools and Techniques: SIEM, SOAR - Applications of AI in Cybersecurity: Threat intelligence, incident response - AI Ethics in Cybersecurity: Bias in AI models, responsible AI development, privacy implications - Case studies of AI in real-world cybersecurity incidents	7

6. References

Textbooks:

1. S. Russell and P. Norvig, "Artificial Intelligence: A Modern Approach, Prearson Education, 4th Edition, 2022

2. Elaine Rich and Kevin Knigh, Introduction to Artificial Intelligence, McGraw Hill, Third Edition, 2017.

Reference Books:

1. Michael Negnevitsley, Artificial Intelligence: A guide to Intelligent Systems, Addison Wesley, Third Edition, 2017.

2. G.F. Luger, and W.A. Stubblefield, Artificial Intelligence: Structures and Strategies for Complex Problem Solving, Addison-Wesley Publishing Company, 2011.

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
PCC-CS 402.1	Define and differentiate various types of intelligent agents and cybersecurity environments, explaining their characteristics and applicability within different security contexts (e.g., network, endpoint, cloud).	Define, Differentiate, Explain	Understand
PCC-CS 402.2	Apply uninformed and informed search algorithms (BFS, DFS, A*, Greedy Best-First Search) to solve cybersecurity problems, such as identifying attack paths or prioritizing vulnerabilities, and evaluate their effectiveness in specific scenarios.	Apply, Evaluate	Apply
PCC-CS 402.3	Analyze and model cybersecurity scenarios using propositional and first-order logic, and design rule-based systems for tasks like intrusion detection or access control, justifying the chosen representation and reasoning methods.	Analyze, Model, Design, Justify	Analyze
PCC-CS 402.4	Evaluate and apply probabilistic reasoning techniques, including Bayes' Theorem and Bayesian networks, to quantify uncertainty in cybersecurity risk assessment and threat modeling, and make informed decisions based on probabilistic evidence.	Evaluate, Apply, Make	Apply
PCC-CS 402.5	Develop and implement machine learning models (e.g., decision trees, perceptrons) for	Develop, Implement, Compare, Address	Create

	cybersecurity applications such as malware detection or anomaly detection, comparing their performance and addressing potential limitations, including ethical considerations.		
PCC-CS 402.6	Critically evaluate the ethical implications of AI in cybersecurity, including bias in AI models and responsible AI development, and analyze real-world case studies to demonstrate the impact of AI on cybersecurity incidents and practices.	Critically Evaluate, Analyze	Evaluate

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	1	1	1	1	1	2	1	1
CO2	3	3	2	2	2	1	1	1	2	2	2	1
CO3	3	3	3	2	2	1	1	1	2	2	2	1
CO4	3	3	2	2	2	1	1	1	2	2	2	1
CO5	3	2	3	2	3	2	1	3	2	2	2	1
CO6	1	2	1	2	1	3	2	3	2	2	1	1

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	1	1
CO2	3	1	1
CO3	3	1	1
CO4	3	1	1
CO5	3	3	2
CO6	2	1	3

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Computer Networks
Course Code	CY-403
Semester	4
Course Category	Program Core Courses
Credits	3
Hours per Week	3L:0T:4P

1. Prerequisites

• Fundamentals of computer architecture and operating systems (including binary representation, memory hierarchy, and process management)

• Basic programming proficiency (e.g., Python or C) with understanding of data structures and algorithmic thinking

• Discrete mathematics fundamentals (logic, sets, combinatorics, and basic probability)

2. Course Learning Objectives

• Guide students to develop a comprehensive understanding of the end-to-end networking stack, from physical media and link-layer framing to transport protocols and application-layer services, and how each layer contributes to reliable data communication.

• Enable students to analyze, compare, and select appropriate networking technologies, protocols, and architectural models (e.g., Ethernet, IP, TCP, DNS, SDN, MPLS) for solving real-world networking problems and designing scalable network solutions.

• Cultivate the ability to evaluate performance, security, and quality-of-service considerations across the network stack, and to apply appropriate mechanisms such as congestion control, encryption, firewalls, and QoS policies.

• Foster practical proficiency in configuring, troubleshooting, and programming network components and services using industry-standard tools and APIs (e.g., socket programming, routing configuration, VLANs, VPNs, and SDN controllers).

• Encourage critical thinking about emerging and advanced networking trends--wireless mobility, cloud-native networking, and software-defined infrastructures--and their impact on future network design and management.

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	**Class Test Full marks**	**Assignment Full marks**	**Attendance Full marks**	**Total Marks**
CIA-1	25	10	5	40
CIA-2	25	10	5	40
End Semester Examination (ESE)	–	–	–	60
Total				100

5. Course Modules

Module	**Topics**	**Hours**
1	**Fundamentals of Computer Networks & Physical Layer** - Introduction to computer networks and the Internet - Network types (LAN, MAN, PAN, WAN) and common topologies (Bus, Star,	8

	Ring, Mesh, Hybrid) - Guided and unguided physical media (twisted-pair, coaxial, fiber-optic, radio, microwave, infrared) - Basic performance metrics: latency, bandwidth, delay, throughput - Switching concepts: circuit switching vs. packet switching - OSI layered architecture vs. TCP/IP model - Medium Access Control fundamentals: ALOHA, CSMA/CD, CSMA/CA, TDMA, FDMA, CDMA - Ethernet fundamentals (CSMA/CD, frame format) and basic Ethernet cabling standards - Core network devices and their functions: hub, repeater, bridge, switch, router - Physical-layer security considerations (cabling security, electromagnetic interference)	
2	**Data-Link Layer, Framing & Error Control** - Data-link layer services and framing techniques - MAC addressing and frame structure - Common data-link protocols: HDLC, PPP, Ethernet, VLAN tagging - Error-detection methods: parity check, checksum, CRC - Simple error-correction code: Hamming code (conceptual overview) - Automatic Repeat reQuest (ARQ) mechanisms: Stop-and-Wait, Go-Back-N, Selective Repeat, sliding-window operation - Flow-control techniques at the data-link layer - Multiple-access protocols: channel partitioning, random-access, CSMA variants	7
3	**Network Layer & IP Addressing** - IPv4 addressing: classful, classless (CIDR), subnet mask, FLSM, VLSM, supernetting - IPv6 addressing fundamentals and representation - Network Address Translation (NAT) and DHCP basics - IP header structure and forwarding process - ARP operation and IPv6 Neighbor Discovery - ICMP functions and common messages - Routing fundamentals: static routing, default routing, unicast routing concepts - Overview of routing protocols (RIP, OSPF, BGP) - conceptual operation without deep algorithmic math - Basic network-layer security: ACLs, IPsec concepts, VPN tunnelling basics	7
4	**Transport Layer - Reliable Data Transfer** - Transport-layer services, multiplexing and demultiplexing - UDP: header fields, checksum, typical use-cases - TCP: three-way handshake, sequence/ack numbers, sliding-window flow control - Reliable data-transfer protocols: Stop-and-Wait, Go-Back-N, Selective Repeat (conceptual mapping to TCP) - TCP congestion-control mechanisms: slow start, congestion avoidance, fast	6

	retransmit/recovery - Port numbers, well-known services, and socket API basics	
5	**Application Layer Services & Internet Applications** - Application-layer service models and protocol stack overview - World Wide Web: HTTP/HTTPS, request/response model, basic TLS concepts - File transfer: FTP and secure alternatives (SFTP, FTPS) - Email protocols: SMTP, POP3, IMAP and security extensions (STARTTLS, DKIM, SPF) - Domain Name System (DNS) operation, caching and DNSSEC basics - Remote access protocols: Telnet vs. SSH - Peer-to-Peer (P2P) file distribution concepts - Socket programming fundamentals for client-server applications - Basic authentication, encryption, and introduction to web-application security (e.g., OWASP Top 10)	6
6	**Advanced & Emerging Network Topics** - Wireless LANs and IEEE 802.11 MAC mechanisms (CSMA/CA, RTS/CTS) - Mobility management and handoff principles for wireless networks - Core network-security concepts: confidentiality, integrity, authentication - Network-layer security: IPsec, VPNs, digital signatures, firewall basics - Software-Defined Networking (SDN) - control vs. data plane, OpenFlow overview - Data-center networking fundamentals: VLANs, overlay networks, virtual switching - Quality of Service (QoS) concepts, traffic classification and shaping - Introduction to MPLS and its role in traffic engineering - Cloud-native networking basics (virtual private clouds, service meshes) and network monitoring/IDS fundamentals	8

6. References

Textbooks:

1. Behrouz A. Forouzan, Data Communications and Networking with TCP/IP Protocol Suite, Sixth Edition TMH, 2022.

2. A. S. Tanenbaum, Computer Networks

Reference Books:

1. Larry L. Peterson, Bruce S. Davie, Computer Networks: A Systems Approach, Fifth Edition, Morgan Kaufmann Publishers Inc., 2012.

2. William Stallings, Data and Computer Communications, Tenth Edition, Pearson Education, 2013.

3. Nader F. Mir, Computer and Communication Networks, Second Edition, Prentice Hall, 2014.

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
CY-403.1	Identify and describe the functions of each OSI and TCP/IP layer, common network topologies, and physical-media types, and recall key performance metrics such as latency, bandwidth, delay and throughput.	Identify	Remember
CY-403.2	Explain data-link layer services, including framing techniques, MAC addressing, and error-control methods (parity, checksum, CRC, Hamming), and illustrate the operation of ARQ protocols (Stop-and-Wait, Go-Back-N, Selective Repeat).	Explain	Understand
CY-403.3	Configure IPv4 and IPv6 addressing schemes, perform subnetting using VLSM/FLSM, set up static routes, NAT and DHCP, and apply basic network-layer security controls such as ACLs.	Configure	Apply
CY-403.4	Analyze the operation of TCP's three-way handshake, sliding-window flow control, and congestion-control algorithms (slow start, congestion avoidance, fast retransmit/recovery), and compare their reliability and performance with UDP.	Analyze	Analyze
CY-403.5	Evaluate common security threats in network protocols (e.g., ARP spoofing, DNS cache poisoning, TCP SYN flood) and implement appropriate mitigation techniques, including IPsec tunnels, TLS/HTTPS, and firewall rule sets.	Evaluate	Evaluate
CY-403.6	Design and prototype a secure, scalable network architecture that integrates Software-Defined Networking, QoS policies, and cloud-native components (virtual private cloud, service mesh), and assess its resilience against identified cyber-security risks.	Design	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	2	1	1	-	-	1	-	2
CO2	3	2	2	2	2	1	1	-	-	2	-	2
CO3	3	3	3	2	3	1	1	1	2	2	2	2
CO4	2	3	2	3	2	1	1	-	-	2	2	2
CO5	3	2	3	3	3	3	2	3	2	3	2	2
CO6	3	3	3	3	3	3	2	3	3	3	3	3

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	1
CO2	3	2	1
CO3	3	3	1
CO4	3	2	1
CO5	3	3	2
CO6	3	3	2

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Hardware Security
Course Code	CY-404
Semester	4
Course Category	Program Core Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

• Discrete Mathematics

• Digital Logic Design

• Introduction to Computer Architecture

2. Course Learning Objectives

• To provide students with a comprehensive understanding of the mathematical foundations of cryptography and the design and implementation of cryptographic primitives in hardware.

• To equip students with the knowledge and skills necessary to analyze and mitigate various hardware security threats, including side-channel attacks, hardware Trojans, and intellectual property theft.

• To enable students to design and implement secure hardware systems, incorporating techniques for protecting against physical attacks and ensuring the integrity and confidentiality of sensitive data.

• To foster critical thinking and problem-solving skills in the context of hardware security by exploring real-world case studies and applying machine learning techniques to enhance security.

• To introduce students to the emerging field of AI/ML in hardware security, enabling them to leverage these technologies for both attack and defense purposes.

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	**Class Test Full Marks**	**Assignment Full Marks**	**Attendance Full Marks**	**Total Marks**
CIA-1	25	10	05	40
CIA-2	25	10	05	40
End Semester Examination (ESE)	-	-	-	60
Total				100 Marks

5. Course Modules

Module	**Topics**	**Hours**
1	**Mathematical Foundations and Cryptographic Primitives** - Number Theory basics relevant to cryptography (Modular arithmetic, prime numbers) - Symmetric-key cryptography (AES, DES - high-level overview) - Public-key cryptography (RSA, Diffie-Hellman - high-level overview) - Hash functions (SHA-256, SHA-3 - high-level overview) - Digital Signatures (basic concepts and applications)	10
2	**Digital Design and Hardware Implementation of Cryptographic Primitives**	6

	- Introduction to FPGAs and VHDL/Verilog (basic concepts) - Implementing basic cryptographic operations (e.g., modular arithmetic) on FPGAs - Hardware implementation of AES/DES (high-level design considerations) - Design for security considerations (power analysis resistance basics)	
3	**Physically Unclonable Functions (PUFs) and True Random Number Generators (TRNGs)** - Physically Unclonable Functions (PUFs): Basic concepts, types (Arbiter PUF, Ring Oscillator PUF), challenges and applications - PUF modeling and machine learning attacks (high-level overview) - True Random Number Generators (TRNGs): Sources of entropy, design considerations, testing for randomness - Implementing TRNGs in hardware (basic concepts)	7
4	**Side-Channel Attacks and Countermeasures** - Power analysis attacks (Simple Power Analysis (SPA), Differential Power Analysis (DPA)) - Electromagnetic attacks (EMA) - Fault injection attacks (high-level overview) - Countermeasures against side-channel attacks (masking, shielding, power balancing - high-level overview)	6
5	**Hardware Security Threats and Mitigation Techniques** - Hardware Trojans: Detection and prevention techniques (high-level overview) - Hardware Intellectual Property (IP) protection: basic concepts and techniques - Secure design methodologies for hardware (high-level overview) - Fault tolerance in cryptographic hardware (basic concepts) - Secure boot and firmware update mechanisms (high-level overview)	7
6	**AI/ML in Hardware Security and Case Studies** - Machine learning for side-channel attack detection and prevention - Machine learning for hardware Trojan detection - AI-based vulnerability analysis of hardware	6

	systems - Case studies: Analysis of recent hardware security breaches and mitigation strategies - Introduction to secure embedded systems design for AI/ML applications	

6. References

Textbooks:

1. D. Mukhopadhyay and R. S. Chakraborty, "Hardware Security: Design, Threats and Safeguards", CRC Press, 2015.

2. Lawrence C. Washington, "Elliptic Curves- Number Theory and Cryptography", ? Chapman and Hall/CRC., Second edition, 2008

3. S. Bhunia and M. Tehranipoor, Hardware Security: A Hand-on Training Approach, Morgan Kauffman, 2018

Reference Books:

1. Ahmad-Reza Sadeghi and David Naccache, "Towards Hardware-intrinsic Security: Theory and Practice", Springer, 2010.

2. Mark Joye and Michael Tunstall, "Fault Analysis in Cryptography", Springer, Second edition, 2012

3. Swarup Bhunia, Sandip Ray, Susmita Sur-Kolay, "Fundamentals of IP and SoC Security: Design Verification, and Debug", Springer, 2017

4. Douglas R. Stinson and Maura B. Paterson, "Cryptography: Theory and Practice", Fourth Edition, CRC Press., 2017

5. Colin O'Flynn and Jasper van Woudenberg, "The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks", No Starch Press, 2022

6. Prabhat Mishra, Subodha Charles, "Network-on-Chip Security and Privacy", Springer, 2021

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
PCC-CS 404.1	Students will be able to explain the fundamental principles of number theory, symmetric-key	Explain	Understand

	cryptography (AES, DES), and public-key cryptography (RSA, Diffie-Hellman), including their mathematical underpinnings and practical applications.		
PCC-CS 404.2	Students will be able to apply their knowledge of VHDL/Verilog to implement basic cryptographic operations, such as modular arithmetic, on FPGAs, demonstrating an understanding of hardware design considerations for security.	Apply	Apply
PCC-CS 404.3	Students will be able to analyze the characteristics and vulnerabilities of Physically Unclonable Functions (PUFs) and True Random Number Generators (TRNGs), including common attacks and mitigation strategies.	Analyze	Analyze
PCC-CS 404.4	Students will be able to evaluate and compare different side-channel attack techniques (SPA, DPA, EMA, fault injection) and their corresponding countermeasures (masking, shielding, power balancing), justifying their choices based on specific scenarios.	Evaluate	Evaluate
PCC-CS 404.5	Students will be able to design and propose mitigation strategies for hardware security threats, such as hardware Trojans and IP theft, incorporating secure design methodologies and fault tolerance techniques, considering secure boot and firmware update mechanisms.	Design	Create
PCC-CS 404.6	Students will be able to critically analyze case studies of hardware security breaches and apply machine learning techniques to detect and prevent side-channel attacks and hardware Trojans, demonstrating an understanding of AI/ML's role in securing hardware systems and embedded AI/ML applications.	Analyze	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	1	1	1	1	1	1	1	2	1	1
CO2	3	2	3	2	3	1	1	1	2	2	2	1
CO3	2	3	1	3	1	1	1	1	1	2	1	1
CO4	2	3	2	3	1	1	1	1	1	2	1	1
CO5	3	2	3	2	2	3	2	3	2	2	2	1
CO6	2	3	2	3	2	2	1	1	2	2	2	1

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	1	1
CO2	1	2	1
CO3	1	1	1
CO4	1	1	1
CO5	1	1	1
CO6	3	2	3

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Mathematics for Cyber Securiy
Course Code	CY-405
Semester	3
Course Category	Program Core Courses
Credits	3
Hours per Week	3L:0T:0P

1. Prerequisites

• Linear Algebra (at least introductory level)

• Calculus (single-variable calculus)

• Introductory Probability and Statistics

2. Course Learning Objectives

• To equip students with a foundational understanding of the mathematical principles underlying modern cybersecurity techniques, emphasizing linear algebra, calculus, probability, and statistics.

• To develop students' ability to apply mathematical concepts to solve real-world cybersecurity problems, including anomaly detection, intrusion detection, and threat modeling.

• To enable students to utilize Python programming to implement and evaluate machine learning models for cybersecurity applications, focusing on dimensionality reduction and model evaluation.

• To foster critical thinking and problem-solving skills in the context of cybersecurity by analyzing and interpreting data using mathematical and statistical methods.

• To provide students with a comprehensive overview of the mathematical foundations of machine learning in cybersecurity, enabling them to understand and critically evaluate existing and emerging techniques.

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

Activities	**Class Test Full Marks**	**Assignment Full Marks**	**Attendance Full Marks**	**Total Marks**
CIA-1	25	10	05	40
CIA-2	25	10	05	40
End Semester Examination (ESE)	-	-	-	60
Total				100 Marks

5. Course Modules

Module	**Topics**	**Hours**
1	**Linear Algebra Fundamentals for Cybersecurity** - Vectors and Matrices: Basic operations, representation in cybersecurity contexts (e.g., representing network connections). - Systems of Linear Equations: Solving techniques and applications in cryptography (e.g., solving linear congruences). - Vector Spaces and Subspaces: Understanding linear dependencies and their relevance to vulnerability analysis. - Linear Transformations: Matrices as transformations, applications in image processing	10

	for steganography detection. - Norms and Distances: Measuring similarity and differences in data for anomaly detection.	
2	**Eigenvalues, Eigenvectors, and Applications in Cybersecurity** - Eigenvalues and Eigenvectors: Computation and interpretation. - Applications in network analysis (e.g., identifying key nodes in a network graph). - Principal Component Analysis (PCA): Dimensionality reduction for intrusion detection systems. - Singular Value Decomposition (SVD): Low-rank approximation for data compression and anomaly detection in network traffic.	8
3	**Calculus and Optimization for Machine Learning in Cybersecurity** - Derivatives and Gradients: Understanding rates of change in security metrics. - Gradient Descent: Optimizing security models (e.g., intrusion detection models). - Convex Optimization: Finding optimal solutions in security problems (e.g., resource allocation for threat mitigation). - Introduction to Multivariable Calculus (Partial Derivatives, Chain Rule): Essential for understanding gradient-based optimization algorithms.	7
4	**Probability, Statistics, and Bayesian Methods for Cybersecurity** - Probability Basics: Understanding risk assessment and threat modeling. - Bayes' Theorem: Applying Bayesian inference to threat prediction and vulnerability analysis. - Common Probability Distributions: Modeling security events (e.g., Poisson distribution for intrusion attempts). - Hypothesis Testing: Evaluating the effectiveness of security measures. - Bayesian Networks: Representing dependencies between security events.	6
5	**Dimensionality Reduction and Python Implementation for Cybersecurity** - Principal Component Analysis (PCA) in Python: Implementing PCA for anomaly detection in network traffic.	5

	- Feature Selection Techniques: Choosing relevant features for intrusion detection systems. - Case Study: Applying dimensionality reduction techniques to a real-world cybersecurity dataset (e.g., network intrusion dataset).	
6	**Introduction to Machine Learning Models for Cybersecurity** - Support Vector Machines (SVM): A brief introduction to SVMs and their application in anomaly detection and classification. - Model Evaluation Metrics: Precision, recall, F1-score, AUC-ROC for evaluating cybersecurity models. - Python Implementation of a Simple Cybersecurity Model: Building a basic model using a chosen algorithm (e.g., logistic regression for phishing detection).	6

6. References

Textbooks:

1. Cheng Soon Ong, Faisal, Marc Peter Deisenroth, Mathematics for Machine Learning, Cambridge University Press, 2020.

Reference Books:

1. W. Cheney, Analysis for Applied Mathematics. New York: Springer Science

2. S. Axler, Linear Algebra Done Right (Third Edition). Springer International Publishing, 2015

3. J. Nocedal and S. J. Wright, Numerical Optimization. New York: Springer Science.

4. J. S. Rosenthal, A First Look at Rigorous Probability Theory (Second Edition). Singapore: World Scientific Publishing, 2006.

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
ESC-M 302.1	Students will be able to explain fundamental linear algebra concepts, including vectors, matrices, systems of linear equations, and vector spaces, and	Explain, Apply	Apply

	apply these concepts to represent and solve problems in cybersecurity contexts such as network analysis and cryptography.		
ESC-M 302.2	Students will be able to compute and interpret eigenvalues and eigenvectors, and apply these concepts to analyze network graphs and perform dimensionality reduction using Principal Component Analysis (PCA) and Singular Value Decomposition (SVD).	Compute, Interpret, Apply	Apply
ESC-M 302.3	Students will be able to apply calculus concepts, including derivatives, gradients, and gradient descent, to optimize machine learning models for cybersecurity applications, such as intrusion detection.	Apply	Apply
ESC-M 302.4	Students will be able to analyze and interpret probability distributions, apply Bayes' Theorem to cybersecurity problems, and perform hypothesis testing to evaluate the effectiveness of security measures.	Analyze, Apply	Analyze
ESC-M 302.5	Students will be able to implement and evaluate dimensionality reduction techniques, such as PCA and feature selection, using Python, and apply these techniques to a real-world cybersecurity dataset for anomaly detection.	Implement, Evaluate, Apply	Apply
ESC-M 302.6	Students will be able to design, implement, and evaluate a simple machine learning model (e.g., using Support Vector Machines or logistic regression) for a cybersecurity task (e.g., intrusion detection or phishing detection), and critically analyze the model's performance using appropriate evaluation metrics.	Design, Implement, Evaluate, Analyze	Evaluate

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	-	-	1	1	-	-	-	1	-	-
CO2	3	2	-	1	1	1	-	-	-	1	-	-
CO3	3	2	1	1	1	1	-	-	-	1	-	-
CO4	3	3	1	2	1	1	-	-	-	1	-	-
CO5	3	2	1	2	3	1	-	-	-	1	1	1
CO6	3	2	3	2	3	1	1	1	1	2	2	1

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	1
CO2	2	3	1
CO3	2	3	1
CO4	3	2	2
CO5	2	3	1
CO6	2	3	2

Dr. B. C. Roy Engineering College, Durgapur

Department of CSE(CS)

Field	Details
Course Name	Data Handling and Data Visualization
Course Code	CY-497
Semester	4
Course Category	Program Core Courses
Credits	2
Hours per Week	0L:0T:4P

1. Prerequisites

• Proficiency in Python Programming (including familiarity with data manipulation libraries like Pandas)

• Foundational Statistics and Data Analysis Concepts (e.g., data types, distributions, aggregation, basic descriptive statistics)

• Introduction to Machine Learning Concepts (understanding the basic ML workflow, common model types, and evaluation metrics)

2. Course Learning Objectives

• To establish a comprehensive understanding of the theoretical foundations, principles, and critical role of data visualization within the Artificial Intelligence and Machine Learning lifecycle.

• To develop students' ability to select, design, and justify appropriate visualization techniques for diverse data types (including high-dimensional, temporal, spatial, and relational data) based on analytical goals and human perceptual principles.

• To equip students with practical proficiency in utilizing key programming libraries and tools (primarily within the Python ecosystem, with exposure to web technologies) for implementing both static and interactive visualizations.

• To integrate visualization as an essential methodology for exploratory data analysis (EDA), model building, performance evaluation, and explainable AI (XAI), enabling deeper insights and effective communication of complex findings.

• To foster critical evaluation skills regarding the effectiveness, ethical implications, and potential biases present in data visualizations used for analysis and communication.

3. Teaching Methodology

• Lectures and Presentations

• Interactive Discussions and Case Studies

• Lab Sessions

• Guest Lectures

4. Evaluation System

5. Course Modules

Module	Topics	Hours
1	**Foundations of Data Visualization for cyber security** - Defining Data Visualization: Value, History, and Scope in cyber security - Visualization Frameworks & Task Abstraction (e.g., Munzner's Analysis & Design) - Human Perception and Cognition in Visualization - Data Types and Relations relevant to ML: Categorical, Ordered, Quantitative, Relational, High-dimensional, Text, Image Features - Theory of Scales and Measurement - The Visualization Zoo: Overview of common chart types and their primary uses - Essential Mathematical & Statistical Concepts for Visualization (Aggregation, Ratios, Distributions) - Visualization Workflow & Process in an cyber security Pipeline (Data Exploration, Model Interpretation, Communication)	7
2	**Design Principles and Core Charting Techniques**	7

	- Principles of Effective Visualization: Graphical Excellence & Integrity - Tufte's Principles: Data-Ink Ratio, Data Density, Chart Junk - Avoiding Distortion: Design and Data Variation, Visual Area and Numerical Measure - Color Theory and Application: Palettes (Categorical, Sequential, Diverging), Accessibility considerations - Narrative Visualization / Storytelling with Data Findings (Annotations, Structure) - Visualizing Amounts: Bar Charts (Standard, Clustered, Stacked), Dot Plots - Visualizing Distributions: Histograms, Density Plots, Box-and-whisker Plots, Violin Plots, Q-Q Plots (for assumption checking) - Visualizing Proportions: Stacked Bar Charts (Percent), Treemaps (intro), Waffle Charts (avoiding Pie Charts)	
3	**Visualizing Complex and Domain-Specific Data** - Visualizing Relationships: Scatter Plots (Bivariate), Bubble Charts, Introduction to Correlation Matrices - Temporal Data Visualization: Line Charts (Individual, Multiple Series), Area Charts, Connected Scatter Plots - Spatial Data Visualization: Choropleth Maps, Symbol Maps, Spatial Heatmaps / Raster Plots, Scatterplot Maps (Geographic Vector/Raster basics) - Hierarchical Data Visualization: Node-Link Diagrams (Trees), Treemaps (revisited for hierarchy), Sunburst Charts - Network/Graph Visualization: Node-Link Graphs, Adjacency Matrices, Basic Network Metrics (Degree, Centrality), Force-directed layouts	7
4	**Implementation Tools for Visualization** - Development Workflow: IDEs (e.g., VS Code), Version Control (Git/Github), Command Line Usage - Python Visualization Ecosystem (Primary Focus): - Matplotlib (Foundational plotting) - Seaborn (Statistical visualization, integration with Pandas) - Plotly (Python) (Interactive charts, dashboards) - Web-based Visualization Fundamentals: HTML, JavaScript (ES6+), DOM Manipulation, JSON Data Format - Web-based Libraries Overview: - Declarative Grammars: Vega-Lite (Concepts and	7

	Usage) - Imperative Libraries: D3.js (Core concepts: selections, data binding, scales, axes - brief overview) - Plotly.js (for web deployment) - Introduction to Dashboarding Tools (e.g., Streamlit, Dash, Tableau concepts)	
5	**Exploratory Data Analysis (EDA) and Interaction** - Data Handling for Visualization: Data Cleaning, Transformation, Reshaping (Pivoting, Melting) using Pandas/similar - Exploratory Data Analysis (EDA) in the cyber security Context: Objectives, Importance, Process - EDA Visualization Techniques: Histograms, Box Plots, Scatter Plots, Pair Plots, Correlation Matrices (Heatmaps), Faceting - EDA Analysis Techniques: Univariate, Bivariate, Multivariate Exploration for Feature Understanding and Selection - Interactive Visualization Principles: Overview + Detail, Filtering, Brushing & Linking - Interactive Dynamics for Visual Analysis: Implementing interaction with Plotly/Seaborn/Vega-Lite - Multi-view Displays & Dashboard Design Principles - Visual Analytics: Connecting Interactive Visualization with Analytical Reasoning	7
6	**Visualization for Model Building, Evaluation, and Explainability (XAI)** - Visualizing High-Dimensional Data: Parallel Coordinates, Dimensionality Reduction Visualization (PCA, t-SNE, UMAP outputs) - Visualization in the ML Workflow: Visualizing Feature Spaces, Cluster Analysis Results, Decision Boundaries (conceptual) - Visualizing Model Performance: Confusion Matrices, ROC Curves, Precision-Recall Curves - Introduction to Explainable AI (XAI): Need for Transparency, Ethical Considerations - Visualization for Interpretable Models: Visualizing Linear Model Coefficients, Decision Trees - Visualization for Model-Agnostic XAI: - Feature Importance (Permutation Importance, SHAP Summary Plots) - Local Explanations (SHAP Force Plots, LIME Explanations)	7

	- Global Explanations (Partial Dependence Plots - PDPs, Individual Conditional Expectation - ICE Plots) - Evaluating Visualizations: Quality Assessment, Identifying Misleading Visualizations, Bias in Visualization	

6. References

Textbooks:

1. Claus O. Wilke, Fundamentals of Data Visualization, O'Reilly, 2019

2. Andy Kirk, Data Visualization A Handbook for Data Driven Design, Sage Publications, 2016

Reference Books:

1. Philipp K. Janert, Gnuplot in Action, Understanding Data with Graphs, Manning Publications, 2010.

2. Alex Campbell, Data Visualization: Ultimate Guide to Data Mining and Visualization, 2020

7. Course Outcomes

ID	Statement	Action Verb	Knowledge Level
PCC- CS 496.1	Explain the fundamental principles of data visualization, including human perception, data types relevant to cyber security, visualization frameworks, and the role of visualization within an AI/ML pipeline.	Explain	Understand
PCC- CS 496.2	Apply principles of effective visual design, color theory, and graphical integrity to create standard chart types (e.g., bar charts, histograms, scatter plots) for representing amounts, distributions, proportions, and basic relationships.	Apply	Apply
PCC- CS 496.3	Utilize Python visualization libraries (e.g., Matplotlib, Seaborn, Plotly) to implement static and interactive visualizations for diverse and	Utilize	Apply

	complex data structures, including temporal, spatial, hierarchical, and network data.		
PCC- CS 496.4	Analyze datasets using interactive Exploratory Data Analysis (EDA) techniques, employing appropriate visualizations to identify patterns, relationships, anomalies, and features relevant to cyber security model development.	Analyze	Analyze
PCC- CS 496.5	Evaluate machine learning model performance and interpret model behavior using established visualization techniques for model diagnostics and Explainable AI (XAI), such as confusion matrices, ROC curves, feature importance plots, and local/global explanation plots (e.g., SHAP, PDP).	Evaluate	Evaluate
PCC- CS 496.6	Design and critique data visualizations and interactive dashboards for effectively communicating insights derived from cyber security models and analyses, considering narrative structure, audience, ethical implications, and potential biases.	Design	Create

8. CO-PO Mapping

CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	3	2	2	2	1	1	-	1	-	2	-	2
CO2	3	2	3	2	1	1	-	2	-	3	-	1
CO3	3	2	3	2	3	-	-	-	1	2	1	2
CO4	3	3	2	3	2	1	-	1	1	2	1	2
CO5	3	3	2	3	3	2	-	2	1	2	1	2
CO6	3	2	3	2	2	3	1	3	2	3	2	2

9. CO-PSO Mapping

CO	PSO1	PSO2	PSO3
CO1	3	2	1
CO2	2	2	1
CO3	2	3	1

CO4	3	2	1
CO5	3	2	2
CO6	2	2	3