COMPUTER SCIENCE & ENGINEERING
COs OF 4TH SEMESTER

CSPC2006 DESIGN AND ANALYSIS OF ALGORITHMS (3-0-0)

Course Outcomes (COs)

CO No	Description
CO1	Analyze algorithms and evaluate their performance using standard methods.
CO2	Apply asymptotic notations to express algorithm efficiency.
CO3	Solve problems using different algorithm design techniques.
CO4	Select appropriate data structures and design methods for given problems.
CO5	Understand P and NP classes and their implications in computational complexity.

CO–PO Mapping (DAA)

COs	Description	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	Analyze algorithms & performance	3	3	2	2	2	-	-	-	2	2	-	2
CO2	Apply asymptotic notations	3	3	2	-	2	-	-	-	2	2	-	2
CO3	Solve problems using design techniques	2	3	3	2	2	-	-	-	2	2	-	2
CO4	Select appropriate data structures & methods	2	3	3	2	2	-	-	-	2	2	-	2
CO5	Understand P and NP classes	2	2	2	2	1	-	-	-	2	2	-	3

CSPC2004 DATABASE ENGINEERING (3-0-0)

Course Outcomes (COs)

CO1: Explain fundamental database concepts and technologies.
CO2: Write and execute SQL queries to solve database problems.
CO3: Apply relational database design principles and normalization.
CO4: Manage transactions and ensure concurrency control in databases.
CO5: Design and implement database applications for practical scenarios.
CO6: Understand database storage structures and access methods.

CO–PO Mapping (Database Engineering)

COs	Description	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	Database concepts & technologies	3	2	2	-	2	-	-	-	-	2	-	1
CO2	SQL programming	2	3	3	2	3	-	-	-	-	2	-	2
CO3	Relational database design	2	3	3	2	2	-	-	-	-	2	-	2
CO4	Transactions & concurrency	2	3	2	2	3	-	-	-	2	2	-	2
CO5	Database application design	2	3	3	2	3	-	-	-	2	2	-	2
CO6	Storage structures & access methods	2	2	3	2	3	-	-	-	2	2	-	2

PCAC2014 IT Fundamentals for Cybersecurity – II (3-0-0)

Course Outcomes (COs)

CO1: Explain fundamentals of LAN, TCP/IP, OSI model, routing basics, and their role in network security.
CO2: Identify vulnerabilities in databases (SQL, Oracle, MongoDB, CouchDB) and apply mitigation techniques like preventing SQL injection.
CO3: Apply generative AI tools for cybersecurity tasks such as vulnerability detection and automated security reporting.
CO4: Perform penetration testing using security tools and analyze different phases of testing.
CO5: Understand incident response lifecycle including planning, detection, containment, recovery, and documentation.
CO6: Apply digital forensic techniques for evidence collection and cybersecurity incident analysis.

CO–PO Mapping

COs	Description	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	Networks & security fundamentals	3	2	2	1	2	2	-	-	2	2	-	2
CO2	Database vulnerabilities & mitigation	2	3	3	2	2	2	-	2	-	2	-	2
CO3	Generative AI in cybersecurity	2	3	3	2	3	2	-	1	2	2	-	3
CO4	Penetration testing techniques	2	3	3	3	3	2	-	2	2	2	1	2
CO5	Incident response management	2	3	2	3	2	2	-	2	3	2	2	2
CO6	Digital forensics & evidence handling	2	3	3	3	2	2	-	2	2	2	1	2

CSPE3018 INTERNET OF THINGS (3-0-0)

Course Outcomes (COs)

CO1: Understand the basic architecture of IoT-based devices.
CO2: Illustrate wireless communication systems in IoT.
CO3: Identify actuators and sensor technologies for sensing real-world entities.
CO4: Apply IoT design methodology and use cloud platforms effectively.
CO5: Deploy an IoT application and connect it to the cloud.
CO6: Compare IoT applications in industrial and real-world scenarios.

CO–PO Mapping (Internet of Things)

COs	Description	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	IoT device architecture	3	2	2	-	2	-	-	-	-	2	-	1
CO2	Wireless communication systems	2	2	2	-	3	-	-	-	-	2	-	1
CO3	Actuators & sensor technologies	2	3	3	2	3	-	-	-	-	2	-	2
CO4	IoT design methodology & cloud	2	3	3	2	3	-	-	-	2	2	-	2
CO5	Deploy IoT application	2	2	3	-	3	-	-	-	2	2	-	2
CO6	Compare IoT applications	1	2	2	-	2	2	-	-	2	3	-	2

CSPE3012 INFORMATION SECURITY AND MANAGEMENT (3-0-0)

Course Outcomes (COs)

CO1: Explain the basic principles, goals, and components of information security.
CO2: Apply cryptographic algorithms and secure communication protocols.
CO3: Implement secure programming and operating system protection mechanisms.
CO4: Analyze database and network security measures to protect data integrity and confidentiality.
CO5: Evaluate administrative, legal, and ethical aspects of information security.

CO–PO Mapping Table (INFORMATION SECURITY AND MANAGEMENT)

COs	Description	PO1	PO2	PO3	PO4	PO5	PO6	PO8	PO9	PO10	PO12
CO1	Principles & goals of InfoSec	3	2	2	-	-	2	1	-	2	1
CO2	Cryptography & secure protocols	2	3	2	2	3	-	-	-	-	2
CO3	Secure programming & OS protection	2	2	3	-	3	-	-	-	-	2
CO4	Database & network security	2	3	2	2	3	-	-	-	-	2
CO5	Administrative & legal aspects	1	2	2	-	-	3	3	2	2	3

CSPC3005 SOFTWARE ENGINEERING (3-0-0)

Course Outcomes(Cos)

On completion of this course, student should be able to:

CO1: Apply and assess the principles of various process models for the software development.

CO2: Demonstrate various software project management activities that include planning, estimations, Risk assessment and Configuration Management

CO3: Perform Requirements modelling and apply appropriate design and testing heuristics to produce quality software systems.

CO4: Demonstrate the complete Software life cycle activities from requirements analysis to maintenance using the modern tools and techniques.

CO5: Escalate the use of various standards and metrics in evaluating the process and product.

CO–PO Mapping (Software Engineering)

COs	Description	PO1	PO2	PO3	PO4	PO5	PO9	PO10	PO11	PO12
CO1	Process models for software development	3	2	2	-	-	-	-	-	1
CO2	Project management, estimation, risk, CM	2	2	2	-	2	2	1	3	-
CO3	Requirements modeling, design & testing	2	3	3	2	2	-	-	-	-
CO4	Software life cycle using modern tools	2	2	3	-	3	2	2	1	-
CO5	Standards and metrics evaluation	2	2	2	2	1	-	-	-	2