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 2022-23

B. TECH. (COMPUTER SCIENCE & ENGINEERING) CYBER SECURITY

About the Department:

The Department of Computer Science & Engineering was established in 2002, is well-equipped with state-of-the-art infrastructure. The state of art infrastructure includes the latest configuration desktops organized in four different laboratories.

The department hosts computers, laptops and labs with internet facilities. The 24X7 network is managed with Cyberoam UTM firewall, and CISCO router offers intranet and internet connectivity. The computer laboratories have high-end servers of IBM and WIPRO along with industry-standard software, viz., Oracle, NetSim, Wireshark, AIX, Robotics Platform, IOT Kit and MSDN. The department promotes high- end computing through Open-Source technologies and hosts NVIDIA DGX DL Workstation.

The Department has a distinction of consistently achieving above 95% results in the final year. Students are encouraged to appear in GATE, CAT, GRE and other competitive examinations which have resulted in an increasing number of students clearing these exams.

Students' teams of CSE have emerged winners at the Grand Finale of 2018, 2019, 2020 and 2022 editions of Smart India Hackathon and have been excelling at the world renowned prestigious International Collegiate Programming Contest, ACM ICPC Asia West Regional Contents since 2015.

Department of Computer Science and Engineering – Cyber Security has successfully organized A National Level Cyber Awareness Week, AARHANT'22 (From 06/09/2022 to 10/09/2022) in the association with Vigilante Cyber Forces for the much-needed awareness regarding the domain and future scope of the Cyber Security in the upcoming time. Around 650 students in and around Nagpur participated in the event and took the most of it.

Departmental Vision:

To continually improve the education environment, in order to develop graduates with strong academic and technical background needed to achieve distinction in the discipline. Excellence is expected in various domains like workforce, higher studies or lifelong learning. To strengthen links between industry through partnership and collaborative development works.

Department Mission:

To develop strong foundation of theory and practices of computer science amongst the students to enable them to develop into knowledgeable, responsible professionals, lifelong learners and implement the latest computing technologies for the betterment of society.

Program Education Objectives:

1. To develop the ability to adapt, participate and invent new technologies and systems in the key domains of Computer Science & Engineering and Cyber Security.
2. To produce skilled graduates to identify the security challenges in the real world and suggest suitable design solutions to cater to industrial needs and excel in innovation and management fields.
3. To inculcate sound Computer Science practices and Cyber security fundamentals among the graduates to meet the dynamically changing technological needs.
4. To imbibe ethical and social responsibility, multidisciplinary team spirit, proficiency in soft skills, entrepreneurship skills and leadership qualities among the students for the betterment of the society.

Programme Outcomes (POs):

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3. **Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
4. **Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. **Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.
6. **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
7. **Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective

presentations, and give and receive clear instructions.

11. **Project management andfinance:** Demonstrate knowledge and understanding oftheengineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. **Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and lifelong learning in the broadest context of technological change.

Programme Specific Outcomes (PSOs):

1. The ability to understand and apply the Computer Science and Cyber Security principles.
2. The ability to develop computational knowledge and project development skills using innovative tools and techniques to solve problems in the areas related to Cyber Security.

Teaching Scheme for B. Tech Computer Science & Engineering (Cyber Security)

Semester - I

Sr. No.	Course Code	Course Name	Hours/week			Credits	Maximum marks			ESE Duration (Hrs)
			L	T	P		Continuous Evaluation	End Sem Exam	Total	
1.	CHT152	Chemistry	3	1	0	4	40	60	100	03
2.	CHP152	Chemistry lab	0	0	3	1.5	25	25	50	-
3.	MAT152	Differential Equation, linear Algebra, Statistics & Probability	3	0	0	3	40	60	100	03
4.	CCT101	Programming for Problem Solving	4	0	0	4	40	60	100	03
5.	CCP101	Programming for Problem Solving Lab	0	0	2	1	25	25	50	-
6.	IDT151	Creativity, Innovation & Design Thinking	1	0	0	1	20	30	50	1.5
7.	CCT102	Computer Workshop	1	0	0	1	20	30	50	1.5
8.	CCP102	Computer Workshop Lab	0	0	2	1	25	25	50	-
9.	HUT151	English	2	0	0	2	40	60	100	03
10.	HUP151	English Lab	0	0	2	1	25	25	50	-
		TOTAL	**14**	**1**	**9**	**19.5**	**300**	**400**	**700**	

Semester – II

Sr. No.	Course Code	Course Name	Hours/week			Credits	Maximum marks			ESE Duration (Hrs)
			L	T	P		Continuous Evaluation	End Sem Exam	Total	
1.	PHT154	Introduction to Quantum Computing	3	1	0	4	40	60	100	03
2.	PHP154	Introduction to Quantum Computing Lab	0	0	3	1.5	25	25	50	-
3.	MAT151	Calculus	3	1	0	4	40	60	100	3
4.	MAP151	Computational Mathematics lab	0	0	2	1	25	25	50	-
5.	CCT103	Digital Electronics	3	0	0	3	40	60	100	03
6.	CCP103	Digital Electronics Lab	0	0	2	1	25	25	50	-
7.	CCT104	Object Oriented Programming	3	0	0	3	40	60	100	03
8.	CCP104	Object Oriented Programming Lab	0	0	2	1	25	25	50	
9.	HUT152	Constitution of India	2	0	0	0	-	-	-	-
10.	PEP151	Yoga/Sports	0	0	2	0	-	-	-	-
		TOTAL	**14**	**2**	**11**	**18.5**	**260**	**340**	**600**	

Semester – III

Sr.	Cate-	Course	Course Name	Hours/week	C	Maximum marks	ESE

No.	gory	Code		L	T	P		Continuous Evaluation	End Sem Exam	Total	Duration (Hrs)
1	PCC	CCT201	Computer Architecture & Organization	4	0	0	4	40	60	100	3 Hrs
2	PCC	CCP202	Python Programming lab	0	0	4	2	25	25	50	-
3	PCC	CCT203	Data Structure & Algorithms	3	1	0	4	40	60	100	3 Hrs
4	PCC	CCP203	Data Structure & Algorithms Lab	0	0	2	1	25	25	50	-
5	PCC	CCT204	Computer Networks	3	1	0	4	40	60	100	3 Hrs
6	PCC	CCP204	Computer Networks Lab	0	0	2	1	25	25	50	-
7	BSC	MAT273	Mathematics for Cyber Security	2	1	0	3	40	60	100	3 Hrs
8	HSSM	HUT253	Business Communication	3	0	0	3	40	60	100	3 Hrs
			Total	**15**	**3**	**8**	**22**	**275**	**375**	**650**	

Semester – IV

Sr. No.	Cate-gory	Course Code	Course Name	Hours/week			Credits	Maximum marks			ESE Duration (Hrs)
				L	T	P		Continuous Evaluation	End Sem Exam	Total	
1.	BSC	MAT262	Probability and Queuing Theory	3	1	0	4	40	60	100	3 Hrs
2.	PCC	CCT205	Operating Systems	3	0	0	3	40	60	100	3 Hrs
3.	PCC	CCP205	Operating Systems Lab	0	0	2	1	25	25	50	-
4.	PCC	CCT206	Design & Analysis of Algorithms	3	0	0	3	40	60	100	3Hrs
5.	PCC	CCP206	Design & Analysis of Algorithms Lab	0	0	2	1	25	25	50	-
6.	PCC	CCT207	Theory of Computation	3	0	0	3	40	60	100	3 Hrs
7.	PCC	CCT208	Cryptography	3	0	0	3	40	60	100	3 Hrs
8.	PCC	CCP208	Cryptography lab	0	0	2	1	25	25	50	-
9.	OEC		Open Elective-I/ MOOC	3	0	0	3	40	60	100	3 Hrs
10.	BSC	CHT252	Environmental Sciences	2	-	-	0	-	-	-	-
			TOTAL	**20**	**1**	**6**	**22**	**315**	**435**	**750**	

Course Code	OPEN ELECTIVE – I
CCT299	Introduction to Network and Cryptography

Semester – V

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	PCC	CCT301	Software Engineering and Project Management	3	0	0	3	40	60	100	3 Hrs
2	PCC	CCP301	Software Engineering and Project Management Lab	0	0	2	1	25	25	50	-
3	PCC	CCT302	Computer Security	3	1	0	4	40	60	100	3 Hrs
4	PCC	CCP302	Computer Security Lab	0	0	2	1	25	25	50	-
5	PCC	CCT303	Artificial Intelligence & Cyber Security	3	0	0	3	40	60	100	3 Hrs
6	PEC	CCT304	Elective-I	3	0	0	3	40	60	100	3 Hrs
7	OEC	CCT398	Open Elective-II	3	0	0	3	40	60	100	3 Hrs
8	PCC	CCP303	Artificial Intelligence & Cyber Security lab	0	0	2	1	25	25	50	3 Hrs
9	MC	HUT353	Indian Traditional Knowledge	2	-	-	0	-	-	-	-
10	PR	CCP305	Mini Project -1	-	-	4	2	25	25	50	-
			TOTAL	**17**	**1**	**10**	**21**	**275**	**375**	**650**	

Course Code	ELECTIVE – I
CCT304-1	Basics of Ethical hacking
CCT304-2	Network & Web Security, Firewalls & VPNs
CCT304-3	Security Policies and implementation

Course Code	Open Elective II
CCT398	Basics of Ethical Hacking

Semester – VI

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	PCC	CCT306	Introduction to Cloud Security	3	0	0	3	40	60	100	3 Hrs
2	PCC	CCP306	Introduction to Cloud Security Lab	0	0	2	1	25	25	50	-
3	PCC	CCT307	Database Management System	3	0	0	3	40	60	100	3 Hrs
4	PCC	CCP307	Database Management System Lab	0	0	2	1	25	25	50	-
5	PCC	CCT308	Compiler Design	3	0	0	3	40	60	100	3 Hrs
6	PCC	CCP308	Compiler Design Lab	0	0	2	1	25	25	50	-
7	PEC	CCT309	Elective-II	3	0	0	3	40	60	100	3 Hrs
8	PEC	CCT310	Elective-III	3	0	0	3	40	60	100	3 Hrs
9	OEC	CCT399	Open Elective-III	3	0	0	3	40	60	100	3 Hrs
10	PR	CCP311	Mini Project-2	0	0	4	2	25	25	50	-
			TOTAL	**18**	**0**	**10**	**23**	**340**	**460**	**800**	

Course Code	ELECTIVE – II	Course Code	ELECTIVE – III
CCT309-1	Wireless & Mobile Device Security	CCT310-1	Managing Risk in Information Systems
CCT309-2	Incident Handling & Response	CCT310-2	IOT Security
CCT309-3	Security Strategies in Windows & Linux	CCT310-3	Application Security
CCT309-4	Security in Distributed Computing	CCT310-4	Threat and Malware Analysis

Course Code	OPEN ELECTIVE III
CCT399	Managing Riskin Information Systems

Semester – VII

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	PEC	CCT401	Elective-IV	3	0	0	3	40	60	100	3 Hrs
2	PEC	CCP401	Elective-IV Lab	0	0	2	1	25	25	50	-
3	PEC	CCT402	Elective-V	3	0	0	3	40	60	100	3 Hrs
4	PEC	CCP402	Elective-V Lab	0	0	2	1	25	25	50	-
5	OEC	CCT498	Open Elective-IV	3	0	0	3	40	60	100	3 Hrs
6	BSC	IDT452	Bio-informatics	2	0	0	2	20	30	50	1.5hr
7	PCC	CCT403	Secure Coding	2	1	0	3	40	60	100	3 Hrs
8	PR	CCP404	Project Phase – I	0	0	12	6	50	50	100	-
Total				**13**	**1**	**16**	**22**	**280**	**370**	**650**	

OR

Semester VIII (6 Months Full Semester Internship)											
Sr. No.	Category	Course code	Course name	Hours/week			Credit	Maximum marks			ESE Duration (Hrs)
				L	T	P		Continuous evaluation	End Sem Exam	Total	
1	PEC	CCT401	Elective - IV	3	0	0	3	40	60	100	3 Hrs
2	PEC	CCP401	Elective-IV Lab	0	0	2	1	25	25	50	-
3	PEC	CCT402	Elective-V	3	0	0	3	40	60	100	3 Hrs
4	PEC	CCP402	Elective-V Lab	0	0	2	1	25	25	50	-
5	BSC	IDT452	Bio-informatics	2	0	0	2	20	30	50	1.5hr
6	PR	CCP405	Industry Internship (one Semester)	0	0	12	12	100	100	200	-
Total				**8**	**0**	**16**	**22**			**550**	

OR

Semester-VII (One Year Internship)											
Sr. No.	Category	Course code	Course name	Hours/week			Credit	Maximum marks			ESE Duration (Hrs)
				L	T	P		Continuous evaluation	End Sem Exam	Total	
1	PEC	CCT401	Elective - IV	3	0	0	3	40	60	100	3 Hrs
2	PEC	CCP401	Elective-IV Lab	0	0	2	1	25	25	50	-
3	PEC	CCT402	Elective-V	3	0	0	3	40	60	100	3 Hrs
4	PEC	CCP402	Elective-V Lab	0	0	2	1	25	25	50	-
5	BSC	IDT452	Bio-informatics	2	0	0	2	20	30	50	1.5hr
6	PR	CCP408	Industry Internship	0	0	24	24	200	200	400	-
Total				**8**	**0**	**28**	**34**			**750**	

Course Code	ELECTIVE – IV	Course Code	ELECTIVE- V
CCT401-1	Database & Email Forensics	CCT402-1	Network Security Administration
CCT401-2	Auditing IT Infrastructure for Compliance	CCT402-2	Cyber Law & Legal Issues in Cyber Security
CCT401-3	Blockchain Security	CCT402-3	Privacy Engineering

Course Code	OPEN ELECTIVE IV
CCT498	Enterprise Architecture and Components (Security by Design)

Semester – VIII

Sr. No.	Cate-gory	Course code	Course name	Hours/week			Credits	Maximum marks			ESE Duration (Hrs)
				L	T	P		Continuous evaluation	End Sem Exam	Total	
1	PEC	CCT405	Elective VI	3	0	0	3	40	60	100	3 Hrs
2	PEC	CCT406	Elective VII	3	0	0	3	40	60	100	3 Hrs
3	PR	CCP407	Project Phase – 2	0	0	12	6	50	50	100	-
			Total	**6**	**0**	**12**		**130**	**170**	**300**	
OR											
1	PR	CCP408	Industry Internship (one Semester)	0	0	12	12	150	150	300	-
			Total	**0**	**0**	**0**	**12**	**150**	**150**	**300**	

Course Code	ELECTIVE – VI	Course Code	ELECTIVE – VII
CCT405-1	Vulnerability Assessment and Penetration Testing	CCT406-1	Mobile Application Security Testing
CCT405-2	Database Security	CCT406-2	Executive Governance and Management in IT Security
CCT405-3	Disaster Recovery & business continuity management	CCT406-3	Security in Social Networks
CCT405-4	Testing Cyber Crime Investigation and Digital Forensics	CCT406-4	Security of Embedded Systems

Honors and Minor Scheme

Honors Scheme

Sr. No.	Sem	Course Code	Course Title	Hrs/ Week			Credits	Maximum Marks			ESE Duration
				L	T	P		CA	ESE	Total	
1	III	CSTH303	Information and Cyber Security	3	0	0	0	40	60	100	3
2	IV	CSTH403	Cyber Security Auditing	3	0	0	0	40	60	100	3
3	V	CSTH503	Cyber Forensics: Threats, Vulnerability, Malware	4	0	0	0	40	60	100	3
4	VI	CSTH603	Security Strategies in Windows and Linux	4	0	0	0	40	60	100	3
5	VII	CSPH703	Project	0	0	8	4	50	50	100	-

Note:

1. Students can opt for MOOC courses as per list provided by the Department at the start of session.
2. Selection, Completion, Examination process of MOOC course to be done during VIII sem duration only.

Minor Scheme

Sr. No.	Sem	Course Code	Course Title	Hrs/ Week			Credits	Maximum Marks			ESE Duration
				L	T	P		CA	ESE	Total	
1.	III	CCTM301	Introduction to Cyber Security	3	0	0	3	40	60	100	3 Hrs
2	IV	CCTM401	Cryptography	3	0	0	3	40	60	100	3 Hrs
3.	V	CCTM501	Network Security Fundamentals	4	0	0	4	40	60	100	3 Hrs
4.	VI	CCTM601	Basics of Ethical Hacking	4	0	0	4	40	60	100	3 Hrs
5.	VII	CCTM701	Digital Forensics	0	0	8	4	40	60	100	3 Hrs

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

Course Code: CHT152 **Course: Chemistry**

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

Course Outcomes:

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

- Predict the properties and interactions of chemical substances by understanding their composition at the atomic level. [**CO for Unit – 1**]
- Conversant in applying unique properties of nano-materials to solve challenges in our life. [**CO for Unit – 2**]
- Explain the differences in the mechanical behavior of engineering materials based upon bond type, structure, composition, and processing. [**CO for Unit – 3**]
- Study chemical kinetics using concepts of computational chemistry. [**CO for Unit – 4**]
- Discuss how spectroscopic methods are used for qualitative and quantitative analyses. [**CO for Unit – 5**]
- Analyse impurities present in the water and suggest the methodology for its removal. [**CO for Unit – 6**]

Syllabus:

Unit 1: Solid State Chemistry (7 Hours)

Bondings in atoms: Primary bonding: ionic, covalent, metallic. Secondary bonding: dipole-dipole, induced dipole-induced dipole, London dispersion/van der Waals, hydrogen. Shapes of molecules: hybridization, LCAO-MO, VSEPR theory.

Electronic material: Band theory: metals, insulators, and semiconductors. Band gaps, doping. Silicon wafer production.

Unit 2: Nano-material-I(7 Hours)

Basics of Nanochemistry: Defination of Nano, Scientific revolution-Atomic Structure and atomic size, emergence and challengs of nanoscience and nanotechnology, carbon age-new form of carbon (CNT to Graphene), One dimensional, Two dimensional and Three dimensional nanostructured materials, mechanical-physical-chemical properties.

Application of Nanomaterial: Molecular electronics and nanoelectronics, Nanotechnology for waste reduction and improved energy efficiency, Carbon Nanotubes for energy storage, Hydrogen Storage in Carbon Nanotubes, nanotechnology based water treatment strategies.

Unit 3: Advanced Materials: (7 hours)

Composite materials: Introduction, Classification: Polymer Matrix Composites, Metal Matrix Composites, Ceramic Matrix Composites, Carbon–Carbon Composites, Fiber-Reinforced Composites and Applications.

Reinforcements: Fibres- Glass, Kevlar, Carbon, Silicon Carbide, And Born Carbide Fibres.

Industrial Polymer: Thermoplastics, Thermosetting Plastics, Polymers used in electronic industries, Piezo and pyroelectric polymers, Polymers in optical media data storagedevices.

Unit 4: Computational Chemistry [6 Hours]

Rate of the reaction, Order and Molecularity of the reaction, Rate expression for Zero Order, First Order and Second Order Reactions, Effect of the temperature, Use of Mathematica for determining rate of the reaction, etc.

Unit 5: Material Characterization using different Spectroscopic Techniques [7 Hours]

Fundamentals of spectroscopy, Infrared Spectroscopy, Electronic Spectrocopy, Nuclear Magnetic Resonance Spectroscopy.

Fundamentals of X-Ray Diffractions (XRD), X-Ray Fluorescence (XRF) spectroscopy.

Unit 6: Water Technology [8 Hours]

Impurities in natural water, hardness and alkalinity, Disadvantages of hardness i. e.sludge and scale formation, softening of water using lime-soda, zeolite and ion-exchange method, advantages and limitations of these water softening processes, Desalination of water using Reverse Osmosis.

Text Books:

1. J. Michael Hollas, Modern Spectroscopy, Fourth Edition, John Wiley and Sons, 2004.
2. William Kemp, Organic Spectroscopy, Third Edition, Palgrave Publication, 1991.
3. Bradley D. Fahlman, Materials Chemistry, Third Edition, Springer Nature, 2018.
4. Brian W. Pfennig, Principles of Inorganic Chemistry, John Wiley and Sons, 2015.
5. Steven S. Zumdahl, Donald J. DeCoste, Chemical Principles,Eighth Edition, Cengage Learning, 2017.
6. Catherine E. Housecroft and Edwin C. Constable, Chemistry: An Introduction to Organic, Inorganic and Physical Chemistry, Third Edition, Pearson Education Limited, 2006.
7. Michael J. Moran and Howard N. Shapiro, Fundamentals of Engineering Thermodynamics, Fifth Edition, John Wiley and Sons, 2006.
8. Donald L. Pavia, Gary M. Lampman, George S. Kriz, and James R. Vyvyan, Introduction to Spectroscopy, Fifth Edition, Cengage Learning, 2009.
9. C. N. R. Rao, A. Muller and A. K. Cheetham, The Chemistry of Nanomaterials: Synthesis, Properties and Applications, Wiley-VCH, 2004.
10. P. C. Jain and Monica Jain, Engineering Chemistry, Dhanpat Rai Publication.
11. S. S. Dara, A Textbook ofEngineering Chemistry, S. Chand Publications.
12. J. D. Lee, Concise Inorganic Chemistry, Fourth Edition, Chapman and Hall Publications.

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

Course Code: CHP152	**Course: Chemistry Lab**
L: 0 Hrs, T: 0 Hr, P: 3 Hr, Per Week	**Total Credits: 1.5**

Course Outcomes:

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:

- Estimate the amount of different impurities in water/waste water samples.
- Estimate rate constants of reactions and order of the reaction from concentration of reactants/products as a function of time and to validate adsorption isotherms.
- Measure molecular/system properties such as surface tension, viscosity of aqueous or other industrially important liquids/mixtures etc.
- Synthesize a polymer or drug molecule or nano-material.
- Use principle of spectroscopic techniques for structural determination.

List of Experiments: [Any Eight from the List]

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

[2] To find out types of alkalinity and estimation of their extent in the water sample.

[3] Estimation of temporary, permanent and total hardness present in the water sample using complexometric titration method.

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

[5] Determination of rate of the reaction of hydrolysis of ethyl acetate at room temperature and analysis of experimental data using Computational Software.

[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] Synthesis of Nano-material/Polymer and its study.

[8] Determination of relative and kinematic viscosities of aqueous solutions of Poly-ethylene glycol (Polymeric Liquid) using Redwood Viscometer (type I or II) at different temperatures.

[9] To study effect of bondings of water molecules with electrolyte (NaCl/KCl) and non-electrolyte solute (Soap) in the solution through Surface Tension Determination.

[10] Study of ion-exchange column for removal of hardness in the water sample.

[11] Demonstrations of organic spectral techniques: IR, NMR.

[12] Demonstration of in-organic spectral techniques: XRD, XRF.

Text 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) A. 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.

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

Course Code: MAT152		**Course:**	**Differential Equation, linear Algebra, Statistics & Probability**
L: 3 Hrs,	**T: 0 Hr, P: 0 Hr, Per Week**	**Total Credits: 3**	

Course Objective:

The objective of this course is to familiarize the prospective engineers with techniques inordinary differential equation, statistics, probability and Matrices. It aims to equip the students to deal with advanced level of mathematics and applications that would be essential for their disciplines.

Course Outcomes

On successful completion of the course, the students will learn:

1. The effective mathematical tools for the solutions of ordinary differential equations that model physical processes.
2. The essential tool of matrices in a comprehensive manner.
3. The ideas of probability and various discrete and continuous probability distributions and the basic ideas of statistics including measures of central tendency, correlation and regression.

Syllabus

Module 1:*First order ordinary differential equations*(7 hours)

Exact, linear and Bernoulli's equations, Euler's equations, Equations not of first degree: equations solvable for p, equations solvable for y, equations solvable for x and Clairaut's type.

Module 2:*Ordinary differential equations of higher orders* (8 hours)

Second order linear differential equations with constant and variable coefficients, method of variation of parameters, Cauchy-Euler equation.

Module 3:*Basic Statistics:* (7 hours)

Curve fitting by the method of least squares- fitting of straight lines, second degree parabolas and more general curves, correlation and regression – Rank correlation, Multiple regression and correlation.

Module 4: **Basic Probability:** (8 hours)

Probability spaces, conditional probability, independence; Discrete random variables, Binomial distribution, Poisson distribution, Normal distribution. Relation between binomial, Poisson and Normal distributions.

Module 5: Matrices (10 hours**)**

Algebra of matrices, Inverse and rank of a matrix, rank-nullity theorem; System of linearequations; Symmetric, skew-symmetric and orthogonal matrices; Eigenvalues and eigenvectors; Diagonalization of matrices; Cayley-Hamilton Theorem, Orthogonal transformation andquadratic to canonical forms.

Topics for Self Learning :

Application of Differential Equations.

Textbooks/References:

1. Erwin Kreyszig, Advanced Engineering Mathematics, 9th Edition, John Wiley & Sons, 2006.
2. W. E. Boyce and R. C. DiPrima, Elementary Differential Equations and Boundary Value Problems, 9th Edition, Wiley India, 2009.
3. S. L. Ross, Differential Equations, 3rd Ed., Wiley India, 1984.
4. E. A. Coddington, An Introduction to Ordinary Differential Equations, Prentice Hall India, 1995.
5. E. L. Ince, Ordinary Differential Equations, Dover Publications, 1958.
6.B.S. Grewal, Higher Engineering Mathematics, Khanna Publishers, 35th Edition, 2000.
7.Theory and Problems of probability and statistics : 2nded :*J. R. Spiegal ,Schaum series*
8. A text book of Applied Mathematics Volume I & II, by P. N. Wartikar and J. N. Wartikar, Pune VidhyarthiGrihaPrakashan, Pune-411030 (India).
9.. S. Ross, A First Course in Probability, 6th Ed., Pearson Education India, 2002.

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

Course Code: CCT101	**Course: Programming for Problem Solving**
L: 4 Hrs, T: 0 Hr, P: 0 Hr, Per Week	**Total Credits: 4**

Course Outcomes :

On successful completion of course student will learn:

1. To formulate simple algorithms for arithmetic and logical problems, translate the algorithms to programs (in C language), test and execute the programs and correct syntax and logical errors.
2. To implement conditional branching, iteration and recursion, to decompose a problem into functions and synthesize a complete program using divide and conquer approach.
3. To use arrays, pointers, structures and I/O operations for the formulation of algorithms and programs.
4. To apply programming to solve matrix addition, multiplication problems and searching & sorting problems.

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,

Preprocessor 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. CSE (Cyber Security)

Course Code: CCP101	**Course: Programming for Problem Solving Lab**
L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week	**Total Credits: 1**

Course Outcomes:

On successful completion of course student will be able to:

1. Understand the fundamentals of C programming and choose the loops and decision making statements to solve and execute the given problem.
2. Implement different Operations on arrays also design functions to solve the given problem using C programming.
3. Understand pointers, structures, unions and apply them to develop programs.
4. Implement file Operations in C programming for a given application.

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

Course Code: IDT151	**Course:**	**Creativity, Innovation & Design Thinking**
L: 1 Hrs, T: 0 Hr, P: 0 Hr, Per Week	**Total Credits: 1**	

Course Outcomes

C1: Be familiar with processes and methods of creative problem solving
C2: Enhance their creative and innovative thinking skills
C3: Practice thinking creatively and innovative design and development

Detailed Topics

UNIT I. Introduction: Making a case for creativity, Creative thinking as a skill, Valuing diversity in thinking: Thinking preferences, Creativity styles, Creativity in problem solving

UNIT 2. Pattern Breaking: Thinking differently , Lateral thinking, Mind stimulation: games, brain-twisters and puzzles, Idea-collection processes, Brainstorming/Brainwriting, The SCAMPER methods, Metaphoric thinking, Outrageous thinking , Mapping thoughts, Other (new approaches)

UNIT 3. Using Math and Science, Systematic logical thinking, Using math concepts, Eight-Dimensional (8D) Approach to Ideation: Uniqueness, Dimensionality, Directionality, Consolidation, Segmentation, Modification, Similarity, Experimentation

UNIT4. Systematic Inventive Thinking: Systematic inventive thinking: The TRIZ methodology, Decision and Evaluation: Focused thinking framework, Six thinking hats , Ethical considerations

UNIT 5. Design for Innovation: Introduction to design for interaction, nine lessons for innovation, difference in creativity and innovation, Building blocks for innovation

UNIT 6.Intellectual Property: Introduction to intellectual property: Patents, Copyrights©, Trademarks ®, Trade Secret, Unfair Competition.

Reference Books and Text Book :

1. Creative Problem Solving for Managers - Tony Proctor - Routledge Taylor & Francis Group
2. 101 Activities for Teaching creativity and Problem Solving - By Arthur B Vangundy - Pfeiffer
3. H. S. Fogler and S.E. LeBlanc, Strategies for Creative Problem Solving, Prentice Hall
4. E. Lumsdaine and M. Lumsdaine, Creative Problem Solving, McGraw Hill,
5. J. Goldenberg and D. Mazursky, Creativity in product innovation. Cambridge University Press, 2002.

Course Assignments for internal continuous assessment of 20 Marks (NO T1 and T2)

- Brain teasers (aka Puzzle Busters, to be solved individually)
- Cartoon captions (small teams)
- TRIZ, a systematic ideation method, reading (individual)
- Book readings and discussions (small teams)
- Small teams presentations on innovation: (1) innovative individual, (2) innovative company, (3) innovative movie / game, (4) sustainable innovation, (5) innovation in business, (6) innovationin art, (7) innovation in architecture, (8) innovative nation, (9) innovation in science, and (10) innovation in engineering.
- Large groups hands-on projects
- Eight-dimensional (8D) ideation method examples
- Large teams videos

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

Course Code: CCT102	**Course: Computer Workshop**
L: 1 Hrs, T: 0 Hr, P: 0 Hr, Per Week	**Total Credits: 1**

Course Objectives

1. Understand the definition and principles of UI/UX Design in order to design with intention.
2. Achieve a deep understanding of the entire life-cycle of design—the process, purpose, and tools.
3. Learn the basics of HCI (human-computer interaction) and the psychology behind user decision-making.
4. Discover the industry-standard tools and specific project deliverables in UI/UX.
5. Explain why you made design decisions, through presentations of assignments and your personal portfolio.

Unit 1:

UI/UX Overview: Intro to UI/UX, Notion & Figma Setup, Design Thinking
User Research: How to identify stakeholders, Figma Basics, How to identify user needs

Unit 2:

User Journeys: Mapping the user journey, Figma Grayscales, Finding solutions & constraint cards
Grayscales & User Testing: UX Principles, Figma Prototype, Understanding user testing

Unit 3:

UI Principles: UI Principles, Color and Font
Style Guide: Components, Responsive Design

Course Outcomes

On successful completion of the course, students will be able to:
1. Understand basics of UI/UX
2. Find solutions and constraint cards.
3. Design responsive UI.

Text Books

1. UI/UX design for designer and developers: by Nathan Clark
2. User Story Mapping software for agile age [Paid subscription on yearly basis]
3. User story mapping by Jeff Patton, O'Reilly Publication

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

Course Code:CCP102	**Course: Computer Workshop Lab**
L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week	**Total Credits: 1**

Course Objectives

Throughout the course, students will be expected to learn Python Language basics to do the following:

1. Understand UI/UX basics and its use in software industry
2. Understand basic use cases of UI/UX.
3. Develop small utilities using UI/UX tools
4. Develop and integrate UI/UX with basic programs

Syllabus

Programs based on:

1. Illustration tool box
2. Storytelling and typography tools
3. UX writing and AR/VR tools
4. Voice technology tools
5. Motion Design, Animated graphics

Course Outcomes

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

1. Design UI/UX use cases using Illustration tool box
2. Design and use storytelling and typography for requirement specification.
3. Use UX writing, AR and VR models to develop interfaces for use cases
4. Develop small applications using voice technology, motion design, and animation.

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

Course Code: HUT151	**Course: English**
L: 2 Hrs, T: 0 Hr, P: 0 Hr, Per Week	**Total Credits: 2**

Course Objectives

The main objective of the subject is to enhance the employability skills of engineering students as well as Communication skills at work place. The sub-objectives are:

1. To develop vocabulary of students.
2. To orient students in basic writing skills.
3. To orient students in functional grammar.
4. To orient students in the process of effective writing.
5. To provide practice and improve students' oral communication skills.

Course Outcomes

1. Students will have good word power.
2. Students will acquire basic writing skills.
3. Students will understand functional grammar and its usage.
4. Students will organize and express their thoughts effectively through written communication.
5. Students will learn oral communication skills in order to handle themselves effectively in an interview and group discussion

SYLLABUS

1. Vocabulary Building

1.1. The concept of Word Formation
1.2. Root words from foreign languages and their use in English
1.3. Acquaintance with prefixes and suffixes from foreign languages in English to form derivatives
1.4. Synonyms, Antonyms and standard abbreviations

2. Basic Writing Skills

2.1 Sentence Structures
2.2 Use of phrases and clauses in sentences
2.3 Importance of proper punctuation
2.4 Creating coherence
2.5 Organizing principles of paragraphs in documents
2.6 Techniques for writing precisely

3. Identifying Common Errors in Writing

3.1 Subject-verb agreement
3.2 Noun-pronoun agreement
3.3 Misplaced modifiers

3.4 Articles
3.5 Redundancies
3.6 Cliches

4. Nature and Style of sensible Writing
4.1 Describing
4.2 Defining
4.3 Classifying
4.4 Providing examples or evidence

5. Writing Practices
5.1 Comprehension
5.2 Precis Writing
5.3 Essay Writing
5.4 Letter Writing
5.5 Email Writing

6. Oral Communication
(This unit involves interactive practice sessions in Language Lab)
• Listening Comprehension
• Pronunciation, Intonation, Stress and Rhythm
• Common Everyday Situations : Conversations and Dialogues
• Communication at Workplace
• Interviews
• Formal Presentations

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

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

Course Code: HUP151	**Course: English Lab**
L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week	**Total Credits: 1**

Course objective:

1. To enhance competency of communication in English among learners.

Course outcomes:

1. Students learn presentation and public speaking skills
2. Students learn to practice effective strategies for Personal Interview and Group Discussions
3. Students learn and effectively apply language skills – listening, speaking, reading and writing

List of Practical (2 hours each for each batch) based on unit 6 (oral communication).

1. Common Everyday Situations: Conversations and Dialogues
2. Pronunciation, Intonation, Stress, and Rhythm
3. Formal Presentations: Orientation
4. Formal Presentations: Practice Session
5. Interviews: Orientation
6. Interviews: Practice Session
7. Communication at Workplace: Group Discussion- Orientation
8. Communication at Workplace: Practice Session

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

Course Code: PHT154	**Course: Introduction to Quantum Computing**
L: 3 Hrs, T: 1 Hr, P: 2 Hr, Per Week	**Total Credits: 4**

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 learn,

1. Basics of complex vector spaces
2. Quantum mechanics as applied in Quantum computing
3. Architecture and algorithms
4. Fundamentals of Quantum computations

Module 1: Complex Vector Spaces

Algebra and Geometry of Complex numbers, Real and Complex Vector Spaces, definitions, properties, basis and dimensions, Generalization to n-dimensional space

Module 2: Linear Algebra

Inner products, Hilbert Spaces, Eigenvalues and Eigenvectors, Hermitian and Unitary Matrices, Tensor Product, Applications of linear algebra in computer graphics, Geometric transforms, Positioning the virtual camera

Module 3: Basic Quantum Theory

Introduction to Quantum mechanics, Schrodinger's time dependent equation, Wave nature of Particles, expectation values, variance, standard deviation, probability density, Stationary states, Infinite square well, Uncertainty principle

Module 4: Classical and Quantum Systems

Deterministic and Probabilistic Systems, Quantum Systems, Observations, Quantum measurement principles, Stochastic matrices, Probabilistic double slit experiment with photons, Entangled states, Quantum clocks

Module 5: Architecture

Bits and Qubits, Classical Gates, Reversible Gates, Quantum Gates, Toffoli and Fradkin Gates, Bloch Sphere, Deusch Gate, No-cloning theorem, Applications in Cryptography and Quantum teleportation

Module 6: Quantum algorithms

Deutsch's algorithm, The Deutsch-Jozsa algorithm, Simon's periodicity algorithm, Grover's search algorithm, Shor's factoring algorithm, Quantum Fourier Transform

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

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

Course Code: PHP154	**Course: Introduction to Quantum Computing Lab**
L: 0 Hrs, T: 0 Hr, P: 3 Hr, Per Week	**Total Credits: 1.5**

Course Outcomes:

The physics laboratory will consist of experiments and programming exercises illustrating the principles of physics relevant to the study of computer science and engineering. During the training in the Physics Lab, the students will be able,

1. To develop skills for experimental verification of physics laws
2. To analyze the results using the mathematical tools
3. To learn the computational techniques
4. To write the project reports

The laboratory will consist of general physics experiments and computational physics practicals

General Physics:

1. Measuring scales and error estimation
2. Verification of Ohm's law and linear least square fitting method
3. Verification of Newton's law of cooling
4. Simple harmonic motion
5. Magnetic flux measurement using the graphical method of integration
6. Measurement, analysis and fitting of non-linear IV characteristics of PN junction diode

Python based Computational Physics:

1. Introduction to Python programming, Environment, Syntax and Data Structures
2. Linear least square fit method for data analysis
3. Plotting of Plank's function and verification of Stefan's law
4. Finding inverse, norm and inner products, rank of a matrix
5. Introduction to quantum computing packages (GitHub repository)
6. Implementation of Deutsch-Josza algorithm using Cirq library

Project

A python based project on the applications of linear algebra, quantum mechanics or quantum computing to solve science and engineering problems.

Reference Books

1. Lab manual prepared by Physics Department, RCOEM, Nagpur
2. Introduction to Python for science and engineering, David Pine, CRC Press 2018

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

Course Code:MAT151	**Course: Calculus**
L: 3 Hrs, T: 1 Hr, P: 0 Hr, Per Week	**Total Credits: 4**

Course Objective:

The objective of this course is to familiarize the prospective engineers with techniques inCalculus and multivariate analysis. 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, the students will learn:

1. The fallouts of Mean Valve Theorems that is fundamental to application of analysis to Engineering problems , to deal with functions of several variables that are essential in most branches of engineering.

2. Basics of improper integrals ,Beta and Gamma functions , Curve Tracing , tool of power series and Fourier series for learning advanced Engineering Mathematics.

3. Multivariable Integral Calculus and Vector Calculus and their applications to Engineering problems.

Syllabus

Module 1: ***Calculus:*** (7 hours)

Rolle's theorem, Mean value theorems, Taylor's and Maclaurin series expansions; Indeterminate forms and L'Hospital's rule; radius of curvature (Cartesian form), evolutes and involutes

Module 2:***Multivariable Calculus (Differentiation)*** (8 hours)

Limit, continuity and partial derivatives, Eulers Theorem, chain rule , total derivative, Jacobians, total
derivative, Maxima, minima and saddle points; Method of Lagrange multipliers.

Module 3 ***Calculus:*** (6 hours)

Evaluation of definite and improper integrals; Beta and Gamma functions and their properties; Tracing of curves(Cartesian form)

Module 4:***Sequences and series:*** (7 hours)

Convergence of sequence and series, tests for convergence, power series, Fourier series: Half range
sine and cosine series, Parseval's theorem.

Module 5: ***Multivariable Calculus (Integration)*** (7 hours)

Multiple Integration: double and triple integrals (Cartesian and polar), change of order of integration in double integrals, Change of variables (Cartesian to polar), Applications: areas and volumes by (double integration) Center of mass and Gravity (constant and variable densities).

Module 6 : Vector Calculus(7 hours)

Vector Differentiation, Directional derivatives, total derivative , Gradient, curl and divergence. Vector integration , Theorems of Green, Gauss and Stokes.

Topics for self learning

Maxima and minima for function of one variable, Geometrical interpretation of Partial Differentiation (Tangent plane and Normal line) , Applications of definite integrals to evaluate perimeter, area, surface areas and volumes of revolutions.

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. A text book of Applied Mathematics Volume I & II, by P. N. Wartikar and J. N. Wartikar, Pune VidhyarthiGrihaPrakashan, Pune-411030 (India).

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

Course Code:MAP151	**Course: Computational Mathematics lab**
L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week	**Total Credits: 1**

Course Outcomes

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. At the end of the Course the students will learn to:

1. Develop skills to impart practical knowledge in real time.
2. Understand principle, concept, working and application of areas in mathematics and compare the results obtained with theoretical calculations.
3. Understand basics of mathematics, and report the results obtained through proper programming.

The Lab turns will be utilized for performing the experiments based on the following list:

1. Calculus
2. Ordinary Differential Equations
3. Statistics
4. Linear Algebra

Suggested References:

1. Computational Mathematics Lab Manual written by the Teaching Faculty of Mathematics Department, RCOEM.

A minimum of 8 experiments to be performed based on the above list.

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

Course Code:CCT103	**Course: Digital Electronics**
L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week	**Total Credits: 3**

Course Outcomes:

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

1. Understanding of various optimization techniques used to minimize and design digital circuits.
2. Analyze and design various combinational logic circuits.
3. Analyze and design various sequential circuits.
4. Design different microprocessor based components of computer system using combinational and sequential circuits.

Course Contents:

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 upto five variable. 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.

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, 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.

UNIT-V- **Programmable logic Design**

Memory & Programmable logic Devices: RAM, Array of RAM IC's, Read only Memory, PLA, PAL, Flash Memories

UNIT-VI- **Fundamentals of Microprocessor**

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

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. A. 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 II, B. TECH. CSE (Cyber Security)

Course Code:CCP103	**Course: Digital Electronics Lab**
L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week	**Total 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 above theory syllabus

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

Course Code:CCT104	**Course: Object Oriented Programming**
L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week	**Total 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, multithreading and streams.

SYLLABUS

UNIT I

Features of Object Oriented Programming languages, Abstraction, Encapsulation, Inheritance, polymorphism and late binding. Concept of a class, Access control of members of a class, instantiating a class, constructor and method overloading.

UNIT II

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, creating packages, importing packages, static and non-static members, Lambda Expressions Introduction, Block, Passing Lambda expression as Argument.

UNIT III

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 IV

Generics, generic class with two type parameter, bounded generics. Collection classes: Arraylist, LinkedList, Hashset, Treeset.

UNIT V

Multithreading: Java Thread models, creating thread using runnable interface and extending Thread, thread priorities, Thread Synchronization, InterThread communications.

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 demonstrate

1. Understand the principles of object-oriented programming; create classes, instantiate objects and invoke methods.

2. Understand concept of generics and implement collection classes. Use exception handling mechanism.

3. Efficiently work with streams, use multithreading for solving classic synchronization problems. Perform java database connectivity and execute basic SQL commands.

4. Understand 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. Cay S. Horstmann and Gary Cornell; Core JAVA Volume-II Advanced Features; Eighth Edition; Prentice Hall, Sun Microsystems Press 2008.

2. Herbert Schildt and Dale Skrien; Java Fundamentals A Comprehensive Introduction; Tata McGraw- Hill Education Private Ltd 2013.

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

Course Code:CCP104	**Course: Object Oriented Programming Lab**
L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week	**Total 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 and JDBC.

SYLLABUS

Experiments based on above Syllabus.

Course Outcomes:

On completion of the course the student will be able to

1. Design solution to problems using concepts of object oriented programming like classes, objects, inheritance with proper exception handling.

2. Use collection classes, generic classes to design programs and perform database connectivity.

3. Implement programs based on streams and multithreading.

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

Course Code:HUT152	**Course: Constitution of India**
L: 2 Hrs, T: 0 Hr, P: 0 Hr, Per Week	**Total Credits: 0**

Course outcome

1. Students will understand the role of constitution in democratic India
2. Students will be responsible students by knowing their fundamental rights and duties
3. Students will develop better understanding of democratic functions of the government of India
4. Students will form better understanding of system of governance for effective participation

Course content

1. Meaning of the constitution law and constitutionalism
2. Historical perspective of the Constitution of India
3. Salient features and characteristics of the Constitution of India
4. Scheme of the Fundamental Rights
5. The scheme of the Fundamental Duties and its legal status
6. The Directive Principles of State Policy – Its importance and implementation
7. Federal structure and distribution of legislative and financial powers between the Union and the States
8. Parliamentary Form of Government in India – The constitution powers and status of the President of India
9. Union Executive: structure, functions
10. Judiciary: Structure, role with special reference to PIL, writ petitions, strengthening of democracy & social justice
11. Amendment of the Constitutional Powers and Procedure
12. Emergency Provisions: National Emergency, President Rule, Financial Emergency
13. Local Self Government – Constitutional Scheme in India
14. Provisions of civil services: Characteristics, functions, merits and demerits
15. Democratic principles in industry

Book

1. Durga Das Basu “An Introduction to Constitution of India” 22nd Edition, LexisNexis

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

Course Code:PEP151	**Course: Yoga/Sports**
L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week	**Total Credits: 0**

Course outcome

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

1. Understand fundamental skills and basic rules of games offered by the Physical Education Department of RCOEM.
2. Obtained health related physical fitness.
3. Develop body-mind co-ordination through games and yoga.
4. Changed sedentary life styles towards active living.

Brief Objectives of Sports/Yoga Practical Classes:

It has long been proven that a healthy body leads to a healthy mind. With a strong belief in this, Physical Education Department at RCOEM will conduct Sports/Yoga Classes with the objective of maintaining health, fitness and wellness of students as well as create awareness about need for good health and physical fitness. The objective would also be to make the all-round development with team spirit, social values as well as to identify and develop leadership qualities in students through various sports activities. Sports activities would also be conducted with the objective to provide better interaction and recreation to the students which is an important neutralizer for stress. Additionally, the objective would be to evaluate the health related fitness of students so asto recommend and conduct specific Yoga and Sports activities. The emphasis is on participation, with healthy competition.

Programme Outline:

 Sports :

1. Introduction to sports, offered by the department.
2. Health and safety issues related to sports; knowledge, recognition and ability to deal with injuries and illness associated with sports.
3. Practicing the fundamental skills and bringing awareness of basic rules and regulations.
4. Conduction of small recreational games and activities.

 Yoga : Includes various sitting, standing and lying Asanas, Suryanamaskars and Pranayamas.

 Physical Efficiency Tests : This includes 6 health related physical fitness tests.

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

Course Code:	**CCT201**	**Course Name:**	**Computer Architecture & Organization**	
L: 4 Hrs	**T: 0 Hrs**	**P: 0 Hrs**	**Per Week**	**Total Credits: 4**

Course Objectives:

1. To impart to students the basic structure of Computers and different data representation techniques
2. To familiarize students with designing of memory hierarchy and control unit
3. To make students aware of I/O organization

Syllabus:

Unit I : Basic Structure Of Computers : Functional units of computer. Instructions set architecture of a CPU Instruction sequencing, Addressing modes, instruction set classification, subroutine & parameter passing, expanding opcode

Unit II : Basic Processing Unit : Bus architecture, Execution of a Complete Instruction, sequencing of control signals, Hardwired control, Micro-programmed Control.

Unit III : Data Representation : signed number representations and their operations, Computer arithmetic – integer addition and subtraction, design of Fast Adders, Multiplication- shift and add, booth's Algorithm, bit-pair recoding, Integer Division-restoring and non-restoring division. Floating point numbers-representation, arithmetic, guard bits and rounding.

Unit IV: Memory System Design : Semiconductor RAM memories, ROM, higher order memory design, multi-module memories, Secondary storage – Magnetic disk, Optical disk.

Unit V : Memory Organization : Memory interleaving, concept of hierarchical memory, cache memory, cache size vs. block size, mapping functions, replacement algorithms, write policy, Virtual Memory. Pipelining : Basic concepts of pipelining, throughput and speedup.

Unit VI : Input/Output Organization : I/O mapped I/O and memory mapped I/O, interrupts and interrupt handling mechanisms, vectored interrupts, synchronous vs. asynchronous data transfer, Direct Memory Access

Course Outcomes:

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

1. Understand the basic components of a computer, including CPU, memories, and input/output, and their organization.
2. Understand the cost performance tradeoff in designing memory hierarchy and instruction sets.
3. Understand the execution of complete instruction and design of control unit.
4. Perform mathematical operations on arithmetic and floating point numbers.

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.

Reference Books:

1. M Mano; Computer System and Architecture; PHI publication; 1993.

2. A.S.Tanenbaum; Structured Computer Organization; Prentice Hall of India Ltd.

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

Course Code:	**CCP202**	**Course Name:**	**Python Programming Lab**		
L: 0 Hrs	**T: 0 Hrs**	**P: 4 Hrs**	**Per Week**	**Total Credits:**	**2**

Course Objectives:

The course focuses on developing the python programming skills to do a variety of programming tasks where the students are encouraged to develop application using python. Apart from the basic constructs of python programming, data structures, object oriented programming, exception handling is covered. The course also targets the coverage of important modules and libraries available in python.

Syllabus:

- Arithmetic, logical operations, Control statements, Functions, Class and OOM
- String, List, Array, Tuples, Dictionary, Set
- Collections, Files, Exception Handling
- Module, Packages, Library
- Plotting, Web scrapping, Multimedia services
- Matplotlib, Pandas, Request, Numpy
- Beautifil soup, Pyglet, Scrapy, PyGame
- Pywin32, PyGTK, Geopy

Course Outcomes:

On completion of the course the student will be able to

1) Understand the usage of various instructions, functions, modules, packages and libraries in python programming
2) Code, debug and execute python program to solve given problem
3) Select an appropriate instruction, function, module and library for writing an efficient and correct code in Python
4) Design a small python-based software to solve a numerical, multimedia, games,location, web-based problems.

Reference Books:

1. Allen B. Downey , " Think Python: How to Think Like a Computer Scientist", Second Edition, Updated for Python 3, Shroff/O'Reilly Publishers, 2016.

2. Shroff “Learning Python: Powerful Object-Oriented Programming; Fifth edition, 2013.
3. David M.Baezly “Python Essential Reference”. Addison-Wesley Professional; Fourth Edition, 2009.
4. David M. Baezly “Python Cookbook” O’Reilly Media; Third edition, 2013.

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

Course Code:	**CCT203**	**Course Name:**	**Data Structure & Algorithms**		
L: 3 Hrs	**T: 1 Hrs**	**P: 0 Hrs**	**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:	**CCP203**	**Course Name:**	**Data Structure & Algorithms 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:	**CCT204**	**Course Name:**	**Computer Networks**		
L: 3 Hrs	**T: 1 Hrs**	**P: 0 Hrs**	**Per Week**	**Total Credits:**	**4**

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:	**CCP204**	**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 CCT204 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 V, B. TECH. CSE (Cyber Security)

Course Code:	**MAT 273**	**Course:**	**Mathematics for Cyber Security**
L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week		**Total Credits:**	**3**

Course Objectives

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.

Syllabus

Module 1: (10 Lectures)
Introduction – Divisibility, Greatest common divisor, Prime numbers, Fundamental theorem of arithmetic, Fermat numbers, Euclidean algorithm, Fermat's theorem, Euler totient function, Euler's theorem.

Module 2: (10 Lectures)
Congruences: Definition , Basic properties of congruences ,Chinese remainder theorem, Quadratic Residues.

Module 3: (10 Lectures)
Euler's formula and roots modulo pq with its application, Discrete Logarithms and the Discrete Log Problem, Pollard's ρ-Algorithm, Primality Testing-Sieving Methods, Fermat's Primality Testing, Pseudoprimes and Probabilistic Primality Testing.

Module 4: (10 Lectures)
Groups, Subgroup, Cyclic groups, group homomorphisms, Permutation groups, Cosets, Field , Finite field, Factorization of polynomials over a field, Elliptic curves, Elliptic curves over finite field.

Course Outcomes

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

1. Understand concept of number Theory and its application to Cyber Security.
2. Understand the ideas of group, ring and an integral domain and apply these structures in coding and cryptography.
3. Understand the significance of elliptic curves and finite fields to the modern world and the internet.

Text Books

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.

Reference Books

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:	**HUT253**	**Course:**	**Business Communication**
L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week		**Total Credits:**	**3**

Course Objectives

The course aims to develop the skills of students of writing effective business documents and applying effective strategies of verbal business communication

Syllabus

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

CO1: Understand the fundamentals and objectives of business communication, and role of audience in effective communication.
CO2: Develop technical writing skills and produce effective workplace documents.
CO3: Apply the rules of English grammar in writing.
CO4: Develop skills to enhance visual appeal of documents.
CO5: Evaluate and apply strategies for effective oral communication for professional needs.

Course Outcomes

Unit1: Fundamentals of Business Communication:
Definition of communication and business communication, Objectives of Business Communication, Audience recognition, Barriers of Communication, Product Promotion, Usage of Social Media, Negotiation Skills, Persuasive Communication, PAC concept

Unit 2: Technical Writing:
Process of Technical Writing, Letters: Job application, Job Description and Resume, enquiry, complaint, order, follow-up, cover/transmittal letters, Sales Letters, and e-mails. Other Forms of Technical Writing: Organizational announcements, Notices, Agenda, Minutes of Meeting, Memorandums.

Unit 3: Grammar for Writing:
Punctuations, Mechanics, Active/ Passive, Transformation of Sentences, Subject-Verb Agreement, Articles, Prepositions

Unit 4: Business Reports:
Basic formats and types - Annual, Progress, Project (Project Charter, Project Timeline), Market Search, Sales, Feasibility/Recommendation, Case Study evaluation.

Unit 5: Preparation of Documents:
Visual Appeal: Document Design, Graphics, Tables, User Manuals, Brochures, Fliers

Unit 6: Effective Oral Communication:
Non- Verbal Communication, Presentation and Public speaking, Group Discussion

Text Books

1. Sharon Gerson, Steven Gerson, "*Technical Communication: Process and Product*", 2018, Pearson
2. Sanjay Kumar, Pushpa Lata, *Communication Skills*, 2nd Edition, Oxford Publication, 2018.
3. Shalini Verma, *Business Communication,* Vikas Publishing House Pvt. Ltd., 2015.
4. P.D. Chaturvedi and Mukesh Chaturvedi, *Fundamentals of Business Communication*, Pearson Publications, 2012.
5. William Strunk Jr. and E.B. White *The Elements of Style,* Allyn & Bacon 'A Pearson Education Company', 2000.

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

Course Code:	**MAT 262**	**Course:**	**Probability & Queuing Theory**
L: 4 Hrs, T: 0 Hr, P: 0 Hr, Per Week		**Total Credits:**	**4**

Course Objectives

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: (10 Lectures)
Review of Discrete and continuous random variable, joint probability function, Marginal and Conditional distribution, Mean , Variance, Covariance of two dimensional random variables.

Module 2:(12 Lectures)
Introduction to stochastic process, Poisson process, random walk, stationary process, transition probability matrix, transition diagram , Markov chain, birth and death process, limiting distributions.

Module 3: (12Lectures)
Modelling of queuing systems, queuing systems with losses, queuing systems allowing waiting time.

Module 4: (12 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), PollaczekKhintchine formula, Queues with unlimited service(M/M/∞).

Course Outcomes

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

1. Apply the concepts of multiple random variables to Engineering Problems.
2. Understand and compute quantitative metrics of performance for queuing systems

Apply and extend queuing models to analyze real world systems.

Text Books

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.

Reference Books

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.

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

Course Code:	**CCT205**	**Course Name:**	**Operating Systems**		
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:	**CCP205**	**Course Name:**	**Operating Systems 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 CCT205 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:	**CCT206**	**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 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.

Text Books:

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 - IV, B.TECH.. CSE (Cyber Security)

Course Code:	**CCP206**	**Course Name:**	**Design & Analysis of Algorithms Lab**	
L: 0 Hrs	**T: 0 Hrs**	**P: 2 Hrs**	**Per Week**	**Total Credits: 1**

Course Objectives:

1. Analyze the performance of algorithms.
2. Demonstrate a familiarity with major algorithms and data structures.
3. Apply important algorithmic design paradigms and methods of analysis.

Syllabus:

Experiment based on syllabus of Design and Analysis Algorithms (CCT206).

Course Outcomes:

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

1. Analyze greedy paradigm and implement greedy algorithms.
2. Analyze divide-and-conquer paradigm and synthesize divide-and-conquer algorithms.
3. Implement algorithms using Dynamic Approach and analyze it to determine its computational complexity.
4. Apply backtracking paradigm to realize real world problems.

Text Books:

1. Thomas H. Cormen et.al. “Introduction to Algorithms”, Prentice Hall of India.
2. Horowitz, Sahani, Rajsekharam, “Computer Algorithms”, Galgotia Publications Pvt. Ltd.

Reference Books:

1. Brassard, Bratley, “Fundamentals of Algorithms”, Prentice Hall
2. Algorithms -- A Creative Approach, 3RD Edition, UdiManber, Addison-Wesley, Reading, MA.

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

Course Code:	**CCT207**	**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:	**CCT208**	**Course Name:**	**Cryptography**		
L: 3 Hrs	**T: 0 Hrs**	**P: 0 Hrs**	**Per Week:3**	**Total Credits:**	**3**

Course Objectives:

To understand basics of Cryptography.

To be able to secure a message over insecure channel by various means.

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:	**CCP208**	**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

To make students aware of various Integrity checks and Authentication algorithms

2. To make students familiar with Application layer security

Syllabus:

Experiments based on CCT208 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:	**CHT252**	**Course:**	**Environmental Sciences**
L: 2 Hrs, T: 0 Hr, P: 0 Hr, Per Week		**Total Credits:**	**0**

Syllabus

Principle of contaminant behaviour and recent trends in environmental pollution control.

UNIT I

Air pollution and its control techniques: (4 lectures)

Contaminant behaviour in the environment, Air pollution due to SOx, NOx, photochemical smog, Indoor air pollution Natural pathways for degradation: Carbon cycle, Sulphur cycle, Nitrogen cycle, Oxygen cycle Factors responsible for altering the composition of atmosphere (deforestation, burning of fossil fuels, industrial and vehicular emissions, CFCs). Techniques to control Air pollution, ambient air quality and continuous air quality monitoring, Control measures at source, Kyoto Protocol, Carbon Credits.

UNIT II

Noise pollution and its control techniques: (2 lectures)

Introduction to noise pollution and its causes. Noise pollution control: Recent advances in noise pollution control and benefits.

UNIT III

Soil pollution and its control techniques: (5 lectures)

Soil pollution: Soil around us, Soil water characteristics, soil pollution. Solid waste management: Composting, vermiculture, landfills, hazardous waste treatment, bioremediation technologies, conventional techniques (land farming, constructed wetlands),and phytoremediation. Degradation of xenobiotics in environment: Petroleum hydrocarbons, pesticides, heavy metals

UNIT IV

Water pollution and its control techniques: (8 lectures)

Major sources of water pollution: Eutrophication, acid mine drains, pesticides and fertilizers, dyeing and tanning, marine pollution, microplastics Techniques to control water pollution: Conventional waste water treatment-types of sewage, ewerage system, alternative systems, primary, secondary and tertiary processes including aerobic and anaerobic techniques, safe disposal. Case studies: Treatment schemes for waste water from dairy, textile, power plants, pharmaceutical industries, and agro based industries such as rice mills

UNIT V

E-wastes (2 lectures)

Introduction, types of e-wastes, environmental impact, e-waste recycling, e-waste management rules.

UNIT VI

Environmental Sustainability: Role of Green technology (5 lectures)

Concept of green technologies, categories, goals and significance, sustainability Green energy, green chemistry, challenges to green technology, advantage and disadvantages of green processes, Eco mark certification- its importance and implementation VII- Different government initiatives (2 lectures)

National ambient air quality standard 2009, Swacch Bharat Abhiyan, National afforestation program and Act- 2016, National river conservation plan, Formation of National Green Tribunal

Course Outcomes

On successful completion of the course, students

1. Will get sufficient knowledge regarding different types of environmental pollutions, their causes, detrimental effects on environment and effective control measures.
2. Will realize the need to change an individual's outlook, so as to perceive our Environmental issues correctly, using practical approach based on observations and self-learning.
3. Will become conversant with recent waste management techniques such as E-wastes, its recycling and management.
4. Will gain knowledge about the modes for sustainable development, importance of green energy and processes.
5. Will be able to identify and analyze environmental problems as well as risks associated with these problems and greener efforts to be adopted, to protect the environment from getting polluted.

Text Books

1. Benny Joseph, Environmental Studies, Mc Graw Hill Education (India) Private Limited
2. B. K. Sharma, Environmental Chemistry, Goel Publishing House, Meerut
3. P Aarne Vesilind, J. Jeffrey Peirce and Ruth F. Weiner, Environmental Pollution and Control,Butterworth-Heinemann
4. D. D. Mishra, S. S. Dara, A Textbook of Environmental Chemistry and Pollution Control, S.Chand & Company Ltd. Sultan Chand & Company

5. Shree Nath Singh, Microbial Degradation of Xenobiotics, Springer-Verlag Berlin Heidelberg
6. P.T. Anastas & J.C. Warner, Green Chemistry: Theory & practice, Oxford University Press
7. P. Thangavel & Sridevi, Environmental Sustainability: Role of Green technologies, Springer publications.

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

Course Code: CCT299 **Course: Introduction to Networks & Cryptography**

L: 3 Hrs, T: 0 Hr, P: 0 Hr, 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 understand basics of Cryptography
4. To learn about how to maintain the Confidentiality, Integrity and Availability of data

Syllabus

Introduction to Networks: Data communication Components:, Various Connection Topology, Protocols and Standards, OSI Model, TCP/IP Model

Fundamentals of Data Link Layer, Fundamentals of Network Layer: Internet Protocol (IP)

Fundamentals & elements of Transport Layers, Fundamentals & elements of Application Layer, Firewalls

Introduction to Cryptography: Introduction to security attacks - services and mechanism, Conventional encryption model - classical encryption techniques - substitution ciphers and transposition ciphers

Stream and block ciphers, Principles of public key crypto systems - RSA algorithm, Diffie-Hellman Key Exchange algorithm

Introduction to Integrity checks and Authentication algorithms: Hashing, Message Digests, Digital Signatures

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.
3. William Stallings, “Cryptography and Network security Principles and Practices”, Pearson / PHI, 5th Edition
4. Behrouz A. Forouzan, Debdeep Mukhopadhyay, “Cryptography and Network Security” 3rd Edition, McGrawHill

Reference Books

1. James F. Kurose and Keith W. Ross: Computer Networking: A Top-Down Approach Featuring the

Internet, 3rd Edition

2. W. Mao, “Modern Cryptography – Theory and Practice”, Pearson Education.

Course Outcomes:

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

1. To understand basics of computer networks and reference models
2. To identify the Design issues of each layer of OSI model
3. To comprehend mechanism of cryptographic attacks
4. To assess the application of various cryptography techniques

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

Course Code: CCT301 **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 V, B.TECH CSE (Cyber Security)

Course Code: CCP301 **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 CCT301 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 V, B. TECH CSE (Cyber Security)

Course Code: CCT302 **Course: Computer Security**

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

Course Objectives

1. To introduce the structure of a network & role of cryptography in communication over an insecure channel
2. To explain & to compare how various attack scenarios work & how security principles work
3. To evaluate risks faced by computer systems
4. 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.

Text Books:

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: CCP302 **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:

- 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.

Practicals based on Theory CCT301

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: CCT303 **Course: Artificial Intelligence & Cyber Security**

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

Course Objectives

The objective of this course is:

1. To introduce basic machine learning algorithm for solving problem.
2. To understand major machine learning algorithms.
3. To learn the role of AI and ML in Botnet and web applications

Course Syllabus

Unit 1:

Foundations for ML: ML Techniques overview, Linear and Logistic regression, K-nearest neighbor Decision Tree, Random Forest algorithm

Unit 2:

Supervised Learning: Linear threshold units, Perceptron, Multilayer networks and back-propagation, Bayes decision rule, Naïve Bayes Classifiers

Unit 3:

Unsupervised Learning: Clustering (K means, Fuzzy-c means), Hidden Markov Models, Gaussian Mixture Modeling, EM-algorithms

Unit 4:

The Role of ML and AI in Security: Where Rules-Based, Signature-Based, and Firewall Solutions Fall Short, Preparing for Unexpected Attacks, Focusing on the Threat of Malicious Bots, Bots and Botnets, Bots and Remote Code Execution

Unit 5:

The Evolution of the Botnet: A Thriving Underground Market, The Bot Marketplace, AI and ML Adoption in Botnets, Staying Ahead of the Next Attack with Threat Intelligence

Unit 6:

AI and ML on the Security Front: A Focus on Web Applications, Finding Anomalies, Bringing ML to Bot Attack Remediation, Using Supervised ML-Based Defenses for Security Events, and Log Analysis, Deploying Increasingly Sophisticated Malware Detection, Using AI to Identify Bots.

Course Outcomes

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

1. Apply supervised machine learning techniques to solve different problems.
2. Use un-supervised machine learning techniques to solve different problems.
3. Apply machine learning models solve cyber security problems.
4. Apply machine learning models in dealing threats on web applications and defense areas.

Text Books

1. Tom Mitchell; Machine Learning- an Artificial Intelligence Approach, Volume-II; Morgan Kaufmann, 1986.
2. Laurent Gil, Allan Liska, (2019), Security With AI And Machine Learning, Shroff/O'Reilly

Reference Books

1. Shalev-Shwartz,S., Ben-David,S., (2014), Understanding Machine Learning: From Theory to Algorithms, Cambridge University Press

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

Course Code: CCP303 **Course: Artificial Intelligence & Cyber Security Lab**

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

Course Prerequisite

Python Programming

Course Objectives

1. To implement basic machine learning algorithm for solving problem.
2. To implement supervised and unsupervised major machine learning algorithms.
3. To learn the role of AI and ML in Botnet and web applications

Course Syllabus

Experiments based on CCT303 syllabus

Course Outcomes

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

1. Implement supervised machine learning techniques
2. Implement un-supervised machine learning techniques for different problems.
2. Apply machine learning models in cyber security areas.

Text Books

1. Tom Mitchell; Machine Learning- an Artificial Intelligence Approach, Volume-II; Morgan Kaufmann, 1986.
2. Laurent Gil, Allan Liska, (2019), Security With AI And Machine Learning, Shroff/O'Reilly

Reference Books

1. Shalev-Shwartz,S., Ben-David,S., (2014), Understanding Machine Learning: From Theory to Algorithms, Cambridge University Press

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

Course Code: HUT353 **Course: Indian Traditional Knowledge**

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

Course Objectives

The course is designed with the objective of developing understanding of the students about the essence of Indian traditional knowledge in terms of its scientific approach, legality, role in natural resource protection, as well as its contribution to philosophy and art.

Syllabus:

Unit 1: Basic Structure of Indian Traditional Knowledge: Vedas, Upavedas, Vedang, Upadang, scientific approach

Unit 2: Ecology and Indian Traditional Knowledge: Meaning, role, case studies

Unit 3: Intellectual Property Rights and Indian traditional Knowledge: Meaning, role in protection of Indian traditional knowledge, cases studies

Unit 4: Indian Philosophical traditions: Nyay, Sankaya, Yog, Mimansa, Jainism, Buddhism, Sikhism, and other approaches

Unit 5: Indian Artistic Traditions: Chitrakala, Murtikala, Vastukala, Sangeet, Sthpatya, Nritya evam Sahitya, case studies.

Unit 6: Knowledge of traditional Indian Science and Technology

Course Outcomes

On successful completion of the course, students will have increased ability to understand the importance and application of:

1. Indian Knowledge system and its scientific approach.
2. Traditional knowledge and protection of nature.
3. The legality and its importance for the protection of Indian traditional knowledge.
4. Indian philosophical tradition.

5. Indian artistic tradition

Reference Books/Material.

1. Amit Jha (2009), Traditional Knowledge System in India, Atlantic Publishers and Distributors.

2. RR Gaur, Rajeev Sangal, GP Bagaria, Human Values and Professional Ethics (Excel Books, New Delhi, 2010)

3. V. Sivaramakrishanan (ed.), Cultural Heritage of India – Course material, Bharatiya Vidya Bhavan, Mumbai, 5th Edition, 2014

4. Swami Jitatmanand, Modern Physics and Vedant, Bharatiya Vidya Bhavan

5. Swami Jitatmanand, Holistic Science and Vedant, Bharatiya Vidya Bhavan

6. S.C. Chatterjee and D.M. Datta, An introduction to Indian Philosophy, University of Calcutta,
1984

7. Pramod Chandra, Indian Arts, Howard University Press, 1984

8. Krishna Chaitanya, Arts of India, Abhinav Publications, 1987

9.https://www.researchgate.net/publication/299625768_Traditional_Knowledge_systems_in_India_ for_biodiversity_conservation/link

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

Course Code: CCT304-1 **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:	**CCT304-2**	**Course:**	**Network and Web Security Firewall and VPN**
L: 3 Hrs,	**T: 0 Hr, P: 0 Hr, Per Week**		**Total Credits: 03**

Course Pre-requisite

Basics of Computer Networks

Course Objectives

1. To understand network security concepts
2. To study the basics Encryption methods to provide network security
3. To conduct testing on various attacks
4. To know Firewall architecture and VPN Tunneling

Syllabus

Unit-1

Network Security

Network Security Model, Encryption techniques, DES Encryption, Public key Cryptography fundamentals and Algorithms: RSA Encryption, Diffie Hellman Algorithm for key exchange signature.

Unit-2

Digital Certificates

Digital Signature, User Authentication: Password certificate based and biometric Authentication, Kerberos, IP Security, SSL Protocol.

Unit-3

Web Security

Cross Site request forgery, cross site scripting and client Injection attack web application authentication Attack.

Unit-4

Web application Overview

Session management, SQL injection Attacks, Web application Configuration test

Unit-5

Firewalls

Understand the of next generation firewall [NGFW]; Introduction to different Firewalls Models, parameters for deciding Firewall for a network; Architecture, Firewall platforms for VM Firewall and hardware firewall. Application of various platforms suiting to different network environment.

Unit-6

Virtual Private Network

Fundamentals of VPN and its protocol, types of VPN Tunnelling, VPN proxy. Intrusion detection

Course Outcome:

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

1. Apply Encryption methods for secure transmission and study key management required for encryption.
2. Develop Concept of Security needed in networks and study various Possible Attacks.
3. Understand authentication requirements and study various authentication mechanisms.
4. Apply Security testing on web application and study the concept of Firewall and VPN.

Text Books:

1. "Cryptography & Network Security", PHI 5th Edition William Stalling
2. "Cryptography & Network Security", Mc Graw Hill Atul Kahate
3. "Cryptography & Network Security", PHI 4th Edition Behrouz Forouzan

Reference Books:

1. "Modern Cryptography, Theory & Practice", Pearson Education. Wenbo Mao
2. "An Introduction to Mathematical Cryptography", Springer. Hoffstein, Pipher, Silvermman.
3. "The Design of Rijndael", Springer. J. Daemen, V. Rijmen
4. "Algorithmic Cryptanalysis", CRC Press. A. Joux
5. "Number Theory", Tata Mc Graw Hill. S. G. Telang
6. "Protocols for Authentication and Key Establishment", Springer. C. Boyd, A. Mathuria
7. "Computer Security", Pearson Education. Matt Bishop
8. Virtual Laboratories: Vlabs, "Cryptography Lab" http://cse29-iiith.vlabs.ac.in/

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

Course Code:	**CCT304-3**	**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

Unit 6: 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

Text Book:

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 V, B. TECH CSE (Cyber Security)

Course Code: CCT398 **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

5. Learn about the hacker mindset and the history of hackers
6. Understand basic networking and security technologies
7. Gain a basic understanding of security policy
8. 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:

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

Text Books:

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

Reference Books:

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

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

Course Code: CCT306 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: CCP306 **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

Practicals based on **CCT306** 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: CCT307 **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: CCP307 **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.

Practicals based on CCT307 syllabus

Experiments covering CCT307 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: CCT308 **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 schemes,-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.

UNIT-VI: 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 VI, B. TECH CSE (Cyber Security)

Course Code: CCP308 **Course: Compiler Design Lab**

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

Course Prerequisite:

Course on Formal Language & Automata Theory and Programming Language.

Course Objectives:

This laboratory course is intended to make the students experiment on the basic techniques of compiler construction and use of various tools for implementation. This will provide deeper insights into the aspects of programming languages and various phases of compiler.

Syllabus:

Experiments based on syllabus of Complier Design (CCT308).

Course Outcomes:

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

1. Use Open-Source tools to create a lexical analyzer and parser.
2. Implement different types of Parsing techniques.
3. Implement various syntax directed translation schemes to generate intermediate code.
4. Implement various code optimization techniques to improve performance of a program segment and code generation.

Text Books:

1. Doug Brown, John Levine, Tony Mason, Lex and Yacc, O'Reilly Media, 2nd Edition, 2012.
2. Des Watson, A Practical Approach to Compiler Construction, Springer, 1st ed. edition, 2017.

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

Course Code: CCT309-1 **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: 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

Unit 6: 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.

Text Books:

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: CCT309-2 **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.

Text Books:

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: CCT309-3 **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.

Text Books:

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: CCT309-4 **Course: Security in Distributed Computing**

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

Course Objectives:

1. To introduce concepts related to distributed computing systems.
2. To learn the principles, architectures, algorithms and programming models used in distributed systems.
3. To focus on security issues in a distributed environment
4. To analyse the role of blockchain technology for implementation of security in distributed systems.

Syllabus

Unit 1: Distributed Computing - I

A Model of Distributed Computations, Logical Time, Global State and Snapshot Recording Algorithms, Terminology and Basic Algorithms, Message Ordering and Group Communication, Termination Detection

Unit 2: Distributed Computing – II

Mutual Exclusion Algorithms, Deadlock Detection, Distributed Shared Memory, Checkpointing and Rollback Recovery, Failure Detectors, Authentication in Distributed Systems, Self-Stabilization

Unit 3:

Common Security Issues and Technologies, Host-Level Threats and Vulnerabilities, Infrastructure-Level Threats and Vulnerabilities, Application-Level Threats and Vulnerabilities, Service-Level Threats and Vulnerabilities

Unit 4:

Host-Level Solutions, Infrastructure-Level Solutions, Application-Level Solutions, Service-Level Solutions, Security Management, Developing Security Strategies, Auditing

Unit 5: Blockchain for Distributed Systems Security

Introduction to Blockchain, Distributed Consensus Protocols, ProvChain, Automotive Security and privacy, Dynamic Key management for IoT, Blockchain-enabled Information Sharing Framework for Cybersecurity

Unit 6: Blockchain Security Analysis & Implementation

Blockcloud Security Analysis, Permissioned and Permissionless Blockchains, Blockchain Memory with Unconfirmed Transactions, Reputation-based Paradigm, Private Blockchain configurations for Improved IoT Security, Blockchain Evaluation platform.

Course Outcomes:

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

1. Establish and implement a distributed computing environment securely.
2. Identify and sustain threats to a distributed computing environment.
3. Utilize blockchain technology for enhancing security in distributed computing.

Text Books:

1. Distributed Computing: Principles. Algorithms and Systems by Ajay D. Kshemkalyani & Mukesh Singhal. Cambridge University Press.

2. Distributed Systems Security: Issues, Processes and Solutions by Abhijit Belapurkar, Anirban Chakrabarti, Harigopal Ponnapalli, Niranjan Varadarajan, Srinivas Padmanabhuni & Srikanth Sundarrajan. Wiley Publishing.

3. Blockchain for Distributed Systems Security. Edited by Charles A. Kamhoua, Laurent L. Njilla, Sachin Shetty. Wiley Publishing.

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

Course Code: CCT310-1 **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.

Text Books:

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: CCT310-2 **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: CCT310-3 **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: CCT310-4 **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

Unit 5: Malware Disassembly

Computer Basics, Assembly Language & Its Operations, Windows x64 Architecture, Disassembly using IDA, Debugging Malicious Binaries

Unit 6: Advanced Malware Analysis

Malware Functionalities & Persistence, Code Injection & Hooking, Malware Obfuscation Techniques, 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.

Text Books:

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 VI, B. TECH CSE (Cyber Security)

Course Code: CCT399 **Course: Managing Risk in Information Systems**

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

Course Objectives:

4. To understand and manage risks associated with the use of information technology.
5. To identify and assess risks to the confidentiality, integrity, and availability of an organization's assets.
6. 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 –

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

Text Books:

5. Managing Risk in Information Systems, Third Edition by Darril Gibson & Andy Igonor. Jones & Bartlett Learning.
6. Measuring and Managing Information Risk: A FAIR Approach by Jack Freund & Jack Jones. Butterworth-Heinemann Publishing.
7. Managing Risk and Information Security, Second Edition by Malcom W. Harkins. Apress Open Publishing.
8. How to Measure Anything in Cybersecurity Risk by Douglas W. Hubbard & Richard Seiersen. Wiley Publishing

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

Course Code: CCT401 – 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.

Unit VI: 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: CCP401-1 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 CCT401-1

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: CCT401-2 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 standardsand 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: CCP401-2 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: CCT401-3 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:	**CCP 401-3**	**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: CCT402-1 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: CCP402-1 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: CCT402-2 Course: Cyber Law & Legal Issues in Cyber Security
L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

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 cyber world.
4. Recognize the importance of digital divide, contingent workers and whistle blowing situations.

SYLLABUS

Unit-1. Cyber Law in India: A beginning, objectives, scope applicability IT Amendment ACT 2008, Overview of rules issued under IT Act 2000. Emergence of Cyberspace, Cyber Jurisprudence. Cyber laws, Important websites and addresses.

Unit-2. Introduction to Cyber Crimes, Classification, causes, case studies on cybercrime, Cyber Frauds: Hacking, Digital Forgery, Cyber Stalking/Harassment, Cyber terrorism, Cyber Defamation, Cyber Torts. Investigate cybercrime: Introduction to OSINT Framework, workflow process.

Unit-3. 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, Cyber extortion. Types of Exploits and Perpetrators.

Unit-4. Intellectual Property: Copy rights, Patents, Trade Secret Laws, Key Intellectual property issues, Plagiarism, Competitive Intelligence, Cybersquatting.

Unit-5. Privacy: The right of Privacy, Protection, Key Privacy and Anonymity issues, Identity Theft, Consumer Profiling, Freedom of Expression, Defamation and Hate Speech.

Unit-6. Ethics of IT Organization: Contingent Workers H- IB Workers, Whistle- blowing, Protection for Whistle- Blowers, Handling Whistle- blowing situation, Digital divide.

Course Outcome:

1. Analyze statutory, regulatory, constitutional, and organizational laws that affect the software professional.
2. Evaluate relationship between ethics and cyber laws with respect to legal dilemmas in the Information Technology field.
3. Interpret various intellectual property rights, Privacy, Protection issues in software development field.
4. Distinguish between Business ethics roles applicable to IT users, IT professional Malpractice, IT organization workers

Textbooks:

1. George Reynolds, “Ethic s in information Technology”,5th edition Cengage Learning
2. Hon C Graff, Cryptography and E-Commerce - A Wiley Tech Brief, Wiley Computer Publisher, 2001
3. Introduction to Open-source Intelligence techniques.by Michael bazzel 6th Edition.

Reference Books:

1. Michael Cross, Norris L Johnson, Tony Piltzecker, Security, Shroff Publishers and Distributors Ltd.

2. Debora Johnson," Computer Ethic s",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)
5. Cyber Crime Law and Practice by CS Mamta Binani, THE INSTITUTE OF company secretaries of india.

Syllabus for Semester VII, B. Tech. Computer Science & Engineering (Cyber Security)
Course Code: CCP402-2 Course: Cyber Law & Legal Issues in Cyber Security Lab
L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week Total Credits: 01

Course Objectives

- Understanding of cyber law concepts and principles
- Familiarity with legal frameworks and regulations
- Ability to analyze and apply legal principles to real-world situations
- Hands-on experience with legal research and analysis

Syllabus

Experiments based on CCT402-2

Course Outcomes

1. Implement various cyber security laws in real life use cases
2. Analyze security principles and implement to solve the problem
3. Apply various legal framework and regulation under IT Act 2000 and IT Act Amendment 2008.
4. Analyze case studies on Business ethics roles applicable to IT users, ITprofessional Malpractice, IT organization workers

Syllabus for Semester VII, B. Tech. Computer Science & Engineering (Cyber Security)
Course Code: CCT402-3 Course: Privacy Engineering
L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Objectives

1. To introduce students to the field of privacy engineering
2. To focus on the design and implementation of privacy-enhancing technologies and practices
3. To learn about the legal, ethical, and social implications of data privacy

Syllabus

Unit I. Evolution of technology, changes in data privacy over the years, relationship between IT and privacy, IoT and privacy, different forms of privacy, real privacy risks, PII, fair information processing principles, data and privacy governance, GAPP

Unit II. Developing privacy policies, enterprise-specific privacy development, internal vs external policies, privacy engineering requirements, privacy requirement use cases, use case metadata, determining data requirements, cloud privacy requirements

Unit III. Privacy engineering lifecycle methodology, enterprise architecture, system engineering lifecycle, use of models within methodology, business and privacy data classes, privacy component class model, privacy component solution, arunner's mobile app

Unit IV. Vacation planner application, vacation planner solution, dynamic modeling, define service components, quality assurance, frameworks to create privacy QA checklist, privacy concerns during QA, privacy impact assessment

Unit V. Privacy responsibilities, privacy awareness and readiness assessments, building operational plan, building communication and training plan, organizational placement and structure, common privacy engineering roles, challenges, business benefits of alignment

Unit VI. Value and metrics for data assets, finding values for data, valuation models, privacy in era of data economics, calculating the cost of privacy, no one-size-fits-all formula, innovation and privacy, societal pressures and privacy, new buildingcode for privacy, privacy engineer's manifesto

Course Outcomes:

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

1. Identify various privacy domains and policies
2. Develop privacy engineering lifecycle models and frameworks
3. Build various privacy domain plans
4. Calculate the cost of privacy

Textbooks

1. The Privacy Engineer’s Manifesto: Getting from Policy to Code to QA to Value by Michelle Finneran Dennedy, Jonathan Fox and Thomas R. Finneran. Apress Open.

Syllabus for Semester VII, B. Tech. Computer Science & Engineering (Cyber Security)
Course Code: CCP402-3 Course: Privacy Engineering Lab
L: 0 Hrs, T: 0 Hr, P: 2 Hr, Per Week Total Credits: 01

Course Objectives:
Students will be able to
1. Learn about various privacy-enhancing technologies
2. Apply these technologies to real-world scenarios.
3. Design and implementation of a privacy-preserving system

Syllabus
Practical based on Syllabus of CCT402-3

Course Outcomes:
On successful completion of the course, students will be able to:
1. Analyze privacy risks and design solutions to mitigate these risks
2. Implement privacy-enhancing technologies such as data anonymization, differential privacy, and secure multiparty computation
3. Evaluate the effectiveness of privacy-enhancing technologies through testingand analysis
4. Apply privacy-enhancing technologies to web and mobile applications

Syllabus for Semester VII, B. Tech. Computer Science & Engineering (Cyber Security)
Course Code: CCT498 Course: Enterprise Architecture and Components (Security By Design)
L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Objectives

1. To familiarize the prospective engineering graduates with the strong fundamental knowledge of enterprise architecture design by security and practices.
2. To facilitate development of design skills on enterprise architecture front.
3. To enable the graduates to apply the theory in practice and to channelize solutionsto challenging real-world problems.

Syllabus

Unit I. Enterprise & Security
The Cultural Legacy: Business Prevention Measuring and Prioritising Business Risk Information Security as the Enabler of Business Adding Value to the Core Product Empowering the Customers, Protecting Relationships and Leveraging Trust What Does 'Security' Mean?

Unit II. Enterprise & Architecture The Origins of Architecture Managing Complexity
Information Systems Architecture Enterprise Security Architecture, Why Architectures Sometimes Fail to Deliver Benefit – and How to Avoid that Fate Security Architecture Needs a Holistic Approach
What Does Architecture Mean?

Unit III. Security Architecture Model
The SABSA®,COBIT 5, TOGAF Model, The Architect's View The Designer's View The Builder's View The Tradesman's View, The Facilities Manager's View The Inspector's View, The SABSA® Matrix, Detailed SABSA® Matrix for the Operational Layer The Security Architecture Model

Unit IV. Systems Approach The Role of Systems Engineering Why a Systems Approach?
What Does the Systems Approach Make You Do? The Need for Systems Engineering in Security Architectures Some Basic Concepts, The Control System Concept, Using the Systems Approach in Security Architecture Case Study on Integrated Financial Systems Advanced Modelling Techniques

Unit V. Return on Investment in Security Architecture
What Is Meant by 'Return on Investment'? Why Do You Need Metrics? The Security Management Dashboard The Balanced Scorecard Approach Business Drivers and Traceability Business Attributes and Metrics Setting Up a Metrics Framework, Maturity Models Applied to Security Architecture

Unit VI. Security Architecture Program
Selling the Benefits of Security Architecture, Getting Sponsorship and BudgetBuilding the Team Getting Started: Fast Track™ Workshops, Programme Planning and Management Collecting the Information, You Need, Getting Consensus on the Conceptual Architecture Architecture Governance and Compliance Architecture Maintenance Long-Term Confidence of Senior Management

Course Outcomes:

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

1. Use enterprise architecture practices and various models.
2. Apply processes for modeling enterprise architecture with security design and solving real-world problems.
3. Analyze the impact of different enterprise architecture strategies on software development.
4. Estimate return on investment in security architecture.

Textbooks

1. “Enterprise Security Architecture” by Nicholas Sherwood, CRC Press

Reference Books

1. “Enterprise Security Architecture for Digital Business” by Geng Lin, O'Reilly

Syllabus for Semester VII, B. Tech. Computer Science & Engineering (Cyber Security)
Course Code: IDT 452 Course: Bio-informatics
L: 2 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 02

Course Objectives

1. Provide an introduction to the field of Bioinformatics.
2. Describe how bioinformatics data is stored and organized.
3. Provide an approach to build search query and sequence alignment.
4. Provide methods for genome analysis.

Syllabus

UNIT-I: Introduction to Bioinformatics: Genome Sequences ORFs, Genes, Introns, Exons, Splice Variants DNA/RNA Secondary Structure, Retrieval methods for DNA sequence, protein sequence and protein structure information.

UNIT-II: Biological Databases – Format and Annotation: Conventions for database indexing and specification of search terms, Common sequence file formats. Annotated sequence databases - primary sequence databases, protein sequence and structure databases; Organism specific databases, Data retrieval tools – Entrez, DBGET and SRS, Submission of (new and revised) data.

UNIT-III: Sequence Similarity Searches: Local versus global, Distance metrics, Similarity and homology, scoring matrices, PAM, BLOSUM, PSSM, Dot Plot.

UNIT-IV: Dynamic programming algorithms: Needleman-wunsch and Smith-waterman, Heuristic Methods of sequence alignment, FASTA, BLAST and PSI BLAST.

UNIT-V: Multiple Sequence Alignment and software tools for pair wise and multiple sequencealignment, Clustal W algorithm - Feng Doolittle algorithm**.** Phylogenetic Analysis: Methods of phylogenetic analysis, UPGMA, WPGMA, neighbour joining method.

UNIT-VI: Genome Analysis: Genomic data and databases, Genomic data analysis strategies,existing software tools, Gene Prediction, NGS data analysis

Course Outcomes:

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

1. Understand the basics of Biological Data acquisition.
2. Implement format, access and retrieval of Biological data.
3. Identify sequence structure, alignment and search query.
4. Understand genome data and analysis.

Textbooks

1. Bioinformatics: Databases and Systems, by Stanley I. Letovsky
2. Bioinformatics Databases: Design, Implementation, and Usage (Chapman & Hall/ CRC Mathematical Biology & Medicine), by Sorin Draghici
3. Data base annotation in molecular biology, principles and practices, Arthur M.Lesk
4. Current topics in computational molecular biology, Tao, Jiang, Ying Xu, MichaelQ.Zang

Reference Books

1. D. Baxevanis and F. Oulette, (2002) “Bioinformatics : A practical guide to the analysisof genes and proteins”, Wiley Indian Edition
2. Cynthia Gibas and Per Jambeck (2001), “Developing Bioinformatics Computer Skills”. O’Reilly press, Shorff Publishers and Distributors Pvt. Ltd., Mumbai.
3. Bryan Bergeron MD (2003), “BioinformaticsComputing”. Prentice Hall India(Economy Edition)

Syllabus for Semester VII, B. Tech. Computer Science & Engineering (Cyber Security)
Course Code: CCT403 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 Coding Standard. 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 VIII, B. E. Cyber Security (Computer Science & Engineering)

Course Code: CCT405-1		**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

Unit VI

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: CCT405-2 Course: Database Security
L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Objectives

1. To understand the fundamental principles of database security
2. To understand the security issues & solutions for Database, Multilevel Database, Distributed database, Outsourced Database and Data Warehouse
3. Learning how to design secure database systems, including the use of accesscontrol mechanisms, encryption, and authentication and authorization protocols

Syllabus

Unit I: Introduction to Database – Relational Database & Management System – ACID Properties, Normalization, RAID, Relational Algebra, Query tree, Data Abstraction (Physical Level, Logical Level & View Level) - Multi-level Database, Distributed Database

Unit II: Security issues in Database – Polyinstantiation - Integrity Lock - Sensitivity Lock – Security Models – Access Control (Grant & Revoke Privileges) - Statistical Database, Differential Privacy. Distributed Database Security

Unit III: Outsourced Database and security requirements – Query Authentication Dimension – Condensed RSA, Merkle Tree, B+ Tree with Integrity and Embedded Merkle B-Tree – Partitioning & Mapping - Keyword Search on Encrypted Data (Text file)

Unit IV: Security in Data Warehouse & OLAP – Introduction, Fact table, Dimensions, Star Schema, Snowflake Schema, Multi-Dimension range query, Data cube - Data leakage in Data Cube, 1- d inference and m-d inference – Inference Control Methods

Unit V: XML – Introduction about XML – Access Control Requirements, Access Control Models: Fine Grained XML Access Control System
Geospatial Database Security – Geospatial data models – Geospatial Authorization, Access Control Models: Geo-RBAC, Geo- LBAC

Unit VI: Privacy-Preserving Data Mining – Introduction - Randomization method: Privacy Quantification, Attacks on Randomization, Multiplicative Perturbations, Data Swapping – K-Anonymity framework – Distributed Privacy-Preserving Data Mining. Database Watermarking – Basic Watermarking Process - Discrete Data, Multimedia, and Relational Data – Attacks on Watermarking - Single Bit Watermarking, Multi bit Watermarking.

Course Outcomes:

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

1. Describe the fundamental principles of database security
2. Identify and assess the potential security threats and vulnerabilities of databasesand database systems
3. Understand the design of secure database systems, using access control mechanisms and various protocols
4. Understand the security measures to protect databases against various types of attacks and breaches

Textbooks

1. Database Security and Auditing, Hassan A. Afyouni, India Edition, CENGAGE Learning, 2009.
2. Database Security, Castano, Second edition, Pearson Education.

Reference Books

1. Michael Gertz and Sushil Jajodia (Editors), Handbook of Database Security: Applications and Trends, ISBN-10: 0387485325. Springer, 2007
2. Osama S. Faragallah, El-Sayed M. El-Rabaie, Fathi E. Abd El-Samie, Ahmed I. Sallam, and Hala S. El-Sayed, Multilevel Security for Relational Databases by; ISBN 978-1- 4822- 0539-8. CRC Press, 2014.
3. Bhavani Thuraisingham, Database and Applications Security: Integrating Information Security and Data Management, CRC Press, Taylor & Francis Group, 2005.

Syllabus for Semester VIII, B. Tech. Computer Science & Engineering (Cyber Security)
Course Code: CCT405-3 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 recover 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 controldecision, and risk reporting - Business Impact Analysis (BIA) concept, benefits andresponsibilities - 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

Unit VI: 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: CCT405-4 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. Tech. Computer Science & Engineering (Cyber Security)
Course Code: CCT406-1 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

Unit VI

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. E. (Computer Science & Engineering)
Course Code: CCT 406-2 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

Unit VI: 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: CCT406-3 Course: Security in Social Networks
L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Objectives

1. To make students familiar with social networks and their applications.
2. To familiarize students with different models and representations of socialnetworks.
3. To enable students to design solutions to query and evaluate the social networks.
4. To enable students to mitigate security threats in OSNs.

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: CCT406-4 Course: Security of Embedded Systems
L: 3 Hrs, T: 0 Hr, P: 0 Hr, Per Week Total Credits: 03

Course Objectives

1. To study the embedded system design and issues in the security protocols.
2. To study characteristics of Wireless Sensor Network along with types of probable attacks.
3. To study debug, trouble shoot basic issues in RTOSs, resource constrained devices and provide security to devices.
4. To study design security protocols for a typical Wireless Sensor Network/IoT Systems.

Syllabus

Unit I Introduction to Embedded Security

Introduction, Review of Security Basics, Services & Mechanisms, Security Requirements in Embedded Systems. Design Challenges in Security for Embedded Systems, Security Gap, Typical Generic Security Threats in Embedded Systems.

Unit II Wireless Sensor Networks as Embedded Systems

Evolution of Human Computer Interfaces, Ubiquitous Computing, Pervasive Computing, The Illustrative Sensor Motes, Typical Configurations, Deployment Models and Issues, Typical Applications, Security Issues, Security in Wireless Sensor Networks, Typical Attacks and Countermeasures. The Denial of Service Attacks on Wireless Sensor Networks.

Unit III Secure Data Aggregation in Wireless Sensor Networks

Motivation for Secure Data Aggregation in Wireless Sensor Networks. End-to-End and Hopby- Hop Secure Data Aggregation and Issues, Design of a Hop-by-Hop Link Layer Security Protocol in Wireless Sensor Networks.

Unit IV Attacks and Issues in Embedded System

Design Issues Viz. Security Issues, Performance Issues, Ciphers, Initialization Vector, Message Authentication Code, Authenticated Encryption Modes. Investigating Replay attacks in Link Layer Security Architectures and Typical Mitigation Approaches. The Replay Protection Algorithms Continued. Flexibly Configurable Link Layer Security Architecture for Wireless Sensor Networks.

Unit V Security and Privacy Issues in IOT Systems

The Internet of Things, Architecture, Constituent Elements, The Security and Privacy Issues in IoT Systems, Overview of the IoT Protocols Viz. Continua for Home Health Devices, DDS, DPWS: WS-Discovery-SOAP-WS Addressing-WDSL-XML Schema, HTTP/REST, MQTT, UPnP, XMPP, ZeroMQ. The IoT Security Protocols viz. ZigBee, Bluetooth, 6LowPAN, RPL. The CoAP.

Unit VI Side Channel Attacks in Embedded Systems

Introduction, Side Channel Attacks, Passive Versus Active Attacks, Timing, Analysis, Power Analysis, Electromagnetic Analysis, Analysis, Analysis Tools and Equipment.

Course Outcomes:

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

1. Describe the significance of security in embedded devices, design issues in the securityprotocols,
2. Classify probable attacks on Wireless Sensor Network along with types.
3. Verify trouble shoot basic issues in RTOSs, resource constrained devices and provide securityto devices.
4. Design security protocols for a real-world Wireless Sensor Network/IoT Systems.

Text Books

1. Fei Hu., “Security and Privacy in Internet of Things (IOT's): Models, Algorithms and Implementations Handcover”, 1 st Edition, CRC Press, 2016.
2. R.Giladi, N. Dimitrios, “Security and Embedded Systems”, VOL 2, IOS Press, 2006.
3. A.G. Voyiatzis, A.G. Fragopoulos, and D.N. Serpanos “Security in Embedded Systems Design Issues inSecure Embedded Systems”, 1 st Edition, CRC press,2005.

Reference Books

1. R. Zurawski, “Embedded Systems Handbook”, 1 st Edition, CRC Press,2006.
2. T. Stapko, “Practical Embedded Security: Building Secure Resource-Constrained Systems”, 2 ndEditions, Newnes, 2007.