DEPARTMENT OF INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING & TECHNOLOGY
UG PROGRAM (CBCS) – B.TECH. CYBERSECURITY
(2025–2026 Batch and onwards)

Semester I

Semester	Course Code	Title of the Course	Course Category	NCrF level	Objectives and outcomes		SDG Goal	Instruction Hours / week			Credit(s)	Marks		
					PEOs	POs		L	T	P		CIA	ESE	Total
I	25 MAU108	Engineering Mathematics- I	BSC	5.5			4,8	3	1	0	4	40	60	100
I	25PHU121	Engineering Physics	BSC	4.5			4,8	3	0	2	4	40	60	100
I	25EVS001	Environmental Science	BSC	4.5			4,8,9,11	2	0	0	2	40	60	100
I	25ENU121	Technical English	HSC	4.5			4,8	3	0	2	4	40	60	100
I	25EEU101	Basics of Engineering	BEC	4.5			4,8,9,11	3	0	0	3	40	60	100
I	25CSU121	Programming for Problem Solving	BEC	4.5	1,2	1-5	4,5 8,9	2	0	4	4	40	60	100
I	25MEU101	Engineering Graphics	BEC	4.5			4,8,9	2	1	0	3	40	60	100
I	25MAC111	NCC/YRC/NSS/Rotary Club	MAC	4.5			8,9,11	0	0	2	0			
	Semester Total										24	280	420	700

Semester II

Semester	Course Code	Title of the Course	Course Category	NCrF level	Objectives and outcomes		SDG Goal	Instruction Hours / week			Credit(s)	Marks		
					PEOs	Pos		L	T	P		CIA	ESE	Total
II	25MAU208	Engineering Mathematics II	BSC	4.5			4,8	3	1	0	4	40	60	100
II	25CHU221	Engineering Chemistry	BSC	4.5			4,8	3	0	2	4	40	60	100
II	25ECU223	Digital System Design	BEC	4.5			4,8,9	2	0	2	3	40	60	100
II	25ITU221	Object Oriented Application Development	PCC	4.5	1-5	1-3	4,5 8, 9	3	0	2	4	40	60	100
II	25ITU222	Data Structures and Algorithms	PCC	4.5	1-5	1-3	4,8, 9	3	0	2	4	40	60	100
II	25IKS001	Introduction to Indian Knowledge System	IKS	4.5			4,8,9, 11	2	0	0	2	40	60	100
II	25MEU211	Design Thinking and Innovations Lab	BEC	4.5			4,8,9	0	0	4	2	40	60	100
II	25MAC201	Indian Constitution and Human Rights	MAC	4.5			4,8,9, 11	2	0	0	2	40	60	100
	Semester Total										25	320	480	800

SEMESTER III

Semester	Course Code	Title of the Course	Course Category	NCrF level	Objectives and outcomes		SDG Goal	Instruction Hours / week			Credit(s)	Marks		
					PEOs	Pos		L	T	P		CIA	ESE	Total
III	25MAU301	Discrete Mathematics	BSC	4.5				3	1	0	4	40	60	100
III	25UHV001	Universal Human Values and Ethics	HSC	4.5				2	0	0	2	40	60	100
III	25CYU321	Fundamentals of Operating Systems	PCC	5	1-5	1-3	4,8,9	3	0	2	4	40	60	100
III	25CYU301	Cybersecurity Essentials	PCC	5	1-5	1-3	4,8,9	3	0	0	3	40	60	100
III	25CYU322	Computer Networking Essentials	PCC	5	1-5	1-3	4,8, 9	3	0	2	4	40	60	100
III	25CYU323	Design and Analysis of Algorithms	PCC	5	1-5	1-3	4,8,9	3	0	2	4	40	60	100
III	25CYU302	Web Application Security	PCC	5	1-5	1-3	4,8,9	3	0	0	3	40	60	100
III	25MAC311	Yoga	MAC				3	0	0	1	0	0	0	0
	Semester Total										24	280	420	700

SEMESTER IV

Semester	Course Code	Title of the Course	Course Category	NCrF level	Objectives and outcomes		SDG Goal	Instruction Hours / week			Credit(s)	Marks		
					PEOs	Pos		L	T	P		CIA	ESE	Total
IV	25CYU421	Cloud Network and Security (AWS)	PCC	5	1-5	1-3	4,5 8, 9	3	0	2	4	40	60	100
IV	25CYU401	Security Audit and Risk Assessment	PCC	5	1-5	1-3	4,5 8, 9	3	0	0	3	40	60	100
IV	25CYU402	Secure Software Engineering	PCC	5	1-5	1-3	4,5 8, 9	3	0	0	3	40	60	100
IV	25CYU403	Cyber Attacks and Countermeasures	PCC	5	1-5	1-3	4,5 8, 9	3	0	0	3	40	60	100
IV	25CYU411	Secure Software Engineering laboratory	PCC	5	1-5	1-3	4,8 , 9	0	0	4	2	40	60	100
IV	25CYU412	Cyber Attacks and Countermeasures Laboratory	PCC	5	1-5	1-3	4,8 , 9	0	0	4	2	40	60	100
IV	25CYU491	Mini Project	PRO	5.5	1-5	1-3	4,8 , 9	0	0	4	2	40	60	100
IV	25IKS002	Vedic Mathematics and Critical Thinking	IKS	4.5			4,8	2	0	0	2	40	60	100
	Semester Total										21	320	480	800

SEMESTER V

Semester	Course Code	Title of the Course	Course Category	NCrF level	Objectives and outcomes		SDG Goal	Instruction Hours / week			Credit(s)	Marks		
					PEOs	Pos		L	T	P		CIA	ESE	Total
V	25CYU501	Artificial Intelligence and Machine Learning	PCC	5.5	1-5	1-3	4,8, 9	3	0	0	3	40	60	100
V	25CYU502	Database Management Systems and Security	PCC	5.5	1-5	1-3	4,8, 9	3	0	0	3	40	60	100
V	25CYU521	Applied Cryptography + Lab	PCC	5.5	1-5	1-3	4,8, 9	3	0	2	4	40	60	100
V		Professional Elective-1	PEC	5.5	1-5	1-3	4,8, 9	3	0	0	3	40	60	100
V		Professional Elective-2	PEC	5.5	1-5	1-3	4,8, 9	3	0	0	3	40	60	100
V		Open Elective-1	OEC	5.5	1-5	1-3	4,8, 9	3	0	0	3	40	60	100
V	25CYU511	Database Management Systems and Security Laboratory	PCC	5.5	1-5	1-3	4,8, 9	0	0	4	2	40	60	100
V	25CYU581	Internship-1	IAS	5.5	1-5	1-3	4,8, 9	0	0	0	1	40	60	100
V	25MAC501	Entrepreneurship and Development	MAC	4.5			4,9	3	0	0	3	40	60	100
	Semester Total										25	360	540	900

SEMESTER VI

Semester	Course Code	Title of the Course	Course Category	NCrF level	Objectives and outcomes		SDG Goal	Instruction Hours / week			Credit(s)	Marks		
					PEOs	Pos		L	T	P		CIA	ESE	Total
VI	25CYU621	Vulnerability Assessment and Penetration Testing + Lab	PCC	5.5	1-5	1-3	4,8, 9	3	0	2	4	40	60	100
VI	25CYU622	Mobile and Wireless Security +Lab	PCC	5.5	1-5	1-3	4,8, 9	3	0	2	4	40	60	100
VI	25CYU623	Cyberforensics + Lab	PCC	5.5	1-5	1-3	4,8, 9	3	0	2	4	40	60	100
VI		Professional Elective-3	PEC	5.5	1-5	1-3	4,8, 9	3	0	0	3	40	60	100
VI		Professional Elective-4	PEC	5.5	1-5	1-3	4,8, 9	3	0	0	3	40	60	100
VI		Open Elective 2 (Online)	OEC	5.5	1-5	1-3	4,8, 9	3	0	0	3	40	60	100
	Semester Total										21	240	360	600

SEMESTER VII

Semester	Course Code	Title of the Course	Course Category	NCrF level	Objectives and outcomes		SDG Goal	Instruction Hours / week			Credit(s)	Marks		
					PEOs	Pos		L	T	P		CIA	ESE	Total
VII	25CYU721	Social Network Security +Lab	PCC	6	1-5	1-3	4,8, 9	3	0	2	4	40	60	100
VII		Professional Elective 5	PEC	6	1-5	1-3	4,8, 9	3	0	0	3	40	60	100
VII		Professional Elective 6	PEC	6	1-5	1-3	4,8, 9	3	0	0	3	40	60	100
VII		Open Elective 3	OEC	6	1-5	1-3	4,8, 9	3	0	0	3	40	60	100
VII	25CYU791	Project Work - Phase I	PRO	6	1-5	1-3	4,8, 9	0	0	12	6	40	60	100
VII	25CYU781	Internship-2	IAS	6	1-5	1-3	4,8, 9	0	0	0	1	40	60	100
	Semester Total										20	240	360	600

SEMESTER VIII

Semester	Course Code	Title of the Course	Course Category	NCrF level	Objectives and outcomes		SDG Goal	Instruction Hours / week			Credit(s)	Marks		
					PEOs	Pos		L	T	P		CIA	ESE	Total
VIII		Open Elective 4 (Online)	OEC	6	1-5	1-3	4,8, 9	3	0	0	3	40	60	100
VIII	25CYU891	Project Work - Phase II	PRO	6	1-5	1-3	4,8, 9	0	0	24	12	40	60	100
	Semester Total										15	80	120	200

St.Peter's Institute of Higher Education and Research								
Department of Information Technology								
B.Tech Cybersecurity Curriculum 2025								
Elective List								
Vertical List 1 - Network Engineer								
S.No	**Course Code**	**Course type**	**Category**	**Course Name**	**L**	**T**	**P**	**C**
1	25CYU531A	Theory	PEC	Java Programming	3	0	0	3
2	25CYU532A	Theory	PEC	IP Address Management	3	0	0	3
3	25CYU631A	Theory	PEC	Remote Infrastructure Management	3	0	0	3
4	25CYU632A	Theory	PEC	Zero Trust Network	3	0	0	3
5	25CYU731A	Theory	PEC	Network Security and Firewalls	3	0	0	3
6	25CYU732A	Theory	PEC	Securing IT Infrastructure	3	0	0	3
Vertical List 2 - Security Engineer								
1	25CYU531B	Theory	PEC	Devops	3	0	0	3
2	25CYU532B	Theory	PEC	Security Reporting Dashboards and PowerBI	3	0	0	3
3	25CYU631B	Theory	PEC	Windows Policy Management	3	0	0	3
4	25CYU632B	Theory	PEC	Malware Analysis and Mitigation Technique	3	0	0	3
5	25CYU731B	Theory	PEC	Security Audit and Risk assessment	3	0	0	3
6	25CYU732B	Theory	PEC	Security Incident Response and Management	3	0	0	3
Vertical List 3 - IAM Engineer								
1	25CYU531C	Theory	PEC	Enterprise ID and Access Management	3	0	0	3

2	25CYU532C	Theory	PEC	Identity & Digital Certificate	3	0	0	3
3	25CYU631C	Theory	PEC	Identity and Access Management Protocols and Standards	3	0	0	3
4	25CYU632C	Theory	PEC	Cybercrimes and Digital Forensics	3	0	0	3
5	25CYU731C	Theory	PEC	IT service delivery	3	0	0	3
6	25CYU732C	Theory	PEC	Legal,Ethical and Social issues in Information Security	3	0	0	3
Vertical List 4 - Security Developer								
1	25CYU531D	Theory	PEC	Secure Coding	3	0	0	3
2	25CYU532D	Theory	PEC	Project Management	3	0	0	3
3	25CYU631D	Theory	PEC	API Security	3	0	0	3
4	25CYU632D	Theory	PEC	Advanced Java Programming	3	0	0	3
5	25CYU731D	Theory	PEC	Ethical Hacking	3	0	0	3
6	25CYU732D	Theory	PEC	Agile Scrum	3	0	0	3

Semester – I

25 MAU108 **ENGINEERING MATHEMATICS - I** **4H – 4C**

Instruction Hours / week: L: 3 T: 1 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**

End Semester Exam: 3 Hours

Course Objectives

- Develop the uses of matrix algebra techniques that is needed by engineers for practical applications.
- Differentiate continuity and differentiability under differential calculus.
- Identify functions of several variables. This is required in many branches of engineering.
- Solve the problems under integral calculus.
- Acquaint the student with mathematical tools needed in evaluating multiple integrals and their applications.

Course Outcomes (COs)

At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Use the matrix algebra methods for solving practical problems	Apply
CO2	Use differential calculus ideas on several variable functions	Apply
CO3	Apply the concept of several variable functions in calculus	Understand
CO4	Apply the concept of integral calculus	Apply
CO5	Apply multiple integral ideas in solving areas, volumes and other applications	Apply

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO1	PSO2	PSO3
CO 1	3	2	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 2	3	2	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 3	3	2	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 4	3	2	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 5	3	2	--	--	--	--	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

Unit I – MATRICES

Eigenvalues and Eigenvectors of a real matrix – Characteristic equation – Properties of Eigen values and Eigen vectors – Cayley-Hamilton theorem – Diagonalization of matrices by orthogonal transformation – Reduction of a quadratic form to canonical form by

orthogonal transformation – Nature of quadratic forms – Applications: Stretching of an elastic membrane.

Unit II – DIFFERENTIAL CALCULUS

Representation of functions – Limit of a function – Continuity – Derivatives – Differentiation rules (sum, product, quotient, chain rules) – Implicit differentiation – Logarithmic differentiation – Applications: Maxima and Minima of functions of one variable.

Unit III – FUNCTIONS OF SEVERAL VARIABLES

Partial differentiation – Homogeneous functions and Euler's theorem – Total derivative – Change of variables – Jacobians – Partial differentiation of implicit functions – Taylor's series for functions of two variables – Applications: Maxima and minima of functions of two variables, Lagrange's method of undetermined multipliers.

Unit IV –INTEGRAL CALCULUS

Definite and Indefinite integrals — Substitution rule — Techniques of Integration — Integration by parts, Trigonometric integrals, Trigonometric substitutions, Integration of rational functions by partial fraction, Integration of irrational functions — Improper integrals.

Unit V – MULTIPLE INTEGRALS

Double integrals – Change of order of integration – Double integrals in polar coordinates – Area enclosed by plane curves – Triple integrals – Volume of solids – Change of variables in double and triple integrals – Applications: Moments and centres of mass, moment of inertia.

SUGGESTED READINGS

1. Kreyszig, E. (2016). Advanced Engineering Mathematics. 10th Edition, John Wiley and Sons.
2. Grewal, B.S. (2018). Higher Engineering Mathematics. 44th Edition, Khanna Publishers.
3. Bali, N., Goyal, M., & Watkins, C. (2009). Advanced Engineering Mathematics. 7th Edition, Firewall Media.
4. Jain, R.K. & Iyengar, S.R.K. (2016). Advanced Engineering Mathematics. 5th Edition, Narosa Publications.
5. Narayanan, S. & Manicavachagom Pillai, T.K. (2009). Calculus, Volume I and II, S. Viswanathan Publishers.

B.E. / B.Tech. (Common to all Branches) **2025-2026**

Semester – I

25PHU121 **EMGINEERING PHYSICS** **5H – 4C**

Instruction Hours / week: L: 3 T: 0 P: 2 Marks: Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Provide a foundational understanding of the electrical properties of materials
- Introduce the fundamental concepts and behaviour of semiconductor materials
- Develop a conceptual and mathematical understanding of elasticity
- Explain the thermal properties of engineering materials
- Examine experimental evidence such as electron diffraction.

Course Outcomes (COs)

At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Discuss the basic electrical properties of materials and classify materials based on band theory.	Understand, Apply
CO2	Explain the properties of semiconductor materials and determine the band gap using appropriate experimental methods.	Understand, Apply
CO3	Calculate different moduli of elasticity and explain their applications in engineering and materials science.	Apply
CO4	Describe the thermal properties of materials and their applications, such as thermal expansion in joints and the functioning of heat exchangers.	Remember, Apply
CO5	Interpret the concept of wave-particle duality and describe experimental evidence, such as electron diffraction, that supports this duality.	Understand

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PSO1	PSO2
CO 1	3	3	3	3	3	3	3	3	3	3	3	3	3	2
CO 2	3	3	3	3	3	3	3	3	3	3	3	3	3	2
CO 3	3	3	3	3	3	3	3	3	3	3	3	3	3	2
CO 4	3	3	3	3	3	3	3	3	3	3	3	3	3	2
CO 5	3	3	3	3	3	3	3	3	1	2	3	3	3	2

1 - low, 2 - medium, 3 - high

Unit-I ELECTRICAL PROPERTIES OF MATERIALS

Classical free electron theory-Expression for Electrical conductivity-thermal conductivity-expression- Wiedmann Franz law- success and failure-electrons in metals-Particle in three dimensional box- degenerate state- Fermi Dirac Statistics-Density of Energy states-Electron in periodic potential-Bloch Theorem- Metals and Insulators-Energy bands in solids-Effective mass of electron- Concept of holes.

Unit II SEMICONDUCTORS AND TRANSPORT PHYSICS

Intrinsic semiconductors- Carrier concentration derivation– Fermi level – variation of Fermi level with temperature –electrical conductivity – band gap determination -extrinsic semiconductors - Carrier concentration in N-type & P-type semiconductors – Variation of fermi level with temperature and impurity concentration.

Unit III PROPERTIES OF MATTER

Elasticity – Poisson's ratio and relationship between moduli (qualitative) - stress-strain diagram for ductile and brittle materials, uses - factors affecting elastic modulus and tensile strength - bending of beams - cantilever - bending moment - Young's modulus determination - theory and experiment - uniform and non-uniform bending - I shaped girders - twisting couple torsion pendulum - determination of rigidity modulus- moment of inertia of a body .

Unit IV THERMAL PHYSICS

Transfer of heat energy – thermal expansion of solids and liquids – expansion joints - bimetallic strips - thermal conduction, convection and radiation – heat conductions in solids – thermal conductivity - Forbe's and Lee's disc method: theory and experiment - conduction through compound media (series and parallel) – thermal insulation – applications: heat exchangers, refrigerators, ovens and solar water heaters.

Unit V QUANTUM PHYSICS

Black body radiation – Planck's theory (derivation) – Compton effect: theory and experimental verification – wave particle duality – electron diffraction – concept of wave function and its physical significance – Schrödinger's wave equation – time independent and time dependent equations – particle in a one-dimensional rigid box – tunnelling (qualitative) - scanning tunnelling microscope.

PRACTICAL EXERCISES

1.Torsional Pendulum-Determination of Moment of Inertia and Rigidity Modulus with equal masses

2. (a) Determination of wavelength, and particle size using Laser

(b) Determination of acceptance angle in an optical fiber

3. Determination of Young's modulus by non-uniform bending method

4. Determination of thermal conductivity of a bad conductor – Lee's Disc method

5. Ultrasonic Interferometer-Determination of Velocity of Ultrasonic waves and Compressibility of the given liquid

6. Determination of band gap of a semiconductor

7. LC circuit and LCR circuit

SUGGESTED READINGS:

1. Charles Kittel – Introduction to Solid State Physics, 8th Edition (2018) Publisher: Wiley
2. Brij Lal and N.Subramaniam, Properties of Matter S. Chand & Co., New Delhi 1994)
3. G. Aruldhas's Quantum Mechanics is the Second Edition, published by PHI Learning in 2008.
4. Donald A. Neamen's Semiconductor Physics and Devices: Basic Principles n the 4th Edition, published in 2012 by McGraw-Hill.
5. Halliday, D., Resnick, R. & Walker, J. “Principles of Physics”. Wiley, 2015.
6. R. Shankar's Principles of Quantum Mechanics is the Second Edition, published in 1994 by Plenum Press
7. Dr. S. Stella Mary, ‘Practical Engineering Physics’ R. K. Publications, 2013
8. C.C. Ouseph, U.J. Rao, V. Vijayendran, ‘Practical Physics and Electronics’, S.Viswanathan Printers and Publishers Pvt. Ltd., 2011

25EVS001 **ENVIRONMENTAL SCIENCE** **Semester – I**
2H – 2C

Instruction Hours / week: L: 2 T: 0 P: 0 **Marks:** Internal: **40**External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Understand the scope and significance of the environment, raise public awareness about various environmental hazards and the structure and function of ecosystems
- Introduce the concept of biodiversity, its different types and the importance of its conservation at global, national, and local levels.
- Understand the causes, effects, and control measures of various environmental hazards, solid waste and disaster management, role of individuals in pollution prevention.
- Understand the need for new and renewable energy sources, focusing on energy management and conservation, and their applications.
- Understand the concepts of global and local environmental issues, various environmental protection laws

Course Outcomes (COs)
At the completion of the course the student will be able to

Cos	Course Outcomes	Blooms Level
CO1	Define the environment and its significance, different environmental hazards, and the roles of producers, consumers, and decomposers in ecosystems,energy flow and the structure of food chains, food webs, and ecological pyramids in various ecosystems.	Understand
CO2	Define biodiversity and its various levels, biodiversity hotspots, threats to biodiversity, and the importance of conserving endangered and endemic species in India using in-situ and ex-situ methods.	Understand
CO3	Identify the causes, effects control of different environmental hazards (air, water, marine, soil, noise, thermal, and nuclear pollution), importance of solid waste management and disaster management (floods, earthquakes, cyclones, and landslides), the role of individuals in preventing pollution and pollution case studies.	Remember
CO4	Explore the role and potential of new and renewable energy sources, different types of renewable energy and their applications, particularly hydrogen, ocean, tidal, and geothermal energy, the concepts and technology behind energy management and conservation.	Understand
CO5	Identify key environmental issues and the role of environmental protection laws in safeguarding ecosystems, wildlife, and forests.	Understand

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO12	PS O1	PS O2	PS O3
CO 1	2	1	3	1	2	2	2	1	1	1	1	3	2	2	2
CO 2	3	2	3	1	2	2	2	1	1	1	1	2	3	2	3
CO 3	2	2	3	1	2	1	2	1	1	1	1	3	2	3	2
CO 4	3	1	2	1	2	2	2	1	1	1	1	2	3	2	3
CO 5	3	2	3	1	1	1	2	1	1	1	1	3	2	3	3

1 - low, 2 - medium, 3 - high

Unit I – ENVIRONMENT AND ECOSYSTEM

Environment – Definition, scope and significance - Public awareness: Risk and hazards - Chemical hazards, Physical hazards, Biological hazards in the environment. Ecosystem - concept -structure and function - producers, consumers and decomposers - Food chain - Food web - Ecological pyramids - Energy flow - Forest, Grassland, desert and aquatic ecosystem

Unit II – BIODIVERSITY AND ITS CONSERVATION

Introduction to Biodiversity - Definition - genetic, species and ecosystem diversity - Values and uses of biodiversity - biodiversity at global, national (India) and local levels - Hotspots, threats to biodiversity - Endangered and endemic species of India - conservation of biodiversity.

Unit III – ENVIRONMENTAL POLLUTION AND MANAGEMENT

Definition, Causes - Effects and control measures of Air, Water, Marine, soil, Noise, thermal and nuclear hazards, Solid waste Management : Causes, effects and control measures of urban and industrial wastes- Role of an individual in prevention of pollution- Pollution case studies- Disaster management : floods, earthquake, cyclone and landslides

Unit IV – RENEWABLE SOURCES OF ENERGY

Role and potential of new and renewable source- Energy management and conservation, New Energy Sources: Need of new sources. Different types of new energy sources. Applications of- Hydrogen energy, Ocean energy resources, Tidal energy conversion. Concept, origin and power plants of geothermal energy

Unit V – ENVIRONMENTAL PROTECTION

Climate change- Global, Regional and local environmental issues. Environmental Impact Assessment. Environment protection act, wildlife protection act. and forest conservation act.

SUGGESTED READINGS

1. Gilbert M.Masters "Introduction to Environmental Engineering and Science", 2nd edition, Pearson Education (2004).
2. Benny Joseph, "Environmental Science and Engineering", Tata McGraw-Hill, New Delhi (2006).
3. Trivedi.R.K., "Handbook of Environmental Laws, Rules, Guidelines, Compliances and Standards", Vol. I and II, Enviro Media, 3rd edition, BPB publication (2010).
4. Anubha Kaushik and C. P. Kaushik's "Perspectives in Environmental Studies", 6th Edition, New Age International Publishers, 2018.
5. Allen, D. T. and Shonnard, D. R., Sustainability Engineering: Concepts, Design and Case Studies, Prentice Hall.
6. Bradley. A.S; Adebayo, A.O., Maria, P. Engineering applications in sustainable design and development, Cengage learning
7. Environment Impact Assessment Guidelines, Notification of Government of India, 2006.
8. Mackenthun, K.M., Basic Concepts in Environmental Management, Lewis Publication, London, 1998.
9. Dharmendra S. Sengar, 'Environmental law', Prentice hall of India PVT. LTD, New Delhi, 2007.
10. Rajagopalan, R, 'Environmental Studies-From Crisis to Cure', Oxford University Press, 2005
11. Erach Bharucha "Textbook of Environmental Studies for Undergraduate Courses" Orient Blackswan Pvt. Ltd. 2013.

Semester – I

25ENU121 **TECHNICAL ENGLISH** **5H – 4C**

Instruction Hours / week: L: 3 T: 0 P: 2 **Marks:** Internal: **40**External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Enhance the communicative competence of learners.
- Assist learners in using language effectively in academic/work contexts.
- Strengthen students' English language skills by engaging them in listening, speaking, and grammar learning activities that are relevant to authentic contexts.
- Develop analytical thinking skills for problem-solving in communicative contexts
- Equip them with writing skills needed for academic as well as workplace contexts.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Listen and comprehend complex academic texts.	Remember
CO2	Read and infer the denotative and connotative meanings of technical texts.	Apply
CO3	Write definitions, descriptions narrations and essays on various topics.	Apply
CO4	Speak fluently and accurately and informal communicative contexts.	Apply
CO5	Express their opinions effectively in both oral and written medium of communication.	Create

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PSO1	PSO2
CO 1	3	3	3	3	3	3	3	2	3	3	3	3	3	2
CO 2	3	3	3	3	3	3	3	2	3	3	3	3	3	2
CO 3	3	3	3	3	3	3	3	2	3	3	3	3	3	2
CO 4	3	3	3	3	3	3	3	2	3	3	3	3	3	2
CO 5	3	3	3	3	3	3	3	2	1	2	3	3	3	2

1 - low, 2 - medium, 3 - high

Unit I INTRODUCTION TO COMMUNICATION SKILLS

Listening–for general information-specific details-conversation: Introduction to classmates. Speaking - Self Introduction; Introducing a friend; Conversation - politeness strategies; Telephone conversation. Reading - Reading brochures (technical context). Writing-Writing emails/letters introducing oneself, Paragraph Writing, Reading Comprehension. Grammar – Parts of Speech, Sentence kinds. Wh-Questions forms and Tags. Vocabulary-Synonyms; One word substitution; Abbreviations &Acronyms (as used in technical contexts).

Unit II: REPORTING AND NARRATIONS

Listening- Listening to podcast, anecdotes/stories/event narration; documentaries and interviews. Speaking- Narrating personal experiences/events; Interviewing a celebrity; Reporting and summarizing of documentaries/podcasts/interviews.Reading- Reading biographies, travelogues, news paper reports, Excerpts from literature, travel and technical blogs. Writing – Report Writing - Short Report on an event. Grammar- Sentence Structures, Tenses. Vocabulary– Antonyms, Word Formation (prefixes & suffixes).

Unit III: ACADEMIC DEVELOPMENT AND COMMERCIAL REVIEWS

Listening- Listen to a classroom lecture. Speaking–Picture description; Giving instruction to use the product; Presenting a product and summarizing a lecture. Reading – Reading advertisements, gadget reviews; user manuals. Writing - Writing definitions; Instructions. Grammar-Active & Passive Voice, The Impersonal Passive., Subject-Verb Agreement; Infinitive and Gerunds. Vocabulary -Compound Words, Homonyms; and Homophones.

Unit IV: SCIENTIFIC REPORTS AND PRESENTATION TECHNIQUES

Listening – Listening to TED Talks; Scientific lectures and educational videos. Speaking – Small Talk; Mini presentations and making recommendations. Reading–News paper articles; Journal reports–and Non Verbal Communication (tables, pie charts etc,).Writing–Writing recommendations; Transferring information from non verbal (chart, graph etc, to verbal mode), Checklists. Grammar–Error correction; If conditional sentences., Vocabulary- Discourse markers, Connectives, Articles.

Unit V: POINT OF VIEW AND PLACEMENTS.

Listening–Listening to debates/discussions; different viewpoints on an issue; and panel discussions. Speaking–Group discussions, Debates, and Expressing opinions through Simulations &Role play. Reading – Reading Editorials and Opinion Blogs. Writing–Job/ application–Cover letter& Resume. Grammar–Numerical adjectives, Punctuation. Vocabulary- Cause & Effect Expressions

PRACTICAL EXERCISES

1. Group Discussion: Practical based on Accurate and Current Grammatical Patterns.
2. Conversational Skills for Interviews under suitable Professional Communication Lab conditions with emphasis on Kinesics
3. Communication Skills for Seminars/Conferences/Workshops with emphasis on Paralinguistics/ Kinesics.
4. Presentation Skills for Technical Paper/Project Reports/ Professional Reports based on proper Stress and Intonation Mechanics.
5.Official/Public Speaking based on suitable Rhythmic Patterns.
6. Argumentative Skills/Role Play Presentation with Stress and Intonation

SUGGESTED READINGS

1. English for Engineers &Technologists Orient Blackswan Private Ltd. Department of English, Anna University,(2020 edition)
2. English for Science &Technology Cambridge University Press, 2021.
3. Technical Communication–Principles And Practices by Meenakshi Raman &Sangeeta Sharma
4. Dr.S.Uma Maheswari. English Workbook for Engineers and Technologists
5. Lakshmi Narayanan,Course Book on Technical English

Semester – I

25EEU101 **BASICS OF ENGINEERING** **3H – 3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To understand the basic calculations and measurements in DC circuits.
- To familiarize with working and characteristics of different DC and AC machines.
- To impart knowledge on the fundamentals of measuring electrical and electronic quantities, various sensors and transducers to measure non-electrical quantities.
- Demonstrate the fundamentals and scope of Mechanical Engineering, covering its core principles, key domains, and emerging technologies
- Identify basic and modern construction materials, explain their engineering properties,

Course Outcomes (COs)

At the completion of the course the student will be able to

Cos	Course Outcomes	Blooms Level
CO1	Perform the basic calculations in DC circuits and measure the various quantities associated with DC circuits.	Understand
CO2	Choose appropriate motor for specific applications based on the motor characteristics	Analyze
CO3	Analyze the functional blocks of a measurement system and the principles of various electrical and electronic instruments,	Analyze
CO4	Describe the scope of Civil Engineering and identify basic and modern construction materials along with their properties	Understand
CO5	Distinguish between different Steams of Mechanical Engineering and to gain foundational knowledge of mechanical systems, tools, and applications.	Understand

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PSO1	PSO2	PSO3
CO 1	3	2	–	2	2	–	–	–	–	–	2	3	3	1	3
CO 2	3	3	–	2	2	–	–	–	–	–	2	3	3	1	3
CO 3	3	3	–	3	3	–	–	–	–	–	2	3	3	2	3
CO 4	2	1	–	–	–	2	2	–	–	–	1	–	–	3	2
CO 5	2	1	–	–	–	–	2	–	–	–	1	–	–	3	2

1 - low, 2 - medium, 3 - high

Unit I: DC CIRCUITS AND MEASUREMENTS

The concept of voltage and current-Electric circuit elements: R, L, C – Independent and dependent sources – Ohm's law- Kirchhoff's law- series and parallel resistive circuits – Voltage and current division – Star-delta transformation - Mesh and nodal analysis of resistive circuits – simple problems - Measurement of voltage, current and power in DC circuits.

Unit II: ELECTRICAL MACHINES

Construction, principle of operation, basic equations, characteristics and applications of DC generators, DC motors, single phase transformers and Single phase induction motors. Working principle of BLDC Motor and its applications in home appliances.

Unit III:ELECTRICAL AND ELECTRONIC INSTRUMENTATION

Functional blocks of a measurement system - types of measurements - Direct and indirect measurements – Classification of instruments – Induction type – dynamometer type wattmeter's- Types of indicating Instruments Principles of Electrical Instruments – Multimeters, Oscilloscopes - Static and Dynamic characteristics of an instrumentation system – Errors in Measurement – Calibration and Standards.. Classification of Transducers: Resistive, Inductive, Capacitive, Thermoelectric, piezoelectric, photoelectric, Hall Effect – electromagnetic flow transducers

Unit IV: INTRODUCTION TO CIVIL ENGINEERING AND MATERIALS

Introduction to Civil Engineering- Basic Construction Materials- Properties of Engineering Materials- Selection of Materials for Construction- Modern Materials in Construction

Unit V SCOPE AND CORE PRINCIPLES OF MECHANICAL ENGINEERING

Design, Manufacturing, Materials, Energy and Power Systems, Kinematics and Robotics, Instrumentation and Control, Emerging Trends, and Smart Applications.

SUGGESTED READINGS:

1.D P Kothari and I.J Nagarath, "Basic Electrical and Electronics Engineering", McGraw Hill Education (India) Private Limited, Third Reprint, 2016.
2.Giorgio Rizzoni, "Principles and Applications of Electrical Engineering", McGraw Hill Education (India) Private Limited, 2010.
3.S.K.Bhattacharya, "Basic Electrical and Electronics Engineering", Pearson India, 2011.
4.Del Toro, "Electrical Engineering Fundamentals", Pearson Education, New Delhi, 2015.
5.Leonard S Bobrow, "Foundations of Electrical Engineering", Oxford University Press, 2013.
6.Rajendra Prasad, "Fundamentals of Electrical engineering", Prentice Hall of India, 2006.
7.Mittle N., "Basic Electrical Engineering", Tata McGraw Hill Edition, 24th reprint 2016.
8.Sawhney, A. K., and Puneet Sawhney "A Course in Electrical and Electronic Measurements and Instrumentation" Dhanpat Rai & Company, 2016

Semester – I

25CSU121 PROGRAMMING FOR PROBLEM SOLVING 6H – 4C

Instruction Hours / week: L: 2 T: 0 P: Marks: Internal: **40** External: **60** Total: **100**

End Semester Exam: 3 Hours

Course Objectives

- Develop the foundational understanding of problem-solving techniques, algorithm design, and programming basics using C and Python.
- Apply conditional and iterative constructs effectively for developing logical, flow-controlled programs in both C and Python.
- Impart knowledge of function-based and modular programming approaches for creating structured, maintainable, and reusable code.
- Equip students with the ability to manipulate arrays, strings, and lists, and apply fundamental searching and sorting algorithms in C and Python..
- Introduce memory management concepts through pointers in C, and provide practical skills in file handling and understanding Python's memory model.

Course Outcomes (COs)

At the completion of the course the student will be able to

Cos	Course Outcomes	Blooms Level
CO1	Construct basic programs using variables, operators, and input/output functions in C and Python	Remember
CO2	Execute decision-making and looping structures to solve common computational problems	Apply
CO3	Assemble modular programs by defining reusable functions with appropriate parameter usage and scope control	Analyze.
CO4	Implement basic searching and sorting algorithms to process structured data arrays, strings, and lists	Create
CO5	Demonstrate the use of pointers and dynamic memory in C, and operate file handling and memory reference concepts in C and Python	Evaluate

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PSO 1	PSO 2
CO 1	3	1	1	2	3	2	2	1	2	1		3	2	3
CO 2	3	2	2	2	3	2	3	2	2	2	2	3	2	3
CO 3	3	2	2	2	3	2	3	2	1	2	1	3	2	3
CO 4	3	2	2	2	3	2	3	2	2	2	2	3	2	3
CO 5	3	1	1	2	3	2	2	2	1	1		3	2	3

1 - low, 2 - medium, 3 - high

Unit I: INTRODUCTION TO PROGRAMMING

Introduction to problem solving, algorithms, and flowcharts, Programming structure in C and Python, Data types, variables, constants, Operators and expressions (arithmetic, relational, logical, assignment, Input/output functions: scanf, printf (C); input(), print() (Python) Type conversion and casting

Unit II: CONTROL FLOW AND ITERATIVE STATEMENTS

Decision-making: if, if-else, nested if, switch-case (C); if-elif-else (Python), Looping constructs: while, for, do-while (C); while, for-in (Python), Loop control: break, continue, pass, Problem-solving using loops (e.g., sum of digits, reverse number, pattern printing)

Unit III:FUNCTIONS AND MODULAR PROGRAMMING

Defining and calling functions in C and Python, Function parameters, return types, recursion, Python-specific: default arguments, keyword arguments, lambda functions, Variable scope and storage classes, Modular programming: creating reusable code blocks

Unit IV:ARRAYS, STRINGS, LISTS

Arrays in C: 1D and 2D, basic operations, Strings in C: declaration, input/output, string.h functions, Python lists: indexing, slicing, built-in methods, list comprehensions, Python strings: methods, slicing, immutability, Searching and sorting algorithms (linear, binary search; bubble, selection sort)

Unit V:POINTERS (C) AND FILE HANDLING IN C AND PYTHON

Pointers in C-declaration and initialization- Pointers and arrays-Pointers and functions (call by reference)

Pointers and structures, Dynamic memory allocation: malloc(), calloc(), realloc(), free(), File Handling in C-and python, Python memory model Mutable vs immutable objects, Function argument passing (by object reference) using id() to understand memory behavior

PRACTICAL EXERCISES (C and Python):

1. Write a Program to convert Celsius to Fahrenheit and vice versa. (Practice: I/O, arithmetic operators, conditionals)
2. Write a Program to simulate Simple Calculator that Perform addition, subtraction, multiplication, and division based on user input. (Practice: switch-case or if-elif-else.)
3. Write a program to check whether a given number is Odd or Even (Practice: conditionals,modulo operator).
4. Write a program to find Factorial of a Number using both iterative and recursive methods.(Practice: loops, recursion).
5. Write a program to Print Fibonacci series up to n terms. (Practice: loop/recursion logic.)
6. Write a program to find the GCD of two numbers. (Practice: functions, logic)
7. Write a program to check if a number is prime. (Practice: loops, conditionals, modularity.
8 Write a program to reverse a 1D array (C) or list (Python). (Practice: arrays/lists, loops)

9 Write a program to check if a given string is a palindrome. (Practice: string manipulation.)
10 Write a program to sort a list/array using bubble sort or selection sort. (Practice: sorting logic).
11 Write a program to define a structure for storing student data and display it. (Practice: structs, functions).
12 Write a program to implement stack using List (Python) Implement push and pop operations. (Practice: lists, stack logic).
13 Write a program to read from and write to a text file. Practice: file I/O basics.
14 Write a program to read a file and count the number of words. (Practice: string handling, file reading.)

SUGGESTED READINGS

1. Paul Deitel and Harvey Deitel, “C How to Program”, 9th Edition, Pearson Education, 2022
2. John Zelle, “Python Programming: An Introduction to Computer Science”, 3rd Edition, Franklin, Beedle & Associates, 2016. ISBN: 978-1590282755..
3. Mark Lutz, “Learning Python”, 5th Edition, O'Reilly Media, 2013.
4. Eric Matthes, “Python Crash Course”, 2nd Edition, No Starch Press, 2019.
5. Charles Severance, “Python for Everybody: Exploring Data in Python 3”, 2nd Edition, Charles Severance, 2020.

B.E. / B.Tech. (Common to all Branches) **2025-2026**

Semester – I

25MEU101 **ENGINEERING GRAPHICS** **3H – 3C**

Instruction Hours / week: L: 1 T: 2 P: Marks: Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Communicate the concepts, ideas and design of Engineering products through graphic skills.
- Acquaint the national standards related to technical drawings.
- Comprehend Orthographic, Isometric and perspective projection to represent the objects in two and three-dimensions.

Course Outcomes (COs)
At the completion of the course the student will be able to

Cos	Course Outcomes	Blooms Level
CO1	Sketch and distinguish between conic curves, cycloids, and involutes, and construct appropriate scales for engineering applications.	Apply
CO2	Identify and apply projection techniques to represent points, lines, and plane surfaces in first angle orthographic views.	Remember
CO3	Assemble and design accurate projections of solid geometries and truncated forms using appropriate methods.	Analysis
CO4	Prepare developments and sections of solids with holes and cut-outs, and evaluate the true shape of these sections.	Evaluate
CO5	Create isometric and perspective projections of simple and compound solids, and utilize CAD tools for visualization.	Create

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO 1	3	2	3	1	2	1	1	1	2	2	2	2	2	2	3
CO 2	3	2	2	1	2	1	1	1	2	2	2	2	2	2	3
CO 3	3	2	2	1	2	1	1	1	2	2	2	2	2	2	3
CO 4	3	2	2	1	2	1	1	1	2	2	2	2	2	2	3
CO 5	3	2	2	1	2	1	1	1	2	2	2	2	2	2	3

1 - low, 2 - medium, 3 - high

Unit I:PLANE CURVES AND FREE HAND SKETCHING

Basic Geometrical constructions, Curves used in engineering practices: Conics – Construction of ellipse, parabola and hyperbola by eccentricity method – Construction of cycloid – construction of involutes of square and circle – Drawing of tangents and normal to the above curves, Scales: Construction of Diagonal and Vernier scales. Visualization concepts and Free Hand sketching: Visualization principles –Representation of Three Dimensional objects – Layout of views- Free hand sketching of multiple views from pictorial views of objects.

Unit II: PROJECTION OF POINTS, LINES AND PLANE SURFACES

Orthographic projection- principles-Principal planes-First angle projection-projection of points. Projection of straight lines (only First angle projections) inclined to both the principal planes - Determination of true lengths and true inclinations by rotating line method and traces Projection of planes (polygonal and circular surfaces) inclined to both the principal planes by rotating object method.

Unit III:PROJECTION OF SOLIDS

Projection of simple solids like prisms, pyramids, cylinder, cone and truncated solids when the axis is inclined to one of the principal planes by rotating object method and auxiliary plane method.

Unit IV:PROJECTION OF SECTIONED SOLIDS AND DEVELOPMENT OF SURFACES

Sectioning of above solids in simple vertical position when the cutting plane is inclined to the one of the principal planes and perpendicular to the other – obtaining true shape of section. Development of lateral surfaces of simple and sectioned solids – Prisms, pyramids cylinders and cones. Development of lateral surfaces of solids with cut-outs and holes.

Unit V:ISOMETRIC AND PERSPECTIVE PROJECTIONS

Principles of isometric projection – isometric scale –Isometric projections of simple solids and truncated solids - Prisms, pyramids, cylinders, cones- combination of two solid objects in simple vertical positions and miscellaneous problems. Perspective projection of simple solids-Prisms, pyramids and cylinders by visual ray method. Computer Aided Drafting (Demonstration Only) Introduction to drafting packages and demonstration of their use.

SUGGESTED READINGS

1. Parthasarathy, N.S.and Vela Murali, “Engineering Drawing”, Oxford University Press, 2015.
2. Bhatt N.D. and Panchal V.M., “Engineering Drawing”, Charotar Publishing House, 53rd Edition,2014.
3. Gopalakrishna K.R., “Engineering Drawing” (Vol. I&II combined), Subhas Stores, Bangalore,(2017).
4. Venugopal K. and Prabhu Raja V., “Engineering graphics”, New Age International (P) Limited,(2008).
5. Natrajan K.V., “A text book of Engineering Graphics”, Dhanalakshmi Publishers, Chennai, (2012).

Semester 2

B.E.,B.Tech. (Common to all Branches) **2025-2026**

Semester – 2

25 MAU208 **ENGINEERING MATHEMATICS -II** **4H – 4C**

Instruction Hours / week: L: 3 T: 1 P: 0 Marks: Internal: **40** External: **60** Total: **100**

End Semester Exam: 3 Hours

Course Objectives

- Define and differentiate the Linear partial differential equations of second and higher order with constant coefficients of both homogeneous and non-homogeneous types.
- Identify Fourier and half range Fourier transform techniques used in wide variety of situations.
- Apply the effective mathematical tools for the solutions of partial differential equations that model several physical processes.
- Evaluate Fourier transform techniques for different functions.
- Identify Z-transforms and Elementary properties of several functions

Course Outcomes (COs)

At the completion of the course the student will be able to

Cos	Course Outcomes	Blooms Level
CO1	Solve the methods of solving Partial differential equations.	Apply
CO2	Apply the concepts in Fourier series.	Apply
CO3	Apply the Partial derivative one-two dimensional concept in solving the Heat flow equations.	Apply
CO4	Solve the problems under Fourier transforms.	Apply
CO5	Identify and apply Z-transform concepts in Problem solving.	Apply

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO 1	3	2	--	--	--	--	--	--	--	--	2	2	--	--	3
CO 2	3	2	--	--	--	--	--	--	--	--	2	2	--	--	3
CO 3	3	2	--	--	--	--	--	--	--	--	2	2	--	--	3
CO 4	3	2	--	--	--	--	--	--	--	--	2	2	--	--	3
CO 5	3	2	--	--	--	--	--	--	--	--	2	2	--	--	3

1 - low, 2 - medium, 3 - high

Unit I:PARTIAL DIFFERENTIAL EQUATIONS

Formation of partial differential equations. Solutions of standard types of first order partial differential equations – Lagrange's linear equation. Linear partial differential equations of second and higher order with constant coefficients of both homogeneous and non-homogeneous types.

Unit II:FOURIER SERIES

Dirichlet's conditions – General Fourier series – Odd and even functions – Half range sine series – Half range cosine series – Root mean square value – Parseval's identity – Harmonic analysis

Unit III:APPLICATIONS OF PARTIAL DIFFERENTIAL EQUATIONS

Classification of PDE – Method of separation of variables – Fourier Series – Solutions of one dimensional wave equation – One dimensional equation of heat conduction – Steady state solution of two dimensional equation of heat conduction (excluding insulated edges).

Unit IV:FOURIER TRANSFORMS

Statement of Fourier integral theorem – Fourier transform pair – Fourier sine and cosine transforms – Properties – Transforms of simple functions – Convolution theorem – Parseval's identity.

Unit V:Z TRANSFORMS

Z-transforms – Elementary properties – Convergence of Z-transform – Initial and final value theorem – Inverse Z-transform using partial fraction and residues – Formation of difference equations.

SUGGESTED READINGS

1. Kreyszig, E., 'Advanced Engineering Mathematics', John Wiley and Sons, 10th Edition, New Delhi, 2016.
2. Grewal, B.S., 'Higher Engineering Mathematics', Khanna Publishers, New Delhi, 44th Edition, 2018.
3. Bali, N., Goyal, M., and Watkins, C., 'Advanced Engineering Mathematics', Firewall Media, New Delhi, 7th Edition, 2009.
4. L.C. Andrews and B. Shivamoggi, 'Integral Transforms for Engineers', SPIE Press, 1999.
5. Narayanan, S., Manicavachagom Pillay, T.K., and Ramanaiah, G., 'Advanced Mathematics for Engineering Students', Vol. II & III, S. Viswanathan Publishers Pvt. Ltd, Chennai, 1998

Semester – 2

25CHU221 ENGINEERING CHEMISTRY 5H – 4C

Instruction Hours / week: L: 3 T: 0 P: 2 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To inculcate a sound understanding of water quality parameters and water treatment techniques.
- To impart knowledge on the basic principles and preparatory methods of nanomaterials.
- To introduce the basic concepts and applications of the phase rule and composites.
- To facilitate the understanding of different types of fuels, their preparation, properties, and combustion characteristics.
- To familiarize the students with the operating principles, working processes, and applications of energy conversion and storage devices.

Course Outcomes (COs)

At the completion of the course the student will be able to

Cos	Course Outcomes	Blooms Level
CO1	Interpret water quality parameters and treatment methods for domestic and industrial use.	Understand
CO2	Differentiate nanomaterials based on their properties, types, and synthesis techniques.	Analyse
CO3	Analyze phase diagrams and composite material systems with respect to their components and applications.	Apply
CO4	Evaluate fuel types, combustion characteristics, and emission parameters for energy efficiency.	Evaluate
CO5	Compare various energy sources and storage systems based on their principles and applications.	Assess

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	2	2	1	-	-	-	-	-	1	-	2	3	3	2
CO2	2	2	1	-	-	-	-	-	-	-	2	3	3	2
CO3	2	2	1	-	-	-	-	-	3	-	2	2	3	2
CO4	2	2	1	-	-	-	-	-	-	-	2	3	3	2
CO5	2	2	1	-	-	-	-	-	-	-	2	3	3	2

1 - low, 2 - medium, 3 - high

Unit I : WATER AND ITS TREATMENT

Water: Sources and impurities, Water quality parameters: Definition and significance of color, odour, turbidity, pH, hardness, alkalinity, TDS, COD and BOD, fluoride and arsenic. Domestic water treatment: Steps involved -primary treatment and disinfection (UV, Ozonation, breakpoint chlorination). Desalination of brackish water: Electro dialysis-Reverse Osmosis. Boiler troubles: Scale and sludge, Boiler corrosion, Caustic embrittlement, Priming and foaming. Treatment of boiler feed water: Internal treatment (phosphate, colloidal, sodium aluminate, and Calgon conditioning) and External treatment – Ion exchange demineralization process and zeolite process.

Unit II :NANOCHEMISTRY

Basics: Distinction between molecules, nanomaterials and bulk materials; Size-dependent properties (optical, electrical, mechanical and magnetic); Types of nanomaterials: Definition, properties and uses of – nanoparticle, nanocluster, nanorod, nanowire and nanotube-Single walled and Multiwalled Nanotubes- Preparation of nanomaterials: sol-gel, solvothermal, laser ablation, chemical vapour deposition, electrochemical deposition and electro spinning. Applications of nanomaterials in medicine, agriculture, energy, electronics, and catalysis.

Unit III :PHASE RULE AND COMPOSITES

Phase rule: Introduction, definition of terms with examples. One component system – water system; Reduced phase rule; Construction of a simple eutectic phase diagram – Thermal analysis; Two component system: lead-silver system – Pattinson process. Composites: Introduction: Definition & Need for composites; Constitution: Matrix materials (Polymer matrix, metal matrix, and ceramic matrix) and Reinforcement (fiber, particulates, flakes, and whiskers). Properties and applications of Metal matrix composites (MMC), Ceramic matrix composites (CMC), and Polymer matrix composites (PMC). Hybrid composites – definition and examples.

Unit IV :FUELS AND COMBUSTION

Fuels: Introduction: Classification of fuels; Coal and coke: Analysis of coal (proximate and ultimate), Carbonization, Manufacture of metallurgical coke (Otto Hoffmann method). Petroleum and Diesel: Fractional distillation of Petroleum- Manufacture of synthetic petrol (Fischer–Tropsch and Bergius process), Knocking – octane number, diesel oil – cetane number; Power alcohol and biodiesel. Combustion of fuels: Introduction: Calorific value – higher and lower calorific values, Theoretical calculation of calorific value; Ignition temperature: spontaneous ignition temperature, Explosive range; Flue gas analysis – ORSAT Method. CO_2 emission and carbon footprint.

Unit V :ENERGY SOURCES AND STORAGE DEVICES

Stability of nucleus: mass defect (problems), binding energy; Nuclear energy: light water nuclear power plant, breeder reactor. Solar energy conversion: Principle, working, and applications of solar cells; Recent developments in solar cell materials. Wind energy; Geothermal energy; Batteries: Types of batteries, Primary battery – dry cell, Secondary battery – NICAD battery, lead acid battery, and lithium-ion battery; Electric vehicles – working principles; Fuel cells: H_2-O_2 fuel cell, microbial fuel cell; Super capacitors: Storage principle, types and examples.

PRACTICAL EXERCISES

1. Determination of hardness of water by EDTA method.
2. Determination of chloride content of water sample by argento metric method.
3. Determination of alkali content of water sample.
4. Determination of strength of given hydrochloric acid using pH meter.
5. Determination of strength of acids in a mixture using conductivity meter.
6. Conductometric titration of strong acid Vs strong base.
7. Estimation of copper by EDTA method.
8. Estimation of iron content by Potentiometry.
9. Determination of molecular weight of polymer using Ostwald viscometer.
10. Conductometric Precipitation titration

SUGGESTED READINGS

1. P. C. Jain and Monica Jain.(2018). Engineering Chemistry, 17th Edition, Dhanpat Rai Publishing Company (P) Ltd, New Delhi.
2. Sivasankar B.(2008). Engineering Chemistry, Tata McGraw-Hill Publishing Company Ltd, New Delhi.
3. S.S. Dara.(2018). A Textbook of Engineering Chemistry, S. Chand Publishing, 12th Edition.
4. Dr. Sayeeda Sultana (2016). Engineering Chemistry, R.K. Publishers, Coimbatore.
5. B. S. Murty, P. Shankar, Baldev Raj, B. B. Rath and James Murday. (2018). Textbook of Nanoscience and Nanotechnology, Universities Press-IIM Series in Metallurgy and Materials Science, .
6. Dr. Sayeeda Sultana, (2016). Practical Engineering Chemistry laboratory manual, R.K. Publishers, Coimbatore, .

Semester – 2

25ECU223 DIGITAL SYSTEM DESIGN 4H – 3C

Instruction Hours / week: L: 2 T: 0 P: 2 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To learn basic techniques for the design of digital circuits and fundamental concepts used in the design of digital systems.
- To understand common forms of number representation in digital electronic circuits and to be able to convert between different representations.
- To implement simple logical operations using combinational logic circuits
- To design combinational logic circuits, sequential logic circuits.
- To impart to student the concepts of sequential circuits, enabling them to analyze sequential systems in terms of state machines
- To implement synchronous state machines using flip-flops.

Course Outcomes (COs)

At the completion of the course the student will be able to

Cos	Course Outcomes	Blooms Level
CO1	Formulate canonical expressions for switching functions.	Understand
CO2	Apply various Boolean function minimization techniques including Karnaugh Map and Quine-McCluskey method to optimize logic circuits	Apply/ Analyze
CO3	Design and implement combinational circuits such as adders, subtractors, multiplexers, encoders, decoders, and code converters using HDL	Apply /create
CO4	Analyze, design, and simulate basic sequential circuits including flip-flops, counters, and shift registers using HDL	Analyze / Create
CO5	Explain the organization and operation of memory devices and apply programmable logic devices for implementing combinational logic.	Understand / Apply

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2
CO 1	**3**	**2**	**1**	**-**	**1**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**1**	**2**	**1**
CO 2	**3**	**3**	**2**	**1**	**1**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**1**	**2**	**2**
CO 3	**3**	**3**	**3**	**2**	**3**	**-**	**-**	**-**	**-**	**1**	**1**	**-**	**1**	**2**	**3**
CO 4	**3**	**2**	**3**	**2**	**2**	**-**	**-**	**-**	**-**	**1**	**1**	**-**	**2**	**1**	**3**

CO 5	**3**	**2**	**2**	**1**	**1**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**2**	**1**	**3**

UNIT I: Number System and Boolean Algebra
Number Systems, Base Conversion Methods, Complements of Numbers, Codes- Binary Codes, Binary Coded Decimal Code and its Properties, Unit Distance Codes, Error Detecting and Correcting Codes. Digital Logic Gates(AND,NAND,OR,NOR,EX-OR,EX-NOR), Properties of XOR Gates, Universal Gates, Basic Theorems and Properties, Switching Functions, Canonical and Standard Form.

UNIT II: Minimization Techniques:
Introduction, The minimization with theorems, The Karnaugh Map Method, Three, Four and Five variable K- Maps, Prime and Essential Implications, Don't Care Map Entries, Using the Maps for Simplifying, Quine-McCluskey Method, Multilevel NAND/NOR realizations

UNIT III: Combinational Circuits:
Design Procedure – Half Adder, Full Adder, Half Subtractor, Full Subtractor, Parallel Binary Adder, Parallel binary subtractor, Binary Multiplier, Multiplexers/De-Multiplexers, decoder, Encoder, Code Converters, Magnitude Comparator.Introduction to HDL — HDL Models of Combinational circuits.

UNIT IV: Sequential Circuits:
Introduction, Basic Architectural Distinctions between Combinational and Sequential circuits, Latches,Flip-Flops, SR,JK,D,T and Master slave, characteristic Tables and equations, Conversion from one type of Flip-Flop to another, Counters - Design of Single Mode Counter, Ripple Counter, Ring Counter, Shift Register, Ring counter using Shift Register - HDL Models of Sequential Circuits

UNIT V: Memory Devices:
Classification of memories – ROM : ROM organization, PROM, EPROM,EEPROM, RAM: RAM organization, Write operation, Read operation, Static RAM , Programmable Logic Devices: Programmable Logic Array(PLA),Programmable Array Logic, Implementation of Combinational Logic circuits using ROM,PLA,PAL

PRACTICAL EXERCISES:
1. Experimental Verification of Logic Gates
2. Design and Experimental verification of Boolean function
3. Design of adders, subtractors& code converters
4. Design of Multiplexers &Demultiplexers.
5. Design of Encoders and Decoders
6. Design of Magnitude Comparators
7. Design and implementation of counters using flip-flops
8. Design and implementation of shift registers.
9. Coding combinational circuits using HDL
10. Coding sequential circuits using HDL

SUGGESTED READINGS

1. Digital Design- Morris Mano, PHI, 3rd Edition.
2. Switching Theory and Logic Design-A. Anand Kumar, PHI, 2nd Edition.
3. Switching and Finite Automata Theory- ZviKohavi & Niraj K. Jha, 3rd Edition, Cambridge.
4. Introduction to Switching Theory and Logic Design – Fredriac J. Hill, Gerald R. Peterson, 3rd Ed, John Wiley & Sons Inc.
5. Digital Fundamentals – A Systems Approach – Thomas L. Floyd, Pearson, 2013.
6. Switching Theory and Logic Design – Bhanu Bhaskara –Tata McGraw Hill Publication, 2012
7. Fundamentals of Logic Design- Charles H. Roth, Cengage Leanring, 5th, Edition, 2004.
8. Digital Logic Applications and Design- John M. Yarbrough, Thomson Publications, 2006.
9. Digital Logic and State Machine Design – Comer, 3rd, Oxford, 2013

Semester-2

25ITU221 OBJECT ORIENTED APPLICATION DEVELOPMENT 4H – 4C

Instruction Hours / week: L: 3 T: 0 P: 2 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

1. Understand and apply the fundamental concepts of object-oriented programming including classes, objects, encapsulation, inheritance, polymorphism, and abstraction.
2. Analyze and implement advanced object-oriented features such as function overloading, operator overloading, templates, and exception handling.
3. Design and develop programs using inheritance hierarchies, virtual functions, and abstract classes to solve complex programming problems.
4. Implement Java-based object-oriented solutions utilizing packages, interfaces, multithreading, and string handling mechanisms.
5. Develop interactive applications with graphical user interfaces using JavaFX controls, components, layouts, and event handling techniques.

Course Outcomes (COs)

At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Analyze programming problems and implement object-oriented solutions using classes, objects, and appropriate OOP constructs.	Apply
CO2	Apply inheritance, polymorphism, and exception handling techniques to develop robust applications	Apply
CO3	Implement appropriate Java programming constructs, including packages, interfaces, and multithreading	Understand
CO4	Demonstrate the concepts of exception handling and file management in both C++ and Java.	Apply
CO5	Evaluate and create interactive GUI applications using JavaFX components and eve handling mechanisms.	Apply

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 8	PO 9	PO10	PO11	PSO 1	PSO 2
CO 1	3	2	2	2	3	1	1	1	2	2	1	1	3	3
CO 2	3	3	3	2	3	1	1	2	2	2	2	2	3	3
CO 3	3	3	3	3	3	1	1	2	2	2	2	2	3	3
CO 4	3	3	3	3	3	1	1	2	2	2	2	2	3	3
CO5	3	3	3	3	3	1	1	2	2	2	2	2	3	3

1 - low, 2 - medium, 3 – high

Unit I – FUNDAMENTAL CONCEPTS OF OOP

Object-Oriented Paradigm - Elements of Object Oriented Programming – Structure of C++ program – Classes and Objects - Defining member functions - Passing and returning objects – Array of objects - Inline functions - Constructors - Parameterized Constructors - Constructor Overloading. Copy Constructor, Destructors, Default arguments - new, delete operators - "this" pointer, Friend classes and Friend functions - Function Overloading – Operator Overloading - Generic programming with templates-Function templates - Class templates

Unit II – INHERITANCE, VIRTUAL FUNCTIONS AND EXCEPTION HANDLING

Inheritance - Base class and derived class relationship - Forms of inheritance - Inheritance and member accessibility - constructors in derived class, abstract class, virtual functions, pure virtual function - Files and Streams - Opening and Closing a file- file modes- file pointers and their manipulation, sequential access to a file-random access to a file-Reading and Writing – Exception handling.

Unit III – INHERITANCE, PACKAGES AND INTERFACES IN JAVA

Java Buzzwords – Overview of Java – Programming Structures in Java – Defining classes in Java - Overloading Methods – Objects as Parameters – Returning Objects –Static, Nested and Inner Classes. Types of Inheritance -Super keyword -Method Overriding – Dynamic Method Dispatch –Abstract Classes – final with Inheritance. Packages and Interfaces: Packages – Packages and Member Access –Importing Packages – Interfaces

Unit IV – EXCEPTION HANDLING, MULTITHREADING AND STRING HANDLING

Exception Handling basics – Multiple catch Clauses – Nested try Statements – Java's Built-in Exceptions – User defined Exception. Multithreaded Programming: Java Thread Model–Creating a Thread and Multiple Threads – Priorities – Synchronization – Inter Thread Communication- Suspending –Resuming, and Stopping Threads –Multithreading. Wrappers – Auto boxing - Strings: Basic String class, methods and String Buffer Class.

Unit V – JAVAFX EVENT HANDLING, CONTROLS AND COMPONENTS

JAVAFX Events and Controls: Event Basics – Handling Key and Mouse Events. Controls: Checkbox, ToggleButton – RadioButtons – ListView – ComboBox – ChoiceBox – Text Controls – ScrollPane. Layouts – FlowPane – HBox and VBox – BorderPane – StackPane – GridPane. Menus – Basics – Menu – Menu bars – MenuItem.

PRACTICAL EXERCISES

1. Design a C++ program to define a Student class and manage student records using an array of objects. Read details of n students, compute total and average marks, and display all records along with the topper.

2. Write a C++ program to create a Box class and demonstrate default constructor, parameterized constructor, constructor overloading, copy constructor, and destructor by creating objects in different ways.

3. Develop a C++ program to implement a BankAccount class where objects are passed as function arguments and returned from functions. Provide operations like

deposit, withdrawal, balance display, and merging two accounts into a new account.

4. Write a C++ program to create a Complex class and overload operators to perform addition, subtraction, multiplication, equality checking, and formatted output of complex numbers.

5. Develop a C++ program to demonstrate friend function and friend class by allowing them to access and modify private data members of an Employee class.

6. Write a C++ program using templates to implement (i) a function template for sorting elements of any data type and (ii) a class template for a stack with push, pop, peek, and empty operations. Demonstrate with at least two data types.

7. Create a C++ program to define an abstract base class Shape with a pure virtual function area(). Derive Circle, Rectangle, and Triangle and use base class pointers to compute and display areas using runtime polymorphism.

8. Develop a C++ program using file streams to store and manage student records in a file. Support adding records, displaying all records, searching by roll number, and updating a record using random file access (seekg/seekp).

9. Write a Java program to define an Employee class and compute salary details. Demonstrate method overloading, objects as parameters, returning objects, and use of static members for common organization details.

10. Create a Java application using user-defined packages to organize classes such as Person, Student, and Faculty. Demonstrate method overriding, dynamic method dispatch, and implement an interface (e.g., Payable) in an appropriate class.

11. Develop a Java program that performs bank transactions and demonstrates exception handling using multiple catch blocks and nested try blocks. Create and use a user-defined exception (e.g., InsufficientBalanceException) for invalid withdrawals.

12. Write a Java program to demonstrate multithreading by creating multiple threads and implementing synchronization with inter-thread communication (wait()/notify()). Also include string processing operations and demonstrate wrapper classes with auto-boxing/unboxing.

13. Design a Java program to demonstrate file handling using FileInputStream/FileOutputStream and BufferedReader/BufferedWriter. The program should write employee/student records to a text file, read and display all records, and search a record by a key field (like ID/roll number). Also include exception handling for file-related errors (FileNotFoundException, IOException).

14. Develop a JavaFX application to demonstrate event handling and UI controls. The GUI should include TextField, RadioButton/CheckBox, ComboBox/ListView, and a Button. On button click (and at least one key/mouse event), the program should collect user selections, validate input, and display the result using a Label/Alert.

Use at least one layout manager (GridPane/BorderPane/VBox) for arranging components.

SUGGESTED READINGS

1. Herbert Schildt, "The Complete Reference C++", Tata McGraw Hill, 2017.
2. E. Balagurusamy," Object-oriented programming with C++", Tata McGraw Hill, 2017.
3. Paul Deitel and Harvey Deitel, "C How to Program with an Introduction to C++", Eighth edition, Pearson Education, 2018.
4. Herbert Schildt, "Java: The Complete Reference", 12th Edition (2021), McGraw-Hill Education.
5. Cay S. Horstmann, "Core Java Volume I – Fundamentals", 12th Edition (2022), Oracle Press.
6. Cay S. Horstmann, "Core Java Volume II – Advanced Features", 12th Edition (2022), Oracle Press.

Semester-2

25ITU222 DATA STRUCTURES AND ALGORITHMS 4H – 4C

Instruction Hours / week: L: 3 T: 0 P: 2 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To understand the basic concepts of ADTs
- To design linear data structures–Stacks and Queues
- To understand linear data structure–Linked List
- To understand Tree and Graph structures
- To understand sorting, searching, and hashing algorithms

Course Outcomes (COs)

At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Understand basic concepts of Data structure and algorithms.	Apply
CO2	Understand and implement linear data structures, such as stack and queues.	Apply
CO3	Understand and implement linear data structures-Linked Lists.	Understand
CO4	Understand and implement efficient tree structures and efficient graph algorithms.	Apply
CO5	Understand and implement different Sorting and Searching algorithms.	Apply

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	2	2	3	2	2	2	3	2	3	1	1	2	2
CO2	2	2	3	1	1	2	2	1	2	1	2	2	2	1	2
CO3	1	3	2	2	1	2	2	1	2	2	2	1	1	2	1
CO4	1	3	3	3	2	2	3	1	1	2	1	2	1	3	2
CO5	3	1	2	1	1	3	3	2	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 - high

UNIT I: INTRODUCTION
Basic Terminologies: Elementary Data Organizations, Analysis of an Algorithm, Asymptotic
Notations, Time-Space trade off, Searching: Linear Search and Binary Search Techniques and their complexity analysis.

UNIT II: STACKS AND QUEUES
ADT Stack and its operations, Applications of Stacks: Expression Conversion and evaluation–Corresponding algorithms and complexity analysis. ADT queue, Types of Queues: Simple Queue, Circular Queue, Priority Queue; Operations on each types of Queues: Algorithms and their analysis.

UNIT III: LINKED LISTS
Singly linked lists: Representation in memory, Algorithms of several operations: Traversing, Searching, Insertion, Deletion from linked list; Linked representation of Stack and Queue, Header nodes, Doubly linked list: operations on it and algorithmic analysis; Circular Linked Lists: all operations their algorithms and complexity analysis.

UNIT IV: TREES AND GRAPHS
Trees: Basic Tree Terminologies, Different types of Trees: Binary Tree, General Tree, Threaded Binary Tree, Binary Search Tree, AVLTree; Tree operations on each of the trees and their algorithms with complexity analysis. Applications of Binary Trees, B Tree, B+ Tree: definitions, algorithms and analysis. Graph: Basic Terminologies and Representations, Graph search and travers al algorithms and Complexity analysis.

UNIT V: SORTING AND HASHING
Objective and properties of different Sorting algorithms: Selection Sort, Bubble Sort, Insertion Sort, Quick Sort, Merge Sort, Heap Sort; Performance and Comparison among all the methods, Hashing: Static Hashing Techniques, Collision resolution techniques, Dynamic Hashing techniques.

PRACTICALEXERCISES: Implement all programs in C++

1. Implements imple ADT programs.
2. Implementation of Stack and Queue ADTs
3. Implement List ADT using Arrays
4. Linked list implementations of List
5. Applications of List, Stack and Queue ADTs
6. Implementation of Tree representation and traversal algorithms
7. Implementation of Graph representation and travers al algorithms
8. Implementation of Sorting and Searching algorithms
9. Implementation of single source shortest path algorithm

SUGGESTED READINGS

1. Mark Allen Weiss,“Data Structures and Algorithm Analysis in C++”,Pearson Education,2014.
2. Aho, Hopcroft and Ullman, “Data Structures and Algorithms”, Pearson Education,1983
3. Thomas H.Cormen, Charles E.Leiserson, Ronald L.Rivest, Clifford Stein, “Introduction to Algorithms", Tata Mcgraw Hill,2002.

Semester – 2

25IKS001 INTRODUCTION TO INDIAN KNOWLEDGE SYSTEM 2H – 2C

Instruction Hours / week: L: 2 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To introduce students to the foundational concepts of the Indian Knowledge System (IKS)
- To explore the relevance and applications of IKS in contemporary times.
- To promote interdisciplinary learning through the integration of traditional Indian knowledge and modern education.

Course Outcomes (COs)
At the completion of the course the student will be able to

Cos	Course Outcomes	Blooms Level
CO1	Describe the meaning, scope, and philosophical foundations of IKS	Remembering
CO2	Summarize the features of Indian education, language, and literary contributions	Understanding
CO3	Illustrate traditional Indian scientific and technological advancements	Applying
CO4	Examine the impact of Indian art, aesthetics, and socio-cultural practices	Analyzing
CO5	Evaluate the relevance and application of IKS in contemporary society	Evaluating

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	3	2	2	2	1	1	2	0	0	0	0	2	1	1
CO2	2	3	2	1	2	0	1	0	0	0	0	1	2	1
CO3	2	2	3	2	2	1	2	1	0	0	0	2	1	2
CO4	1	1	2	3	2	2	2	1	0	0	0	1	2	2
CO5	1	1	1	2	3	3	2	2	0	0	0	1	3	3

1 - low, 2 - medium, 3 - high

Unit I: FOUNDATIONS OF INDIAN KNOWLEDGE SYSTEM
Meaning and Scope of IKS-Historical evolution and literary sources: Vedas, Upanishads, Puranas-Philosophical foundations: Darshanas (Nyaya, Vaisheshika, Samkhya, Yoga, Mimamsa, Vedanta)-Interdisciplinary nature of IKS.

Unit II: EDUCATION, LANGUAGE, AND LITERATURE
Traditional education systems: Gurukula, Pathashalas-Higher education: Nalanda, Takshashila-Role of Sanskrit and regi1onal languages-Contributions of Panini, Bhartrihari-Epics and classical literature.

Unit III: SCIENCE AND TECHNOLOGY IN IKS
Mathematics: Sulbasutras, Aryabhata, Bhaskara-Astronomy: Surya Siddhanta-Ayurveda: Tridosha, healing systems-Metallurgy, Vastu Shastra, water management-

Unit IV: INDIAN ART, CULTURE, AND SOCIETY
Music, dance, painting, sculpture-Rasa theory, Natya Shastra-Festivals, rituals, socio-cultural life-Dharma, Purusharthas, social organization.

Unit V: CONTEMPORARY RELEVANCE AND APPLICATIONS OF IKS
IKS in modern education and research-Sustainable practices in agriculture, ecology, lifestyle-Yoga and meditation in wellness-Role of IKS in national identity and global relevance.

SUGGESTED READINGS

1. Kapil Kapoor (Ed.)– Encyclopedia of Hinduism, Rupa Publications, Comprehensive overview of philosophical and literary foundations of IKS.
2. Michel Danino – The Indian Mind: A Cultural and Philosophical Perspective, DK Printworld-Offers insight into Indian civilization's unique philosophical frameworks and relevance today.
3. V. Sivaramakrishnan (Ed.)– Cultural Heritage of India, Ramakrishna Mission Institute of Culture-Multi-volume work covering various aspects of Indian science, arts, literature, and education.
4. Subhash Kak, David Frawley & N.S. Rajaram– In Search of the Cradle of Civilization, Motilal Banarsidass-Discusses early Indian contributions to science, mathematics, and cosmology.
5. Bharatiya Vidya Bhavan Series– History and Culture of Indian P*eople*-A classic multi-volume series offering a deep dive into ancient Indian education, society, arts, and sciences.
6. Debroy, Bibek – The Bhagavad Gita, Upanishads, and the Vedas (Translations)-For primary source reading and understanding scriptural references in IKS.
7. R. Balasubramanian (Ed.) – The Bloomsbury Research Handbook of Indian Epistemology *and Metaphysics*
8. Yoga Sutras of Patanjali (Various commentaries) – for insights into yoga, wellness, and consciousness studies.

Semester – 2

25MEU211 DESIGN THINKING AND INNOVATIONS LAB **4H – 2C**

Instruction Hours / week: L: 0 T: 0 P: 4 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Demonstrate the significance of design thinking and contrast it with traditional problem-solving techniques.
- Manipulate each phase of the design thinking process to solve human-centered problems.
- Equip students with essential tools and techniques for user-centered design, creative idea generation, and rapid prototyping
- Understand innovation types, overcome barriers, analyze success stories, and effectively pitch ideas.
- Build innovative models through ideation and prototyping tools and strategies**.**

Course Outcomes (COs)

At the completion of the course the student will be able to

Cos	Course Outcomes	Blooms Level
CO1	Distinguish between traditional and design thinking approaches through hands-on comparisons.	Understand
CO2	Applythe five phases of design thinking to solve a user-focused problem.	Apply
CO3	Createand use empathy-based design tools to develop human-centric solutions.	Create
CO4	Analyze innovation types, strategies, case studies, and confidently pitch ideas to stakeholders**.**	Analyze
CO5	Develop sustainable, impactful solutions through design thinking and prototyping**.**	Create

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO 1	3	2	1	1	2	2	3	3	3	2	2	3	2	3	2
CO 2	3	3	2	2	3	2	3	2	3	2	3	3	3	3	3
CO 3	3	3	3	2	3	2	2	2	2	1	3	3	3	3	3
CO 4	2	2	2	2	2	2	2	2	3	2	2	2	2	2	2
CO 5	3	2	2	2	2	3	3	3	3	2	3	3	3	3	2

1 - low, 2 - medium, 3 - high

Unit I: INTRODUCTION TO DESIGN THINKING

Definition and importance of design thinking - Comparison with traditional problem-solving approaches - Key principles: Empathy, experimentation, and iteration. Problem Reframing Techniques.

Unit II: PHASES OF DESIGN THINKING

Empathize: Understanding users and their needs - Define: Framing the right problem to solve.Ideate: Generating a wide range of ideas - Prototype: Building representations of ideas - Test: Gathering feedback to refine solutions.

Unit III:TOOLS AND TECHNIQUES

Empathy maps, user personas, journey mapping - Brainstorming, SCAMPER, mind mapping -

Rapid prototyping techniques: sketches, models, digital tools. Rapid idea generation tools for expanding creative thinking.

Unit IV:INNOVATION STRATEGIES

Types of innovation: product, process, business model - Barriers to innovation and how to overcome them - Case studies of successful innovations- Presenting and pitching ideas to stakeholders

Unit V:SUSTAINABLE DESIGN AND PROTOTYPING

Design thinking for sustainability and social Impact. Tangible outcomes in terms of design and prototype development.

SUGGESTED READINGS

1.Jeanne Liedtka, Randy Salzman, Daisy Azer, Experiencing Design: The Innovator's Journey, Columbia Business School Publishing, 2021

2. Arne van Oosterom, Marcel Zwiers, This is Design Thinking. This is Service Design Doing, BIS Publishers, 2020

3.Nigel Cross, Design Thinking: Understanding How Designers Think and Work, Bloomsbury Academic, 2nd Edition, 2022

4.Michael Lewrick, Patrick Link, Larry Leifer, The Design Thinking Toolbox: A Guide to Mastering the Most Popular and Valuable Innovation Methods, Wiley, 2020

5.Robert Curedale, Design Thinking Process and Methods 5th Edition, Design Community College Inc., 2021.

Semester – 2

25MAC201 INDIAN CONSTITUTION AND HUMAN RIGHTS 2H – 2C

Instruction Hours / week: L: 2 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives.

- To create the basic philosophical tenets of Indian Constitution and Human Rights.
- To underline the significance of our Constitution as Fundamental Law of the land and its features.
- To respect human rights, rule of law and democracy.
- To gain In-depth insight into the constitutional, statutory and institutional aspects of human rights protection in India.
- To identify the constitutional provisions dealing with human rights and special legislations dealing with protection of vulnerable and marginalized groups.

Course Outcomes (COs)

At the completion of the course the student will be able to

Cos	Course Outcomes	Blooms Level
CO1	Demonstrate the provisions under the Constitution of India dealing with human rights	Remember
CO2	Display the nature and scope of special legislations dealing with protection of human rights of marginalized and vulnerable sections**.**	Understand
CO3	Apply practically human rights law to specific human rights problems in India	Apply
CO4	Analyze complex human rights problems and apply relevant provisions of human rights law in India to a hypothetical situation/case study**..**	Analyze
CO5	Acquainted with the theoretical knowledge of the underpinnings of the human rights framework in India, its operation and issues associated with its implementation.	Create

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO 1	2	2	1	3	3	3	3	3	3	3	2	3	3	2	2
CO 2	3	3	3	3	3	3	3	3	2	2	3	3	3	2	3
CO 3	3	3	2	2	1	3	3	3	3	3	2	3	3	2	3
CO 4	3	2	3	3	3	2	3	2	3	3	3	1	3	2	3
CO 5	2	3	1	3	2	3	2	3	2	3	3	3	2	1	2

1 - low, 2 - medium, 3 - high

Unit I :THE CONSTITUTION
Definition and Principles of the Constitution – Socio, Economic and Political Conditions in India at the time of Independence – Contents and Amendments to the Constitution.

Unit II : FUNDAMENTAL RIGHTS
Historical Perspectives on Rights in India – Fundamental Rights in India – Provisions in Articles 14 to 32 and its implications on Human Rights – Right against unlawful detention.

Unit III: DUTIES, DIRECTIVE PRINCIPLES AND AFFIRMATIVE ACTIONS
Fundamental Duties of a citizen in India - Directive Principles - Policy and Practices in Reservation – Affirmative Actions: Special Provisions for SCs and STs.

Unit IV: PROTECTION OF WEAKER SECTIONS OF SOCIETY
Constitutional Provisions for the Protection of women and children - Safeguard for the Labours – Minorities – Tribals.

Unit V: ENFORCEMENT MECHANISM AND EVALUATION
Protection of Human Rights Act 1993 – National and State Human Rights Commissions – Role of Judiciary in Human Rights Protection – Critical Appraisal of the Current Status of Human Rights in India – AFSPA.

SUGGESTED READINGS

1. Desai, A.R. (ed.) (1986), Violations of Democratic Rights in India, Bombay: Popular Prakashan.
2. Meghraj Kapurderiya (2013) Indian Philosophical Foundation of Human Rights, New Delhi: R.P. Publications.
3. Mishra, P.K. (2012) Human Rights: Human Rights: Acts, Statues and Constitutional Provisions, Jaipur: Ritu Publications.
4. Satish Chandra (1995) Minorities in National And International Laws, New Delhi: Deep and Deep Publications.

SEMESTER – 3

B.E. / B.Tech. (Common to all Branches) **2025-2026**

Semester – 3

25MAU301 DISCRETE MATHEMATICS WITH PROBABILITY AND STATISTICS 4H – 4C

Instruction Hours / week: L: 3 T: 0 P: 2 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Define and identify the properties under set theory.
- Analyze the concepts of algebraic structure
- Demonstrate the probability the or to solve the problems**.**
- Apply and identify the concepts of testing the hypothesis
- Apply and classify the design of experiments and its applications to solve the problems.

Course Outcomes (COs)

At the completion of the course the student will be able to

Cos	Course Outcomes	Blooms Level
CO1	Apply the knowledge of sets and Logic and do simple problems	Remember
CO2	Get thorough knowledge Algebraic Structure	Understand
CO3	Apply the concept of Probability in real life problems and derive at the solution	Apply
CO4	Identify large sample and small sample test to various test for single mean, double mean and variance.**.**	Analyze
CO5	Classify One-way or Two-way ANNOVA and construct the table, finally solve the problem.	Create

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 8	PO 9	PO1 0	PO1 1	PO 12	PS O1	PS O2	PS O3
CO 1	2	2	1	3	3	3	3	3	3	3	3	2	3	3	2	2
CO 2	3	3	3	3	3	3	3	3	3	2	2	3	3	3	2	3
CO 3	3	3	2	2	1	3	3	3	1	3	3	2	3	3	2	3
CO 4	3	2	3	3	3	2	3	2	2	3	3	3	1	3	2	3
CO 5	2	3	1	3	2	3	2	3	3	2	3	3	3	2	1	2

1 - low, 2 - medium, 3 - high

UNIT I:SETS AND LOGIC

Basic Notations – Sets - Set and Properties - Set laws - The Boolean algebra of sets -The Boolean identities for sets – Propositional Logic – Propositional equivalences – Predicates and Quantifiers.

UNIT II :ALGEBRAIC STRUCTURES

Algebraic systems – Semi groups and monoids - Groups – Subgroups – Homomorphism's –Normal subgroup and Cossets – Lagrange's theorem – Definitions and examples of Rings and Fields.

UNIT III :PROBABILITY

Probability - The axioms of probability - Conditional probability - Baye' stheorem - Discrete and continuous random variables - Moments – Moment generating functions - Binomial, Poisson, Geometric, Uniform, Exponential and Normal distributions.

UNIT IV :TESTING OF HYPOTHESIS

Sampling distributions – Estimation of parameters – Statistical hypothesis - Large sample tests based on Normal distribution for single mean and difference of means – Tests based on t, Chi-square and F distributions for variance.

UNIT V :DESIGN OF EXPERIMENTS

Basic Principles of Design of Experiments - Randomization, Replication, Local Control, Analysis of Variance - One - way and Two-way Classification - Completely Randomized Design and Randomized Block Design.

SUGGESTED READINGS

1. .P.Tremblay. R. Manohar "Discrete Mathematical Structures with applications to Computer Science "Tata Mc-Graw-Hill Publishing company pvt. Ltd. New Delhi, 35thedition, 2008.

2. Veerajan.T, Discrete Mathematics with Graph Theory and Combinatorics", 10^{th} edition, Tata Mc-Graw-Hill Companies, 2010.

3. An Introduction to Probability Theory and Its Applications: By William Feller

4. Probability and statistics for engineers and scientists: By Ronald E. Walpole, Raymond H. Myers, Sharon L. Myers, Keying E. Ye

5. Fundamentals of Statistics by P.R. Vital-2000

Semester– 3

25UHV001 UNIVERSAL HUMAN VALUES 3H – 3C

Instruction Hours / week: L: 3 T: 0 P: 2 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To understand the need, basic guidelines, content, and process of value education
- To develop right understanding and relationship at all levels of living
- To understand harmony in the human being, family, society, and nature
- To relate the holistic understanding with professional ethics
- To apply value-based principles in personal and professional life.

Course Outcomes (COs)

At the completion of the course the student will be able to

Cos	Course Outcomes	Blooms Level
CO1	Demonstrate understanding of the holistic development of a human being.	Remember
CO2	Distinguish between physical needs and the needs of the self.	Understand
CO3	Apply human values in family and societal interactions	Apply
CO4	Analyze nature and existence in terms of mutual harmony and co-existence.	Analyze
CO5	Integrate ethical human conduct in their professional practice	Create

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 8	PO 9	PO1 0	PO1 1	PO 12	PS O1	PS O2	PS O3
CO 1	2	2	1	3	3	3	3	3	3	3	3	2	3	3	2	2
CO 2	3	3	3	3	3	3	3	3	3	2	2	3	3	3	2	3
CO 3	3	3	2	2	1	3	3	3	1	3	3	2	3	3	2	3
CO 4	3	2	3	3	3	2	3	2	2	3	3	3	1	3	2	3
CO 5	2	3	1	3	2	3	2	3	3	2	3	3	3	2	1	2

1 - low, 2 - medium, 3 - high

UNIT I : Introduction to Value Education:
Right Understanding, Relationship and Physical Facility (Holistic Development and the Role of Education) Understanding Value Education, Self-exploration as the Process for Value Education, Continuous Happiness and Prosperity – the Basic Human Aspirations, Happiness and Prosperity – Current Scenario, Method to Fulfil the Basic Human Aspirations.

UNIT II: Harmony in the Human Being
Understanding Human being as the Co-existence of the Self and the Body, Distinguishing between the Needs of the Self and the Body, The Body as an Instrument of the Self, Understanding Harmony in the Self, Harmony of the Self with the Body, Programme to ensure self-regulation and Health.

UNIT III: Harmony in the Family and Society
Harmony in the Family – the Basic Unit of Human Interaction, 'Trust' – the Foundational Value in Relationship, 'Respect' – as the Right Evaluation, Other Feelings, Justice in Human-to-Human Relationship, Understanding Harmony in the Society, Vision for the Universal Human Order.

UNIT IV: Trees and Graphs
Understanding Harmony in the Nature, Interconnectedness, self-regulation and Mutual Fulfilment among the Four Orders of Nature, Realizing Existence as Co-existence at All Levels, The Holistic Perception of Harmony in Existence.

UNIT V: Implications of the Holistic Understanding - a Look at Professional Ethics
Natural Acceptance of Human Values, Definitiveness of (Ethical) Human Conduct, A Basis for Humanistic Education, Humanistic Constitution and Universal Human Order, Competence in Professional Ethics Holistic Technologies, Production Systems and Management Models-Typical Case Studies, Strategies for Transition towards Value-based Life and Profession

SUGGESTED READINGS

1. Gaur, R.R., Sangal, R., & Bagaria, G.P., A Foundation Course in Human Values and Professional Ethics, Publisher: Excel Books, New Delhi, 2022.
2. Sharma, S. B., Education for Values, Environment and Human Rights, Publisher: Lotus Press, New Delhi, 2022
3. Pathania, A. , Value Education: Perspectives and Practices, Pearson Education India, 2023
4. The Textbook A Foundation Course in Human Values and Professional Ethics, R R Gaur, R Asthana, G P Bagaria, 2nd Revised Edition, Excel Books, New Delhi, 2019. ISBN 978-93-87034- 47-1

Semester – 3

25CYU321 FUNDAMENTALS OF OPERATING SYSTEMS 4H – 4C

Instruction Hours / week: L: 3 T: 0 P: 2 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To understand the basic concepts of major operating system components and its design principles.
- To provide an in-depth exposure to process management.
- To understand various memory management techniques.
- To understand storage management concepts
- To be familiar with the basics of virtual machines and Mobile OS.

Course Outcomes (COs)

At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Analyze various scheduling algorithms and process synchronization	Apply
CO2	Explain deadlock prevention and avoidance algorithms	Apply
CO3	Compare and contrast various memory management schemes	Understand
CO4	Explain the functionality of filesystems, I/Osystems, and Virtualization	Apply
CO5	To compare Ios and Android Operating systems	Apply

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	2	2	3	2	2	2	3	2	3	1	1	2	2
CO2	2	2	3	1	1	2	2	1	2	1	1	2	2	1	1
CO3	1	3	2	2	1	2	2	1	2	2	1	1	1	2	1
CO4	1	3	3	3	2	2	3	1	1	2	1	2	1	3	2
CO5	3	1	2	1	1	3	3	2	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 - high

UNIT I: INTRODUCTION

Computer-SystemOrganization,Computer-SystemArchitecture,Operating-SystemStructure,Operating- System Operations, Operating-System Services. User and Operating- System Interface, System Calls, Types of System Calls, System Programs.

UNIT II: PROCESS MANAGEMENT

Process Concept, Process Scheduling, Operations on Processes, Inter-process communication, Multicore Programming, Multithreading Models. Scheduling: Basic Concepts, Scheduling Criteria, Scheduling Algorithms. The Critical-Section Problem, Peterson's Solution, Semaphores, Classic Problems of Synchronization. Deadlock :Deadlock Characterization, Methods for Handling Deadlocks, Deadlock Prevention, Deadlock Avoidance, Deadlock Detection.

UNIT III: MEMORY MANAGEMENT

Swapping, Contiguous Memory Allocation. Segmentation, Paging, Structure of the Page Table Demand Paging, Page Replacement, Allocation of Frames, Thrashing.

UNIT IV: STORAGE MANAGEMENT

File Concept, Access Methods, File-System Mounting, File-System Structure, File-System Implementation, Directory Implementation, Allocation Methods. Disk Structure, Disk Attachment, Disk Scheduling. I/O Hardware:I/Odevices,Devicecontrollers,DirectmemoryaccessPrinciplesofI/OSoftware:GoalsofInterrupt handlers, Device drivers, Device independent I/O software.

UNIT V: VIRTUAL MACHINES AND MOBILE O.S

Virtual Machines–History, Benefits and Features, Building Blocks, Types of Virtual Machines and their Implementations, Virtualization and Operating-System Components; Mobile OS - iOS and Android.

PRACTICAL EXERCISES:

1. Installation of windows operating system
2. Illustrate UNIX commands and Shell Programming
3. Process Management using System Calls : Fork, Exit, Getpid, Wait, Close
4. Write C programs to implement the various CPU Scheduling Algorithms
5. Illustrate the inter process communication strategy
6. Implement mutual exclusion by Semaphore
7. Write C programs to avoid Deadlock using Banker's Algorithm
8. Write a C program to Implement Deadlock Detection Algorithm
9. Write C program to implement Threading
10. Implement the paging Technique using C program
11. Write C programs to implement the following Memory Allocation Methods
a. First Fit b. Worst Fit c. Best Fit
12. Write C programs to implement the various Page Replacement Algorithms
13. Write C programs to Implement the various File Organization Techniques
14. Implement the following File Allocation Strategies using C programs
a. Sequential b. Indexed c. Linked
15. Write C programs for the implementation of various disk scheduling algorithms

SUGGESTED READING

1.AbrahamSilberschatz,PeterBaerGalvinandGregGagne,“OperatingSystemConcepts”, 10th Edition, John Wiley and Sons Inc., 2018.

2. AndrewSTanenbaum,"ModernOperatingSystems",Pearson,5thEdition,2022NewDelhi.

3. Ramaz Elmasri,A. Gil Carrick, David Levine,“ Operating Systems A Spiral Approach” Tata McGraw Hill Edition,2010

4.WilliamStallings,"OperatingSystems:InternalsandDesignPrinciples",7thEdition, Prentice Hall, 2018.

5. AchyutS.Godbole,AtulKahate,“OperatingSystems”,McGrawHillEducation,2016

25CYU301 **CYBER SECURITY ESSENTIAL** **Semester – 3**
4H – 3C

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To understand various types of cyber-attacks and cyber-crimes
- To learn threats and risks within context of the cyber security
- To have an overview of the cyber laws & concepts of cyber forensics
- To study the defensive techniques against these attacks
- To understand various cyber security privacy issues

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Analyze and interpret the concept of different attacks	Apply
CO2	Analyze and Implement Cyber Security Regulations and Roles of International Law	Apply
CO3	Implement the attacks on Mobile and Wireless devices	Understand
CO4	Analyze organizational implications of Cybersecurity	Apply
CO5	Design and analyze concepts of data privacy attacks	Apply

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO 1	3	1	2	2	3	2	2	2	3	2	3	1	1	2	2
CO 2	2	2	3	1	1	2	2	1	2	1	2	2	2	1	2
CO 3	1	3	2	2	1	2	2	1	2	2	2	1	1	2	1
CO 4	1	3	3	3	2	2	3	1	1	2	1	2	1	3	2
CO 5	3	1	2	1	1	3	3	2	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 - high

UNIT I: INTRODUCTION TO CYBER SECURITY

Basic Cyber Security Concepts, layers of security, Vulnerability, threat, Harmful acts, Internet Governance – Challenges and Constraints, Computer Criminals, CIA Triad, Assets and Threat, motive of attackers, active attacks, passive attacks, Software attacks, hardware attacks, Cyber Threats-Cyber Warfare, Cyber Crime, Cyber terrorism, Cyber Espionage, etc., Comprehensive Cyber Security Policy.

UNIT II: CYBER SPACE AND THE LAW & CYBERFORENSICS

Introduction, Cyber Security Regulations, Roles of International Law. The INDIAN Cyberspace, National Cyber Security Policy. Historical background of Cyber forensics, Digital Forensics Science, The Need for Computer Forensics, Cyber Forensics and Digital evidence, Forensics Analysis of Email, Digital Forensics Lifecycle, Forensics Investigation, Challenges in Computer Forensics.

UNIT III: CYBERCRIME - MOBILE AND WIRELESS DEVICES

Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication service Security, Attacks on Mobile/Cell Phones, Organizational security Policies and Measures in Mobile Computing Era, Laptops

UNIT IV: CYBER SECURITY- ORGANIZATIONAL IMPLICATIONS

Introduction, cost of cybercrimes and IPR issues, web threats for organizations, security and privacy implications, social media marketing: security risks and perils for organizations, social computing and the associated challenges for Organizations.

UNIT V: PRIVACY ISSUES

Basic Data Privacy Concepts: Fundamental Concepts, Data Privacy Attacks, Data linking and profiling, privacy policies and their specifications, privacy policy languages, privacy in different domains- medical, financial, etc

SUGGESTED READINGS

1.Nina Godbole and Sunit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal
Perspectives, Wiley
2.B.B. Gupta, D.P. Agrawal, Haoxiang Wang, Computer and Cyber Security: Principles, Algorithm, Applications, and
Perspectives, CRC Press, ISBN 9780815371335,2018.
3. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press
4. Introduction to Cyber Security, Chwan-Hwa (john) Wu,J. David Irwin, CRC Press T&F Group.

Semester – 3

25CYU322 COMPUTER NETWORKING ESSENTIALS 4H – 4C

Instruction Hours / week: L: 3 T: 0 P: 2 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- The main objectives of this course are to
- To understand the concept of layering in networks
- To know the functions of protocols of each layer of TCP/IP protocol suite.
- To visualize the end-to-end flow of information.
- To understand the components required to build different types of networks
- To learn concepts related to network addressing and routing

Course Outcomes (COs)

At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Identify the appropriate application layer and transport layer protocols required to implement various network applications.	Apply
CO2	Identify better routes by applying appropriate intra AS protocols and inter AS protocols	Apply
CO3	Apply effective address management techniques and configure IPv6 protocols	Understand
CO4	elect the appropriate LAN technology and MAC layer protocols	Apply
CO5	elect the type of medium and frequency range for data transmission	Apply

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	2	2	2	2	2	1	3	2	3	1	1	2	2
CO2	2	2	3	1	1	2	1	1	2	1	1	2	2	1	2
CO3	2	3	2	2	1	2	1	1	2	2	1	1	1	2	2
CO4	2	3	3	3	2	3	1	1	1	2	1	2	1	3	2
CO5	3	1	2	1	1	2	1	1	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 - high

UNIT I: INTRODUCTION AND APPLICATION LAYER

Data Communication - Building networks – Network Edge, Access and Core – Layered Architecture – OSI Model – Internet Architecture (TCP/IP) Networking Devices: Hubs, Bridges, Switches, Routers, and Gateways – Top-down Approach – Application layer - Sockets – Application Layer protocols – HTTP – FTP Email Protocols – DNS.

UNIT II: TRANSPORT LAYER

Transport Layer functions – End to end semantics – Multiplexing and Demultiplexing – User Datagram Protocol – UDP Applications – Transmission Control Protocol – Connection establishment and release – Flow Control – Retransmission Strategies – Congestion Control – Quality of Service

UNIT III: NETWORK LAYER

Network Layer: Switching concepts – Packet switching - Routing – Distance Vector and Link State Algorithms – Routing Information Protocol, Open Shortest Path First and Broder Gateway Protocol – Congestion Control mechanisms in Routers – Software Defined Networks – Control Plane and Data Plane.

UNIT IV: IP ADDRESSING

IPV4 Packet Format and Addressing – Subnetting – Classless Inter-Domain Routing – Variable Length Subnet Mask – Dynamic Host Configuration Protocol – Network Address Translation – Internet Control Message Protocol – Need for IPv6 – Addressing methods and types in IPv6 – IPv6 header – Transition from IPv4 to IPv6.

UNIT V: DATA LINK AND PHYSICAL LAYERS

Data Link Layer – Framing – Flow control – Error control – Media Access Control – Ethernet Basics – Carrier Sense Multiple Access / Collision Detection – Virtual LAN – Wireless LAN - 802.11 variants – MAC Layer – CSMA/CA - Physical layer – Signals – Bandwidth and Data Rate – Encoding – Multiplexing – Shift Keying – Transmission Media.

PRACTICALEXERCISES:

1. Learn to use commands like tcpdump, netstat, ifconfig, nslookup and traceroute. Capture ping and trace route PDUs using a network protocol analyzer and examine.

2. Write a HTTP web client program to download a webpage using TCP sockets

3. Applications using TCP sockets like :a) Echo client and echo server b)Chat

4. Simulation of DNS using UDP sockets.

5. Use a tool like Wire shark to capture packet sand examine the packets

6. Write a code simulating ARP/RARP protocols.

7. Study of Network simulator(NS)and Simulation of Congestion Control Algorithms using NS.

8. Study of TCP/UDP performance using Simulation tool.

9. Simulation of Distance Vector/Link State Routing algorithm.

10. Simulation of an error correction code (like CRC).

SUGGESTED READINGS

1.James F. Kurose, Keith W. Ross, “Computer Networking: A Top-Down and Approach”, Eighth Edition, Pearson Education, 2022.
2.Larry L. Peterson, Bruce S. Davie, “Computer Networks: A Systems Approach”, Sixth Edition, Morgan Kaufmann Publishers Inc., 2022.
3.William Stallings, “Data and Computer Communications”, Tenth Edition, Pearson Education, 2017.
4.Ying-Dar Lin, Ren-Hung Hwang, Fred Baker, “Computer Networks: An Open-Source Approach”, McGraw Hill, 2012
5.Andrew S Tanenbaum, Nick Feamster and David J Wether all, “Computer Networks”, Sixth Edition, Pearson Education, 2022

Semester – 3

25ITU323 DESIGN AND ANALYSIS OF ALGORITHMS 4H – 4C

Instruction Hours / week: L: 3 T: 0 P: 2 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To learn about the process of problem solving
- To be conversant with algorithms for common problems
- To analyse the algorithms for time/space complexity
- To learn to write algorithms for a given problem using different design paradigms.
- To understand computational complexity of problems

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Analyze algorithms based on time and space complexity	Apply
CO2	Design efficient Divide and conquer and its variants for solving problems.	Apply
CO3	Apply greedy methods and dynamic programming strategies for solving real- world problems	Understand
CO4	Design and implement Linear programming, backtracking, and branch and bound techniques towards efficient problem-solving.	Apply
CO5	Understand the computational theory and the methods to prove NP-complete problems	Apply

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO 1	3	1	2	2	2	2	2	1	3	2	3	1	1	2	1
CO 2	2	2	3	1	1	2	1	1	2	1	1	2	2	1	1
CO 3	2	3	2	2	1	2	1	1	2	2	1	1	1	2	2
CO 4	2	3	3	3	2	3	1	1	1	2	1	2	1	3	2
CO 5	3	1	2	1	1	2	1	1	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 - high

UNIT I: FUNDAMENTALS

The Role of Algorithms in Computing – Designing Algorithms – Algorithmic Thinking – Fundamental stages of Problem-solving - Analyzing Algorithms – Iterative Algorithms - Step Count and Operation Count— measuring of Input size, Measuring Run time – Best, worst and average case complexity – Rate of growth - Recursive Algorithms: Formulation and solving recurrence equations – Guess and Verify method – Substitution method - Asymptotic analysis – asymptotic Notations – Asymptotic complexity classes.

UNIT II : DIVIDE AND CONQUER AND ITS VARIANTS

Introduction to Divide and Conquer - Merge Sort – Quicksort - Long Integer Multiplication – Divide and Conquer recurrences - Recursion Tree Method – Master Theorem –- Transform and Conquer Approach: Gaussian Elimination Method – LU and LUP Decomposition – Solving set of equations using LUP – Matrix Inverse and Determinant using LUP approach - Decrease and Conquer Paradigm - Binary Search and Insertion Sort.

UNIT III: GREEDY ALGORITHMS AND DYNAMIC PROGRAMMING APPROACH

Greedy Strategy—Generic Greedy Algorithm—Activity Selection—Fractional Knapsack—Dynamic Programming—Elements of Dynamic Programming—Principle of Optimizity—Computing Binominal Coefficient—Matrix Chain Multiplication—Longest Common Subsequence—String Edit—Solving Knapsack problem using dynamic programming approach.

UNIT IV: INCREMENTAL APPROACH, BACKTRACKING AND BRANCH & BOUND

Linear Programming: Formulation of LPPs – Iterative development – Applications of Linear Programming - Standard form – Simple solution using Graph techniques - Simplex Algorithm – Maximization and Minimization of problems - Duality - Backtracking: Basics of Backtracking- 8-queen - Sum of Subsets, Branch and Bound: Least cost with Branch and Bound - 0/1 Knapsack.

UNIT V: COMPUTATIONAL COMPLEXITY

Understanding of Computational Complexity – Solvability - Tractability - Decision Problems - Decidability - NP-Hard – NP-Completeness – Reducibility Satisfiability Problem and Cook's Theorem - NP-Completeness Proofs for problems like SAT - 3CNF - Clique – Overview of Randomized Algorithm – Randomized Quicksort – Overview of approximation algorithm – set cover.

PRACTICAL EXERCISES:

1. Design of simple problems, sample problems in Hackerrank, like, diagonal difference in matrices. Computation of step count and operation count for merge sort and Quicksort. Implementation of time complexity in Python .

2. Design and implement Merge sort, Quick sort, Insertion sort and Binary search algorithms.

3. Design and implement solution using dynamic programming for knapsack problem.
4. Implementation of matrix inverse using Gaussian Elimination problem

5. Design and Implement solution for 8 queens problem.

6. Design and Implementation of Simplex algorithm.

7. Design and Implementation of approximation algorithm for set cover problem

SUGGESTED READINGS

1. Thomas H Cormen, Charles E Leiserson, Ronald L Revest, Clifford Stein, “Introduction to Algorithms” 4th Edition, The MIT Press Cambridge, Massachusetts London, England, 2022.
2. S.Sridhar, “Design and Analysis of Algorithms”, Second Edition, Oxford University Press, 2024.
3. Antany Levitin, “Introduction to the Design and Analysis of Algorithms”, Third Edition, Pearson Education, 2012.
4.Steven S. Skiena, “The Algorithm Design Manual”, Second Edition, Springer, 2010.
5. Robert Sedgewick, Kevin Wayne, “Algorithms”, Fourth Edition, Pearson Education, 2011.

Semester-3

25CYU302 WEB APPLICATION SECURITY **4H – 3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To understand the fundamentals of web application security
- To focus on wide aspects of secure development and deployment of web applications
- To learn how to build secure APIs
- To learn the basics of vulnerability assessment and penetration testing
- To get an insight about Hacking techniques and Tools

Course Outcomes (COs)

At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Understanding the basic concepts of web application security and the need for it	Apply
CO2	Be acquainted with the process for secure development and deployment of web applications	Apply
CO3	quire the skill to design and develop Secure Web Applications that use Secure APIs	Understand
CO4	Be able to get the importance of carrying out vulnerability assessment and penetration testing	Apply
CO5	quire the skill to think like a hacker and to use hackers tool sets	Apply

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO 1	3	1	2	2	3	2	2	2	3	2	3	1	1	2	2
CO 2	2	2	3	1	1	2	2	1	2	1	2	2	2	1	2
CO 3	1	3	2	2	1	2	2	1	2	2	2	1	1	2	1
CO 4	1	3	3	3	2	2	3	1	1	2	1	2	1	3	2
CO 5	3	1	2	1	1	3	3	2	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 – high

UNIT I :FUNDAMENTALS OF WEB APPLICATION SECURITY

The history of Software Security-Recognizing Web Application Security Threats, Web Application Security, Authentication and Authorization, Secure Socket layer, Transport layer Security, Session Management-Input Validation.

UNIT II :SECURE DEVELOPMENT AND DEPLOYMENT

Web Applications Security - Security Testing, Security Incident Response Planning,The Microsoft Security Development Lifecycle (SDL), OWASP Comprehensive Lightweight Application Security Process (CLASP), The Software Assurance Maturity Model (SAMM).

UNIT III :SECURE API DEVELOPMENT

API Security- Session Cookies, Token Based Authentication, Securing Natter APIs: Addressing threats with Security Controls, Rate Limiting for Availability, Encryption, Audit logging, Securing service-to-service APIs: API Keys , OAuth2, Securing Microservice APIs: Service Mesh, Locking Down Network Connections, Securing Incoming Requests.

UNIT IV :VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Vulnerability Assessment Lifecycle, Vulnerability Assessment Tools: Cloud-based vulnerability scanners, Host-based vulnerability scanners, Network-based vulnerability scanners, Database-based vulnerability scanners, Types of Penetration Tests: External Testing, Web Application Testing, Internal Penetration Testing, SSID or Wireless Testing, Mobile Application Testing.

UNIT V :HACKING TECHNIQUES AND TOOLS

Social Engineering, Injection, Cross-Site Scripting(XSS), Broken Authentication and Session Management, Cross-Site Request Forgery, Security Misconfiguration, Insecure Cryptographic Storage, Failure to Restrict URL Access, Tools: Comodo, OpenVAS, Nexpose, Nikto, Burp Suite, etc

SUGGESTED READINGS

1. Andrew Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications, First Edition, 2020, O'Reilly Media, Inc.
2. Bryan Sullivan, Vincent Liu, Web Application Security: A Beginners Guide, 2012, The McGraw-Hill Companies.
3. Neil Madden, API Security in Action, 2020, Manning Publications Co., NY, USA.
4. Michael Cross, Developer's Guide to Web Application Security, 2007, Syngress Publishing, Inc.
5. Ravi Das and Greg Johnson, Testing and Securing Web Applications, 2021, Taylor & Francis Group, LLC.
6. Prabath Siriwardena, Advanced API Security, 2020, Apress Media LLC, USA.
7. Malcom McDonald, Web Security for Developers, 2020, No Starch Press, Inc.
8. Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams Grey Hat Hacking: The Ethical Hacker's Handbook, Third Edition, 2011, The McGraw-Hill Companies.

B.E. / B.Tech. (Common to all Branches) **2025-2026**

Semester-3

25MAC311 **YOGA** **4H – 3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Articulate and Focus on goal sand move away from demotivating and corrosive environment.
- Explain the concept and dimensions of wellness which help in pursuing their goals
- Demonstrate the practices that can promote wellness.
- Plan and follow a daily routine that includes Physical Exercises, Yoga, and Meditation.
- Demonstrate behavior's aligned to universal HumanValues.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Articulate and Focus on goals and move away from demotivating and corrosive environment	Apply
CO2	Explain the concept and dimensions of wellness which help in pursuing their goals.	Apply
CO3	monstrate the practices that can promote wellness	Understand
CO4	Plan and follow a daily routine that includes Physical Exercises, Yoga, and Meditation	Apply
CO5	Demonstrate behaviours aligned to universal Human Values.	Apply

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	2	2	3	2	2	2	3	2	3	1	1	2	2
CO2	2	2	3	1	1	2	2	1	2	1	2	2	2	1	2
CO3	1	3	2	2	1	2	2	1	2	2	2	1	1	2	1
CO4	1	3	3	3	2	2	3	1	1	2	1	2	1	3	2
CO5	3	1	2	1	1	3	3	2	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 – high

UNIT I : PHYSICAL HEALTH

Introduction to SKY -Education as a means of Youth Empowerment-Simplified Physical exercises-Yogasanas(Rules-SunSalutation-Dandasana-Chakrasana-Vrichasana-Trikonasana-Vajrasana-Pranayama-NadiSuddhi-ClearancePractice).

UNIT II : STRENGTHENING THE LIFE FORCE

Reasons for Diseases-Philosophy of Kaya Kalpa -Maintaining Youthfulness & Postponing Aging –Transformation of Food in to seven Body Constituents-Greatness of Seminal Fluid-Limit and Method in Five Factors- Kaya Kalpa Practice.

UNIT III : WELLNESS OF MIND

Classification of Mind Waves-Agna Meditation-Shanthi Meditation-Thuriya Meditation-Blessing and Benefits-Virtues: Individual Virtues and Societal Virtues -Morals (Importance of Introspection, Six Temperaments and Mano evering, Benefits of Meditation).

UNT IV : PROSPERITY B OF MIND-PARTI

Philosophy of Life (Purpose of Life,Philosophy of Life, Five Duties-Safe guarding Natural Resources)-Analysis of Thoughts (Ten stages of the Mind-The Five Kosas-Thoughts-Analysis of thoughts and practice)- Moralisation of Desires(Desires-Explanation, Nature, Reasons, Moralisation Practice).

UNIT V: PROSPERITY OF MIND-PARTII

Neutralisation of Anger (Anger-Reasons, Effects, Peace, Tolerance and Forgiving, Neutralisation) –Eradication of Worries(Reasons,Effects,Correctivemeasures,Eradication)-DiversityinMen-LoveandCompassion **.**

SEMESTER – 4

B.E. / B.Tech. (Common to all Branches) **2025-2026**

Semester-4

25CYU421 CLOUD NETWORK AND SECURITY 4H – 4C

Instruction Hours / week: L: 3 T: 0 P: 2 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To understand basics of cloud computing and security.
- To understand secure cloud architecture
- To understand cloud compliance requirements and Trusted cloud security
- To gain knowledge on how to recover from disaster in cloud security
- To gain knowledge on advanced cloud security architecture.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Explain the concepts of cloud computing and cloud security	Remember
CO2	Analyze and secure the cloud infrastructure	Analyze
CO3	Analyze and implement cloud compliance requirements	Analyze
CO4	Implement recovery strategies during disaster	Apply
CO5	Analyze and Implement strategies to overcome cyber attacks on the cloud network.	Analyze

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	2	2	2	2	2	1	3	2	3	1	1	2	1
CO2	2	2	3	1	1	2	1	1	2	1	1	2	2	1	1
CO3	2	3	2	2	1	2	1	1	2	2	1	1	1	2	2
CO4	2	3	3	3	2	3	1	1	1	2	1	2	1	3	2
CO5	3	1	2	1	1	2	1	1	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 – high

UNIT I :INTRODUCTION TO CLOUD COMPUTING AND RISK MANAGEMENT

Cloud Computing Essentials, Overview of Cloud Computing, Cloud Security Baselines, Cloud Security,
Privacy, and Trust Baselines, Infrastructure as a Service (IaaS), Risk and Trust Assessment: Schemes for
Cloud Services, Cloud Security Risk Management, Secure Cloud Risk Management: Risk Mitigation Methods

UNIT II :SECURING THE CLOUD INFRASTUCTURE

Specification and Enforcement of Access Policies in Emerging Scenarios, Cryptographic Key Management for Data Protection, Cloud Security Access Control: Distributed Access Control, Cloud User Controls, Cloud Computing Security Essentials and Architecture, Cloud Computing Architecture and Security Concepts, Secure Cloud Architecture**.**

UNIT III :CLOUD COMPLIANCE REQUIREMENTS

Negotiating Cloud Security Requirements with Vendors, Managing Legal Compliance Risk in the Cloud and Negotiating Personal Data Protection Requirements with Vendors, Integrity Assurance for Data Outsourcing, Secure Computation Outsourcing, Computation Over Encrypted Data, Trusted Computing Technology, Computing Technology for Trusted Cloud Security.

UNIT IV :PREPARING FOR DISASTER RECOVERY

Simplifying Secure Cloud Computing Environments with Cloud Data Centers, Availability, Recovery, and Auditing across Data Centers**.**

UNIT V :ADVANCED CLOUD COMPUTING SECURITY

Advanced Security Architectures for Cloud Computing, Side-Channel Attacks and Defences on Cloud Traffic, Future Directions in Cloud Computing Security: Risks and Challenges

PRACTICAL EXERCISES:

1. Simulate a cloud scenario using Cloud Sim and run a scheduling algorithm not present in Cloud Sim
2. Simulate resource management using cloud sim
3. Simulate log forensics using cloud sim
4. Simulate a secure file sharing using a cloud sim
5. Implement data anonymization techniques over the simple dataset (masking, k-anonymization, etc)
6. Implement any encryption algorithm to protect the images
7. Implement any image obfuscation mechanism
8. Implement a role-based access control mechanism in a specific scenario
9. Implement an attribute-based access control mechanism based on a particular scenario
10. Develop a log monitoring system with incident management in the cloud

SUGGESTED READINGS

1**.** Cloud Computing Security, John R. Vacca, September 2016, CRC Press
2. Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Ronald L. Krutz and Russell Dean Vines, 2010, MISL-WILEY series
3.Cloud Security Concepts, Applications and Perspectives, Brij B.Gupta, 2021, CRC Press
4. Cloud Security For Dummies: Hone Your Vision, Shift Your Energy, Make Your Move,2022

25CYU401 **SECURITY AUDIT AND RISK ASSESSMENT** **Semester-4**
4H – 3C

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Outline the fundamentals of security audit components and process
- Illustrate various security audit phases and methods to audit the resources
- Outline the process of data collection for security risk assessment
- Explain how the collected risky data are analyzed to find the final risk score
- Introduce the concepts of risk assessment methodology

Course Outcomes (COs)

At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	describe the concepts of Security audit components and process	Remember
CO2	apply the various security audit phases and methods to audit the resources	Apply
CO3	demonstrate the process of data collection for security risk assessment	Analyze
CO4	evaluate the risk score using risk data analysis techniques	Apply
CO5	assess the risk with different risk assessment methodology	Analyze

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3	2	2	2	2	2	1	3	2	3	1	1	2	2
CO2	2	2	3	1	1	2	1	1	2	1	1	2	2	1	2
CO3	3	3	2	2	1	2	1	1	2	2	1	1	1	2	2
CO4	2	3	3	3	2	3	1	1	1	2	1	2	1	3	1
CO5	3	3	2	1	1	2	1	1	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 – high

UNIT I :BASICS OF INFORMATION SECURITY

Security Metrics and Reporting, Common Issues and Variances of Performance Metrics, Introduction to Security Audit, Need, Steps in Security Audit. Auditable resources in an organization, Servers and Storage devices, Infrastructure and Networks, Communication Routes, Lab1: Working with Trojans, Backdoors and sniffer for monitoring network communication System, Information Security Methodologies (Black-box, White-box, Grey-box), Phases of Information Security Audit and Strategies, Ethics of an Information Security Auditor.Lab2: Understanding Data Packet Sniffers, Security Audit Part I- Auditing PC-based Accounting System, Auditing Operating Systems, Auditing Networks, Auditing Electronic Data Interchange, Controlling and auditing Database Management Systems. Lab 3: Windows Hacking – NT LAN Manager, Secure password recovery.

UNIT II :SECURITY AUDIT

Pre-audit checklist, Information Gathering, Vulnerability Analysis, Lab 1: UDP Scan Using nmap, TCP Connect Scan Using nmap, TCP SYN Scan Using nmap External Security Audit, Internal Network Security Audit, Firewall Security Audit, Lab 2: Vulnerability Identification and Prioritization, IDS Security Auditing, Social Engineering Security Auditing, Web Application Security Auditing, Information Security Audit Deliverables& Writing Report, Result Analysis, Post Auditing Actions, Report Retention etc. Lab 3: Web Application Security Configuration.

UNIT III :FUNDAMENTALS OF RISK

What is Risk? –Information Security Risk Assessment Overview Drivers, Laws, and Regulations-Risk Assessment Framework – Lab1: Risk assessment with NIST framework. Phases of Security Risk Assessment, Data Collection: The Sponsors- The Project Team- Data Collection Mechanisms, Executive Interviews- Document Requests- IT Assets Inventories, Lab2: Data Collection using Container method, Profile & Control Survey-Consolidation, Lab3: Survey Consolidation of the collected data.

UNIT IV :RISK ANALYSIS

Compiling Observations-Data Analysis: Preparation of catalogues- Lab1: Prepare an automated Threat-vulnerability pair matrix, System Risk Computation, Designing Impact Analysis Scheme-Confidentiality, Integrity and Availability, Impact Score, Lab2: Preparation of an automated impact score, designing control analysis, Designing Likelihood Analysis: Exposure, Frequency, Controls, Computing Final Risk Score, Lab3:Preparation of an automated Likelihood score and final risk score.

UNIT V :RISK CLASSIFICATION AND PRIORITIZATION

Stem Risk Analysis-Risk Classification, Risk Ranking, Individual Risk Reviews, and Prepare the Risk Analysis with individual system risk review and threat and vulnerability risk review, Organization risk Analysis, Risk Prioritization- Organization and System Specific Risk prioritization and Treatment, Prepare an automated Organization and system specific risk prioritization and treatment template. Risk Assessment Methodologies- Result- Risk Registers-Process summary-post mortem. Prepare the risk register.

SUGGESTED READINGS

1. Mark Talabis, “Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis”, Syngress; 1 edition, ISBN: 978-1-59749-735-0, 2013.
2. Whitman, Michael E., and Herbert J. Mattord. Management of information security. Cengage Learning, 2013
3**.**Andrew Vladimirov Michajlowski, Konstantin, Andrew A. Vladimirov, and Konstantin V. Gavrilenko Assessing information security: strategies, tactics, logic, and framework. IT’S Governance Ltd, 2010.
4**.** https://www.sans.org/reading-room/whitepapers/threats/implementing-vulnerability-managementprocess-34180

25CYU411 **SECURE SOFTWARE ENGINEERING** **Semester-4**
4H – 3C

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Know the importance and need for software security.
- Know about various attacks.
- Learn about secure software design.
- Understand risk management in secure software development.
- Know the working of tools related to software security

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Identify various vulnerabilities related to memory attacks	Remember
CO2	Apply security principles in software development	Apply
CO3	Evaluate the extent of risks.	Analyze
CO4	Involve selection of testing techniques related to software security in the testing phase of software development.	Apply
CO5	Use tools for securing software	Analyze

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO 1	3	1	2	2	2	2	2	1	3	2	3	1	1	2	2
CO 2	2	2	3	1	1	2	1	1	2	1	1	2	2	1	2
CO 3	2	3	2	2	1	2	1	1	2	2	1	1	1	2	2
CO 4	2	3	3	3	2	3	1	1	1	2	1	2	1	3	2
CO 5	3	1	2	1	1	2	1	1	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 – high

UNIT I:NEED OF SOFTWARE SECURITY AND LOW-LEVEL ATTACKS

Software Assurance and Software Security - Threats to software security - Sources of software insecurity - Benefits of Detecting Software Security - Properties of Secure Software – Memory-Based Attacks: Low-Level Attacks Against Heap and Stack - Defense Against Memory-Based Attacks

UNIT II:SECURE SOFTWARE DESIGN

Requirements Engineering for secure software - SQUARE process Model - Requirements elicitation and prioritization- Isolating The Effects of Untrusted Executable Content - Stack Inspection – Policy Specification Languages – Vulnerability Trends – Buffer Overflow – Code Injection - Session Hijacking. Secure Design - Threat Modeling and Security Design Principles.

UNIT III:SECURITY RISK MANAGEMENT

Risk Management Life Cycle – Risk Profiling – Risk Exposure Factors – Risk Evaluation and Mitigation – Risk Assessment Techniques – Threat and Vulnerability Management.

UNIT IV:SECURITY TESTING

Traditional Software Testing – Comparison - Secure Software Development Life Cycle - Risk Based Security Testing – Prioritizing Security Testing With Threat Modeling – Penetration Testing – Planning and Scoping - Enumeration – Remote Exploitation – Web Application Exploitation - Exploits and Client Side Attacks – Post Exploitation – Bypassing Firewalls and Avoiding Detection - Tools for Penetration Testing.

.

UNIT V:SECURE PROJECT MANAGEMENT

Governance and security - Adopting an enterprise software security framework - Security and project management - Maturity of Practice.

SUGGESTED READINGS

1. Julia H. Allen, “Software Security Engineering”, Pearson Education, 2008
2. Evan Wheeler, “Security Risk Management: Building an Information Security Risk Management Program from the Ground Up”, First edition, Syngress Publishing, 2011
3. Chris Wysopal, Lucas Nelson, Dino Dai Zovi, and Elfriede Dustin, “The Art of Software Security Testing: Identifying Software Security Flaws (Symantec Press)”, Addison-Wesley Professional, 2006
Assessing information security: strategies, tactics, logic, and framework. IT’S Governance Ltd, 2010.
4. Robert C. Seacord, “Secure Coding in C and C++ (SEI Series in Software Engineering)”, Addison-Wesley Professional, 2005
5. Jason Grembi, “Developing Secure Software”

Semester-4

25CYU412 CYBERATTACKS AND COUNTERMEASURES 4H – 3C

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Identify and analyze various types of cyber attacks.
- Understand vulnerabilities in networks, systems, and applications
- Design and implement countermeasures to prevent or mitigate attacks.
- Understand risk management in secure software development.
- Understand Cryptography and Encryption Countermeasures

Course Outcomes (COs)

At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Identify Cyber threats and Cyber-attacks.	Remember
CO2	Demonstrate a solid understanding of foundational cybersecurity concepts, principles, and best practices	Analyze
CO3	An Apply risk assessment methodologies to evaluate and prioritize potential vulnerabilities within a given system or network.	Apply
CO4	Design and develop security plans and strategies to ensure the integrity of information in compliance with best practices, relevant policies, standards, and regulations.	Analyze
CO5	Evaluate the impact of cybersecurity decisions on privacy, compliance, and organizational reputation and adhere to ethical standards in the field.	Analyze

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO 1	3	3	2	2	2	2	2	1	3	2	3	1	1	2	2
CO 2	2	2	3	1	1	2	1	1	2	1	1	2	2	1	2
CO 3	3	3	2	2	1	2	1	1	2	2	1	1	1	2	2
CO 4	2	3	3	3	2	3	1	1	1	2	1	2	1	3	1
CO 5	3	3	2	1	1	2	1	1	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 – high

UNIT I :INTRODUCTION TO CYBERSECURITY & THREAT LANDSCAPE

Cyber security goals, CIA triad, threat actors, Overview of Cyber security: Fundamental concepts, objectives, and importance, Cyber Threat Landscape: Types of cyber threats, attack vectors, and motivations, Malwares, Ransomwares. Current Trends: Analysis of recent cyber threats and emerging trends in the cyber security landscape.

UNIT II :SOCIAL ENGINEERING, NETWORK AND WEB APPLICATION ATTACKS

Human factors, phishing kits, spear-phishing, DoS, DDoS, spoofing, sniffing, MITM, SQL injection, XSS, CSRF, OWASP.

UNIT III :SECURITY FUNDAMENTALS AND RISK ASSESSMENT

Security Foundations: Principles, protocols, and standards in cybersecurity. Vulnerability Assessment: Techniques for identifying and assessing vulnerabilities. Risk Management: Understanding risk, assessing potential impacts, and prioritizing security measures.

UNIT IV :IMPLEMENTING SECURITY MEASURES AND INCIDENT RESPONSE

Security Controls: Designing and implementing security measures, including firewalls, antivirus, encryption, and access controls. Incident Response Planning: Developing and implementing an incident response plan. Security Monitoring: Using tools and techniques to monitor for potential security incidents. System Hardening & Patch Management

UNIT V :LEGAL ETHICAL AND REGULATORY ISSUES

Legal and Ethical Considerations: Understanding the legal and ethical aspects of cybersecurity, including compliance, privacy, and responsible disclosure. GDPR, HIPAA, digital forensics basics. Emerging Threats & Future Trends : AI threats, quantum cryptography, IoT security.

SUGGESTED READINGS

1.Sammons, John, and Michael Cross, “The basics of cyber safety: computer and mobiledevice safety made easy”, Syngress
2. Charles P. Pfleeger, Shari Lawrence, Pfleeger Jonathan Margulies, “Security inComputing”, Pearson.
3. Brooks, Charles J., Christopher Grow, Philip Craig, and Donald Short, “Cybersecurity essentials”, Sybex
4. William Stallings "Network Security Essentials", Pearson.

Semester-4

25CYU411 SECURE SOFTWARE ENGINEERING LABORATORY 4H – 2C

Instruction Hours / week: L: 0 T: 0 P: 4 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

PRACTICAL EXERCISES

1. Implement the SQL injection attack.
2. Implement the Buffer Overflow attack.
3. Implement Cross Site Scripting and Prevent XSS.
4. Perform Penetration testing on a web application to gather information about the system, then initiate XSS and SQL injection attacks using tools like Kali Linux.
5. Develop and test the secure test cases
6. Penetration test using kali Linux

Semester-4

25CYU412 **CYBERATTACKS AND COUNTER MEASURES LABORATORY** **4H – 2C**

Instruction Hours / week: L: 0 T: 0 P: 4 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Objectives:

- Simulate and analyze various types of cyber attacks.
- Apply defensive techniques using industry-standard tools.
- Configure and test firewalls, IDS/IPS, and secure network settings.
- Develop incident response and log analysis skills.

Lab Requirements:

- Virtual lab environment (e.g., VirtualBox, VMware, or Cyber Range)
- Kali Linux, Metasploit, Wireshark, Snort, Burp Suite, Security Onion
- Target machines (e.g., DVWA, Metasploitable, Windows VM)

Practical Exercises:

1. Network Scanning and Reconnaissance - Use Nmap, Netcat, and Wireshark for scanning
2. Vulnerability Scanning - Perform scans using Nessus/OpenVAS
3. Exploiting System Vulnerabilities - Use Metasploit to exploit known vulnerabilities
4. Malware Analysis Basics - Analyze malware behavior in sandboxed environment
5. Phishing Simulation - Craft and detect phishing emails using tools like Gophish
6. SQL Injection and XSS - Exploit and mitigate web application flaws (DVWA)
7. Wireless Network Attacks - Crack Wi-Fi passwords, detect rogue Aps
8. IDS/IPS Setup and Detection - Deploy and configure Snort or Suricata
9. Firewall Configuration - Configure ip tables and pf Sense rules
10. Log Analysis and SIEM Tools - Analyze logs using ELK Stack or Security Onion
11. Incident Response Drill - Simulate incident handling steps
12. System Hardening - Apply patches, disable services, secure user accounts

SEMESTER - 5

B.E. / B.Tech. (Common to all Branches) **2025-2026**

Semester-5

25CYU501 ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING 4H – 3C

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Study about uninformed and Heuristic search techniques
- Learn techniques for reasoning under uncertainty
- Introduce Machine Learning and supervised learning algorithms
- Study about ensembling and unsupervised learning algorithms
- Learn the basics of deep learning using neural networks

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Use appropriates arch algorithms for problem solving	Remember
CO2	Develop probabilistic reasoning frameworks using Bayesian networks, and differentiate between exact and approximate inference methods	Understand
CO3	Develop and evaluate linear classification models using discriminant functions and probabilistic approaches such as logistic regression and Naive Bayes classifiers.	Understand
CO4	Analyze and implement ensemble learning techniques, including model combination schemes such as voting, bagging, boosting, and stacking, to improve prediction performance.	Analyze
CO5	Analyze the architecture and learning mechanism of perceptrons and multilayer perceptrons (MLPs), including the role of activation functions.	Analyze

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO 1	3	1	2	2	2	2	2	1	3	2	3	1	1	2	1
CO 2	2	2	3	1	1	2	1	1	2	1	1	2	2	1	1
CO 3	2	3	2	2	1	2	1	1	2	2	1	1	1	2	2
CO 4	2	3	3	3	2	3	1	1	1	2	1	2	1	3	2
CO 5	3	1	2	1	1	2	1	1	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 – high

UNIT1: PROBLEM SOLVING

Introduction to AI-AI Applications-Problem solving agents–search algorithms–uninformed search strategies – Heuristic search strategies – Local search and optimization problems – adversarial search – constraint satisfaction problems (CSP).

UNIT II:PROBABILISTIC REASONING

Acting under uncertainty–Bayesian inference– naïve bayes models. Probabilistic reasoning– Bayesian networks – exact inference in BN – approximate inference in BN – causal networks.

UNIT III:SUPERVISED LEARNING

Introductiontomachinelearning–LinearRegressionModels:Leastsquares, single & multiple variables, Bayesian line AR regression, gradient descent, Linear Classification Models: Discriminant function–Probabilistic discriminative model - Logistic regression, Probabilistic generative model – Naive Bayes, Maximum margin classifier – Support vector machine, Decision Tree, Random forests.

UNIT IV:ENSEMBLE TECHNIQUES AND UNSUPERVISED LEARNING

Combining multiple learners: Model combination schemes, Voting, Ensemble Learning-bagging, boosting, stacking, Unsupervised learning :K-means, Instance Based Learning: KNN, Gaussian mixture models and Expectation maximization.

UNIT V:NEURAL NETWORKS

Perceptron- Multi layer perceptron, activation functions, network training–gradient descent optimization–stochastic cgradient descent, error back pro pagation, from shallow networks to deep networks–Unit saturation(akathe vanishing gradient problem) –ReLU, hyper parameter tuning, batch normalization, regularization, drop out.

SUGGESTED READINGS

1**.** Stuart Russell and Peter Norvig, “Artificial Intelligence –A Modern Approach”, Fourth Edition, Pearson Education, 2021.
2. Ethem Al paydin,“Introduction to Machine Learning”, MITPress, Fourth Edition,2020.
3.Dan W.Patterson, “Introduction to Artificial Intelligence and Expert Systems”, Pearson Education,2007.
4. Kevin Night, Elaine Rich, and NairB., “Artificial Intelligence”, McGrawHill,2008.
5. Patrick H.Winston, "Artificial Intelligence", Third Edition, Pearson Education,2006

Semester-5

25CYU502 DATABASE MANAGEMENT SYSTEMS AND SECURITY 4H – 3C

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To learn the fundamentals of data models, conceptualize and depict a database system using ER diagram.
- To study the principles to be followed to create an effective relational database and write SQL queries to store/retrieve data to/from database systems.
- To know the fundamental concepts of transaction processing, concurrency control techniques and recovery procedure.
- To understand the need of security in Database Management systems
- To learn how to secure Database Management systems

Course Outcomes (COs)

At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Model an application's data requirements using conceptual modeling and design database schemas based on the conceptual model.	Remember
CO2	Formulate solutions to a broad range of query problems using relational algebra/SQL.	Understand
CO3	Demonstrate an understanding of normalization theory and apply such knowledge to the normalization of a database.	Analyze
CO4	Run transactions and estimate the procedures for controlling the consequences of concurrent data access.	Analyze
CO5	Able to handle security issues in database management systems	Analyze

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	2	2	2	2	2	1	3	2	3	1	1	2	2
CO2	2	2	3	1	1	2	1	1	2	1	1	2	2	1	2
CO3	2	3	2	2	1	2	1	1	2	2	1	1	1	2	2
CO4	2	3	3	3	2	3	1	1	1	2	1	2	1	3	2
CO5	3	1	2	1	1	2	1	1	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 – high

UNIT I :RELATIONAL DATABASES

Data Models – Relational Data Models – Relational Algebra – Structured Query Language – Entity-Relationship Model – Mapping ER Models to Relations – Distributed Databases – Data Fragmentation – Replication.

UNIT II :DATABASE DESIGN

ER Diagrams – Functional Dependencies – Non-Loss Decomposition Functional Dependencies – First Normal Form – Second Normal Form – Third Normal Form – Dependency Preservation – Boyce/Codd Normal Form – Multi-Valued Dependencies and Fourth Normal Form – Join Dependencies and Fifth Normal Form.

UNIT III :TRANSACTION MANAGEMENT

Transaction Concepts – ACID Properties – Serializability – Transaction Isolation Levels – Concurrency Control – Need for Concurrency – Lock-Based Protocols – Deadlock Handling – Recovery System – Failure Classification – Recovery Algorithm.

UNIT IV:**DATABASE SECURITY**

Need for database security – SQL Injection Attacks – The Injection Technique – SQLi Attack Avenues and Types.

UNIT V:**ACCESS CONTROL AND ENCRYPTION**

Database Access Control – SQL based access definition – Cascading Authorizations – Role-based access control – Inference – Database encryption.

SUGGESTED READINGS

1. Abraham Silberschatz, Henry F. Korth, S. Sudharshan, “Database System Concepts”, Seventh Edition, Tata McGraw Hill, 2021
2. William Stallings, Lawrie Brown, “Computer Security: Principles and Practice”, Fourth Edition, Pearson, 2019
3. C.J. Date, A. Kannan and S. Swamynathan, “An Introduction to Database Systems”, Pearson Education, Eighth Edition, 2006.
4. Raghu Ramakrishnan and Johannes Gehrke, “Database Management Systems”, Third Edition, McGraw Hill, 2014.

Semester-5

25CYU521 APPLIED CRYPTOGRAPHY 4H – 4C

Instruction Hours / week: L: 3 T: 0 P: 2 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To learn about Modern Cryptography.
- To focus on how cryptographic algorithms and protocols work and how to use them.
- To build a Pseudo random permutation.
- To construct Basic cryptanalytic techniques.
- To provide instruction on how to use the concepts of block ciphers and message authentication codes.

Course Outcomes (COs)

At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Interpret the basic principles of cryptography and general cryptanalysis.	Remember
CO2	Determine the concepts of symmetric encryption and authentication.	Understand
CO3	Identify the use of public key encryption, digital signatures, and key establishment.	Remember
CO4	Articulate the cryptographic algorithms to compose, build and analyze simple cryptographic solutions.	Analyze
CO5	Express the use of Message Authentication Codes	Analyze

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO 1	3	3	2	2	2	2	2	1	3	2	3	1	1	2	2
CO 2	2	2	3	1	1	2	1	1	2	1	1	2	2	1	2
CO 3	3	3	2	2	1	2	1	1	2	2	1	1	1	2	2
CO 4	2	3	3	3	2	3	1	1	1	2	1	2	1	3	1
CO 5	3	3	2	1	1	2	1	1	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 – high

UNIT I : INTRODUCTION

Basics of Symmetric Key Cryptography, Basics of Asymmetric Key Cryptography, Hardness of Functions. Notions of Semantic Security (SS) and Message Indistinguishability (MI): Proof of Equivalence of SS and MI, Hard Core Predicate, Trap-door permutation, Goldwasser-Micali Encryption. Goldreich-Levin Theorem: Relation between Hardcore Predicates and Trap-door permutations.

UNIT II :FORMAL NOTIONS OF ATTACKS

Attacks under Message Indistinguishability: Chosen Plaintext Attack (IND-CPA), Chosen Ciphertext Attacks (IND-CCA1 and IND-CCA2), Attacks under Message Non-malleability: NM-CPA and NM-CCA2, Inter-relations among the attack model

UNIT III :RANDOM ORACLES

Provable Security and asymmetric cryptography, hash functions. One-way functions: Weak and Strong one-way functions. Pseudo-random Generators (PRG): Blum-Micali-Yao Construction, Construction of more powerful PRG, Relation between One-way functions and PRG, Pseudo-random Functions (PRF).

UNIT IV : BUILDING A PSEUDORANDOM PERMUTATION

The Luby Rack off Construction: Formal Definition, Application of the Luby Rackoff Construction to the construction of Block Ciphers, The DES in the light of Luby Rack off Construction.

UNIT V : MESSAGE AUTHENTICATION CODES

Left or Right Security (LOR). Formal Definition of Weak and Strong MACs, Using a PRF as a MAC, Variable length MAC. Public Key Signature Schemes: Formal Definitions, Signing and Verification, Formal Proofs of Security of Full Domain Hashing. Assumptions for Public Key Signature Schemes: One-way functions Imply Secure One-time Signatures. Shamir's Secret Sharing Scheme. Formally Analyzing Cryptographic Protocols. Zero Knowledge Proofs and Protocols.

PRACTICAL EXERCISES:

1. Implement Feige-Fiat-Shamir identification protocol.
2. Implement GQ identification protocol.
3. Implement Schnorr identification protocol.
4. Implement Rabin one-time signature scheme.
5. Implement Merkle one-time signature scheme.
6. Implement Authentication trees and one-time signatures.
7. Implement GMR one-time signature scheme.

SUGGESTED READINGS

1. Hans Delfs and Helmut Knebl, Introduction to Cryptography: Principles and Applications, Springer Verlag.
2. Wenbo Mao, Modern Cryptography, Theory and Practice, Pearson Education (Low Priced Edition).
3. ShaffiGoldwasser and MihirBellare, Lecture Notes on Cryptography, Available at http://citeseerx.ist.psu.edu/.
4. OdedGoldreich, Foundations of Cryptography, CRC Press (Low Priced Edition Available), Part 1 and Part 23.

Semester-5

25CYU511 **DATABASE MANAGEMENT SYSTEMS AND SECURITY LABORATORY** **4H – 2C**

Instruction Hours / week: L: 0 T: 0 P: 4 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

PRACTICALEXERCISES:

1.Create a data base table ,add constraints (primary key, unique, check, Not null), insert rows, update and delete rows using SQL DDL and DML commands.
2. Create a set of tables, add foreign key constraints and incorporate referential integrity.
3. Querythedatabasetablesusingdifferent‘where’clauseconditionsandalsoimplementaggregate functions.
4. Query the database tables and explore subqueries and simple join operations
5. Write user defined functions and stored procedures in SQL.
6. SQL Injection Basics - Perform classic and blind SQL attacks on DVWA and mitigate using prepared statements.
7. Audit Logging & Log Analysis- Enable logging on MySQL/PostgreSQL and analyze activity for suspicious behavior.
8. Vulnerability Scanning of DBMS - Scan for known DBMS vulnerabilities using Open VAS/Nessus
9. Secure Backup and Recovery - Perform encrypted DB backups using mysqldump and test restoration securely.
10. Data-at-Rest and Data-in-Transit Encryption - Use TDE (Transparent Data Encryption) or SSL for database traffic encryption.

Semester-5

25MAC501 ENTREPRENEURSHIP AND STARTUPS 3H – 3C

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Demonstrate an understanding of the evolution, characteristics, and role of entrepreneurship in society.
- Construct knowledge of the startup ecosystem, including key support systems and government initiatives.
- Assemble techniques for opportunity identification and early-stage startup design.
- Manipulate domain-specific tools and knowledge (Engineering/Science/Arts) to build sector-specific startup models.
- Create a complete entrepreneurial plan

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Interpret the basic principles of cryptography and general cryptanalysis.	Remember
CO2	Determine the concepts of symmetric encryption and authentication.	Understand
CO3	Identify the use of public key encryption, digital signatures, and key establishment.	Remember
CO4	Articulate the cryptographic algorithms to compose, build and analyze simple cryptographic solutions.	Analyze
CO5	Express the use of Message Authentication Codes	Analyze

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO 1	3	3	2	2	2	2	2	1	3	2	3	1	1	2	2
CO 2	2	2	3	1	1	2	1	1	2	1	1	2	2	1	2
CO 3	3	3	2	2	1	2	1	1	2	2	1	1	1	2	2
CO 4	2	3	3	3	2	3	1	1	1	2	1	2	1	3	1
CO 5	3	3	2	1	1	2	1	1	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 – high

SEMESTER – 6

B.E. / B.Tech. (Common to all Branches) **2025-2026**

Semester-6

25CYU621 **VULNERABILITY ASSESSMENT AND PENETRATION TESTING** **4H – 4C**

Instruction Hours / week: L: 3 T: 0 P: 2 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Introduce Vulnerability Assessment and Penetration Testing
- To be familiar with the Penetration Testing and Tools
- To get an exposure to Metasploit exploitation tool, Linux exploit and Windows exploit
- To gain knowledge on Web Application Security Vulnerabilities, Vulnerability analysis and Malware Analysis

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Explain the ethical considerations and legal implications in conducting ethical hacking activities using appropriate tools.	Remember
CO2	Analyze social engineering, physical penetration and insider attacks using automating penetration	Analyze
CO3	Identify report penetration tests effectively to develop and execute Linux and Windows exploits, bypassing memory protections.	Remember
CO4	Illustrate web application security vulnerabilities to conduct vulnerability analysis.	Analyze
CO5	Inspect protection against client-side browser exploits.	Analyze

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	2	2	2	2	2	1	3	2	3	1	1	2	1
CO2	2	2	3	1	1	2	1	1	2	1	1	2	2	1	1
CO3	2	3	2	2	1	2	1	1	2	2	1	1	1	2	2
CO4	2	3	3	3	2	3	1	1	1	2	1	2	1	3	2
CO5	3	1	2	1	1	2	1	1	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 – high

UNIT I: INTRODUCTION TO VULNERABILITY ASSESSMENT AND PENETRATION TESTING

Why You Need to Understand Your Enemy's Tactics, Recognizing the Gray Areas in Security, Conducting a Social Engineering Attack, Common Attacks Used in Penetration Testing, Preparing Yourself for Face-to-Face Attacks, Defending Against Social Engineering Attacks.

UNIT II: TYPES OF PENETRATION ATTACKS

Physical Penetration Attacks**:** Need of Physical Penetration, Conducting a Physical Penetration, Common Ways into a Building, Defending Against Physical Penetrations, **Insider Attacks:** Conducting an Insider Attack, Defending Against Insider Attacks. **Metasploit:** The Big Picture, Getting Metasploit, Using the Metasploit Console to Launch Exploits, Exploiting Client-Side Vulnerabilities with Metasploit, Penetration Testing with Metasploit's Meterpreter, Automating and Scripting Metasploit

UNIT III: EXPLOITS AND MANAGING PENETRATION ATTACKS

Basic Linux Exploits**:** Stack Operations, Buffer Overflows, Local Buffer Overflow Exploits, Exploit Development Process. Windows Exploits: Compiling and Debugging Windows Programs, Writing Windows Exploits, Understanding Structured Exception Handling (SEH), Understanding Windows Memory, Protections (XP SP3, Vista 7 And Server 2008), Bypassing Windows Memory Protections. Managing a Penetration Test**:** Planning a Penetration Test, Structuring a Penetration Testing Agreement, Execution of a Penetration Test, Information Sharing During a Penetration Test, Reporting the Results of a Penetration Test.

UNIT IV: **WEB APPLICATION SECURITY VULNERABILITIES**

Overview of Top Web Application Security Vulnerabilities, Injection Vulnerabilities, Cross-Site Scripting Vulnerabilities, The Rest of the OWASP Top Ten, SQL Injection Vulnerabilities, Cross-Site Scripting Vulnerabilities. Vulnerability Analysis: Passive Analysis: Source Code Analysis, Binary Analysis.

UNIT V: CLIENT-SIDE BROWSER EXPLOITS AND MALWARE ANALYSIS

Internet Explorer Security Concepts, History of Client- Side Exploits and Latest Trends, Finding New Browser-Based Vulnerabilities, Heap Spray to Exploit, Protecting Yourself from Client-Side Exploit. Collecting Malware and Initial Analysis: Malware, Latest Trends in Honeynet Technology, Catching Malware: Setting the Trap, Initial Analysis of Malware.

PRACTICAL EXERCISES:

1**.** Monitoring Network Traffic: To analyze and capture network traffic to identify patterns, detect anomalies and assess overall network performance and security.

2. Host & Services Discovery using Nmap: To identify active hosts and the services they are running within a network using Nmap, enabling a comprehensive understanding of the network environment.

3. Vulnerability Scanning using OpenVAS: To perform a systematic assessment of networked systems using OpenVAS to identify potential vulnerabilities that could be exploited by attackers.

4. Internal Penetration Testing
a. Mapping
b. Scanning
c. Gaining Access through CVEs
d. Sniffing POP3/FTP/Telnet Passwords
e. ARP Poisoning
f. DNS Poisoning
To perform a thorough internal penetration test that systematically assesses the security of the organization's network infrastructure by mapping network resources, scanning for vulnerabilities, exploiting known weaknesses and demonstrating attack techniques, including credential sniffing and poisoning attacks, in order to identify and mitigate potential security risks effectively

5. External Penetration Testing
a. Evaluating External Infrastructure
b. Creating Topological Map & Identifying IP Address of Target
c. Lookup Domain Registry for IP Information
d. Examining Use of IPv6 at Remote Location
To conduct a comprehensive external penetration test aimed at evaluating the security of the organization's external infrastructure by assessing vulnerabilities, mapping the network topology, gathering IP and domain registry information, and examining the implementation of IPv6, ultimately identifying potential entry points and recommending measures to strengthen defences against external threats.

6. Vulnerability Scanning with Nessus
To utilize Nessus for comprehensive vulnerability scanning, identifying security weaknesses in systems and providing recommendations for remediation.

7. Web Application Assessment with Nikto & Burp Suite
To evaluate web applications for security vulnerabilities using Nikto and Burp Suite, identifying issues such as misconfigurations and common vulnerabilities in web applications.

SUGGESTED READINGS

1. Gray Hat Hacking - The Ethical Hackers Handbook, Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, and Terron Williams, 3rd Edition, Tata McGraw-Hill.
2. The Web Application Hacker’s Hand Book - Discovering and Exploiting Security flaws, Dafydd Suttard, Marcuspinto,1st Edition, Wiley Publishing.
3. Penetration Testing: Hands-on Introduction to Hacking, Georgia Weidman, 1st Edition, No Starch Press.

Semester-6

25CYU622 MOBILE AND WIRELESS SECURITY 4H – 4C

Instruction Hours / week: L: 3 T: 0 P: 2 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To conceptualize the wireless environment in terms of security and privacy
- To impart state-of-the-art technologies of wireless network security
- To analyze the various categories of threats, vulnerabilities, countermeasures in wireless and mobile networking
- To familiarize students with the issues and technologies involved in designing a wireless system that is robust against attacks.
- To understand the security and privacy problems in the realm of wireless networks and mobile computing

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Explain wireless and mobile network security and its relation to the new security-based protocols	Remember
CO2	Apply proactive and defensive measures to counter potential threats, attacks and intrusions.	Apply
CO3	Design secured wireless and mobile networks that optimize accessibility whilst minimizing vulnerability to security risks.	Understand
CO4	Impart state-of-the-art technologies and protocols of wireless network security	Analyze
CO5	Identify and investigate in-depth both early and contemporary threats to mobile and wireless networks security	Analyze

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3	2	2	2	2	2	1	3	2	3	1	1	2	2
CO2	2	2	3	1	1	2	1	1	2	1	1	2	2	1	2
CO3	3	3	2	2	1	2	1	1	2	2	1	1	1	2	2
CO4	2	3	3	3	2	3	1	1	1	2	1	2	1	3	1
CO5	3	3	2	1	1	2	1	1	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 – high

UNIT I: INTRODUCTION TO WIRELESS TECHNOLOGIES

Design Factors, security threats and vulnerabilities present at the different protocol layers, family of security protocols and algorithms used in the existing wireless networks (Bluetooth, Wi-Fi, WiMAX and LTE standards).

UNIT II: INTRODUCTION TO MOBILE NETWORK TECHNOLOGIES

Vulnerabilities Threats And Attack Entry Points. Categorization Of Attacks in Mobile Networks, Signaling Attacks. Threats And Attacks In 4g Networks- Attacks Against Security and Confidentiality, Ip-Based Attacks, Gtp- Based Attacks, Volte Sip-Based Attacks, Diameter-Based Attacks.

UNIT III: EMERGING PHYSICAL LAYER SECURITY IN WIRELESS COMMUNICATIONS

Class of information- Theoretic security, artificial-noise-aided security, security-oriented beam forming, security-oriented diversity, and physical-layer secret key generation techniques. Review on various wireless jammers, open challenges in wireless security.

UNIT IV:SECURITY IN AD HOC WIRELESS NETWORKS

Network Security Requirements, Issues and Challenges in Security Provisioning, Network Security Attacks, Key Management in Adhoc Wireless Networks, Secure Routing in Adhoc Wireless Networks.

UNIT V: RFID SECURITY AND PRIVACY

RFID chips Techniques and Protocols, RFID anti-counterfeiting, Man-in-the-middle attacks on RFID systems, Digital Signature Transponder, Combining Physics and Cryptography to Enhance Privacy in RFID Systems, Scalability Issues in Large-Scale Applications, An Efficient and Secure RFID Security Method with Ownership Transfer, Policy-based Dynamic Privacy Protection Framework leveraging Globally Mobile RFIDs, User-Centric Security for RFID based Distributed Systems, Optimizing RFID protocols for Low Information Leakage, RFID: an anti-counterfeiting tool.

PRACTICAL EXERCISES:

1. Introduction to Mobile Platforms - Analyze app permissions, security features (Android vs iOS).
2. Static Analysis of Android Apps - Decompile APK using APK Tool, JADX; find hardcoded secrets.
3. Dynamic App Analysis - Use Burp Suite to intercept HTTP/S traffic from a test mobile app.
4. Insecure Data Storage - Explore and exploit weak storage (Shared Preferences, SQLite DB, internal storage).
5. Authentication & Authorization Flaws - Bypass login screens and token validation using Frida or runtime code injection.
6. Wireless Traffic Sniffing - Capture Wi-Fi traffic using Wireshark and Airodump-ng; identify unencrypted data.
7. Bluetooth Attacks - Scan for and exploit nearby Bluetooth devices using bluetoothctl and hcitool
8. Mobile Malware Analysis - Install and analyze benign malware samples in an emulator using MobSF.
9. Mobile App Penetration Testing - Conduct full test of a custom insecure app using OWASP MASVS as a guide.
10. Wi-Fi Intrusion Detection - Set up basic detection using Kismet, monitor rogue devices.

Tools Required:

- Android Studio / Android Virtual Device (AVD)
- Kali Linux (for wireless tools)
- Wireshark, Airodump-ng, Aircrack-ng, Reaver
- Burp Suite
- MobSF (Mobile Security Framework)
- APKTool, JADX
- Real Android device (optional), Bluetooth dongle

SUGGESTED READINGS

1. Makki, S. K., Reiher, P., Makki, K., Pissinou, N., & Makki, S. (Eds.). (2007). ***Mobile and wireless network security and privacy***. Springer Science & Business Media.

2. Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). **A survey on wireless security: Technical challenges, recent advances, and future trends**. *Proceedings of the IEEE*, *104*(9), 1727-1765.

3. Kitsos, P., & Zhang, Y. (2008). ***RFID security*** (Vol. 233). Springer Science+ Business Media, LLC.

4. Cache, J., & Liu, V. (2007). Hacking Wireless Exposed

25CYU623 **CYBER FORENSICS** **Semester-6**
4H – 4C

Instruction Hours / week: L: 3 T: 0 P: 2 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To learn cyber crime and forensics
- To become familiar with forensics tools
- To learn to analyze and validate forensics data
- To understand cyber laws and the admissibility of evidence with case studies
- To learn the vulnerabilities in network infrastructure with ethical hacking

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Understand the basics of cybercrime and computer forensics	Understand
CO2	Apply several different computer forensic tools to a given scenario	Apply
CO3	Analyze and validate forensics data	Analyze
CO4	Understand Admissibility of evidence in India with Cyber laws and Case Studies	Understand
CO5	Identify the vulnerabilities in a given network infrastructure	Analyze

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	1	2	2	2	2	2	1	3	2	3	1	1	2	2
CO2	2	2	3	1	1	2	1	1	2	1	1	2	2	1	2
CO3	2	3	2	2	1	2	1	1	2	2	1	1	1	2	2
CO4	2	3	3	3	2	3	1	1	1	2	1	2	1	3	2
CO5	3	1	2	1	1	2	1	1	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 – high

UNIT I: INTRODUCTION TO CYBER CRIME AND FORENSICS

Introduction to Traditional Computer Crime, Traditional problems associated with Computer Crime. Role of ECD and ICT in Cybercrime - Classification of Cyber Crime. The Present and future of Cybercrime - Cyber Forensics -Steps in Forensic Investigation - Forensic Examination Process - Types of CF techniques - Forensic duplication and investigation - Forensics Technology and Systems - Understanding Computer Investigation – Data Acquisition.

UNIT II : EVIDENCE COLLECTION AND FORENSICS TOOLS

Processing Crime and Incident Scenes – Digital Evidence - Sources of Evidence -Working with File Systems. - Registry - Artifacts - Current Computer Forensics Tools: Software/ Hardware Tools - Forensic Suite - Acquisition and Seizure of Evidence from Computers and Mobile Devices - Chain of Custody- Forensic Tools

UNIT III: ANALYSIS AND VALIDATION

Validating Forensics Data – Data Hiding Techniques – Performing Remote Acquisition – Network Forensics – Email Investigations – Cell Phone and Mobile Devices Forensics - Analysis of Digital Evidence - Admissibility of Evidence - Cyber Laws in India - Case Studies.

UNIT IV: ETHICAL HACKING

Introduction to Ethical Hacking – Footprinting and Reconnaissance - Scanning Networks - Enumeration - System Hacking - Malware Threats – Sniffing – Email Tracking.

UNIT V :ETHICAL HACKING IN WEB

Social Engineering - Denial of Service - Session Hijacking - Hacking Web servers - Hacking Web Applications – SQL Injection - Hacking Wireless Networks - Hacking Mobile Platforms.

PRACTICAL EXERCISES:

1. Study and Explore the following forensic tools:
(a) FTK Imager
(b) Autopsy
(c)EnCase Forensic Imager
(d) Last Activity View
(e) USB Deview
2. Recover deleted files using FTK Imager
3. Acquire forensic image of hard disk using EnCase Forensics Imager and also perform integrity checking/validation
4. Restore the Evidence Image using EnCase Forensics Imager.
5. Study the following:
(a) Collect Email Evidence in Victim PC.
(b) Extract Browser Artifacts (Chrome History view for Google Chrome)
6. Use USB Deview to find the last connected USB to the system
7. Perform Live Forensics Case Investigation using Autopsy
8. Study Email Tracking and Email Tracing and write a report on them.

SUGGESTED READINGS

1. Bill Nelson, Amelia Phillips, Christopher Steuart, — Guide to Computer Forensics and Investigationsll, Cengage Learning, India Sixth Edition, 2019.
2. CEH official Certified Ethical Hacking Review Guide, Wiley India Edition, Version 11, 2021.
3. Dejey, S. Murugan - Cyber Forensics, Oxford University Press, India, 2018
4. John R.Vacca, “Computer Forensics “, Cengage Learning, 2005

SEMESTER - 7

B.E. / B.Tech. (Common to all Branches) **2025-2026**

Semester-7

25CYU721 **SOCIAL NETWORK SECURITY** **4H – 4C**

Instruction Hours / week: L: 3 T: 0 P: 2 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To develop semantic web related simple applications
- To explain Privacy and Security issues in Social Networking
- To explain the data extraction and mining of social networks
- To discuss the prediction of human behavior in social communities
- To describe the Access Control, Privacy and Security management of social networks

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Develop semantic web related simple applications	Remember
CO2	Address Privacy and Security issues in Social Networking	Remember
CO3	Explain the data extraction and mining of social networks	Understand
CO4	Discuss the prediction of human behavior in social communities	Understand
CO5	Describe the applications of social networks	Understand

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO 1	3	3	2	2	2	2	2	1	3	2	3	1	1	2	2
CO 2	2	2	3	1	1	2	1	1	2	1	1	2	2	1	2
CO 3	3	3	2	2	1	2	1	1	2	2	1	1	1	2	2
CO 4	2	3	3	3	2	3	1	1	1	2	1	2	1	3	1
CO 5	3	3	2	1	1	2	1	1	3	2	3	2	2	2	1

1 - low, 2 - medium, 3 – high

UNIT I : FUNDAMENTALS OF SOCIAL NETWORKING

Introduction to Semantic Web, Limitations of current Web, Development of Semantic Web, Emergence of the Social Web, Social Network analysis, Development of Social Network Analysis, Key concepts and measures in network analysis, Historical overview of privacy and security, Major paradigms, for understanding privacy and security

UNIT II : SECURITY ISSUES IN SOCIAL NETWORKS

The evolution of privacy and security concerns with networked technologies, Contextual influences on privacy attitudes and behaviors, Anonymity in a networked world

UNIT III : EXTRACTION AND MINING IN SOCIAL NETWORKING DATA

Extracting evolution of Web Community from a Series of Web Archive, Detecting communities in social networks, Definition of community, Evaluating communities, Methods for community detection and mining, Applications of community mining algorithms, Tools for detecting communities social network infrastructures and communities, Big data and Privacy.

UNIT IV : PREDICTING HUMAN BEHAVIOR AND PRIVACY ISSUES

Understanding and predicting human behavior for social communities, User data Management, Inference and Distribution, Enabling new human experiences, Reality mining, Context, Awareness, Privacy in online social networks, Trust in online environment, What is Neo4j, Nodes, Relationships, Properties .

UNIT V : ACCESS CONTROL, PRIVACY AND IDENTITY MANAGEMENT

Understand the access control requirements for Social Network, Enforcing Access Control Strategies, Authentication and Authorization, Roles-based Access Control, Host, storage and network access control options, Firewalls, Authentication, and Authorization in Social Network, Identity & Access Management, Single Sign-on, Identity Federation, Identity providers and service consumers, The role of Identity provisioning.

PRACTICALEXERCISES:

1. Design own social media application
2. Create a Network model using Neo4j
3. Read and write Data from Graph Database
4. Find “Friend of Friends” using Neo4j
5. Implement secure search in social media
6. Create a simple Security & Privacy detector

SUGGESTED READINGS

1. Peter Mika, “Social Networks and the Semantic Web, First Edition, Springer 2007.
2. BorkoFurht, “Handbook of Social Network Technologies and Application, First Edition, Springer, 2010.
3. Learning Neo4j 3.x “Second Edition By Jérôme Baton, Rik Van Bruggen, Packet publishing
4. David Easley, Jon Kleinberg, “Networks, Crowds, and Markets: Reasoning about a Highly Connected World‖, First Edition, Cambridge University Press, 2010.
5. Easley D. Kleinberg J., “Networks, Crowds, and Markets – Reasoning about a Highly Connected World”, Cambridge University Press, 2010.
6. Jackson, Matthew O., “Social and Economic Networks”, Princeton University Press, 2008

Elective List
Vertical List 1 - Network Engineer

B.E. / B.Tech. (Common to all Branches) **2025-2026**

25CYU531A **JAVA PROGRAMMING** **4H – 3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- To impart the core language features of Java and its Application Programming Interfaces (API)
- To demonstrate the use of threads, exceptions, files and collection frameworks in Java
- To familiarize students with GUI based application development and database connectivity.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Comprehend Java Virtual Machine architecture and Java Programming Fundamentals.	Remember
CO2	Design applications involving Object Oriented Programming concepts such as inheritance, association, aggregation, composition, polymorphism, abstract classes and interfaces.	Remember
CO3	Design and build multi-threaded Java Applications and Build software using concepts such as files, collection frameworks and containers.	Understand
CO4	Design and implement Java Applications for real world problems involving Database Connectivity and Graphical User Interface using JavaFX	Understand
CO5	Design, Develop and Deploy dynamic web applications using Servlets and Java Server Pages	Understand

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO 1	3	3	3	3	-	-	-	-	1	2	3	3	2	1	3
CO 2	2	1	3	2	2	-	-	-	1	2	2	3	3	1	3
CO 3	3	1	3	3	1	-	-	-	1	2	1	1	1	3	3
CO 4	3	2	3	2	1	-	-	-	1	2	2	3	2	2	1
CO 5	2	3	3	2	2	-	-	-	1	3	3	2	3	1	3

1 - low, 2 - medium, 3 – high

UNIT I : Java Fundamentals

Java Basics: Java Design goal - Features of Java Language - JVM – Bytecode - Java source file structure basic programming constructs Arrays one dimensional and multi-dimensional enhanced for loop String package. Class Fundamentals - Object Object reference array of objects constructors methods over- loading this reference static block - nested class inner class garbage collection finalize() Wrapper classes. Inheritance types - use of super - Polymorphism abstract class interfaces packages and sub packages

UNIT II: Robustness and Concurrency

Exception Handling - Exceptions Errors - Types of Exception - Control Flow in Exceptions - Use of try, catch, finally, throw, throws in Exception Handling - user defined exceptions - Multithreading Thread creation sharing the workload among threads synchronization inter thread communication deadlock

UNIT III: Files, Streams and Object serialization

Data structures: Java I/O streams Working with files Serialization and deserialization of objects Lambda expressions, Collection framework List, Map, Set Generics Annotations

UNIT IV: GUI Programming and Database Connectivity

GUI programming using JavaFX, exploring events, controls and JavaFX menus Accessing databases using JDBC connectivity

UNIT V: Servlet and Java Server Pages

Introduction to servlet - Servlet life cycle - Developing and Deploying Servlets - Exploring Deployment Descriptor (web.xml) - Handling Request and Response - Session Tracking Management. JSP Tags and Expressions - JSP Expression Language (EL) - Using Custom Tag - JSP with JavaBean.

SUGGESTED READINGS

1. Herbert Schildt, The Complete Reference -Java, Tata McGraw-Hill Education, Tenth Edition, 2017.
2. Paul J. Deitel, Harvey Deitel ,Java SE8 for Programmers (Deitel Developer Series) 3rd Edition, 2014
3. Y. Daniel Liang, Introduction to Java programming-comprehensive version-Tenth Edition, Pearson ltd 2015
4**.** Paul Deitel Harvey Deitel ,Java, How to Program, Prentice Hall; 9th edition , 2011.
5. Cay Horstmann BIG JAVA, 4th edition, John Wiley Sons,2009

25CYU532A **IP ADDRESS MANAGEMENT** **4H – 3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Introduce the fundamentals of IP addressing (IPv4 and IPv6) and subnetting.
- Explain the planning and allocation of IP addresses in enterprise and ISP environments.
- Provide knowledge of tools and techniques for managing IP address spaces.
- Equip students with the ability to implement IP Address Management (IPAM) systems.
- Explore automation and security aspects of IP address management.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Describe IP addressing schemes including IPv4 and IPv6.	Understand
CO2	Design and implement efficient subnetting and supernetting plans.	Remember
CO3	Apply IP address planning strategies for small to large-scale networks.	Apply
CO4	Configure and manage IPAM tools for dynamic and static IP allocation.	Understand
CO5	Integrate automation and security into IP address management workflows.	Analyze

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3	3	3	-	-	-	-	1	2	3	3	2	1	3
CO2	2	1	3	2	2	-	-	-	1	2	2	3	3	1	3
CO3	3	1	3	3	1	-	-	-	1	2	1	1	1	3	3
CO4	3	2	3	2	1	-	-	-	1	2	2	3	2	2	1
CO5	2	3	3	2	2	-	-	-	1	3	3	2	3	1	3

1 - low, 2 - medium, 3 – high

UNIT I: IP Addressing

IP addressing basics: IPv4 structure, address classes, Private vs Public IP addresses, Reserved and special addresses, Need for IP address management, Transition to IPv6 – structure and representation.

UNIT II: Subnetting and Supernetting

Subnetting concepts, subnet masks, CIDR, VLSM (Variable Length Subnet Mask), Supernetting Techniques, Subnetting practice and case studies, IPv6 subnetting.

UNIT III: IP Address Planning and Allocation

Hierarchical address planning, DHCP configuration and management, Static vs dynamicaddress Allocation, Address planning for enterprises and ISPs, Documentation and IP inventoryManagement.

UNIT IV: IPAM Tools and Implementation

Introduction to IPAM (IP Address Management), Open-source and commercial IPAM tools (e.g., phpIPAM, Infoblox), Integration with DNS and DHCP, Address lease tracking and monitoring, Configuration and deployment of IPAM systems

UNIT V: Automation and Security in IPAM

Automating IP address assignments (scripts, APIs), Role of Ansible, Python in network Automation, Security issues in IPAM, Access control, logging, and audit trails, Case studies and best practices in enterprise IP management

SUGGESTED READINGS

1**. Silvia Hagen**, *IPv6 Essentials*, O'Reilly Media
2. **Ralph Droms**, *The DHCP Handbook*, Sams Publishing
3**. Michael Dooley, Timothy Rooney**, *IPv6 Deployment and Management*, Cisco Press
4. Documentation of IPAM tools like phpIPAM, Infoblox, etc.
5. RFCs related to IP addressing and subnetting (RFC 1918, RFC 4193, RFC 4291)

25CYU631A REMOTE INFRASTRUCTURE MANAGEMENT 4H – 3C

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Understand the architecture and components of Remote Infrastructure Management (RIM).
- Explore the tools, technologies, and practices used for managing IT infrastructure remotely.
- Learn to monitor, manage, and troubleshoot servers, networks, storage, and endpoints remotely.
- Introduce automation, virtualization, and cloud technologies in RIM.
- Understand IT service management frameworks (like ITIL) for effective infrastructure operations.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Describe the architecture, components, and benefits of RIM.	Understand
CO2	Implement remote monitoring and management practices for IT infrastructure.	Remember
CO3	Apply tools for managing network, server, storage, and endpoint infrastructure remotely.	Apply
CO4	Integrate automation and virtualization in remote infrastructure tasks.	Understand
CO5	Apply ITSM practices for incident, problem, and change management in RIM environments.	Analyze

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3	3	3	-	-	-	-	1	2	3	3	2	1	3
CO2	2	1	3	2	2	-	-	-	1	2	2	3	3	1	3
CO3	3	1	3	3	1	-	-	-	1	2	1	1	1	3	3
CO4	3	2	3	2	1	-	-	-	1	2	2	3	2	2	1
CO5	2	3	3	2	2	-	-	-	1	3	3	2	3	1	3

1 - low, 2 - medium, 3 – high

UNIT I: Introduction to Remote Infrastructure Management

Definition, evolution, and scope of RIM, Components: network, server, storage, and endpoint Management, Benefits and challenges of RIM, RIM lifecycle and architecture, Remote support models (Onsite-Offshore, NOC, etc.)

UNIT II: Remote Monitoring and Management

Network monitoring tools (Nagios, Zabbix, PRTG), Server and application monitoring, Remote desktop and endpoint management tools (TeamViewer, RDP, AnyDesk),Event and log management (Syslog, SNMP), Performance and availability monitoring

UNIT III: Infrastructure Management Tools and Techniques

Configuration management tools (Puppet, Chef, Ansible), Asset and inventory management, Patch and update management, Backup and disaster recovery, Scripting for remote automation (Bash, PowerShell)

UNIT IV: Virtualization and Cloud in RIM

Virtual infrastructure management (VMware, Hyper-V), Cloud infrastructure management (AWS, Azure, GCP), Remote access to virtual machines and containers, Infrastructure as a Service (IaaS) management, Cloud monitoring and cost optimization

UNIT V: IT Service Management and Security in RIM

Overview of ITIL practices, Incident, problem, and change management, SLA monitoring and reporting, Security issues in RIM, Secure access: VPN, SSH, encryption, multi-factor authentication, Compliance and audit requirements

SUGGESTED READINGS

1. Kamesh Ganeson, *Remote Infrastructure Management*, Wiley
2. **Kief Morris**, *Infrastructure as Code*, O'Reilly Media
3. **TIL Foundation Handbook**, TSO (The Stationery Office)
4. Vendor Documentation (e.g., Nagios, Ansible, AWS, VMware)

25CYU632A **ZERO TRUST NETWORK** **4H – 3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Introduce the principles and architecture of the Zero Trust Security Model.
- Examine how traditional perimeter-based models differ from Zero Trust.
- Explore components such as identity verification, micro-segmentation, and continuous monitoring.
- Analyze how Zero Trust can be implemented across enterprise environments including cloud and hybrid infrastructures.
- Discuss tools, frameworks, and case studies to design and evaluate Zero Trust deployments.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Explain the principles, needs, and evolution of the Zero Trust model.	Understand
CO2	Compare traditional and Zero Trust architectures and identify security gaps.	Remember
CO3	Design access policies and implement micro-segmentation in network security.	Apply
CO4	Integrate identity, device, and network-level controls in a Zero Trust environment.	Understand
CO5	Evaluate real-world Zero Trust solutions and perform security posture assessments.	Analyze

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO 1	3	3	3	3	-	-	-	-	1	2	3	3	2	1	3
CO 2	2	1	3	2	2	-	-	-	1	2	2	3	3	1	3
CO 3	3	1	3	3	1	-	-	-	1	2	1	1	1	3	3
CO 4	3	2	3	2	1	-	-	-	1	2	2	3	2	2	1
CO 5	2	3	3	2	2	-	-	-	1	3	3	2	3	1	3

1 - low, 2 - medium, 3 – high

UNIT I:Zero Trust Security

Security evolution: From perimeter to Zero Trust, Principles of Zero Trust: Never Trust, Always Verify, Core components: Identity, device, network, applications, and data, Zero Trust architecture models (Forrester, NIST), Use cases and benefits in modern IT environments

UNIT II: Identity and Access Management (IAM)

Role of identity in Zero Trust, Identity Providers (IdPs), Single Sign-On (SSO), MFA, Conditional access policies, Least privilege and Role-Based Access Control (RBAC), Identity governance and lifecycle management

UNIT III: Network Segmentation and Micro-segmentation

Need for segmentation in Zero Trust, Traditional vs software-defined segmentation, Micro-segmentation techniques using SDN, firewalls, Policy creation and enforcement, Network visibility and trust zones

UNIT IV: Continuous Monitoring and Threat Detection

Real-time monitoring and telemetry, User and Entity Behavior Analytics (UEBA), Security Information and Event Management (SIEM), Zero Trust in incident response and threat detection Integration with SOAR (Security Orchestration, Automation and Response)

UNIT V: Zero Trust Deployment and Case Studies

Zero Trust in cloud, hybrid, and on-premise infrastructure, Implementation roadmaps and frameworks (e.g., NIST SP 800-207), Vendor solutions: Google BeyondCorp, Microsoft Zero Trust, Cisco ZTNA, Challenges in deployment: Legacy systems, compliance, scalability, Case studies and success stories

SUGGESTED READINGS

1**. Evan Gilman & Doug Barth**, *Zero Trust Networks: Building Secure Systems in Untrusted Networks*, O'Reilly.

2. **NIST Special Publication 800-207**, *Zero Trust Architecture*

3. Cisco Zero Trust Architecture Guide

4. Microsoft & Google whitepapers on Zero Trust

25CYU731A NETWORK SECURITY AND FIREWALLS 4H – 3C

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Understand the fundamentals of network security threats and vulnerabilities.
- Learn key security mechanisms including authentication, encryption, and access control. Explore the configuration and use of firewalls to secure network boundaries.
- Examine intrusion detection and prevention systems (IDS/IPS).
- Enable students to design secure network architectures with effective firewall strategies.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Identify network security threats, vulnerabilities, and attacks.	Understand
CO2	Apply cryptographic techniques for secure communication.	Apply
CO3	Configure and deploy firewall policies for network protection.	Apply
CO4	Use intrusion detection and prevention systems for threat management.	Understand
CO5	Design and evaluate secure network architectures with layered defense mechanisms.	Analyze

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3	3	3	-	-	-	-	1	2	3	3	2	1	3
CO2	2	1	3	2	2	-	-	-	1	2	2	3	3	1	3
CO3	3	1	3	3	1	-	-	-	1	2	1	1	1	3	3
CO4	3	2	3	2	1	-	-	-	1	2	2	3	2	2	1
CO5	2	3	3	2	2	-	-	-	1	3	3	2	3	1	3

1 - low, 2 - medium, 3 – high

UNIT I: Network Security Overview

Introduction to network security, Threats: Malware, phishing, DDoS, spoofing, MITM, Security goals: Confidentiality, Integrity, Availability, Vulnerabilities and risk assessment, Overview of security policies and network defense strategies

UNIT II: Cryptography and Secure Communication

Symmetric and asymmetric encryption (AES, RSA), Hashing algorithms (SHA, MD5), Digital signatures and certificates, Public Key Infrastructure (PKI), VPNs and secure tunneling (IPSec, SSL/TLS)

UNIT III: Firewalls and Packet Filtering

Firewall fundamentals: Types and characteristics, Packet filtering and stateful inspection, NAT, Proxy Firewalls, Application Layer Firewalls, Designing firewall rules and ACLs, Perimeter security and demilitarized zones (DMZ)

UNIT IV: Intrusion Detection and Prevention Systems (IDS/IPS)

IDS and IPS: Types and architectures, Signature-based vs anomaly-based detection,Tools and frameworks (Snort, Suricata, OSSEC), Incident response and alert management, Integration with SIEM systems

UNIT V: Network Security Design and Implementation

Network segmentation and isolation, Defense in depth strategy, Secure router and switch configuration, Securing wireless networks, Case studies on enterprise security architecture and firewall deployment

SUGGESTED READINGS

1. William Stallings, *Network Security Essentials: Applications and Standards*, Pearson
2. **Behrouz A. Forouzan**, *Cryptography and Network Security*, McGraw Hill
3**. Chris Brenton & Cameron Hunt**, *Mastering Network Security*, Sybex
4. **NIST SP 800 Series** – Security Guidelines
5. Vendor documentation: Cisco ASA, Palo Alto, pfSense, Fortinet

25CYU732A SECURING IT INFRASTRUCTURE 4H – 3C

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- Introduce the key components of IT infrastructure and the need for securing them.
- Explain the threats, vulnerabilities, and risk mitigation techniques in IT environments.
- Provide practical knowledge on securing endpoints, servers, networks, and data centers.
- Familiarize students with security frameworks, standards, and best practices.
- Equip learners with skills to implement layered and adaptive security mechanisms.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Identify and analyze security threats to IT infrastructure components.	Understand
CO2	Apply security principles to protect servers, endpoints, and network devices.	Apply
CO3	Configure and manage security controls across infrastructure layers.	Apply
CO4	Evaluate and implement compliance-based security frameworks.	Understand
CO5	Design secure IT infrastructures with appropriate tools and policies.	Analyze

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1	3	3	3	3	-	-	-	-	1	2	3	3	2	1	3
CO2	2	1	3	2	2	-	-	-	1	2	2	3	3	1	3
CO3	3	1	3	3	1	-	-	-	1	2	1	1	1	3	3
CO4	3	2	3	2	1	-	-	-	1	2	2	3	2	2	1
CO5	2	3	3	2	2	-	-	-	1	3	3	2	3	1	3

1 - low, 2 - medium, 3 – high

UNIT I: Introduction to IT Infrastructure Security

Components of IT Infrastructure: Servers, networks, storage, endpoints, Need for securing IT infrastructure, Threats, vulnerabilities, and attack vectors, Risk assessment and management, Security policies and governance

UNIT II: Securing Network Infrastructure

Network access control and segmentation, Firewalls, routers, and switch security, Intrusion detection and prevention systems, VPNs and remote access security, Network monitoring and logging.

UNIT III: Endpoint and Server Security

Endpoint protection: Antivirus, EDR, patch management, Securing Windows and Linux servers, User account and privilege management, Application whitelisting and hardening techniques, Secure configuration management

UNIT IV: Data Center and Cloud Infrastructure Security

Physical security of data centers, Virtualization security (VMs, hypervisors), Securing cloud environments (AWS, Azure, GCP), Identity and access management in the cloud, Cloud security controls and shared responsibility model

UNIT V: Security Standards, Compliance, and Best Practices

Overview of ISO/IEC 27001, NIST, PCI-DSS, HIPAA, Security frameworks and implementation roadmaps,Incident response and disaster recovery planning, Auditing, logging, and continuous monitoring,Case studies on securing enterprise IT infrastructures

SUGGESTED READINGS

1**. Chris Moschovitis**, *Cybersecurity Program Development for Business*, Wiley
2. **Thomas R. Peltier**, *Information Security Policies, Procedures, and Standards*, Auerbach
3**. NIST SP 800-53**, *Security and Privacy Controls for Information Systems*
4. Microsoft, AWS, and Google Cloud Security Documentation
5. Online resources and whitepapers from SANS, ISACA, and OWASP

Vertical - 2 Security Engineer

B.E. / B.Tech. (Common to all Branches) **2025-2026**

25CYU531B **Devops** **4H – 3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

By the end of this course, students will:

1. Understand the need and importance of DevOps in modern software development.
2. Learn about various tools and practices used in the DevOps lifecycle.
3. Apply Continuous Integration and Continuous Deployment (CI/CD) pipelines.
4. Understand containerization using Docker and orchestration with Kubernetes.
5. Implement monitoring and logging to ensure system reliability and performance.

Course Outcomes (COs)

At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Explain the DevOps culture, principles, and benefits in software development.	Apply
CO2	Design and implement automated CI/CD pipelines.	Understand
CO3	Apply version control using Git and GitHub in collaborative environments.	Apply
CO4	Deploy and manage containerized applications using Docker and Kubernetes.	Apply
CO5	Utilize configuration management and infrastructure as code tools like Ansible and Terraform.	Understand

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO8	PO9	PO 10	PO 11	PO 12	PSO1	PSO2	PSO3
CO1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO2	3	3	2	--	--	--	--	--	--	--	--	--	1	2	--	--
CO3	3	3	3	2	2	--	--	--	--	--	--	--	1	2	--	--
CO4	2	2	3	2	2	3	--	--	--	--	--	--	1	2	--	--
CO5	2	2	3	3	3	2	2	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

UNIT I: Introduction to DevOps and Version Control
Evolution of DevOps: Traditional vs DevOps model-DevOps principles: CALMS (Culture, Automation, Lean, Measurement, Sharing)-DevOps lifecycle and automation-Introduction to version control systems-Git basics: in it, clone, commit, push, pull, branches, merge-GitHub/GitLab workflows: feature branching, pull requests-Hands-on: Setting up a GitHub repo and basic Git operations.

UNIT II: Continuous Integration (CI) and Build Automation
Introduction to CI/CD and benefits - Jenkins architecture and setup - Build tools: Maven, Gradle - Jenkins pipelines (Scripted vs Declarative) - Integrating Git with Jenkins - Running test cases and generating reports in CI - Tools: Circle CI, Travis CI (overview) - Hands-on: Build a basic CI pipeline using Jenkins.

UNIT III: Configuration Management and Infrastructure as Code (IaC)
Overview of configuration management-Ansible: Architecture, playbooks, roles, inventory - Introduction to Terraform: Providers, resources, state files - Comparison: Ansible vs Puppet vs Chef - Infrastructure provisioning on AWS/Azure/GCP using Terraform - Hands-on: Write Ansible playbooks and use Terraform for infrastructure setup.

UNIT IV: Containerization and Orchestration
Virtualization vs containerization - Docker basics: Images, containers, Docker file, volumes, networks - Docker Compose and multi-container applications - Container registries: Docker Hub - Kubernetes architecture: Pods, Replica Sets, Deployments, Services – Mini kube and kube ctl commands - Helm charts (basic) - Hands-on: Create and deploy Docker containers and Kubernetes pods.

UNIT V: Monitoring, Logging and Security in DevOps
Importance of monitoring and logging in DevOps - Monitoring tools: Prometheus and Grafana basics - Log management: ELK stack (Elasticsearch, Logstash, Kibana) - Application Performance Monitoring (APM) – Dev Sec Ops: Integrating security in CI/CD pipeline. Common security tools: SonarQube, OWASP ZAP - Hands-on: Setup Prometheus-Grafana dashboard; analyze logs using ELK.

SUGGESTED READINGS:

1. The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations,*Gene Kim, Jez Humble, Patrick Debois, John Willis* IT Revolution Press
2. Accelerate: The Science of Lean Software and DevOps,*Nicole Forsgren, Jez Humble, Gene Kim*, IT Revolution Press
3. Site Reliability Engineering: How Google Runs Production Systems,*Betsy Beyer et al.*, O'Reilly Media
4. The Phoenix Project: A Novel About IT, DevOps, and Helping Your Business Win,*Gene Kim, Kevin Behr, George Spafford*, IT Revolution Press
5. Docker Deep Dive, *Nigel Poulton*, Leanpub / Self-published
6. Kubernetes Up & Running: Dive into the Future of Infrastructure,*Brendan Burns, Joe Beda, Kelsey Hightower*,O'Reilly Media
7. Infrastructure as Code,*Kief Morri,* O'Reilly Media

25CYU532B Security Reporting Dashboards and PowerBI 4H –3C

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives
The course aims to:

1. Understand the principles and techniques for designing security reporting dashboards.
2. Learn data visualization best practices in the context of cybersecurity.
3. Acquire proficiency in Microsoft Power BI for building interactive dashboards.
4. Analyze security event data from various sources and represent it effectively.
5. Integrate Power BI with security information and event management (SIEM) tools.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Explain the need and principles of security reporting in enterprise environments.	Apply
CO2	Design and build interactive dashboards using Microsoft Power BI.	Apply
CO3	Perform data preparation, modeling, and transformation for cybersecurity use cases.	Understand
CO4	Visualize and analyze security log data from systems like firewalls, IDS/IPS, and SIEMs.	Apply
CO5	Integrate Power BI with third-party security tools and cloud services for real-time reporting.	Apply

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO8	PO9	PO 10	PO 11	PO 12	PSO1	PSO2	PSO3
CO1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO2	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO3	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO4	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO5	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 – high

UNIT I: Introduction to Security Reporting and Dashboards
Basics of cybersecurity monitoring and reporting - Importance of dashboards in security operations - Types of security dashboards: Executive, Operational, Technical - Key metrics and KPIs in cybersecurity: incident count, MTTR, threat level, etc - Data sources: Firewalls, IDS/IPS, Endpoint Protection, SIEM (e.g., Splunk, Sentinel) - Principles of effective dashboard design - Case studies on SOC dashboards.

UNIT II: Power BI Fundamentals
Overview of Microsoft Power BI ecosystem: Desktop, Service, Mobile - Power BI interface and components - Data sources and connectors (CSV, Excel, databases, APIs) - Import vs Direct Query - Data transformation using Power Query Editor - Data modeling: relationships, primary/foreign keys, star and snowflake schema - Hands-on: Importing and shaping raw security log data in Power BI.

UNIT III: Data Modeling and DAX for Security Reporting
Introduction to DAX (Data Analysis Expressions) - Measures vs Calculated Columns - Time intelligence functions for trend analysis - Filtering and aggregating log data using DAX - Creating hierarchy fields (date, time, event type) - Role-playing dimensions (e.g., multiple date fields) - Hands-on: Build a security alert dashboard with dynamic filtering and KPIs.

UNIT IV: Visualization and Interactivity
Choosing the right visuals for security data: bar, matrix, gauge, heat maps - Designing real-time alerts dashboards using streaming datasets - Tooltips, slicers, bookmarks, drillthrough and drilldown - Conditional formatting for risk levels and alerts - Creating custom visuals and themes - Power BI security features: row-level security, permissions, and sharing - Hands-on: Create an interactive SOC dashboard with real-time threat indicators.

UNIT V: Integration and Deployment in Security Environments
Connecting Power BI with: Microsoft Sentinel, Azure Security Center, Splunk (via REST APIs or data exports), Syslog / Security Event logs - Gateway configuration for on-premise data sources - Embedding dashboards into portals or web apps - Publishing to Power BI service and scheduling refreshes - Case study: Building a unified threat dashboard for enterprise visibility - Hands-on: Integrate Power BI with a sample security event dataset and deploy.

SUGGESTED READINGS:

1. **Pro Power BI Desktop** by Adam Aspin
   Apress, Latest Edition
2. **Cybersecurity Ops with Bash** by Paul Troncone & Carl Albing
   O'Reilly, 2022 (for log handling and preprocessing)
3. **Practical Power BI** by Devin Knight et al.
   Packt Publishing

25CYU631B Windows Policy Management 4H –3C

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

This course aims to:

1. Understand the principles and architecture of Windows operating systems and domain-based policy management.
2. Learn to configure and manage Group Policy Objects (GPOs) in enterprise environments.
3. Explore security policies, user rights, and advanced policy settings.
4. Apply policy management for secure, automated, and scalable Windows environments.
5. Monitor, troubleshoot, and audit Group Policies and policy enforcement mechanisms.

Course Outcomes (COs)

At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Describe the architecture and components of Windows policy management.	Apply
CO2	Configure and deploy Group Policy Objects (GPOs) for users and computers.	Apply
CO3	Enforce security policies, access control, and auditing using GPOs.	Understand
CO4	Troubleshoot and maintain group policy infrastructure and results.	Apply
CO5	Apply policy management to real-world enterprise-level administrative tasks.	Apply

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO8	PO9	PO 10	PO 11	PO 12	PSO1	PSO2	PSO3
CO1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO2	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO3	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO4	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO5	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

UNIT I: Introduction to Windows Policy Management
Overview of Windows OS architecture. - Introduction to Active Directory (AD) and domain structures - Need for centralized management and policies - Introduction to Group Policy: what, why, and how it works - Local Group Policy vs Domain-based GPOs. - Tools: Group Policy Management Console (GPMC), GPUpdate, Resultant Set of Policy (RSoP) - Overview of GPO processing order and inheritance (LSDOU).

UNIT II: Creating and Managing Group Policy Objects (GPOs)
Understanding GPO scope, precedence, and inheritance - Creating, editing, and linking GPOs to OUs/domains - Group Policy templates: ADM and ADMX - Managing multiple GPOs: backup, restore, import, copy - Filtering policies with Security Groups and WMI filters - Block inheritance and enforce GPO settings - Delegation of GPO management rights - Hands-on: Create and deploy a basic GPO for a department in an AD environment.

UNIT III: Configuring User and Computer Settings
Overview of GPO nodes: Computer Configuration vs User Configuration - Configuring desktop environments: start menu, desktop wallpaper, taskbar, etc - Folder redirection, logon scripts, and startup/shutdown scripts -Software deployment via GPO - Drive mappings and printer deployments - Power settings and network policies - Hands-on: Configure startup scripts and folder redirection policies.

UNIT IV: Security Policies and Enforcement
Windows security settings in Group Policy - Password policies, account lockout, and Kerberos settings - User rights assignment and security options - Software restriction policies (SRP) and AppLocker - Windows Firewall configuration via GPO - BitLocker and encryption policy management - Auditing policies and Event Log settings - Hands-on: Enforce security baselines via GPO.

UNIT V: Troubleshooting, Monitoring, and Best Practices
Understanding Group Policy processing issues - Using RSoP and GP Result for policy diagnostics - Event Viewer and troubleshooting GPO application errors - Replication and latency issues in multi-domain environments - Group Policy performance tuning and delay policies - Using Microsoft Security Compliance Toolkit - Policy design best practices: naming conventions, documentation, testing before deployment.
Case study: Enterprise-wide policy management for a hybrid AD setup.

SUGGESTED READINGS:

1. **Group Policy: Fundamentals, Security, and the Managed Desktop**
   Author: Jeremy Moskowitz
   Publisher: Wiley | Latest Edition
   A comprehensive guide to policy management in Windows environments.

2. **Windows Server 2019 & PowerShell All-in-One For Dummies**
   Author: Sara Perrott, Jeffrey R. Shapiro
   Publisher: Wiley

25CYU632B Malware Analysis and Mitigation Technique 4H –3C

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

This course aims to:

1. Provide in-depth knowledge of malware types, attack vectors, and behaviors.
2. Teach static and dynamic analysis techniques to dissect and understand malware.
3. Explore reverse engineering and memory forensics for advanced analysis.
4. Equip students with practical skills to detect, prevent, and mitigate malware attacks.
5. Introduce modern tools and frameworks used in malware analysis and defense.

Course Outcomes (COs)

At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Identify and classify various types of malware and their attack mechanisms.	Apply
CO2	Apply static and dynamic analysis techniques to analyze malicious binaries.	Apply
CO3	Use reverse engineering and debugging tools to inspect malware behavior	Understand
CO4	Investigate malware using memory forensics and behavior-based detection.	Apply
CO5	Implement mitigation techniques to prevent and contain malware attacks.	Apply

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO8	PO9	PO 10	PO 11	PO 12	PSO1	PSO2	PSO3
CO1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO2	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO3	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO4	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO5	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

UNIT I: Introduction to Malware and Attack Vectors
Definition and objectives of malware - Malware taxonomy: viruses, worms, trojans, ransomware, spyware, adware, rootkits, etc.- Malware lifecycle and infection methods - Attack vectors: phishing, drive-by downloads, USB, macro-based attacks - Command and Control (C2) infrastructure - Real-world malware incidents (e.g., WannaCry, NotPetya, Emotet) -Case Study: Analysis of recent ransomware attack trends

UNIT II: Static Malware Analysis
Overview of static vs dynamic analysis - File formats: PE (Portable Executable), ELF - Tools: PEiD, Exeinfo PE, Dependency Walker - Disassemblers: IDA Free, Ghidra basics - Analyzing strings, metadata, and embedded resources - Signature-based detection: YARA rules, AV signatures - Hashing algorithms: MD5, SHA-256 in malware detection - Hands-on: Perform basic static analysis on malware samples

UNIT III: Dynamic Analysis and Sandboxing
Setting up a safe lab environment (VMs, isolated network, snapshots) - Tools: Cuckoo Sandbox, Any.Run, Procmon, Process Explorer, RegShot - Monitoring file system, registry, and process activity - Network traffic analysis: Wireshark, FakeNet-NG - Behavior analysis and Indicators of Compromise (IOCs) - Anti-analysis techniques used by malware (evasion, obfuscation) - Hands-on: Analyze malware using Cuckoo Sandbox and generate a behavior report

UNIT IV: Reverse Engineering and Memory Forensics
Basics of reverse engineering and debugging - Tools: x64dbg, OllyDbg, Ghidra advanced usage - Understanding malware control flow, function calls, and obfuscated code - Code unpacking and decryption techniques - Memory analysis fundamentals - Tools: Volatility Framework, Rekall - Extracting and analyzing malware from memory dumps -Hands-on: Reverse engineer a packed malware sample and perform memory analysis.

UNIT V: Mitigation Techniques and Defenses
Antivirus and endpoint detection systems (EDR/XDR) - Host-based and network-based protection strategies - Application whitelisting, sandboxing, and behavior-based detection Patching and vulnerability management - Threat intelligence: MITRE ATT&CK framework Incident response: containment, eradication, recovery - Malware prevention best practices: user education, access control
Case study: Mitigation plan for a simulated malware outbreak

SUGGESTED READINGS:

1. "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" By Michael Sikorski and Andrew Honig – No Starch Press
2. "The Art of Memory Forensics" By Michael Hale Ligh, Andrew Case, Jamie Levy, and AAron Walters – Wiley
3. MITRE ATT&CK Framework – https://attack.mitre.org/
4. Online Platforms and Labs:
    - https://malware-traffic-analysis.net/
    - https://www.honeynet.org/

25CYU731B **Security Audit and Risk assessment** **4H –3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

By the end of this course, students will be able to:

1. Understand the concepts of security auditing and risk management in information systems.
2. Learn how to identify, assess, and mitigate security risks.
3. Apply frameworks and standards for security audits (e.g., ISO 27001, NIST).
4. Gain practical skills in designing and conducting security audits.
5. Understand legal, regulatory, and compliance aspects of information security.

Course Outcomes (COs)

At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Describe the fundamental principles of security audits and risk assessments.	Apply
CO2	Analyze risks using qualitative and quantitative assessment methodologies.	Understand
CO3	Design and execute an end-to-end security audit process.	Understand
CO4	Apply security frameworks and standards to real-world scenarios.	Apply
CO5	Evaluate compliance requirements and recommend controls for mitigation.	Understand

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO8	PO9	PO 10	PO 11	PO 12	PSO1	PSO2	PSO3
CO1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO2	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO3	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO4	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO5	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

UNIT I: Introduction to Security Auditing and Risk Assessment

Overview of Information Security - Principles of Security Auditing - Risk Management Concepts - Threats, Vulnerabilities, and Controls - Risk Identification and Risk Analysis - Security Policies and Procedures

UNIT II: Security Audit Planning and Methodologies

Audit Planning and Preparation - Types of Audits: Internal, External, Compliance, Technical - Defining Scope and Objectives -Audit Checklist Development -Audit Methodologies: COBIT, ISO 27001, NIST SP 800-53 - Documentation and Evidence Collection

UNIT III: Risk Assessment and Analysis Techniques

Risk Assessment Methodologies: Qualitative, Quantitative, Hybrid - Risk Matrix and Heat Maps -Asset Valuation and Risk Calculations - Business Impact Analysis (BIA) - Threat Modeling and Vulnerability Assessment - Residual Risk and Risk Treatment Plans -

UNIT IV: Security Control Evaluation and Audit Execution

Technical Controls (Firewalls, IDS/IPS, Encryption, Authentication) - Physical and Administrative Controls - Audit Tools and Techniques (Nessus, Nmap, Wireshark, SIEM) - Log Analysis and Monitoring - Incident Response Auditing - Audit Report Writing and Presentation

UNIT V: Legal, Ethical, and Compliance Aspects

Legal and Regulatory Requirements (GDPR, HIPAA, PCI-DSS) - Ethics in Information Security - Governance, Risk, and Compliance (GRC) - Data Privacy and Protection Laws - Business Continuity and Disaster Recovery Planning - Case Studies and Best Practices.

SUGGESTED READINGS:

1.Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis
– Douglas J. Landoll, Syngress

2.IT Security Risk Control Management: An Audit Preparation Plan
– Raymond Pompon, Apress

25CYU732B **Security Incident Response and Management** **4H –3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

The course aims to:

1. Introduce the principles and frameworks of incident response.
2. Enable students to identify, classify, and analyze different types of security incidents.
3. Equip learners with practical skills for handling real-time security incidents.
4. Discuss tools and technologies used in incident detection and management.
5. Explore post-incident activities such as root cause analysis, reporting, and improvements.

Course Outcomes (COs)

At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Explain key concepts and lifecycle stages of incident response.	Apply
CO2	Detect and analyze different types of security incidents.	Apply
CO3	Design and implement effective incident response plans.	Understand
CO4	Use forensic and analytical tools for incident investigation.	Apply
CO5	Evaluate and report on incidents and apply lessons learned for continuous improvement.	Apply

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO8	PO9	PO 10	PO 11	PO 12	PSO1	PSO2	PSO3
CO1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO2	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO3	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO4	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO5	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

UNIT I: Introduction to Security Incidents and Response

Definition and Types of Security Incidents - Common Causes of Security Incidents - Phases of Incident Response Lifecycle - Organizational Roles in Incident Response - Establishing an Incident Response Capability (IRC) - Incident Classification and Severity Levels - Indicators of Compromise (IoC)

UNIT II: Preparation and Detection

Incident Response Planning and Policy Development - Creating an Incident Response Team (IRT/CSIRT) - Detection Mechanisms: IDS, IPS, SIEM, Honeypots - Log Management and Monitoring - Threat Intelligence and Data Sources - Use of MITRE ATT&CK Framework - Detecting Insider Threats and APTs

UNIT III: Incident Analysis and Containment

Techniques for Analyzing Malware and Suspicious Activities - Triage and Incident Prioritization - Network Forensics and Packet Analysis - Containment Strategies: Short-term and Long-term - Host Isolation and Network Segmentation - Legal and Ethical Considerations during Containment

UNIT IV: Eradication, Recovery, and Post-Incident Activities

Eradication of Malware and Removing Persistence Mechanisms - System and Data Recovery Procedures - Patch Management and Secure Re-imaging - Evidence Collection and Chain of Custody - Root Cause Analysis (RCA) - Post-Incident Review and Reporting - Metrics for Measuring Response Effectiveness

UNIT V: Legal, Compliance, and Case Studies

Legal Framework and Regulatory Requirements (e.g., GDPR, HIPAA, PCI-DSS) - Industry Standards: NIST SP 800-61, ISO/IEC 27035 - Incident Disclosure and Communication Protocols - Public Relations and Media Management during Incidents Case Studies: NotPetya, SolarWinds, Equifax, Target Breach - Emerging Trends in Incident Response (AI/ML, SOAR)

SUGGESTED READINGS:

1. Computer Security Incident Handling Guide (NIST SP 800-61 Revision 2)
   – National Institute of Standards and Technology (Free and Authoritative)
2. Incident Response & Computer Forensics (3rd Edition)
   – Jason Luttgens, Matthew Pepe, Kevin Mandia – McGraw Hill

Vertical 3 - IAM Engineer

B.E. / B.Tech. (Common to all Branches) **2025-2026**

25CYU531C **Enterprise ID and Access Management** **4H –3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

By the end of this course, students will be able to:

1. Understand the core principles and components of Identity and Access Management (IAM) in enterprise environments.
2. Analyze the architecture and operational mechanisms of IAM solutions.
3. Learn directory services, access controls, authentication, and authorization.
4. Explore real-world enterprise IAM implementations using tools like Active Directory, LDAP, and cloud IAM.
5. Gain practical skills in IAM governance, compliance, and risk management.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Explain the fundamentals of IAM, including identification, authentication, and authorization mechanisms.	Apply
CO2	Analyze different access control models and their application in enterprise environments.	Apply
CO3	Implement directory-based IAM systems using LDAP and Microsoft Active Directory.	Understand
CO4	Evaluate and configure federated identity management and Single Sign-On (SSO) mechanisms.	Apply
CO5	Apply IAM governance policies and regulatory compliance in enterprise settings.	Apply

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO 1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 2	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 3	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 4	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 5	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

Unit I : **Introduction to IAM**

Definition, Importance of IAM in Enterprise Security-Components of IAM: Identification, Authentication, Authorization-IAM lifecycle: Provisioning, De-provisioning-Identity Federation and Trust Models-IAM Standards: SAML, OAuth, OpenID Connect, SCIM

Unit II : Access Control Models and Authentication

Access Control: Discretionary (DAC), Mandatory (MAC), Role-Based (RBAC), Attribute-Based (ABAC)-Multifactor Authentication (MFA), Password Policies-Biometrics, Tokens, Smart Cards-Authentication Protocols: Kerberos, RADIUS, TACACS+

Unit III : **Directory Services and Identity Stores**

LDAP: Concepts, Schema, Queries-Microsoft Active Directory: Domains, Forests, Trusts-Integration of applications with directories-Identity Synchronization and Provisioning

Unit IV : **Federation, SSO, and Cloud IAM**

Identity Federation Architecture-SSO concepts and implementation-Federation Protocols: SAML 2.0, OAuth 2.0, OpenID Connect-IAM in Cloud Environments: AWS IAM, Azure AD, Google Cloud IAM

Unit V : IAM Governance, Risk, and Compliance

IAM Policy Framework and Best Practices-Governance Tools: Access Reviews, Role Mining-Compliance Requirements: GDPR, HIPAA, SOX-Case Studies: IAM failures and mitigation strategies

SUGGESTED READINGS:

- *Identity and Access Management: Business Performance Through Connected Intelligence* by Ertem Osmanoglu
- *Digital Identity* by Phillip J. Windley
- *Cloud Security and Privacy* by Tim Mather, Subra Kumaraswamy, and Shahed Latif
- Microsoft, AWS, Google documentation on IAM

25CYU532C **Identity and Digital Certificate** **4H –3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

This course aims to:

1. Introduce the concept of digital identity in secure communication and e-authentication systems.
2. Provide knowledge of cryptographic methods used in identity management.
3. Explain the role and functioning of digital certificates and Public Key Infrastructure (PKI).
4. Analyze real-world identity validation systems and certificate lifecycle management.
5. Emphasize regulatory, legal, and privacy frameworks related to digital identities.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Understand the concept of digital identity and its significance in modern communication systems.	Apply
CO2	Apply cryptographic techniques in identity creation and validation.	Apply
CO3	Analyze the architecture and working of digital certificates and PKI.	Understand
CO4	Evaluate identity management frameworks and digital certificate lifecycle processes.	Apply
CO5	Understand compliance, privacy, and regulatory aspects associated with digital identity and certificates.	Apply

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO 1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 2	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 3	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 4	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 5	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

Unit I: Introduction to Identity and Authentication
Digital identity: definition, components, and lifecycle-Identity proofing and credential issuance-Authentication vs Authorization-Identity models: centralized, federated, decentralized-Identity threats: impersonation, spoofing, phishing

.

Unit II : **Cryptography Fundamentals for Identity**
Symmetric and Asymmetric Encryption-Hash functions and digital signatures-Key generation and key management-Role of cryptography in identity verification-Cryptographic protocols for secure identity management

Unit III: Digital Certificates and PKI
Digital certificates: X.509 format and structure-Certification Authorities (CAs) and Registration Authorities (RAs)-Certificate generation, renewal, and revocation-PKI Architecture and Certificate Policies-Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP)

Unit IV: Identity Management Systems and Applications
Certificate-based Authentication-Role of smart cards, tokens, and biometrics-Identity Federation and SSO (Single Sign-On)-IAM solutions using digital certificates (LDAP, Active Directory)-Case studies: Aadhaar, e-passport, Banking PKI systems

Unit V: Legal, Privacy, and Compliance Framework
Digital identity and privacy: GDPR, HIPAA-Digital signature laws: IT Act 2000 (India), eIDAS (EU)-Trust frameworks and policy enforcement-Risk analysis in digital certificate deployment-Future trends: Blockchain identity, Self-sovereign identity

SUGGESTED READINGS:

- *Understanding PKI: Concepts, Standards, and Deployment Considerations* by Carlisle Adams and Steve Lloyd
- *Digital Identity* by Phillip J. Windley
- *Handbook of Digital and Multimedia Forensics* by John Vacca
- Official standards: RFC 5280 (X.509), NIST Digital Identity Guidelines
- Government frameworks: Aadhaar Technical Specs, eIDAS Regulations

25CYU631C Identity and Access Management Protocols and Standards **4H –3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

The course aims to:

1. Understand the core concepts and need for identity and access management (IAM).
2. Learn various industry-standard IAM protocols like SAML, OAuth, OpenID Connect, and Kerberos.
3. Explore directory services and federation standards used for identity integration.
4. Examine the implementation and interoperability challenges in real-world IAM systems.
5. Emphasize security, compliance, and best practices in IAM protocol deployment.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Explain the fundamentals and components of identity and access management systems.	Apply
CO2	Analyze and apply industry-standard authentication and authorization protocols.	Apply
CO3	Evaluate directory services and identity federation standards.	Understand
CO4	Demonstrate the implementation and configuration of IAM protocols in enterprise scenarios.	Apply
CO5	Assess compliance, security, and integration challenges in IAM systems.	Apply

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 8	PO 9	PO1 0	PO1 1	PO 12	PS O1	PS O2	PS O3
CO 1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 2	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 3	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 4	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 5	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

Unit I : **Foundations of Identity and Access Management**
Definition of IAM and its role in enterprise security-Core components: Authentication, Authorization, Accounting (AAA)-Identity lifecycle management-Types of identities: User, Application, Device-Centralized, federated, and decentralized identity models

.

Unit II : **Authentication Protocols**
Password-based authentication and limitations-Multi-factor authentication (MFA)-Kerberos: Protocol flow, tickets, KDC-RADIUS and TACACS+: use in network security-Modern authentication frameworks

Unit III : **Authorization and Federation Protocols**
SAML 2.0: Assertions, bindings, metadata, use cases-OAuth 2.0: Roles (client, resource owner, etc.), flows (Auth Code, Implicit, etc.)-OpenID Connect: ID token, scopes, claims-Identity Federation: Trust establishment and use cases-Comparison of OAuth vs OIDC vs SAML

Unit IV : Directory Services and Identity Stores
Lightweight Directory Access Protocol (LDAP)-Microsoft Active Directory (AD) structure and replication-Integrating IAM with AD and LDAP-Directory schema design and search operations-Cloud-based directory services: Azure AD, AWS IAM

Unit V : Security, Compliance, and IAM Standards
Identity Governance and Administration (IGA)-Standards and Frameworks: SCIM, XACML, NIST 800-63-Compliance: GDPR, HIPAA, SOX in IAM context-Identity Threat Detection and Mitigation-Best practices in protocol implementation and interoperability

SUGGESTED READINGS:

- Identity and Access Management: Business Performance Through Connected Intelligence by Ertem Osmanoglu
- Digital Identity by Phillip J. Windley
- Cloud Security and Privacy by Tim Mather, Subra Kumaraswamy, and Shahed Latif
- Microsoft, AWS, Google documentation on IAM

B.E. / B.Tech. (Common to all Branches) **2025-2026**

25CYU632C Cybercrimes and Digital Forensics 4H –3C

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

The objectives of this course are to:

1. Understand the nature, classification, and growth of cybercrimes in the digital age.
2. Study legal frameworks, IT laws, and the role of law enforcement in cybercrime control.
3. Gain knowledge about digital forensics processes, tools, and techniques.
4. Analyze procedures for collecting, preserving, and analyzing digital evidence.
5. Examine case studies of cybercrimes and forensic investigations to understand practical aspects.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Explain various types of cybercrimes and their legal implications.	Apply
CO2	Understand national and international cyber laws and their enforcement.	Apply
CO3	Apply digital forensic techniques to collect and analyze electronic evidence.	Understand
CO4	Use forensic tools for examining file systems, networks, emails, and mobile devices.	Apply
CO5	Analyze real-world cybercrime cases and prepare investigation reports.	Apply

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO 1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 2	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 3	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 4	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 5	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

Unit I: Introduction to Cybercrimes
Definition and origin of cybercrime-Classification of cybercrimes: hacking, phishing, identity theft, cyber terrorism, etc-Causes and motives behind cybercrimes-Cybercrime tools and methods-Cyberstalking, cyberbullying, online frauds-Cybercrime against individuals, property, and government.

Unit II: Cyber Laws and Legal Frameworks
Overview of Indian IT Act 2000 and amendments-Legal aspects of cybercrimes: jurisdiction and admissibility-Cybercrime regulations in USA (CFAA), EU (GDPR, ePrivacy), and other countries-Role of CERT-IN, Interpol, and other law enforcement agencies-Challenges in enforcing cyber laws-Intellectual property issues in cyberspace-Digital signature and electronic evidence laws.

Unit III: Introduction to Digital Forensics
Digital Forensics: Definition, objectives, and process-Types of digital forensics: Computer, Network, Mobile, Email-Chain of custody and evidence handling-Forensic acquisition methods: disk imaging, live vs dead analysis-Legal admissibility of digital evidence-Forensic analysis standards: ISO/IEC 27037.

Unit IV: Digital Forensic Techniques and Tools
File system analysis: FAT, NTFS, ext3/ext4-Memory forensics and volatile data acquisition-Email and browser forensics-Network forensics: sniffing, packet analysis, logs-Mobile device *forensics: Android and iOS tools-Popular tools: FTK, Autopsy, EnCase, Wireshark, Cellebrite.*

Unit V:Case Studies and Reporting
Investigating cyber fraud and financial scams-Insider threats and data leakage investigations-Ransomware attack investigations-Real-life cybercrime case studies: analysis and methodology-Report writing and presenting digital forensic findings-Ethics, privacy, and legal responsibilities in forensic practice-Trends in cybercrime and future challenges.

SUGGESTED READINGS:

1. *Cyber Crime and Digital Evidence* by Sumit Belapure and Nina Godbole
2. *Guide to Computer Forensics and Investigations* by Bill Nelson, Amelia Phillips, Christopher Steuart
3. *Cybersecurity and Cyber Laws* by Alfred Basta, Nadine Basta
4. *Digital Forensics with Kali Linux* – Shiva V. N. Parasram
5. Indian IT Act, 2000 with Amendments
6. NIST SP 800-101: Guidelines on Mobile Device Forensics
7. CERT-IN advisories and forensic manuals

B.E. / B.Tech. (Common to all Branches) **2025-2026**

25CYU731C **IT Service Delivery** **4H –3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

This course aims to:

1. Provide an understanding of the concepts and principles of IT service delivery and management.
2. Introduce ITIL framework and its components for service strategy, design, transition, operation, and continual improvement.
3. Enable students to plan and implement IT services aligned with business goals.
4. Cover key processes such as incident, problem, change, and service-level management.
5. Highlight tools, metrics, governance, and best practices for delivering reliable and secure IT services.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Explain the fundamental concepts and lifecycle of IT service delivery using frameworks like ITIL.	Apply
CO2	Identify and describe key processes involved in IT service strategy, design, and transition.	Apply
CO3	Apply service operation practices including incident, problem, and access management.	Understand
CO4	Evaluate service-level agreements (SLAs), capacity, availability, and IT continuity management.	Apply
CO5	Analyze real-world scenarios and suggest service improvement strategies using KPIs and metrics.	Apply

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 8	PO 9	PO10	PO11	PO 12	PS O1	PS O2	PS O3
CO 1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 2	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 3	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 4	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 5	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

Unit I: Introduction to IT Service Management and ITIL
Definition of IT Service and Service Management-Need for IT Service Delivery in enterprises-Overview of ITIL (v3 & 4) framework-IT Service Lifecycle: Strategy, Design, Transition, Operation, CSI-Benefits and challenges of implementing ITIL-Overview of other frameworks: COBIT, ISO 20000, MOF.

Unit II: Service Strategy and Design
Service Strategy: Business value, service portfolio, demand and financial management-Service Design: Design coordination, service catalog, service level management (SLM)-Availability, Capacity, and Continuity Management-Information security management in service design-Supplier management and outsourcing considerations.

Unit III: Service Transition
Purpose and scope of service transition-Change management: process, roles, types-Release and deployment management-Knowledge management: data-information-knowledge-wisdom hierarchy-Service asset and configuration management (CMDB)-Transition planning and support.

Unit IV: Service Operation
Event management and monitoring tools-Incident management: priorities, SLAs, ticketing tools-Problem management: root cause analysis, proactive vs reactive-Access management and request fulfillment-Operational control and facilities management-Service desk roles, metrics, and types.

Unit V: Continual Service Improvement (CSI) and Governance
CSI lifecycle and 7-step improvement process-Key Performance Indicators (KPIs) and metrics for CSI-Maturity models and benchmarking-IT governance and compliance (ISO/IEC 20000, SOX, GDPR)-Integration of Agile/DevOps with ITSM-Case studies: Banking, Healthcare, and Cloud-based service delivery.

SUGGESTED READINGS:

- *ITIL Foundation Exam Study Guide* – Liz Gallacher & Helen Morris
- *Foundations of IT Service Management* – Jan van Bon (Van Haren Publishing)
- *Service Management for Dummies* – Judith Hurwitz
- ITIL v4 Official Documentation – AXELOS
- ISO/IEC 20000: IT Service Management Standard
- COBIT 5 Framework – ISACA
- ITSM tools documentation: ServiceNow, BMC Remedy, JIRA Service Management

25CYU732C **Legal, Ethical, and Social Issues in Information Security** **4H –3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

The course aims to:

1. Introduce the legal frameworks governing information security and data protection.
2. Discuss ethical theories, principles, and their application in cybersecurity decision-making.
3. Analyze social implications of surveillance, privacy, and digital rights.
4. Understand intellectual property laws, cybercrime legislation, and liability concerns.
5. Enable students to evaluate current issues and case studies in cybersecurity from a legal, ethical, and societal perspective.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Describe the legal environment affecting information security and data protection.	Apply
CO2	Apply ethical principles to decision-making in cybersecurity contexts.	Apply
CO3	Analyze social concerns such as digital privacy, surveillance, and online behavior.	Understand
CO4	Interpret and evaluate national and international laws related to cybercrime and IP rights.	Apply
CO5	Evaluate ethical dilemmas and legal issues through real-world information security case studies.	Apply

CO-PO Mapping

CO / PO	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 8	PO 9	PO10	PO11	PO 12	PSO1	PSO2	PSO3
CO 1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 2	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 3	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 4	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO 5	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

Unit I : **Introduction to Legal and Ethical Foundations**
Information security concepts and legal requirements-Cyberlaw: scope and need-Professional ethics in IT: integrity, confidentiality, accountability-Ethical theories: utilitarianism, deontology, virtue ethics-Code of ethics: ACM, IEEE, $(ISC)^2$.

Unit II : **Information Security and Data Protection Laws**
Indian IT Act 2000 and its amendments-Data protection laws: GDPR, HIPAA, CCPA-Legal issues in data breaches, identity theft, and online fraud-Electronic contracts and digital signatures-Legal admissibility of digital evidence-Jurisdictional challenges in cyberspace

Unit III : **Intellectual Property and Cybercrime**
Copyright, trademarks, patents in the digital age-Software licensing: open-source vs proprietary-Cybercrime classification: financial, social, political-Laws against hacking, malware distribution, cyberstalking-Digital piracy, plagiarism, and enforcement-International treaties: WIPO, TRIPS

Unit IV : **Ethical and Social Issues in Information Security**
Surveillance vs privacy: legal and ethical dilemmas-Social engineering and human factor in cybersecurity-Workplace monitoring and employee rights-Net neutrality and censorship-Algorithmic bias, AI ethics, and data ethics-Impact of social media and misinformation.

Unit V : Case Studies and Global Perspectives
Case Study 1: Facebook– Cambridge Analytical-Case Study 2: Ransomware and Corporate Liability- Case Study 3: Aadhaar and biometric privacy in India - Cyberwarfare and state-sponsored attacks-Ethics in cybersecurity research (e.g., responsible disclosure)- Global cooperation in cybersecurity and law enforcement

SUGGESTED READINGS:

- *Cyberlaw: The Indian Perspective* – Pavan Duggal
- *Computer Security: Principles and Practice* – William Stallings
- *Ethics in Information Technology* – George Reynolds
- *Cybersecurity and Cyberlaw* – Alfred Basta, Nadine Basta
- Indian IT Act, 2000 (updated)
- General Data Protection Regulation (GDPR)
- ACM/IEEE Codes of Ethics
- CERT-IN and NIST Cybersecurity Framework

Vertical List 4 – Security Developer

B.E. / B.Tech. (Common to all Branches) **2025-2026**

5CYU531D **Secure Coding** **4H –3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

- By the end of this course, students will be able to:
- Understand the principles of secure software development and threats posed by insecure coding practices.
- Learn to identify and mitigate common security vulnerabilities in code.
- Apply secure coding practices in modern programming languages.
- Understand secure design and architecture patterns in software development.
- Evaluate and apply tools for secure software analysis and testing..

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Explain common software vulnerabilities and their exploitation.	Apply
CO2	Identify insecure coding patterns in programs and suggest fixes.	Understand
CO3	Apply secure programming techniques to mitigate security risks.	Apply
CO4	Use tools for static and dynamic code analysis to find vulnerabilities.	Apply
CO5	Demonstrate secure software design principles and threat modeling.	Understand

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO8	PO9	PO 10	PO 11	PO 12	PSO1	PSO2	PSO3
CO1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO2	3	3	2	--	--	--	--	--	--	--	--	--	1	2	--	--
CO3	3	3	3	2	2	--	--	--	--	--	--	--	1	2	--	--
CO4	2	2	3	2	2	3	--	--	--	--	--	--	1	2	--	--
CO5	2	2	3	3	3	2	2	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

Unit I: Introduction to Secure Coding and Software Security
Software security fundamentals and goals - Importance of secure coding practices - Software Development Life Cycle (SDLC) and Security - Common causes of software vulnerabilities - Case studies: Real-world software security failures - Overview of OWASP Top 10

Unit II – Common Coding Vulnerabilities
Buffer Overflows - Integer Overflows and Underflows - Format String Vulnerabilities-Command Injection, SQL Injection-Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF)-Insecure Deserialization-Broken Authentication and Session Management-Directory Traversal and Path Manipulation

Unit III :Secure Programming Techniques
Input validation and output encoding-Secure memory management-Exception and error handling-Use of secure APIs-Cryptographic principles in secure coding-Secure session and cookie handling-Logging and auditing securely-Defensive programming and code robustness

Unit IV:Secure Software Design and Architecture
Principles of secure design (least privilege, defense in depth)-Threat modeling (STRIDE, DREAD)-Attack surface reduction-Secure design patterns (e.g., input sanitation, sandboxing)-Secure use of authentication, authorization mechanisms-Secure data storage and transmission-Software assurance and risk assessment

Unit V: Tools and Techniques for Secure Code Analysis
Static Analysis Tools (e.g., SonarQube, Coverity)-Dynamic Analysis Tools (e.g., Valgrind, AFL)-Fuzz Testing-Secure code review process-Penetration testing overview-CI/CD integration for secure coding-DevSecOps principles

SUGGESTED READINGS:
1. Michael Howard, David LeBlanc – Writing Secure Code, Microsoft Press.
2. Mark G. Graff, Kenneth R. van Wyk – Secure Coding: Principles & Practices, O'Reilly.
3. OWASP Foundation – OWASP Top 10 Project (https://owasp.org/www-project-top-ten/)
4. Robert C. Seacord – Secure Coding in C and C++, Addison-Wesley.
5. NIST Secure Software Development Framework (SSDF)

25CYU631D **API Security** **4H –3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

This course aims to:

1. Understand the fundamentals of APIs and their security implications.
2. Learn about threats, vulnerabilities, and attack vectors specific to APIs.
3. Apply authentication, authorization, and encryption techniques to secure APIs.
4. Use industry standards and best practices (e.g., OAuth2, OpenID Connect, JWT).
5. Perform threat modeling, testing, and implement secure API development strategies.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Explain API architectures, types, and security fundamentals.	Apply
CO2	Identify common vulnerabilities and attacks on APIs and mitigation techniques.	Apply
CO3	Implement secure authentication and authorization for APIs.	Understand
CO4	Use modern API security standards such as OAuth2, JWT, and OpenID Connect.	Apply
CO5	Apply secure design, testing, and monitoring practices to APIs.	Apply

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO8	PO9	PO 10	PO 11	PO 12	PSO1	PSO2	PSO3
CO1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO2	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO3	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO4	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO5	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

Unit I: Introduction to APIs and Security Basics
What is an API? Types (REST, SOAP, Graph QL)-API lifecycle and architecture-Differences between web application and API security-Common API data formats (JSON, XML)-Role of HTTP methods (GET, POST, PUT, DELETE)-Introduction to API Security and OWASP API Security Top 10-Attack surface in APIs.

Unit II: API Vulnerabilities and Attacks
Injection attacks (SQL, XML, Command injection)-Broken Object Level Authorization (BOLA)-Broken Function Level Authorization (BFLA)-Excessive data exposure and mass assignment-Rate limiting and abuse-Cross-Site Scripting (XSS) and CORS misconfiguration-API key leakage and session hijacking-Case studies of real-world API breaches

Unit III: API Authentication and Authorization
Basic Auth, API Keys, Bearer Tokens-Role-Based Access Control (RBAC)-Attribute-Based Access Control (ABAC)-OAuth 2.0 and its grant types (Authorization Code, Client Credentials)-OpenID Connect and single sign-on (SSO)-JSON Web Tokens (JWT): structure, signing, validation-Token expiration, refresh, and revocation

Unit IV: Secure API Design and Best Practices
Secure coding practices for API development-Input validation, output encoding, and schema validation (JSON schema)-Rate limiting and throttling-CORS configuration and same-origin policy-API gateways and firewalls-Secure logging, auditing, and monitoring-Zero Trust for APIs-Versioning and backward compatibility

Unit V: API Security Testing and Monitoring
Static and dynamic API security testing (SAST, DAST)-API fuzzing and penetration testing-Postman for API testing-Tools: OWASP ZAP, Burp Suite, Postman Security, Insomnia-Threat modeling with STRIDE for APIs-Real-time monitoring and alerting-CI/CD integration for secure API deployments-DevSecOps practices for API lifecycle

SUGGESTED READINGS:

1. Prabath Siriwardena – Advanced API Security, Apress.
2. Phil Sturgeon – Designing APIs with Swagger and OpenAPI.
3. Kudzanai Manditereza – Hands-On API Security.
4. OWASP Foundation – OWASP API Security Top 10 (https://owasp.org/www-project-api-security/)
5. NIST SP 800-204 – Security Strategies for Microservices and APIs

***B*.E. / B.Tech. (Common to all Branches)** **2025-2026**

25CYU632D **Advanced Java Programming** **4H –3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

The course aims to:

1. Provide an understanding of Java programming fundamentals and object-oriented concepts.
2. Develop the ability to create robust, efficient, and portable Java applications.
3. Introduce core libraries, exception handling, multithreading, and collections in Java.
4. Enable GUI application development using AWT and Swing.
5. Explore file handling, networking, and database connectivity in Java.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Understand Java fundamentals and apply OOP concepts in Java programs.	Apply
CO2	Develop Java applications using classes, interfaces, packages, and exception handling.	Apply
CO3	Apply multithreading and collections to build efficient programs.	Understand
CO4	Design GUI-based applications using AWT and Swing.	Apply
CO5	Implement file I/O, network communication, and JDBC-based database applications.	Apply

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO8	PO9	PO 10	PO 11	PO 12	PSO1	PSO2	PSO3
CO1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO2	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO3	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO4	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO5	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

Unit I –Java Fundamentals and Object-Oriented Programming
History and features of Java-Java Virtual Machine (JVM), Bytecode-Data types, variables, operators, control structures-Classes and objects, methods, constructors-Access specifiers, static and final keywords-Inheritance, method overloading and overriding-Abstract classes and interfaces-Encapsulation and polymorphism-'this' and 'super' keywords

Unit II –Packages, Exception Handling, and Strings
Creating and using packages-Java API packages: java.lang, java.util, java.io-Exception handling: try-catch, throw, throws, finally-Built-in and user-defined exceptions-String and StringBuffer classes-Wrapper classes and auto-boxing/unboxing-Assertions and debugging techniques

Unit III - Multithreading and Collections Framework
Threads: life cycle and thread class-Runnable interface and thread synchronization-Inter-thread communication-Thread priorities and daemon threads-Java Collections Framework: List, Set, Map-ArrayList, LinkedList, HashSet, TreeSet, HashMap-Generics in Java-Iterator and ListIterator

Unit IV –GUI Programming with AWT and Swing
AWT components: Button, Label, TextField, TextArea, Checkbox, Choice-Layout managers: FlowLayout, BorderLayout, GridLayout-Event handling: ActionEvent, MouseEvent, KeyEvent-Delegation event model-Swing components: JFrame, JButton, JTextField, JTable, JList-Creating menus using JMenuBar-Dialogs and popups-Applets and parameter passing

Unit V – File Handling, Networking, and JDBC
File streams: FileInputStream, FileOutputStream-Object serialization and deserialization-Reader and Writer classes-Java networking: InetAddress, Socket, ServerSocket, DatagramSocket-URL and HttpURLConnection-Introduction to JDBC-Connecting to databases, executing queries, PreparedStatement-Transaction management and metadata

SUGGESTED READINGS:

1. Herbert Schildt – Java: The Complete Reference, McGraw-Hill.
2. E. Balagurusamy – Programming with Java, McGraw-Hill.
3. Kathy Sierra, Bert Bates – Head First Java, O'Reilly.
4. Bruce Eckel – Thinking in Java, Prentice Hall.
5. Oracle Java Documentation – https://docs.oracle.com/en/java/

B.E. / B.Tech. (Common to all Branches) **2025-2026**

25CYU731D **Ethical Hacking** **4H –3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

The objectives of this course are to:

1. Introduce the fundamental principles, tools, and techniques of ethical hacking.
2. Enable students to understand vulnerabilities and attack vectors across networks, systems, and applications.
3. Provide hands-on exposure to reconnaissance, scanning, enumeration, and exploitation techniques.
4. Explore system and web application security through penetration testing and defensive strategies.
5. Develop ethical awareness and professional responsibility in cybersecurity practice.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Explain the concepts, types, and legal aspects of ethical hacking.	Apply
CO2	Perform information gathering, scanning, and enumeration to discover vulnerabilities.	Apply
CO3	Exploit system and network vulnerabilities using penetration testing tools.	Understand
CO4	Identify and exploit common web application vulnerabilities.	Apply
CO5	Apply defensive techniques and recommend countermeasures to mitigate threats.	Apply

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO8	PO9	PO 10	PO 11	PO 12	PSO1	PSO2	PSO3
CO1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO2	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO3	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO4	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO5	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

Unit I : Introduction to Ethical Hacking and Cybersecurity

Overview of hacking, hacker types (white, black, gray)-Ethical hacking vs penetration testing-Phases of ethical hacking-Cybercrime and cyber laws-Responsibilities of an ethical hacker-Security audit process and compliance (ISO, PCI-DSS)-Virtualization and lab setup for ethical hacking.

Unit II : **Foot printing, Scanning, and Enumeration**

Foot printing techniques: Active, passive, and open-source intelligence (OSINT)-WHOIS, DNS interrogation, Google hacking-Scanning networks: Port scanning, ping sweep, IP sweep-Tools: Nmap, Net cat, Hping3-Banner grabbing and OS fingerprinting-Enumeration of users, services, and shares-Network mapping and vulnerability assessment.

Unit III*:* System Hacking and Malware Analysis

Password cracking techniques: brute-force, dictionary, rainbow tables-Privilege escalation and backdoor installation-Keyloggers, rootkits, spyware, trojans-Steganography and steganalysis-Covering tracks: log tampering, clearing traces-Sniffing attacks and ARP poisoning-Tools: John the Ripper, Cain & Abel, Metasploit.

Unit IV: Web Application and Wireless Hacking

Web architecture and attack surface-SQL injection, Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF)-Command injection, insecure direct object references-Security misconfigurations and file inclusion attacks-Tools: Burp Suite, OWASP ZAP-Wireless network vulnerabilities-WEP/WPA cracking, rogue access points, Evil Twin attack.

Unit V: Defensive Techniques and Countermeasures

Intrusion Detection and Prevention Systems (IDS/IPS)-Firewalls, honeypots, and security policies-Endpoint and antivirus solutions-Patch management and system hardening-Secure coding practices-Penetration testing process and report writing-Case studies of real-world cyber attacks and mitigations-Legal and ethical responsibilities of security professionals.

SUGGESTED READINGS:

1. *William Stallings – Computer Security: Principles and Practice, Pearson.*
2. *CEH Official Study Guide – EC-Council.*
3. *Patrick Engebretson – The Basics of Hacking and Penetration Testing, Syngress.*
4. *OWASP – Web Application Security Project (https://owasp.org)*
5. *Kali Linux Documentation – https://www.kali.org/docs/*

B.E. / B.Tech. (Common to all Branches) **2025-2026**

25CYU732D **Agile and Scrum** **4H –3C**

Instruction Hours / week: L: 3 T: 0 P: 0 **Marks:** Internal: **40** External: **60** Total: **100**
End Semester Exam: 3 Hours

Course Objectives

This course aims to:

1. Introduce the fundamental concepts and values of Agile software development.
2. Understand the Scrum framework including its roles, artifacts, and ceremonies.
3. Explore Agile planning, estimation, and product backlog management techniques.
4. Apply Scrum practices through simulations or real-world Agile projects.
5. Evaluate Agile adoption challenges, metrics, and continuous improvement practices.

Course Outcomes (COs)
At the completion of the course the student will be able to

COs	Course Outcomes	Blooms Level
CO1	Explain the principles, values, and benefits of Agile methodologies.	Apply
CO2	Describe the Scrum framework, roles, events, and artifacts..	Apply
CO3	Apply Agile planning and estimation techniques like user stories, story points, and velocity	Understand
CO4	Implement Scrum in software development projects through simulations or case studies.	Apply
CO5	Analyze Agile metrics and evaluate process improvement strategies for Agile adoption.	Apply

CO-PO Mapping

CO / PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO8	PO9	PO 10	PO 11	PO 12	PSO1	PSO2	PSO3
CO1	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO2	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO3	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO4	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--
CO5	3	2	--	--	--	--	--	--	--	--	--	--	1	2	--	--

1 - low, 2 - medium, 3 - high

Unit I : Agile Software Development Fundamentals

History and evolution of Agile-The Agile Manifesto: Values and principles-Agile vs. Traditional methodologies (Waterfall, V-model)-Benefits and challenges of Agile-Agile process models: Scrum, XP, Kanban, Lean, SAFe-Agile mindset and cultural shift-Agile tools overview (JIRA, Trello, Asana).

Unit II: Scrum Framework in Depth

Overview of Scrum and its significance-Scrum roles: Product Owner, Scrum Master, Development Team-Scrum artifacts: Product Backlog, Sprint Backlog, Increment-Scrum events: Sprint, Sprint Planning, Daily Scrum, Sprint Review, Sprint Retrospective-Definition of Done (DoD), Definition of Ready (DoR)-Scrum of Scrums and scaling Scrum for large teams-Agile contracts and governance.

Unit III : **Agile Planning and Estimation**

Agile project initiation and roadmaps-Product vision and product backlog creation-Writing effective user stories and acceptance criteria-Story points, planning poker, T-shirt sizing-Release planning and sprint planning techniques-Velocity tracking and burndown/burnup charts-Capacity planning and backlog refinement.

Unit IV : **Scrum in Practice and Team Collaboration**

Implementing Scrum in real-world projects-Agile team dynamics and cross-functional teams-Managing distributed Scrum teams-Servant leadership and coaching mindset-Role of Agile coaches and Scrum Masters-Case studies: Agile transformations in industry-Simulating a Scrum project from start to finish.

Unit V : Agile Metrics, Quality, and Continuous Improvement

Agile performance metrics: Velocity, Lead time, Cycle time, Defect rate-KPIs for Scrum teams-Agile testing strategies and Test-Driven Development (TDD)-Continuous Integration (CI) and Continuous Deployment (CD)-Retrospective techniques and continuous improvement-Scaling Agile (SAFe, LeSS, Disciplined Agile Delivery)-Challenges in Agile adoption and change management strategies.

SUGGESTED READINGS:

- Ken Schwaber & Jeff Sutherland – The Scrum Guide (Latest Edition – https://scrumguides.org)
- Mike Cohn – Agile Estimating and Planning, Pearson
- Robert C. Martin – Clean Agile: Back to Basics, Prentice Hall
- Henrik Kniberg – Scrum and XP from the Trenches, InfoQ
- Scaled Agile Framework – https://www.scaledagileframework.com/
- Atlassian Agile Tutorials – https://www.atlassian.com/agile