ఆంధ్రప్రదేశ్ కేంద్రీయ విశ్వవిద్యాలయం

आंध्रप्रदेश केंद्रीय विश्वविद्यालय

Central University of Andhra Pradesh

Jnana Seema, Ananthapuramu

School of Interdisciplinary and Applied Sciences

Department of Computer Science and AI

Vidya Dadati Vinayam

(Education Gives Humility)

PG Diploma in Cyber Security

w.e.f. Academic Year 2025 - 2026

CONTENTS

PG Diploma in Cyber Security

Introduction to the Programme

The Postgraduate Diploma in Cyber Security (PGDCS) is one of the new postgraduate programmes being offered by CUAP from the 2025-26 academic year. Cybersecurity is one of the emerging areas of computing. This program prepares students to assess the security needs of computer and network systems, recommend safeguard solutions, and manage the implementation and maintenance of security devices, systems, and procedures. The program includes programming, networking, cryptography, security system design, risk assessment and policy analysis, user access issues, investigation techniques, and troubleshooting.

Cybersecurity is among the niche areas of specialization in the contemporary world. There is a compelling need for professionals empowered to develop defense mechanisms for cybersecurity and contribute to the development and growth of the cybersecurity sector. The Postgraduate Diploma in Cyber Security program has been envisaged to nurture young talent in the niche domain of cybersecurity.

Objectives:

- To provide foundational and advanced knowledge in cybersecurity, ethical hacking, network security, digital forensics, and information security management systems.
- To develop skilled professionals capable of identifying, analyzing, and mitigating cyber threats using industry-relevant tools and best practices.
- To empower learners with hands-on experience through labs, simulations, and projects that simulate real-world cyber attack and defense scenarios.

Learning Outcomes:

On successful completion of the programme, students should be able to:

- Apply foundational and advanced concepts of cybersecurity, ethical hacking, and cryptography to protect systems and networks.
- Understand and apply relevant cyber laws, data protection regulations, and ethical principles in the field of information security.
- Design and implement secure system architectures, protocols, and firewalls tailored to organizational needs.

Programme Structure:

- Post Graduate Diploma is a one-year program divided into two semesters with a total of around 40 credits.
- The program is designed with a combination of Core Courses and MOOCS.
- Students need to complete 2 MOOC courses in I,II semester.
- In semester II students will undergo for Dissertation Work.

Programme Structure

S. No	Course Code	Title of the Course	Total Credits	Credits Distributions		
				L*	T*	P*
Semester– I						
1.	PDCBS101	Introduction to Cyber Security	4	3	0	1
2.	PDCBS102	Network Security	4	3	0	1
3.	PDCBS103	Python Programming	4	3	0	1
4.	PDCBS111	MOOCs/NPTEL/SWAYAM*	3	3	-	-
5.	PDCBS112	MOOCs/NPTEL/SWAYAM*	3	3	-	-
6.	PDCBS125	Internship/Lab	2	-	-	2
Total			**20**	**15**	**0**	**5**
S.No	**Course Code**	**Title of the Course**	**Total Credits**	**Credits Distribution**		
				L*	**T***	**P***
Semester– II						
1.	PDCBS201	Cyber Security, Tools, Techniques and Counter Measures	4	3	0	1
2.	PDCBS202	Artificial Intelligence in Cyber Security	4	3	0	1
3.	PDCBS211	MOOC/NPTEL/SWAYAM*	3	3	-	-
4.	PDCBS212	MOOC/NPTEL/SWAYAM*	3	3	-	-
5.	PDCBS228	#Project Work /Dissertation	6	-	-	6
Total			**20**	**12**	**0**	**8**

***L:** Lectures, ***T**: Tutorials, ***P**: Practical

***: Appropriate online Content available recommended by the department at the time of enrollment**

#: Project Work is compulsory and have to submit to the department one week before the second semester examination. Department faculty will allot a supervisor to each student at the end of the first semester.

Note: 1. MOOCs are chosen by the student based on the availability of the courses offered on SWAYAM & other related platforms as suggested/recommended by the Department.

2. The desired changes may be made by the Department in the programme structure as and when necessary with the prior approval of the BOS.

Credit Distribution

Semester	Total Credits
Semester-I	20
Semester-II	20
Total	**40**

Important Information to Students

1. **Eligibility:**
   i. Students pursuing/completed PG/Ph.D. programmes in any other educational institution . with B.Sc in Computer Science/Mathematics/Physics BCA/B.Com (Computer Applications) or any B.Tech/MTech or MCA/M.Sc in Computer Science/Mathematics/Physics or any degree with Computer Science as Subject
   ii. CUAP/Non CUAP students pursuing any PG/PhD Programmes can enroll for PG Diploma Programmes offered by the University
   iii. Non CUAP students shall have to appear for an Entrance Examination conducted by the University
   iv. A student can enroll for as many PG Diploma Programmes as he/she wishes to
2. The minimum duration for completion of any Postgraduate Diploma Programme is two semesters (one academic year).
3. Maximum duration of completion of programme is two years.
4. A student should have minimum 75% attendance in classes, seminars, practical/ lab in each course of study without which he/she will not be allowed for the Semester -end examination.
5. All theory courses in the programme shall have Continuous Internal Assessment (CIA) component of 40 marks and a Semester-end component of 60 marks. The minimum pass marks for a course is 50%.
6. The student has to appear 3 CIA tests of 15 marks each per semester in each course from which the best 2 performances shall be considered for the purpose of calculating the marks. A record of the continuous assessment is maintained by the department. The remaining 10 marks are awarded based on participation and performance in:
   - Assignments
   - Class presentations
   - Seminars
   - Quizzes
7. A student should pass separately in both CIA and the Semester-end Examination.
8. Semester-end examination shall consist of objective type questions, descriptive type questions, short answer questions and case studies or any others.
9. A student failing to secure the minimum pass marks in the CIA is not allowed to take the semester-end examination of that course. She/He has to redo the course by attending special classes for that course and get the pass percentage in the internal tests to become eligible to take the semester-end examination.
10. Students failing a course due to lack of attendance should redo the course.

SEMESTER-I

Course Code: **PDCBS101** Core/ Elective: **Core** No. of Credits: **4** No. of Hours**: 75**	**Introduction to Cyber Security**

Course Objectives

- Introduce the core principles and concepts of cyber security, including the CIA triad (Confidentiality, Integrity, Availability).
- Examine the frameworks and standards related to security management, governance, risk, and compliance (GRC).
- Explore strategies for contingency planning, including incident response, disaster recovery, and business continuity planning.

Learning Outcomes

After completion of the course students will be able to:

- Understand governance, risk management, and compliance frameworks, and how they apply to organizational security.
- Develop and evaluate cyber security policies, including enterprise, issue-specific, and system-specific policies (ESSP, ISSP, SYSSP).
- Identify and assess cyber risks, and apply strategies for mitigation and control.
- Understand the strategic importance of privacy and data protection in business and governance contexts.

Course Outline:

UNIT-I **15 hours**

Introduction - Introduction to cyber security, Confidentiality, integrity, and availability. Foundations - Fundamental concepts, CIA, CIA triangle, data breach at target. Security management, Governance, risk, and compliance (GRC)- GRC framework, security standards.

UNIT-II **15 hours**

Contingency planning - Incidence response, Disaster Recovery, BCP. Cyber security policy - ESSP, ISSP, SYSSP. Risk Management - Cyber Risk Identification, Assessment, and Control.

UNIT-III **15 hours**

Cyber security: Industry perspective - Defense Technologies, Attack, Exploits. Cyber security technologies - Access control, Encryption, Standards. Foundations of privacy - Information privacy, Measurement, Theories.

UNIT-IV **15 hours**

Privacy regulation - Privacy, Anonymity, Regulation, Data Breach. Privacy regulation in Europe, Privacy: The Indian Way - Data Protection, GDPR, DPDP, Aadhar.

UNIT-V **15 hours**

Information privacy: Economics and strategy, Economic value of privacy, privacy valuation, WTA and WTC, Business strategy and privacy, espionage, Privacy vs safety.

References:

1. Introduction to Cyber Security available at http://uou.ac.in/foundation-course
2. Fundamentals of Information Security http://uou.ac.in/progdetail?pid=CEGCS-17
3. Cyber Security Techniques http://uou.ac.in/progdetail?pid=CEGCS-17
4. Cyber Attacks and Counter Measures: User Perspective http://uou.ac.in/progdetail?pid=CEGCS-17
5. Information System http://uou.ac.in/progdetail?pid=CEGCS-1

Course Code: **PDCBS102** Core/ Elective: **Core** No. of Credits: **4** No of Hours**: 75**	**Network Security**

Course Objectives

- Introduce the fundamentals of communication networks and network-based attacks.
- Explain key cryptographic methods and their applications in securing networks.
- Develop practical understanding of firewalls, IDS, and post-quantum cryptography.

Learning Outcomes

After completion Students will be able to:

- Understand basic network structures and identify common security threats.
- Apply symmetric and public key cryptography for secure communication.
- Describe modern security technologies, including blockchain, IoT, and cloud.
- Understand firewalls, intrusion detection, and future cryptographic trends.

Course Outline:

UNIT-I **15 hours**

Basics of Communication Networks, Basics of Communication Networks (contd.), Different Types of Attacks on Networks.

UNIT-II **15 hours**

Mathematical Background for Cryptography, Principles of Cryptography: Symmetric Key Cryptography and Public Key Cryptography

UNIT-III **15 hours**

Message Integrity, Cryptographic Hash Functions, and Digital Signatures, Authentication, Public Key Infrastructure, Certificates

UNIT-IV **15 hours**

Transport-Layer Security, Network-Layer Security and Virtual Private Networks, Security in Wireless Local Area Networks, Wireless Cellular Network Security, Firewalls and Intrusion Detection Systems.

UNIT-V **15 hours**

Cryptocurrencies and Blockchain, Cloud Security, Security of the Internet of Things (IoT), Hardware Security, Anonymous Connections and Onion Routing, Post-Quantum Cryptography

References:

1. C. Kaufman, R. Perlman, M. Speciner, R. Perlner,"Network Security: Private Communication in a Public World",Pearson Education, 3rd edition, 2024
2. J. Kurose, K. Ross, "Computer Networking: A Top Down Approach", 8th Edition, Pearson Education, 2022
3. B.L. Menezes, R. Kumar, "Cryptography, Network Security, and Cyber Laws", Cengage Learning India Pvt. Ltd.,2018
4. J. Edney, W.A. Arbaugh, "Real 802.11 Security: Wi-Fi Protected Access and 802.11i", Pearson Education, 2004
5. W. Stallings, "Cryptography and Network Security:Principles and Practice", Pearson Education, 8th edition, 2023
6. L. Peterson, B. Davie, "Computer Networks: A Systems Approach", 6th Edition, Morgan Kaufmann, 2021

Course Code: **PDCBS103** Core/ Elective: **Core** No. of Credits: **4** No of Hours: **75**	**Python Programming**

Course Objectives

- Introduce the fundamentals of programming and structured problem-solving.
- Teach Python syntax, data types, control structures, and basic programming constructs.
- Explore built-in data structures like lists, tuples, and dictionaries.
- Develop skills in functions, modules, file handling, and exception management.
- Encourage clean coding, modular design, and debugging techniques.

Learning Outcomes

Students will be able to:

- Understand program design, flowcharts, and structured programming methods.
- Write Python programs using variables, operators, conditionals, and loops.
- Work with strings, lists, tuples, and dictionaries effectively.

Course Outline:

UNIT-I **15 hours**

Planning the Computer Program: Concept of problem solving, Problem definition, Program design, Debugging, Types of errors in programming, Documentation. Techniques of Problem Solving: Flowcharting, decision table, algorithms.

UNIT-II **15 hours**

Structured programming concepts, Programming methodologies viz. top-down and bottom-up programming. Introduction to Python: Structure of a Python Program, Elements of Python, Python Interpreter, Using Python as calculator, Python shell, Indentation. Atoms, Identifiers and keywords, Literals, Strings and Operators.

UNIT-III **15 hours**

Conditional Statements and Looping: Branching, Looping, Conditional Statement, Exit function, Difference between break, continue and pass. String Manipulation: Understanding string, Accessing Strings, Basic Operations, String slices, Function and Methods. List: Introduction to list, Accessing list, list operations, Working with lists, Function and Methods.

UNIT-IV **15 hours**

Tuples: Introduction to tuple, Accessing tuples, Operations, Working, Functions and Methods. Dictionary: Introduction to dictionaries, Accessing values in dictionaries, Working with dictionaries, Properties, Functions. Python Functions: Defining a function, Calling a function, Types of functions, Function Arguments, Anonymous functions, Global and local variables, Organizing python codes using functions.

UNIT-V **15 hours**

Python Modules: Organizing Python projects into modules, Importing own module as well as external modules, Understanding Packages, modules and external packages. Input-Output: Printing on screen, reading data fromkeyboard, Opening and closing file, Reading and writing files, Functions. Exception Handling: Introduction to Exception, Exception Handling, Except clause, Try ? finally clause, User Defined Exceptions.

References:

1. B. Downey, Think Python, 2e: How to Think Like a Computer Scientist, O'Reilly, 2015.
2. Shaw, LEARN PYTHON 3 THE HARD WAY, Addison-Wesley, 2017.
3. Arockia Mary P, Problem Solving and Python Programming, Shanlax Publications, 2021.
4. C. Morris, "https://www.kaggle.com/learn/python," [Online].
5. "https://docs.python.org/3/tutorial/index.html," [Online].

SEMESTER-II

Course Code: **PDCBS201** Core/ Elective: **Core** No. of Credits: **4** No of Hours: **75**	**Cyber Security, Tools, Techniques and Counter Measures**

Course Objectives

- Introduce essential concepts of cyber threats, risks, and countermeasures.
- Familiarize students with tools used for vulnerability scanning, password cracking, and web inspection.
- Understand firewall configurations, IDS, malware protection, and desktop security.
- Explore legal, ethical, and policy issues in cyber security, including social engineering and intellectual property.

Learning Outcomes

Students will be able to:

- Identify cyber threats, risks, and attack vectors, and understand cyber kill chains.
- Use common cyber security tools for scanning, analysis, and penetration testing.
- Configure firewalls and understand the role of IDS and wireless security.

Course Outline:

UNIT-I **15 hours**

Cyber Security Essentials, Attack Vectors, Threat, Risk and Vulnerability,Advanced Persistent Threat and Cyber Kill Chain, Cyber Security Framework.

UNIT-II **15 hours**

Firewall and Packet Filters, Introduction to Windows and Linux Firewall,Attacks on Wireless Networks, Scanning For Web Vulnerabilities Tools and HTTP Utilities.

UNIT-III **15 hours**

Application Inspection Tools, Password Cracking and Brute-Force Tools, Web Attack, Information Security Basics to Policy-I.

UNIT-IV **15 hours**

Web Attack, Information Security Basics to Policy-II, Intrusion Detection System, IT Assets and Wireless Security, Cyber Security Assurance Framework, Desktop Security and Malware

UNIT-V **15 hours**

E-Commerce and Web-Application Security, Social Engineering, Internet Crime and Act, Intellectual Property in the Cyber world

References:

1. Cyber Security – Understanding Cyber Crimes, Computer Forensics and Legal Perspectives Author: Nina Godbole, Sunit Belapure, Publisher: Wiley India

2. Information Systems Security – Security Management, Metrics, Frameworks and Best Practices Author: Nina Godbole, Publisher: Wiley India

Course Code: **PDCBS202** Core/ Elective: **Core** No. of Credits: **4** No. of Hours: **75**	**Artificial Intelligence in Cyber Security**

Course Objectives

- Introduce AI and machine learning concepts with applications in cyber security.
- Explore threat detection using supervised, unsupervised, and ensemble learning techniques.
- Analyze advanced topics such as adversarial attacks on ML models and AI system vulnerabilities.

Learning Outcomes

Students will be able to:

- Apply machine learning techniques for classifying threats, attacks, and malware.
- Use decision trees and profiling for context-based malicious event detection.
- Understand adversarial attack types and assess the robustness of AI-based security models.

Course Outline:

UNIT-I **15 hours**

Overview on Machine Learning with use cases from cybersecurity, classification of threats, attacks, vulnerabilities, malware, trojans etc.

UNIT-II **10 hours**

Classification of malware using pervised/unsupervised learning based on signatures and profiling. Decision Tree and context based malicious event detection.

UNIT-III **15 hours**

Time Series Analysis and Ensemble modelling to detect deviation from normal behaviour, case studies in Reconnaissance detection.

UNIT-IV **15 hours**

Efficient Network Anomaly detection; familiarize with various stages of network attack and address using deep neural networks, develop intrusion detection systems.

UNIT-V **15 hours**

Adversarial attacks on ML systems, model poisoning, black box attacks, white box attacks, state-of-art research paper reading on deep learning systems.

References:

1. Machine Learning and Security by David Freeman, Clarence Chio Publisher: O'Reilly Media, Inc. Release Date: February 2018 ISBN: 9781491979891
2. Malware Data Science by Joshua Saxe with Hillary Sanders, ISBN-10: 1-59327-859-4 ISBN-13: 978-1-59327-859-5 Publisher: William Pollock

Course Code: **PDCBS228** Core/ Elective: **Core/Compulsory** No. of Credits: **6** No of Hours: **One Semester**	**Project Work / Dissertation**

Objective:

Implement some of the existing techniques and develop some new algorithm/ tool and produce meaningful research outputs.

Each student will work on a dissertation to apply the knowledge of Cyber Security Techniques for solving a wide variety of real-world problems. Problems may be decided based on literature survey by standard research articles. Significance of proposed problem and the state-of the art to be explored. Relevant tools may be used for demonstrating the results with physical meaning and create necessary research components

Student is required to submit a detailed project report on the selected topic for their project as per the guidelines decided by the department. The project work is to be evaluated through presentations and viva-voce during the semester and final evaluation will be done at the end of the semester as per the guidelines decided by the department from time to time.

However, candidate may visit research labs/institutions with the due permission of chairperson on recommendation of supervisor concerned.