RCOEM

Shri Ramdeobaba College of
Engineering and Management, Nagpur

SHRI RAMDEOBABA COLLEGE OF ENGINEERING AND MANAGEMENT, NAGPUR – 440013

An Autonomous College affiliated to Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, Maharashtra (INDIA)

PROGRAMME SCHEME & SYLLABI
2023-24

B. TECH. (CSE-Cyber Security)

B. Tech. Computer Science and Engineering [2023-24]
Teaching & Evaluation Scheme [B. Tech CSE-Cyber Security]

Semester -I

Sr. No.	Category	Course Code	Course Name	Hours/ week			Credits	Maximum marks			ESE Duration (Hrs)
				L	T	P		CE	ESE	Total	
1.	BSC	CHT1001	Chemistry of Smart Materials	2	0	0	2	50	50	100	2
2.	BSC	CHP1001	Chemistry of Smart Materials Lab	0	0	2	1	50	-	50	-
3.	BSC	MAT1002	Calculus	3	0	0	3	50	50	100	3
4.	ESC	CCT1001	Digital Electronics	3	0	0	3	50	50	100	3
5.	ESC	CCP1001	Digital Electronics Lab	0	0	2	1	50	-	50	-
6.	ESC	CCT1002	Programming for problem solving	3	0	0	3	50	50	100	3
7.	ESC	CCP1002	Programming for problem solving Lab	0	0	2	1	50	-	50	-
8.	VSEC	CCT1003	Computer Workshop – I	1	0	0	1	50	-	50	-
9	VSEC	CCP1003	Computer Workshop – I Lab	0	0	2	1	50	-	50	-
10	HSSM -IKS	HUT1001	Foundational Literature of Indian Civilization	2	0	0	2	50	50	100	2
11.	CCA	PET1001	Sports-Yoga-Recreation	1	0	0	1	50	-	50	-
12.	CCA	PEP1001	Sports-Yoga-Recreation Lab	0	0	2	1	50	-	50	-
			TOTAL	**15**	**0**	**10**	**20**			**850**	**-**

Semester-II

Sr. No.	Category	Course Code	Course Name	Hours/week			Credits	Maximum marks			ESE Duration (Hrs)
				L	T	P		Continuous Evaluation	End Sem Exam	Total	
1.	BSC	PHT2001	Introduction to Quantum Computing	2	1	0	3	50	50	100	3
2.	BSC	PHP2001	Introduction to Quantum Computing Lab	0	0	2	1	50	-	50	-
3.	BSC	MAT2002	Discrete Mathematics	3	0	0	3	50	50	100	3
4.	BSC	MAP2001	Computational Mathematics Lab	0	0	2	1	50	-	50	-
5.	BSC	CHT2007	Bioinformatics	2	0	0	2	50	50	100	2
6.	ESC	CCT2001	Object Oriented Programming	3	0	0	3	50	50	100	3
7.	ESC	CCP2001	Object Oriented Programming Lab	0	0	2	1	50	-	50	-
8.	PCC	CCT2002	Computer Architecture	2	0	0	2	50	50	100	2
9	VSEC	CCT2003	Computer Workshop – II	1	0	0	1	50	-	50	-
10	VSEC	CCP2003	Computer Workshop – II Lab	0	0	2	1	50	-	50	-
11.	AEC	HUT2002	English for Professional Communication	2	0	0	2	50	50	100	2
12.	AEC	HUP2002	English for Professional Communication Lab	0	0	2	1	50	-	50	-
13.	CCA	HUP0001	Liberal/Performing Art	0	0	2	1	50	-	50	-
14.	VEC	HUT2004	Foundation Course in Universal Human Values	1	0	0	1	50	-	50	-
			TOTAL	16	1	12	23	-	-	1000	-

List of courses offered under the Basket of Liberal Arts (HUP0001)

Course Code	Course Name
HUP0001-1	Fundamentals of Indian Classical Dance: Bharatnatayam
HUP0001-2	Fundamentals of Indian Classical Dance: Kathak
HUP0001-3	Introduction to Digital Photography
HUP0001-4	Introduction to Japanese Language and Culture
HUP0001-5	Art of Theatre
HUP0001-6	Introduction to French Language
HUP0001-7	Introduction to Spanish Language
HUP0001-8	Art of Painting
HUP0001-9	Art of Drawing
HUP0001-10	Nature camp
PEP0001-21	Disaster Management through Adventure Sports
PEP0001-22	Self-defense Essentials and Basics Knowledge of Defense forces
CHP0001-31	Art of Indian traditional cuisine
CHP0001-32	Remedies by Ayurveda

Exit option: Award of UG Certificate in Major with 43 credits and an additional 8 credits.			
Exit Courses			
1	Web Designer	Online/ offline certification Course	8
2	IT Support Engineer		8
3	Certified Programmer (language learned in Sem-1 and/or Sem-2 [C, C++, Java, Python])		8

Semester - III								Maximum marks			ESE Duration (Hrs)
Sr. No.	**Category**	**Course Code**	**Course Title**	**L**	**T**	**P**	**Credits**	**Continuous Evaluation**	**End Sem Exam**	**Total**	
1	PCC	CCT3001	Data Structures	3	1	0	4	50	50	100	3
2	PCC	CCP3001	Data Structures Lab	0	0	2	1	25	25	50	-
3	PCC	CCT3002	Computer Networks	3	0	0	3	50	50	100	3
4	PCC	CCP3002	Computer Networks Lab	0	0	2	1	25	25	50	-
5	PCC	CCP3003	Software Lab-I	0	0	2	1	25	25	50	-
6	MDM	MAT3003	Mathematics for Cyber Security	3	0	0	3	50	50	100	3
7	OE	IDT2980	Open Elective - I	1	0	0	2	50	50	100	3
8	HSSM	CCP3005	Idea Lab	0	0	4	2	25	25	50	-
9	PCC	CCT3006	Cyber Law and Ethics	2	0	0	2	50	50	100	2
10	AEC	HUT3001	Business Communication	2	0	0	2	50	50	100	2
			TOTAL	**19**	**1**	**10**	**21**	**-**		**800**	**-**

Semester - IV								Maximum marks			ESE Duration (Hrs)
Sr. No.	**Category**	**Course Code**	**Course Title**	**L**	**T**	**P**	**Credits**	**Continuous Evaluation**	**End Sem Exam**	**Total**	
1	PCC	CCT4001	Operating Systems	3	0	0	3	50	50	100	3
2	PCC	CCP4001	Operating Systems Lab	0	0	2	1	25	25	50	-
3	PCC	CCT4002	Cryptography	3	0	0	3	50	50	100	3
4	PCC	CCP4002	Cryptography Lab	0	0	2	1	25	25	50	-
5	PCC	CCT4003	Theory of Computation	3	0	0	3	50	50	100	3
6	MDM	MAT4002	Probability and Queuing Theory	3	0	0	3	50	50	100	3
7	OE	IDT2990	Open Elective - II	3	0	0	3	50	50	100	3
8	PCC	CCP4005	Software Lab-II	0	0	2	1	25	25	50	-
9	CEP/FP/ZZ	CCP4006	Community Engagement Project	0	0	4	2	25	25	50	-
10	HSSM	MBT4001	Business and Organizational Management	2	0	0	2	50	50	100	2
11	VEC	HUT4002	Environmental Education	2	0	0	2	50	50	100	2

			TOTAL	**19**	**0**	**10**	**24**	**-**	**-**	**900**	**-**

Exit option: Award of UG Certificate in Major with 88 credits and an additional 8 credits.			
Exit Courses			
1	Application Development (Android)	Online/offline certification Course	8
2	Certified Software Engineer (DevOps)		8
3	Certified Network Defender (CND) – EC - Council		8

B.Tech. CSE (Cyber Security) Scheme: 2023-24

Semester - V								Maximum marks			ESE
Sr. No.	**Category**	**Course Code**	**Course Title**	**L**	**T**	**P**	**Credits**	**Continuous Evaluation**	**End Sem Exam**	**Total**	**Duration (Hrs)**
1	PCC	CCT5001	Design & Analysis of Algorithms	3	0	0	3	50	50	100	3
2	PCC	CCT5002	Computer Security	3	0	0	3	50	50	100	3
3	PCC	CCP5002	Computer Security Lab	0	0	2	1	25	25	50	-
4	PCC	CCT5003	Basics of Ethical Hacking	3	0	0	3	50	50	100	3
5	PCC	CCP5003	Basics of Ethical Hacking Lab	0	0	2	1	25	25	50	-
6	PCC	CCT5004	Program Elective-1	3	0	0	3	50	50	100	3
7	MDM	CCT5005	Artificial Intelligence and Machine Learning	3	0	0	3	50	50	100	3
8	MDM	CCP5005	Artificial Intelligence and Machine Learning Lab	0	0	2	1	25	25	50	-
9	OE	IDT3980	Open Elective - III	3	0	0	3	50	50	100	2
			TOTAL	**18**	**0**	**6**	**21**	**-**	**-**	**750**	**-**

Semester - VI								Maximum marks			ESE Duration (Hrs)
Sr. No.	**Category**	**Course Code**	**Course Title**	**L**	**T**	**P**	**Credits**	**Continuous Evaluation**	**End Sem Exam**	**Total**	
1	PCC	CCT6001	Introduction to Cloud Security	3	0	0	3	50	50	100	3
2	PCC	CCP6001	Introduction to Cloud Security Lab	0	0	2	1	25	25	50	-
3	PCC	CCT6002	Database Management System	3	0	0	3	50	50	100	3
4	PCC	CCP6002	Database Management System Lab	0	0	2	1	25	25	50	-
5	PCC	CCT6003	Software Engineering and Project Management	3	0	0	3	50	50	100	3
6	PCC	CCP6003	Software Engineering and Project Management Lab	0	0	2	1	25	25	50	-
7	PCC	CCT6004	Program Elective-2	3	0	0	3	50	50	100	3
8	PCC	CCT6005	Program Elective-3	3	0	0	3	50	50	100	3
9	PCC	CCT6006	Deep Learning	2	0	0	2	50	50	100	2
10	VSEC	CCP6007	Mini Project	0	0	4	2	25	25	50	-
			TOTAL	**17**	**0**	**10**	**22**			**800**	

Exit Option: Award of UG Certificate in Major with 131 credits and an additional 8 credits.			
Exit Courses			
1	Certified Cloud Engineer (AWS, AZURE)	Online/ offline certification Course	8
2	Certified Cloud Security (ZScaler)		8
3	Certified Ethical Hacker (EC - Council)		8

B.Tech. CSE (Cyber Security) Scheme: 2023-24

Semester - VII								**Maximum marks**			**ESE**
Sr. No.	**Category**	**Course Code**	**Course Title**	**L**	**T**	**P**	**Credits**	**Continuous Evaluation**	**End Sem Exam**	**Total**	**Duration (Hrs)**
1	PCC	CCT7001	Compiler Design	3	0	0	3	50	50	100	3
2	PCC	CCT7002	Secure Coding	3	0	0	3	50	50	100	3
3	PCC	CCT7003	Network Security Administration	3	0	0	3	50	50	100	3
4	PCC	CCP7003	Network Security Administration Lab	0	0	2	1	25	25	50	-
5	PCC	CCT7004	Program Elective-4	3	0	0	3	50	50	100	3
6	PCC	CCP7004	Program Elective-4 Lab	0	0	2	1	25	25	50	-
7	MDM	CCP7005	Data Visualization Techniques	0	0	2	1	25	25	50	-
8	Prj	CCP7006	Major Project I	0	0	8	4	50	50	100	
			TOTAL	**12**	**0**	**14**	**19**			**650**	**-**
OR											
1	INTR	CCP7007	Industry Internship	0	0	24	12	100	100	200	
2	PCC	CCT7008	NPTEL-1/ MOOC-1				03	50	50	100	
3	PCC	CCT7009	NPTEL-2/ MOOC-2				03	50	50	100	
4	PCC	CCT7010	NPTEL-3/ MOOC-3				01	50	50	100	
			TOTAL	**0**	**0**	**24**	**19**	**250**	**250**	**500**	

Semester - VIII								**Maximum marks**			**ESE**
Sr. No.	**Category**	**Course Code**	**Course Title**	**L**	**T**	**P**	**Credits**	**Continuous Evaluation**	**End Sem Exam**	**Total**	**Duration (Hrs)**
1	PEC	CCT8001	Program Elective-5	3	0	0	3	50	50	100	3
2	PEC	CCT8002	Program Elective-6	3	0	0	3	50	50	100	3
3	Project	CCP8003	Major Project II	0	0	12	6	50	50	100	-
Total								**150**	**150**	**300**	
OR											
1	PEC	CCT8004	Research Methodology	3	0	0	3	50	50	100	3
2	Project	CCP8005	Research Project	0	0	12	6	50	50	100	-
3	PEC	CCT8001	Program Elective-5	3	0	0	3	50	50	100	3
Total								**150**	**150**	**300**	
OR											
1	Internship	CCP8006	Internship / TBI Internship	0	0	24	12	100	100	200	
			TOTAL	**0**	**0**	**24**	**12**			**200**	**-**

B.Tech. CSE (Cyber Security) Scheme: 2023-24

SSElectives Basket:

Program Elective - 1	**Program Elective - 2**	**Program Elective - 3**	**Program Elective - 4**	**Program Elective - 5**	**Program Elective - 6**
CCT5004 – 1 Operating Systems for Cyber Security	CCT6004 – 1 Wireless & Mobile Device Security	CCT6005 – 1 Managing Risk in Information Systems	CCT7004 – 1 Database & Email Forensics	CCT8001 -1 Vulnerability Assessment and Penetration Testing	CCT8002 – 1 Testing Cyber Crime Investigation and Digital Forensics
CCT5004 – 2 Threat and Malware Analysis	CCT6004 – 2 Incident Handling & Response	CCT6005 – 2 IoT Security	CCT7004 – 2 Auditing IT Infrastructure for Compliance	CCT8001- 2 Disaster Recovery & business continuity management	CCT8002 – 2 Executive Governance and Management in IT Security
CCT5004 – 3 Security Policies and implementation	CCT6004 – 3 Security Strategies in Windows & Linux	CCT6005 – 3 Application Security	CCT7004 – 3 Blockchain Security	CCT8001 - 3 Mobile Application Security Testing	CCT8002 – 3 Security in Social Networks

List of Open Electives:

Sr. No.	**Subject Code**	**Name of Subject**
Open Elective I	IDT2980	Cyber Defense Strategies
Open Elective II	IDT2990	Network Security Fundamentals
Open Elective III	IDT3980	Basics of Ethical Hacking

Syllabus for B.Tech. Semester I

(CSE- Cyber Security, Artificial Intelligence and Machine learning, Data science)

Course Code	**CHT1001**				
Category	Basic Science Course				
Course Title	**Chemistry of Smart Materials**				
Scheme & Credits	L	T	P	Credits	Semester I
	2	0	0	2	

Course Outcomes

On successful completion of course student will learn:

1. Classify and explain the different types of sensors for various applications.
2. Discuss unique properties of nano-materials to solve challenges in our life and applications in computational world.
3. Discuss how spectroscopic methods are used for qualitative and quantitative analysis.
4. Analyze the utilization of green computing technology for environmental issues

UNIT-I: Smart Sensors and Materials

RFID and IONT materials: Synthesis, properties and applications in logistic information, intelligent packaging systems (Graphene oxide, carbon nanotubes (CNTs) and polyaniline). Sensors: Introduction, types of sensors (Piezoelectric and electrochemical), nanomaterials for sensing applications (Strain sensors, gas sensor, biomolecules and volatile organic compounds).

UNIT-II: Nanomaterials

Introduction, classification, size dependent properties, surface area, optical and catalytic properties, Synthesis methods of nanomaterials- Top down and bottom-up approach.

Carbon nanomaterials: Types, properties and applications of CNT and graphene. Applications of nano materials.

UNIT-III: Characterization Techniques and computational tools:

Fundamentals of spectroscopy, Electronic Spectroscopy, Nuclear Magnetic Resonance Spectroscopy. Basics of Nuclear magnetic resonance quantum computer

Synthesis of drugs, basic soft-wares for bio-chemical assessment of drugs.

UNIT-IV: Green Computing and Chemistry

E-wastes- Types, environmental and health risks, segregation and recycling (Hydrometallurgical, pyrometallurgical and direct recycling), Extraction of precious metals from e-wastes, Twelve principles of Green Chemistry. Green Computing, Role of Green Computing in Environment and Research, Green devices and Green data Servers.

Text Books:

1. Shikha Agrawal , Engineering Chemistry : Fundamentals and Applications, Cambridge University Press.
2. Dr. Rajshree Khare, A Textbook of Engineering Chemistry(AICTE), S.K. Kataria & Sons.
3. S. S. Dara, A Textbook of Engineering Chemistry, S. Chand Publications.
4. A. K. Das and M. Das, An introduction to nanomaterials and nanoscience, CBS Publishers and Distributors
5. M Afshar Alam, Sapna Jain, Hena Parveen, Green Computing Approach Towards Sustainable

Development, Wiley Interscience Publications.
6. Sensor & transducers, D. Patranabis, 2nd edition, PHI

Reference Books:

1. E-waste recycling and management: present scenarios and environmental issues, Khan, Anish, and Abdullah M. Asiri. 2019, Springer, Vol. 33. ISBN: 978-3-030-14186-8.
2. Hans-Eckhardt Schaefer, Nanoscience: The Science of the Small in Physics, Engineering, Chemistry, Biology and Medicine, Springer-Verlag Berlin Heidelberg.

Syllabus for B.Tech. Semester I
(CSE- Cyber Security, Artificial Intelligence and Machine learning, Data science)

Course Code	CHP1001				
Category	Basic Science Course				
Course Title	Chemistry of Smart Materials Lab				
Scheme & Credits	**L**	**T**	**P**	**Credits**	**Semester I/II**
	0	0	2	1	

The Chemistry laboratory course will consist of experiments illustrating the principles of chemistry relevant to the study of science and engineering.

The students will learn to:

1. Apply the fundamental principles of measurement and skills in preparation and handling of hazardous chemicals and interpret the statistical data related to measurements.
2. Estimate the rate constants of reactions and order of the reaction and/or to validate adsorption isotherms.
3. Use of various computational tools for analysis of different spectral properties and bio-activities.

List of Experiments:

[1] Preparation of different Solutions: Molar solution, Normal solution and percent solution and Determination of concentration.

[2] Demonstration of Handling of hazardous chemicals, MSDS (material safety data sheet), waste minimization strategies and chemical waste disposal.

[3] Basic statistical analysis of results of neutralization of acid against the base and preparing acceptable graphs using software.

[4] Prediction of infrared/NMR spectral and analytical data of organic molecules using Computational Software.

[5] Spectroscopic/Colorimetric determine of wavelength of maximum absorption of chemical/biological compound in solution and determination of concentration using Lambert-Beer's Law.

[6] To study chemical kinetics of peroxydisulphate and iodide ions reactions and to find out order of the reaction and analysis of experimental data using Computational Software.

[7] Molecular docking of drugs using open computational software.

[8] Determination of rate of the reaction at room temperature and analysis of experimental data using Computational Software

[9] Use of open access software for the interpretation of various parameters of materials including drugs

[10] Estimation of Copper from PCB

Suggested Books/Reference Books:

1. S. S. Dara, A Textbook on Experiments and Calculations in Engineering Chemistry, S. Chand Publications.
2. J. B. Yadav, Advanced Practical Physical Chemistry, Krishna's Prakashan Media (P) Limited.
3. J. Elias, Collection of Interesting General Chemistry Experiments, Universities Press Publications.
4. V. K. Ahluwalia, S. Dhingra and A. Gulati, College Practical Chemistry, Universities Press Publications.
5. Ashutosh Kar , Advanced Practical Medicinal Chemistry, New Age International Publisher.

Suggested Reference Books:

1. David Young, Computational Chemistry: A Practical Guide for Applying Techniques to RealWorld Problems, Wiley Interscience Publications

Annexure 4 (2023-24)

Syllabus for Bachelor of Technology
(Computer Science/ AIML/Data Science/ Cyber Security/IT Engineering)

Semester I

Course Code: MAT 1002	**Course Name: Calculus**
L: 3Hrs. T: 0 Hrs. P: 0 Hrs. Per week	**Total Credits:3**

Course Objective

The objective of this course is to familiarize the prospective engineers with techniques in Calculus. It aims to equip the students with standard concepts and tools at an intermediate to advanced level that will serve them well towards tackling more advanced level of mathematics and applications that they would find useful in their disciplines.

Course Outcomes

On successful completion of the course, student shall be able to

1. Apply the concepts of continuity and differentiability to find Taylor's and Maclaurin series.
2. Understand the methods of partial derivatives and apply these concepts to determine extreme values of the functions of two variables.
3. Demonstrate the basic knowledge of vector differentiation and line integral.
4. Understand proper and improper integrals and use it find area, length, volume and surface of revolution
5. Internalize convergence of sequences and apply it to determine whether infinite series convergent or divergent with appropriate tests.

Syllabus

Module 1 :(8 Lectures)

Differential Calculus: Functions of single variable: Review of limit, continuity and differentiability. Mean value theorems: Rolle's theorem, Lagrange's theorem, Cauchy's theorem, Taylor's theorem, Taylor's and Maclaurin series.

Module 2: (8 Lectures)

Partial Differentiation: Partial derivatives, Euler's Theorem, chain rule, total derivative, Jacobians, Maxima, Minima for the functions of two variables.

Module 3: (8 Lectures)

Vector Calculus: Scalar and vector fields, gradient of scalar point function, directional derivatives, divergence and curl of vector point function, Line integral.

Module 4: (8 Lectures)

Integral Calculus: Fundamental theorem of Integral calculus, mean value theorems, evaluation of definite integrals, applications in area, length, volumes and surface of solids of revolutions, Improper integrals: Beta and Gamma functions.

Module 5: (8 Lectures)

Infinite series: Sequences, Infinite series of real and complex numbers, Cauchy criterion, tests of convergence, absolute and conditional convergence, uniform convergence, power series, radius of convergence.

Textbooks/References

1. Erwin Kreyszig, Advanced Engineering Mathematics, 9th Edition, John Wiley & Sons, 2006.
2. Veerarajan T., Engineering Mathematics for first year, Tata McGraw-Hill, New Delhi, 2008.
3. N.P. Bali and Manish Goyal, A text book of Engineering Mathematics, Laxmi Publications, Reprint, 2010.
4. B.S. Grewal, Higher Engineering Mathematics, Khanna Publishers, 35th Edition, 2000.
5. Ramana B.V., Higher Engineering Mathematics, Tata McGraw Hill New Delhi, 11th Reprint, 2010.
6. P. N. Wartikar and J. N. Wartikar, A text book of Applied Mathematics Volume I & II, Pune Vidhyarthi Griha Prakashan, Pune-411030 (India).

Syllabus for Semester I, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCT1001 **Category:** Engineering Science Course (ESC)

Course: Digital Electronics **L:** 3Hrs**, T:** 0Hr**, P:** 0Hr**, Per Week, Credits:** 3

Course Objectives

The objective of this course is to familiarize the prospective engineers with:

1. Logic functions using Boolean algebraic theorems and techniques
2. Conventional combinational and sequential circuits including conversions of flip-flops.
3. The exploration of the semiconductor memories and programmable logic devices.
4. The basic concept of microprocessor with addressing mode and instruction set for programming.

SYLLABUS

UNIT-I: **Basics of Digital Electronics**

Motivation for digital systems: Logic and Boolean algebra, Number Systems. Logic Gates & Truth Tables, Demorgan's law, Minimization of combinational circuits using Karnaugh maps up to five variables. Map manipulation-essential prime implicants, non-essential prime implicants**.**

UNIT-II: Combinational Circuit Design

Design procedure: Multiplexers, Demultiplexer, Encoders, Decoders, Code Converters, Adders, Subtractor (Half, Full), BCD Adder/ Subtractor, ripple and carry look-ahead addition booth's Algorithm, bit-pair recoding, Integer Division- restoring and non-restoring division

UNIT-III: Sequential circuit Design-I

Storage elements, Flip-flops and latches: D, T, J/K, S/R flip-flops. Master Slave Conversion of one of type of F/F to another Sequential circuit. Analysis –Input equations, state table, and analysis with J-K Flip flops. Sequential circuit Design, Design procedure, designing with D & J-K Flip flop.

UNIT-IV: Sequential circuit Design-II

Counters, asynchronous and synchronous design using state and excitation tables. Registers & Shift registers., Mealey & Moore Machines

UNIT-V: Memory & Programmable logic Devices

Semiconductor RAM memories, Static and Dynamic Memories, ROM, higher order memory design, multi-module memories, Memory interleaving, Secondary storage – Magnetic disk, Optical disk, PLA, PAL.

UNIT-VI: Fundamental of Microprocessor

Introduction to µp 8085, Addressing modes, Instruction set, Programming of µp 8085

Course Outcomes

After successful completion of this course, the student will be able to,

1. Outline binary arithmetic operations and optimize Boolean functions using Karnaugh map (k-map) method.
2. Apply combinational circuits for realization of basic building blocks of conventional digital circuits.
3. Design sequential blocks like flip flops, counters, registers, simple finite state machine and similar circuits.

4. Describe the memory elements and combinational digital circuits implementation with programmable logic devices.
5. Use addressing modes and instruction set of target microprocessors for writing efficient assembly language programs.

Text Books

1. Morris Mano; Digital Logic Design; Fourth edition, McGraw Hill
2. R.P.Jain; Modern Digital Electronic; Fourth edition; Tata McGraw-Hill.
3. V.J.Vibhute; 8-Bit Microprocessor & Microcontrollers; fifth edition.

Reference books

1. Anand Kumar; Fundamental of Digital Electronics; Second Edition, PHI
2. A.P.Godse; Digital circuit & design; Technical Publications; 2009.
3. Ramesh Gaonkar; 8-bit Microprocessor; CBS Publishers; 2011.

Syllabus for Semester I, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCP1001 **Category:** Engineering Science Course (ESC)

Course: Digital Electronics Lab **L:** 0Hr**, T:** 0Hr**, P:** 2Hrs**, Per Week, Credits:** 1

Course Outcome

On Successful completion of course, students will be able to:

1. Use logic gates for designing digital circuits
2. Implement combinational circuits using VHDL
3. Implement sequential circuits using VHDL
4. Apply the knowledge gained for their project work based on the hardware digital circuits

Practical based on the above theory syllabus

Syllabus for Semester I, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCT1002 **Category:** Engineering Science Course (ESC)

Course: Programming for Problem Solving **L:** 3Hrs**, T:** 0Hr**, P:** 0Hr**, Per Week, Credits:** 3

Course Outcomes

On successful completion of course student will learn:

1. Create C programs using loops and decision making statements to solve and execute the given problem.
2. Develop programs and functions one dimensional and two dimensional arrays.
3. Apply the concept of pointers, structures to develop programs.
4. Implement files in C to store the data for the given problem.

UNIT-I: Introduction to Programming

Introduction to components of a computer system (disks, memory, processor, where a program is stored and executed, operating system, compilers etc.) Idea of Algorithm: Steps to solve logical and numerical problems. Representation of Algorithm: Flowchart /Pseudocode with examples. Arithmetic expressions and precedence

UNIT-II: C Programming Language

Introduction to C language: Keywords, Constant, Variable, Data types, Operators, Types of Statements,

Pre-processor Directives, Decision Control Statement-if, if-else, nested if-else statement, switch case, Loops and Writing and evaluation of conditionals and consequent branching.

UNIT-III: Arrays and Basic Algorithms

Arrays: 1-D, 2-D, Character arrays and Strings. Searching, Basic Sorting Algorithms (Bubble, Insertion and Selection), Finding roots of equations, notion of order of complexity through example programs (no formal definition required)

UNIT-IV: Functions and Recursion

User defined and Library Functions, Parameter passing in functions, call by value, passing arrays to functions: idea of call by reference. Recursion: As a different way of solving problems. Example programs, such as Finding Factorial, Fibonacci series, Ackerman function etc. Quick sort or Merge sort.

UNIT-V: Pointers and Structures

Structures, Defining structures, Array of Structures, Introduction to pointers, Defining pointers, Pointer arithmetic, pointer operators, Use of Pointers in self-referential structures, notion of linked list (no implementation)

UNIT-VI: File handling

Streams in C, Types of Files, File Input/ Output Operations: Modes of file opening, Reading and writing the file, Closing the files, using fflush ().

Text Books:

1. Programming in ANSI C: E. Balguruswami McGraw Hill
2. Mastering C: K. R. Venugopal and S. R. Prasad, Tata McGraw Hill

Reference Books

1. Programming with C: Byron Gottfried, Schaums Outline Series.
2. Let Us C: Yashwant Kanetkar, BPB Publication

Syllabus for Semester I, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCP1002 **Category:** Engineering Science Course (ESC

Course: Programming for Problem Solving Lab **L:** 0Hr**, T:** 0Hr**, P:** 2Hrs**, Per Week, Credits:** 1

Course Outcomes

On successful completion of course student will be able to:

1. Create C programs using loops and decision making statements to solve and execute the given problem.
2. Develop programs and functions one dimensional and two dimensional arrays.
3. Apply the concept of pointers, structures to develop programs.
4. Implement files in C to store the data for the given problem.

Practical based on above theory syllabus

Syllabus for Semester I, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCT1003 **Category:** Vocational & Skill Enhancement Course (VSEC)

Course: Computer Workshop-1 **L:** 1Hr**, T:** 0Hr**, P:** 0Hr**, Per Week, Credits:** 1

Course Objectives

1. Understand the definition and principles of UI/UX in order to design with intention.
2. Achieve an understanding of the life-cycle of application design—the process, purpose, and tools.
3. Learn the basics of HCI (human-computer interaction) and the psychology behind user decision-making.
4. Explore UI/UX tools to interpret requirements of modern applications.
5. Elaborate design decisions through presentations of assignments.

Unit 1: UI/UX Overview:

Introduction to UI/UX, Principles of UI/UX, UI Components, Design Thinking, Interaction Design, Usability.

Unit 2: UI Programming:

Basic of HTML5, Elements of HTML5, Background of CSS, Bootstrap CSS, Fundamentals of JavaScript, HTML DOM Manipulations.

Unit 3: UX Programming:

Figma Basics, How to identify user needs, Wireframe and Prototype, Digital Storytelling.

Course Outcomes

On successful completion of the course, students will be able to:

1. Understand basics of UI/UX
2. Design and develop web pages using HTML, CSS and JavaScript
3. Infer the significance of Wireframing and build prototypes.

Text Books

1. UI/UX design for designer and developers: by Nathan Clark
2. Web Design: A Beginner’s Guide Second Edition by Wendy Willard
3. User story mapping by Jeff Patton, O'Reilly Publication

Syllabus for Semester I, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCP1003 **Category:** Vocational & Skill Enhancement Course (VSEC)

Course: Computer Workshop-1 Lab **L:** 0Hr**, T:** 0Hr**, P:** 2Hrs**, Per Week, Credits:** 1

Course Objectives

1. Understand the definition and principles of UI/UX in order to design with intention.
2. Achieve an understanding of the life-cycle of application design—the process, purpose, and tools.
3. Learn the basics of HCI (human-computer interaction) and the psychology behind user decision-making.
4. Explore UI/UX tools to interpret requirements of modern applications.
5. Elaborate design decisions through presentations of assignments.

Syllabus:

Practical based on Theory Syllabus

Course Outcomes

On successful completion of the course, students will be able to:

1. Design and develop static web pages using HTML and CSS
2. Develop dynamic web pages using JavaScript
3. Create high-fidelity designs and prototypes in Figma

Scheme

Appendix -1

Shri Ramdeobaba College of Engineering and Management
Department of Humanities
Syllabus and Scheme of IKS course

Course Code	Course Name	Sem.	Hours/week	Credits	Maximum marks	ESE
					Continuous Evaluation	2 hours
HUT1001/ 2001	**Foundational Literature of Indian Civilization**	I/II	2	2	50	50

Course outcome:

At the end of the course the students will be able to achieve the following: CO1: Understand the Indian knowledge system and its scientific approach

CO2: Get introduced to the Vedic corpus and recognize the multi-faceted nature of the knowledge contained in the Vedic corpus

CO3: Understand the salient features of the philosophical systems of the Vedic and non- Vedic schools

CO4: Develop a basic understanding of the ancient wisdom recorded in various Indian literary work

Syllabus

1. **Unit 1: Overview of Indian Knowledge System:** Importance of ancient knowledge, defining IKS, IKS classification framework, Historicity of IKS, Some unique aspects of IKS.
2. **Unit 2: The Vedic corpus:** Introduction of Vedas, four Vedas, divisions of four Vedas, six Vedangas, Distinct features of Vedic life.
3. **Unit 3: Indian Philosophical systems:** Development and unique features, Vedic schools of philosophy, *Samkhya* and *Yoga* School of philosophy, *Nayay* and *Vaisesika* school of philosophy, *Purva-mimamsa* and *Vedanta* schools of Philosophy, Non-vedic philosophies: Jainism, Buddhism, and other approaches
4. **Unit 4: Indian wisdom through ages:** *Panchtantras,* ***Purans*****:** contents and issues of interests, ***Itihasa:*** uniqueness of the two epics (Ramayan and Mahabharata), Key issues and messages from Ramayana, Mahabharata – a source of worldly wisdom*;*

   Indian ancient Sanskrit literature: *Kalidas, Vishakadutta*, *Bhavbhuti, Shudraka**

***any one text as decided by the course teacher**

Reference material

1. B. Mahadevan, Vinayak Rajat Bhar, Nagendra Pavana R. N., *"Introduction to Indian Knowledge System: Concepts and Applications"* PHI, 2022
2. S.C. Chatterjee and D.M. Datta, *An introduction to Indian Philosophy,* University of Calcutta, 1984

SHRI RAMDEOBABA COLLEGE OF ENGINEERING & MANAGEMENT, NAGPUR DEPARTMENT OF PHYSICAL EDUCATION

Syllabus of Semester I UG Engineering Program

COURSE: SPORTS-YOGA-RECREATION			
L: 1 Hrs. T: 0 Hrs. P: 2 Hrs. Per Week			Total Credit: 02
	Course Code	**Credit**	**No. of Lecture/Practical**
Theory	PET 1001	1	1 Hour per week
Practical	PEP 1001	1	2 Hours per week

Aim of the Course: The course aims at creating awareness about the fundamentals of Physical Education, Sports, Yoga, Recreation and its effectiveness to promote Health and wellness through Healthy Lifestyle.

Objectives of the Course:

1. To impart the students with basic concepts of Sports, Yoga and Recreational activities for health and wellness.
2. To familiarize the students with health-related Exercise and evaluate their Health-related Fitness.
3. To make Overall growth & development with team spirit, social values and leadership qualities among students through various sports, games and Yogic activities.
4. To create Environment for better interaction and recreation among students as neutralizer for stress through various minor and recreational games.

Course Outcomes: On completion of the course, students will be able to:

1. Understand fundamental skills, basic principle and practices of sports and Yoga.
2. Practically learn the principles of implementing general and specific conditioning of physical exercises and yoga.
3. Develop Health-related fitness and Body-mind co-ordination through various fitness activities, sports, recreational games and yoga.
4. practice Healthy & active living with reducing Sedentary Life style.

Course Content: Unit1:- Theory: Introduction

- Meaning, Definition and Importance of Health & Wellness
- Dimensions of Health and Wellness
- Factors influencing Health and Wellness
- Physical Fitness, Nutrition, Habits, Age, Gender, Lifestyle, Body Types
- Health & Wellness through Physical Activities, Sports, Games, Yoga and Recreation activities
- Causes of Stress & Stress relief through Exercise and Yoga
- Safety in Sports

SHRI RAMDEOBABA COLLEGE OF ENGINEERING & MANAGEMENT, NAGPUR DEPARTMENT OF PHYSICAL EDUCATION

Unit 2: - Practical- Exercises for Health and Wellness

.

- Warm-Up and Cool Down - General & Specific Exercises
- Physical Fitness Activities
- Stretching Exercises
- General & Specific Exercises for Strength, Speed, Agility, Flexibility, coordinative abilities
- Cardiovascular Exercises
- Assessment of BMI
- Relaxation techniques
- Physical Efficiency Tests

Unit 3: - Yoga

- Shukshma Vyayam
- Suryanamaskar
- Basic Set of Yogasanas – Sitting, standing, supine and prone position
- Basic Set of Pranayama & Meditation

References:

1. Russell, R.P. (1994). Health and Fitness Through Physical Education. USA: Human Kinetics.
2. Uppal, A.K. (1992). Physical Fitness. New Delhi: Friends Publication.
3. AAPHERD "Health related Physical Fitness Test Manual."1980 Published by Association drive Reston Virginia
4. Kumar, Ajith. (1984) Yoga Pravesha. Bengaluru: Rashtrothanna Prakashana.
5. Dr. Devinder K. Kansal, A Textbook of Test Evaluation, Accreditation, Measurements and Standards (TEAMS 'Science)

Shri Ramdeobaba College of Engineering & Management,
Nagpur Syllabus for Semester B.Tech. I / II

(Cyber Security, Artificial Intelligence and Machine learning, Data Science, Computer Science and Engineering and Information Technology)

Course Code	PHT 2001/1006				
Category	Basic Science Course				
Course Title	Introduction to Quantum Computing (Theory)				
Scheme& Credits	L	T	P	Credits	Semester I / II
	2	1	0	3	

Course Objectives

1. To introduce the fundamentals of quantum computing to students
2. The problem-solving approach using finite dimensional mathematics

Course Outcomes

After successful completion of the course, the students will be able to -

1. Use the basic quantum theory relating to the probabilistic behaviour of an electron in an atom.
2. Utilize the knowledge of complex vector space in the domain of quantum theory.
3. Analyse classical and quantum approach towards the quantum computation.
4. Classify deterministic and probabilistic systems and analyse quantum observations and quantum measurements.
5. Use quantum gates in building architecture and quantum algorithms.

Module 1: Basic Quantum Theory

Brief introduction about Quantum Computers and Quantum mechanics, Wave nature of Particles, Bohr's quantization condition, Heisenberg's Uncertainty principle, Wave function, probability, Schrodinger's wave equation, Operators, Electron in an infinite potential well, Eigen value and Eigen functions.

Module 2: Complex Vector Spaces

Algebra and Geometry of Complex numbers, Real and Complex Vector Spaces, definitions, properties, Abelian group, Euler's formula, Dr Moivre's formula, Matrix properties.

Module 3: Linear Algebra in Quantum Computing

Basis and Dimensions, Inner products, Hilbert Spaces, Eigenvalues and Eigenvectors, Hermitian and Unitary Matrices, Tensor Product, Applications of linear algebra in computer graphics.

Module 4: Classical and Quantum Systems

Deterministic and Probabilistic Systems, Quantum Systems, Stochastic billiard ball, Probabilistic double slit experiment with bullet and photon, Superposition of states, assembling systems, Entangled states.

Module 5: Quantum representation of systems

Dirac notations, Stern-Gerlach experiment, transition amplitude, norm of the ket, Bloch Sphere, Observables, Spin matrices, commutator operator, expectation values, variance, standard deviation, Heisenberg's uncertainty principle in matrix mechanics, measuring, dynamics, observations.

Module 6: Architecture and Algorithms

Bits and Qubits, Classical Gates and their equivalent quantum representation, Reversible Gates: CNOT, Toffoli, Fredkin, gates, outline of Pauli X, Y, Z gates, Hadamard gates, Deutsch Gate.
Quantum Algorithms: Deutsch's algorithm, Grover's search algorithm.
Applications of quantum computing in Cryptography, Quantum teleportation, Cybersecurity, banking, finance, advance manufacturing and artificial intelligence.

Text Book

1. Quantum computing for computer scientists, Noson S. Yanofsky, Mirco A. Mannucci, Cambridge University Press 2008
2. Introduction to Quantum Mechanics, 2nd Edition, David J. Griffiths, Prentice Hall New Jersey 1995

Reference Books

1. Quantum computing explained, David McMahon, Wiley-interscience, John Wiley & Sons, Inc. Publication 2008
2. Quantum computation and quantum information, Michael A. Nielsen and Isaac L. Chuang, Cambridge University Press 2010

Shri Ramdeobaba College of Engineering and Management, Nagpur
Syllabus for Semester B.Tech. I / II
(Cyber Security, Artificial Intelligence and Machine learning, Data science, Computer Science and Engineering and Information Technology)

Course Code	PHP 2001/1006				
Category	Basic Science Course				
Course Title	Introduction to Quantum Computing Lab				
Scheme & Credits	L	T	P	Credits	Semester I / II
	0	0	2	1	

Course Outcomes:

The physics laboratory will consist of experiments and programming exercises illustrating the principles of quantum physics and quantum computing relevant to the study of computer science and engineering.

On completion of the course, the students will be able to

1. Develop skills required for experimentation and verification of physics laws.
2. Utilise Mathematica software for graph plotting and for least squares fitting of the experimental data.
3. Compare the properties of real and complex matrices with reference to their use in quantum system.
4. Apply the computational methods to solve eigenvalues and eigenfunctions, tensor products.
5. Simulate classical and quantum gates.

List of Experiments:

1. Introduction to IBM quantum computer.
2. Simulation of classical gates by quantum representation of the gates and inputs.
3. Arithmetic operations using IBM Quantum computer.
4. Simulation of quantum gates: CNOT gate, Toffoli gate, Fredkin gate, Hadamard gate on IBM quantum computer.
5. Linear and Nonlinear data fitting by least squares fit method
6. Working with Vectors.
7. Working with Matrices: Real and Complex numbers.
8. Eigen values, Eigen functions, Properties of Inner Product and Unitary Matrices, Tensor Product.
9. Verification of Ohm's law and error analysis of the data using Linear Least Square Fit (LLSF) method.
10. Analysis of energy values and wavefunction using Mathematica software

Reference Books

1. Lab manual prepared by Physics Department, RCOEM, Nagpur

Syllabus for Bachelor of Technology (Computer Science/ AIML/Data Science/ Cyber Security/IT Engineering)

Semester II

Course Code: MAT 2002 **Course Name: Discrete Mathematics**

L: 3Hrs. T: 0 Hrs. P: 0 Hrs. Per week **Total Credits:3**

Course Objective:

The objective of this course is to expose student to understand the basic importance of Logic, Number theory, Algebraic structures like groups and Fieild, combinatorics and graph theory l in computer science and Information technology.

Course Outcomes

On successful completion of the course, student shall be able to

1. Formulate problems and solve recurrence relations
2. Apply techniques of number theory to solve problems from linear congruences, coding theory etc. in cryptography.
3. Internalize logical notations to define and reason about fundamental mathematical concepts and use it derive logical inference.
4. Apply groups and fields in coding theory.
5. Understand the Lattice as algebraic structure and use it for pattern recognition and in cryptography.

Syllabus

Module 1: (9 Lectures)

Combinatorics: Addition and multiplication rule in combinatorics, Linear and

Circular permutation, Combination, Binomial Identities, Inclusion and Exclusion Principle, distribution Principle, recurrence relations, generating function, examples using ordinary power series and exponential generating functions.

Module 2: (8 Lectures)

Modular Arithmetic: Modular Arithmetic, Euclid's Algorithm, primes, Fermat's theorem, Euler's theorem, Diophantine equations, Linear congruences, Chinese Remainder theorem, application to Cryptography.

Module 3: (7 Lectures)

Mathematical Logic: Statement and notations, connectives, Negation, conjunction, disjunction, conditional & bi-conditional statement. Tautologies, equivalence of formulas, Duality law, Tautological implications, Theory of inference for statement calculus.

Module 4: (9 Lectures)

Groups and Fields: Group definitions and examples, cyclic group, permutation groups, subgroups and homomorphism, co-sets, Lagrange's theorem and Normal subgroup, Error correcting codes, Hamming codes. Finite field, Galois field.

Module 5: (7 Lectures)

Lattice theory: Lattices as partially ordered set, Properties of Lattice, Lattices as algebraic system, sub lattices, direct product, homomorphism, some special Lattices.

Text Books:

1. Discrete Mathematical Structures with Applications to Computer Science: *J. P. Tremblay and R. Manohar , Tata McGraw-hill.*
2. Discrete Mathematics: *Babu Ram, Pearson Publication.*
3. Combinatorial Mathematics: C. *L. Liu & D. P. Mohapatra, 3rd edition, Tata McGraw-hill.*
4. David M Burton, 'Elementary Number Theory' , McGraw Hill, Seventh edition 2014.

Reference Books:

1. Foundations of Discrete Mathematics: *K. D. Joshi, New age international Publication.*
2. Discrete Mathematics: *Kolman, Busby & Ross, Pearson Publication.*

Annexure 1 (2023-24)

Syllabus

B.Tech First year (Computer Science/ AIML/Data Science/ Cyber Security Engineering)

Department: Mathematics Course: Computational Mathematics Lab
Course Code: MAP2001 L:0 Hr., T:0 Hr., P:2Hrs., Per week Total Credits:1
Course Objectives:

The computational Mathematics Lab course will consist of experiments demonstrating the principles of Mathematics relevant to the study of Science and Engineering. Students will show that they have learnt Laboratory skills that will enable them to properly acquire and analyze the data in the lab and draw valid conclusions. On successful completion of the course students shall be able to:

Proposed Course Outcomes:

By using open source software SageMath Students will be able to

CO1: Download SageMath and use it as an advance calculator.

CO2: Sketch and analyze function graphs.

CO3: Apply the concepts of differential calculus to find extreme value of continuous functions and analyze solutions of difference equations

CO4: Evaluate improper integrals and its applications to find length, area, volume, centre of gravity and mass.

CO5: Understand and Analysis Data inscription standards.

CO6: Analyze the data to find best fit curve.

Mapping of Course outcomes (COs) withExperiments

Exp. No.	Name of Experiments	Mapped COs
1	To use SageMath as advanced calculator	CO1
2	2D Plotting with SageMath	CO2
3	3D Plotting with SageMath	CO2
4	Differential Calculus with SageMath	CO3
5	Solution of difference equations in SageMath	CO3
6	To Learn Cryptography by using SageMath	CO5
7	Curve Fitting by using SageMath	CO6
8	Integral Calculus with SageMath	CO4

Head of the Department

Syllabus for B. Tech. Semester-II,

CSE-Cyber Security, CSE-Artificial Intelligence and Machinelearning, CSE-Data science, Computer Science and Engineering

Course Code	**CHT 2007**				
Category	Basic Science Course				
Course Title	**Bioinformatics**				
Scheme& Credits	L	T	P	Credits	Semester II
	2	0	0	2	

Course Outcomes:

After the successful completion of the course, students shall be able to

CO1: Explain the functioning of various metabolic processes in the human body. CO2: Acknowledge the importance of metabolic simulations in drug discovery,

CO3: Explain the functioning of various types of the drugs for therapeutic applications. CO4: Use knowledge of bioinformatics for basic formulation of drug design

Unit- I Introduction to Biomolecules

Carbohydrates: Introduction and classification

Amino Acid: Chemistry properties and metabolism.

Proteins: primary, Secondary, tertiary and quaternary structure,

Lipids: Chemistry, Metabolism of fatty acids, Phospholipids, Cholesterol regulation of metabolism. Nucleic Acid: Chemistry of DNA and RNA,

Vitamins: Structure and functions of some vitamins.

Unit-II Introduction to bioinformatics:

Introduction, Biological data: Sequence, gene expression, pathways and molecular interaction: Data bases: Sequence, Gene bank, Dogmass- central and peripheral, The standard genetic code, applications.

Unit -III Drug and Data Bases

Drug and Data bases: Introduction, classification of drugs, Drug Solubility/permeability, Drug Likeness Introduction to metabolic engineering and systems biology, role of metabolic simulations in drug discovery,

Unit-IV Computer Aided Drug Design

Introduction to molecular docking, rigid docking, flexible docking, 3D pharmacophore, 3D data base searching and virtual searching, pharmacophore modelling, brief introduction about various online tools for drug designing and molecular docking.

Text Books

1. Upadhayay, K. Upadhayay, N. Nath, Biophysical Chemistry (Principles and Techniques), Himalaya Publishing House, 2009.
2. David L. Nelson and Michael M. Cox, Lehninger Principles of Biochemistry, Fifth Edition, W. H. Freeman and Company, New York, 2008.

1

3. Young David. Computational drug design: A Guide for Computational and Medicinal Chemists.Publisher: Wiley. 2009. ISBN: 9780470126851

Reference books:

1. Bioinformatics: Sequence and Genome Analysis, Mount. D. W, CSHL Press, New York 2nd Edition 2004.
2. Introduction to Bioinformatics by Arthur M. Lesk University of Cambridge, Published in theUnited States by Oxford University Press Inc., New York
3. Introduction to Computational Biology: Maps, Sequences and Genomes, Waterman, M.,Chapman and Hall, 1995.
4. Abraham, Donald (Ed). Burger's medicinal chemistry and drug discovery. Publisher: John Wiley& Sons, Inc. 2003. ISBN: 0471270903
5. Schlick, T. Molecular modelling and simulation: an interdisciplinary guide. Publisher: Springer.2002. ISBN: 0-387-95404-X
6. Leach, Andrew. Molecular Modelling: Principles and Applications. Publisher: Prentice Hall.2001. ISBN: 0582239338.
7. Jensen, Jan H. Molecular Modeling Basics. Publisher: CRC Press. 2010. ISBN: 978- 1420075267
8. Hinchliffe Alan. Molecular modelling for beginners. Publisher: John Wiley and Sons Ltd. 2008.ISBN: 978 0470513149

E- Text book

1. Computer Aided Drug Design by Prof. Mukesh Doble, Biotechnology, IIT, Madras(SwayamNPTEL)

Syllabus for Semester II, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCT2001 **Category:** Engineering Science Course (ESC)

Course: Object Oriented Programming **L:** 3Hrs**, T:** 0Hr**, P:** 0Hr**, Per Week, Credits:** 3

Course Objectives

1. To make students understand Fundamental features of an object oriented language like Java: object classes and interfaces, exceptions and libraries of object collections
2. Introduce students with fundamental concepts like exception handling, generics, collection classes and streams.

Unit I: Features of Object-Oriented Programming languages, Abstraction, Encapsulation, Inheritance, polymorphism and late binding. Programming paradigms, Bytecode, JDK, JRE, JVM. Concept of a class and object, ways of representing objects, access control of members of a class, instantiating a class, constructor.

Unit II: Concept of overloading: Constructor Overloading, Function Overloading. Arrays and Array of objects, Wrapper classes (Integer, Double etc.), String Class, creating packages, importing packages. Lambda Expressions Introduction, Block, Passing Lambda expression as Argument

Unit III: Concept of inheritance, methods of derivation, use of super keyword and final keyword in inheritance, run time polymorphism, abstract classes and methods, Interface, implementation of interface, static and non-static members.

Unit IV: Exceptions, types of exception, use of try catch block, handling multiple exceptions, using finally, throw and throws clause, user defined exceptions, Introduction to streams, byte streams, character streams, file handling in Java, Serialization.

Unit V: Generics, generic class with two type parameter, bounded generics. Collection classes: Arraylist, LinkedList, TreeSet, HashMap, Iterator, ListIterator, Comparator, Comparable

Unit VI: Introduction to Design Patterns, Need of Design Pattern, Classification of Design Patterns, Role of Design Pattern in Software design, Creational Patterns, Structural Design Patterns and Behavioral Patterns.

Course Outcomes:

On successful completion of the course, students will be able to:

1. Understand the object-oriented programming features, classes, objects and methods.
2. Develop efficient programs by implementing the concept of Inheritance, polymorphism exception handling.
3. Use the concept of generics, collections, streams to develop solution to the given problem.
4. Analyze characteristics and need of design pattern in software design process.

Text Books

1. Herbert Schildt; JAVA The Complete Reference; Ninth Edition, Tata McGraw- Hill Publishing Company Limited.
2. Design Patterns By Erich Gamma, Pearson Education

Reference Books

1. Paul Deitel, Harvey Deitel; Java 9 for Programmers; Pearson
2. Herbert Schildt and Dale Skrien; Java Fundamentals A Comprehensive Introduction; Tata McGraw- Hill Education Private Ltd 2013

Syllabus for Semester II, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCP2001 **Category:** Engineering Science Course (ESC)

Course: Object Oriented Programming Lab **L:** 0Hr**, T:** 0Hr**, P:** 2Hr**, Per Week, Credits:** 1

Course Objectives

1. To develop ability of students to implement basic concepts and techniques of object oriented programming paradigm like encapsulation, inheritance, polymorphism, exception handling.
2. Develop solution to problems using collection classes, generics, streams, multithreading.

Course Outcomes

On completion of the course the student will be able to

1. Develop the solutions using basic features of Object-Oriented Programming.
2. Design efficient and reusable solutions using inheritance and exception handling techniques.
3. Create and use type-safe object through generics and collection classes.

SYLLABUS

Experiments based on the above Syllabus.

Syllabus for Semester II, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCT2002 **Category:** Programme Core Course (PCC)

Course: Computer Architecture **L:** 2Hrs**, T:** 0Hr**, P:** 0Hr**, Per Week, Credits:** 2

Course Objectives

The objective of this course is to familiarize the prospective engineers with:

1. Concepts of computer architecture by developing understanding of various functional units, components of computers and working of all the modules.
2. Design principles of modern computers including memory, bus system, input/output operation, interrupt handling mechanism and parallelization.

SYLLABUS

UNIT I: Basic Structure of Computers: Functional units of computer, basic operational concepts- Instruction, processor and memory, operating steps, address, Big- and Little-endian assignments, Instructions set architecture of a CPU- Instruction Formats, Instruction sequencing, addressing modes, and instruction set classification, subroutine & parameter passing, expanding opcode, RISC and CISC.

UNIT II: Basic Processing Unit and Data Representation: Basic Concepts- Instruction execution, Bus architecture- One bus and Multi-bus, Execution of a Complete Instruction, sequencing of control signals, Hardwired control, Micro-programmed Control. Floating point numbers-representation, guard bits and rounding.

UNIT III: Memory & Input/output: Cache memory, Cache size vs. block size, mapping functions, replacement algorithms, Cache read/write policy, Virtual Memory, I/O mapped I/O and memories mapped I/O, interrupt and interrupt handling mechanisms, vectored interrupts, synchronous vs. asynchronous data transfer, Bus Arbitration, Direct Memory Access

UNIT IV: Pipelining: Basic concepts of pipelining, throughput and speedup, Introduction of Parallel Computing: SISD, MISD, SIMD, MIMD

Course Outcomes:

On Successful completion of course, students will be able to:

1. Demonstrate the understanding about the functional units of a digital computer system.
2. Execute complete instruction on different types of bus architectures with control signal generation.
3. Analyse memory, multiprocessor and multicore architectures and their implications in parallel computing.

Text Books

1. V.C.Hamacher, Z.G.Vranesic and S.G.Zaky; Computer Organisation; 5th edition; Tata McGraw Hill, 2002.
2. W. Stallings; Computer Organization & Architecture; PHI publication; 2001.
3. J. P. Hayes; Computer Architecture & Organization; 3rd edition; McGraw-Hill; 1998.
4. Reference Books
5. M Mano; Computer System and Architecture; PHI publication; 1993.
6. A.S.Tanenbaum; Structured Computer Organization; Prentice Hall of India Ltd.

Syllabus for Semester II, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCT2003 **Category:** Vocational & Skill Enhancement Course (VSEC)

Course: Computer Workshop-2 **L:** 1Hr**, T:** 0Hr**, P:** 0Hr**, Per Week, Credits:**1

Course Objective

The objective of this course is to familiarize the students with an important web framework for developing user interfaces. It aims for developing high end web applications by the use of ReactJS features.

Course Outcomes

After successful completion of this course, the student will be able to,

1. Implement the fundamentals of React with Java Script and JSX
2. Understand Templating concept along with different types of components in ReactJS
3. Understand different state and Life Cycle Methods
4. Implement Router with react Router.

Course Contents UNIT-I

Introduction to React

React JS Introduction, Advantages of React JS, Introduction to JSX, Difference between JS and JSX.

UNIT-II

Components in React

React Components overview, Types of components, Controlled, Split Up, Composable, Reusable, Component Declarations and Styling Components

State and it significance, Read state and set state, Passing data to component using props, Validating props using prop Types, Supplying default values to props using default Props

UNIT-III

Routing with react router

Introduction to React Router, Routing in single page applications, Browser Router and Hash Router components Configuring route with Route component.

Text Books

1. Pure React- a step by step guide - Dave Ceddia
2. Road to learn react - Robin Wieruch
3. React in Action 1st Edition - Mark Tielens Thomas

Syllabus for Semester II, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCP2003 **Category:** Vocational & Skill Enhancement Course (VSEC)

Course: Computer Workshop-2 Lab **L:** 0Hr**, T:** 0Hr**, P:** 2Hrs**, Per Week, Credits:**1

Course Objective

The objective of this course is to familiarize the students with an important web framework for developing user interfaces. It aims for developing high end web applications by the use of ReactJS features.

Syllabus:

Practical based on Theory Syllabus

Course Outcomes

After successful completion of this course, the student will be able to

1. Understanding the fundamentals of ReactJS including components, props, state, and lifecycle methods.
2. Design and implement complex applications by composing smaller, reusable components together.
3. Building Web Applications to create dynamic and interactive web applications using React and other related technologies like JSX and ES6.
4. Implement React Router to handle client-side routing and create single-page applications.

Shri Ramdeobaba College of Engineering and Management
Department of Humanities

Course Code	Course Name	Sem.	Hours/week	Credits	Maximum marks	ESE
					Continuous Evaluation	2 hours
HUT1002/2002	English for Professional Communication	I/II	2	2	50	50

Syllabus and Scheme of English for Professional Communication Theory Scheme

Course Objectives

The main objective of this course is to enhance the employability skills of students as well as prepare them for effective work place communication.

Course outcomes:

On successful completion of the course the students will be able to achieve the following:

CO1. Demonstrate effective use of word power in written as well as oral communication.
CO2. Understand the techniques of listening and apply the techniques of reading comprehension used in professional communication.
CO3. Apply the principles of functional grammar in everyday as well as professional communication.
CO4. Effectively implement the comprehensive principles of written communication by applying various writing styles.
CO5. Create precise and accurate written communication products.

Unit-1: Vocabulary Building

1.1 Importance of using appropriate vocabulary
1.2 Techniques of vocabulary development
1.3 Commonly used power verbs, power adjectives and power adverbs.
1.4 Synonyms, antonyms, phrases & idioms, one-word substitutions and standard abbreviations

Unit -2: Listening and Reading Comprehension

2.1 Listening Comprehension: active listening, reasons for poor listening, traits of a good listener, and barriers to effective listening
2.2 Reading Comprehension: types and strategies.

Unit -3: Functional Grammar and Usage

3.1 Identifying Common Errors in use of: articles, prepositions, modifiers, modal auxiliaries, redundancies, and clichés
3.2 Tenses
3.3 Subject-verb agreement, noun-pronoun agreement
3.4 Voice

Unit-4: Writing Skills

4.1 Sentence Structures

4.2 Sentence Types
4.3 Paragraph Writing: Principles, Techniques, and Styles

Unit-5: Writing Practices

5.1 Art of Condensation: Précis, Summary, and Note Making
5.2 Correspondence writing techniques and etiquettes – academic writing
5.3 Essay Writing

Books

1. *Communication Skills*. Sanjay Kumar and PushpLata. Oxford University Press. 2011.
2. *Practical English Usage.* Michael Swan. OUP. 1995.
3. *Remedial English Grammar.* F.T. Wood. Macmillan.2007
4. *On Writing Well.* William Zinsser. Harper Resource Book. 2001
5. *Study Writing.* Liz Hamp-Lyons and Ben Heasly. Cambridge University Press. 2006.
6. *Exercises in Spoken English.* Parts. I-III. CIEFL, Hyderabad. Oxford University Press

Shri Ramdeobaba College of Engineering and Management
Department of Humanities

Syllabus and Scheme of English for Professional Communication Practical

Scheme

Course Code	Course Name	Sem.	Hours/week	Credits	Maximum marks
HUP1002/2002	English for Professional Communication Lab	I/II	2	1	50

Course Objective

To enhance competency of communication in English among learners

Course Outcomes

On completion of English Lab course, students will be able to achieve the following:

CO1: Apply effective listening and speaking skills in professional and everyday conversations.

CO2: Demonstrate the techniques of effective Presentation Skills

CO3: Evaluate and apply the effective strategies for Group Discussions

CO4: Analyse and apply the effective strategies for Personal Interviews

CO5: Implement essential language skills- listening, speaking, reading, and writing

Syllabus

List of practicals

Computer Assisted + Activity Based Language Learning Practical 1: Everyday Situations: Conversations and Dialogues – Speaking Skills **Practical 2:** Pronunciation, Intonation, Stress, and Rhythm

Practical 3: Everyday Situations: Conversations and Dialogues – Listening Skills

Activity Based Language Learning

Practical 4: Presentation Skills: Orientation & Mock Session **Practical 5:** Presentation Skills: Practice

Practical 6: Group Discussions: Orientation & Mock Session

Practical 7: Group Discussions: Practice

Practical 8: Personal Interviews: Orientation & Mock Session

Practical 9: Personal Interviews: Practice

Scheme and syllabus

Course Code	Course Name	Sem.	Hours/week	Credits	Maximum Marks (Continuous Evaluation)
HUP0001-1	Fundamentals of Indian Classical Dance: Bharatnatayam	I/II	2	1	50

Course objective

The course aims to introduce the students to Bharatnatyam, an important element of Indian traditional knowledge system. The course will not only provide the learning and skill to perform this art but would also enhance many mental and physical aspects of the students such as strength, flexibility, discipline, self-confidence, creativity, focus, coordination, etc.

Course Outcomes

On completion of the course, students will be able to achieve the following:

CO1: Understand the importance of dance and Bharatnataym as an Indian dance form CO2: Develop skills to perform the dance form at its basic level.

CO3: Evaluate their strengths and interest to take bridge course to give *Pratham* (1st level formal exam of Bharatnatayam).

Syllabus

Practical -1: Orientation in Bharatnatayam

Practical-2: Tattu Adavu till 8, Naatta Adavu 4 Steps, Pakka Adavu 1 step, Metta Adavu 1 Step, Kuditta Metta Adavu 4 Steps,

Practical -3: Practice sessions

Practical-4: Tatta Kuditta Adavu (Metta), Tatta Kuditta Adavu (Metta) 2 Steps, Tirmanam Adavu 3 Steps, Kattu Adav - 3 Steps, Kattu Adav - 3 Steps

Practical-5: Practice sessions

Practical-6: Tiramanam (front) 3 Steps, Repeat of Tiramanam (Overhead) 3 Steps, Practical-7: practice sessions

Practical – 8: final practice sessions and performances.

Recommended reading

1. *Introduction to Bharata's Natyasastra*, Adya Rangacharya, 2011
2. *The Natyasastra and the Body in Performance: Essays on the Ancient Text*, edited by Sreenath Nair, 2015
3. *Bharatanatyam How to ... : A Step-by-step Approach to Learn the Classical Form*, Eshwar Jayalakshmi, 2011

Scheme and syllabus

Course Code	Course Name	Sem.	Hours / week	Credits	Maximum Marks (Continuous Evaluation)
HUP0001-2	Fundamentals of Indian Classical Dance: Kathak	I/II	2	1	50

Course objective

The course aims to introduce the students to Kathak, an important element of Indian traditional knowledge system. The course will not only provide the learning and skill to perform this art but would also enhance many mental and physical aspects of the students such as strength, flexibility, discipline, self-confidence, creativity, focus, coordination, etc.

Course Outcomes

On completion of the course, students will be able to achieve the following: CO1: Understand the importance of dance and Kathak as an Indian dance form CO2: Develop skills to perform the dance form at its basic level.

CO3: Evaluate their strengths and interest to take bridge course to give *Prarambhik* (1^{st} level formal exam of Kathak).

Syllabus

Practical -1: Orientation in Kathak. Correct posture of kathak, Basic Movements and exercise Stepping, Chakkar of 5 count (Bhramari),

Practical -2: practice sessions of practical 1

Practical -3: Hastaks, Hastaks and Steppings, Reciting asamyukta Mudra shloka, Hastak and steppings

Practical -4: practice sessions of practical 3

Practical -5: Todas and Asamyukta hasta mudra shlok, Vandana of Shlok, 2 Todas and Vandana, Ghante Ki Tihai,

Practical -6: practice sessions of practical 5

Practical -7: 2 1 Chakkardar Toda and Ginnti Ki Tihai, 2 Todas and 1 Chakkardar Toda, practice sessions

Practical -8: Final performances.

Recommended reading

1. Kathak Volume1 A "Theoretical & Practical Guide" (Kathak Dance Book), Marami Medhi & Debasish Talukdar, 2022, Anshika Publication (13 September 2022)

Scheme and syllabus

Course Code	Course Name	Sem.	Hours/week	Credits	Maximum Marks (Continuous Evaluation)
HUP0001-3	Introduction to Digital Photography	I/II	2	1	50

Course objective

The course aims to develop basic skills of students in digital photography to lay a foundation for them as a hobby and/or a profession.

Course outcome:

At the end of the course the students will be able to achieve the following:

CO1: Develop an understanding of the technical aspects and aesthetics of Photography. CO2: Apply the rules of digital photography for creating photographs.

CO3: Develop skills to enhance photographs through post processing. CO4: Create a portfolio of their photographs in selected genre.

Syllabus

Practical 1: **Orientation in digital photography:** Genres, camera handling and settings Practical 2: **Rules of Composition**

Practical 3: **Rules of Composition**: practice sessions

Practical 4: **Understanding Exposure and Art of Pre-Visualization**

Practical 5: **Rules of Composition and Art of Pre-Visualization:** practice sessions

Practical 6: **Post Processing Photographs and Portfolio creation**

Practical 7: **Post Processing Photographs:** practice sessions

Practical 8: **Portfolio finalization and presentation in selected genre.**

Reference material

1. Scott Kelby (2020) *The Digital Photography Book: The Step-by-Step Secrets for how to Make Your Photos Look Like the Pros*, Rocky Nook, USA
2. Larry Hall (2014) *Digital Photography Guide: From Beginner to Intermediate: A Compilation of Important Information in Digital Photography*, Speedy Publishing LLC, Newark
3. J Miotke (2010) *Better Photo Basics: The Absolute Beginner's Guide to Taking Photos Like a Pro*, AMPHOTO Books, Crown Publishing Group, USA

Scheme and syllabus

Course Code	Course Name	Sem.	Hours/week	Credits	Maximum Marks (Continuous Evaluation)
HUP0001-4	Introduction to Japanese Language and Culture	I/II	2	1	50

Course objective

The course aims to develop basic communication skills in Japanese Language and help develop a basic understanding of Japanese culture in cross-cultural communication.

Course outcome

CO1: Gain a brief understanding about Japan as a country and Japanese culture.
CO2: Develop ability to use vocabulary required for basic level communication in Japanese language. CO3: Able to write and read the first script in Japanese language.
CO4: Able to frame simple sentences in Japanese in order to handle everyday conversations CO5: Able to write in basic Japanese about the topics closely related to the learner.

Syllabus

Practical-1: Orientation about Japan, its language, and its culture
Practical-2: Communication Skills 1: Vocabulary for basic Japanese language
Practical -3: Practice sessions
Practical-4: Writing Skills 1: Reading and writing first script in Japanese
Practical-5: Practice sessions
Practical- 6: Communication Skills 2: framing sentences
Practical- 7: Practice sessions
Practical- 8: Writing Skills 2: Write basic Japanese and practice

Recommended reading

1. Marugoto Starter (A1) Rikai - Course Book for Communicative Language Competences, by The Japan Foundation, Goyal Publishers & Distributors Pvt. Ltd (ISBN: 9788183078047)
2. Japanese Kana Script Practice Book – Vol. 1 Hiragana, by Ameya Patki, Daiichi Japanese Language Solutions (ISBN: 9788194562900)

Scheme and syllabus

Course Code	Course Name	Sem.	Hours / week	Credits	Maximum Marks (Continuous Evaluation)
HUP0001-5	Art of Theatre	I/II	2	1	50

Course objectives:

The course aims to develop in the students, an actor's craft through physical and mental training.

Course Outcomes:

On completion of the course, students will be able to achieve the following:

CO1: Understand and synthesize the working of the prominent genres of theatre across the world. CO2: Apply the skill of voice and speech in theatre and public speaking

CO3: Apply the art of acting and also develop generic skills such as confidence, communication skills, self-responsibility, motivation, commitment, interpersonal skills, problem solving, and self-discipline. CO4: Apply skills acquired related to technical/production aspects of theatre and also develop problem solving and interpersonal skills.

Syllabus:

Syllabus

Practical 1: **Orientation in theatre**

Practical 2: **Voice and Speech training**

Practical 3: **Voice and Speech training**: practice sessions Practical 4: **Art of acting**

Practical 5: **Art of acting:** practice sessions

Practical 6: **Art of script writing**

Practical 7: **Art of script writing:** practice sessions

Practical 8: **Final performances**

Reference books:

1. Boleslavsky, R. (2022). *Acting: The First Six Lessons* (1st ed., pp. 1-92). Delhi Open Books.
2. Shakthi, C. (2017). *No Drama Just Theatre* (1st ed., pp. 1-171). Partridge.
3. Bruder, M., Cohn, L. M., Olnek, M., Pollack, N., Previto, R., & Zigler, S. (1986). *A Practical Handbook for the Actor* (1st ed.). Vinatge Books New York.

Scheme and syllabus

Course Code	Course Name	Sem.	Hours/week	Credits	Maximum Marks (Continuous Evaluation)
HUP0001-6	Introduction to French Language	I/II	2	1	50

Course objective:

To help build a foundation and interest in French language so that the students can pursue the proficiency levels of the language in higher semesters.

Course outcomes:

On successful completion of the course the students will be able to achieve the following:
CO1. Demonstrate basic knowledge about France, the culture and similarities/differences between India and France
CO2. Learn to use simple language structures in everyday communication. CO3. Develop ability to write in basic French about themselves and others. CO4. Develop ability to understand beginner level texts in French

Syllabus
List of Practicals

Practical-1: Orientation about France, the language, and culture
Practical-2: Communication Skills 1: Vocabulary building for everyday conversations
Practical -3: Practice sessions
Practical-4: Reading and writing Skills : Reading and writing simple text in French
Practical-5: Practice sessions
Practical-6: Communication Skills 2: listening comprehension
Practical-7: Practice sessions
Practical-8: Writing Skills: Write basic French and practice

Recommended reading

1. 15-minute French by Caroline Lemoine
2. Cours de Langue et de Civilisation Françaises by G. Mauger Vol. 1.1
3. Cosmopolite I by Natalie Hirschsprung, Tony Tricot

Scheme and syllabus

Course Code	Course Name	Sem.	Hours/week	Credits	**Maximum Marks (Continuous Evaluation)**
HUP0001-7	Introduction to Spanish Language	I/II	2	1	50

Course objective:

To help build a foundation and interest in Spanish language so that the students can pursue the proficiency levels of the language in higher semesters.

Course outcomes:

On successful completion of the course the students will be able to achieve the following:
CO1. Demonstrate basic knowledge about Spain, the culture and similarities/differences between India and France
CO2. Learn to use simple language structures in everyday communication. CO3. Develop ability to write in basic Spanish about themselves and others. CO4. Develop ability to read and understand beginner level texts in Spanish

Syllabus
List of Practicals

Practical-1: Orientation about Spain, the language, and culture
Practical-2: Communication Skills 1: Vocabulary building for everyday conversations
Practical -3: Practice sessions
Practical-4: Reading and writing Skills : Reading and writing simple text in Spanish
Practical-5: Practice sessions
Practical-6: Communication Skills 2: listening comprehension
Practical-7: Practice sessions
Practical-8: Writing Skills: Write basic Spanish and practice

Recommended reading

1. 15-Minute Spanish by Ana Bremon
2. Aula Internacional 1 by Jaime Corpas ,Eva Garcia, Agustin Garmendia.
3. Chicos Chicas Libro del Alumno by María Ángeles Palomino

Scheme and syllabus

Course Code	Course Name	Sem.	Hours/week	Credits	Maximum Marks (Continuous Evaluation)
HUP0001-8	Art of Painting	I/II	2	1	50

Course objective

Painting is fundamentally about learning to see, and to transport that vision onto paper through a variety of mark making techniques. This course aims to develop basic skills of students in painting to lay a foundation for them as a hobby and/or a profession.

Course outcome:

At the end of the course the students will be able to achieve the following: CO1: Become familiar with the basic methods, techniques & tools of painting. CO2: Train the eye and hand to develop sense of balance, proportion and rhythm. CO3: Develop the ability to observe and render simple natural forms.
CO4: Enjoy the challenging and nuanced process of painting.

Syllabus

Practical 1: **Orientation in Painting tools & basics of lines, shapes, light, shadows and textures**
Practical 2: **The art of observation** how to see shapes in drawing
Practical 3: **Introduction Water color** how to handle water paints
Practical 4: **Introduction to acrylic colors** how to handle acrylic paints
Practical 5: **Explore layering paint and capturing the quality of light with paint.**
Practical 6: **Create landscape painting**
Practical 7: **Create Abstract painting**
Practical 8: **Paint on Canvas** (try to recreate any famous painting)

Reference material

1. Drawing made easy by Navneet Gala; 2015th edition
2. Alla Prima II Everything I Know about Painting--And More by Richard Schmid with Katie Swatland
3. Daily Painting: Paint Small and Often To Become a More Creative, Productive, and Successful Artist by Carol Marine

Scheme and syllabus

Course Code	Course Name	Sem.	Hours/ week	Credits	Maximum Marks (Continuous Evaluation)
HUP0001-9	Art of Drawing	I/II	2	1	50

Course objective

Drawing is fundamentally about learning to see, and to transport that vision onto paper through a variety of mark making techniques. This course aims to develop basic skills of students in drawing to lay a foundation for them as a hobby and/or a profession.

Course outcome:

At the end of the course the students will be able to achieve the following: CO1: Become familiar with the basic methods, techniques & tools of drawing. CO2: Train the eye and hand to develop sense of balance, proportion and rhythm. CO3: Develop the ability to observe and render simple natural forms.
CO4: Enjoy the challenging and nuanced process of drawing.

Syllabus

Practical 1: **Orientation in Drawing tools & basics of lines, shapes, light, shadows and textures**
Practical 2: **The art of observation** how to see shapes in drawing
Practical 3: **One/two-point basic linear perspective**
Practical 4: **Nature drawing and landscapes**
Practical 5: **Gestalt principles of visual composition**
Practical 6: **Figure drawing**: structure and proportions of human body
Practical 7: **Gesture drawing:** expression and compositions of human figures Practical 8: **Memory drawing:** an exercise to combine the techniques learnt

Reference material

1. Drawing made easy by Navneet Gala; 2015th edition
2. Perspective Made Easy (Dover Art Instruction) by Ernest R. Norling

Scheme and syllabus

Course Code	Course Name	Sem.	Hours/week	Credits	Maximum Marks (Continuous Evaluation)
HUP0001-10	**Nature camp**	II	2	1	50

Course Objective: To create an opportunity for the students to develop affinity with nature and thus subsequently impact their ability to contribute towards sustainability of nature.

Course outcome:

After the completion of the course the students will be able to do the following:

CO1: Develop an affinity with nature by observing and understanding it marvels with guidance from experts

CO2: Develop an understanding of the challenges and solutions associated with nature and its conservation.

Course content

In collaboration with the Forest Department and/or a local NGO working in the field of environment conservation, this course would be conducted in 24 hours. Students will be taken to a tiger reserve in Central Indian region or Forest fringe villages or work with an NGO from Central Indian region working on natural resource management. The camps (for 2 days) will cover any one of the following topics as decided by the course coordinator:

1. Awareness about each element of biodiversity (camps on moths, butterflies, birds, other wildlife etc)
2. Environment management (water, forest, wildlife) – practices of Forest Department in managing a tiger reserve, and other aspects of water and forest conservation.
3. Sustainable natural resource management - initiatives by rural communities and local NGOs
4. Man-animal conflict and solutions (socio-economic and technical) – role of local communities and Forest Department
5. Traditional practices in environment conservation – role of local communities and local NGOs

SHRI RAMDEOBABA COLLEGE OF ENGINEERING & MANAGEMENT,
NAGPUR DEPARTMENT OF PHYSICAL EDUCATION

Syllabus of Semester I and II UG Engineering Program COURSE:
DISSASTER MANAGEMENT THROUGH ADVENTURE SPORTS

Code: PEP0001-21 **Course Type:** Liberal Arts

L: 0 Hrs. T: 0 Hrs. P: 2 Hrs. Per Week **Total Credits:** 01

Objectives of the Course:

To enable the student:

1. To inculcate rational thinking and scientific temper among the students.
2. To develop critical awareness about the social realities among the students.
3. To build up confidence, courage and character through adventure sports.

Course Outcomes:

On completion of the course, students will be able to:

1. Understand the meaning and importance of Adventure sports.
2. Learn the various types of adventure sports, the equipment and resources required to practice disaster Management activities.
3. Learn the safety measures about different risk and their management.
4. To apply Disaster management theory to institutional & Societal problems and situations.

Course Content:

1. Basic adventure
2. First AID
3. various types of knots
4. Shelter making
5. Disaster management
6. Team building and goal setting
7. Realization of fear, risk and their roles and analyzing safety Management Plan

SHRI RAMDEOBABA COLLEGE OF ENGINEERING & MANAGEMENT, NAGPUR DEPARTMENT OF PHYSICAL EDUCATION

Syllabus of Semester I and II UG Engineering Program

COURSE: SELF-DEFENSE ESSENTIALS AND BASICS KNOWLEDGE OF DEFENSE FORCES

Course Code: PEP0001-22 **Course Type:** Liberal Arts

L: 0 Hrs. T: 0 Hrs. P: 2 Hrs. Per Week **Total Credits:** 01

Course Outcomes:

On completion of the Course the student will be able to:

- Understand the meaning, need and fitness requirements to implement self-defense
- Learn the basic techniques of selected combative sports.
- Learn to prepare basic Physical Training for Defense forces.
- Implement survival techniques during emergencies.

Course Content:

- General conditioning and self-defense specific conditioning
- Applications of techniques of combative sports for self-defense.
- Self-defense techniques for specific situations: chain snatching, knife or stick attack, holding from back or front etc.
- Basic Military Knowledge and exposure making students Confident, bold, disciplined and trains them to join Armed Forces.

Course Code	CHP0001-31				
Category	Basket of Liberal Learning Course				
Course Title	**Art of Indian traditional cuisine**				
Scheme& Credits	L	T	P	Credits	Semester I/II
	0	0	2	1	

Course outcome:
At the end of the course the students will be able to achieve the following:

CO1: Understand the factors that affect regional eating habits and the unique ingredients found in variousstates of India
CO2: Get insight to prepare popular dishes from various regions of India. ·

Module 1: Indian Regional foods and snacks - factors effecting eating habits.
Module 2: Indian gravies – ingredients, their importance
Module 3: Indian Sweets - ingredients, their importance
Module 4: Presentation of Indian Meals, Menu Planning, Food Costing
Module 5: Food Preservatives and Safety

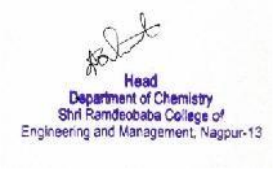
List of experiments:

1) Introduction to cookery: does and don'ts
2) Introduction to Indian cuisine, philosophy and classification.
3) Regional influence on Indian Food- factors affecting eating habits
4) Preparation of Garam masala and or Chat masala with ingredients and their importance
5) Preparation of different gravies such as white, yellow or brown gravies with ingredients and theirimportance
6) Preparation of Indian sweets like Besan ke laddu with ingredients and their importance
7) Presentation of meal, Menu planning and Food costing
8) Common chemical food preservatives and their safety standards.

Reference books

[1] Arora, K.,; Theory of cookery; First Edition, Frank Brothers Company (Pub) Pvt. Ltd., 2008 ISBN:9788184095036, 8184095031
[2] Philip, Thangam . E.,; Modern Cookery: Vol. 1; Sixth Edition, Orient BlackSwan., 2008 ISBN:9788125040446, 8125040447ali
[3] Parvinder S;Quantity Food Production Operations and Indian Cuisine (Oxford Higher Education); FirstEdition; Oxford University Press, 2011 ISBN 10: 0198068492 ISBN 13: 9780198068495
[4] Singh, Yogesh; A Culinary Tour of India; First Edition I.K. International Publishing House Pvt. Ltd.
ISBN 978-93-84588-48-9
[5] Singh Shakesh;Simplifying Indian Cuisine;First Edition, Aman Publications, ISBN81-

8204-054-X
[6] Dubey Krishna Gopal; The Indian Cuisine;PHI Learning Pvt. Ltd.ISBN978-81 203-4170-8



Course Code	**CHP0001-32**				
Category	Basket of Liberal Learning Course				
Course Title	**Introduction to Remedies by Ayurveda**				
Scheme & Credits	L	T	P	Credits	Semester I/II
	0	0	2	1	

Course outcome:

At the end of the course the students will be able to achieve the following

CO1: Know basic principle of Ayurvedic formulations. CO2:
Different types of Natural Remedies.
CO3: Basic idea about their Characterization

Module 1- Introduction to Ayurveda
Module 2- Different types of Ayurvedic formulations: Churn, Bhasma, Vati, Tailum Module 3- Introduction to Methods of preparation
Module 4 -Characterization, applications Practicals
based on above syllabus

1) Preparations of some medicinal oils like Bramhi tel, Bramhi Awala, Vatnashak Tel, Bhurngraj Tel etc.
2) Preparation of Churn, like Trifala Churn, Hingastak Churn, Trikut Churn etc.
3) Preparation of some Bhasmas and vati

Books

1) Chemistry and Pharmacology of Ayurvedic Medicinal Plants by Mukund Sabnis, Chaukhambha Amarbharati Prakashan.
2) Everyday Ayurveda by Shailesh Rathod
3) A text Book of Rasashastra by Vikas Dhole and Prakash Paranjpe
4) A text Book of Bhaiajya Kalpana Vij¯nana

Course Code	HUT2004				
Category	Value Education Course (VEC)				
Course Title	**Foundation course in Universal Human Values**				
Scheme & Credits	L	T	P	Credits	Semester II
	1	0	0	1	

Course Objectives:

1. To help the student see the need for developing a holistic perspective of life
2. To sensitize the student about the scope of life – individual, family (inter-personal relationship), society and nature/existence
3. To strengthen self-reflection
4. To develop more confidence and commitment to understand, learn and act accordingly

Course outcome:
On completion of course, students will be able to achieve the following:
CO1: Develop a holistic perspective of life
CO2: Better understanding of inter-personal relationships and relationship with society and nature.
CO3: An ability to strengthen self-reflection.

Syllabus
Unit 1:- Aspirations and concerns

Need for Value Education: Guidelines and content of value education.
Exploring our aspirations and concerns:Knowing yourself, Basic human aspirations Need for a holistic perspective, Role of UHV; Self-Management: harmony in human being

Unit 2:- Health
Harmony of the Self and Body, Mental and physical health; Health for family, friends and society.

Unit 3:- Relationships and Society
Harmony in relationships, Foundational values: Trust, Respect, Reverence for excellence, Gratitude and love; harmony in society; harmony with nature.

Reference Material:

1. The primary resource material for teaching this course consists of

Text book: R.R Gaur, R Sangal, G P Bagaria, A foundation course in Human Values and professional Ethics, Excel books, New Delhi, 2010, ISBN 978-8-174-46781-2

2. Reference books:

a) B L Bajpai, 2004, Indian Ethos and Modern Management, New Royal Book Co., Lucknow. Reprinted 2008.
b) PL Dhar, RR Gaur, 1990, Science and Humanism, Commonwealth Purblishers.
c) Sussan George, 1976, How the Other Half Dies, Penguin Press. Reprinted 1986, 1991
d) Ivan Illich, 1974, Energy & Equity, The Trinity Press, Worcester, and HarperCollins, USA
e) Donella H. Meadows, Dennis L. Meadows, Jorgen Randers, William W. Behrens III, 1972, limits to Growth, Club of Rome's Report, Universe Books.
f) Subhas Palekar, 2000, How to practice Natural Farming, Pracheen(Vaidik) Krishi Tantra Shodh, Amravati.
g) A Nagraj, 1998, Jeevan Vidya ek Parichay, Divya Path Sansthan, Amarkantak.
h) E.F. Schumacher, 1973, Small is Beautiful: a study of economics as if people mattered, Blond & Briggs, Britain.
i) A.N. Tripathy, 2003, Human Values, New Age International Publishers.

Syllabus for Semester III
B. Tec. Computer Science & Engineering (Cyber Security)

Course Code: CCT3001 **Course Name: Data Structures**
L: 3 Hrs T: 1 Hr P: 0 Hr Per Week **Total Credits: 4**

Course Objectives:

1. To impart to students the basic concepts of data structures and algorithms.
2. To familiarize students on different searching and sorting techniques.
3. To prepare students to use linear (stacks, queues, linked lists) and non-linear (trees, graphs) data structures.
4. To enable students to devise algorithms for solving real-world problems.

Syllabus:

UNIT I Data Structures and Algorithms Basics

- Introduction: basic terminologies, elementary data organizations, data structure operations; abstract data types (ADT) and their characteristics.
- Algorithms: definition, characteristics, analysis of an algorithm, asymptotic notations, time and space tradeoffs.
- Array ADT: definition, operations and representations – row-major and column- major.

UNIT II Stacks and Queues

- Stack ADT: allowable operations, algorithms and their complexity analysis, applications of stacks – expression conversion and evaluation (algorithmic analysis), multiple stacks.
- Queue ADT: allowable operations, algorithms and their complexity analysis for simple queue and circular queue, introduction to double-ended queues and priority queues.

UNIT III Linked Lists

- Singly Linked Lists: representation in memory, algorithms of several operations: traversing, searching, insertion, deletion, reversal, ordering, etc.
- Doubly and Circular Linked Lists: operations and algorithmic analysis. Linked representation of stacks and queues, header node linked lists.

UNIT IV Sorting and Searching

- Sorting: different approaches to sorting, properties of different sorting algorithms (insertion, Shell, quick, merge, heap, counting), performance analysis and comparison.
- Searching: necessity of a robust search mechanism, searching linear lists (linear search, binary search) and complexity analysis of search methods.

UNIT V Trees

- Trees: basic tree terminologies, binary tree and operations, binary search tree [BST] and operations with time analysis of algorithms, threaded binary trees.
- Self-balancing Search Trees: tree rotations, AVL tree and operations, B+-tree: definitions, characteristics, and operations (introductory).

UNIT VI Graphs and Hashing

- Graphs: basic terminologies, representation of graphs, traversals (DFS, BFS) with complexity analysis, path finding (Dijkstra's SSSP, Floyd's APSP), and spanning tree (Prim's method) algorithms.
- Hashing: hash functions and hash tables, closed and open hashing, randomization methods (division method, mid-square method, folding), collision resolution techniques.

Course Outcomes:

On completion of the course the student will be able to

1. Recognize different ADTs and their operations and specify their complexities.
2. Design and realize linear data structures (stacks, queues, linked lists) and analyze their computation complexity.
3. Devise different sorting (comparison based, divide-and-conquer, distributive, and tree-based) and searching (linear, binary) methods and analyze their time and space requirements.
4. Design traversal and path finding algorithms for Trees and Graphs.

Text Books:

1. Ellis Horowitz, Sartaj Sahni & Susan Anderson-Freed, Fundamentals of Data Structures in C, Second Edition, Universities Press, 2008.
2. Mark Allen Weiss; Data Structures and Algorithm Analysis in C; Second Edition; Pearson Education; 2002.
3. G.A.V. Pai; Data Structures and Algorithms: Concepts, Techniques and Application; First Edition; McGraw Hill; 2008.

Reference Books:

1. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein; Introduction to Algorithms; Third Edition; PHI Learning; 2009.
2. Ellis Horowitz, Sartaj Sahni and Sanguthevar Rajasekaran; Fundamentals of Computer Algorithms; Second Edition; Universities Press; 2008.
3. A. K. Sharma; Data Structures using C, Second Edition, Pearson Education, 2013.

Syllabus for Semester - III, B.TECH. CSE (Cyber Security)

Course Code: CCP3001 Course Name: Data Structure Lab

L: 0 Hrs T: 0 Hrs P: 2 Hrs Per Week Total Credits: 1

Course Objectives:

1. To enable students to employ different searching and sorting methods.
2. To prepare students to identify and apply linear (stacks, queues, linked lists) and non- linear (trees, graphs) data structures in solving problems.
3. To encourage students to design and execute tree-based algorithms for solving real- world problems.

Syllabus:

Experiments based on CCT203 Syllabus in C | C++

Course Outcomes:

On completion of the course the student will be able to

1. Design and realize different linear data structures.
2. Identify and apply specific methods of searching and sorting to solve a problem.
3. Implement and analyze operations on binary search trees and AVL trees.
4. Implement graph traversal algorithms, find shortest paths and analyze them.

Reference Books:

1. K R. Venugopal and Sudeep. R Prasad; Mastering C; Second Edition; McGraw Hill; 2015.
2. Ellis Horowitz, Sartaj Sahni & Susan Anderson-Freed, Fundamentals of Data Structures in C, Second Edition, Universities Press, 2008.
3. Mark Allen Weiss; Data Structures and Algorithm Analysis in C; Second Edition; Pearson Education; 2002.

Syllabus for Semester - III, B.TECH. CSE (Cyber Security)

Course Code:	**CCT3002**	**Course Name:**	**Computer Networks**		
L: 3 Hrs	**T: 0 Hrs**	**P: 0 Hrs**	**Per Week**	**Total Credits:**	**3**

Course Objectives:

1. To develop an understanding of modern network architectures from a design and performance perspective.
2. To introduce the student to the major concepts involved in network protocols.
3. To provide an opportunity to do network programming.

Syllabus:

UNIT I

- Data communication Components: Representation of data and its flow Networks, Various Connection Topology, Protocols and Standards, OSI model, Transmission Media, LAN: Wired LAN, Wireless LANs, Techniques for Bandwidth utilization: Multiplexing - Frequency division, Time division and Wave division

UNIT II

- Data Link Layer: Error Detection and Error Correction - Fundamentals, Block coding, Hamming Distance, CRC; Flow Control and Error control protocols - Stop and Wait, Go back – N ARQ, Selective Repeat ARQ.

UNIT III

- Medium Access Sub Layer: Switching, Random Access, Multiple access protocols - Pure ALOHA, Slotted ALOHA, CSMA/CD, CDMA/CA, IEEE 802 standard protocols.

UNIT IV

- Network Layer: Internet Protocol (IP) – Logical Addressing: IPV4, IPV6; Address mapping: ARP, RARP, BOOTP and DHCP–Delivery, Forwarding and Unicast Routing protocols.

UNIT V

- Transport Layer: Elements of Transport protocols: Addressing, Connection establishment,
- Connection release, Crash recovery, User Datagram Protocol (UDP), Transmission Control Protocol
- (TCP), TCP Congestion Control; Quality of Service, QoS improving techniques: Leaky Bucket and
- Token Bucket algorithm.

UNIT VI

- Application Layer: Domain Name Space (DNS), DDNS, TELNET, EMAIL, File Transfer Protocol (FTP), WWW, HTTP, SNMP, Bluetooth, Firewalls

Course Outcomes:

On successful completion of the course, students will be able to:

1. Understand basics of computer networks and reference models
2. Identify the Design issues of each layer of OSI model
3. Implement the protocols of OSI model

Text Books:

1. Computer Networks: 5th ed by Andrew. S. Tanenbaum. PHI Publication.
2. Data Communications and Networks: 3rd ed by Behrouz A. Forouzan. Tata McGraw Hill Publication.

Reference Books:

1. James F. Kurose and Keith W. Ross: Computer Networking: A Top-Down Approach Featuring the Internet, 3rd Edition.
2. William Stallings, “Data and Computer Communications”, PHI 6th Edition

Syllabus for Semester - III, B. TECH. CSE (Cyber Security)

Course Code:	**CCP3002**	**Course Name:**	**Computer Networks Lab**		
L: 0 Hrs	**T: 0 Hrs**	**P: 2 Hrs**	**Per Week**	**Total Credits:**	**1**

Course Objectives:

1. To introduce use of different network simulation software.
2. To analyze performance of different protocols at various layers of a network architecture.
3. To demonstrate the implementation of various networking concepts.

Syllabus:

Experiments based on CCP3002 Syllabus.

Course Outcomes:

On successful completion of the course, students will be able to:

1. Simulate and then configure different types of networks.
2. Implement algorithms present in different layers of OSI model
3. Implement networking concepts like server, client and addressing mechanism.

Syllabus for Semester - III, B.TECH. CSE (Cyber Security)

Course Code:	**CCP3003**	**Course Name:**	**Software Lab 1**		
L: 0 Hrs	**T: 0 Hrs**	**P: 2 Hrs**	**Per Week**	**Total Credits:**	**1**

Course Objectives:

1. To introduce the Python programming language.
2. To teach how to use Python for cybersecurity tasks.
3. To develop skills in automating security tasks using Python.

Syllabus:

Lab 1: Introduction to Python & Python Basics

- Overview of Python
- Installation and setup
- Variables, data types, and operators
- Control flow: loops and conditional statements
- Functions and modules

Lab 2: Working with Files

Lab 3: Python Libraries for Cyber Security

- Introduction to key libraries (e.g., socket, requests, scapy)
- Using libraries for network programming and analysis

Lab 4: Web Scraping and Data Analysis

Lab 5: Network Security with Python

Lab 6: Web Application Security

Lab 7: Cryptographic Operations

Lab 8: Penetration Testing with Python

Course Outcomes:

After successful completion of the course students will be able to:

1. Write Python scripts to automate security tasks.
2. Use Python libraries for network analysis and penetration testing.
3. Develop simple security tools using Python.

Reference books:

Title: Black Hat Python: Python Programming for Hackers and Pentesters
Author: Justin Seitz
Publisher: No Starch Press

Title: Violent Python: A Cookbook for Hackers, Forensic Analysts, Penetration Testers and Security Engineers
Author: TJ O'Connor
Publisher: Syngress

Title: Python Forensics: A Workbench for Inventing and Sharing Digital Forensic Technology
Authors: Chet Hosmer, Joshua I. James
Publisher: Syngress

Title: Python Network Programming for Network Engineers (Python Programming for Network Engineers)
Author: Brandon Rhodes, John Goerzen
Publisher: O'Reilly Media

Title: Gray Hat Python: Python Programming for Hackers and Reverse Engineers
Author: Justin Seitz
Publisher: No Starch Press

Syllabus for Semester - III, B.TECH. CSE (Cyber Security)

Course Code:	**MAT3003**	**Course Name:**	**Mathematics for Cyber Security**		
L: 3 Hrs	**T: 0 Hrs**	**P: 0 Hrs**	**Per Week**	**Total Credits:**	**3**

Course Objective:

1. Introduce basic concepts and knowledge in number theory, together with a wide variety of interesting applications of discrete mathematics.
2. Train students to solve problems from algorithm design and analysis, coding theory etc. and to apply techniques of number theory in cryptography.
3. Provide a foundational understanding and application of linear algebra concepts relevant to various aspects of computer science and related fields

Syllabus:

Module 1: (9 Lectures) Algebra of matrices, Inverse and rank of a matrix, rank-nullity theorem; System of linear equations; orthogonal matrices; Eigenvalues and eigenvectors; Diagonalization of matrices; Cayley-Hamilton Theorem, Orthogonal transformation and quadratic to canonical forms.

Module 2: (9 Lectures)
Ring, Subring, Integral Domain, Field, Finite field, Factorization of polynomials over a field, Elliptic curves, Elliptic curves over finite field.

Module 3: (12 Lectures)
Fermat's Number , Fermat's theorem, Euler's theorem, Pseudoprimes, Quadratic Residues, Primitive roots. Euler's formula and roots modulo pq with its application, RSA algorithm in cryptography.

Module 4: (8 Lectures)
Discrete Logarithms and the Discrete Log Problem, Pollard's ρ-Algorithm, Primality Testing-Sieving Methods, Fermat's Primality Testing, and Probabilistic Primality Testing.

Course Outcomes:

On successful completion of the course, student shall be able to

1. Understand matrix algebra and use it to compute Eigen values, Eigen vectors and orthogonal transformations.
2. Apply concepts of group and ring theory to solve problems related to elliptic curves over finite field.
3. Apply Modular arithmetic to generate public key, privet key in security system algorithm.
4. Apply techniques of number theory to solve problems from algorithm design and analysis, coding theory etc. in cryptography

Textbooks:

1. Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery, 'An introduction to the theory of numbers', John Wiley and Sons 2004.
2. David M Burton, 'Elementary Number Theory' , McGraw Hill, Seventh edition 2014.
3. Fraleigh J. B., 'A first course in abstract algebra', Narosa, 1990.
4. B.S. Grewal, Higher Engineering Mathematics, Khanna Publishers, 35th Edition, 2000.

References:

1. Wade Trappe, Lawrence C. Washington, 'Introduction to Cryptography with Coding Theory', Pearson Education International 2012.
2. Baumslag, Fine, Kreuzer, Rosenberger., 'A Course in Mathematical cryptography', De Gruyter Graduate, 2015.

Syllabus for Semester - III, B.TECH. CSE (Cyber Security)

Course Code:	**CCP3005**	**Course Name:**	**Idea Lab**		
L: 0 Hrs	**T: 0 Hrs**	**P: 4 Hrs**	**Per Week**	**Total Credits:**	**2**

Course Objective:

1. The course aims to provide participants with a comprehensive understanding of design thinking principles, prototyping fundamentals, entrepreneurship essentials, and business development strategies.

2. Through a combination of theoretical learning and hands-on exercises, participants will gain the knowledge and skills necessary to identify market needs, develop innovative solutions, and successfully launch entrepreneurial ventures.

Syllabus:

Module 1: Introduction to Design Thinking and Ideation, Understanding the design thinking process, Empathy and user-centered design, Ideation techniques: brainstorming, mind mapping, etc., Identifying market needs and opportunities.

Module 2: Prototyping Fundamentals, Introduction to rapid prototyping tools and techniques, Hands-on exercises in prototyping using low-fidelity materials, Iterative design process: testing and refining prototypes

Module 3: Entrepreneurship Essentials, Introduction to entrepreneurship and lean startup methodology, developing a value proposition and business model canvas, Identifying target customers and validating market demand

Module 4: Business Development and Pitching, crafting persuasive pitches and presentations, Financial modeling and revenue projections, Pitching prototypes and business concepts to a panel of experts

Module 5: Project Implementation and Showcase, implementing prototypes and gathering user feedback, Iterating based on feedback and improving prototypes, Final showcase event: presenting prototypes and business ventures to peers, faculty, and industry, professionals.

Course Outcome:

After Completing this course students will be able to:

1. Gain a deep understanding of the design thinking process, generating creative ideas through ideation techniques, and translating ideas into actionable prototypes.
2. Acquire proficiency in rapid prototyping tools and techniques, enabling them to efficiently create and iterate low-fidelity prototypes.
3. Develop skills in testing and refining prototypes through an iterative design process.
4. Implement prototypes, gather user feedback, and iterate based on insights gained.

Syllabus for Semester - III, B.TECH. CSE (Cyber Security)

Course Code:	**CCT3006**	**Course Name:**	**Cyber Law and Ethics**		
L: 2 Hrs	**T: 0 Hrs**	**P: 0 Hrs**	**Per Week**	**Total Credits:**	**2**

Course Objectives:

1. Describe laws governing cyberspace and analyze the role of Internet Governance in framing policies for Internet security
2. Identify intellectual property right issues in the cyberspace and design strategies to protect your intellectual property
3. Understand the importance of freedom of expression, defamation and hate speech in the Cyber world.
4. Recognize the importance of digital divide, contingent workers and whistle blowing situations.

Syllabus:

UNIT I: Cyber laws and rights in today's digital age; IT Act, Intellectual Property Issues connected with use and management of Digital Data, Emergence of Cyberspace, Cyber Jurisprudence.

UNIT II: Cyber Crimes against Individuals, Institution and State, Hacking, Digital Forgery, Cyber Stalking/Harassment, Cyber terrorism, Cyber Defamation, Different offenses under IT Act, 2000,Cyber Torts.

UNIT III: Ethics in business world, Ethics in IT, Ethics for IT professionals and IT users, IT professional malpractices, communications eavesdropping, computer break-ins, denial-of-service, destruction and modification of data, distortion and fabrication of information, Types of Exploits and Perpetrators.

UNIT IV: Intellectual Property: Copyrights, Patents, Trade Secret Laws, Key Intellectual property issues, Plagiarism, Competitive Intelligence, Cybersquatting, Information warfare policy and ethical Issues.

UNIT V: Privacy: The right of Privacy, Protection, Key Privacy and Anonymity issues, Identity Theft, Consumer Profiling, Defamation, Freedom of Expression, Anonymity, National, Security Letters, Defamation and Hate Speech.

UNIT VI: Ethics of IT Organization: Contingent Workers H- IB Workers, Whistle- blowing, Protection for Whistle- Blowers, Handling Whistle- blowing situation, Digital divide.

Course Outcomes:

On successful completion of course student will learn:

1. To identify and analyse statutory, regulatory, constitutional, and organizational laws that affect the software professional.
2. To understand various cyber laws with respect to legal dilemmas in the Information Technology field.
3. To interpret various intellectual property rights, Privacy, Protection issues in software development field.
4. To understand the role of ethics in IT organization.

Textbooks:

1. George Reynolds, “Ethics in information Technology”,5th edition, Cengage Learning

2. Hon C Graff, Cryptography and E-Commerce - A Wiley Tech Brief, Wiley Computer Publisher,2001

Reference Books:

1. Michael Cross, Norris L Johnson, Tony Piltzecker, Security, Shroff Publishers and Distributors Ltd.
2. Debora Johnson," Computer Ethics",3/e Pearson Education.
3. Sara Baase, "A Gift of Fire: Social, Legal and Ethical Issues, for Computing and the Internet," PHI Publications.
4. Chris Reed & John Angel, Computer Law, OUP, New York, (2007).

Syllabus for Semester - III, B.TECH. CSE (Cyber Security)

Course Code:	**HUT3001**	**Course Name:**	**Business Communication**		
L: 2 Hrs	**T: 0 Hrs**	**P: 0 Hrs**	**Per Week**	**Total Credits:**	**2**

Course Objectives

The course aims to develop the skills of students to proficiently craft compelling business documents and employ strategic verbal communication techniques. By honing these skills, students will gain the ability to convey ideas persuasively and interact confidently in diverse business contexts.

Syllabus

UNIT 1: Fundamentals of Business Communication (6 Hours)

Definition of communication, Emergence of communication as a key concept in the Corporate and Global world, Types- Internet, Blogs, E-mails, social media, Channels- Formal and Informal: Vertical, Horizontal, Diagonal, Grapevine, Persuasive Communication- Negotiation Skills, PAC concept

UNIT 2: Business Correspondence (6 Hours)

Planning, Writing, and Completing Business Messages

Personnel Correspondence: Job Application Letter, Letter of Acceptance of Job Offer, Letter of Resignation, Letter of Appointment, Promotion and Termination, Letter of Recommendation

Trade Correspondence: Inquiry, Order, Credit and Status Enquiry, Complaints, Claims, Adjustments, Consumer Grievance Letters

UNIT 3: Visual and Content Creation (6 Hours)

Visual design principles, Ethics of visual communication, selecting visuals for presenting data, Content Creation: Website, Help file, User Guides, Promotional leaflets and fliers

UNIT 4: Reports (4 Hours)

Basic formats and types of reports - Feasibility, Progress, Project, Case Study Evaluation, Agenda, Notices, Minutes of Meeting, Organizational announcements, Statement of Purpose.

UNIT 5: Communication for Employment (4 Hours)

Pre-interview technique- NOISE Analysis, Job Description and Resume, Creating LinkedIn Profile, Effective use of job portals, Business etiquette.

Text Books

1. Sharon Gerson, Steven Gerson, "Technical Communication: Process and Product", 2018, Pearson
2. Courtland L Bovee, John V Thill and Roshan Lal Raina "Business Communication Today", 14th edition Pearson
3. P.D. Chaturvedi and Mukesh Chaturvedi, Fundamentals of Business Communication, Pearson Publications, 2012

Reference Books:

1. Shalini Verma, Business Communication, Vikas Publishing House Pvt. Ltd., 2015.
2. Sanjay Kumar, Pushpa Lata, Communication Skills, 2nd Edition, Oxford Publication, 2018
3. William Strunk Jr. and E.B. White, The Elements of Style, Allyn & Bacon, A Pearson Education

Company, 2000

Course Outcomes:

On successful completion of the course the students will be able to achieve the following:

CO1: Understand the fundamentals of business communication.

CO2: Apply tools and techniques to create effective workplace correspondence.

CO3: Analyse and apply visual design principles to create business documents.

CO4: Understand and evaluate information to draft reports.

CO5: Apply and evaluate strategies for effective communication for employment.

Syllabus for Semester - IV, B.TECH. CSE (Cyber Security)

Course Code:	**CCT4001**	**Course Name:**	**Operating System**		
L: 3 Hrs	**T: 0 Hrs**	**P: 0 Hrs**	**Per Week**	**Total Credits:**	**3**

Course Objectives:

1. The course focuses on developing a fundamental knowledge of operating systems.
2. The course targets at the detail understanding of the basic tasks such as scheduling, memory management and File systems
3. It also covers the complex concepts of inter process communication and deadlocks

Syllabus

Unit I: Introduction: Concept of Operating Systems, Generations of Operating systems, Types of Operating Systems, OS Services, System Calls, Structure of an OS - Layered, Monolithic, Microkernel Operating Systems, Concept of Virtual Machine, Case study on LINUX and Windows Operating System.

Unit II: Processes: Definition, Process Relationship, Different states of a Process, Process State transitions, Process Control Block (PCB), Context switching.
Threads: Definition, Various states, Benefits of threads, Types of threads, Concept of multithreads.
Process Scheduling: Foundation and Scheduling objectives, Types of Schedulers, Scheduling criteria: CPU utilization, Throughput, Turnaround Time, Waiting Time, Response Time; Scheduling algorithms: Pre-emptive and Non-pre-emptive, FCFS, SRTF, Priority, RR, Case study on Process Management in LINUX Operating System.

Unit III: Inter-process Communication: Critical Section, Race Conditions, Mutual Exclusion,
Peterson's solution, Hardware Solution, Semaphores, Monitors, Message Passing, Classical IPC Problems: Producer-Consumer Problem, Reader-Writer Problem, Dinning Philosopher Problem etc.

Unit IV: Deadlocks: Definition, Necessary and sufficient conditions for Deadlock, Deadlock Prevention, Deadlock Avoidance: Banker's algorithm, Deadlock detection and Recovery.

Unit V: Memory Management: Basic concept, Logical and Physical address mapping, Memory allocation: Contiguous Memory allocation – Fixed and variable partition, Internal and External fragmentation and Compaction, Paging: Principle of operation – Page allocation, Hardware support for paging, Protection and sharing, Advantages & Disadvantages of paging.
Virtual Memory: Basics of Virtual Memory, Hardware and control structures, Locality of reference, Page fault, Working Set, Dirty page/ Dirty bit, Demand paging; Page Replacement algorithms: First in First Out (FIFO), Least Recently used (LRU), and Optimal.

Unit VI: File Management: Concept of File, Access methods, File types, File operations, Directory structure, File System structure, Allocation methods, Free-space management.
Disk Management: Disk structure, Disk scheduling - FCFS, SSTF, SCAN, C-SCAN, LOOK, C- LOOK, Disk reliability, Disk formatting, Boot block, Bad blocks, case study on File Systems in LINUX operating System.

Course Outcomes

On successful completion of the course, students will be able to:

1. Describe and classify differing structures for operating systems.

2. Understand the role of various components (process, page, file systems etc.) of operating system.
3. Analyze and apply resource (CPU, Memory, Disk) management policies.
4. Determine challenges in inter process communication and design solution for it.

Text Books

1. Operating System Concepts, 8th Edition by A. Silberschatz, P.Galvin, G. Gagne, Wiley India Edition.
2. Modern Operating Systems, 2nd Edition by Andrew Tanenbaum, PHI.

Reference Books

1. Operating Systems: Internals and Design Principles, 5th Edition, William Stallings, Prentice Hall of India.
2. Understanding the Linux Kernel, 3rd Edition, Daniel P. Bovet, Marco Cesati, O'Reilly

Syllabus for Semester - IV, B.TECH. CSE (Cyber Security)

Course Code: CCP4001 Course Name: Operating System Lab
L: 0 Hrs T: 0 Hrs P: 2 Hrs Per Week Total Credits: 1

Course Objectives:

Using C language in Linux environment:

1. To develop ability of students to design and implement concepts of operating systems such as system calls, CPU scheduling, process/thread management.
2. To develop the components and management aspects of concurrency management, memory management, and File management.

Syllabus:

Experiments based on CCT4001 Syllabus.

Course Outcomes:

On completion of the course the student will be able to :

1. Demonstrate LINUX commands and implement system commands.
2. Implement process and process schedulers.
3. Design and implement solution to handle synchronization and deadlock.
4. Implement memory management and File management solutions.

Syllabus for Semester - IV, B.TECH. CSE (Cyber Security)

Course Code: CCT4002 Course Name: Cryptography

L: 3 Hrs T: 0 Hrs P: 0 Hrs Per Week Total Credits: 3

Course Objectives:

1. To understand basics of Cryptography.
2. To be able to secure a message over insecure channel by various means.
3. To learn about how to maintain the Confidentiality, Integrity and Availability of data To understand various protocols to protect against the threats in the networks

Syllabus:

UNIT I: Introduction to Cryptography

Introduction to security attacks - services and mechanism, Mathematics of Cryptography- Integer Arithmetic, Modular Arithmetic, introduction to cryptography - Conventional Encryption: Conventional encryption model - classical encryption techniques - substitution ciphers and transposition ciphers – cryptanalysis – steganography

UNIT II: Stream & Block Ciphers

Mathematics of Symmetric-key Cryptography- Algebraic Structures- Groups, ring & Finite field, stream and block ciphers - Modern Block Ciphers: Block ciphers principals - Shannon's theory of confusion and diffusion - fiestal structure - data encryption standard (DES) - strength of DES - block cipher modes of operations - DES – AES.

Unit III: Confidentiality and Modular Arithmetic

Confidentiality using conventional encryption - traffic confidentiality - key distribution, Mathematics of Asymmetric-key cryptography- random number generation - Introduction to graph, prime and relative prime numbers - modular arithmetic - Fermat's and Euler's theorem - primality testing - Euclid's Algorithm - - discrete algorithms.

Unit IV: Public key cryptography and Authentication requirements

Principles of public key crypto systems - RSA algorithm - security of RSA - key management –Diffie - Hellman key exchange algorithm - introductory idea of Elliptic curve cryptography – Elgamal encryption – Message Authentication and Hash Function: Authentication requirements - authentication functions - message authentication code - hash functions - birthday attacks – security of hash functions and MACS.

Unit V: Integrity checks and Authentication algorithms

MD5 message digest algorithm - Secure hash algorithm (SHA) Digital Signatures: Digital Signatures - authentication protocols - digital signature standards (DSS) - proof of digital signature algorithm - Authentication Applications: Kerberos and X.509 - directory authentication service

Unit VI: Application Layer Security, IP Security and Key Management

Electronic mail security-pretty good privacy (PGP), S/MIME, IP Security: Architecture - Authentication header - Encapsulating security payloads - combining security associations- key management.

Course Outcomes:

1. Understand various cryptographic Techniques.
2. Apply various public key cryptography techniques.
3. Implement hashing and digital signature techniques.
4. Apply IP security techniques.

Text Books:

1. William Stallings, “Cryptography and Network security Principles and Practices”, Pearson/PHI ,5th Edition
2. Wade Trappe, Lawrence C Washington, “Introduction to Cryptography with coding theory”, Pearson.
3. Behrouz A. Forouzan, Debdeep Mukhopadhyay, “Cryptography and Network Security” 3rd Edition, McGrawHill.

Reference Books:

1. W. Mao, “Modern Cryptography – Theory and Practice”, Pearson Education.
2. Charles P. Pfleeger, Shari Lawrence Pfleeger – Security in computing – Prentice Hall of India.

Syllabus for Semester - IV, B.TECH. CSE (Cyber Security)

Course Code: CCP4002 Course Name: Cryptography Lab
L: 0 Hrs T: 0 Hrs P: 2 Hrs Per Week Total Credits: 1

Course Objectives:

Using programming languages in Linux environment.

1. To develop ability of students to understand and implement concepts of various cryptographic techniques.
2. To make students aware of various Integrity checks and Authentication algorithms.
3. To make students familiar with Application layer security.

Syllabus:

Experiments based on CCP4002 Syllabus.

Course Outcomes:

On completion of the course the student will be able to:

1. Understand and implement various public key cryptography techniques
2. Apply various types of integrity checks and authentication mechanisms.
3. Design and Implement Application layer security techniques.

Syllabus for Semester - IV, B.TECH. CSE (Cyber Security)

Course Code: CCT4003 Course Name: Theory of Computation

L: 3 Hrs T: 0 Hrs P: 0 Hrs Per Week Total Credits: 3

Course Objectives:

1. To provide students an understanding of basic concepts in the theory of computation.
2. To teach formal languages and various models of computation.
3. To exhibit fundamental concepts related with computability theory.

Syllabus:

UNIT I: Basics of Sets and Relation, Countability and Diagonalisation, Principle of mathematical induction, Pigeon-hole principle. Fundamentals of formal languages and grammars, Chomsky hierarchy of languages.

UNIT II: Finite automata: Deterministic finite automata (DFA), Nondeterministic finite automata (NFA) and equivalence with DFA, Minimization of finite automata, NFA with Epsilon Transitions, Finite Automata with output.

UNIT III: Regular expressions and Regular languages, Regular grammars and equivalence with finite automata, properties of regular languages, pumping lemma for regular languages, Context- free grammars (CFG) and language (CFL), parse trees, ambiguity in CFG, Reduction of CFGs, Chomsky and Greibach normal forms

UNIT IV: Push Down Automata: Deterministic pushdown automata and Non-Deterministic pushdown automata, Acceptance by two methods: Empty stack and Final State, Equivalence of PDA with CFG, closure properties of CFLs.

UNIT V: Turing machines: The basic model for Turing machines (TM), Turing recognizable (recursively enumerable) and Turing-decidable (recursive) languages, variants of Turing machines, unrestricted grammars and equivalence with Turing machines, TMs as enumerators.

UNIT VI: Undecidability: Church-Turing thesis, Universal Turing machine, Undecidable problems aboutv languages, Recursive Function Theory.

Course Outcomes:

On successful completion of the course, students will be able to demonstrate

1. Describe the formal relationships among machines, languages and grammars.
2. Design and optimize finite automata for given regular language.
3. Design Push Down Automata, Turing Machine for given languages.
4. Demonstrate use of computability, decidability, recursive function theory through problem solving.

Text Books:

1. John E. Hopcroft, Rajeev Motwani and Jeffrey D. Ullman, Introduction to Automata Theory, Languages, and Computation, Pearson Education Asia.

Reference Books:

1. Harry R. Lewis and Christos H. Papadimitriou, Elements of the Theory of Computation, Pearson

Education Asia.
2. Dexter C. Kozen, Automata and Computability, Undergraduate Texts in Computer Science, Springer.
3. Michael Sipser, Introduction to the Theory of Computation, PWS Publishing.
4. John Martin, Introduction to Languages and The Theory of Computation, Tata McGraw Hill.

Syllabus for Semester - IV, B.TECH. CSE (Cyber Security)

Course Code: MAT4002 Course Name: Probability and Queuing Theory

L: 3 Hrs T: 0 Hrs P: 0 Hrs Per Week Total Credits: 3

Course Objective:

1. Acquire skills in handling situations involving several random variables and functions of random variables.
2. Understand and characterize phenomena which evolve with respect to time in a probabilistic manner.
3. Be exposed to basic characteristic features of a queuing system and acquire skills in analyzing queuing models.

Syllabus:

Module 1: (9 Lectures) Joint probability function, Marginal and Conditional distribution, Mean , Variance, Covariance of two dimensional random variables.

Module 2: (9 Lectures)

Introduction to stochastic process, Poisson process, random walk, stationary process, transition probability matrix, transition diagram, Markov chain, birth and death process.

Module 3: (10 Lectures)

Modelling of queuing systems, queuing systems with losses, queuing systems allowing waiting time.

Module 4: (10 Lectures)

Markovian Models: Single server queues(M/M/1), Multi-server Queues(M/M/C), Finite Source model M/G/1 (steady state solution only), Pollaczek Khintchine formula, Queues with unlimited service(M/M/∞).

Textbooks:

1. Medhi J., "Stochastic Processes", New Age Publishers, New Delhi, 1994
2. T. Veerarajan, "Probability, Statistics and Random process", Tata McGraw Hill, Second Edition, New Delhi, 2003.
3. Kishore S. Trivedi, " Probability and statistics with reliability, Queuing and computer science application, PHI private Ltd, 2009.
4. B.S. Grewal, Higher Engineering Mathematics, Khanna Publishers, 35th Edition, 2000.

References:

1. Gross, D. and Harris, C.M., "Fundamentals of Queuing theory", John Wiley 2014.
2. Ross, S., "A first course in probability", Pearson Education, Sixth Edition, Delhi, 2002.
3. Allen., A.O., "Probability, Statistics and Queuing Theory", Academic press, New Delhi, 1981

Course Outcomes:

On successful completion of the course, student shall be able to

1. Understand Joint Probabilities and compute quantitative metrics of performance for queuing systems.
2. Analyze stochastic models, calculating probabilities, transition probabilities and steady state probabilities within stochastic system.

3. Model queuing system with losses and waiting time.
4. Apply and extend queuing models to analyze real world

Syllabus for Semester - IV, B.TECH. CSE (Cyber Security)

Course Code: IDT2990 Course Name: Open Elective II – Network Security Fundamentals

L: 2 Hrs, T: 0 Hrs, P: 0 Hrs Per Week Total Credits: 2

Course Objectives:

1. To get to know various threats on networks
2. To design security policies for network
3. To use various tools for network security

Syllabus:

Network Security Overview, Understanding Vulnerabilities, Understanding Defenses, Malware & Social Engineering Attacks,

Application & Network Attacks, Vulnerability Assessment, Host, Application & Data Security, Cryptography, Security Policies, Secure Design,

Web Security, Router Security, Firewalls, IDS/IPS, Remote Access, Endpoint Security, VPNs, PKI, Key Management, SSL/TLS,

Wireless Security, Logging & Auditing, Cloud and Virtualization Security, Access Control Fundamentals, RADIUS, TACACS, LDAP,

Authentication & Account Management, SSO, Risk Mitigation.

Textbooks:

1. Network Security Fundamentals by Gert De Laet & Gert Schauwers. Cisco Press.
2. CompTIA Security+: Guide to Network Security Fundamentals, Seventh Edition by Mark Ciampa. Cengage Publishing.

Course Outcomes:

After the successful completion of the course, students shall be able to –

1. Distinguish between different cyber threats and attacks on networks.
2. Enhance network security structurally through security policies and network design.
3. Implement security tools and rules for network perimeter protection.

Syllabus for Semester - IV, B.TECH. CSE (Cyber Security)

Course Code: CCP4005 Course Name: Software Lab - II

L: 0 Hrs T: 0 Hrs P: 2 Hrs Per Week Total Credits: 1

Course Objectives:

- To introduce students to open-source tools and IDEs used in network security.
- To provide students with hands-on experience in network scanning, vulnerability assessment, threat detection, and firewall configuration.
- To develop students' analytical and critical thinking skills for identifying and mitigating security threats.
- To prepare students to apply cybersecurity principles and practices in real-world scenarios.

Course Content:

Network Scanning and Enumeration (Wireshark, Nmap, Zenmap, Netcat etc.), Vulnerability Assessment (OpenVAS, Nikto, etc.), Lynis, Threat Detection using snort, Firewalls (pfSense: Exploring pfSense for configuring network security and firewalls) and UFW (Uncomplicated Firewall), Creating virtual environments for secure testing and practice. Web application security tools. Case Studies and Real-World Scenarios (Security incidents analysis and best practices)

Course Outcomes:

After successful completion of the course students will be able to:

- perform network scanning and enumeration using open-source tools.
- conduct vulnerability assessments, threat detection and audits using appropriate tools.
- Configure, manage firewalls for securing network environments and apply cybersecurity principles to real-world scenarios and case studies.

Reference Books:

1. **Network Security Assessment** by Chris McNab: Provides in-depth coverage of network scanning, enumeration, and vulnerability assessment tools and techniques.
2. **The Practice of Network Security Monitoring** by Richard Bejtlich - Offers insights into threat detection using tools like Snort and real-world network security monitoring practices.
3. **pfSense: The Definitive Guide** by Christopher M. Buechler and Jim Pingle - Comprehensive guide to pfSense for configuring network security and firewalls.
4. **Web Application Security: A Beginner's Guide** by Bryan Sullivan - Covers web application security tools and best practices.

Case Studies:

1. **Stuxnet Worm** - Analyze the Stuxnet worm as a case study for threat detection and incident response.
2. **Target Data Breach** - Study the Target data breach case as an example of a security incident analysis.
3. **WannaCry Ransomware Attack** - Explore the WannaCry ransomware attack as a case study for vulnerability assessment and mitigation.

Additional Resources:

1. **Wireshark User's Guide** - Official documentation for Wireshark to deepen understanding of network packet analysis.

2. **Nmap Network Scanning** by Gordon Fyodor Lyon - Comprehensive guide to Nmap for network scanning and enumeration.
3. **OpenVAS Documentation** - Official documentation for OpenVAS for vulnerability assessment.
4. **Snort Intrusion Detection** - Official documentation for Snort for intrusion detection.

Syllabus for Semester - IV, B.TECH. CSE (Cyber Security)

Course Code: CCP4006 Course Name: Community Engagement Project

L: 0 Hrs T: 0 Hrs P: 4 Hrs Per Week Total Credits: 2

Course Objectives:

The objective of Community Engagement Project is to instill a sense of social responsibility amongst the students, empowering them to apply their knowledge and skills to positively impact and contribute to the society.

Execution Plan for the Subject:

The students will impart their knowledge and skills in the society by identifying the potential needs or identify a society need and address it by building a technical solution.

Course Outcomes:

On successful completion of the course, students will be able to:

1. Propose a community engagement project tailored to address society needs by devising a strategy or solution to address it.
2. Apply technical knowledge or skills towards execution of the proposed solution.
3. Evaluate the effectiveness of the project in addressing community needs.
4. Demonstrate ethical principles, project management skills, teamwork and communication skills for project completion within the confines of a deadline.

Syllabus for Semester - IV, B.TECH. CSE (Cyber Security)

Course Code: MBT4001 Course Name: Business and Organizational Management

L: 2 Hrs T: 0 Hrs P: 0 Hrs Per Week Total Credits: 2

Objectives

1. To understand business and its role in society.
2. To enable the student to undertake business activities.
3. To familiarize the students with concepts and principles of management.
4. To impart knowledge on the functions of management among the students

Syllabus:

Unit 1: Introduction to Management: Concept of Management, nature and importance & Functions of Management, Overview of management principles and Theories: Taylor's Scientific Management, Henri Fayol's Principles of Management, Role of managers in modern business environments.

Unit 2 Planning and Decision Making: Importance of planning in organizational success, Types of plans: strategic, tactical, operational, Decision-making process and its components, Tools and techniques for effective decision making.

Unit 3: Organizing: Concept & Principles of Organizing; Formal/Informal Organizations, Virtual Organizations, Organization Structure: Factors affecting Organization structure, Span of Management, Delegation of Authority, Centralization and Decentralization.

Unit 4: Staffing & Controlling: Nature & Scope of Staffing, Man Power Planning - Concept and importance, Meaning and Definition of Controlling, Features and Importance of Controlling, Process of Controlling.

Unit 5: Management of Change in organization: Meaning and Definition of Management of Change, Need for change, Types of Change, Process of planned change, Resistance to change.

Unit 6: Business organization & its Form: Concept, Meaning, Features, Stages of development of Business, importance of business; Classification of Business activities; Business Organization: Meaning, characteristics, objectives, Business Organization, Forms of Business Ownership/ Formats, Micro, Small & Medium Enterprises

Books recommended:

1. Essential of Management by Knootz & O Donnel
2. Practice of Management by Peter Drucker
3. Management and Organization by Louise and Allen
4. Management by P. Subba Rao, Himalaya Publishing House
5. Principles & Practice of Management by L. M Prasad Sultan Chand & Sons
6. Principles of Business management by Dr. Pratibha M.Siriya Sai Jyoti Publication

Course Outcome:

Students will be able to

1. Understand the fundamentals of management and its significance in achieving organizational goals.
2. Apply planning and decision-making techniques to enhance organizational effectiveness.
3. Analyze organizational structures and processes for efficient staffing, controlling, and managing change.

Syllabus for Semester - IV, B.TECH. CSE (Cyber Security)

Course Code: HUT4002 Course Name: Environment Education

L: 2 Hrs T: 0 Hrs P: 0 Hrs Per Week Total Credits: 2

Syllabus:

UNIT 1: Humans and the Environment (UNIT 4)

Great ancient civilizations and the environment, Indic Knowledge and Culture of sustainability; Middle Ages and Renaissance; Industrial revolution and its impact on the environment; Population growth and natural resource exploitation; Global environmental change; emergence of environmentalism

UNIT 2: Natural Resources and Sustainable Development (4 Hours)

Definition of resource; Classification of natural resources

Water resources; Soil and mineral resources; Energy resources; Sustainable Development Goals (SDGs)

UNIT 3: Environmental Issues: Local, Regional and Global (6 Hours)

Environmental issues and scales, Pollution, Land use and Land cover change, Global change, case studies/field visit

UNIT 4: Conservation of Biodiversity and Ecosystems (6 Hours)

Biodiversity and its distribution – India and the world; Ecosystems and ecosystem services, Threats to biodiversity and ecosystems; Major conservation policies and practises, case studies/field visit

UNIT 5: Environmental Management (6 Hours)

Introduction to environmental laws and regulation, Concept of Circular Economy, Life cycle analysis; Cost-benefit analysis; Environmental audit and impact assessment; Concept of 3R (Reduce, Recycle and Reuse) and sustainability; Ecolabeling /Ecomark scheme, case studies/field visit.

Reference Books:

1. Fisher, Michael H. (2018) An Environmental History of India- From Earliest Times to the Twenty-First Century, Cambridge University Press.
2. Headrick, Daniel R. (2020) Humans versus Nature- A Global Environmental History, Oxford University Press.
3. Simmons, I. G. (2008). Global Environmental History: 10,000 BC to AD 2000. Edinburgh University Press
4. Singh, J.S., Singh, S.P. & Gupta, S.R. 2006. Ecology, Environment and Resource Conservation. Anamaya Publications https://sdgs.un.org/goals
5. Harris, Frances (2012) Global Environmental Issues, 2nd Edition. Wiley- Blackwell.
6. Rajagopalan, R. (2011). Environmental Studies: From Crisis to Cure. India: Oxford University Press.
7. Krishnamurthy, K.V. (2003) Textbook of Biodiversity, Science Publishers, Plymouth, UK
8. Singh, Kartar and Anil Shishodia (2007) 'Environmental Economics: Theory and Applications", Sage,
9. Karpagam. M (2019) Environmental Economics: A textbook, Sterling
10. Jørgensen, Sven Marques, Erik João Carlos and Nielsen, Søren Nors (2016) Integrated Environmental

Management, A transdisciplinary Approach. CRC Press.
11. Theodore, M. K. and Theodore, Louis (2021) Introduction to Environmental Management, 2ndEdition. CRC Press.
12. Barrow, C. J. (1999). Environmental management: Principles and practice. Routledge.
13. Tiefenbacher, J (ed.) (2022), Environmental Management - Pollution, Habitat, Ecology, and Sustainability, Intech Open, London. 10.5772/
14. Richard A. Marcantonio, Marc Lame (2022). Environmental Management: Concepts and Practical Skills. Cambridge University Press.
15. N. Mani (2020) Environmental Economics, New NC Century
16. Subhashini Muthukrishnan (2015) Economics of Environment, PHI
17. Rabindra N. Bhattacharya (2001) Environmental Economics: An Indian Perspective, Oxford University press

Course Outcomes:

On successful completion, of course student will able to do the following:

CO1: Understand and appreciate the historical context of human interactions with the environment.

CO2: Understand the concept of natural resources and their sustainable development

CO3: Develop a critical understanding of the environmental issues of concern

CO4: Understand the concepts of ecosystems, biodiversity and conservation

CO5: Understand broad aspects of environmental management and assessment systems

Syllabus for Semester - V, B.TECH. CSE (Cyber Security)

Course Code: CCT5001 Course Name: Design & Analysis of Algorithms

L: 3 Hrs T: 0 Hrs P: 0 Hrs Per Week Total Credits: 3

Course Objectives:

1. Students should learn techniques for effective problem solving in computing.
2. Students should analyze different paradigms of problem solving to solve a given problem in an efficient way.

Syllabus:

UNIT I: Mathematical foundations for arithmetic and geometric series, Recurrence relations and their solutions, Principles of designing algorithms and complexity calculation, Asymptotic notations for analysis of algorithms, worst case and average case analysis, amortized analysis and it's applications.

UNIT II: Divide and Conquer- basic strategy, Binary Search, Quick sort, Merge sort, Strassen's matrix multiplication, Maximum sub-array problem, Closest pair of points problem, Convex hull problem.

UNIT III: Greedy method – basic strategy, fractional knapsack problem, Minimum cost spanning trees, Huffman Coding, activity selection problem ,Find maximum sum possible equal to sum of three stacks, K Centers Problem.

UNIT IV: Dynamic Programming -basic strategy, Bellmen ford algorithm, all pairs shortest path, multistage graphs, optimal binary search trees, traveling salesman problem, String Editing, Longest Common Subsequence problem and its variations.

UNIT V: Basic Traversal and Search Techniques, breadth first search and depth first search, connected components. Backtracking basic strategy, 8-Queen's problem, graph coloring, Hamiltonian cycles, sum of subset problem, Introduction to Approximation algorithm.

UNIT VI: NP-hard and NP-complete problems, basic concepts, non-deterministic algorithms, NP-hard and NP complete, decision and optimization problems, polynomial reduction, graph based problems on NP Principle, vertex cover problem, clique cover problem

Course Outcomes:

On successful completion of the course, students will be able to:

1. Understand mathematical formulation, complexity analysis and methodologies to solve the recurrence relations for algorithms.
2. Design Greedy and Divide and Conquer algorithms and their usage in real life examples.
3. Design Dynamic programming and Backtracking Paradigms to solve the real life problems.
4. Understand NP class problems and formulate solutions using standard approaches.

Textbooks:

1. Thomas H. Cormen et.al; “Introduction to Algorithms”; 3 Edition; Prentice Hall, 2009.
2. Horowitz, Sahani and Rajasekaram; “Computer Algorithms”, Silicon Press, 2008.
3. Brassard and Bratley; “Fundamentals of Algorithms”, 1 Edition; Prentice Hall, 1995. 4. Richard

Johnsonbaugh, “Algorithms”, Pearson Publication, 2003.

Reference Books:

1. Parag Himanshu Dave, Balchandra Dave, “Design and Analysis of Algorithms” Pearson Education, O'relly publication
2. Richard Johnsonbaugh, “Algorithms”, Pearson Publication, 2003.

Syllabus for Semester V, B. TECH CSE (Cyber Security)

Course Code: CCT5002 Course: Computer Security

L: 3 Hrs, T: 1 Hr, P: 0 Hr, Per Week Total Credits: 4

Course Objectives

To introduce the structure of a network & role of cryptography in communication over an insecure channel

1. To explain & to compare how various attack scenarios work & how security principles work
2. To evaluate risks faced by computer systems
3. To summarize security mechanisms available in operating systems

Syllabus

Unit 1: Computer Security Foundations

History of Computer Crimes & Information System Security, Hardware Elements of Security, Data Communications, Network Topologies, Protocols & Design, Common Language for Computer Security Incident Information, Mathematical Models of Computer Security

Unit 2: Threats and Vulnerabilities

Understanding Studies & Surveys of Computer Crime, Psychology of Computer Criminals, Looming Threats – Insider Threat & Information Warfare, Computer System Penetration Malicious Code & Fooling Attacks, Mobile Code, Social Engineering & Low-Tech Attacks, Web-Based Vulnerabilities, Physical Threats to Computer Systems

Unit 3: Computer Security Technology and Principles

Cryptographic Tools, Identification & User Authentication, Access Control, Gateway Security Devices, Firewalls, Intrusion Detection & Intrusion Prevention Systems, Virtual Private Networks & Secure Remote Access, Securing Stored Data.

Unit 4: Operating System Security

System Security Requirements & Planning, Operating Systems Hardening, Linux/Unix Security, Windows Security, MAC Security, Virtualization Security, Software Security & Trusted Systems, File Sharing, Protection Mechanisms

Unit 5: Computer Defense -The Human Factor

Ethical Decision Making & High Technology, Employment Practices & Policies, Vulnerability Assessment, Operations Security & Production Controls, Email & Internet Use Policies, Implementing a Security Awareness Program, Security Standards for Products

Unit 6: IT Security Management

Security Audits, Application Controls, Monitoring & Control Systems, Data Backups & Archives, Incident Response, Business Continuity & Disaster Recovery, Quantitative Risk Assessment & Risk Management.

Course Outcome

After the successful completion of the course, students shall be able to –

1. Identify & distinguish between different cyber-attack vectors.
2. Harden computer systems & upgrade cybersecurity in different operating systems.
3. Analyze and manage IT security in organizations by implementing multiple security controls.

Textbooks:

1. Computer Security Handbook, Sixth Edition. Edited by Seymour Bosworth, M.E. Kabay & Eric Whyne. Wiley Publishing.

2. Computer Security: Principles & Practice, Fourth Edition by William Stallings & Lawrie Brown. Pearson Publish

Syllabus for Semester V, B. TECH CSE (Cyber Security)

Course Code: CCP5002 Course: Computer Security Lab

L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week Total Credits: 1

Course Objectives:

The objective of this Lab is:

1. To make the students experiment on the basic techniques of security and use of various tools for implementation. This will provide deeper insights into the aspects of security.

Practical based on Theory CCT5002

Course Outcomes

After the successful completion of the course, students shall be able to –

1. Determine and analyze software vulnerabilities and security solutions to reduce the risk of exploitation.
2. Analyze and resolve security issues in networks and computer systems to secure an IT infrastructure.
3. Design, develop, test and evaluate secure software.

Syllabus for Semester V, B. TECH CSE (Cyber Security)

Course Code: CCT5003 Course: Basics of Ethical Hacking

L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Pre-requisite

- Basic concepts in networking and programming

Course Objectives

1. Learn about the hacker mindset and the history of hackers
2. Understand basic networking and security technologies
3. Gain a basic understanding of security policy
4. Explore various vulnerability analysis techniques.

Syllabus:

Unit-1: Introduction and Ethics: Ethical Hacking, Types of Hackers, Phases of Ethical Hacking, Fundamentals of computer networking. TCP/IP protocol stack, IP addressing and routing, Common Network Threats/Attacks

Unit-2: Cryptography: Introduction to cryptography, private-key encryption, public-key encryption, Key exchange protocols, cryptographic hash functions, applications, Digital signatures, Attacks on cryptosystems

Unit-3: Vulnerability Analysis & System Hacking: Vulnerability Analysis, Types of Vulnerability Analysis, Vulnerability Assessment Tools, System Hacking, Password Cracking, Penetration testing, Hiding Files, Clearing logs

Unit-4: DoS and Session Hijacking: DoS attack, DDoS attack, Common symptoms of DoS/DDoS attack Categories of DoS/DDoS Attack Vectors, session hijacking, Application and Network level session hijacking

Unit-5: Sniffing: Malware and its propagation ways, Malware components, Types of malware, Concept of sniffing, Types of sniffing, Types of sniffing attacks

Unit-6: IDS & Firewall: Intrusion Detection System (IDS), Types of Intrusion Detection Systems, Introduction to Firewalls, Types of Firewalls, Introduction to Honeypots, Case studies: various attacks scenarios and their remedies.

Course Outcome:

At the end of the course, the students should be able to:

1. Develop the core foundations of ethics and cryptography in regards to computer security
2. Analyzing the vulnerability with respect to hacking, DDOS attack and session hijacking
3. Classify various types of malware and sniffing attacks on network
4. Analyzing various attacks scenario and remedies and detecting the attack with IDS.

Text Books:

1. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy, 2nd Edition, Patrick Engebreston, ISBN: 0124116442

Reference Books:

1. Penetration Testing: A Hands-On Introduction to Hacking, Georgia Weidman, ISBN: 1593275641
2. ETHICAL HACKING: A Comprehensive Beginner's Guide to Learn and Master Ethical Hacking, Hein Smith, Hilary Morrison

Syllabus for Semester V, B. TECH CSE (Cyber Security)

Course Code: CCP5003 Course: Basics of Ethical Hacking Lab

L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week Total Credits: 1

Course Objectives:

The objective of this Lab is:

1. To make the students experiment on the basic techniques of ethical hacking and use of various tools for implementation.

Practical based on Theory CCT5003

Course Outcome:

At the end of the course, the students should be able to:

1. Identify the vulnerability with respect to hacking, DDOS attack and session hijacking
2. Handle various types of malware and sniffing attacks on network
3. Implement various attacks scenarios and remedies and detecting the attack with IDS.

Syllabus for Semester V, B. TECH CSE (Cyber Security)

Course Code: CCT5005 Course: Artificial Intelligence and Machine Learning

L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Outcomes:

1. Understand the fundamental concepts of Artificial Intelligence (AI) and Machine Learning (ML).
2. Learn problem-solving, search strategies, and reasoning techniques in AI.
3. Understand various machine learning models, algorithms, and their applications.
4. Develop AI and ML models using programming frameworks.
5. Explore real-world applications of AI & ML in various domains.

Unit 1: Introduction to AI & ML (6 Hours)

Introduction to AI: History and Evolution of AI, Strong AI vs. Weak AI, AI Applications in various domains like Healthcare, Finance, and Robotics. Problem-Solving and Search Strategies: AI as a Problem-Solving Tool, State Space Representation, Problem Formulation in AI. Search Strategies in AI: Uninformed Search: Breadth-First Search (BFS), Depth-First Search (DFS), Informed Search (Heuristic Search): A* Algorithm, Greedy Best-First Search

Unit 2: Knowledge Representation and Reasoning (8 Hours)

Knowledge Representation Techniques: Representation of Facts, Knowledge, and Logic, Semantic Networks, Frames, and Scripts. Logic-Based Representation: Propositional Logic: Syntax and Semantics, First-Order Logic (FOL): Syntax, Semantics, and Inference. Reasoning in AI: Forward Chaining & Backward Chaining, Resolution in Logic

Handling Uncertainty in AI: Probability-Based Reasoning: Bayesian Networks

Fuzzy Logic: Fuzzy Sets, Membership Functions, and Applications

Expert Systems: Definition and Structure of Expert Systems, Case Study of an AI-Based Expert System

Unit 3: Fundamentals of Machine Learning (9 Hours)

Introduction to Machine Learning: Definition and Need, Types of ML: Supervised, Unsupervised, and Reinforcement Learning. Regression Techniques: Linear Regression, Polynomial Regression, Logistic Regression

Classification Techniques: Decision Trees, Naïve Bayes Classifier, k-Nearest Neighbors, Support Vector Machines (SVM). Model Evaluation Metrics: Overfitting & Underfitting, Bias-Variance Trade-off. Performance Metrics: Accuracy, Precision, Recall, F1-Score, ROC Curve. Unsupervised Learning: Clustering Techniques: k-Means Clustering, Hierarchical Clustering, DBSCAN.

Unit 4: Neural Networks & Deep Learning (9 Hours)

Introduction to Neural Networks: Biological Neurons vs. Artificial Neurons, Perceptron Model. Multi-Layer Perceptron (MLP) and Backpropagation: Structure of a Multi-Layer Neural Network, Backpropagation Algorithm Deep Learning Overview: Introduction to Deep Learning Architectures, Convolutional Neural Networks (CNNs): CNN Architecture, Convolution and Pooling Layers Applications in Image Processing. Recurrent Neural Networks (RNNs): Basics of RNNs, Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRU), Applications in Time-Series Forecasting.

Unit 5: Reinforcement Learning & Natural Language Processing (8 Hours)

Reinforcement Learning (RL): Basics of Reinforcement Learning, Markov Decision Process (MDP), Q-Learning and Deep Q-Networks, Applications of RL in Gaming and Robotics. Introduction to Natural Language Processing (NLP): NLP Overview and Applications. NLP Techniques and Applications: Sentiment Analysis using ML and Deep Learning. Text Generation using NLP Models (GPT, Transformers), Chatbots and Virtual Assistants.

Textbook:

1. Stuart Russell & Peter Norvig – Artificial Intelligence: A Modern Approach
2. Tom Mitchell – Machine Learning
3. Ian Goodfellow, Yoshua Bengio, Aaron Courville – Deep Learning

Reference Books:

1. Christopher Bishop – Pattern Recognition and Machine Learning
2. François Chollet – Deep Learning with Python
3. Sutton & Barto – Reinforcement Learning: An Introduction

Syllabus for Semester V, B. TECH CSE (Cyber Security)

Course Code: CCP5005 Course: Artificial Intelligence and Machine Learning Lab

L: 0Hrs, T: 0 Hr, P: 2 Hr, Per Week Total Credits: 01

Course Outcomes:

Upon successful completion of this practical lab, students will be able to:

1. Apply AI Search Algorithms for Problem Solving
2. Develop AI-Based Decision-Making Systems
3. Implement Machine Learning Models for Prediction
4. Perform Data Clustering and Classification
5. Apply Natural Language Processing (NLP) Techniques

List of Practical

1. Implement BFS and DFS algorithms.
2. Implement the A Algorithm* to find the optimal path in a grid-based environment.
3. Create a simple Expert System using IF-THEN rules for medical diagnosis.
4. Use basic NLP techniques to create a rule-based chatbot.
5. Implement Linear Regression for House Price Prediction
7. Implement Logistic Regression for Disease Prediction.
8. Implement k-Means Clustering for Customer Segmentation
9. Implement the Decision Tree Classifier for Iris Dataset
10. Implement Sentiment Analysis using Naïve Bayes

Syllabus for Semester VI, B. TECH CSE (Cyber Security)

Course Code: CCT5004 – 1 Course: Operating Systems for Cyber Security

L: 3Hrs T: 0Hr P: 0Hr Per Week Total Credits: 3

Course Objectives

1. Demonstrate basic OS operations and command-line tools across Windows, Linux, and macOS for cybersecurity tasks.
2. Configure and use security-focused OSs and tools for penetration testing and network monitoring.
3. Simulate OS feature abuses and build secure, multi-OS lab environments for cybersecurity testing.

Syllabus

Unit 1: OSs as tools in cybersecurity, differences in OS use vs OS architecture, importance of multi-OS fluency, CLI as the universal interface, essential shell operations, shell scripting basics, identifyingOS type and version, smart command-line operations in Linux macOS and Windows, basic toolchainsin OSs for cybersecurity, privilege context understanding

Unit 2: Security-relevant Windows operations, PowerShell for security tasks, event log navigation,scheduled tasks and persistence in Windows, Linux service management and logging, systemd and SysVinit differences, sudoers and privilege management, macOS security model overview, keychain and launch agent abuse, file permissions and ACLs across OSs, using process and service viewers effectively

Unit 3: Kali Linux overview and customization, tool classification in penetration testing OSs, ParrotOS and privacy integration, BlackArch modular toolset, REMnux for malware analysis, FLARE VM for reverse engineering, forensic live OS boot concepts, persistent vs non-persistent setups, kernel tracing basics, handling encrypted persistence in offensive OSs, secure OS configuration for offensive use

Unit 4: Security Onion setup and use, network sensor configuration, Wazuh agent management, T-Pot and deception OS use cases, Sysmon configuration and deployment, parsing Syslog and EVTX, unified2 format and alerts, osquery and endpoint visibility, system call monitoring, log forwarding tools, using custom Linux sensors, honeypot OS usage, building passive and active detection platforms

Unit 5: OS features abused by attackers, scheduled task abuse, cron and systemd misuse, registry key and launch agent persistence, using signed binaries for exploitation, environment misconfigurations, Windows LOLBAS and Linux native tool misuse, simulating persistence creation across OSs, application hijacking via OS features, scripting privilege escalation pathways, security evasion tactics. Building multi-OS lab environments, differences in VM and live boot security

Reference Materials and Sources

- Core Reference Sources (General Use Across Units)
    - The Linux Command Line by William Shotts – Excellent for terminal literacy and
    - Linux navigation (Units 1, 2, 3, 5)
    - Windows Internals, Part 1 by Mark Russinovich – Use selected content on Windows
    - services, registry, processes (Unit 2, 5)
    - macOS Internals by Jonathan Levin – For understanding macOS launch agents,

    - sandboxing, and process control (Unit 2, 5)
    - The Art of Memory Forensics by Ligh, Case, et al. – Great for OS forensic behavior
    - and monitoring techniques (Units 4, 5)
    - Kali Linux Revealed by Offensive Security – Primary for Unit 3 (also useful in Units
    - 5, 6)
    - Parrot OS and BlackArch Wikis / Docs – Use official documentation for practical use
    - and configuration (Unit 3)
    - Security Onion Documentation – Essential for Unit 4 (log monitoring, network sensor
    - setup)
    - Sysinternals Suite Documentation by Microsoft – Deeply useful for Windows analysis,
    - log inspection, and LOLBAS (Units 2, 4, 5)
- Unit 1 References
    - The Linux Command Line – Shotts
    - The Mac Terminal Reference – MacOSPro
    - Microsoft Docs – PowerShell fundamentals & scripting
    - OverTheWire.org wargames – hands-on terminal fluency
- Unit 2 References
    - Windows Internals – selected chapters
    - Microsoft Learn: PowerShell for Security
    - Linux Basics for Hackers – No Starch Press
    - macOS Security & Privacy Guide – Micah Lee
- Unit 3 References
    - Kali Linux Revealed – Offensive Security
    - Parrot OS Docs – official site
    - BlackArch Linux Guide – official documentation
    - REMnux Documentation – docs.remnux.org
    - FLARE VM GitHub – github.com/mandiant/flare-vm
- Unit 4 References
    - Security Onion Documentation – docs.securityonion.net
    - Wazuh Documentation – documentation.wazuh.com
    - Sysmon + NXLog guides – Microsoft & open-source blogs
    - The Art of Memory Forensics – Linux/Windows logging chapters
    - osquery.io – deployment & query reference
- Unit 5 References
    - LOLBAS Project – lolbas-project.github.io
    - GTFOBins – gtfobins.github.io
    - Red Team Field Manual (RTFM) – quick reference
    - PayloadsAllTheThings GitHub – github.com/swisskyrepo/PayloadsAllTheThings

Syllabus for Semester VI, B. TECH CSE (Cyber Security)

Course Code: CCT5004 – 2 Course: Threat and Malware Analysis

L: 3 Hrs T: 0 Hr P: 0 Hr Per Week Total Credits: 3

Course Objectives

1. To identify malware types based on static & behavioral analysis
2. To determine malware types & capabilities
3. To evaluate potential threat from malware activity

Syllabus

Unit 1: Introduction to Cyber Threat Intelligence (CTI)

Essential Terminology, Types of Threats, APTs & IoCs, Where to Begin? The Intelligence Cycle, The Diamond Model, Cyber Kill Chain, Cyber Threat Lifecycles & Frameworks

Unit 2: Structured Intelligence & Business Planning

MITRE ATT&CK Framework, STIX Language, Intelligence Reporting, Intelligence Report Structure, Collection Sources, Threat Intelligence Budgeting, Intelligence Analysts

Unit 3: CTI Implementation

Organizational Footprint, Primary Considerations for CTI Implementation, Developing the Core CTI Team, Introduction to OSINT, OSINT Platforms, OSINT Research Technologies, CTI Prioritization

Unit 4: Introduction to Malware Analysis:

History, Types of Malwares, Types of Malware Analysis, Malware Analysis Lab Setup, Static Malware Analysis, Dynamic Malware Analysis. Malware Disassembly: Computer Basics, Assembly Language & Its Operations, Windows x64 Architecture, Disassembly using IDA, Debugging Malicious Binaries

Unit 5: Advanced Malware Analysis

Malware Functionalities & Persistence, Code Injection & Hooking, Malware ObfuscationTechniques, Hunting Malware Using Memory Forensics, Detecting Advanced Malware Using Memory Forensics

Course Outcomes:

After the successful completion of the course, students shall be able to

1. Use intelligence models for identifying and classifying threats.
2. Apply standard techniques for CTI implementation.
3. Conduct deep malware analysis using static and dynamic analysis processes.

Textbooks:

1. Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Managers, First Edition by Aaron Roberts. Apress Publishing.
2. The Threat Intelligence Handbook: A Practical Guide for Security Teams to Unlocking the Power of Intelligence. Edited by Chris Pace. CyberEdge Press.
3. Learning Malware Analysis by Monappa K A, Packt Publishing
4. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski &

Andrew Honig. No Starch Press.
5. Certified Threat Intelligence Analyst (CTIA) by EC-Council. EC-Council Academia

Syllabus for Semester V, B. TECH CSE (Cyber Security)

Course Code: CCT5004 – 3 Course: Security Policies and Implementation

L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Objectives:

1. To analyze the need for security policies, procedures and security awareness
2. To understand the types & approaches of policy designing
3. To identify security policies considerations & implement them
4. To critique existing security policy for its effectiveness and completeness.

Syllabus

Unit 1: The Need for IT Security Policy Frameworks

Introduction to Security Policies, Information Systems Security, Information Assurance Information systems Security Policies, Business Drivers for Information Security Policies

Unit 2: Role of Governance and Business

Compliance Laws – India, Compliance Laws – International, Seven Domains of IT Infrastructure, Business Challenges & Policies to Mitigate the Risks, Information Security Policy Implementation Issues

Unit 3: Policy Framework & Designing

Program Framework Policy, Business Considerations for Framework, Information Assurance Considerations, IT Security Standards & Frameworks, How to Design, Organize, Implement & Maintain IT Security Policies, IT Security Policy Framework Approaches

Unit 4: Types of Policies

User Domain Policies, IT Infrastructure Security Policies, Data Classification and Handling Policies, Risk Management Policies, Incident Response Team (IRT) Policies, Special Access Policies, Physical Security Policy, DLP Policies,

Unit 5: Implementing and Maintaining IT Security Policy Framework

IT Security Policy Implementation, Employee Awareness & Training, Using Social Psychology to Implement Security Policies, IT Security Policy Enforcement, IT Policy Compliance and Compliance Technologies

Additional Learning Module

Project - Policy Research & Implementation

Project 1 – Research on Existing and/or Lack of Cybersecurity Polices in Local IT Companies, Analyse the Results and Generate a Comprehensive & Customised List of Cybersecurity Policies for the Companies

Project 2 –Understand Given Scenario of a New Company, according to the Company Description, Suggest Necessary Policies, Design the Policies, Having Professional Format, Conduct a Mock Policy Training Session

Textbook:

1. Security Policies and implementation Issues, Third Edition by Robert Johnson & Chick Easttom. Jones & Bartlett Learning.
2. Computer Security Handbook, Sixth Edition. Edited by Seymour Bosworth, M.E. Kabay & Eric Whyne. Wiley

Publishing.

Course Outcomes:

After the successful completion of the course, students shall be able to –

1. Recognize the suitable cybersecurity policies based upon an organization's IT infrastructure.
2. Design clear, concise and compliant cybersecurity policies.
3. Effectively enforce cybersecurity policies and oversee their updation in organizations

Syllabus for Semester VI, B. TECH (Computer Science & Engineering)

Course Code: CCT6001 Course: Introduction to Cloud Security

L: 3 Hrs T: 0 Hr P: 0 Hr Per Week Total Credits:03

Pre-requisites

Operating Systems, Computer Security

Course Objectives

The objective of this course is to impart necessary and practical knowledge of components of Cloud computing and develop skills required to design real-life cloud-based projects by:

1. Learning basics of cloud and challenges in its implementation.
2. Understanding the cloud environment and its security issues.
3. Understanding the various ways to secure cloud programming environments.

Syllabus

UNIT I: Introduction. Evolution of Cloud Computing, Cloud Fundamentals: Cloud Definition, Evolution, Architecture, Cloud Characteristics – Elasticity in Cloud – On-demand Provisioning, Applications, deployment models - Public, Private and Hybrid Clouds, and service models - Infrastructure as a Service (IaaS) - Resource Virtualization: Server, Storage, Network. Platform as a Service (PaaS) - Cloud platform & Management: Computation, Storage. Software as a Service (SaaS) - Anything as a service (XaaS), Security as a service. Vulnerability Issues and Security Threats, Security Challenges.

UNIT II: Virtualization. Definition, Understanding and Benefits of Virtualization. Implementation Level of Virtualization, Virtualization Structure/Tools and Mechanisms, Issues with virtualization, virtualization technologies and architectures, introduction to Various Hypervisors, virtualization of data centers, and Virtual Machine level Security, Virtualization security Issues.

UNIT III: Resource Management and Load Balancing. Distributed Management of Virtual Infrastructures, Resource management, Load Balancing. Interoperability, Migration and Fault Tolerance: Issues with interoperability, Cloud Migration, Migration of virtual Machines and techniques. Fault Tolerance Mechanisms. Risk Assessment on Cloud Migration.

UNIT IV: Cloud Data Security and Storage. Cloud storage: Introduction to Storage Systems, Cloud Storage Concepts, Data in the cloud- Cloud file systems. Data level Security, Data Protection (rest, at transit, in use), Data Information lifecycle, Cloud Data Audit, Multi-tenancy Issues.

UNIT V: Identity and Access Management. Introduction to Identity and Access Management, IAM Challenges, IAM Architecture, IAM Standards and Protocols for Cloud Services, Cloud Authorization Management.

UNIT VI: Cloud Infrastructure Security. The Network Level, Host Level, Application Level. Cloud Configuration & Patch Management, Cloud Change management. SLA Requirements, Cloud Compliance, Policy, Governance. Cloud Intrusion Detection, Cloud Forensics Challenges, Cloud Incident Response.

Course Outcomes

On successful completion of the course, the student will be able to:

1. Articulate the concepts of cloud computing, its various deployment and service models and vulnerabilities.
2. Develop solutions based on the concept of virtualization, resource management and migration.
3. Design measures for cloud data security and identity management.
4. Provide recommendations for Cloud Infrastructure Security based on cloud compliance and policies.

Text Books:

1. Kai Hwang, Geoffrey C. Fox and Jack J. Dongarra, "Distributed and cloud computing from Parallel Processing to the Internet of Things", Morgan Kaufmann, Elsevier – 2012
2. Tim Mather, SubraKumaraswamy, and Shahed Latif, "Cloud Security and Privacy An Enterprise Perspective on Risks and Compliance", O'Reilly 2009

Reference Books:

1. Barrie Sosinsky, " Cloud Computing Bible" John Wiley & Sons, 2010
2. "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Ronald L. Krutz,Russell Dean Vines, Wiley Publishers.
3. "Cloud Computing Principles and Paradigms", Rajkumar Buyya,James Broberg, Andrzej Gościński, Wiley Publishers,2011.

Syllabus for Semester VI, B. TECH CSE (Cyber Security)

Course Code: CCP6001 **Course: Introduction to Cloud Security Lab**

L: 0 Hrs T: 0 Hr P: 2 Hr Per Week **Total Credits: 1**

Course Objectives

The objective of this course is to impart necessary and practical knowledge of components of Cloud computing and develop skills required to build real-life cloud- based projects by:

1. Studying various cloud environments and challenges in its implementation.
2. Implementing various cloud programming concepts to secure the cloud.
3. Designing and developing processes involved in creation of a secure cloud-based application.

Syllabus

Practical based on CCT6001 syllabus.

Course Outcomes

On completion of this course, the students will be able to:

1. Configure various virtualization tools.
2. Design and deploy measures for cloud data security and identity management.
3. Install and use a generic cloud environment for Cloud Infrastructure Security.

Syllabus for Semester VI, B. TECH CSE (Cyber Security)

Course Code: CCT6002 Course: Database Management System

L: 3 Hrs, T: 0 Hr, P: 0 Hr Per Week Total Credits: 3

Course Objectives

The objective of this course is:

1. To understand the role of a database management system in an organization.
2. To construct simple and advanced database queries using a data language.
3. To understand and apply logical database design principles and database normalization.
4. To recognize the need for transaction management and query processing.

Syllabus

Unit 1: Database - Fundamentals and Architecture

Databases and Database Users, Characteristics of the Database Approach, Advantages of Using the DBMS Approach, When Not to Use a DBMS, Data Models, Schemas, and Instances, Three-Schema Architecture and Data Independence, Database Languages and Interfaces, The Database System Environment. Introduction to NoSQL databases and In-Memory databases.

Unit 2: Relational Model and SQL

Relational Model Concepts, Relational Model Constraints and Relational Database Schemas, Update Operations, Transactions, and Dealing with Constraint Violations, SQL Data Definition, Data Types and Constraints, Data Management in SQL, Transforming ER Model into Relational Model.

Unit 3: Database Design and Normalization

Functional Dependencies, Inference Rules, Equivalence, and Minimal Cover, Properties of Relational Decomposition, Normal Forms Based on Primary Keys, General Definitions of Second and Third Normal Forms, Boyce-Codd Normal Form, Other Dependencies and Normal Forms.

Unit 4: Indexing and Hashing

Ordered Indices, B+-Tree Index Files and its Extensions, Static Hashing and Dynamic Hashing, Comparison of Ordered Indexing and Hashing, Bitmap Indices, Some General Issues Concerning Indexing.

Unit 5: Query Processing and Optimization

Measures of Query Cost, Query Operation: Selection, Sorting and Join Operation, Transformation of Relational Expressions, Estimating Statistics of Expression Results, Choice of Evaluation Plans.

Unit 6: Transaction Processing, Concurrency Control and Recovery

Introduction to Transaction Processing, Characterizing Schedules Based on Recoverability, Characterizing Schedules Based on Serializability, Two-Phase Locking Techniques for Concurrency Control, Deadlock Handling and Multiple Granularity, Database Recovery Techniques.

Course Outcomes:

After successful completion of this course, the student will be able to:

1. Model data requirements for an application using conceptual modeling tools.
2. Design database schemas by applying normalization techniques.
3. Execute efficient data storage and retrieval queries using SQL.
4. Use concurrency control and database recovery in transaction management.

Text Books:

1. Abraham Silberschatz, Henry F. Korth and S. Sudarshan; “Database System Concepts”; Sixth Edition, Tata McGraw Hill, 2011.
2. Ramez Elmasri and Shamkant Navathe; “Fundamentals of Database Systems”; Sixth Edition, Addison Wesley 2011.

Reference Books:

1. Raghu Ramakrishnan and Johannes Gehrke; “Database Management Systems”; Third Edition; Tata McGraw Hill Publication, 2003.
2. Rini Chakrabarti and Shilbhadra Dasgupta; “Advanced Database Management System”; Dreamtech Press India Pvt. Ltd (Wiley India); 2014.

Syllabus for Semester VI, B. TECH CSE (Cyber Security)

Course Code: CCP6002 Course: Database Management System Lab

L: 0 Hrs T: 0 Hr P: 2 Hr Per Week Total Credits: 1

Course Objectives

The objective of this Lab is:

1. To enable students to use DDL, DML and DCL.
2. To prepare students to conceptualize and realize database objects (tables, indexes, views and sequences) and execute SQL queries.
3. To encourage students to design and execute PL/SQL blocks and triggers.

Practical based on CCT6002 syllabus

Experiments covering CCT6002 syllabus in Oracle 11g or12c | MySQL.

[Added experiments to be conducted to demonstrate handling of databases on cloud and demonstrating use of NoSQL]

Course Outcomes:

After successful completion of this course, the student should be able to:

1. Demonstrate database user administration and authorizations.
2. Execute simple, nested, multiple table, and advanced queries for data retrieval.
3. Construct PL-SQL block structure and Trigger for specific application.
4. Implement various integrity constraints, views, sequences, indices and synonym on database.

Reference Books

1. James Groff, Paul Weinberg and Andy Oppel, SQL - The Complete Reference, 3rd Edition, McGraw Hill, 2017.

Syllabus for Semester VI, B.TECH. CSE (Cyber Security)

Course Code: CCT6003 Course: Software Engineering and Project Management

L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 3

Course Objectives

The objective of this course is:

1. To familiarize the prospective engineering graduates with the strong fundamental knowledge of software engineering and practices.
2. To facilitate development of interpersonal skills and practicing group dynamics with work ethics.
3. To enable the graduates to apply the theory in practice and to channelize solutions to challenging real-world problems.

Syllabus

Unit 1: Introduction to Software Engineering, Software engineering principles, Software Myths, Software Engineering - a Layered Technology, Software Process Framework, Requirements Engineering Tasks, Requirement Engineering Process, Eliciting Requirement: Software Requirements Specification. Software Process Models: Waterfall Model, Incremental Process Models, Evolutionary Process Models, Specialized Process Models.

Unit 2: Agile Process Models, Requirements Analysis, Analysis Modeling Approaches, Data Modeling, Object-Oriented Analysis, Scenario-Based Modeling, Flow-Oriented Modeling, Class-based Modeling, Behavioral Model. Design Engineering Concepts, Design Model.

Unit 3: Software Project Management, The Business Case, Project Success and Failure, Project Evaluation, Cost-benefit evaluation technique, Project Planning-stepwise project Planning, Software Effort Estimation- Albrecht Function Point Analysis, COCOMO Model, COSMIC Function Point, Project Scheduling.

Unit 4: Testing Life Cycle, Testing Strategies - Structural Testing, Functional Technique, Static testing, Dynamic testing, Unit Testing, Integration Testing, Validation Testing, System Testing, Debugging. Software Approaches - Black-Box Testing, White-Box Testing, Web Testing, Test case design, building and execution. Automated Testing.

Unit 5: Software Quality, A Framework for Product Metrics, Metrics for Analysis and Design Models, Metrics for Source Code, Metrics for Testing and Maintenance. Metrics for process and project - Software measurement, metrics for software quality, metrics for small organization, Managing people in software environment.

Unit 6: Risk management - Risk strategies, Software risk identification, Risk refinement, RMMM, Risk Response development and Risk Response Control, Risk Analysis, Agile risk management using Jira, Software Configuration Management, SCM Repository, SCM Process, Estimation, Software reengineering, Reverse engineering.

Course Outcomes:

After successful completion of this course, the student will be able to:

1. Use software engineering practices and various models.
2. Apply software engineering processes for modeling and solving real-world problems.
3. Analyze the impact of different software testing strategies on software products.
4. Estimate project cost and quality of a software prototype.

Text books and Reference Books:

1. Roger Pressman, Software Engineering - A Practitioner's Approach, Sixth Edition, McGraw Hill, 2010.
2. Ian Somerville, Software Engineering, Seventh Edition, Pearson Education, 2008.
3. Rajib Mall, Software Project Management, Fifth Edition, McGraw Hill, 2008.
4. Pankaj Jalote, Software Engineering: A Precise Approach, Wiley Publication, 2010.

Syllabus for Semester VI, B. TECH CSE (Cyber Security)

Course Code: CCP6003 Course: Software Engineering and Project Management Lab

L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week Total Credits: 1

Course Objectives

The objective of this Lab is:

1. To familiarize students with UML modeling tool and processes.
2. To help students understand and model software solutions applying the best software engineering practices.
3. To introduce students to the state-of-the-art tools in testing and validation of standalone and web applications.

Practicals based on CCT6003 syllabus

Using UML 2.X Tools and Open-Source Testing Tools (JUnit, Selenium, Katalon, etc)

Course Outcomes:

After successful completion of this course, the student should be able to:

1. Create documentation of an effective approach by analyzing the software engineering problem.
2. Design different structural models for the underlying problem.
3. Construct behavioral models for the underlying problem.
4. Validate the software product using appropriate testing strategies.

Syllabus for Semester VI, B. TECH CSE (Cyber Security)

Course Code: CCT6004 – 1 Course: Wireless & Mobile Device Security

L: 3 Hrs, T: 0 Hr, P: 0 Hr Per Week Total Credits: 3

Course Objectives:

1. To comprehend the fundamental concepts of mobile and wireless network security
2. To identify security threats in wireless networks and design strategies to manage network security
3. To assess design required for a secured network application considering all possible threats

Syllabus

Unit 1: Wireless Network Foundations

Introduction to Wireless & Mobile Networks, Historical Evolution – Networks, Networking Models - ISO, TCP/IP, IP Addressing, Subnetting, Supernetting, IPv4 vs IPv6, Wired vs Wireless, Security Threats Overview: Wired, Wireless & Mobile, International Compliance Standards

Unit 2: Wireless LAN

WLAN & Operations, Wireless Technologies - IrDA, Bluetooth, Wibree, Wi-Fi, WiMAX, RFID etc., Wireless Protocols, Wireless Communication Languages, Wireless Devices.

Unit 3: Security in Wireless Networks

Attacks on Wireless Networks, Attacking Wireless Networks, Securing Wireless Networks, Handling Wireless Guest Access & Rogue Access Points, Bluetooth Security, WiMAX Security

Unit 4: Security in Wireless Sensor Networks

Overview of Wireless Sensor Networks & Their Security, Vulnerabilities & Attacks in Wireless Sensor Networks, Symmetric & Public-Key Primitives, Key Management, WSN Link-Layer Security Frameworks, Secure Routing & Data Aggregation, Privacy Protection & Intrusion Detection

Unit 5:

Part 1: IoT Security

Introduction to IoT, IoT Architecture, Flawed IoT Devices, Security Requirements for IoT, IoT Threats & Attacks - Physical & Logical, IoT Security Framework, Secure IoT Design

Part 2: Mobile Network & Device Security

Introduction to Mobile Networks, Mobile Communication Security Challenges - Android, iOS, Windows, Mobile Device Security Models - Android, iOS, Windows, BYOD Security, Mobile Wireless Attacks & Remediation, Mobile Device Fingerprinting, Mobile Malware & Application-Based Threats.

Course Outcomes:

After the successful completion of the course, students shall be able to –

1. Determine the different existent wireless & mobile technologies and differentiate between their real-world implementations.
2. Establish the modern-day threats prevailing upon major wireless technologies like Wi-Fi, Bluetooth, WSNs, IoT etc.
3. Administer practical security solutions to wireless technologies.

Textbooks:

1. Wireless and Mobile Device Security, Second Edition by Jim Doherty. Jones & Bartlett Learning.

2. Wireless Network Security, First Edition. Edited by Yang Xiao, Xuemin Shen & Ding-Zhu Du. Springer Publishing.
3. Wireless Network Security: A Beginner's Guide by Tyler Wrightson. McGraw-Hill Publishing.
4. Wireless and Mobile Network Security: Security Basics, Security in On-the-shelf and Emerging Technologies. Edited by Hakima Chaouchi & Maryline Laurent- Maknavicius. Wiley Publishing.
5. Wireless Sensor Network Security by Javier Lopez & Jianying Zhou. IOS Press.
6. IoT Security Issues, First Edition by Alasdair Gilchrist. De Gruyter Publishing

Syllabus for Semester VI, B. TECH CSE (Cyber Security)

Course Code: CCT6004 – 2 Course: Incident Handling & Response

L: 3 Hrs, T: 0 Hr, P: 0 Hr Per Week Total Credits: 3

Course Objectives:

1. To critically analyze and assess the impact of security incidents & response initiation
2. To recognize the importance of forensics and to follow well-defined processes and procedures
3. To understand & interpret the various stages in the lifecycle of forensic activities
4. To examine the technical, communication, and coordination aspects involved in providing an incident response

Syllabus

Unit 1: Preparing for the Inevitable Incident

Real-World Incidents, IR Management Essentials, Pre-Incident Preparation, Incident Handling vs Incident Response, Security Incident vs Security Event & Breach, First Responder

Unit 2: Incident Response Initiation

Stages of Incident Response, Security Incident Response Team Members, Incident Evidence, Incident Response Tools, Incident Investigation, Initial Lead Development, Incident Scope Discovery

Unit 3: Role of Forensics

The Forensic Process, Forensics Team Member Requirements, Forensics Team Policies and Procedures, Management of Forensics Evidence Handling, Forensics Tools, Legalities of Forensics, Forensics Team oversight

Unit 4: Incident Containment, Data Collection & Analysis

Live Data Collection, Forensic Duplication, Network Evidence Collection, Enterprise Services, Data Analysis Methodology, Investigating Windows, Linux and MAC Operating Systems, Investigating Applications, Malware Triage

Unit 5: Incident Eradication & Post-Incident Activities

Incident Analysis Report Writing, Remediation Team Forming, Remediation Plan Design, Remediation Implementation, Designing Strategic Recommendations, Employee Awareness & Training, Effective Stakeholder Communication

Unit 6: Incident Response Governance

Incident Response Policies and Procedures, Legal Requirements and Considerations, Governmental Laws, Policies and Procedures, General Team Management, Corporate IT- Related Security Relationship with SIR&FT, Relationship Management.

Course Outcomes:

After the successful completion of the course, students shall be able to –

1. Differentiate between cyber incidents and respond appropriately to them.
2. Use various digital forensic strategies and techniques to handle incidents and analyse them.
3. Conduct successful incident management activities in compliance with required standards.

Textbooks:

1. Incident Response & Computer Forensics, Third Edition by Jason T. Luttgens, Matthew Pepe & Kevin Mandia, Mc Graw Hill Education.
2. Computer Incident Response and Forensics Team Management: Conducting a Successful incident Response by Leighton R. Johnson III. Syngress Publishing

Syllabus for Semester VI, B. TECH CSE (Cyber Security)

Course Code: CCT6004 – 3 Course: Security Strategies in Windows & Linux

L: 3 Hrs T: 0 Hr P: 0 Hr Per Week Total Credits: 3

Course Objectives:

1. To identify the vulnerabilities in Windows & Linux operating system
2. To analyse the security architecture of Windows and Linux operating system
3. To analyse the best practices to respond and recover from a security breach

Syllabus

Unit 1: Microsoft Windows Security Situation

Information Systems Security, Microsoft EULA Microsoft Windows & Applications IT Infrastructure, Anatomy of Microsoft Windows Vulnerabilities, Windows OS Components & Architecture, Access control & Authentication, Users, Groups & Active Directory, Windows Attack Surfaces and Mitigation, Windows Security Monitoring & Maintenance

Unit 2: Managing & Maintaining Microsoft Windows Security

Access Controls in Windows, Windows Encryption Tools & Technologies, Windows Protection from Malware, Group Policy Control in Windows, Windows Security Profile & Audit Tools, Windows Backup & Recovery Tools, Windows Network Security, Windows Security Administration

Unit 3: Microsoft Windows Operating System and Application Security Trends and Directions

Windows Operating System Hardening, Microsoft Application Security, Windows Incident Handling & Management, Windows and the Security Lifecycle, Best Practices for Windows and Application Security

Unit 4: Linux Overview and Security Brief

Linux History, Linux Distributions, Linux in the Modern World, The Commands of Linux, Security Threats to Linux, Basic Components of Linux Security

Unit 5: Layered Security and Linux

User Privileges and Permissions, Filesystems, Volumes and Encryption, Securing Services, Networks, Firewalls, SELinux, AppArmor, Networked Filesystems & Remote Access, Networked Application Security, Kernel Security Risk Mitigation

Unit 6: Building a Layered Linux Security Strategy

Managing Security Alerts & Updates, Building & Maintaining a Security Baseline, Testing & Reporting, Detecting & Responding to Security Breaches, Best Practices & Emerging Technology

Course Outcomes:

After the successful completion of the course, students shall be able to

1. Recognize the attack surface on different versions & flavors of Windows & Linux operating systems.
2. Design strategic security plans for operating system security in Windows & Linux.
3. Administer layered security controls in Windows & Linux operating systems.

Textbooks:

1. Security Strategies in Windows Platforms and Applications, Third Edition by Michael G. Solomon. Jones and Bartlett Learning.
2. Security Strategies in Linux Platforms and Applications, Second Edition by Michael Jang & Ric Messier. Jones and Bartlett Learning

Syllabus for Semester VI, B. TECH CSE (Cyber Security)

Course Code: CCT6005 – 1 **Course: Managing Risk in Information Systems**

L: 3 Hrs T: 0 Hr P: 0 Hr Per Week **Total Credits: 3**

Course Objectives:

1. To understand and manage risks associated with the use of information technology.
2. To identify and assess risks to the confidentiality, integrity, and availability of an organization's assets.
3. To assess treatment of risks in accordance with risk mitigation plans & policies.

Syllabus

Unit 1: Introduction to Risk Management

What is Risk? Risk Classification, Basic Concepts of Risk, Risk Matrices, Lie Factors, Misconceptions, and Other Obstacles to Measuring Risk, Risk Identification Techniques, Risk Management Process, Risk Handling Strategies

Unit 2: Risk Management Business Challenges

Managing Risk: Threats, Vulnerabilities and Exploits, Understanding and Maintaining Compliance, Governance and Internal Partner, Governance and Internal Partnerships: How to Sense, Interpret, and Act on Risk, External Partnerships: The Power of Sharing Information, People are the Perimeter

Unit 3: FAIR Risk

Introduction to FAIR Risk, FAIR Terminology, Risk Measurement, Risk Analysis, FAIR Interpretation, Risk Scenarios using FAIR, Implementing FAIR-based Risk Management Model

Unit 4: Risk Management Frameworks & Systems

Enterprise Network Risk Management (ERM) Framework, NIST Risk Management Framework, COSO ERM Framework, COBIT Framework, Risk Management Information Systems (RMIS), Developing a Risk Management Plan

Unit 5: Risk Mitigation

Defining Risk Assessment Approaches, Performing Risk Assessment, Identifying Assets and Activities to be Protected, Identifying and Analyzing Threats, Vulnerabilities and Exploits, Identifying and Analyzing Risk Mitigation Controls, Planning Risk Mitigation Throughout an Organization

Unit 6: Risk Mitigation Plans and Policies

Turning a Risk Assessment into a Risk Mitigation Plan, Mitigating Risk with a Business Impact Analysis, Mitigating Risk with a Disaster Recovery Plan, Mitigating Risk with a Computer Incident Response Plan, Enterprise Network Risk Management Policy.

Course Outcomes:

After the successful completion of the course, students shall be able to –

1. Determine risk location, extent and impact on an organization.
2. Perform cyber-risk analysis using FAIR terminology.
3. Successfully eradicate and/or mitigate cyber risks in organizations.

Textbooks:

1. Managing Risk in Information Systems, Third Edition by Darril Gibson & Andy Igonor. Jones & Bartlett Learning.
2. Measuring and Managing Information Risk: A FAIR Approach by Jack Freund & Jack Jones. Butterworth-Heinemann Publishing.
3. Managing Risk and Information Security, Second Edition by Malcom W. Harkins. Apress Open Publishing.
4. How to Measure Anything in Cybersecurity Risk by Douglas W. Hubbard & Richard Seiersen. Wiley Publishing

Syllabus for Semester VI, B. TECH CSE (Cyber Security)

Course Code: CCT6005 – 2 Course: IoT Security

L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 3

Course Objectives:

1. Ability to understand the Security requirements in IoT
2. Examine in detail IoT device vulnerabilities
3. Understand how these vulnerabilities should be addressed and mitigated
4. Understand the IoT authentication and Cloud Security.

Syllabus

Unit I: Introduction of IoT

Definition, Characteristics, Physical design, Logical design, Functional blocks, Components in internet of things, Sensors and Actuators, M2M and IoT Technology, Fundamentals Devices and gateways.

Unit II: Requirement of IoT Security

Security Requirements in IoT Architecture - Security in Enabling Technologies -Security Concerns in IoT Applications. Security Architecture in the Internet of Things, Security Requirements in IoT - Insufficient Authentication/Authorization – Insecure, Access Control - Threats to Access Control, Privacy, and Availability - Attacks Specific to IoT.

Unit III- IoT Vulnerabilities

Threats to Access Control, Privacy, and Availability - Attacks Specific to IoT. Vulnerabilities – Secrecy and Secret-Key Capacity-Authentication/Authorization for Smart Devices - Transport Encryption – Attack & Fault trees

Unit IV: Role of Cryptography in IoT Security

Cryptographic primitives and its role in IoT – Encryption and Decryption – Hashes – Digital Signatures – Random number generation – Cipher suites – key management fundamentals – cryptographic controls built into IoT messaging and communication protocols – IoT Node Authentication

Unit V: Attacks and Remedies

Basic attacks, User anonymity, Perfect forward secrecy, reply attack, offline password guessing attack, user impersonation attack, Man in middle attack, Smart card loss and stolen attack, Server spoofing attack, Denial of Service attack and Distributed DoS

Unit VI: IoT Authentication and Cloud Security

Authentication layered architecture- Physical layer authentication, Network layer authentication, data processing layer authentication, application layer authentication, IoT node authentication-introduction, architecture, Phases-System setup phase by gateway node, sensors and user registrations, key exchange phase, login phase and authentication, password update phase, device adding phase, Cloud services and IoT – offerings related to IoT from cloud service providers – Cloud IoT security controls – An enterprise IoT cloud security architecture – New directions in cloud enabled IoT computing

Course Outcomes

After the successful completion of the course, students shall be able to

1. Secure a connected IoT product from scratch.
2. Identify the main threats and attacks on IoT products and services.
3. Build and deploy secure IoT solutions

4. Examine End-to-End IoT Security in detail.

Textbooks

1. Practical Internet of Things Security (Kindle Edition) by Brian Russell, Drew Van Duren
2. Securing the Internet of Things Elsevier
3. Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations
4. Internet of Things Security- Challenges, Advances, and Analytics, Patel Chintan and Nishant Doshi, CRC Press, Taylor and Francis Group
5. IoT Security Issues, Alasdair Gilchrist, DEG Press.

Syllabus for Semester VI, B. TECH CSE (Cyber Security)

Course Code: CCT6006 – 3 Course: Application Security

L: 3 Hrs T: 0 Hr, P: 0 Hr Per Week Total Credits: 3

Course Objectives

1. To describe web-based applications and associated threats
2. To understand the security architecture in web-based applications
3. To evaluate vulnerabilities in web application security
4. To comprehend Android application security framework
5. To comprehend iOS application security framework

Syllabus

Unit 1: Introduction to Application Security

The History of Software Security, Introduction to Types of Modern-day Applications, Application Architectures- Web Apps, Android Apps, iOS Apps, Thick-Client Apps, Application Testing Methodologies, Application Security Testing Lab Setup

Unit 2: Web Application Security - I

Web App Reconnaissance, API Analysis, Third-Party Dependencies, Architecture Weak Points, OWASP Top 10 & SANS 25, Hacking Web Applications

Unit 3: Web Application Security – II

Securing Modern Web Applications, Secure Application Architecture, reviewing code for Security, Vulnerability Management, Defending Against Attacks, Securing Third-Party Dependencies

Unit 4: Android Application Security - I

Current State of Android Application Security, Android App Permissions, Basic Android Testing, OWASP Mobile Top 10, Hacking Android Applications

Unit 5: Android Application Security – II

Application Security Essentials, Permissions & Policy File, Crypto APIs, Securing Application Data, Securing Server Interactions, Future of Android App Security

Unit 6: iOS Application Security

iOS Security Model, Debugging with LLDB, Networking & Interprocess Communication, Data Leakage & Injection Attacks, Encryption and Authentication, Mobile Privacy concerns.

Course Outcomes:

After the successful completion of the course, students shall be able to –

1. Discern the cyber-attack methods on applications and correlate them with application- specific technologies.
2. Perform ethical hacking procedures on applications to assess their cyber-risk level.
3. Use modern-day techniques to secure applications against cyber-attacks.

Text Books:

1. Web Application Security: Exploitation and Countermeasures for Modern Web Applications by Andrew Hoffman. O'Reilly Publishing.
2. OWASP Web Security Testing Guide v4.2 by OWASP Foundation
3. OWASP Mobile Security Testing Guide v1.4 by OWASP Foundation
4. Android Application Security Essentials by Pragati Ogal Rai. Packt Publishing.
5. iOS Application Security: The Definitive Guide for Hackers and Developers by David Thiel. No Starch Press.

Syllabus for Semester VI, B. TECH CSE (Cyber Security)

Course Code: CCT6006 Course: Deep Learning

L: 3 Hrs T: 0 Hr, P: 0 Hr Per Week Total Credits: 3

Course Objectives:

1. To introduce basic deep learning algorithms.
2. To understand real world problem which will be solved by deep learning methods.
3. To apply deep learning to a own applications.

Course Syllabus:

UNIT I: Basic of Deep Learning

History of Deep Learning, McCulloch Pitts Neuron, Thresholding Logic, Perceptrons, Perceptron Learning Algorithm and Convergence, Multilayer Perceptrons (MLPs), Representation Power of MLPs, Sigmoid Neurons, Feed forward Neural Networks

UNIT II: Training of feedforward Neural Network

Representation Power of Feed forward Neural Networks, Training of feed forward neural network, Gradient Descent, Gradient Descent (GD), Momentum Based GD, Nesterov Accelerated GD, Stochastic GD, AdaGrad, RMSProp, Adam

UNIT III: Regularization

Activation Function and Initialization Methods: Sigmoid, Tanh, Relu, Xavier and He initialization,
Regularization: Bias and variance, Overfitting, L1 and L2 regualarization, Batch Normalization, Dropout, PCA

UNIT IV: Convolution Neural Network (CNN)

Convolutional Neural Networks, 1D convolution network, 2D convolution network Visualizing Convolutional Neural Networks, Guided Backpropagation

UNIT V: Recurrent Neural Network (RNN)

Recurrent Neural Networks, Backpropagation through Time (BPTT), Vanishing and Exploding Gradients, Long Short Term Memory (LSTM) Cells, Gated Recurrent Units (GRUs). Variants of CNN and RNN: Encoder Decoder Models, Attention Mechanism, LeNet, AlexNet, ZF-Net, VGGNet, GoogLeNet, ResNet

Course Outcomes:

On successful completion of the course, students will be able to:

1. Train fully connected deep neural networks to real world problems.
2. Evaluate the performance of different deep learning models with respect to the optimization, bias-variance trade-off, overfitting and underfitting etc.
3. Apply the convolution networks and recurrent neural networks in context with real world problem solving.
4. Design variants of convolution networks and recurrent neural networks for various real-world problems.

Textbooks:

1. Sandro Skansi, Introduction to Deep Learning, Springer

2. Charu C. Aggarwal. Neural Networks and Deep Learning: A Textbook. Springer. 2019.
3. Ian Goodfellow and Yoshua Bengio and Aaron Courville. Deep Learning. An MIT Press book. 2016.
4. Dr. S Lovelyn Rose,Dr. L Ashok Kumar,Dr.D Karthika Renuka, Deep Learning using Python,Willey Publication

Reference Books:

1. Bishop, C., M., Pattern Recognition and Machine Learning, Springer, 2006.
2. Yegnanarayana, B., Artificial Neural Networks PHI Learning Pvt. Ltd, 2009.
3. Ravindran, K. M. Ragsdell, and G. V. Reklaitis, Engineering Optimization: Methods and Applications, John Wiley & Sons, Inc., 2016.

Syllabus for Semester VII, B. TECH CSE (Cyber Security)
Course Code: CCT7001 Course: Compiler Design
L: 3 Hrs T: 0 Hr P: 0 Hr Per Week Total Credits: 3

Course Prerequisite: Course on Theory of Computation.

Course Objectives:

1. To understand the theory and practice of compiler implementation.
2. To explore the principles, algorithms, and data structures involved in the design and construction of compilers.
3. To understand various phases of compiler and their working.

Syllabus

UNIT-I: Introduction to Compilers

Introduction to Compilers, Phases of compiler design, Relating Compilation Phases with Formal Systems, Lexical Analysis- Lexical analysis, tokens, pattern and lexemes, Design of Lexical analyzer, Regular Expression, transition diagram, recognition of tokens, Lexical Errors.

UNIT-II: Syntax Analysis

Specification of syntax of programming languages using CFG, Top-down parser, design of LL(1) parser, bottom up parsing techniques, LR parsing, Design of SLR, CLR, LALR parsers, Parser Conflicts.

UNIT-III: Syntax directed translation

Study of syntax directed definitions & syntax directed translation sche~~m~~es, Type and Type Checking, implementation of SDTS, intermediate notations- postfix, syntax tree, TAC, translation of Assignment Statement, expressions, controls structures, Array reference.

UNIT-IV: Code optimization

Machine-independent Optimisation- Local optimization techniques, loop optimization- control flow analysis, data flow analysis, Loop invariant computation, Induction variable removal, other loop optimization techniques, Elimination of Common sub expression, and Machine- dependent Optimisation techniques.

UNIT-V: Code generation

Problems in code generation, Simple code generator, code generation using labelling algorithm, Code Generation by Dynamic Programming.

Storage allocation & Error Handling

Run time storage administration stack allocation, Activation of Procedures, Storage Allocation Strategies, symbol table management, Error detection and recovery- lexical, syntactic and semantic.

Course Outcomes:

After successful completion of the course students will be able to:

1. Implement lexical analyzer from language specification.
2. Realize bottom up and top-down parsers incorporating error handling.

3. Demonstrate syntax directed translation schemes, their implementation for different programming language constructs.
4. Implement different code optimization and code generation techniques using standard data structures.

Text Books:

1. Aho, Sethi, and Ullman; Compilers Principles Techniques and Tools; Second Edition, Pearson education, 2008.
2. Alfred V. Aho and Jeffery D. Ullman; Principles of Compiler Design; Narosa Pub.House, 1977.
3. Manoj B Chandak, Khushboo P Khurana; Compiler Design; Universities Press, 2018.

Reference Books:

1. Vinu V. Das; Compiler Design using Flex and Yacc; PHI Publication, 2008.
2. V. Raghavan; Principles of Compiler Design, McGraw Hill Education (India), 2010.

Syllabus for Semester VII, B. Tech. Computer Science & Engineering (Cyber Security)
Course Code: CCT7002 Course: Secure Coding
L: 2 Hrs, T:1Hr, P: 0 Hr, Per Week Total Credits: 03

Course Objectives

1. To comprehend the fundamentals of Secure coding and its significance.
2. To identify various security attacks on an application
3. To recognize and remove common coding errors that lead to vulnerabilities in an application.
4. To comprehend various secure coding techniques for developing a secureapplication.

Syllabus

Unit I Fundamentals of Secure Coding: Security, CIA Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts- exploit, threat, vulnerability, risk, attack. Malware Terminology: Rootkits, Trapdoors, Botnets, Keyloggers, Honeypots. Active and Passive Security Attacks. IP Spoofing, Teardrop, DoS, DDoS, XSS, SQL injection, Smurf, Man in middle, Format String attack. Types of Security, Vulnerabilities- buffer overflows, Invalidated input, race conditions, access- control problems, weaknesses in authentication, authorization, or cryptographic practices. Access Control Problems.

Unit II Need for secure systems: Proactive Security development process, Secure Software Development Cycle (S-SDLC), Security issues while writing SRS, Design phase security, Development Phase, Test Phase, Maintenance Phase, Writing Secure Code – Best Practices SD3 (Secure by design, default and deployment), Security principles and Secure Product Development Timeline

Unit III Threat modeling process and its benefits: Identifying the Threats by Using Attack Trees and rating threats using DREAD, Risk Mitigation Techniques and Security Best Practices. Security techniques, authentication, authorization. Defense in Depth and Principle of Least Privilege

Unit IV Secure Coding Techniques: Protection against DoS attacks, Application Failure Attacks, CPU Starvation Attacks, Insecure Coding Practices In Java Technology. ARP Spoofing and its countermeasures. Buffer Overrun-Stack overrun, Heap Overrun, Array Indexing Errors, Format String Bugs. Security Issues in C Language: String Handling, Avoiding Integer Overflows and Underflows and Type Conversion Issues- Memory Management Issues, Code Injection Attacks, Canary based countermeasures using StackGuard and Propolice. Socket Security, Avoiding Server Hijacking, Securing RPC, ActiveX and DCOM.

Unit V Database and Web-specific issues: SQL Injection Techniques and Remedies, Race conditions, Time of Check Versus Time of Use and its protection mechanisms. Validating Input and Interprocess Communication, Securing Signal Handlers and File Operations. XSS scripting attack and its types – Persistent and Non persistent attack XSS Countermeasures and Bypassing the XSS Filters

Unit VI Testing Secure Applications: Security code overview, secure software installation. The Role of the Security Tester, Building the Security Test Plan. Testing HTTP-Based Applications, Testing File-Based Applications, Testing Clients with Rogue Servers

Course Outcomes:

On successful completion of the course, students will be able to:

1. Understand the basics of secure programming
2. Analyze the most frequent programming errors leading to software vulnerabilities
3. Identify security problems in software
4. Comprehend and protect against security threats and software vulnerabilities
5. Apply their knowledge to the construction of secure software systems

Textbooks

1. Writing Secure Code, Michael Howard and David LeBlanc,Microsoft Press.
2. Buffer Overflow Attacks: Detect, Exploit, Prevent by Jason Deckar,Syngress.
3. Threat Modeling, Frank Swiderski and Window Snyder,Microsoft Professional.

Reference Books

1. Robert C. Seacord, Secure Coding in C and C++, 2nd Edition, Addison-Wesley, 2013
2. CERT C CodingStandard. Available online: https://wiki.sei.cmu.edu/confluence/display/c/SEI+CERT+C+Coding+Standa rd
3. Wenliang Du, Computer Security – A hands-on Approach, Second Edition, Create space Independent Pub; 2019.

Syllabus for Semester VII, B. Tech. Computer Science & Engineering (Cyber Security)
Course Code: CCT7003 Course: Network Security Administration
L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Objectives

1. Learn the building blocks of network architecture and its security.
2. Understand the implementation of security controls in an organizational environment.
3. Explore high-level network management tools, techniques & procedures.

Syllabus

Unit I: Network security overview, benefits of good security practices, 3 Ds of security, business processes vs technical controls, risk analysis and defensemodels, threat vectors, Lollipop model, Onion model, security policy development - developers, audience, organization, topics, policy implementation

Unit II: Security organization, separation of duties, security operations management, lifecycle management, enforcement, data classification, documentation, authentication, EAP, authorization, ACLs, data security architecture, securingdata in flight, file encryption, digital rights management

Unit III: Security management architecture, AUP, administrative security, accountability controls, activity monitoring and audit, secure network design,wireless impact, remote access considerations, network hardening, anti- spoofing and source routing, logging

Unit IV: Types of firewalls, NAT, VPN protocols, SSL VPNs, client/server remote access threats, remote client security, radio frequency security, data-link layer wireless security flaws, wireless network hardening practices

Unit V: IDS types and detection models, Wireless IDS, IPS, IDS logging and alerting, IDS deployment considerations, integrity and availability architecture, patching, backups, system and network redundancy, network role-based security, proxy servers, credit card security

Unit VI: Disaster recovery, business continuity, malicious mobile code, countermeasures, creating a computer security defense plan, network regulations, Computer Fraud and Abuse Act, unauthorized access to electronic communications, compliance with laws in conducting incident response

Course Outcomes:

On successful completion of the course, students will be able to:

1. Identify different elements of network security.
2. Understand the management level of security implementation.
3. Implement network security controls to different network segments.
4. Determine network-specific security solutions.
5. Evaluate network security shortcomings and fulfill them.

Textbooks

1. Network Security: The Complete Reference by Roberta Bragg, Mark Rhodes-Ousley and Keith Strassberg. McGraw-Hill Publishing.

Syllabus for Semester VII, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCP7003 Course: Network Security Administration Lab

L: 2 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 1

Course Objectives

1. Implement risk analysis and defense models in networks.
2. Classify, authenticate and authorize different elements of network infrastructure.
3. Generate and implement organization-specific network defense plans.

Course Outcomes:

On successful completion of the course, students will be able to:

1. Design security processes & policies for network security.
2. Implement authentication and authorization controls in networks.
3. Secure data transmissions and stored data within a network.
4. Implement network perimeter security through firewall, IDS, IPS andVPNs.
5. Comply network security with governing laws and standards.

Syllabus for Semester VII, B. Tech Computer Science & Engineering (Cyber Security)
Course Code: CCT7004 – 1 Course: Database and Email Forensics
L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Objectives

The objective of this course is to familiarize students with

1. Digital forensics and investigation
2. Database forensics in depth
3. Email Forensics

Syllabus

Unit I: Introduction to Digital Forensics – In this module the students will get the basic understanding of what digital forensics is all about and how forensic investigations happen.

Unit II: Why is database forensics important? – In this module the students will learn the emphasis of database forensics and shall analyze the findings as well.

Unit III: Perform forensics on databases – This will be a mix of theory and practical knowledge where the students will learn how to perform forensic investigations on different databases

Unit IV: All about Email – In this module the students shall get in depth knowledge of email systems, clients and servers along with their characteristics.

Unit V: Understanding electronic record management – In this module the students will learn more about the way electronic records are managed in the real time domain.
Understanding email crimes – In this module the students will learn about different case studies about email crimes that have happened in the past and will also learn about the email crime laws.

Course Outcomes:

On successful completion of the course, students will be able to:

1. Define basics of digital forensics.
2. Describe about databases and the way their forensics are done
3. Interpret how email works and how such crimes are investigated
4. Evaluate the case studies of email crimes and laws that are laid for emailcybercrime.

Textbooks

1. Digital Forensics and Incident Response by Gerard Johansen
2. Digital Forensics by Dr. Jeetendra Pande and Dr. Ajay Prasad

Reference Books

1. Expert witness- Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Expert_witness 208
2. Expert witness, http://einvestigations.com/computer-forensics/expert-witness/

3. Information Technology Act, 2000 - Wikipedia, https://en.wikipedia.org/wiki/Information_Technology_Act,_2000
4. Legal aspects of computing - Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/Legal_aspects_of_computing

Syllabus for Semester VII, B. Tech Computer Science & Engineering (Cyber Security)

Course Code: CCP7004 – 1 Course: Database & Email Forensics Lab

L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week Total Credits: 01

Course Objectives

1. To implement database security practices for solving problems.
2. To implement email parsing systems.
3. To learn the role of forensics in Email & Database security incident handling

Syllabus

Experiments based on CCT7004 – 1

Course Outcome

On successful completion of the course, students will be able to:

1. Implement various database security practices
2. Implement database forensic techniques
3. Apply email parsing algorithms for email forensics
4. Analyse the case studies of email crimes and laws that are laid for email cybercrime

Syllabus for Semester VII, B. Tech Computer Science & Engineering (Cyber Security)
Course Code: CCT7004 – 2 Course: Auditing IT Infrastructure for Compliance
L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Objectives

1. Learn about the importance of information security auditing and different auditing standards.
2. Understand audit scoping and perform standard-specific security audits in different types of organizations.
3. Explore higher level security governance concepts like CMMI, Quality Assurance etc.

Syllabus

Unit I: Introduction to COBIT, Using COBIT to Assess Internal Controls, COBIT Assurance Framework Guidance, ISACA IT Auditing Standards Overview, Risk Management Fundamentals, Quantitative Risk Analysis Techniques, IT Audit Risk and COSO ERM, Performing Effective IT Audits

Unit II: General Controls in Today's IT Environments, ITIL Service Management Best Practices, Systems Software and IT Operations General Controls, Evolving Control Issues: Wireless Networks, Cloud Computing, and Virtualization

Unit III: IT Application Control Elements, Selecting Applications for IT Audit Reviews, Auditing Applications under Development, Application Review Case Study: Client-Server Budgeting System, Importance of Reviewing IT Application Controls, Micro Project - IT Application Auditing

Unit IV: Software Engineering Concepts, CMMI: Capability Maturity Model for Integration, IT Audit, Internal Control, and CMMI, IT Auditing in SOA Environments, Computer-Assisted Audit Tools and Techniques (CAATTs)

Unit V: IT Controls and the Audit Committee, Role of the Audit Committee for IT Auditors, Audit Committee Review and Action on Significant IT Audit Findings, Compliance with IT-Related Laws and Regulations, Understanding and Reviewing Compliance with ISO Standards, Controls to Establish an Effective IT Security Environment

Unit VI: Auditing Telecommunications and IT Communications Networks, Building an Effective IT Internal Audit Function, Quality Assurance Auditing and ASQ Standards, Live Project - IT Security Auditing

Course Outcomes:

On successful completion of the course, students will be able to:

1. Understand and identify different information security audit standards and frameworks.
2. Differentiate between the compliance requirements of different audit frameworks.
3. Carry out standard IT auditing procedures in organizations.
4. Perform analysis on audit findings and calculate cyber risk.
5. Generate quality audit reports and effectively communicate them to organizations.

Textbooks

1. IT Audit, Control, and Security by Robert R. Moeller. Wiley Publishing.

Reference Books

1. Auditing Information and Cyber Security Governance – A Controls-Based Approachby Robert E. Davis|2021 Edition. CRC Press.

Syllabus for Semester VII, B. Tech Computer Science & Engineering (Cyber Security)

Course Code: CCP7004 – 2 Course: Auditing IT Infrastructure for Compliance Lab

L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week Total Credits: 1

Course Objectives

1. Apply different auditing standards as per organization's requirement.
2. Design audit scope and conduct industry-standard audits.
3. Implement security governance through CMMI, quality assurance etc.

Course Outcomes:

On successful completion of the course, students will be able to:

1. Design audit checklists based on different auditing standards.
2. Scope out necessary elements of auditing.
3. Conduct Information Security audits at organization level.
4. Analyze audit findings and generate remediations and conclusion.
5. Design standardized and detailed audit reports.

Syllabus for Semester VII, B. Tech. (Computer Science & Engineering) (Cyber Security)

Course Code: CCT7004 – 3 Course: Blockchain Security

L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Objectives

1. This course aims to provide a survey on blockchain and the topics around such as history of blockchain, cryptography it uses, Bitcoin and other currencies, consensus algorithms, smart contracts, Ethereum, scalability and various use cases.

Syllabus

Unit I: Blockchain Introduction: Blockchain Technology Mechanisms & Networks, Blockchain Origins, Blockchain Objectives, Blockchain Users & Adoption, Blockchain Challenges, P2P Systems, Hash Pointers and Data Structures, Blockchain Transactions

Unit II: Consensus Mechanism: ermissioned Blockchain, Permisionless Blockchain, Different Consensus Mechanism- Proof of Work, Proof of Stake, Proof of Activity, Proof of Burn, Proof of Elapsed Time, Proof of Authority, Proof of Importance.

Unit III: Cryptography Fundamentals: Encryption, Digital Signatures, Public-Key Cryptography, Private Key Cryptography, Distributed Denial-of-Service (DDoS) Attack, 51% Attack, Double spending problem, Merkel Tree, Security Threats to Blockchain Technology

Unit IV: Crypto currency and Wallet: Types of Wallet, Desktop Wallet, App based Wallet, Browser based wallet, Metamask, Creating a account in Metamask, Use of faucet to fund wallet, transfer of cryptocurrency in metamask.

Unit V: Smart contract and Ethereum Overview of Ethereum, Writing Smart Contract in Solidity, Remix IDE , Different networks of ethereum, understanding blocks in blockchain, compilation and deployment of smart contracts in Remix

Unit VI: Use Cases: Enterprise application of Block chain: Cross border payments, Know Your Customer (KYC), Food Security, Block chain enabled Trade, We Trade – Trade Finance Network, Supply Chain Financing, Identity on Block chain, Blockchain in energy sector, Blockchain in governance

Course Outcomes:

On successful completion of the course, students will be able to:

1. Realize the importance of blockchain technology and consensus mechanism
2. Identifying the security risks and challenges associated with blockchain technology
3. Implement browser-based wallets and smart contracts in Remix IDE
4. Recognize the importance of blockchain security in various enterprise applications.

Text Books

1. Mastering Blockchain: Third Edition by Imran Bashier, Packt Publishing, 2020, ISBN: 9781839213199,

Reference Books

1. Blockchain: Blueprint for a New Economy by Melanie Swan, Oreilly Publication
2. Mastering Ethereum, by Andreas M. Antonopoulos, Gavin Wood
3. Bitcoin and Cryptocurrency Technologies (Princeton textbook) by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder

Syllabus for Semester VII, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCP7004-3 Course: Blockchain Security Lab

L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week Total Credits: 01

Course Objectives

This course aims to provide hands-on experience with blockchain development tools and frameworks, and will be able to use them to build and test their own blockchain projects.

Syllabus:

Experiments based on the above syllabus CCT401-3

Course Outcome:

On completion of the course the student will be able to

1. Realize different blockchain tools and framework
2. Implement smart contracts for the development of enterprise applications
3. Apply different wallets for the deployments of smart contracts
4. Analyze blockchain security in various enterprise applications

Syllabus for Semester VII, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCP7005 Course: Data Visualization Techniques

L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week Total Credits: 01

Course Objectives

1. To introduce advanced tools and libraries for creating interactive and dynamic visualizations.
2. To apply cognitive and perceptual principles to the design of complex data dashboards.
3. To develop skills in transforming multi-dimensional data into meaningful visual stories for stakeholders.

Syllabus

- **Module I: Advanced Python/R Visualization:** Mastery of specialized libraries (Seaborn, Plotly, Plotnine) for multi-variate data and high-dimensional aesthetics.
- **Module II: Interactive Visuals & Web Frameworks:** Introduction to building web-based interactive charts using Bokeh, Dash, or Streamlit.
- **Module III: Geospatial and Temporal Mapping:** Visualizing data with geographical components using Folium, Geopandas, or Leaflet.
- **Module IV: Dashboarding & Business Intelligence:** Design and development of professional dashboards using industry tools like Tableau, Power BI, or Google Data Studio.
- **Module V: Data Storytelling:** Techniques for creating author-driven and reader-driven narratives with emphasis on annotations and highlighting.

List of Practicals

1. **Multi-variate Analysis:** Create a matrix of visualizations (Facet Grids/Pair Plots) to explore correlations in a high-dimensional dataset.
2. **Interactive Distributions:** Design an interactive histogram and box-plot set that allows users to filter data by categories using **Plotly**.
3. **Geospatial Visualization:** Create a Choropleth map to visualize regional statistics (e.g., COVID-19 cases or Sales by state) using **Folium**.
4. **Network Graphing:** Visualize a social network or a relationship dataset using **NetworkX** or **Gephi** to identify clusters and influencers.
5. **Interactive Time-Series:** Build a time-series dashboard with "range sliders" and "selectors" to analyze trends over a decade.
6. **Hierarchical Data:** Implement a Treemap or Sunburst chart to represent nested categories (e.g., Product Hierarchy or File Systems).
7. **Web-based Dashboard (Part 1):** Develop a single-page interactive data app using **Streamlit** that takes user input to update charts in real-time.
8. **Web-based Dashboard (Part 2):** Deploy a multi-page dashboard with **Dash/Plotly** incorporating data tables and download features.
9. **Business Intelligence Case Study:** Create a sales performance dashboard in **Tableau/Power BI** featuring KPIs, Gauges, and Drill-down charts.
10. **Visualizing Uncertainty:** Create a plot representing error bars, confidence intervals, and probability distributions for a predictive model.

11. **Final Project: Data Story:** Develop a comprehensive "Data Story" on a public dataset (e.g., Kaggle/UCI) using an interactive notebook or dashboard, adhering to best practices of perception.

Course Outcomes:

On successful completion of the course, students will be able to:

- **CO1:** Use advanced visualization libraries to preprocess and map complex data onto appropriate visual aesthetics.
- **CO2:** Analyze multi-dimensional datasets to discover hidden patterns and choose the most effective visualization technique for specific data types.
- **CO3:** Evaluate visual representations based on principles of human perception, cognitive load, and design best practices to ensure clarity and accuracy.
- **CO4:** Design and deploy interactive, web-based dashboards and visual stories that facilitate data-driven decision-making for end-users.

Text Books

1. Claus O. Wilke, *"Fundamentals of Data Visualization – A Primer on Making Informative and Compelling Figures"*, O'Reilly, 2019.
2. Cole Nussbaumer Knaflic, *"Storytelling with Data: A Data Visualization Guide for Business Professionals"*, Wiley, 2015.
3. Kyran Dale, *"Data Visualization with Python and JavaScript"*, 2nd Edition, O'Reilly, 2022.

Reference Books

1. Edward Tufte, *"The Visual Display of Quantitative Information"*, 2nd Edition, Graphics Press, 2001.
2. Tamara Munzner, *"Visualization Analysis and Design"*, AK Peters Visualization Series, CRC Press, 2014.
3. Scott Murray, *"Interactive Data Visualization for the Web: An Introduction to Designing with D3"*, O'Reilly, 2017.

Syllabus for Semester VIII, B. E. Cyber Security (Computer Science & Engineering)

Course Code: CCT8001 -1 Course: Vulnerability Assessment and Penetration Testing

L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Objectives

1. Learn about various hacking concepts and requirements of setting-up a penetration testing lab.
2. Learn to use Kali Linux and different penetration testing tools.
3. Explore advanced penetration testing concepts.

Syllabus

Unit I: Setting up virtual lab, Configuring the Network for Your Virtual Machine, Setting Up Android Emulators, Target Virtual Machines, Setting a Static IP Address, Setting up external servers, Using Kali Linux, Programming

Unit II: Tools of the trade, Using Metasploit Framework, Types of Shells, Msfcli, Creating standalone payloads, Information gathering, Red team recon, Finding Vulnerabilities, Capturing Traffic

Unit III: Exploitation, Exploiting WebDAV default credentials, Exploiting Open phpMyAdmin, Exploiting Third-party Web Applications, Exploiting NFS shares, Password attacks, Client-side exploitation - Browser, PDF, Java etc.

Unit IV: Social engineering, Mass email attacks, Multipronged attacks, Compromising the network, Bypassing anti-virus applications, Post exploitation, Privilege escalation, Lateral movement, Pivoting, Persistence

Unit V: Web application testing, Using BurpSuite, SQL injection, XPath injection, LFI, RFI, CSRF, XSS, Wireless attacks, Physical attacks, Stack-based buffer overflowin linux and windows, Known vulnerability in War-FTP, Locating & controlling EIP**.**
Structured exception handler overwrites, Finding attack string in memory, Using a short jump, Fuzzing, Finding bugs with code review, Porting exploits, Replacing shellcode, Writing Metasploit modules, Exploitation mitigation techniques

Course Outcomes:

On successful completion of the course, students will be able to:

1. Apply penetration testing concepts to network and applications.
2. Identify vulnerabilities in target technology and exploit them.
3. Carry out privilege escalation activities in breached networks.
4. Implement social engineering and physical attacking methods for penetration testing.
5. Design custom hacking scripts.

Textbooks

1. Penetration Testing: A Hands-On Introduction to Hacking by Georgia Weidman|2014 Edition. No Starch Press.
2. The Hacker Playbook 3: Practical Guide to Penetration Testing by Peter Kim

Syllabus for Semester VIII, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCT8001- 2 Course: Disaster Recovery and Business Continuity Management
L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Objectives

1. Understand the concept of business continuity
2. Learn the importance of a BCP (business continuity planning)
3. See how load balancing maintains business continuity
4. Know the details of DCP (Disaster recovery plan)
5. Learn how to choose the right fail over solution

Syllabus

Unit I: Introduction to Business Continuity Management (BCM) and Disaster Recovery (DR)-Terms and definitions, BCP under a Governance and BCP Policy making Project Scope and Planning,

Unit II: Business Organization Analysis, BCP Team Selection, Resource Requirements, Legal and Regulatory Requirements, Business Impact Analysis

Unit III: Concepts of threat, vulnerabilities, and hazard - Risk Management process - Risk assessment, risk control options analysis, risk control implementation, risk control decision, and risk reporting -Business Impact Analysis (BIA) concept, benefits and responsibilities - BIA methodology - Assessment of financial and operational impacts, identification of critical IT systems and applications, identifications of recovery requirements and BIA reporting

Unit IV: IT recovery strategy, Business continuity strategy development framework - Cost- benefit assessment - Site assessment and selection - Selection of recovery options -Strategy considerations and selection - Linking strategy to plan - Coordinating with External Agencies
-Business continuity plan contents - Information Systems aspects of BCP - Crisis Management - Emergency response plan and crisis communication plan - Awareness, training and communication - Plan activation - Business Continuity Planning Tools.

Unit V: Database recovery - Recovery Plan Development, Personnel Notification, DR site- concepts and management, Backups and Offsite Storage, Backup Media Formats, Software Escrow Arrangements, External Communications, Utilities Logistics and Supplies, Emergency Handling for Crisis Management, safety and rescue of personnel in emergency

Plan maintenance requirements and parameters - Change management and control - Business Continuity Plan Audits. Disaster Recovery – Definitions - Backup and recovery - Threat and risk assessment - Site assessment and selection - Disaster Recovery Road map - Disaster Recovery Plan (DRP)preparation - Vendor selection and implementation - Difference between BCP and DRP - Systems and communication security during recovery and repair, ISMS policies, ISO 27000

Course Outcomes:

On successful completion of the course, students will be able to:

1. Identify the integral aspects of Business Continuity Management
2. Analyze common organizational risks and threats to business system continuity
3. Evaluate an organization's ability to recover from a given disaster or event
4. Apply business continuity and disaster recovery principles to enhance abusiness continuity plan

Textbooks

1. Disaster Recovery Handbook –M Wallace and Lawrence Webber , AMACOM; 3rd edition (22 March 2018)
2. Disaster Recovery Planning-S.S.Kambhmmettu

Reference Books

1. CISSP handbook

Syllabus for Semester VIII, B. Tech. Computer Science & Engineering (Cyber Security)
Course Code: CCT8001-3 Course: Mobile Application Security Testing
L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Objectives

1. Learn about various types of mobile application development platforms.
2. Learn to use different mobile app penetration testing tools and frameworks.
3. Explore mobile application security concepts.

Syllabus

Unit I: Evolution of mobile apps, Mobile app security, OWASP mobile security project, Mobile security tools, Analyzing iOS Applications, Understanding the Security Model, Understanding iOS Applications, Jailbreaking Explained, Understanding the Data Protection API, Understanding the iOS Keychain, Understanding Touch ID, Reverse Engineering iOS Binaries

Unit II: Analyzing Android applications, Understanding security model, Reverse engineering applications, Attacking Android applications, Accessing storage and login, misusing insecure communications, Tools: Xposed framework, Cydia substrate

Unit III: Identifying and exploiting android implementation issues, reviewing pre- installed apps, Exploiting devices, Infiltrating user data, Writing secure android applications, Principle of least exposure, Storing files securely, Securing WebViews, Logging

Unit IV: Analyzing Windows Phone Applications, Understanding the Security Model, Understanding Windows Phone 8.x Applications, Building a test environment, Analyzing application binaries, Attacking Windows Phone Applications, Attacking Transport Security, Identifying Interprocess Communication Vulnerabilities, Patching .NET Assemblies

Unit V: Identifying windows phone implementation issues, Identifying Insecure Application Settings Storage, Identifying Data Leaks, Identifying Insecure Data Storage, Insecure Random Number Generation, Insecure Cryptography and Password Use, Writing Secure Windows Phone Applications, Storing and Encrypting Data Securely, Securing Data in Memory and Wiping Memory, Secure XML Parsing, Avoiding Native Code Bugs Analyzing BlackBerry Applications, Understanding BlackBerry Legacy, Understanding the BlackBerry 10 Security Model, BlackBerry 10 Jailbreaking, Using Developer Mode, The BlackBerry 10 Device Simulator, Accessing App Data from a Device, Accessing BAR Files, Attacking BlackBerry Applications, Traversing Trust Boundaries

Course Outcomes:

On successful completion of the course, students will be able to:

1. Understand different mobile app development operating systems.
2. Identify vulnerabilities in android, windows, blackberry and iOS phones.
3. Reverse engineer mobile apps on multiple platforms.
4. Set up mobile app security testing labs for different operating systems.
5. Secure mobile apps.

Textbooks

1. The Mobile Application Hacker's Handbook by Dominic Chell, Tyrone Erasmus, Shaun Colley and Ollie Whitehouse. Wiley Publishing.

Syllabus for Semester VIII, B. Tech. Computer Science & Engineering (Cyber Security)
Course Code: CCT8002 – 1 Course: Testing Cyber Crime Investigation and Digital Forensics
L: 4 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 04

Course Objectives

The objective of this course is to familiarize students with

1. Different Cyber laws
2. Types of cyber crimes
3. The way investigations are done

Syllabus

Unit I

Introduction to Cyber Laws – In this module the students will get the basic understanding all the cyber laws that are currently in effect.

Unit II Types of cybercrimes – In this module the students will learn the different types of cybercrimes along with analysis on different case studies.

Unit III Social Media Investigation – This module will be a detailed case study analysis module which will focus on different social media crimes and the way they are investigated.

Unit IV Communication Device Based Investigation– In this module the students shall get in depth knowledge of introduction to the communication devices, knowledge on laws related to interception, knowledge on CDR, CDR formats, CDR analysis and investigations on VOIP communications using case studies.

Unit V Mobile Forensics – In this module the students will learn about the introduction to mobile forensics, types of memories on mobile phones, techniques of mobile forensics and the investigation process.

Unit VI Investigation on Financial Frauds and Cybercrime– In this module the students will learn about Introduction to investigation of financial frauds and cybercrime, steps to follow in case of financial frauds, Investigation on ATM withdrawal frauds, online transaction frauds, bank to bank transfer frauds and about the indicative notice under 91 CrPC issued to the banks.

Course Outcomes:

On successful completion of the course, students will be able to:

1. Define types of cyber laws.
2. Evaluate about types of cybercrimes pertaining in today's cyber society.
3. Describe how investigations are done based on the case studies

Textbooks

1. Combating Cyber Crimes by National Center for Justice and the Rule of Law
2. National Cyber crime reference handbook by National Cyber Safety and Security Standards, Ministry of Defence, Ministry of Electronics and Information Technology and

Reference Books

1. https://www.ojp.gov/pdffiles1/nij/187736.pdf
2. https://cc.iittp.ac.in/pdfs/Doc%202%20National%20Cyber%20Crime%20Reference%20Handbook%20III%20Edition.pdf

Syllabus for Semester VIII, B. E. (Computer Science & Engineering)
Course Code: CCT8002 – 2 Course: Executive Governance and Management in IT Security
L: 3 Hrs, T: 0 Hrs, P: 0 Hrs, Per Week Total Credits: 03

Course Objectives

1. To understand formation of an organization wide information security strategy
2. To study approach behind interactions between the C-Suite of the company.
3. To know how to manage risks at an acceptable level
4. To critique creation of information security policies

Syllabus

Unit I: Information Security Strategy: Evolution of Information Security, Organization Historical Perspective, Understand the External Environment, The Internal Company Culture, Prior Security Incidents, Audits, Security Strategy Development Techniques

Unit II: Security Management Organization Structure: Relevance of Security Leadership Roles, Security Leader Titles, Techie versus Leader, The Security Leaders Library, Security Leadership Defined, Security Leader Soft Skills, Security Functions

Unit III: Managing the Risk: Accepting Organizational Risk, Risk Ownership Management, Qualitative vs Quantitative Risk Analysis, Risk Management Process, Risk Mitigation Options

Unit IV: Creation of Information Security Policies: Importance of Information Security Policies, Canned Security Policies, Policies, Standards, Guidelines Definitions, Approach for Developing Information Security Policies, Policy Review Process

Unit V: Security Compliance & Control Frameworks: Security Control Frameworks and Standard Examples, Existence of Standards, Integration of Standards and Control Frameworks, Auditing Compliance, Adoption Rate of Standards, The Standards/Framework Value Proposition Security Controls & Incidents.
Managerial Controls, Technical Controls, Operational Controls, Anatomy of an Audit, Audit Execution Phase, Effective Security Communication, Security Incidents & Handling, The Law and Information Security

Course Outcomes:

On successful completion of the course, students will be able to:

1. Use enterprise information security practices and various strategies.
2. Apply information security risk evaluation processes for modeling and solving real- world problems.
3. Analyze the impact of different information security policies in enterprise scenarios.
4. Estimate the value propositions of the information security frameworks.

Textbooks

1. Information Security Governance Simplified, Todd Fitzgerald, CRC Press

Reference Books

1. Enterprise Security: A Data-Centric Approach to Securing the Enterprise, Aaron Woody, Packt Publishing

Syllabus for Semester VIII, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCT8002 – 3 Course: Security in Social Networks

L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Objectives

1. s

SYLLABUS

UNIT – I: Networks and Society

Network preliminaries; Social Networks: Introduction and Applications; Overview of Social Network Analysis; Social Media Content and Levels of Network Analysis.

Networks and Graphs: Types of Networks; Representation of Networks; Network Properties.

UNIT – II: Network Measures

Node Centrality: Degree, Closeness, Betweenness, Edge Betweenness, Katz, Eigen Vector Centrality; Edge and Flow Betweenness; PageRank; Hub and Authority.

Associativity, Transitivity and Reciprocity; Similarity: Structural and Regular Equivalence; Degeneracy: k-Core, Coreness, Core Periphery.

UNIT – III: Network Growth Models and Community Detection

Properties of Real-World Networks: Small World Property, Scale Free Property; Random Network Model; Ring Lattice Network Model; Preferential Attachment Model; Price's Model; Six Degrees of Separation. Types of Communities; Community Detection Methods: Disjoint Community Detection, Overlapping Community Detection, Local Community Detection; Community Detection versus Community Search; Community Evaluation.

UNIT – IV: Ego Networks and Information Diffusion

Ego Network – Overview and Characteristics; Ego Network Measures: Structural Holes, Density, Brokerage. Information Diffusion Overview; Explicit Networks: Herd Behavior, InformationCascades; Implicit Networks: Epidemical Models, Diffusion of Innovation.

UNIT – V: Security Challenges in Social Networking

The dark side of OSNs and Media; User responses; Opportunities in OSNs; Taxonomy of OSN attacks; Taxonomy of OSN solutions; Malware attacks and Phishing attacks in OSNs.

UNIT – VI: Threats and Preventive Measures in OSNs

Attackers and Social Media Platforms; Social media attacks based on account types; Cyber security tools for protecting user accounts. Identity theft and cyber bullying in OSNs.

General practices to protect – system, accounts and information; Issues and challenges in existing security solutions; principles to protect user account on social platform.

Course Outcomes:

On completion of the course the student will be able to

1. Analyze network data and complex graphs structures.

2. Apply the basics of social network analysis at various levels.
3. Model various interactions between individuals and actors.
4. Analyze the impact of different attacks on OSNs.

Textbooks and References:

1. Tanmoy Chakraborty; Social Network Analysis; First Edition; Wiley India; 2021.
2. Niyati Aggarwal and Adarsh Anand; Social Networks: Modeling and Analysis;CRC Press; 2022.
3. Brij B. Gupta and Somya Ranjan Sahoo; Online Social Network Security: Principles, Algorithms, Applications and Perspectives; CRC Press; 2021.

References:

1. David Easley and Jon Kleinberg; Networks, Crowds, and Markets: Reasoning about a Highly Connected World; Cambridge University Press; 2001.
2. Michael Cross; Social Media Security: Leveraging Social Networking while Mitigating Risk; Elsevier Science; 2013.
3. Stanley Wasserman and Katherine Faust; Social Network Analysis: Methods and Applications; Cambridge University Press; 1994.
4. Carl Tim and Richard Perez; Seven Deadliest Social Network Attacks; Elsevier Science; 2010

Syllabus for Semester VIII, B. Tech. Computer Science & Engineering (Cyber Security)

Course Code: CCT8004 Course: Research Methodology

L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Outcomes

1. Ability to critically evaluate current research and propose possible alternate directions for further
2. work.
3. Ability to develop hypothesis and methodology for research
4. Ability to comprehend and deal with complex research issues in order to communicate their
5. scientific results clearly for peer review.

Syllabus

Introduction to research methodology: Meaning of Research, Objectives of Research, Motivation in Research, Types of Research, Research Approaches, Significance of Research, research Methods versus Methodology, Research and Scientific Method, Research Process, Criteria of good Research, Necessity and Techniques of Defining the Problem, Meaning and need of Research Design, Features of a Good Design, Important Concepts Relating to Research Design, Different Research Design, Research ethics, Stress management.

Literature review, Data collection and sampling design: Review concepts and theory, review previous findings, Sources of data: Primary and secondary data, Methods of data collection, Sampling fundamentals

Modelling and Analysis: Probability distributions, Processing and analysis of data, Data analysis skills, Distributions, Statistical and multivariate analysis, Correlation and regression, Fundamentals of Time series analysis, spectral analysis, Error analysis, Simulation techniques

Algorithmic processes in Computer science research domains: Soft computing, Artificial intelligence, NLP, Image processing, Data management techniques, Networks and security, Software systems

Research Reports: Structure and components of Research report, Types of report, Layout of research report, Mechanisms and tools for writing research report, LaTeX

Text and Reference Books

1. C. R. Kothari, Research Methodology Methods and Techniques, 2nd revised edition, New Age.
2. Richard I Levinamp; DavidS.Rubin,StatisticsforManagement,7/e.PearsonEducation,2005.
3. DonaldR.Cooper,PamelaS.Schindler,BusinessResearchMethods,8/e,TataMcGraw - HillCo. Ltd., 2006.
4. Bendat and Piersol, Random data: Analysis and Measurement Procedures, Wiley Interscience,
5. 2001.
6. Shumway and Stoffer, Time Series Analysis and its Applications, Springer, 2000.
7. Jenkins, G. M., and Watts, D.G., Spectral Analysis and itsApplications,HoldenDay,1986.