Dayananda Sagar University

School of Engineering
Deverakaggalahalli, Harohalli, Bengaluru 562112

Department of Computer Science and Engineering

(Cyber Security)

SCHEME AND SYLLABUS

B.Tech. PROGRAMME– 2023-27 BATCH

DAYANANDA SAGAR UNIVERSITY

(A State Private University under the Karnataka
Act No. 20 of 2013) Approved By UGC &
AICTE, New Delhi.

VISION

To be a centre of excellence in education, research & training, innovation & entrepreneurship and to produce citizens with exceptional leadership qualities to serve national and global needs.

MISSION

To achieve our objectives in an environment that enhances creativity, innovation and scholarly pursuits while adhering to our vision.

VALUES

The Pursuit of Excellence

A commitment to strive continuously to improve ourselves and our systems with the aim of becoming the best in our field.

Fairness
A commitment to objectivity and impartiality, to earn the trust and respect of society.

Leadership
A commitment to lead responsively and creatively in educational and research processes.

Integrity and Transparency
A commitment to be ethical, sincere and transparent in all activities

and to treat all individuals with dignity and respect.

SCHOOL OF ENGINEERING

SCHOOL OF ENGINEERING

(Hosur Main Road, Kudlu Gate, Bengaluru-560 068)

Approved By UGC & AICTE, New Delhi.

VISION

To transform life through Excellence and Innovation in Engineering Education and Research with an emphasis on Sustainable, Inclusive Technology and Global needs.

MISSION

To Develop School of Engineering at Dayananda Sagar University, as Center of Excellence by imparting Quality Education and Research to generate highly Competent, Skilled and Humane manpower to face emerging Technological, Scientific and Social challenges with Ethics, Integrity, Credibility and Social concern.

LEADERSHIPS

Sl. No	Name	Position
1	Dr. D. Hemachandra Sagar	Chancellor, DSU
2	Dr. D. Premachandra Sagar	Pro Chancellor, DSU
3	Mr. Galiswamy	Secretory
4	Dr. Amith R Bhatt	Vice Chancellor, DSU
5	Prof. Janardhan R	Pro Vice Chancellor, DSU
6	Dr. Puttamadappa C	Registrar, DSU
7	Dr. Uday Kumar Reddy	Dean, SOE, DSU
8	Dr. Kousalya Govardhanan	Dean, Research, DSU
9	Dr. Ramesh R. Galigekere	Dean, Academics
10	Dr. S Senthil	Professor & Dean, School of Computer Applications
11	Dr. Nagaraja S R	Professor and Chairman Department of Aerospace Engineering
12	Dr. Jayavrinda Vrindavanam	Professor and Chairman, Department of CSE (Artificial Intelligence and Machine Learning)
13	Dr. Girisha G S	Professor and Chairman, Department of Computer Science and Engineering
14	Dr. Durbadal Chattaraj	Associate Professor and Chairman, Department of CSE (Cyber Security)
15	Dr. Shaila S G	Professor and Chairman, Department of CSE (Data Science)
16	Dr. M Shahina Parveen	Professor and Chairperson Department of Computer Science & Technology
17	Dr. Arun Balodi	Professor and Chairman, Department of ECE
18	Dr. Vinayak B Hemadri	Professor and Chairman Department of Mechanical Engineering
19	Dr. Pramod Kumar Naik	Associate Professor and Chairman, Department of AI & Robotics

GOVERNING REGULATIONS FOR

BACHELOR OF TECHNOLOGY (B. TECH) – 2021

PREAMBLE

The School of Engineering under Dayananda Sagar University (DSU) provides Science & Technology based education leading to the development of high caliber engineers suitable for Industry and Scientific Organization. The curriculum focuses on knowledge-based course work integrated with skill development as a part of training. It equally helps in inculcating the scientific temper for the lifelong processes of learning. At the Under Graduate level, a candidate goes through the foundation courses in Science, Humanities & Engineering. Each department ensures that the courses cover both the core & electives courses, as required. Provision for Institutional elective help the candidates to acquire interdisciplinary knowledge base or specialize significantly in an area outside the parent discipline

DEFINITIONS OF KEY WORDS

(i) **Academic Year:** Two consecutive odd, even semesters and a summer term for make up if required.

(ii) **Course:** Usually referred to as a subject, a course may consist of any of Lecture/Tutorials/Practical /Seminar/Mini project/Project work.

(iii) **Credit:** A unit by which the course work is measured. One credit is equivalent to one hour of lecture or one hour of tutorial or two hours of laboratory/practical/ workshop practice per week.

(iv) **Credit Point:** It is the product of grade point and number of credits per course.

(v) **Cumulative Grade Point Average (CGPA):** It is the measure of overall cumulative performance over all semesters. It is expressed upto two decimal places.

(vi) **First Attempt:** If a candidate has completed all formalities of academic requirement in a term and become eligible to attend the examinations and attend all the end semester examinations, such attempt shall be considered as first attempt.

(vii) **Grade Point:** It is a numerical weight allotted to each letter grade on a 10-point scale.

(viii) **Letter Grade:** It is an index of the performance in a said course. Grades are denoted by alphabets.

(ix) **Programme:** An educational activity leading to award a Degree or Certificate.

(x) **Semester Grade Point Average:** It is a measure of performance during a semester. It shall be expressed up to two decimal places.

(xi) **Transcript:** Based on the grades earned, a grade certificate shall be issued after every semester to the candidate registered

(xii) **Failure:** It is the case of appearing for Semester End Examinations, but fails to obtain minimum passing marks in Semester End Examinations.

(xiii) **Detain:** It is the case of not satisfying the eligibility criteria w.r.t Attendance /Internal Assessment in each course to appear for Semester End Examination.

(xiv) **Audit Course:** A course to be taken by the student without benefit of a grade or a credit.

(xv) **Not Fit For The Program (NFFTP):** It is the failure of satisfying the criteria laid down by regulations to continue the program of study, which leads to the termination from the University.

RULES AND REGULATION

UG 1 All B. Tech programmes offered by the University shall be governed by the DSU B. Tech Rules and Regulations – 2021.

UG 2 The B. Tech. rules and regulations shall be applicable to any new discipline(s) that may be introduced in future.

UG 3 A candidate shall become eligible for the award of the B.Tech. Degree after fulfilling all the academic requirements as prescribed by the B.Tech. Rules and Regulations of DSU.

UG 4 ELIGIBILITY FOR ADMISSION

UG 4.1. Admission to First Year Bachelor of Technology shall be open to candidates who have passed the second year Pre-University or XII standard or equivalent examination recognized by the University.

UG 4.2. The candidate shall have studied and passed English as one of the courses and secured not less than forty five percent (45%) marks in aggregate with Physics and Mathematics as compulsory courses, along with any one of the following courses, namely, Chemistry, Bio- Technology, Computer Science, Biology and Electronics. Eligibility shall be 40% in optional courses in case of candidates belonging to SC/ST and OBC candidates from Karnataka.

UG 4.3. Admission to II year /III Semester Bachelor of Technology under

Lateral entry shall be open to the candidates who have passed diploma or equivalent

UG 4.4. Admission to II year /III Semester Bachelor of Technology under Lateral entry shall be open to the candidates who have passed diploma or equivalent

UG 4.6. Admission to II year /III Semester Bachelor of Technology shall be open to candidates who have passed B. Sc. degree from a recognized University or equivalent as recognized by the University and secure not less than 45% marks in aggregate (including all semesters). Eligibility shall be 40% in case of candidates belonging to SC/ST and OBC candidates from Karnataka.

UG 4.7. B.Sc. Graduates seeking admission under Lateral entry shall take up bridge Courses as prescribed in the Scheme of Teaching.

UG 5. ACADEMIC SESSION

UG 5.1. Each academic session is divided into two semesters of approximately sixteen Weeks duration and a summer term: an odd semester (August -December), an even semester (January - May) and summer term (Make-up term) June-July.

UG 5.2. The approved schedule of academic activities for a session, inclusive of dates for registration, mid-semester and end-semester examinations, vacation breaks, shall be laid down in the Academic Calendar for the session.

UG 6. CHANGE OF BRANCH

UG 6.1. Normally a candidate admitted to a particular branch of the undergraduate programme will continue studying in that branch till completion.

UG 6.2. However, in special cases, the University may permit a candidate to change from one branch of studies to another after the first two semesters. Such changes will be permitted, in accordance with the provisions laid down hereinafter.

UG 6.3. Only those candidates will be considered eligible for change of branch after the second semester, who have completed all the credits required in the first two semesters of their studies in their first attempt, without having to pass any course requirement in the summer term examination.

UG 6.4. Applications for a change of branch must be made by intending eligible candidates in the prescribed form. The academic section will call for applications at the end of second semester of each academic year and the completed forms must be submitted by the last date specified in the notification.

UG 6.5. Candidates may enlist their choices of branch, in order of preference, to which they wish to change over. It will not be permissible to alter the choices after the application has been submitted.

UG 6.6. Change of branch shall be made strictly in the order of merit of the applicants. For this purpose, the CGPA obtained at the end of the second semester shall be considered. In case of a tie, SGPA of second semester followed by SGPA of first semester shall decide the tie.

UG 6.7. The applicants may be allowed a change in branch, strictly in order of merit, course to the limitation that the strength of a branch should not fall below the existing strength by more than ten percent and should not go above the sanctioned strength by more than ten percent. The minimum class strength of 75% should be maintained, while considering the change of branch.

UG 6.8. All changes of branch made in accordance with the above rules shall be effective from the third semester of the applicants concerned. No change of branch shall be permitted after this.

UG 7. COURSE STRUCTURE

UG 7.1. Medium of instruction, examination and project reports shall be in English except in case of any language audit courses.

UG 7.2. Teaching of the courses shall be reckoned in credits: Credits are assigned to the Courses based on the following general pattern:

(a) One credit for each lecture period.
(b) One credit for each tutorial period.
(c) One credit per two hours for each Laboratory or Practical or work shop session.
(d) Credits for seminar, mini project, project as indicated in the scheme/curriculum of teaching.

UG 7.3. In order to qualify for a B. Tech. degree of the University, a candidate is required to complete the credit requirement as prescribed in the scheme/curriculum for a particular Programme.

UG 7.4. The program of a study consists of the following components:

(i) Humanities and Social Sciences including Management courses
(ii) Basic Science courses
(iii) Engineering Science courses
(iv) Professional core courses
(v) Open Electives
(vi) Project work, seminar and internship
(vii) Mandatory/Audit Courses

UG 7.5. Every B. Tech. Programme shall have a curriculum and syllabi for the courses approved by the Board of Governors. Board of Studies will discuss and recommend the syllabi of all the under graduate courses offered by the department from time to time before sending the same to the Academic Council. Academic Council will consider the proposals from the Board of Studies and make recommendations to the Board of Management and Board of Governors for consideration and approval. For all approved courses, the copyright shall be with DSU.

UG 7.6. Every B. Tech. Programme shall have a curriculum and syllabi for the courses approved by the Board of Governors. Board of Studies will discuss and recommend the syllabi of all the under graduate courses offered by the department from time to time before sending the same to the Academic Council. Academic Council will consider the proposals from the Board of Studies and make recommendations to the Board of Management and Board of Governors for consideration and approval. For all approved courses, the copyright shall be with DSU.

UG 8. REGISTRATION

UG 8.1. Every candidate is required to register for approved courses through the assigned Faculty Advisor at the end of previous semester or first week of the current semester, as notified by the Academic Calendar.

UG 8.2. The Dean may cancel the registration of one or more courses if they are found to violate some rules or if there are restrictions imposed due to disciplinary reasons.

UG 8.3. The student is permitted to drop a course/s from the registered courses, within 4 weeks after the start of the Semester/Year as notified in the academic calendar, with the permission of Faculty Advisor and Chairperson / Dean / Principal of the respective School/College and no mention will be made in the grade card for dropped courses.

UG.8.4. The student is permitted to withdraw course/s from the registered courses, within 4 weeks before the start of the Semester/Year End Examinations as notified in the academic calendar, with the permission of Faculty Advisor and Chairperson / Dean / Principal of the respective School / College and Grade "W" will be awarded for course/s that were withdrawn.

UG 8.5. For the courses with "W" grade, the students should re-register subsequently when offered, either in MOOCS or in-class or summer term and fulfil the passing criteria to secure a grade in that course for change from "W" grade.

UG 8.6. Only those candidates shall be permitted to register who have:

(a) The academic eligibility to move to higher semesters (UG 9 & UG 11)
(b) Cleared all University, Hostel and Library dues and fines (if any) of the previous semesters,
(c) Paid all required advance payments of University and Hostel dues for the current semester,
(d) Not been debarred from registering on any specific ground.
(e) A minimum CGPA of 4 in the previous semesters

UG 9. EXAMINATION: ASSESSMENT CRITERIA & ELIGIBILITYFOR PROGRESSION

UG 9.1. The Continuous Internal Assessment (CIA), shall normally be conducted by the assessment components spread through the running semester; the components of CIA may be tests, mid-term exam, quiz, term paper, simulation-based problem solving, open-book test, solving open-end problems, mini-projects, seminars, viva-voce, awarding marks for attendance and such activities that enhance original thinking of students. The Course instructor shall announce the detailed methodology for conducting the various components of CIA together specifying component-wise weightages right in the commencement of each semester.

UG 9.2. The Semester End Examinations (SEE) shall be conducted at the end of each semester. The components may be a closed or open book examination, project demo, viva-voce, and/or a por presentation.

UG 9.3. and SEE shall respectively have 60:40 percent weightage. The Vice-Chancellor, on the recommendations of the Dean of Faculty and Department Chair, in exceptional cases, may approve the variation in this weightage ratio.

UG 9.4. The performance of a student with respect to a course in a semester shall be the combined score of marks/points, he/she secures in CIA and SEE, put together. A minimum of securing 40% marks, combining both the CIA with SEE marks secured with respect to a course, shall entail the student a PASS in the course. The Vice- Chancellor, in such cases where the entire class has fared poorly in the course, upon receiving a representation by the students / department, and based on the
recommendations of the committee constituted for the purpose, may review the criterion of 40%.

UG 9.5. ATTENDANCE ELIGIBILITY

UG 9.5.1. Candidates are required to attend all the classes (Lectures, Tutorials, Practical, Workshop Practice, etc.) for which they have been registered.

UG 9.5.2. The candidate shall not be allowed to appear for the end semester examination if his/her attendance falls below 85% in each course and shall be awarded a "NE" grade in that course.

UG 9.5.3. A provision for condonation of 10% of the attendance by the Vice-Chancellor on the specific recommendation of the chairman of the department and Dean, showing reasonable cause such as:

(a) Any medical emergencies/ illness where the candidate requires rest for the specified number of days certified by a Government Doctor only /any death in the family (near and dear ones).

(b) If the student represents the University in Sports/ Cultural Activities/Extra- curricular activities/Co-curricular activities.

(c) If a student presents a Paper in National/ International Conferences or attends any recognized Workshops/Seminars.

UG 9.5.4. If the period of leave is for a short duration (less than two weeks), prior application for leave shall have to be submitted to the Chairman of the Department concerned stating fully the reasons for the leave requested for along with supporting document(s). Such leave will be granted by the Chairman of the Department. However, the student shall comply with 9.5.2 and 9.5.3. of regulations.

UG 9.5.5. If the period of absence is likely to exceed two weeks, a prior application for grant of leave will have to be submitted through the Chairman of the Department to the Dean with supporting documents in each case. The decision to grant leave shall be taken by the Dean on the recommendation of the Chairman of the Department. However, the student shall comply with 9.5.2 and 9.5.3. of regulations.

UG 9.5.6. It shall be the responsibility of the candidate to intimate the concerned course instructor(s) regarding his/her absence before availing the leave.

UG 9.6. CONTINUOUS INTERNAL ASSESSMENT

UG 9.6.1. Candidate shall participate in all components of Continuous Internal Assessment (CIA) to become eligible to take up the Semester End Examination or else 'NE' grade shall be awarded. However, the Vice-Chancellor, under exceptional circumstances on the recommendations of Dean of Faculty and Department Chair, may exempt a student from participation in CIA component/s and permit taking up SEE.

UG 9.6.2. There shall be no marks improvement of Continuous Internal Assessment; however, the withdrawal and re-registering of the course shall be permitted.

UG 9.6.3. Continuous Evaluation consists of:

UG 9.6.3.1. Under normal circumstances for theory courses, total CIA weightage shall be a total of 60%, put together all components with varying weightages; Under exceptional circumstances with the approval of the Vice-Chancellor on the recommendation of Dean of the School, the weightage of CIA may be lower/higher than 60%.

The components of CIA may be tests, mid-term exam, quiz, term paper, simulation- based problem solving, open-book test, solving open-end problems, mini-projects, seminars, viva-voce, awarding marks for attendance and such activities that enhance original thinking of students.

UG 9.6.3.2. Under normal circumstances for the practical courses (laboratory, workshops, and any such hands-on activity), total CIA weightage shall be a total of 60%, put together all components with varying weightages; Under exceptional circumstances with the approval of the Vice-Chancellor on the recommendation of Dean of the School, the weightage of CIA may be lower/higher than 60%.

CIA may have components such as conduction of an experiment, record writing, viva- voce, tests, simulation, mid-term exam, quiz, demo, term paper, mini-projects, seminars, marks for attendance and activities which enhances original thinking of students.

UG 10. GRADING

UG 10.1. There shall be continuous assessment of a candidate's performance throughout the semester and grades shall be awarded by the concerned course instructor and/or the appropriate committee appointed for this purpose on the following basis.

UG 10.2. The grading will normally be based on CIA and SEE.

UG 10.3. Practical Courses/ Work Shop Practice: The evaluation will be based on instructor's continuous internal assessment, a test and end semester examination.

UG 10.4. The weightage assigned to different components of continuous internal assessment will be announced by the concerned instructor(s) in the beginning of the semester

UG 10.5. The results of performance of the candidates in the Continuous Internal assessment Test shall be announced by the instructors.

UG 10.6. In case of seminar, evaluation will be as determined by the grade awarding Committee (as per the Program scheme).

UG 10.7. Mini project /projects will be based on Continuous evaluation by Guide(s) and Semester End Examination (as per the Program scheme)

UG 10.8. The results of performance of the candidates shall be announced by the Controller of Examinations.

UG 10.9. METHOD OF AWARDING LETTER GRADES

UG 10.9.1. Relationships among Grades, Grade points and % of marks are listed in Table1.

UG 10.10. DESCRIPTION OF GRADES

UG 10.10.1. Table 1 shows the relationships among the grades, grade points and percentage of marks.

Table 1: Grade, Points, Grade Description and % of marks

GRADE	GRADE POINTS	DESCRIPTION	% MARKS
O	10	Outstanding	90 to 100
A+	9	Excellent	80 to 89
A	8	Very Good	70 to 79
B+	7	Good	60 to 69
B	6	Above Average	55 to 59
C	5	Average	50 to 54
P	4	Pass	40 to 49
F	0	Fail	< 40
AP	-	Audit Pass	-
AF	-	Audit Fail	-
IC	-	In Complete	-
NE	-	Not Eligible	-
W	-	Withdrawn	-

UG 10.10.2. A student will have to ensure a minimum CGPA of 4, to become eligible for the award of the degree.

UG 10.10.3. A candidate shall have to repeat all courses in which he/she obtains 'F' Grades until a passing grade is obtained.

UG 10.10.4. An IC grade denotes incomplete performance in any Theory and/or Practical Assessment. It may be awarded in case of absence on medical grounds or other special circumstances for SEE. Requests for IC grade should be made at the earliest but not later than the last day of SEE.

UG 10.10.5. The student can appear for the course/s with IC grade, when exams are conducted subsequently by the University for those Courses.

UG10.11. EVALUATION OF PERFORMANCE

UG10.11.1. The performance of a candidate shall be evaluated in terms of the Semester Grade Point Average (SGPA) which is the Grade Point Average for a semester, Cumulative Grade Point Average (CGPA) which is the Grade Point Average for all the completed semesters.

UG 10.11.2. The Earned Credits (EC) are defined as the sum of course credits for courses in which candidates have been awarded grades between O to P. (Table 1)

UG 10.11.3. Points earned in a semester = (Course credits X Grade point) for Grades O - P

UG 10.11.4. The SGPA is calculated on the basis of grades obtained in all courses, except audit courses and courses in which F grade or below, registered for in the particular semester.

$$\text{SGPA} = \frac{\text{Points secured in the semester (O – P Grades)}}{\text{Credits registered in the semester, excluding audit}}$$

UG 10.11.5. The CGPA is calculated on the basis of all pass grades, except audit courses. Cumulative points secured in all the passed courses (O – P Grades)

$$\text{CGPA} = \frac{}{\text{Cumulative registered credits, excluding audit}}$$

UG 10.12. WITHHOLDING OF GRADES

UG 10.12.1. Grades shall be withheld when the candidate has not paid his/her dues or when there is a disciplinary action pending against him/her

UG 10.13.1. Conversion formula for the conversion of CGPA into percentage is Percentage of Marks Scored = (CGPA Earned − 0.75) × 10

UG 11. PROMOTION CRITERIA AND ENROLLMENTS TO HIGHER SEMESTERS

UG 11.1. During registration to the higher semesters, the following criteria/conditions for promotion, shall be satisfied.

UG 11.1.1. A student shall 'Not Eligible' (NE) for writing SEE if he/she does not comply to the minimum prescribed attendance in any course that carry a credit.
Students shall register afresh for such course/s, whenever offered next, to meet the attendance requirements and secure a pass grade, subsequently in that course/s.

UG 11.1.2. In a semester (ODD / EVEN), a student is deemed to be Not Eligible (NE) if he/she does not satisfy minimum attendance requirements criteria in a credit course.
If this course happens to be a prerequisite to a connected course in the subsequent semester, then the student shall not be permitted to register for that connected course until he / she secures pass grade in the prerequisite course by complying to the minimum attendance requirement when the prerequisite course is offered next (either during summer term or regular semester).

UG 11.1.3. A student shall be permitted to register for FOUR credited courses or to a total of 16 credits whichever is higher along with pending audit courses, if any, during a summer term by paying the prescribed course registration fee per credit notified by the university from time to time.

UG 11.1.4. A student shall be permitted to register for FOUR credited courses or to a total of 16 credits whichever is higher along with pending audit courses, if any, during a summer term by paying the prescribed course registration fee per credit notified by the university from time to time.

UG 11.1.5. Candidates who secure 'F' grade in any courses in regular semester or summer term shall secure PASS grade in such course/s either in the subsequent summer term examination or shall repeat in the next appropriate semester whenever it is/they are offered, i.e. odd semester courses during odd semesters examinations and even semester courses during even semester examinations, respectively.

UG 11.2. In case of failure in Practical/Workshop practice course the candidate in any semester may clear it in the subsequent summer term examination or semester examination.

UG 11.3. In case a candidate fails in Practical/ Workshop practice he/she shall register when it is offered next either in the summer term or subsequent semester, as the case may be.

UG 11.4. Candidates may add and drop course(s) with the concurrence of the Faculty Advisor, and under intimation to the concerned course instructors and the academic section provided this is done within the date mentioned in the Academic Calendar.

UG 11.5. SUMMER TERM & MAKEUP EXAMINATIONS

UG 11.5.1. A summer term program may be offered by a department and with the approval of the Dean.

UG 11.5.2. Summer term courses will be announced by the Academic Affairs Office at the end of the even semester and before the commencement of the end semester examination. A candidate will have to register for summer term courses by paying the prescribed fees within the stipulated time in the announcement.

UG 11.5.3. The total number of contact hours in any summer term program will be the same as in the regular semester course. The assessment procedure in a summer term course will also be similar to the procedure for a regular semester course.

UG 11.5.4. Candidates granted semester drop by the Board of Governors, on medical ground, shall be allowed to clear the concerned courses in summer term course and subject to conditions as stated under clauses 11.5.1, 11.5.2.and 11.5.3.

UG 11.5.5. The Candidates with "NE" grade shall register for summer term by paying the prescribed fees.

UG 11.5.6. Candidates who are awarded 'F' grades in regular semester examinations have the option to register for the concerned courses in summer term examinations to the conditions as stated under clauses 11.5.1, 11.5.2.and 11.5.3above, or they can re-sit for subsequent semester/summer term examination only.

UG 11.5.7. Provision for make-up exam shall be available to the students who might have missed to attend the Semester / Annual end examinations of one or more courses for exceptional cases arising out of natural calamities / medical emergencies / death of a member in the family, with the permission of Faculty Advisor and Chairperson / Dean / Principal of the respective School/College. All such cases have to be exclusively to be approved by the Vice-Chancellor and ratified in the Academic Council / BOM / BOG. All such courses approved for makeup examinations are awarded a transitory grade "IC" (incomplete grade)

UG 11.5.8. The makeup examinations shall be held as notified in the academic calendar or through an exclusive notification duly approved by the Vice-chancellor.

UG 12. DURATION OF THE PROGRAMME

UG 12.1. Normally a candidate should complete all the requirements for under graduate Programme in four years. However, academically weaker candidates who do not fulfil some of the requirements in their first attempt and have to repeat them in subsequent semesters may be permitted up to eight consecutive years (from the first year of registration) to complete all the requirements of the degree.

UG 12.2. Normally a candidate under lateral entry should complete all the requirements for undergraduate Programme in three years. However, academically weaker candidates who do not fulfil some of the requirements in their first attempt and have
(from the second-year registration) to complete all the requirements of the degree.

UG 13. TERMINATION FROM THE PROGRAMME

UG 13.1. A candidate may also be compelled to leave the Program in the University on disciplinary grounds.

UG 13.2. On having been found to have produced false documents or having made false declaration at the time of seeking admission.

UG 13.3. On having been found to be pursuing regular studies and/or correspondence courses (leading to degree or diploma) in any other college, university or an educational institution simultaneously.

UG 13.4. On having been found to be concurrently employed and performing duty or carrying out business in contravention to academic schedules of the University and without seeking approval from the University.

UG 13.5. If a student fails to earn a pass grade even after 4 attempts such a student is terminated from the university on the grounds of NOT FIT FOR THE PROGRAM (NFFTP).

UG 13.6. If a student secures a CGPA less than 4.0, 4 times during entire duration of the program of study, such a student is terminated from the university on the grounds of NOT FIT FOR THE PROGRAM (NFFTP).

UG 13.7. However, if the student appeals for reconsideration of termination from the university under NFFTP rule by providing the guanine reasons to the Vice-Chancellor through the Dean of Faculty, then the Vice-Chancellor may consider constituting a committee for the purpose of review and provide 2 additional attempts on the recommendations of the committee.

UG 14. TEMPORARY WITHDRAWAL FROM THE UNIVERSITY

UG 14.1.1. He/she applies to the University within at least 6 weeks of the commencement of the semester or from the date he last attended his/her classes whichever is later, stating fully the reasons for such withdrawal together with supporting documents and endorsement of his/her guardian.

UG 14.1.2. The University is satisfied that, counting the period of withdrawal, the candidate is likely to complete his/her requirements of the B. Tech. Degree within the time limits specified in Clause 12.1 or 12.2 above.

UG 14.1.3. There are no outstanding dues or demands in the University/Hostel/Department/ Library.

UG 14.1.4. Normally, a candidate will be permitted only one such temporary withdrawal during his/her tenure as a candidate of the undergraduate programme.

UG 15. TRANSFER OF CANDIDATES

UG 15.1. Transfer of candidates from higher education institutions outside University shall be considered at the beginning of Third and Fifth Semesters but subject to confirmation of equivalence.

UG 15.2. The candidates shall apply for equivalence with the No-objection for admission to DSU from the University where they are perusing their study.

UG 15.3. The candidates must have passed in all courses in the earlier semesters prior to transfer.

UG 16. ELIGIBILITY FOR THE AWARD OF B. TECH. DEGREE

A candidate shall be declared to be eligible for the award of B. Tech. degree if he/she has:

UG 16.1. Completed all the credit requirements for the degree with a CGPA 4.0 or higher at the end of the Programme.

UG 16.2. Satisfactorily completed all the mandatory audit courses.

UG 16.3. No dues to the University, Department, Hostels.

UG 16.4. No disciplinary action pending against him/her.

UG 17. AWARD OF DEGREE

The award of B. Tech. degree must be recommended by the Academic Council and approved by the Board of Management and Board of Governors of the DSU.

UG 18. CONDUCT AND DISCIPLINE

UG 18.1. Candidates shall conduct themselves within and outside the precincts of the University in a manner befitting the candidates of an institution of national importance. The University has a separate ordinance Code and Conduct of Candidates which is applicable to all candidates of the University.

UG 19. REPEAL AND SAVINGS

Notwithstanding anything contained in these Regulations, the provisions of any guidelines, orders, rules or regulations in force at the University shall be inapplicable to the extent of their inconsistency with these Regulations. The Academic Council, Board of Management and Board of Governors of Dayananda Sagar University may revise, amend or change the regulations from time to time.

UG 20. INTERPRETATION

Any questions as to the interpretation of these Regulations shall be decided by University, whose decision shall be final. The University shall have the powers to issue clarifications to remove any doubt, difficulty or anomaly which may arise during the implementation of the provisions of these regulations

Department of Computer Science and Engineering (Cyber Security)

VISION

Ignite and nurture young learners to provide a sustainable, humane, and research-centric educational platform in the domain of cybersecurity for building a robust, resilient, and attack-free digital universe.

MISSION

1. Provide committed and competent faculty and educational infrastructure to impart the theoretical and practical foundation of cybersecurity in the emanating youth.
2. Establish MoUs and Centre of Excellences (CoEs) with Information Technology Sector to provide industry-ready cybersecurity graduates with research instinct imbibed for the sustainable development of young learners
3. Build collaborative and teamwork-centric project-oriented learning environment, to address global challenges whilst preserving human and ethical values.

Encourage young minds to educate society to restore nationwide human safety and security in digital world.

PROGRAM OUTCOMES (PO'S):

A graduate of Computer Science and Engineering (Cyber Security) program will demonstrate:

PO1- Engineering Knowledge: Apply knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

PO2- Problem Analysis: Identify, formulate, research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO3- Design/Development of Solutions: Design solutions for complex engineering problems and design system components or processes that meet specified needs with appropriate consideration for public health and safety, cultural, societal, and environmental considerations.

PO4- Conduct Investigations of Complex Problems: Use research-based knowledge and research methods, including design of experiments, analysis and interpretation of data, and synthesis of information to provide valid conclusions.

PO5- Engineering Tool Usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools, including prediction and Modeling, to complex engineering activities with an understanding of limitations.

PO6- The Engineer and The World: Apply reasoning informed by contextual knowledge to assess societal, health, safety, legal, and cultural issues and the consequent responsibilities relevant to professional engineering practice.

PO7-Ethics: Apply ethical principles and commit to professional ethics, responsibilities, and norms of engineering practice (including diversity and inclusive behavior).

PO8-Individual and Collaborative Team Work: Function effectively as an individual, and as a member or leader in diverse teams and in multidisciplinary settings.

PO9-Communication: Communicate effectively on complex engineering activities with the engineering community and 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.

PO10- Project Management and Finance: Demonstrate knowledge and understanding of engineering 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.

PO11:Life-long Learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change

PSOs

1. Ability to understand, analyse and develop computer programs in the areas related to networking, cryptography, web development and database management by adhering software development life cycle.

2. Graduate students will be able to develop data, resource, and asset protection strategies for organizations, processes, peoples, and individuals through Cybersecurity-centric skills

SEMESTER-1

SL. NO	PROGRAM CODE	Course code	COURSE TITLE	SCHEME OF TEACHING					Duration in Hrs Exam	Examination (Maximum Marks)		
				L	T	P	J	C		CIE	SEE	TM
1	101-105, 121-123 & 141	23EN1101	LINEAR ALGEBRA AND DIFFERENTIAL EQUATIONS	3	0	0	0	3	3	60	40	100
2	101-105, 121-123 & 141	23EN1102	ENGINEERING CHEMISTRY	2	0	2	0	3	3	60	40	100
3	101-105, 121-123 & 141	23EN1103	INTRODUCTION TO MECHANICAL ENGINEERING	2	0	2	0	3	3	60	40	100
4	101-105, 121-123 & 141	23EN1104	INTRODUCTION TO ELECTRICAL ENGINEERING	2	0	0	0	2	3	60	40	100
5	101-105, 121-123 & 141	23EN1105	C PROGRAMMING FOR PROBLEM SOLVING	2	1	2	0	4	3	60	40	100
6	101-105, 121-123 & 141	23EN1106	ENGINEERING MECHANICS	2	0	0	0	2	3	60	40	100
7	101-105, 121-123 & 141	23EN1107	TECHNICAL ENGLISH	2	0	0	0	2	1	100	-	100
8	101-105, 121-123 & 141	23EN1108	ENVIRONMENTAL SCIENCE	1	0	0	0	1	1	50	-	50
9	101-105, 121-123 & 141	23EN1109	KANNADA KALI / MANASU	1	0	0	0	0	1	50	-	50
			TOTAL	17	1	6	0	20		560	240	800

L – Lecture, T – Tutorial, P – Practical, J – Project, C – No. of Credits, CIE – Continuous Internal Evaluation,
SEE- Semester End Examinations, TM – Total Marks

SL	PROGRAM CODE	COURSECODE	COURSE TITLE	SCHEME OF TEACHING					Duration of exam	Examination (Maximum Marks)		
				L	T	P	J	C		CIE	SEE	TM
1	101-105, 121-123 & 141	23EN1101	LINEAR ALGEBRA AND DIFFERENTIAL EQUATIONS	3	0	0	0	3	3	60	40	100
2	101-105, 121-123 & 141	23EN1110	ENGINEERING PHYSICS	3	0	2	0	4	3	60	40	100
3	101-105, 121-123 & 141	23EN1111	INTRODUCTION TO ELECTRONICS ENGINEERING	3	0	0	0	3	3	60	40	100
4	101-105, 121-123 & 141	23EN1112	C PROGRAMMING FOR PROBLEM SOLVING	2	1	2	0	4	3	60	40	100
5	101-105, 121-123 & 141	23EN1113	ENGINEERING GRAPHICS AND DESIGN THINKING	2	0	2	0	3	3	60	40	100
6	101-105, 121-123 & 141	23EN1114	BIOLOGY FOR ENGINEERS	2	0	0	0	2	1	100	-	100
7	101-105, 121-123 & 141	23EN1115	CONSTITUTION OF INDIA AND PROFESSIONAL ETHICS	1	0	0	0	1	1	50	-	50
TOTAL				16	1	6	0	20	17	450	200	650

L – Lecture, T – Tutorial, P – Practical, J – Project, C – No. of Credits, CIE – Continuous Internal Evaluation,
SEE- Semester End Examinations, TM – Total Marks.

SEMESTER-II

SL	PROGRAM CODE	COURSE CODE	COURSE TITLE	SCHEME OF TEACHING					Duration in Hrs Exam	Examination (Maximum Marks)		
				L	T	P	J	C		CIE	SEE	TM
1	101-105, 121-123 & 141	23EN1201	SINGLE AND MULTIVARIATE CALCULUS	3	0	0	0	3	3	60	40	100
2	101-105, 121-123 & 141	23EN1202	OBJECT ORIENTED PROGRAMMING	2	1	2	0	4	3	60	40	100
3	101-105, 121-123 & 141	23EN1102	ENGINEERING CHEMISTRY	2	0	2	0	3	3	60	40	100
4	101-105, 121-123 & 141	23EN1103	INTRODUCTION TO MECHANICAL ENGINEERING	2	0	2	0	3	3	60	40	100
5	101-105, 121-123 & 141	23EN1104	INTRODUCTION TO ELECTRICAL ENGINEERING	2	0	0	0	2	3	60	40	100
6	101-105, 121-123 & 141	23EN1106	ENGINEERING MECHANICS	2	0	0	0	2	3	60	40	100
7	101-105, 121-123 & 141	23EN1107	TECHNICAL ENGLISH	2	0	0	0	2	1	100	-	100
8	101-105, 121-123 & 141	23EN1108	ENVIRONMENTAL SCIENCE	1	0	0	0	1	1	50	-	50
9	101-105, 121-123 & 141	23EN1109	KANNADA KALI / MANASU	1	0	0	0	0	1	50	-	50
TOTAL				17	1	6	0	20		560	240	800

L – Lecture, T – Tutorial, P – Practical, J – Project, C – No. of Credits, CIE – Continuous Internal Evaluation, SEE- Semester End Examinations, TM – Total Marks.

SCHEME - B.TECH – 2023-24 ONWARDS II SEM - PHYSICS CYCLE

SL	PROGRAM CODE	COURSE CODE	COURSE TITLE	SCHEME OF TEACHING					Contact Hours /Week	Examination (Maximum Marks)		
				L	T	P	J	C		CIE	SEE	TM
1	101-105, 121-123 & 141	23EN1201	SINGLE AND MULTIVARIATE CALCULUS	3	0	0	0	3	3	60	40	100
2	101-105, 121-123 & 141	23EN1202	OBJECT ORIENTED PROGRAMMING	2	1	2	0	4	3	60	40	100
3	101-105, 121-123 & 141	23EN1110	ENGINEERING PHYSICS	3	0	2	0	4	3	60	40	100
4	101-105, 121-123 & 141	23EN1111	INTRODUCTION TO ELECTRONICS ENGINEERING	3	0	0	0	3	3	60	40	100
5	101-105, 121-123 & 141	23EN1113	ENGINEERING GRAPHICSAND DESIGN THINKING	2	0	2	0	3	3	60	40	100
6	101-105, 121-123 & 141	23EN1114	BIOLOGY FORENGINEERS	2	0	0	0	2	01	100	-	100
7	101-105, 121-123 & 141	23EN1115	CONSTITUTION OF INDIA AND PROFESSIONAL ETHICS	1	0	0	0	1	01	50	-	
			TOTAL	16	1	6	0	20	17	450	200	650

L – Lecture, T – Tutorial, P – Practical, J – Project, C – No. of Credits, CIE – Continuous Internal Evaluation, SEE-Semester End Examinations, TM – Total Marks.

Definitions / Descriptions

Definition of Credit:	
1 Hour Lecture (L) Per Week	01 Credit
1 Hour Tutorial (T) Per Week	01 Credit
1 Hour Practical (P) Per Week	0.5 Credit
1 Hour Project (J) Per Week	0.5 Credit

Course code and Definition:	
BSC	Basic Science Courses
ESC	Engineering Science Courses
HSMC	Humanities and Social Sciences including Management Courses
IPCC	Integrated Professional Core Course
PCC	Professional Core Courses
PEC	Professional Elective Courses
OEC	Open Elective Courses
SEC	Skill Enhancement Courses
UHV	Universal Human Value Course
PROJ	Project Work
INT	Internship

Implementation of National Education Policy (NEP) 2020 for the B. Tech students of Batch 2023-2027

The implementation of Curriculum follows NEP 2020 and addresses the following features and categories of courses:

1. Student Centric flexible curriculum.
2. Inter-disciplinary Courses,
3. Multi-disciplinary Courses,
4. Ability Enhancement Courses,
5. Skill Enhancement Courses,
6. Value Added Courses,
7. Product Design and Development,
8. Internship (Rural Internship, Industry Internship, Research/Development Internship), and
9. Multiple Exit and Multiple Entry

    - Certificate in Engineering after completion of first year.
    - Diploma in Engineering after completion of second year.
    - Advanced Diploma in Engineering after completion of third year.
    - Degree in Engineering after completion of fourth year.

III SEMESTER													
S.N.	Course Type	Course Code	Course Name	Teaching Department	Teaching Hours / Week				Examination				credits
					Lecture	Tutorial	Practical	Project	Duration in Hours	CIE Marks	SEE Marks	Total Marks	
					L	T	P	J					
1	BSC	23CY2301	Transforms and Numerical Techniques	MAT	3	0	0	0	03	60	40	100	**3**
2	IPCC	23CY2302	Data Structures	CSE(CY)	3	0	2	0	03	60	40	100	**4**
3	IPCC	23CY2303	Digital Logic Design	ECE	3	0	2	0	03	60	40	100	**4**
4	PCC	23CY2304	Discrete Mathematics and Graph Theory	CSE(CY)	3	0	0	0	03	60	40	100	**3**
5	PCC	23CY2305	Introduction to Computer Networks	CSE(CY)	3	0	2	0	03	60	40	100	**4**
6	AEC	23LSXXXX	Liberal Studies	Any Dept.	1	0	0	0	01	50	--	50	**1**
7	TPC	23CY2306	Cognitive and Technical Skills-I	TPO	2	0	0	0	01	100	--	100	**2**
			Total		**18**	**0**	**6**	**0**		**450**	**200**	**650**	**21**

Liberal Studies	
Course Code	**Course Name**
23LS0001	Drama
23LS0002	Dance
23LS0003	Music
23LS0004	Photography
23LS0005	Introduction to Japanese language
23LS0006	Law for Engineers
23LS0007	Canvas Painting
23LS0008	Communication in Sanskrit
23LS0009	Vedic Mathematics
23LS0010	Critical Thinking
23LS0011	Introduction to Film Studies
23LS0012	Yoga & Meditation
23LS0013	Cyber Crimes, Policies & Laws
23LS0014	Holistic Medicine
23LS0015	3-D Modelling using Tinkercad
23LS0016	Brief Introduction to Psychology **
23LS0017	Innovation to Design**
23LS0018	Introduction to Indian Art- An Appreciation **
23LS0019	Body Language: Key to Professional Success **
23LS0020	Stress Management **
23LS0021	Water, Society and Sustainability **
23LS0022	Business Fundamentals for Entrepreneurs (Part 1: Internal Operation) **
23LS0023	Moral Thinking: An Introduction to VALUES and Ethics**
23LS0024	Gender Justice and Workplace Security**

sn

IV SEMESTER														
S. N.	Course Type	Course Code	Course Name	Teaching Department	Teaching hours/Week			Examination					Credits
					Lecture	Tutorial	Practical	Project	Duration in Hours	CIE Marks	SEE Marks	Total Marks	
					L	T	P	J					
1	BSC	23CY2401	Probability & Statistics	MAT	3	0	0	0	03	60	40	100	3
2	IPCC	23CY2402	Design and Analysis of Algorithms	CSE(CY)	3	0	2	0	03	60	40	100	4
3	IPCC	23CY2403	Database Management System	CSE(CY)	3	0	2	0	03	60	40	100	4
4	IPCC	23CY2404	Introduction to Cyber Security	CSE(CY)	3	0	0	0	03	60	40	100	3
5	PCC	23CY2405	Cyber Forensics and Cyber Law	CSE(CY)	3	0	0	0	03	60	40	100	3
6	PCC	23CY2406	Computer Organization and Architecture	CSE(CY)	3	0	0	0	03	60	40	100	3
7	TPC	23CY2407	Cognitive and Technical Skills-II	TPO									P/F
			Total		**20**	**0**	**4**	**0**		**460**	**240**	**700**	**22**

V SEMESTER													
SN	**Course Type**	**Course Code**	**Course Name**	**Teaching Department**	**Teaching hours/Week**				**Examination**				**Credit**
					Lecture	**Tutorial**	**Practical**	**Project**	**Duration in Hours**	**CIE Marks**	**SEE Marks**	**Total Marks**	
					L	**T**	**P**	**J**					
1	PCC	23CY3501	Introduction to Automata and Complier Design	CSE	3	0	2	0	03	60	40	100	**4**
2	PCC	23CY3502	Security Engineering and Project Management	CSE(CY)	3	0	0	0	03	60	40	100	**3**
3	IPCC	23CY3503	Operating Systems	CSE	3	0	2	0	03	60	40	100	**4**
4	PCC	23CY3504	Cryptography and Network Security	CSE(CY)	3	0	2	0	03	60	40	100	**4**
5	PCC	23CY3505	Security Operations and Cyber Défense	CSE(CY)	3	0	0	0	03	60	40	100	**3**
6	PEC-1	22CY35XX	Professional Elective Course – I	CSE(CY)	3	0	0	0	03	60	40	100	**3**
7	SEC	23CY35XX	Skill Enhancement -I	CSE(CY)	1	0	2	0	01	100	-	100	**2**
8	TPC	23CY35XX	Cognitive and Technical Skills-III	TPO	**-**	**-**	**-**	**-**	-	-	-	-	**P/F**
					19	**0**	**8**	**0**		**460**	**240**	**700**	**23**

Professional Elective Course– I	
Course Code	**Course Name**
23CY3506	Wireless Security
23CY3507	Secure Coding
23CY3508	Big Data
23CY3509	Database Security
Skill Enhancement Course– I	
Course Code	**Course Name**
23CY3510	Introduction to IPR and Registration
23CY3511	Full Stack Development

VI SEMESTER													
SN	**Course Type**	**Course Code**	**Course Name**	**Teaching Department**	**Teaching hours/Week**				**Examination**				**Credits**
					Lecture	**Tutorial**	**Practical**	**Project**	**Duration in Hours**	**CIE Marks**	**SEE Marks**	**Total Marks**	
					L	**T**	**P**	**J**					
1	IPCC	23CY3601	Innovation and Entrepreneurship	CSE(CY)	2	0	0	0	03	60	40	100	**2**
2	PCC	23CY3602	Cloud Security	CSE(CY)	3	0	2	0	03	60	40	100	**4**
3	PCC	23CY3603	Tools and Techniques for Ethical Hacking	CSE(CY)	3	0	2	0	03	60	40	100	**4**
4	OEC-1	230EXXXX	Open Elective – I	CSE(CY)	3	0	0	0	03	60	40	100	**3**
5	PEC-2	23CY36XX	Professional Elective Course – II	CSE(CY)	3	0	0	0	03	60	40	100	**3**
6	PEC-3	23CY36XX	Professional Elective Course – III/ MOOC Course	CSE(CY)	3	0	0	0	03	60	40	100	**3**
7	SEC	23CY36XX	Skill Enhancement -II	CSE(CY)	1	0	2	0	01	100	-	100	**2**
8	TPC	23CY36XX	Cognitive and Technical Skills-IV	TPO	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**P/F**
					18	**0**	**6**	**0**		**460**	**240**	**700**	**21**

Open Elective – I	
Course Code	**Course Name**
23OE0028	Cyber Security Essentials
23OE0029	Network Security Essentials

Professional Elective Course– II	
Course Code	**Course Name**
23CY3604	Telecommunication Security
23CY3605	Application Security
23CY3606	Internet of Things
23CY3607	Image Processing and Data Privacy

Professional Elective Course– III / MOOC Course	
Course Code	**Course Name**
23CY3608	Blockchain Technology
23CY3609	Cyber Ethics, Privacy and Legal Issues
23CY3610	MOOC COURSE (As per the courses listed on the NPTEL/ SWAYAM platform as designated by the department)
23CY3611	Hardware Security

Skill Enhancement Course– II	
Course Code	**Course Name**
23CY3612	Universal Human Values
23CY3613	Research Writing

VII SEMESTER													
SN	**Course Type**	**Course Code**	**Course Name**	**Teaching Department**	**Teaching hours/Week**				**Examination**				
					Lecture	**Tutorial**	**Practical**	**Project**	**Duration in Hours**	**CIE Marks**	**SEE Marks**	**Total Marks**	**Credit**
					L	**T**	**P**	**J**					
1	IPCC	23CY4701	Risk Assessment and Security Audit	CSE(CY)	3	0	0	0	03	60	40	100	**3**
2	PROJOM	23CY4702	Capstone Project _Phase I	CSE(CY)	0	0	0	12	03	60	40	100	**6**
2	OEC-2	23OEXXXX	Open Elective II	CSE(CY)	3	0	0	0	03	60	40	100	**3**
3	PEC-4	23CY47XX	Professional Elective Course – IV	CSE(CY)	3	0	0	0	03	60	40	100	**3**
4	PEC-5	23CY47XX	Professional Elective Course – V	CSE(CY)	3	0	0	0	03	60	40	100	**3**
					12	**0**	**0**	**12**		**300**	**200**	**500**	**18**

Professional Elective Course– IV	
Course Code	Course Name
23CY4703	Vulnerability Management and Penetration Testing
23CY4704	Endpoint Security
23CY4705	IoT and IIoT Security
23CY4706	Operating Systems Security

Professional Elective Course– V	
Course Code	**Course Name**
23CY4707	Quantum Cryptography
23CY4708	Disk & Memory Forensics
23CY4709	Big Data Security
23CY4710	Embedded System Security

Open Elective – II	
Course Code	**Course Name**
23OE0053	Cryptography
23OE0054	Digital Forensics*

VIII SEMESTER												
S. N	**Course Type**	**course Code**	**Course** Name	**Teaching Department**	**Teaching Hours / Week**				**Examination**			**Credits**
					Lecture	**Tutorial**	**Practical**	**Project**	**CIE Marks**	**SEE Marks**	**Total Marks**	
					L	**T**	**P**	**J**				
1	PROJ	23CY4801	Capstone Project-Phase II	Resp. Dept.	0	0	0	20	60	40	100	**10**
2	INT	23CY4802	Research Internship/ Industry Internship	Resp. Dept.	-	-	-	6	100	-	100	**3**
3	PCC	23CY4803	Leadership, Policy & Authentic Intelligence, Societal Impact Engineering	Resp. Dept.	2	0	0	0	100	–	100	**2**
			Total		**0**	**0**	**0**	**26**	**260**	**40**	**300**	**15**

SEMESTER	**I**					
YEAR	**I**					
COURSE CODE	**22EN1101**					
TITLE OF THE COURSE	**LINEAR ALGEBRA & DIFFERENTIAL EQUATIONS**					
SCHEME OF INSTRUCTION	Lecture Hours (L)	Tutorial Hours (T)	Practical Hours (P)	Project Hours (J)	Total Hours	Credits
	3	-	-	-	39	3

COURSE OBJECTIVES:

- Understanding basic concepts of linear algebra to illustrate its power and utility through applications to science and Engineering.
- Apply the concepts of vector spaces, linear transformations, matrices and inner product spaces in engineering.
- The course is discussed with algebraic as well as geometric perspectives.
- Solve problems in cryptography, computer graphics and wavelet transforms.

COURSE OUTCOMES:

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	Apply the abstract concepts of matrices and system of linear equations using decomposition methods	L3
CO2	Implement the basic notion of vector spaces and subspaces	L3
CO3	Apply the concept of vector spaces using linear transforms which is used in computer graphics and inner product spaces	L3
CO4	Applications of linear transforms in computer graphics and imaging	L3
CO5	Applications of orthogonality in various domains	L3

COURSE CONTENT:

MODULE 1	**8Hrs**
Linear algebra: Introduction - The Geometry of Linear Equations - Row reduction and echelon forms- Rank of a matrix - Gaussian Elimination - Solution sets of linear equations – LU decomposition - Inverse of a matrix by Gauss-Jordan method.	
MODULE 2	**8Hrs**
Vector spaces and subspaces: Linear spaces – Subspaces - Linear independence – Span - Bases and Dimensions -Finite dimensional vector spaces, Fundamental subspaces associated with a matrix.	

MODULE 3	**9Hrs**
Linear transformations and orthogonality: Linear transformations – Basic properties - Invertible linear transformation - Matrices of linear transformations - Vector space of linear transformations – Inner Product, Orthogonal Vectors - Projections onto Lines - Projections and Least Squares - The Gram-Schmidt Orthogonalization process, QR Factorization.	
MODULE 4	**7Hrs**
Eigenvalues and eigenvectors: Introduction to Eigenvalues and Eigenvectors - Diagonalization of a Matrix- Diagonalization of symmetric matrices - Quadratic forms.	
MODULE 5	**7Hrs**
Differential equations: Linear second order ordinary differential equation with constant coefficients – Solutions of homogenous and non-homogenous equations - Method of undetermined coefficients – method of variation of parameters – Solutions of Cauchy-Euler and Cauchy-Legendre differential equations.	

TEXT BOOKS:

1. D C Lay, S R Lay and JJ McDonald, Linear Algebra and its Applications, Pearson India, Fifth edition.
2. Linear Algebra and its Applications by Gilbert Strang, 4 th Edition, Thomson Brooks/Cole, Second Indian Reprint 2007.
3. Introductory Linear Algebra- An applied first course, Bernard Kolman and David, R. Hill, 9th Edition, Pearson Education, 2011.
4. Thomas' Calculus, George Thomas, D. Weir and J. Hass, 2014, 13th edition, Pearson.

REFERENCES:

1. Introduction to Linear Algebra, Gilbert Strang, 5th Edition, Cengage Learning (2015).
2. Higher Engineering Mathematics by B S Grewal, 42 nd Edition, Khanna Publishers.
3. Elementary Linear Algebra, Stephen Andrilli and David Hecker, 5th Edition, Academic Press (2016).
4. Contemporary linear algebra, Howard Anton, Robert C Busby, Wiley 2003.
5. Practical Linear Algebra, Farin and Hansford, CRC Press (2013).

****

SEMESTER	**I/II**					
YEAR	**I**					
COURSE CODE	**22EN1103**					
TITLE OF THE COURSE	**ENGINEERING CHEMISTRY**					
SCHEME OF INSTRUCTION	L	T	P	J	Total Hours	Credits
	3	-	2	-	39(L)+26(P) = 65	4

COURSE OBJECTIVES:

- To provide chemical concepts most relevant to engineering students and demonstrate them in an applied context.
- To expose to the principles required to understand important contemporary topics like alternate energy sources, corrosion control, polymer technology, phase equilibria nanomaterials and green chemistry and catalysis.
- To emphasize on applications of these concepts to real world problems

COURSE OUTCOMES:

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	Appreciate the basic principles of electrochemistry, use of different types of electrodes in analysis and evaluate cell potential for different cell reactions.	L2
CO2	Know construction, working and applications of various energy storage devices such as batteries, fuel cells and supercapacitors.	L2
CO3	Understand basic principles of corrosion and apply suitable techniques for corrosion control. Also know the technological importance and processes involved in metal finishing.	L3
CO4	Know the synthesis, structure –property relationship and applications of commercially important polymers and polymer composites. Understand properties and applications of nanomaterials. Also learn the principles of green chemistry for a sustainable and eco-friendly world	L3
CO5	Differentiate various instrumental techniques involved in determining chemical reactions	L3

COURSE CONTENT:	
MODULE 1	**8Hrs**
Chemical energy source: Introduction to energy; Fuels - definition, classification, importance of hydrocarbons as fuels; Calorific value-definition, Gross and Net calorific values (SI units). Determination of calorific value of a solid / liquid fuel using Bomb calorimeter. Numerical problems on GCV&NCV. Petroleum cracking-fluidized catalytic cracking. Reformation of petrol. octane number, cetane number, anti-knocking agents, power alcohol, Biodiesel & Biogas. **Solar energy:** Thermal energy: Photovoltaic cells- Introduction, definition, importance, working of PV cell. Solar grade silicon physical and chemical properties relevant to photo-voltaics, doping of silicon by diffusion technique.	

MODULE 2	8Hrs
Energy science and technology: Single electrode potential - Definition, origin, sign conventions. Standard electrode potential- Definition-Nernst equation expression and its Applications. EMF of a cell- Definition, notation and conventions. Reference electrodes– Calomel electrode, Ag/AgCl electrode. Measurement of standard electrode potential. Numerical problems on EMF. Ion-selective electrode- glass electrode **Battery technology:** Basic concepts including characteristics of anode, cathode, electrolyte and separator. Battery characteristics. Classification of batteries–primary, secondary and reserve batteries. State of the art Batteries-Construction working and applications of Zn-air, Lead acid battery, Nickel-Metal hydride and Lithium ion batteries. Introduction to fuel cells, types of fuel cells. Construction, working and application of Methanol-Oxygen fuel cell.	
MODULE 3	**8Hrs**
Corrosion science: Definition, Chemical corrosion and Electro-chemical theory of corrosion, Types of corrosion, Differential metal corrosion, Differential aeration corrosion (pitting and water line corrosion), Stress corrosion. Corrosion control, Metal Coatings-Galvanization, Tinning and its disadvantages. Cathodic protection of Corrosion: Sacrificial anode method and current impression method. **Surface Modification Techniques:** Definition, Technological importance of metal finishing. Significance of polarization, decomposition potential and over-voltage in electroplating processes, Electroless Plating. Distinction between electroplating and Electroless plating, advantages of electroless plating. Electroless plating of copper.	
MODULE 4	**8Hrs**
High Polymers: Introduction to polymers, Glass transition temperature, structure and property relationship. Synthesis, properties and applications of Teflon. PMMA. Elastomers - Deficiencies of natural rubber and advantages of synthetic rubber. Synthesis and application of silicone rubber, Conducting Polymers-Definition, mechanism of conduction in polyacetylene. Structure and applications of conducting polyaniline. **Nanotechnology:** Introduction, properties, synthesis by sol-gel. Fullerenes, Carbon nanotubes, dendrimers and nano-composites.	
MODULE 5	**7Hrs**
Water Technology: Impurities in water. Hardness of Water: Types of Hardness and determination of total hardness of water by using disodium salt of ethylenediaminetetraacetic acid method, Potable water treatment by Electro dialysis and Reverse Osmosis. Water analysis- Biochemical oxygen demand and Chemical oxygen demand. Determination of COD. Numerical problems on COD. Sewage treatment. **Instrumental Methods of Analysis:** Instrumental methods of analysis, Principles of spectroscopy- Beer's Lamberts law, Difference between spectrometer and spectrophotometer, Potentiometry, Conductometry (Strong acid against strong base, weak acid against strong base, mixture of strong acid and a weak acid against strong base).	

List of Laboratory/Practical Experiments activities to be **26Hrs**

Volumetric Analysis and Preparations

Evaluation of quality of water in terms of total hardness by Complexometric titration.

Determination of Chemical Oxygen Demand (COD) of the given industrial waste water sample.

Determination of Alkalinity of the given water sample

Preparation of MgO nanoparticles by solution combustion method (Demonstration experiment) and spectrometric analysis.

Electroless plating of copper (Demo experiment) Preparation of Polyaniline (Demo experiment)

Instrumental methods of Analysis

Potentiometric titration–Estimation of FAS using standard $K_2Cr_2O_7$ solution.

Conductometric estimation of hydrochloric acid using standard sodium hydroxide solution

Determination of viscosity coefficient, surface tension, density of a given liquid

Colorimetric estimation of copper in a given solution

Determination of Pka of given weak acid.

Determination of calorific value of coal/oil using Bomb calorimeter (Group

TEXT BOOKS:

1. Dr. S. Vairam, Engineering Chemistry, Wiley-India Publishers, 2017
2. S. S. Dara and S. S. Umare, "A Textbook of Engineering Chemistry", S. Chand & Company LTD, New Delhi, 2015

REFERENCES:

1. Prasanta Rath, "Engineering Chemistry", Cengage Learning India PVT, LTD, Delhi, 2015
2. Shikha Agarwal, "Engineering Chemistry-Fundamentals and Applications", Cambridge University Press, Delhi, 2015
3. Dayanada Sagar University laboratory manual
4. J. Bassett, R.C. Denny, G.H. Jeffery, Vogel's, Text book of quantitative inorganic analysis, 4th edition

****

Dayananda Sagar University

School of Engineering
Deverakaggalahalli, Harohalli, Bengaluru 562112

SEMESTER	**I/II**					
YEAR	**I**					
COURSE CODE	**22EN1104**					
TITLE OF THE COURSE	**ELEMENTS OF MECHANICAL ENGINEERING**					
SCHEME OF INSTRUCTION	L	T	P	J	Total Hours	Credits
	2	-	2	-	26(L)+26(P) = 52	3

COURSE OBJECTIVES:

The course will enable the students to

- Acquire a basic understanding of renewable energy resources and basic concepts of hydraulic turbines.
- Acquire knowledge of various engineering materials and metal joining techniques.
- Acquire essential knowledge of modern manufacturing tools and techniques.
- Acquire knowledge on basics of refrigeration and air-conditioning.
- Explain about the cooling of electronic devices.
- Acquire knowledge of basic concepts of mechatronics and robotics.
- Explain about the electric and hybrid vehicles.

COURSE OUTCOMES:

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	Describe basic concepts of renewable energy resources and power generation	L2
CO2	Distinguish various engineering materials and metal joining techniques	L2
CO3	Demonstrate different modern manufacturing tools and techniques	L3
CO4	Make use of basic concepts of refrigeration and air- conditioning concepts	L3
CO5	Illustrate essential knowledge of basic concepts of mechatronics and robotics	L2
CO 6	Comprehend the important concepts of electric and hybrid vehicles	L2

COURSE CONTENT:	
MODULE 1 Energy Sources and Power Generation	**10 Hrs**
Review of energy sources: Construction and working of Hydel power plant, Thermal power plant, Nuclear power plant, Solar power plant, Tidal power plant, Wind power plant. Principle and Operation of Hydraulic turbines, Pelton Wheel, Francis Turbine and Kaplan Turbine. Working of Centrifugal Pump & reciprocating pump. **Thermodynamics:** System, boundary, surroundings, types of systems, Zeroth law, First and second laws of thermodynamics, Efficiency, COP, Carnot theorem	
MODULE 2 Engineering Materials and Metal Joining Processes	**10 Hrs**
Metals-Ferrous: Tool steels and stainless steels. Non-ferrous /metals: aluminum alloys. **Ceramics-** Glass, optical fiber glass, cermets. **Composites-** Fiber reinforced composites, Metal matrix Composites.	
Smart materials- Piezoelectric materials, shape memory alloys, semiconductors, and super-insulators. **Metal Joining Processes:** Fitting, Sheet metal, Soldering, brazing and Welding: Definitions. Classification and methods of soldering, brazing, and welding. Brief description of arc welding, Oxy- acetylene welding, Introduction to TIG welding and MIG welding.	
MODULE 3 Modern Manufacturing Tools and Techniques	**12 Hrs**
CNC: Introduction, components of CNC, advantages and applications of CNC, CNC Machining centres and Turning Centers Concepts of Smart Manufacturing and Industrial IoT. **Additive Manufacturing:** Introduction to reverse Engineering, Traditional manufacturing vs Additive Manufacturing, Computer aided design (CAD) and Computer aided manufacturing (CAM) and Additive Manufacturing (AM), Different AM processes, Rapid Prototyping, Rapid Tooling, **3D printing:** Introduction, Classification of 3D printing process, Applications to various fields.	
MODULE 4 Thermal Systems and Management	**10 Hrs**
Heat in Electronic Devices: Modes of Heat Transfer, heat generation in electronics, temperature measurement, heat sink, Cooling of electronic devises: Active, Passive, and Hybrid Cooling. **Refrigeration:** Principle of refrigeration, Refrigeration effect, Ton of Refrigeration, COP, Refrigerants and their desirable properties. Principles and Operation of Vapor Compression and Vapor absorption refrigeration. Applications of Refrigerator. **Air-Conditioning:** Classification and Applications of Air Conditioners. Concept and operation of Centralized air conditioning system.	
MODULE 5 Advanced Technologies	**10 Hrs**
Mechatronics: Introduction, Concept of open-loop and closed-loop systems, Examples of Mechatronic systems and their working principle. **Robotics:** Introduction, Robot anatomy, Joints & links, common Robot configurations. Applications of Robotics in Material Handling, Processing, Assembly, and Inspection. **Electric and Hybrid Vehicles:** Introduction, Components of Electric and Hybrid Vehicles, Drives and Transmission. Advantages and disadvantages of EVs and Hybrid vehicles.	

List of Laboratory/Practical Experiments activities to be conduct

Demonstration on Principle and Operation of any one Turbo-machine
Demonstration on pumps
Visit any one Conventional or Renewable Energy Power Plant and prepare a comprehensive report.
One exercises each involving Fitting and Sheet metal.
One exercises each involving welding and Soldering.
Study oxy-acetylene gas flame structure and its application to gas welding
Demonstration on Principle and Operation of CNC machine.
Demonstration on Principle and Operation of 3D printing process.
Demonstration of anyone Heat transfer application device and prepare a comprehensive report.
Demonstration of anyone air conditioning system.
Demonstration of the machine consists of Gear Trains.
Demonstration of various elements of mechatronic system.
Demonstration of any one model of Robot

TEXT BOOKS:

1. Basic and Applied Thermodynamics, P.K.Nag, Tata McGraw Hill 2nd Ed., 2002
2. Non-Conventional Energy Sources, G.D Rai, Khanna Publishers, 2003
3. Elements of Workshop Technology (Vol. 1 and 2), Hazra Choudhry and Nirzar Roy, Media Promoters and Publishers Pvt. Ltd., 2010
4. Thermal Management in Electronic Equipment, HCL Technologies, 2010
5. Robotics, Appu Kuttan KK K. International Pvt Ltd, volume 1

REFERENCES:

- An Introduction to Mechanical Engineering, Jonathan Wickert and Kemper Lewis, Third Edition, 2012
- Turbo Machines, M. S. Govindegowda and A. M. Nagaraj, M. M. Publications 7Th Ed, 2012
- Manufacturing Technology- Foundry, Forming and Welding, P.N. Rao Tata McGraw Hill 3rd Ed., 2003.
- Thermal Management of Microelectronic Equipment, L. T. Yeh and R. C. Chu, ASME Press, New York, 2002
- Fundamentals of Robotics: Analysis and Control, Robert J. Schilling, Pearson Education (US).

SEMESTER	**I/II**					
YEAR	**I**					
COURSE CODE	**22EN1105**					
TITLE OF THE COURSE	**INTRODUCTION TO ELECTRICAL ENGINEERING**					
SCHEME OF INSTRUCTION	L	T	P	J	Total Hours	Credits
	3	**-**	**-**	**-**	**39**	**3**

COURSE OBJECTIVES:

This course enables students:

- To impart basic knowledge of electrical quantities such as current, voltage, power and energy
- To distinguish between passive and active electrical components
- To explain the general structure of electrical power system
- To define basic laws of electric circuit and to solve related problems
- To understand basics of earthing, protective devices and wiring
- To introduce concepts, analogies and laws of magnetic circuits
- To learn the working principle, construction and characteristics of various DC machines
- To study the construction, principle of operation and types of transformers
- To understand the working principles of measuring equipment.

COURSE OUTCOMS:

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	Explain the basic knowledge about the Electric and Magnetic circuits.	L2
CO2	Analyze the working of various Electrical Machines.	L3
CO3	Applying basic laws and determine various circuit parameters in AC and DC Circuits.	L3
CO4	Explain the construction, basic principle of operation, applications and determine performance parameters of various measuring instruments.	L2
CO5	Outline the knowledge of Green Energy, Electrical Safety Rules & standards course.	L3

COURSE CONTENT:	
MODULE 1	**8Hrs**
ELECTRICAL CIRCUIT CONCEPTS: Voltage and current sources: independent, dependent, ideal and practical; V-I relationships of resistor, ohm's law, inductor, and capacitor; types of electrical circuits, voltage and current divider rule, Kirchhoff's laws, Peak, average and rms values of ac quantities; apparent, active and reactive powers; phasor analysis, Power factor, impedance and admittance, power and energy in electrical elements, introduction to3 phase systems.	
MODULE 2	**8Hrs**
MAGNETIC CIRCUIT CONCEPTS: Basics of magnetic circuits, laws of magnetism, magnetic field, magnetic lines of force, permeability, Electromagnetic Fields: Relation between field theory and circuit theory; numerical on capacitance calculations, Biot-Savart's law, Ampere's law, Curl, Faraday's law, Lorentz force, Inductance, Self and Mutual inductance of simple configurations.	
MODULE 3	**8Hrs**
DC MACHINES AND TRANSFORMERS: DC Machines: Basic principles of electromagnetic energy conversion, Construction, operation, characteristics, performance, of dc generators and motors, testing of dc machines, applications, Transformers: Construction, working principle, equivalent circuit, voltage regulation, efficiency, Auto-transformers.	
MODULE 4	**8Hrs**
SI units, systematic and random errors in measurement, expression of uncertainty - accuracy and precision index, propagation of errors. General working principles andconstruction of indicating instruments. Electro-magnetic Instruments for the measurement of current, voltage, power and energy. Instruments for the measurementof power factor, frequency, Potentiometers. CRO, Calibration of instruments; importance, procedures and standards.	
MODULE 5	**7Hrs**
POWER STATION PRACTICES, ECONOMICS, AND GREEN ENERGY CONCEPTS: Energy generation-Conventional generation of electrical energy using thermal, hydro, nuclear and, non-conventional sources of energy; overview on green energy technology, load forecasting, electricity tariffs, power factor improvement, power plant economics, Overview on electrical safety standards in industries	

TEXT BOOKS:

1. D.P.Kothari and I.J. Nagrath, "Basic Electrical Engineering", 4th Edition, Tata McGrawHill, 2010
2. B.L Thereja and A.K Thereja, "A text book of Electrical Technology (Vol III)(Transmission, distribution, and Utilization)", 23rd Edition, S Chand and Company

REFERENCES:

1. Clayton Paul, Syed A Nasar and Louis Unnewehr, 'Introduction to ElectricalEngineering', 2nd Edition, McGraw-Hill, 1992
2. P.S. Dhogal, 'Basic Electrical Engineering – Vol. I& II', 42nd Reprint, McGraw-Hill, 2012.
3. K Sawhney, A course in Electrical and Electronic Measurements andInstrumentation Dhanpat Rai & Co. (P) Limited January 2015
4. NPTEL - https://nptel.ac.in/courses/108/108/108108076/

****

DAYANANDA SAGAR UNIVERSITY

Dayananda Sagar University

School of Engineering
Deverakaggalahalli, Harohalli, Bengaluru 562112

SCHOOL OF ENGINEERING

SEMESTER	**I**					
YEAR	**I**					
COURSE CODE	**22EN1102**					
TITLE OF THE COURSE	**C PROGRAMMING FOR PROBLEM SOLVING**					
SCHEME OF INSTRUCTION	L	T	P	J	Total Hours	Credits
	2	**-**	**2**	**-**	**26(L)+26(P) = 52**	**3**

COURSE OBJECTIVES:

- To develop student competence in writing clear, correct, and maintainable programs that implement known algorithms.

COURSE OUTCOMES:

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	Express algorithms learned implicitly in school explicitly in algorithmic form and calculate the number of basic operations (exact or upper bound).	L3
CO2	Trace the execution of short programs/code fragments involving fundamental programming constructs.	L4
CO3	Write a short program/code fragment for a given task using fundamental programming constructs.	L3
CO4	Debug a short program/code fragment with fundamental programming constructs manually, and debug more complex code using a modern IDE and associated tools.	L4
CO5	Design a large program, conduct a personal code review, and contribute to a small-team code review focused on common coding errors and maintainability using a provided checklist.	L3

COURSE CONTENT:

MODULE 1	**7 Hrs**
Basics and overview of C: Introduction to Problem Solving using Algorithms and Flowchart: Key features of Algorithms: Sequence, Decision, Repetition with examples. Background, structure of C program, keywords, Identifiers, Data Types, Variables, Constants, Input / Output statements, Operators (Arithmetic, relational, logical, bitwise etc.), Expressions, Precedence and Associativity, Expression Evaluation, Type conversions. Conditional Branching Statements-if and switch statements, iterative statements (loops)-while, for, do-while statements, Loop examples, Nested loops, break, continue, go to statement.	

MODULE 2	**5 Hrs**
Arrays: Introduction, declaration & initialization of array, reading and writing array elements, Operations on array: Traversal, searching, sorting. Declaration and Initialization of two-dimensional arrays. Matrix Operations (addition, subtraction, multiplication, transpose) using two-dimensional array.	
Strings: definition, declaration, initialization, and representation. String handling functions and character handling functions.	
MODULE 3	**6 Hrs**
Pointers: Definition and declaration and initialization of pointers. Accessing values using pointers. Accessing array elements using pointers. **Functions:** Definition and declaration. Built-in functions and User-defined functions. Categories of functions with example. Pointers as function arguments, array as function argument, Call-by-value and call-by-reference. Recursion.	
MODULE 4	**4 Hrs**
Structures: Purpose and usage of structures. Declaration of structures. Assignment with structures. Structure variables and arrays. Nested structures. Student and employee database implementation using structures. **Unions**: Declaration and initialization of a union. Difference between structures and unions. Example programs.	
MODULE 5	**4 Hrs**
Memory allocation in C programs: Dynamic memory allocation, memory allocation process, allocating a block of memory, releasing the used space, altering the size of allocated memory. **Files**: Defining, opening and closing of files. Input and output operations.	

List of Laboratory/Practical Experiments activities to be conducted
1. Design a C program to Swapping of two numbers. (Simple Expressions).
2. Design a C program to find the simple interest as per the below conditions (Simple expressions, Integer division issues (data loss), Explicit typecasting, when p, t, rare integers and si is float.
3. Design a C program to find the largest of 3 numbers. a) Using if and no else. (Conditionals) b) Using nested if. (conditionals and Boolean expressions) c) Using Ladder if else if d) Using Ternary operator.
4. Design a program that takes three coefficients (a, b, and c) of a Quadratic equation (ax2+bx+c=0) as input and compute all possible roots.
5.Design a C program to read the vehicle type (Use c or C for car, b or B for bus, t or T for Tempo for vehicle type) and Duration of customer vehicle parked in parking slot. Parking fare is calculated as per the rates given below: print the total parking charges.

Vehicle	First Rate	Second Rate
Car	Rs 20/hr for first 2hr	Rs 30/hr for next
Bus	Rs 40/hr for first 2hr	Rs 50/hr for next
Tempo	Rs 30 /hr for first 2hr	Rs 40/hr for next

6. a Write a program to calculate the factorial of a given number.
b Write a program using four functions to check if the given number is a palindrome.

7.a Sum of natural numbers (sum(n) = n + sum(n-1);).

b. Write a program to calculate Power of a number ($b^n = b * b^{n-1}$).

8. a. Write a program to calculate nth Fibonacci number given first two numbers in the series.

Inputs	N	Output
0,1	3	2
1,5	4	11
2,4	7	42
8,1	5	19
3,5	6	34

b. Write a program to calculate GCD of two numbers.

9. Write a program to emulate a calculator with the following operations: Addition, Subtraction, Multiplication, Division – using functions, switch and break.)

10. Write a program using four functions to compute the sine of a value using Taylor's series approximation - pass by value.

11. Write a program to find the sum of n different using four functions and arrays.
Use the following function prototype:
void input(int n, int a[n]);
int add(int n, int a[n]);
void output(int n, int a[n],int sum) and main().

12. Write a program to add two matrices using separate function for input, add matrices, display matrix and main function.

13. String handling:
a) Write a function to reverse the string in reverse and display it. (Strings))
b) Write a function to concatenate the two strings without using strcat.(Strings)
c) Write a function to find the length of the string.

14. Write a program using Bubble sort technique to sort an array of integer elements (Sorting technique, Const array arguments.)

15. Write a program to search an array of elements of data type requested by the user for a given item using binary search algorithm. (Searching technique, Const array arguments).
16. Write a program with functions to add and multiply two complex numbers. Define a structure Complex to represent a complex number. The main function should call other functions for the purposes of input, computations and display. (Structs as arguments).
17. Define a structure, student, to store the following data about a student: rollno (integer), name (string) and marks(integer) . Your program must contain the following functions: (Array of Structures). · A function to read the students data. · A function to display records of each student. · A function to sort the records of student Rank Wise · A function prints all students details · A function to search student details by Rollno · A function to print the names of the students having the highest test score

TEXT BOOKS:

1. Brian W. Kernigham and Dennis M. Ritchie, (2012) "The C Programming Language", 2nd Edition, PHI.
2. ReemaThareja, "Programming in C". Oxford University Press, Second Edition, 2016

REFERENCES:

1. R. S Bichkar, "Programming with C and Data Structure", University Press, 2014
2. Behrouz A. Forouzan, Richard F. Gilberg, "Computer Science - A Structured Approach Using C", Cengage Learning, 2007
3. Brian W. Kernigham and Dennis M. Ritchie, "The C Programming Language", 2nd Edition, PHI, 2012
4. Vikas Gupta, "Computer Concepts and C Programming", Dreamtech Press 2013.

****

SEMESTER	**I/II**					
YEAR	**I**					
COURSE CODE	**22EN1106**					
TITLE OF THE COURSE	**BIOLOGY FOR ENGINEERS**					
SCHEME OF INSTRUCTION	L	T	P	J	Total Hours	Credits
	3	-	-	-	**39**	**3**

COURSE OBJECTIVES:

- To introduce students to basics modern biological concepts with an emphasis on how bio-processes are analogous to engineering field, as a multidisciplinary field.
- To make students understand basic engineering principles imminently run physiological processes particularly about engineering designs and solutions are arrived citing body functional examples.
- To motivate students of engineering that many bio-solutions could be foundational to design, develop better processes, products and useful to achieve quality of life.

COURSE OUTCOMES:

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	Student appreciates and explains the biological mechanisms of living organisms from the perspective of engineers and find solutions to solve bio-engineering problems with appropriate tools.	L2
CO2	Explain optimal designs in engineering that are bio-mechanical in nature and build and use by observing and understanding bio-physiological processes involved in sensing, locomotion, and knowledge application of range of bio-chemicals.	L3
CO3	Demonstrate that bio-chemical, bio-sensory, bio-processes could be path-finders to optimise similarities for functional aspects of electronic, computer, mechanical, electrical machines	L3

COURSE CONTENT:	
MODULE 1	**8Hrs**
Biomimetics: Biology for Engineers, Body Fluid: Blood- Mechanics of heart, Blood pressure, Life molecules: Water, Carbohydrates, Proteins, Lipids and Nucleic acids, Biomimetics: Bio-processes - engineering analogies	
MODULE 2	**8Hrs**
Bioenergy: Unit of life: Human and Plant cell, Metabolism: Enzymes as Bio-catalysts and physiological entities, Development- Bioenergy from Sun-Photosynthesis	

MODULE 3	8Hrs
Biomechanics (Human Body Movement Mechanics): Normal Human Movement: Force-Vector of Body; Movement Angles; Muscle contraction -Relaxation; Posture – Static & Dynamic; Ideal and abnormal posture, Practical: Stepping-Lifting-Sit-Stand.	

MODULE 4	8 Hrs
Bioelectronics: Brain & Computer: Senso-neural networks, IoT as applied to biology, Bionic Eye: Mechanism of Vision, Electronic Nose: Bio-olfactory mechanisms (Science of smell), Impulses: Cardiac and Nerve, Biological Clock, Circadian rhythm	
MODULE 5	**7 Hrs**
Biopharma: Metabolic syndromes, Cancer and its diagnostics, Lab on a chip, Bio-Sensors, Drug Discovery	

REFERENCES:

- Campbell, N. A.; Reece, J. B.; Urry, Lisa; Cain, M, L.; Wasserman, S. A.; Minorsky, P. V.; Jackson, R. B. Pearson. "Biology: A global approach", , Global Edition, 10/E, 2014
- David Nelson, Michael Cox. "Lehninger Principles of Biochemistry". W H Freeman & Company, Seventh Edition, 2017.
- Janine M Benvus. "Biomimicry: Innovation inspired by Nature". William Morrow Paperbacks, 2002.
- Lecture Notes, PPT slides by course instructor.

****

SEMESTER	**I/II**					
YEAR	**I**					
COURSE CODE	**22EN1107**					
TITLE OF THE COURSE	**CONSTITUTION OF INDIA AND PROFESSIONAL ETHICS**					
SCHEME OF INSTRUCTION	L	T	P	J	Total Hours	Credits
	1	**-**	**-**	**-**	**13**	**1**

COURSE OBJECTIVES:

This course enables students:

- To provide basic information about Indian constitution.
- To identify individual role and ethical responsibility towards society.

COURSE OUTCOMS:

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	Understand state and central policies, fundamental duties.	L2
CO2	Understand Electoral Process, special provisions.	L2
CO3	Understand powers and functions of Municipalities, Panchayats and Cooperative Societies.	L2
CO4	Understand Engineering ethics and responsibilities of Engineers	L2

COURSE CONTENT:	
MODULE 1:	**7Hrs**
Introduction to the Constitution of India, the making of the constitution and salient features of the constitution. Preamble to the Indian constitution fundamental rights & its limitations. Directive principles of state policy & relevance of directive principles state. Policy fundamental Duties.	
MODULE 2	**6Hrs**
Union Executives – President, Prime Minister, Parliament, Supreme Court of India. State Executives – Governor Chief Minister, State Legislature High Court of State. Electoral Process in India, Amendment Procedures, 42nd, 44th, 74th, 76th, 86th & 91st amendments. Special provision for SC & ST, special provision for Women, children & backward classes, Emergency provisions. Powers and functions of municipalities, panchyats and co – operative Societies.	

TEXT BOOKS:

1. Brij Kishore Sharma," Introduction to the Constitution of India", PHI Learning Pvt. Ltd., New Delhi, 2011.
2. Durga Das Basu: "Introduction to the Constitution on India", (Students Edn.) Prentice Hall, 19th / 20th Edn., 2001.

REFERENCES:

1. M.V. Pylee, "An Introduction to Constitution of India", Vikas Publishing, 2002.

****

SEMESTER	**I/II**					
YEAR	**I**					
COURSE CODE	**22EN1109**					
TITLE OF THE COURSE	**KANNADA KALI**					
SCHEME OF INSTRUCTION	L	T	P	J	Total Hours	Credits
	1	**-**	**-**	**-**	**13**	**1**

COURSE OBJECTIVES:

This course enables students:

- To introduce Kannada language & culture to Non – Kannada speakers.
- To train them to communicate in colloquial Kannada with connivance.

COURSE OUTCOMS:

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	The learners can communicate in Kannada & acquaint themselves with Kannada culture.	L2

COURSE CONTENT:	
MODULE 1:	**7Hrs**
Introduction to Karnataka & Kannada Culture, Evolution of Kannada. Introduction to Kannada Alphabets. Introduction to Kannada Numbers.	
MODULE 2	**6Hrs**
Kannada words, sentences & phrase making for colloquial communication.	

REFERENCES:

1. Kannada Kali –Dr. Lingadevaru Halemane
2. Kannada Paatagalu– Editor: Dr. Chandrashekara Kambara.
3. SLN Sharma & K Shankaranarayana "Basic Grammar", Navakarnataka Publications.
4. Spoken Kannada. Publication: Kannada Sahitya Parishat Bengaluru.

SEMESTER	**II**					
YEAR	**I**					
COURSE CODE	**22EN1201**					
TITLE OF THE COURSE	**SINGLE AND MULTI VARIABLE CALCULUS**					
SCHEME OF INSTRUCTION	L	T	P	J	Total Hours	Credits
	3	-	-	-	39	3

COURSE OBJECTIVES:

- To analyze and solve constrained and unconstrained optimization problems.
- To understand the meaning of the definite integral both as a limit of Riemann sums and as the net accumulation of a rate of change.
- To find volumes of solids by calculating appropriate double integrals in rectangular and polar coordinates.
- To relate rectangular coordinates in 3-space to spherical and cylindrical coordinates.
- To evaluate triple integrals and use them to find volumes in rectangular, cylindrical and spherical coordinates.
- To evaluate line integrals of curves and vector fields and interpret such quantities as work done by a force.
- To use Green's theorem to evaluate line integrals along simple closed contours on the plane.
- To apply Stoke's theorem to compute line integrals along the boundary of a surface.
- To apply Divergence theorem to evaluate surface integral.
- To have a good foundation of Sequences of Bounded, Monotonic and Convergence.

COURSE OUTCOMES:

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	Understand basic calculus concept such as limit, continuity and derivatives	L2
CO2	Compute partial derivatives and use it to give polynomial approximation of functions in several variables	L3
CO3	Apply calculus concepts to solve real-world problems such as optimization and related rates problems	L3
CO4	Evaluate integrals of functions or vector-related quantities over curves, surfaces, and domains in two- and three-dimensional space	L5
CO5	Apply Fundamental Theorem of Line Integrals, Green's Theorem, Stokes' Theorem, or Divergence Theorem to evaluate integrals	L3
CO6	Distinguish between the concepts of sequence and series, and determine limits of sequences and convergence and approximate sums of series	L3

COURSE CONTENT:	
MODULE 1	**9Hrs**
Differential Calculus: Functions of two or more variables: Definition, Region in a plane, Level curves, Level surfaces, Limits, Continuity, Partial derivatives, Differentiability, Gradients, Directional derivatives, Normals to level curves and tangents, Extreme values and saddle points, Lagrange multipliers. **Self-Learning Component:** Single variable calculus	
MODULE 2	**9Hrs**
Integral calculus: Double integral and iterated integrals - Cartesian and polar coordinates, Volume of solids of revolution, Triple integral, Change of variables, Multiple integrals in cylindrical and spherical coordinates.	
MODULE 3	**9Hrs**
Vector Calculus: Line Integrals, Vector Fields, Work, Circulation and flux, Path independence, Potential functions, and Conservative fields, Green's theorem in the plane, Surface area and surface integrals, Surface area of solid of revolution, Parametrized surfaces, Stokes' theorem, The Divergence theorem.	
MODULE 4	**6Hrs**
Sequence and Series, I: Sequences of real numbers and their convergence criteria, Infinite series, Sequence of partial sums, Tests for convergence/divergence - n^{th} term test, Boundedness and monotonicity, Integral, Condensation, Comparison, Ratio and root tests	
MODULE 5	**6Hrs**
Sequence and Series II: Alternating series, Absolute and conditional convergence, Rearrangement theorem, Power series, Taylor and Maclaurin series (one and two variables)	

TEXT BOOKS:

1. Thomas' Calculus, George B. Thomas, D. Weir and J. Hass, 2014, 13th edition, Pearson.
2. Erwin Kreyszig, Advanced Engineering Mathematics, 2015, 10th Edition, Wiley India.

REFERENCES:

1. Higher Engineering Mathematics, B.S. Grewal, 2015, 43rd Edition, Khanna Publishers.
2. Higher Engineering Mathematics, John Bird, 2017, 6 th Edition, Elsevier Limited.
3. Calculus: Early Transcendentals, James Stewart, 2017, 8 th edition, Cengage Learning.
4. Engineering Mathematics, K.A. Stroud and Dexter J. Booth, 2013, 7 th Edition, Palgrave Macmillan.
5. Basic Multi Variable Calculus, Marsden, Tromba and Weinstein, W.H. Freeman, Third Edition

****

SEMESTER	**I/II**					
YEAR	**I**					
COURSE CODE	**22EN1109**					
TITLE OF THE COURSE	**ENGINEERING PHYSICS**					
SCHEME OF Instruction	L	T	P	J	Total Hours	Credits
	3	-	2	-	39(L)+26(P)=65	4

COURSE OBJECTIVES:

- To introduce the basic concepts of Quantum mechanics which are essential in understanding and solving problems in engineering,
- To understand Band structure of solids, Semiconductors and electrical conductivity of SC's, and their applications.
- To explain semiconductor devices like LED, Photodiode and Solar cell and Semiconductor BJT.
- To review different types of Engineering materials –Electronic, electrical, mechanical and Magnetic materials and Dielectric material Properties and their applications in Science and Engineering.
- Classify the magnetic materials based on susceptibility and their temperature dependence
- To understand different crystal systems and determine structure by miller-indices
- To explain Thin-film Phenomena, Thin-film fabrication Process and their applications in engineering.
- To learn how to fabricate Nano materials by using Top-down and Bottom–up approach& To review Nano science and technology and its practical applications in biology, engineering and medicine.

COURSE OUTCOMEs:

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	Describe the concepts of Quantum mechanics and applications of Schrodinger time independent wave equation in one dimension	L1
CO2	Illustrate Semiconductors, Semiconductor devices like Photodiode, LED, Solar cell and BJT and its applications	L3
CO3	Distinguish the different engineering materials such as Electronic, electrical and mechanical materials properties and their applications in engineering	L2
CO4	Apply the concept of magnetism to magnetic data storage devices.	L3

CO5	Classify Lattice parameters of different crystalline solids by using X-ray diffraction methods and its applications in science and engineering.	L2
O6	Interpret Basic concepts of thin films and thin film deposition processes and their applications leads to Sensors and engineering devices	L3
CO7	Categorize Nano materials, Properties, and fabrication of Nano materials by using Top-down and Bottom –up approach's - Applications for Science and technology	L2

COURSE CONTENT:

MODULE1	**8Hrs**

Quantum Mechanics: Foundations of quantum theory, wave function and its properties, de-Broglie hypothesis, Heisenberg uncertainty principle, one dimensional time independent Schrodinger wave equation, eigen values and eigen functions, applications: one dimensional motion of an electron in a potential-well.

LASER PHYSICS: Introduction to lasers, conditions for laser action, requisite of a laser system principle, construction and working of Nd-YAG and semiconductor laser, application of lasers in defense (LASER range finder), engineering (data storage) and applications of LASERS in medicine.

MODULE 2	**8Hrs**

Semiconductor Physics: Band structure, Fermi level in intrinsic and extrinsic semiconductors, Density of energy states in conduction and valence bands of a semiconductor (Mention the expression), Expression for concentration of electrons in conduction band (Derivation), Hole concentration in valance band (Mention the expression), Intrinsic carrier concentration, Conductivity of semiconductors, Hall effect, Numericals.

Semiconducting devices for optoelectronics applications: - Principle and working of LED, photodiode, Solar cell, BJT.

MODULE 3	**8Hrs**

Dielectrics: Introduction – Dielectric polarization **–** Dielectric Polarizability, Susceptibility and Dielectric constant - Types of polarizations: Electronic, Ionic and Orientation polarizations (qualitative) – Lorentz Internal field (Expression only) – Claussius - Mossoti equation (derivation) – Applications of Dielectrics – Numericals.

Magnetic Materials: Introduction - Magnetic dipole moment - Magnetization-Magnetic susceptibility and permeability - Classification of magnetic materials: Dia, para, Ferro, antiferro & Ferri magnetic materials - Domain concept for Ferromagnetism & Domain walls (Qualitative) - Hysteresis - soft and hard magnetic materials - Engineering applications.

MODULE 3	8Hrs

Crystallography: Lattice, unit cell, lattice parameters, crystal systems, Bravais lattices, Packing fraction for SCC, BCC and FCC crystal systems. Introduction to Miller Indices. Determination of Crystal structure by Miller Indices. Expression for Inter-planar distance. X-ray diffraction, Bragg's law and Determination of Crystal structure by Powder method. Numericals.

Mechanical Engineering Materials – mechanical properties: stress- strain curve for different materials. Introduction to Tensile strength, Compressive strength, Ductility, Toughness, Brittleness,
Impact strength, Fatigue, Creep. Testing of engineering materials: Hardness Tests: Brinell and Vickers hardness test.

MODULE 5	7Hrs

Thin films technology: Introduction to thin-films-Advantages of thin-films over bulk materials. Thin film deposition processes- Physical vapour deposition (Thermal evaporation technique, and sputtering technique) process, Applications of Thin films.

Nano Science &technology: Introduction to Nano materials, Classification of nano materials, Size dependent properties of materials, Top-down and Bottom-up approach- Ball-milling and Photolithography, Process. Fundamental Principles of Biophysics & Applications of Nano technology inBiology and Engineering.

List of Laboratory/Practical Experiments activities to be conduct

I-V characteristics of a Zener Diode

I–V Characteristics of a Zener diode in forward and reverse bias condition (Module 2)

Planck's constant

Measurement of Planck's constant using LED (Module 2)

Transistor characteristics

Input and output characteristics of a NPN transistor in C-E configuration (Module2)

Dielectric constant

Determination of dielectric constant of a dielectric material (Module 2)

Torsional Pendulum

Determination of moment of inertia of a circular disc using torsional pendulum

Diffraction grating

Determination of wavelength of a laser light using diffraction grating (Module 4)

LCR series and parallel resonance

Study the frequency response of a series and parallel LCR circuit (Module 3)

TEXT BOOKS:

1. S. M. Sze, Semiconductor devices, Physics and Technology, Wiley. Publishing
2. Engineering Physics (2019), DSU Pearson, New Delhi.

REFERENCES:

1. M. Young (1977), Optics & Lasers An Engineering Physics approach, Springer
2. K.L. Chopra, Thin film Phenomena, McGraw Hill, New York.
3. S. O. Pillai (2018), Solid State Physics, revised edition, New Age International Publishers, New Delhi
4. M N Avadhanulu, P G Kshirsagar, TVS Arun Murthy (2018), A textbook of Engineering Physics, S Chand, New Delhi.

SEMESTER	**I/II**					
YEAR	**I**					
COURSE CODE	**222EN1110**					
TITLE OF THE COURSE	**ENGINEERING MECHANICS**					
SCHEME OF Instruction	L	T	P	J	Total Hours	Credits
	3	-	-	-	39	3

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	Understand free body diagrams and principle of statics	L2
CO2	Analyze structures using concept of equilibrium conditions considering effect of frictional forces	L4
CO3	Describe the centroid and moment of inertia of composite geometrical sections	L2
CO4	Calculate axial forces in members of determinate truss	L3
CO5	Demonstrate plane kinematics and kinetics of particles/rigid bodies	L3

COURSE OBJECTIVES:

The course will enable the students to

- Explain different types of forces, equilibrium conditions and related theorems
- Illustrate Couples and equivalent force couple system and related problems
- Explain concepts of friction and their relevance in Engineering problems
- Describe centroid, center of gravity, moment of inertia and mass moment of inertia and their relevance in Engineering problems
- Describe Trusses and its classification
- Determine axial forces in members of Planar determinate Truss

Illustrate various concepts in dynamics and related problems COURSE OUTCOMES:

COURSE CONTENT:	
MODULE 1	**9Hrs**
Introduction to Engineering Mechanics: Introduction to Engineering Mechanics, Force Systems Basic concepts, Particle Equilibrium in 2-D & 3-D; Rigid Body equilibrium; System of Forces, Coplanar Concurrent Forces, Resultant- Moment of Forces and its Application; Couples and Resultant of force System, Equilibrium of System of Forces, Free body diagrams, Equations of Equilibrium.	
MODULE 2	**8Hrs**
Friction: Introduction, Types of friction, Limiting friction, Cone of Friction, Laws of Friction, Static and Dynamic Friction; Motion of Bodies, wedge friction, Ladder friction, related problems.	
MODULE 3	**8Hrs**
Centroid, Centre and gravity and Moment of inertia: Introduction, Centroid of simple figures from first principle, centroid of composite sections; Centre of Gravity and its implications; Area moment of inertia Definition, Moment of inertia of plane sections from first principles, Theorems of moment of inertia, Moment of inertia of standard sections and composite sections; Mass moment inertia of circular plate, Cylinder and Prism.	
MODULE 4	**7 Hrs**
Analysis of Truss: Introduction, Classification of trusses, Equilibrium in two and three dimension; Method of Sections; Method of Joints; To determine if a member is in tension or compression; Simple Trusses; Zero force members.	
MODULE 5	**8 Hrs**
Dynamics: Introduction, Rectilinear motion; Plane curvilinear motion (rectangular path, and polar coordinates); Projectile motion, Basic terms, general principles in dynamics; Types of motion, motion and simple problems; D Alembert's principle and its applications in plane motion and connected bodies.	

TEXT BOOKS:

1. Irving H. Shames (2006), Engineering Mechanics, 4th Edition, Prentice Hall publications.
2. A Nelson (2009), Engineering Mechanics: Statics and dynamics, Tata McGraw Hill publications.

REFERENCES:

1. F. P. Beer and E. R. Johnston (2011), Vector Mechanics for Engineers, Vol I - Statics, Vol II, –
2. Dynamics, 9th Ed, Tata McGraw Hill publications.
3. R.C. Hibbler (2006), Engineering Mechanics: Principles of Statics and Dynamics, Pearson Press.
4. Bansal R.K.(2010), A Text Book of Engineering Mechanics, Laxmi Publications.
5. H.J. Sawant, S.P Nitsure(2018), Elements of Civil Engineering and Engineering
6. Mechanics, Technical Publications.

****

Dayananda Sagar University

School of Engineering

Deverakaggalahalli, Harohalli, Bengaluru 562112

SEMESTER	**I/II**					
YEAR	**I**					
COURSE CODE	**22EN1111**					
TITLE OF THE COURSE	**INTRODUCTION TO ELECTRONICS**					
SCHEME OF INSTRUCTION	L	T	P	J	Total Hours	Credits
	3	**-**	**-**	**-**	**39**	**3**

COURSE OBJECTIVES:

This course enables students:

- To introduce the concepts of fundamentals of semiconductor devices with the basic knowledge of the flow of current in semiconductor devices such as diodes and transistors
- To Explain the characteristics of various semiconductor devices and the concept of Integrated circuits
- To understand the principles of electronic circuits for operations of energy conversions from AC to DC, noise removal and building the required power supply
- To understand how a particular electronic device can increase the power of a signal and also to be acquainted with gain calculations
- To implement the Boolean functions and to realize basic logic gate operations and logic functions
- To understand the basics of communication system, to modify the characteristics of carrier signals according to the information signals
- To study the fundamentals of electromagnetic waves
- To identify and understand the different blocks present in transmitter and receiver.
- To describe various parameters of Op-Amp, its characteristics and specifications.
- To understand the various applications of Op-Amp.

COURSE OUTCOMS:

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	Explain the fundamentals of semiconductor devices, analog and digital circuits	L2
CO2	Design and analyze the behavior of analog and digital circuits.	L3
CO3	Outline the overview of communication systems and oscillators. Solve various kinds of numerical problems.	L3
CO4	Develop the analog and digital circuits using simulation tool	L3

COURSE CONTENT:

MODULE 1 **8Hrs**

Semiconductor Diodes: Semiconductor materials- intrinsic and extrinsic types, Ideal Diode. Terminal characteristics of diodes: p-n junction under open circuit condition, p-n junction under forward bias and reverse bias conditions, p-n junction in breakdown region, Zener diode, Series voltage regulator, Rectifier Circuits: Half wave and full wave, Reservoir and smoothing circuits.

MODULE 2	8Hrs
Transistors: Introduction, Transistor construction, operation and characteristics; Configuration types: Common base and common emitter configuration, Active region operation of transistor, Transistor amplifying action, Biasing the BJT: fixed bias, emitter feedback bias, collector feedback bias and voltage divider bias, Transistor as a switch: cut-off and saturation modes. Field Effect Transistors: Construction and characteristics of n-channel JFET, Types of power amplifiers: Class A operation, Class B operation, Class AB operation.	
MODULE 3	**8Hrs**
Operation Amplifier: Ideal Op-amp, Differential amplifier: differential and common mode operation common mode rejection ratio (CMRR), Practical op-amp circuits: inverting amplifier, non-inverting amplifier, comparator, summing amplifier, integrator, differentiator. The concept of positive feedback, Oscillator circuits using op amps: RC phase shift oscillator, Wein bridge oscillator.	
MODULE 4	**8Hrs**
Communication system: The radio frequency spectrum, electromagnetic waves, A simple CW transmitter and receiver, modulation, demodulation, AM transmitter, FM transmitter, tuned radio frequency receiver, Super heterodyne receiver. RF amplifiers, AM demodulators.	
MODULE 5	**7Hrs**
Digital circuits: Logic functions, Switch and lamp logic, logic gates, combinational, Logic, bistables/flipflops, application of Flip flops, Integrated circuit logic devices: introduction to Microprocessor and microcontrollers (Architecture), Related Problems.	

TEXT BOOKS:

1. Electronic Devices and Circuit Theory: Robert L Boylestad and Louis Nashelsky, Pearson Education, Eleventh Edition, 2013.
2. Electronic Circuits: Fundamentals and applications, Michael Tooley, Elsevier, Third edition, 2006.

REFERENCES:

1. David A Bell, Electronic Devices and Circuits, PHI, 5th edition, 2007.
2. Millman & Halkias, Electronics Devices and Circuits, McGraw Hill, second edition, 2010
3. Modern Digital and Analog Communication Systems by B.P. Lathi. Oxford University Press, Fourth edition, 2010
4. NPTEL- https://nptel.ac.in/courses/122/106/122106025/
   Virtual Labs- http://vlabs.iitkgp.ac.in/be/

****

SEMESTER	**I/II**					
YEAR	**I**					
COURSE CODE	**22EN1112**					
TITLE OF THE COURSE	**ENGINEERING GRAPHICS & DESIGN THINKING**					
SCHEME OF Instruction	L	T	P	J	Total Hours	Credits
	2	**-**	**2**	**-**	**26(L)+26(L)**	**3**

COURSE OBJECTIVES:

- To create awareness and emphasize the need for Engineering Graphics & design thinking
- To learn using professional CAD software for construction of geometry
- To understand the concepts of orthographic and isometric projections
- To construct orthographic projection of points, lines, planes and solids
- To construct development of surfaces of solids
- To construct isometric projections of planes and solids
- To create simple engineering 3D components
- To work in a team for creating conceptual design of products
- To learn application of design methods and tools on real world problem

COURSE OUTCOMES:

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	Explain usage of instruments, dimensioning & tolerances, conventions and standards related to working drawings	L1
CO2	Construct points, lines, planes and solids using orthographic projections principles	L3
CO3	Construct & understand development of lateral surfaces of solids	L3
CO4	Construct geometries of planes and solids using isometric projection principles	L3
CO5	Apply the design thinking principles and recognize the significance of innovation	L3
CO6	Design various part models related to engineering field using AutoCAD modelling software	L3

COURSE CONTENT:	
MODULE 1 **Introduction to engineering graphics**: Fundamentals, Drawing standard - BIS, dimensioning, Lines, lettering, scaling, symbols, dimensioning & tolerances, conventions, Introduction to orthographic projection. Types of projections & their principles **- (For CIA only)** **Introduction to computer aided drafting software**- Co-ordinate system and reference planes HP, VP, RPP & LPP of 2D/3D. Selection of drawing sheet size and scale. Commands and creation of Lines, coordinate points, axes, polylines, square, rectangle, polygons, splines, circles, ellipse, text, move, copy, off-set, coloring, mirror, rotate, trim, extend, break, chamfer, fillet and curves **- (For CIA only)**	**4 Hrs**

MODULE 2	**12 Hrs**
Projection of points and lines- Orthographic projections of points in all the quadrants, Orthographic projections of lines- inclined to both the principal planes - Determination of true lengths and true inclinations by rotating line method. **Orthographic projections of planes** viz triangle, square, rectangle, pentagon, hexagon and circular laminae.	
MODULE 3	**16 Hrs**
Projection of solids & development of surfaces: Projection of simple solids like prisms, pyramids, cylinder & cone when the axis is inclined to one or both of the principal planes by change of position method, Development of lateral surfaces of simple solids – Prisms, pyramids cylinders and cones.	
MODULE 4	**12 Hrs**
Isometric projections: Isometric scale, Isometric projection of hexahedron (cube), regular prisms, pyramids, cylinders, cones and spheres, Isometric projection of combination of two solids Conversion of Isometric Views to Orthographic Views & Conversion of orthographic views to isometric projections.	
MODULE 5	**8 Hrs**
Introduction to design thinking for innovations: A brief history of Design, Engineering Design process, Product development cycle, creation of models and their presentation in standard 3D view. Theory, Practice & Examples in Design thinking, Storytelling, Creativity and Idea Generation, Concept Development, Testing and Prototyping. **(For CIA only)**	

List of Laboratory activities to be conducted

Manual & Computer Sketching problems for all the modules in sketch book and also take print out of the problems.

Problems to be solved in first quadrant system.

Minor Project for Design thinking in a group of students with VIVA- (Examples on Solid Modeling

- Using 3D Modelling Software & Physical Model Prototype).

TEXT BOOKS:

1. "A Textbook of Computer Aided Engineering Drawing", Gopalakrishna, K. R. and Sudheer Gopala Krishna (2017), Subash Publishers, Bangalore, India.
2. "Engineering Design- A Project Based Introduction", C. L. Dym and Patrick Little, John Wiley & Sons (2022)

REFERENCES:

1. "Engineering Drawing", Bhatt N.D., 3rd Edition, Charotar Publishing House, Gujarat, India, (2019)
2. "Engineering Drawing with Introduction to AutoCAD" Dhananjay. A. J, Tata McGraw-Hill Publishing Company Ltd, (2018)
3. "Engineering Design Methods: Strategies for Product Design", N. Cross, John Wiley, 2021.

****

SEMESTER	**I/II**					
YEAR	**I**					
COURSE CODE	**22ENN1114**					
TITLE OF THE COURSE	**ENVIRONMENTAL SCIENCE**					
SCHEME OF Instruction	L	T	P	J	Total Hours	Credits
	1	**-**	**-**	**-**	**13**	**1**

COURSE OBJECTIVES:

- To understand the concepts of environment, pollution, energy resources
- To learn water as a resource, rain water harvesting as a method of conversation of water
- To explain solid waste and its management
- To learn environmental Protection Act laws, environmental Impact Analysis and air monitoring

COURSE OUTCOMES:

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	Critically elucidate the basic concepts that govern environmental quality, ambient air quality standards	L2
CO2	Compare different Energy resource and their environmental implications	L2
CO3	Identify different types of pollution, waste stream	L2
CO4	Identify different natural and manmade disasters and prevention	L2
CO5	Apply the process of environmental impact assessment and implications of Indian Environment Laws	L2

COURSE CONTENT:	
MODULE 1	**3 Hrs**
Definition of environment; Scope and importance of environmental studies; Basic concepts: Xenobiotic, natural & anthropogenic; why are we concerned? Eco-kinetic & Bio-kinetic Properties of a xenobiotic, Dose-Response Relationships; 3 T's, Chronic and acute effects.	
MODULE 2	**4 Hrs**
Pollution: Criteria Air pollutants – Ozone, Particulate Matter, Carbon Monoxide, Nitrogen, Oxides, Sulphur Dioxide, Lead; Acid Rain Cycle. Water as a resource; Lentic and Lotic Water Systems; Rain Water Harvesting; Water Pollution; Noise pollution-sources and effects of noise; Municipal Solid Waste: Hazardous Waste: Electronic Waste: Biomedical Waste; Solid Waste Management: Landfills, composting Process.	
MODULE 3	**2 Hrs**
Energy Types of energy: Conventional sources of energy, fossil fuel, Coal, Solar, wind; Non-conventional Sources of Energy, Biofuels - biomass, biogas.	

MODULE 4	2 Hrs
Disasters & Management; Definition, Natural (Earthquakes, landslides, floods), Man-made disasters (biological, chemical, nuclear, radiological explosions) – definition, causes and management and/or mitigation strategies; Bhopal & Chernobyl Disasters.	
MODULE 5	**2 Hrs**
Environmental Impact Assessment (EIA); Air pollution monitoring and Ambient Air Quality Standards (AAQS); Environment Protection Act, 1986.	

TEXT BOOKS:

1. Benny Joseph (2005). "Environmental Studies", Tata McGraw – Hill Publishing Company Limited, New Delhi.
2. R. J. Ranjit Daniels and Jagadish Krishnaswamy (2014). "Environmental Studies" (2014), Wiley India Pvt Limited, New Delhi.

REFERENCE BOOKS:

1. P. Aarne Vesilind, Susan M. Morgan, Thomson (2008). "Introduction to Environmental Engineering" (2008), Thomson learning, Second Edition, Boston.
2. R. Rajagopalan (2005). "Environmental Studies – From Crisis to Cure" Oxford University Press, New Delhi.

****

SEMESTER	**I/II**					
YEAR	**I**					
COURSE CODE	**22EN1114**					
TITLE OF THE COURSE	**TECHNICAL ENGLISH**					
SCHEME OF Instruction	L	T	P	J	Total Hours	Credits
		-	**2**	**-**	**26**	**1**

COURSE OBJECTIVES:

- To enhance their communicative skills
- To equip students with oral and appropriate written communication skills
- To inculcate students with employability and job search skills
- To achieve proficiency in English
- To create interest among the students about any topic
- To learn the use of body language and improve verbal message
- To acquire skills for placement
- To help them frame their ideas and thoughts in a proper manner.

COURSE OUTCOMES:

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	Make a complete Group Project: Poster Making, Power Point Presentation, Abstract Writing, Project Paper, Facing Viva	L2
CO2	Skit Performance on any social awareness theme in group.	L2
CO3	Learning how to create a Cover Letter, Job Application and Resume.	L3

COURSE CONTENT:	
MODULE 1	**4 Hrs**
Group Project: How to create a Poster & do Power Point Presentation. Learn to write an Abstract & Project Paper. Applying the basic etiquettes while facing Viva.	
MODULE 2	**12 Hrs**
Skit Performance: How to write a script. Use of powerful vocabulary, focus on pronunciation and maintaining the body language.	
MODULE 3	**16 Hrs**
Cover Letter, Job Application and Resume: Learn to create a resume. How to fill a Job Application form & create a proper Cover letter.	

REFERENCES:

1. Chauhan, Gajendra S., L. Thimmesha and Smita, Kashiramka (2019) Technical Communication, Cengage Learning, New Delhi

****

Dayananda Sagar University

School of Engineering
Deverakaggalahalli, Harohalli, Bengaluru 562112

SEMESTER	**II**					
YEAR	**I**					
COURSE CODE	**22EN1202**					
TITLE OF THE COURSE	**PYTHON PROGRAMMING FOR PROBLEM SOLVING**					
SCHEME OF Instruction	**L**	T	P	J	Total Hours	Credits
	2	**-**	**2**	**-**	**26(L)+26(P)**	**3**

COURSE OBJECTIVES:

- To understand basic concepts of computational thinking.
- To introduce python programming for problem solving.
- To introduce different debugging and unit testing tools.
- To solve real world problems using python data structures.
- Learn to handle files and exception handling in python.
- To explore Python's object-oriented features.
- To build Web services and Networked programs in python.
- To train students to design an application as part of the course mini- project using computational thinking with python.

COURSEOUTCOMES:

CO No.	Outcomes	Bloom's Taxonomy Level
CO1	Understand basic concepts of computational thinking.	L2
CO2	Outline basic python programming for problem solving.	L2
CO3	Apply computational thinking to solve real world programs using Python	L3
CO4	Build python programs using core data structures like list, dictionaries and tuples	L3
CO5	Implement object-oriented concepts using python	L3
CO6	Design applications related to web services and network Programming.	L3

COURSE CONTENT:	
MODULE 1	**5Hrs**
INTRODUCTION: Values, expressions and statements, Conditional execution, Functions, Iterations	
MODULE 2	**6Hrs**
PYTHON DATA STRUCTURES: Python Data Structures: Strings, Arrays, Lists, Tuples, Sets and Dictionaries	
MODULE 3	**5Hrs**
PYTHON OBJECTS: Classes and Objects: Creating classes, Using Objects, Accessing attributes, Classes as Types, Introduction to Multiple Instances, Inheritance.	
MODULE 4	**5Hrs**

EXCEPTION HANDLING: Try-Except, Exception syntax, examples, Types of exception with except, multiple exceptions with except, Try-Finally, raise exceptions with arguments, Python built-inexceptions, User-defined exceptions, Assertions

MODULE 5	**5Hrs**
PYTHON FILES & LIBRARIES: Files: File types, modes, File functions, File attributes, File positions, Looping over file. Basics of NumPy and Pandas	

1. Python program to evaluate Values, expressions, and statements, Conditional execution, and Functions Iterations
   a. prompt the user to enter an integer and reverse it. And print the sum of the reversed integer.
   b. Write a python program to find whether a number (num1) is a factor of 255.
   c. Write a python program to find whether a number (num1) is a factor of 255.
   d. Write a program to find the sum of the following series:
      i. 1 + 1/3 + 1/5 + 1/7 + up to 'N' terms.
      ii.1 + x/1! + x3/2! + x5/3! + x7/4 +x2n-1/n!

2. Python program to evaluate Python Collections
   a. Write a Python Program to demonstrate the inbuilt functions of Strings, List, and sets.
   b. Write a Python program for counting a specific letter 'o' in a given string; the number oftimes vowel 'o' appears.
   c. Write a Python Program to find the frequency of each word in given strings/strings
   d. Store the following for 'n' countries, using a dictionary:
      I. Name of a country, country's capital, per capita income of the country.
      II. Write a program to display details of the country with the highest and second lowest per capita income.
3. Write a python program to create two classes "Python" and "Java" having data members "version" and "name" and a member function "display()". With the help of the object, print the appropriate messages.
4. Create a class "Employee" with init method to initialize data members: Name, Designation, Ph. No.,and a member function display (). Create an instance for the class and display the details of the employee

5.Write an interactive calculator! User input is assumed to be a formula that consist of a number, an operator (at least + and -), and another number, separated by white space (e.g. 1 + 1). Split user input using str.split(), andcheck whether the resulting list is valid:

a. If the input does not consist of 3 elements, raise a FormulaError, which is a custom Exception.
b. Try to convert the first and third input to a float (like so: float_value = float (str_value)). Catch any Value Error that occurs, and instead raise a Formula Error
c. If the second input is not '+' or '-', again raise a Formula Error

If the input is valid, perform the calculation and print out the result. The user is then prompted to provide new input, and so on, until the user enters quit.

3. Write a Python program to count the number of lines in a text file and read the file line by line and store it into a list as well as find the longest word in the file.
4. Write a Python program to create a list of student details: usn, name dob and email {using dictionary} and write a list to a file.
5. Generate one-hot encodings for an array in numpy.
6. Write a Pandas program to import excel data into a Pandas dataframe and find a list of employees where hire_date is between two specific month and year.

TEXT BOOKS:

1. “Python for Everybody-Exploring Data Using Python 3”, Dr. Charles R. Severance,

REFERENCES:

1. “Computer Science Using Python: A Computational Problem- Solving Focus”, Charles Dierbach, Introduction John Wiley, 2012.
2. “Introduction to Computation and Programming Using Python”, John V Guttag,Prentice Hall of India, 2015.
3. "How to think like a Computer Scientist, Learning with Python", Allen Downey, JeffreyElkner andChris Meyers, Green Tea Press, 2014.
4. “Learning to Program with Python”, Richard L. Halterman, 2011.

****

TRANSFORMS AND NUMERIAL TECHNIQUES

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – III

Course Code	: 22CY2301	**Credits**	: 03
Hours / Week	: 03 Hours	**Total Hours**	: 39 Hours
L–T–P–J	: 3–0–0–0		

Course Learning Objectives:

This Course will enable students to:

1. **Apply** their knowledge of Laplace transforms and inverse Laplace transforms to proficiently solve linear ordinary differential equations with constant coefficients, facilitating the analysis and modelling of complex systems.
2. **Analyze** periodic functions using Fourier series, assessing the convergence properties and precision of the series expansion, thereby enhancing their ability to understand and manipulate periodic phenomena.
3. **Utilize** complex exponential form, Fourier transforms of basic functions, and Fourier sine and cosine transforms to solve problems involving Fourier integrals, developing proficiency in applying these techniques to various mathematical scenarios.
4. **Employ** numerical methods, including Euler's Method, Runge-Kutta 4th order, Adams- Bashforth, and Adams-Moulton Methods, to solve differential equations and effectively analyze dynamic systems, enabling them to model real-world phenomena and make accurate predictions**.**
5. **Apply** finite difference methods, including the Crank-Nicolson method and appropriate techniques for hyperbolic PDEs, to effectively solve different types of partial differential equations (PDEs) such as elliptic, parabolic, and hyperbolic equations, enhancing their

problem-solving skills in the context of differential equations and their applications.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only traditional lecture method, but different *type of teaching methods* may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt the* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher order Thinking questions in the class.
6. Adopt ***Problem Based Learning***, which fosters students' Analytical skills, develop thinking skills such as the ability to evaluate, generalize, and analyse information rather than simply recall it.
7. Show the ***different ways to solve*** the same problem and encourage the students to come up with their own creative ways to solve them.
8. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the students' understanding.

UNIT – I: Laplace Transform and Inverse Laplace Transform	**09 Hours**
Laplace Transforms of Elementary functions (without proof), Laplace Transforms of $e^{at}f(t)$, $t^n f(t)$ and $\frac{f(t)}{t}$, Periodic functions, Unit step function and impulse functions Inverse Laplace Transforms- By the method of Partial Fractions, Logarithmic and Trigonometric functions, Convolution Theorem, Inverse Laplace transform using Convolution Theorem Solution to Differential Equations by Laplace Transform.	
UNIT – II: Fourier Series	**09 Hours**
Periodic Functions, Trigonometric Series, Fourier series Standard function, Functions of any Period 2L, Even and Odd functions, Half-range Expansions. Practical Harmonic analysis (calculate average power and RMS values of periodic waveforms)	

UNIT – III: Fourier Transform	**06 Hours**
Calculation of Fourier integrals using complex exponential form, Fourier transform of basic functions Fourier sine and cosine transforms.	
UNIT – IV: Numerical Methods for Solving Ordinary Differential Equations	**07 Hours**
Euler's Method-Basic principles of Euler's method for solving first-order ODEs, Runge-Kutta 4th order, Multistep Methods-Explanation of multistep methods (Adams-Bashforth, Adams–Moulton Methods), Second-Order ODE. Mass–Spring System (Euler Method, Runge–Kutta Methods)	
UNIT – V: Numerical Methods for Partial Differential Equations	**08 Hours**
Classification of PDEs (elliptic, parabolic, hyperbolic), Difference Methods (Laplace and Poisson Equations), Derivation of finite difference approximations, Crank–Nicolson Method, Method for Hyperbolic PDEs	

Course Outcome	**Description**
At the end of the course the student will be able to:	
1	**Apply** Laplace transforms and inverse Laplace transforms to solve linear ordinary differential equations with constant coefficients, demonstrating proficiency in system analysis and modelling.
2	**Analyse** periodic functions using Fourier series and evaluate the convergence properties and precision of the series expansion.
3	**Solve** problems involving Fourier integrals by applying complex exponential form, Fourier transforms of basic functions, and Fourier sine and cosine transforms.
4	**Utilize** numerical methods such as Euler's Method, Runge-Kutta 4th order, Adams-Bashforth, and Adams-Moulton Methods to solve differential equations and analyze dynamic systems
5	**Apply** finite difference methods, including the Crank-Nicolson method and appropriate techniques for hyperbolic PDEs, to solve various types of partial differential equations (PDEs) such as elliptic, parabolic, and hyperbolic equations.

Table: Mapping Levels of COs to POs / PSOs														
COs	**Program Outcomes (POs)**												**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	3	2	2	1					1					
CO2	3	2	2						1					
CO3	3	2	2	1					1					
CO4	3	2	2	1					1					
CO5	3	2	2	1					1					

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Erwin Kreyszig, Advanced Engineering Mathematics, 2015, 10th Edition, Wiley India.

REFERENCE BOOKS:

1. Higher Engineering Mathematics, B.S. Grewal, 2015, 43rd Edition, Khanna Publishers.
2. Higher Engineering Mathematics, John Bird, 2017, 6 th Edition, Elsevier Limited.

E-Resources:

1. https://nptel.ac.in/courses/111106139
2. https://nptel.ac.in/courses/111101164
3. https://nptel.ac.in/courses/111105038

**********\

DATA STRUCTURES

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – III

Course Code	: 22CY2302	**Credits**	: 04
Hours / Week	: 03 Hours	**Total Hours**	: 39(Th)+26(P) Hours
L–T–P-J	: 3–0–2-0		

Prerequisites:

Proficiency in a C programming language.

Course Learning Objectives:

This Course will enable students to:

1. **Understand** the basic approaches for analysing and designing data structures.
2. **Introduce** dynamic memory allocation and C language concepts required for building data structures
3. **Develop** essential skills to construct data structures to store and retrieve data quickly and **efficiently**.
4. **Utilize** different data structures that support different sets of operations which are suitable for various applications.
5. **Explore & Implement** how to insert, delete, search and modify data in any data structure-Stack, Queues, Lists, Trees.
6. **Develop** applications using the available data structure as part of the course for mini-project.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only traditional lecture methods, but different *types of teaching methods* may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt the* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note taking, annotating, and roleplaying.

3. Show ***Video/Animation*** films to explain functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher order Thinking questions in the class.
6. Adopt ***Problem Based Learning***, which fosters students' Analytical skills, develop thinking skills such as the ability to evaluate, generalize, and analyse information rather than simply recall it.
7. Show the ***different ways to solve*** the same problem and encourage the students to come up with their own creative ways to solve them.
8. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the students' understanding.

UNIT – I	**08 Hours**

INTRODUCTION:

Introduction to Data Structure, Classification, C Structure and Union, Array Definition, Representation, Operations (Insertion, Deletion, Search and Traversal), Two/Multidimensional Arrays, sparse matrix, C Pointers

TB1: 1.1, 1.2,1.3.1-1.3.4; TB2: 2.5; RB1: 5.1 – 5.12, 6.4

UNIT – II	**09 Hours**

INTRODUCTION TO ADT:

Stack: Definition, Array Representation of Stack, Operations on Stacks.

Applications of Stack: Expression evaluation, Conversion of Infix to Postfix, Infix to Prefix Recursion, Tower of Hanoi

Queue: Definition, Representation of Queues, Operations of Queues, Circular Queue.

Applications of Queue: Job Scheduling, A Maze Problem

TB1: 2.1, 2.2, 2.3, 3.2, 3.3; TB2: 3.3,3.4,3.5

UNIT – III	**09 Hours**

DYNAMIC DATA STRUCTURES:

Linked List: Types, Representation of Linked Lists in Memory. Traversing, Searching, Insertion & Deletion from Linked List. Circular List, Doubly Linked List, Operations on Doubly Linked List (Insertion, Deletion, Traversal).

Applications: Stack & Queue Implementation using Linked Lists.

Case Study: Josephus problem.

TB1: 4.2,4.3,4.5

UNIT – IV	**08 Hours**
TREES: Basic Terminology, Binary Trees and their representation, Complete Binary Trees, Binary Search Trees, Threaded Binary Trees, Operations on Binary Trees (Insertion, Deletion, Search & Traversal). **Applications:** Expression Evaluation **Case Study:** Game Tree TB1: 5.5.3,5.5.4,5.6; TB2: 5.1,5.2,5.3,5.5,5.7	
UNIT – V	**05 Hours**
Efficient Binary Search Trees: Optimal Binary Search Trees, AVL Trees, Red Black Trees, Splay Trees. **Case Study**: B Trees TB2: 10.1,10.2,10.3,10.4, 11.2	

Course Outcome	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	**Demonstrate** the key C programming concepts such as pointers, structures, unions and arrays data structures to perform operations such as insertion, deletion, searching, sorting, and traversing.	L3
2	**Utilize** the fundamental concepts of stacks and queues to solve the standard applications like tower of Hanoi, conversion and evaluation of expressions, job scheduling and maze.	L3
3	**Implement** Singly Linked List, Doubly Linked List, Circular Linked Lists, stacks and queues using linked list**.**	L3
4	**Develop** critical thinking and problem-solving skills by designing and implementing efficient algorithms for Non-linear tree data structure and perform insertion, deletion, search and traversal **operations** on it.	L3
5	**Apply** advanced techniques, such as balancing algorithms for AVL trees, Splay trees and Red-Black trees to maintain the balance and efficiency of binary trees.	L3

Table: Mapping Levels of COs to POs / PSOs														
COs	**Program Outcomes (POs)**												**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	3												2	
CO2	3		3									2	2	
CO3	3		3									2	2	
CO4	3	2	3									2	2	
CO5	3	2	3									2	2	

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS(TB):

1. A.M. Tannenbaum, Y Langsam, M J Augentien "Data Structures using C", 1st Edition, Pearson, 2019.
2. Ellis Horowitz, Susan Anderson-Freed, and Sartaj Sahni, "Fundamentals of Data structures in C", 2nd Edition, Orient Longman, 2008.

REFERENCE BOOKS:

1. Brian. W. Kernighan, Dennis. M. Ritchie, "The C Programming Language", 2nd Edition, Prentice-Hall, 1988.
2. Gilbert & Forouzan, "Data Structures: A Pseudo-code approach with C", 2nd Edition, Cengage Learning,2014.
3. Jean-Paul Tremblay & Paul G. Sorenson, "An Introduction to Data Structures with Applications", 2nd Edition, McGraw Hill, 2013.
4. R.L. Kruse, B.P. Learly, C.L. Tondo, "Data Structure and Program design in C", 5th Edition, PHI ,2009.

E-Resources:

1. https://nptel.ac.in/courses/106102064
2. https://www.coursera.org/learn/data-structures?specialization=data-structures- algorithms
3. https://www.udemy.com/topic/data-structures/free/
4. https://www.mygreatlearning.com/academy/learn-for-free/courses/data-structures
5. https://cse01-iiith.vlabs.ac.in/
6. https://kremlin.cc/k&r.pdf

Activity Based Learning (Suggested Activities in Class)

1. Real world problem solving using group discussion.
2. Role play E.g., Stack, Queue, etc.,
3. Demonstration of solution to a problem through programming.
4. Flip class activity E.g., arrays, pointers, dynamic memory allocation, etc

LABORATORY EXPERIMENTS

Total Contact Hours: 26

Following are experiments to be carried out using either C programming language

1. To Implement C programs with concepts of pointers, structures.
2. To implement multidimensional array Matrix Multiplication.
3. To search elements in data structure with different search methods.
4. To implement stack, queue and their variations using arrays.
5. To implement stack, queue and their variations using singly linked lists
6. To implement conversion & evaluation of expression using stacks.
7. To Implement doubly circular Linked Lists and variations and use them to store data and perform operations on it.
8. To Implement Addition/multiplication of 2 polynomial using linked lists
9. To implement binary tree traversal techniques.

OPEN-ENDED EXPERIMENTS

1. A man in an automobile search for another man who is located at some point of a certain road. He starts at a given point and knows in advance the probability that the second man is at any given point of the road. Since the man being sought might be in either direction from the starting point, the searcher will, in general, must turn around many times before finding his target. How does he search to minimize the expected distance travelled? When can this minimum expectation be achieved?
2. The computing resources of a cloud are pooled and allocated according to customer demand. This has led to increased use of energy on the part of the service providers due to the need to maintain the computing infrastructure. What data structure will you use for allocating resources which addresses the issue of energy saving? Why? Design the solution.
3. Mini-Project on applying suitable data structure to a given real-world problem.

****

DIGITAL LOGIC DESIGN

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – III

Course Code	:	22CY2303	**Credits**	:	04
Hours / Week	:	03 Hours	**Total Hours**	:	39(Th) + 26(P) Hours
L–T–P-J	:	3–0–2-0			

Course Learning Objectives:

This Course will enable students to:

1. **Translate** the elements of digital logic functions to digital system abstractions using Verilog.
2. **Illustrate** simplification of Boolean expressions using Karnaugh
3. **Mode**l combinational logic circuits for arithmetic operations and logical operations
4. **Analyse** and model sequential elements flip-flops, counter, shift registers.
5. **Outline** the concept of Mealy Model, Moore Model and apply FSM to solve a given design problem.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only traditional lecture method, but different *type of teaching methods* may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt the* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher order Thinking questions in the class.
6. Adopt ***Problem Based Learning***, which fosters students' Analytical skills, develop thinking skills such as the ability to evaluate, generalize, and analyse information rather than simply recall it.
7. Show the ***different ways to solve*** the same problem and encourage the students to come up with their own creative ways to solve them.
8. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the students' understanding.

UNIT – I	08 Hours

INTRODUCTION:

Number System- Binary, Hexa, Decimal, Octal and its conversion. Canonical Notation - SOP & POS forms, Minimization of SOP and POS forms.

ARITHMETIC CIRCUITS AND VERILOG MODELLING

Adders: Half adder, full adder, Ripple carry adder, parallel adder /subtractor, fast adders-CLA, comparator- 2 bit. Simplification using K-Maps

Introduction to Verilog, Syntax of Verilog coding, Modelling styles in Verilog, Verilog Operators, Test bench for simulation

UNIT – II	07 Hours

Combinational Circuit Building Multiplexers 4:1, 8:1, decoders 3:8, 2:4, demultiplexers 1:4, encoders 8:3, 4:2, code converters- B to G and G to B- Simplification using K-Maps

Verilog for combinational circuits, if else, case-casex, casez, for loop, generate.

UNIT – III	08 Hours

Sequential Circuits-1

Basic Latch, Gated latches, Flip Flops SR, D, JK, T, master-slave flip-flops JK, Characteristic equations, 0's and 1's Catching Problem, Race round condition, Switch debounce, shift registers- SISO, SIPO, PISO, PIPO, Setup time, Hold time, Propagation Delay

UNIT – IV	08 Hours

Sequential Circuits-2

Binary counters – asynchronous and synchronous, mod-n counter, ripple counter- 4 bit.
Verilog blocking and non-blocking,
Mealy Model, Moore Model, State machine notation, Construction of Finite State Machine.

UNIT – V	08 Hours

Introduction to Electronic Design Automation:

FPGA Design Flow, ASIC Design flow, architectural design, logic design, simulation, verification and testing, 3000 Series FPGA architecture.

Applications:

Design 4 Bit ALU, 7 Segment display, Vending Machine, 3 Pipeline.

Laboratory Experiments

Experiments are conducted using Verilog tool /Kits	
1.	Introduction to Xilinx tool, FPGA flow
2.	Adder – HA, FA using data flow and behaviour modelling styles
3.	Adder – HA, FA using structural modelling style
4.	Combinational designs – I (blocking and non-blocking/looping examples) **a.** Multiplexer: 4:1, 8:1 MUX. **b.** De Multiplexer: 1:4, 1:8 DEMUX.
5.	Combinational designs – II (different types of case statements) **c.** Encoder with and without Priority: 8:3 and 4:2. **d.** Decoder: 3:8 and 2:4.
6.	Design of 4-bit ALU
7.	Flip Flop: D FF, T FF, JK FF
8.	Design of Mod – n Up/Down Counter with Synchronous reset
9.	Design of Mod – n Up/Down Counter with Asynchronous reset.
10.	Design of Universal shift Register using FSM

Course Outcome	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	**Interpret** Boolean Expressions of digital design in simplified form	L2
2	**Build** the various elements of digital logic system with Verilog	L3
3	**Construct** Combinational and Sequential logic circuits	L3
4	**Analyse** the hardware model of a digital system at different levels of abstraction in Verilog	L4
5	**Evaluate** the functionality of digital design by implementing on FPGA kits	L5
6	**Design digital** systems using FSM	L3

Table: Mapping Levels of COs to POs / PSOs

Cos	Program Outcomes (POs)												PSOs		
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
CO1	3	-	1	-	-	-	-	-	-	-	1	-	1	-	-
CO2	3	2	1	2	3	-	-	-	1	-	1	1	2	1	-
CO3	3	2	3	1	2	-	-	1	1	-	1	1	2	1	-
CO4	3	3	2	3	3	1	-	1	-	1	2	1	2	2	1
CO5	3	3	2	3	3	1	-	-	-	1	-	-	2	2	1
CO6	3	3	3	3	3	2	-	1	2	2	2	2	2	1	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. M. Morris Mano Michael D. Ciletti, "Digital Design with an Introduction to the Verilog HDL", 6th Edition, Pearson Education, 2014.

2. Stephen Brown, Zvonko Vranesic, "Fundamentals of Digital Logic with Verilog design", McGraw Hill, 2014.

3. Nazein M. Botros, "HDL programming (VHDL and Verilog)", Dreamtech Press, 2006.

4. Douglas J Smith, "HDL Chip Design", Doone publications 1996.

REFERENCE BOOKS:

1. John M Yarbrough, "Digital Logic Applications and Design", Thomson Learning, 2014.

2. Donald D. Givone, "Digital Principles and Design", McGraw Hill, 2015.

3. Samir Palnitkar, "Verilog HDL: A Guide to Digital Design and Synthesis", Pearson Education, 2016.

E-Resources:

1. https://archive.nptel.ac.in/courses/106/105/106105165/
2. https://nptel.ac.in/courses/117105080

Activity Based Learning (Suggested Activities in Class)

1. Design problem solving and Programming using group discussion. E.g., Traffic light controller, Digital Clock, Elevator.
2. Demonstration of solution to a problem through simulation

DISCRETE MATHEMATICS AND GRAPH THEORY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – III

Course Code	: 22CY2304	**Credits**	: 03
Hours / Week	: 03 Hours	**Total Hours**	: 39 Hours
L–T–P–J	: 3–0–0–0		

Course Learning Objectives:

This Course will enable students to:

1. **Learn** the set theoretic concept and its application in theory of computation.
2. **Determine** the concepts of mathematical induction, recursive relations and their application.
3. **Illustrate** the association of functions, relations, partial ordered set and lattices with problems related to theoretical computer science and network models.
4. **Discuss** the basics of graph theory and its application in computer networks. Learn the concepts of counting techniques and its application.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes.

1. **Lecture method** means it includes not only traditional lecture method, but different type of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching**: Adopt the Active learning that includes brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and roleplaying.
3. Show **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, ask at least three Higher order Thinking questions in the class.
6. Adopt **Problem Based Learning**, which fosters students' Analytical skills, develop thinking skills such as the ability to evaluate, generalize, and analyse information rather than simply recall it.
7. Show the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them.
8. Discuss how every **concept can be applied to the real world** - and when that possible, it helps improve the students' understanding.

UNIT – I	08 Hours
SET THEORY: Sets and subsets, Operations on Sets: Basic set operations, algebraic properties of sets, The Addition Principle **RELATIONS AND ITS PROPERTIES:** Relations and their properties, N-Ary Relations and their applications, Representing relations. ***Textbook – 2: 1.1, 1.2; Textbook – 1: 7.1., 7.2, 7.3***	
UNIT – II	**06 Hours**
RELATIONS AND ORDER RELATIONS: Closure of relations, Equivalence Relations, Partial Orderings, Functions, The Growth of Functions. **Self-Study:** Transitive Closure and Warshall's Algorithm. ***Textbook – 1: 7.4., 7.5, 7.6, 3.2***	
UNIT – III	**08 Hours**
MATHEMATICAL INDUCTION AND RECURSION: Mathematical Induction, Recurrence Relations: Rabbits and the Fibonacci Numbers, The Tower of Hanoi, Code word Enumeration, Solving Linear Recurrence Relations **Self-Study:** Basic Connectives and Truth Tables ***Textbook-1: 4.1;6.1, 6.2;1.1***	
UNIT – IV	**09 Hours**
GRAPH THEORY: Graphs and Graph Models. Graph Terminology and Special Types of Graphs: Basic Terminology, Some Special Simple Graphs, Bipartite Graphs, Complete Bipartite Graphs. Representing Graphs and graph isomorphism: Adjacency lists, Adjacency Matrices, Incidence Matrices, Connectivity: Paths, Connectedness in Undirected and Directed Graphs, Vertex and Edge connectivity and their applications. ***Textbook-1: 8.1, 8.2, 8.3, 8.4***	
UNIT – V	**08 Hours**
GRAPHS AND ITS APPLICATIONS: Euler and Hamilton Paths and their applications, Planar Graphs and their Applications, Graph Colouring and its applications. ***Textbook-1: 8.5, 8.7, 8.8***	

Course Outcome	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	**Identify** the membership of the Set and Relations and perform basic Algebraic operations.	L3
2	**Illustrate** the concept of Mathematical Induction and create linear recurrence relations for the given problem.	L4
3	**Construct** different types of graphs based on the properties and the real time applications of graph theoretical concepts.	L3
4	**Analyze** the methods for optimizing the solution for graph coloring problem, Eulerian and Hamiltonian circuits/planes.	L4

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	3	1	2					1	1	1		2	2	1
CO2	3	3	2					1	1	1		2	2	1
CO3	3	3	3					1	1	1		1	2	1
CO4	3	3	3					1	1	1		2	2	1
AVG	3	2.5	2.5					1	1	1		1.75	2	1

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Kenneth H. Rosen, "Discrete Mathematics and its applications", Tata McGraw Hill, 2003.
2. Bernard Kolman, Robert C. Busby, Sharon Ross, "Discrete Mathematical Structures", 3rd Edition, PHI 2001.

REFERENCE BOOKS:

1. Ralph P. Grimaldi, "Discrete and Combinatorial Mathematics", IV Edition, Pearson Education, Asia, 2002.
2. J. P. Tremblay, R. Manohar, "Discrete Mathematical Structures with applications to computer Science", Tata McGraw Hill, 1987.
3. J K Sharma, "Discrete Mathematics", 3rd edition, 2013, Macmillan India Ltd.

E-Resources:

1. Discrete Mathematics with Algorithms by M. O. Albertson, J. P. Hutchinson - J. 1988, Wiley.
2. Discrete Mathematics for Computer Science, Gary Haggard, John Schlipf, Sue Whitesides, Thomson Brooks/Cole, 2006.
3. http://ocw.mit.edu/courses/mathematics/
4. http://www.nptelvideos.in/2012/11/discrete-mathematical-structures.html
5. http://cglab.ca/~discmath/notes.html
6. https://www.cs.odu.edu/~toida/nerzic/content/web_course.html

Activity Based Learning (Suggested Activities in Class)

1. Real world problem solving and puzzles using group discussion.
2. Demonstration of solution to a problem using graph theory.

****

INTRODUCTION TO COMPUTER NETWORKS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – III

Course Code	: 22CY2305	**Credits**	: 04
Hours / Week	: 03 Hours	**Total Hours**	: 39(Th) + 26(P) Hours
L–T–P-J	: 3–0–2-0		

Course Learning Objectives:

This Course will enable students to:

1. **Outline** the basic principles of computer networking and how computer network hardware and software operate.
2. **Evaluate** the operation and performance of practical data link protocols using the principles of framing, error detection and correction.
3. **Apply** the principles of network layer design to the analysis and evaluation of routing algorithms, congestion control techniques, internetworking and addressing.
4. **Investigate** the basic transport layer facilities and essentials of transport. protocol
5. **Illustrate** the working of various application layer protocols.

Teaching-Learning Process (General Instructions)

1. These are sample new pedagogical methods, where teachers can use to accelerate the attainment of the various course outcomes.
2. ***Lecture method*** means it includes not only traditional lecture methods, but different *types of teaching methods* may be adopted to develop the course outcomes.
3. ***Interactive Teaching:*** *Adopt the* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note taking, annotating, and roleplaying.
4. Show ***Video/Animation*** films to explain functioning of various concepts.
5. Encourage ***Collaborative*** (Group Learning) Learning in the class.
6. To make ***Critical thinking***, ask at least three Higher order Thinking questions in the class.
7. Adopt ***Problem Based Learning***, which fosters students' Analytical skills, develop thinking skills such as the ability to evaluate, generalize, and analyse information rather than simply recall it.
8. Show the ***different ways to solve*** the same problem and encourage the students to come up with their own creative ways to solve them.
9. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the students' understanding.

UNIT – I	08 Hours
INTRODUCTION: Networks, network types, internet history, standards and administration (TB1-Ch1); Network models: Protocol layering, TCP/IP protocol suite, the OSI model (TB1-Ch2); Transmission media: Introduction, guided media, unguided media (TB1-Ch7); Switching: Introduction, circuit-switched networks, packet switching (TB1-Ch8).	
UNIT – II	**08 Hours**
Link layer addressing; (TB1-Ch10) Error detection and correction: Cyclic codes, checksum, forward error correction; (TB1-Ch10) Data link control: DLC services, data link layer protocols; (TB1-Ch11 & TB2-Ch3) Media access control: Random access, virtual LAN. (TB1-Ch12, Ch15)	
UNIT – III	**08 Hours**
Network layer design issues; (TB2-Ch5) Routing algorithms; (TB2-Ch5) Congestion control algorithms; (TB2-Ch5) Quality of service, and internetworking; (TB2-Ch5) The network layer in the internet: IPv4 addresses, IPv6; (TB2-Ch5, TB1-Ch19) Internet control protocols, OSPF (Open Shortest Path First), IP (Internet Protocol); (TB2-Ch5)	
UNIT – IV	**08 Hours**
The transport service, elements of transport protocols; (TB2-Ch6) Congestion control; (TB2-Ch6)	

The internet transport protocols: UDP (User Datagram Protocol), TCP (Transport Control Protocol); (TB2-Ch6) Performance problems in computer networks, and network performance measurement. (TB2-Ch6)

UNIT – V	07 Hours
Introduction, client server programming, WWW (World Wide Web) and HTTP (Hyper Text Transfer Protocol); (TB1-Ch27) FTP (File Transfer Protocol); (TB1-Ch26) E-mail, telnet, (TB1-Ch26 & TB2-Ch7) DNS (Domain Naming System); (TB2-Ch7) SNMP (Simple Network Management Protocol) (TB1-Ch28)	

Course Outcome	Description	Bloom's Taxonomy Level
At the end of the course, the student will be able to:		
1	**Elaborate** the basic concepts of data communications including the key aspects of networking and their interrelationship, packet switching, circuit switching and cell switching as internal and external operations, physical structures, types, models, and internetworking.	L6
2	**Apply** the concept of Hamming distance, the significance of the minimum Hamming distance and its relationship to errors as well as the detection and correction of errors in block codes.	L3
3	**Estimate** the mechanics associated with IP addressing, device interface, the association between physical and logical addressing, and how the Internet protocols IPv4, and IPv6 operate.	L6
4	**Evaluate** the concept of reliable and unreliable transfer protocol of data and how TCP and UDP implement these concepts.	L5
5	**Infer** the significance, and purpose of protocols (FTP, SMTP), standards, and use in data communications and networking and **analyze** the most common DNS resource records that occur in a zone file.	L4

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	3	-	-	-	-	-	-	-	-	-	-	-	1	-
CO2	3	3	3		-	-	-	-	-	-	-	-	2	-
CO3	3	3	3	-	-	-	-	-	-	-	-	-	2	-
CO4	3	3	3	-	-	-	-	-	-	-	-	-	1	-
CO5	3	3	3	-	-	-	-	-	-	-	-	-	1	-

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low) TEXT BOOKS**

1. Behrouz A. Forouzan, —Data Communications and Networking||, TataMcGraw- Hill,5thEdition, 2012.

2. Andrew S. Tanenbaum, David.J. Wetherall, —Computer Networks||, Prentice-Hall, 5th Edition, 2010.

REFERENCE BOOKS:

1. Chwan-Hwa Wu, Irwin, —Introduction to Computer Networks and Cyber Security||, CRC publications, 2014.
2. Douglas E. Comer, —Internetworking with TCP/IP —, Prentice-Hall, 5thEdition,2011.
3. Peterson, Davie, Elsevier, —ComputerNetworks,5thEdition,2011
4. Comer, —Computer Networks and Internets with Internet Applications,4thEdition,2004.

E-Resources:

1. http://computer.howstuffworks.com/computer-networking-channel.htm
2. https://www.geeksforgeeks.org/layers-osi-model/
3. https://www.wikilectures.eu/w/Computer_Network
4. https://technet.microsoft.com/en-us/network/default.aspx

Activity Based Learning (Suggested Activities in Class)

5. Real world problem solving using group discussion.
6. Flip class activity

LABORATORY EXPERIMENTS

1. Analyse the various line coding techniques used for data transmission of a digital signal over a transmission line
2. Design a program for error-detecting code using CRC-CCITT (16- bits).
3. Design a program to find the shortest path between vertices using Belman- ford algorithm
4. Given a graph derive the routing table using distance vector routing and link state routing algorithm
5. Try out some simple subnetting problems.
6. Using TCP/IP sockets, write a client–server program to make the client send the file name and to make the server send back the contents of the requested file if present. Implement the above program using message queues or FIFOs as IPC channels
7. Implement a webserver program to fetch a URL request and display the home page of the same in the browser
8. Implement a simple DNS server to resolve the IP address for the given domain name

DAYANANDA SAGAR UNIVERSITY

Dayananda Sagar University

School of Engineering
Deverakaggalahalli, Harohalli, Bengaluru 562112

SCHOOL OF ENGINEERING

PROBABILITY AND STATISTICS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – IV

Course Code	: 22CY2401	**Credits**	: 03
Hours / Week	: 03 Hours	**Total Hours**	: 39 Hours
L–T–P–J	: 3–0–0–0		

Course Learning Objectives:

This Course will enable students to:

1. **Apply** statistical principles and probability concepts to solve complex problems in real-world scenarios involving uncertainty and randomness.
2. **Evaluate** and select appropriate probability distributions and statistical techniques to analyze and interpret data accurately in various applications.
3. **Justify** the use of estimation methods and hypothesis testing techniques for drawing meaningful inferences about population parameters.
4. **Analyze** and interpret sample test results for different statistical relationships, such as means, variances, correlation coefficients, regression coefficients, goodness of fit, and independence, to make informed decisions.
5. **Identify** sample tests using appropriate statistical procedures to investigate the significance of observed data and communicate findings effectively.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only traditional lecture method, but different *type of teaching methods* may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt the* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher order Thinking questions in the class.

6. Adopt ***Problem Based Learning***, which fosters students' Analytical skills, develop thinking skills such as the ability to evaluate, generalize, and analyse information rather than simply recall it. 7. Show the ***different ways to solve*** the same problem and encourage the students to come up with their own creative ways to solve them. 8. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the students' understanding.	
UNIT – I : Probability	**09 Hours**
Definitions of Probability, Addition Theorem, Conditional Probability, Multiplication Theorem, Bayes' Theorem of Probability	
UNIT – II: Random Variables and their Properties and Probability Distributions	**09 Hours**
Discrete Random Variable, Continuous Random Variable, Joint Probability Distributions Their Properties, Probability Distributions: Discrete Distributions: Binomial, Poisson Distributions and their Properties; Continuous Distributions: Exponential, Normal, Distributions and their Properties.	
UNIT – III: Estimation and testing of hypothesis	**06 Hours**
Sample, Populations, Statistic, Parameter, Sampling Distribution, Standard Error, Un-Biasedness, Efficiency, Maximum Likelihood Estimator, Notion & Interval Estimation.	
UNIT – IV: Sample Tests-1	**07 Hours**
Large Sample Tests Based on Normal Distribution, Small Sample Tests: Testing Equality of Means, Testing Equality of Variances, Test of Correlation Coefficient	
UNIT – V: Sample Tests-2	**08 Hours**
Test for Regression Coefficient; Coefficient of Association, 2 – Test for Goodness of Fit, Test for Independence.	

Course Outcome	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	**Apply** the principles of probability to solve complex problems in various real-world scenarios.	L2 & L3
2	**Solve** and **compare** different probability distributions, including discrete and continuous random variables, in order to make informed decisions and predictions.	L2 & L3
3	**Apply** statistical estimation techniques, such as maximum likelihood estimation and interval estimation, to draw meaningful inferences about population parameters from sample data.	L3
4	**Examine** hypothesis testing methods, including large and small sample tests, to assess the significance of observed data and draw valid conclusions.	L4
5	**Analyze** statistical relationships and perform sample tests to assess the Equality of means in different populations, Correlation coefficients between variables to determine the strength and direction of the relationship. Independence of variables using appropriate statistical tests to assess the absence of any relationship.	L4

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	3	2	2		2				1					
CO2	3	2	2		2				1					
CO3	3	2	2						1					
CO4	3	2	2		2				1					
CO5	3	2	2		2				1					

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Probability & Statistics for Engineers and Scientists, Walpole, Myers, Myers, Ye. Pearson Education.

REFERENCE BOOKS:

1. Probability, Statistics and Random Processes T. Veerarajan Tata McGraw – Hill
2. Probability & Statistics with Reliability, Queuing and Computer Applications, Kishor S. Trivedi, Prentice Hall of India ,1999

E-Resources:

1. https://nptel.ac.in/courses/106104233
2. https://nptel.ac.in/courses/117103067
3. https://nptel.ac.in/courses/103106120
4. https://www.coursera.org/learn/probability-intro#syllabus
5. https://nptel.ac.in/courses/111104073

Activity Based Learning (Suggested Activities in Class)

1. Tools like Python programming, R programming can be used which helps student to develop a skill to analyze the problem and providing solution.
2. Regular Chapter wise assignments/ Activity/Case studies can help students to have critical thinking, developing an expert mind set, problem-solving and teamwork.

Following are Assignments/ Activities Can be carried out using either R programming language or Python Programming or excel solver.

1. There are n people gathered in a room. What is the probability that at least 2 of them will have the same birthday? (Use excel solver, R Programming, Python Programming)
   a. Use simulation to estimate this for various n., and Produce Simulation Graph.
   b. Find the smallest value of n for which the probability of a match is greater than 0.5.
   c. Explore how the number of trials in the simulation affects the variability of our estimates.

2. **Case Study 1: Customer Arrivals at a Coffee Shop**
   a. A coffee shop wants to analyze the number of customer arrivals during its morning rush hour (7:00 AM to 9:00 AM). The shop has been recording the number of customer arrivals every 15 minutes for the past month.
   b. Data: The data consists of the number of customer arrivals recorded at the coffee shop during each 15-minute interval for the past month.
   c. Here is a sample of the data:

Time Interval	Customer Arrivals
00 AM - 7:15 AM	**6**
15 AM - 7:30 AM	**4**
30 AM - 7:45 AM	**9**
45 AM - 8:00 AM	**7**
00 AM - 8:15 AM	**5**
15 AM - 8:30 AM	**8**
30 AM - 8:45 AM	**10**
45 AM - 9:00 AM	**6**

analyse the customer arrivals and determine the probability distribution that best fits the data. Specifically, explore both discrete and continuous probability distributions, including the binomial, Poisson, exponential, and normal distributions.

3. **Case Study 2: Comparing the Performance of Two Groups**
    a. Suppose you are a data analyst working for a company that manufactures a new energy drink. The marketing team conducted a promotional campaign in two different cities (City A and City B) to determine the effectiveness of the campaign in increasing sales. The sales data for a random sample of customers in each city was collected over a week. Your task is to compare the average sales between the two cities and test whether there is a significant difference in the variance of sales.
    b. **Data**: Let's assume the following sample data for the number of energy drinks sold in each city:

City A: [30, 28, 32, 29, 31, 33, 34, 28, 30, 32]

City B: [25, 24, 26, 23, 22, 27, 29, 30, 26, 24]

perform a two-sample t-test to test the equality of means and a test for equality of variances using Python's SciPy library.

4. **case study 3:** testing independence between two categorical variables.
    a. Data: Sample of 100 employees, and each employee is classified as either Male or Female. They were asked to rate their job satisfaction on a scale of 1 to 5, where 1 represents low satisfaction and 5 represents high satisfaction. The data is as follows:

Employee	Gender	Job Satisfaction
1	Male	4
2	Female	3
3	Male	2
4	Female	5
...	...	...
100	Female	4

    b. Test for independence between gender and job satisfaction, use the chi-squared test in R.

****

DESIGN AND ANALYSIS OF ALGORITHMS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – IV

Course Code	: 22CY2402	**Credits**	: 03
Hours / Week	: 03 Hours	**Total Hours**	: 39(Th)+26(P) Hours
L–T–P–J	: 3–0–2–0		

Course Learning Objectives:

This Course will enable students to:

1. **Analyze** the non-recursive and recursive algorithms and to represent efficiency of these algorithms in terms of the standard Asymptotic notations.
2. **Acquire** the knowledge of Brute Force and Divide and Conquer techniques to design the algorithms and apply these methods in designing algorithms to solve a given problem.
3. **Master** the Decrease and Conquer, Transform and Conquer algorithm design techniques, and Time versus Space Trade-offs.
4. **Learn** Greedy method and dynamic programming methods and apply these methods in designing algorithms to solve a given problem.
5. **Understand** the importance of Backtracking and Branch and Bound algorithm design techniques to solve a given problem.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only traditional lecture method, but different *type of teaching methods* may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt the* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher order Thinking questions in the class.
6. Adopt ***Problem Based Learning***, which fosters students' Analytical skills, develop thinking skills such as the ability to evaluate, generalize, and analyse information rather than simply recall it.
7. Show the ***different ways to solve*** the same problem and encourage the students to come up with their own creative ways to solve them.
8. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the students' understanding.

UNIT – I	08 Hours

INTRODUCTION:

What is an Algorithm? Fundamentals of Algorithmic Problem Solving.
(Text Book-1: Chapter 1: 1.1 to 1.2)
FUNDAMENTALS OF THE ALGORITHMS EFFICIENCY:
Analysis Framework, Asymptotic Notations and Standard notations and common functions ***(Text Book-2: Chapter 3: 3.1, 3.2)***,
Mathematical Analysis of Non-recursive and Recursive Algorithms,
(Text Book-1: Chapter 2: 2.1, 2.3, 2.4,)

UNIT – II	08 Hours

BRUTE FORCE:

Background, Selection Sort, Brute-Force String Matching. TSP
(Text Book-1: Chapter 3: 3.1, 3.2)
DIVIDE AND CONQUER:
General method, Recurrences: The substitution method, The recursion-tree method, The master method.
(Text Book-2: Chapter 4: 4.4, 4.5),
Merge sort, Quick sort, Binary Search, Multiplication of large integers,
Case study: Strassen's Matrix Multiplication.
(Text Book-1: Chapter 4: 4.1 to 4.3, 4.5)

UNIT – III	06 Hours

DECREASE & CONQUER:

General method, Insertion Sort, Graph algorithms: Depth First Search, Breadth First Search, Topological Sorting
TRANSFORM AND CONQUER:
Case study: Heaps and Heap sort.

TIME AND SPACE TRADEOFFS:
Input Enhancement in String Matching: Horspool's algorithm, Hashing: Open and Closed hashing.
(Text Book-1: Chapter 5: 5.1 to 5.3, Chapter 6: 6.3 to 6.4, Chapter 7: 7.2 to 7.3)

UNIT – IV	9 Hours

GREEDY TECHNIQUE:

General method of Greedy technique, Single-Source Shortest Paths: General method, The Bellman-Ford algorithm, Single-Source Shortest Paths in DAGs, Dijkstra's Algorithm
(Text Book-2: Chapter 24: 24.1 to 24.3).
Minimum Spanning Trees: Prim's Algorithm, Optimal Tree problem: Huffman Trees;
Case study: Kruskal's Algorithm. Fractional Problem
(Text Book-1: Chapter 9: 9.1, 9.2, 9.4).
DYNAMIC PROGRAMMING:
General method, The Floyd-Warshall Algorithm, Johnson's algorithm for sparse graphs ***(Text Book- 2: Chapter 25: 25.1 to 25.3)***,
The Knapsack problem ***(Text Book-1: Chapter 8: 8.4).***

UNIT – V	08 Hours
LIMITATIONS OF ALGORITHMIC POWER P, NP and NP-complete problems ***(Text Book-1: Chapter 11: 11.3***) **BACKTRACKING:** General method, N-Queens problem, Subset-sum problem. ***(Text Book-1: Chapter 12: 12.1***) **BRANCH AND BOUND:** General method, Travelling Salesman problem, Approximation algorithms for TSP. **Case study:** Knapsack Problem. ***(Text Book-1: Chapter 12: 12.2, 12.3***)	

Course Outcome	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	**Exemplify** the algorithm design techniques and standard Asymptotic notations. Analyze non-recursive and recursive algorithms to obtain worst-case running times of algorithms using asymptotic analysis	L3
2	**Interpret** the brute-force, divide-and-conquer paradigms and explain when an algorithmic design situation calls for it. Recite algorithms that employ this paradigm. Synthesize divide-and-conquer algorithms. Derive and solve recurrences describing the performance of divide-and-conquer algorithms.	L3
3	**Demonstrate** the Decrease and Conquer, Transform and Conquer algorithm design techniques and analyze the performance of these algorithms.	L3
4	**Identify and interpret** the greedy technique, dynamic-programming paradigm as to when an algorithmic design situation calls for it. Recite algorithms that employ this paradigm. Synthesize dynamic-programming algorithms and analyze them	L3
5	**Illustrate** the Backtracking, Branch and Bound algorithm design paradigms and explain when an algorithmic design situation calls for it. Recite algorithms that employ these paradigms. **Summarize** the limitations of algorithmic power.	L3

Table: Mapping Levels of COs to POs / PSOs														
COs	**Program Outcomes (POs)**												**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	3	3										2		3
CO2	3	3	2									2		3
CO3	3	3										1		3
CO4	3	3	2									2		3
CO5	3	3										1		3

3: Substantial (High) **2: Moderate (Medium** **1: Poor (Low) TEXT BOOKS**

1. Anany Levitin, "Introduction to the Design & Analysis of Algorithms", 2nd Edition, Pearson Education, 2011.
2. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein, "Introduction to Algorithms", 3rd Edition, PHI, 2014.

REFERENCE BOOKS:

1. Horowitz E., Sahni S., Rajasekaran S, "Computer Algorithms", Galgotia Publications, 2001.
2. R.C.T. Lee, S.S. Tseng, R.C. Chang & Y.T. Tsai, "Introduction to the Design and Analysis of Algorithms A Strategic Approach", Tata McGraw Hill, 2005.

E-Resources:

1. https://nptel.ac.in/courses/106/101/106101060/
2. http://cse01-iiith.vlabs.ac.in/
3. http://openclassroom.stanford.edu/MainFolder/CoursePage.php?course=IntroToAl gorithms
4. https://www.coursera.org/specializations/algorithms

Activity Based Learning (Suggested Activities in Class)

1. Real world problem solving and puzzles using group discussion. E.g., Fake coin identification, Cabbage puzzle, Konigsberg bridge puzzle etc.,
2. Demonstration of solution to a problem through programming.

LABORATORY EXPERIMENTS

Total Contact Hours: 26

Following are experiments to be carried out using either C programming language or Object-oriented programming language:

1. Apply divide and conquer method and Design a C program to implementation of Binary Search algorithm.
2. Sort a given set of n integer elements using Merge Sort method and compute its time complexity. Demonstrate this algorithm using Divide-and-Conquer method.
3. Sort a given set of n integer elements using Quick Sort method and compute its time complexity. Demonstrate this algorithm using Divide-and-Conquer method.
4. Incorporate the array data structure and demonstrate whether a given unweighted graph is connected or not using DFS method.
5. Implement the graph traversal technique using BFS method to print all the nodes reachable from a given starting node in an unweighted graph.
6. Compute the Transitive Closure for a given directed graph using Warshall's algorithm.
7. For a given weighted graph, construct an All-Pairs Shortest Paths problem using Floyd's algorithm and implement this algorithm to find the shortest distance and their shortest paths for every pair of vertices.
8. Implement 0/1 Knapsack problem using Dynamic Programming Memory Functions technique
9. Find Minimum Cost Spanning Tree for a given weighted graph using Prim's and Kruskal's algorithm.
10. From a given vertex in a weighted connected graph, determine the Single Source Shortest Paths using Dijkstra's algorithm.
11. Mini project proposal should be submitted and Implementation should be done based on the problem stated in the proposal

Open ended experiments

1. Implement Fractional Knapsack problem using Greedy Method.
2. Implement N-Queens problem using Backtracking technique.
3. Implementation of Travelling Sales man problem using Dynamic programming.

DATABASE MANAGEMENT SYSTEM

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – IV

Course Code	: 22CY2403	**Credits**	: 04
Hours / Week	: 03 Hours	**Total Hours**	: 39(Th)+26(P) Hours
L–T–P–J	: 3–0–2–0		

Course Learning Objectives:

This course will enable students to:

1. **Acquire** the concept of databases, Entity-Relationship Model and relational model for creating and designing databases for the real-world scenario.
2. **Develop** queries to extract data from the databases using a structured query language.
3. **Differentiate** SQL and NoSQL.
4. **Demonstrate** the operations on MongoDB, Database connectivity with front end and **Optimize** the Database design using Normalization Concepts.
5. **Understand** the importance of Transaction Management, Concurrency control mechanism and recovery techniques.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	10 Hours
INTRODUCTION TO DATABASE SYSTEMS: Introduction, Characteristics of the Database Approach, Advantages of using DBMS Approach, Data Models, Schemas, Instances and Data Independence, Three Schema Architecture, various components of a DBMS. ***(Text Book-1: Chapter 1: 1.1 to 1.4, 1.6, Chapter 2: 2.1,2.2, 2.4)*** **ENTITY-RELATIONSHIP MODEL:** Entity Types, Entity Sets, Attributes and Keys, Relationship types, Relationship Sets, Roles and Structural Constraints; Weak Entity Types; ER Diagrams ***(Text Book-1: Chapter 7: 7.3, 7.4, 7.5, 7.7)***.	
UNIT – II	**07 Hours**
RELATIONAL MODEL: Relational Model Concepts, Relational Model Constraints and Relational Database Schemas, Update operations and Dealing with Constraint Violations. ***(Text Book-1: Chapter 3: 3.1 to 3.3).*** **SQL –THE RELATIONAL DATABASE STANDARD:** SQL Data Definition and Data types, Specifying constraints in SQL, Basic Queries in SQL-Data Definition Language in SQL, Data Manipulation Language in SQL; ***(Text Book-1: Chapter 4: 4.1 to 4.4).***	
UNIT – III	**08 Hours**
SQL –THE RELATIONAL DATABASE STANDARD: Additional Features of SQL; Views (Virtual Tables) in SQL; Database Programming Issues and Techniques; ***(Text Book-1: Chapter 4: 4.5; Chapter 5: 5.1 to 5.4).*** **SQL AND NOSQL DATA MANAGEMENT:** Triggers, Database connectivity using Python, SQL vs NoSQL, Introduction to MongoDB, ***(Text Book-1: Chapter 5: 5.2,5.3) (Text Book-2 Chapter 1: 1.1 to 1.5***)	
UNIT – IV	**07 Hours**
NOSQL DATA MANAGEMENT: Data Types, Data Modelling, CRUD Operations. ***(Text Book-2 Chapter 1: 1.1 to 1.5***) **DATABASE DESIGN:** Design Guidelines, Functional Dependencies; Normal Forms Based on Primary Keys; General Definitions of Second and Third Normal Forms; Boyce-Codd Normal Form; ***(Text Book-1: Chapter 14: 14.1 to 14.5)***	
UNIT – V	**07 Hours**
TRANSACTION MANAGEMENT The ACID Properties; Transactions and Schedules; Concurrent Execution of Transactions; Concurrency Control Mechanisms; Error recovery methods. ***(Text Book-1: Chapter 20: 20.1 to 20.5, Chapter 21: 21.1 to 21.3, Chapter 22: 22.1 to 22.4***)	

Course Outcome	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	**Use** the basic concepts of database management system in the design and creating database blueprint using E-R model and relational model.	L3
2	**Formulate** SQL and NoSQL queries for building structure and unstructured databases	L3
3	**Demonstrate** database connectivity using vendor specific drivers	L3
4	**Apply** normalization techniques to design relational database management system	L3
5	**Adapt** Transaction Management, concurrency control and recovery management techniques in database management system.	L3

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	3	3	2	-	-	-	-	-	2	2	-	2	3	-
CO2	3	2	1	-	3	-	-	-	2	2	-	2	3	-
CO3	2	2	2	-	3	-	-	-	2	2	-	2	3	-
CO4	3	1	2	-	1	-	-	-	2	2	-	2	3	-
CO5	2	1	-	-	-	-	-	-	2	2	-	2	3	-

1. http://nptel.ac.in/courses/106106093/
2. https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-830- database-systems-fall-2010/lecture-notes/
3. http://agce.sets.edu.in/cse/ebook/DBMS%20BY%20RAGHU%20RAMAKRISHNAN.pdf
4. http://iips.icci.edu.iq/images/exam/databases-ramaz.pdf
5. https://db-class.org/
6. https://www.w3schools.com/mongodb/

Activity Based Learning (Suggested Activities in Class)

1. Database designing and data extraction using group discussion.
2. Collaborative Activity is minor project development with a team of 4 student

LABORATORY EXPERIMENTS

Total Contact Hours: 26

Following are experiments to be carried out using either oracle or mysql, Mongo Db .

1. Design any database with at least 3 entities and establish proper relationships between them. Draw suitable ER/EER diagrams for the system. Apply DCL and DDL commands.
2. Design and implement a database and apply at least 10 Different DML Queries for the following task.
    a. For a given input string display only those records which match the given pattern or a phrase in the search string. Make use of wild characters and like operators for the same. Make use of Boolean and arithmetic operators wherever necessary
3. Write SQL statements to join table and retrieve the combined information from tables.
4. Execute the Aggregate functions count, sum, avg, min, max on a suitable database. Make use of built in functions according to the need of the database chosen .
5. Retrieve the data from the database based on time and date functions like now(), date(), day(), time() etc., Use of group by and having clauses.
6. Write and execute database trigger. Consider row level and statement level triggers.
7. Write and execute program to perform operations on MongoDb Database.
8. Write and execute program to perform CRUD operations.

Open Ended Experiments

1. Consider the Table “employees”, write a SQL query to remove all the duplicate emails of employees keeping the unique email with the lowest employee id, return employee id and unique emails.

    table: employees

employee_id	employee_name	email_id
101	|Liam Alton	li.al@abc.com
102	|Josh Day	jo.da@abc.com
103	|Sean Mann	se.ma@abc.com
104	|Evan Blake	ev.bl@abc.com
105	|Toby Scott	jo.da@abc.com

2. A salesperson is a person whose job is to sell products or services. Consider the table "Sales" [given below]. Write a SQL query to find the top 10 salesperson that have made highest sale. Return their names and total sale amount.

Table: sales

TRANSACTION_ID	SALESMAN_ID	SALE_AMOUNT
501	18	5200.00
502	50	5566.00
503	38	8400.00
599	24	16745.00
600	12	14900.00

Table: salesman

SALESMAN_ID	SALESMAN_NAME
11	Jonathan Goodwin
12	Adam Hughes
13	Mark Davenport
59	Cleveland Hart
60	Marion Gregory

INTRODUCTION TO CYBER SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – IV

Course Code	: 22CY2404	**Credits**	: 03
Hours / Week	: 03 Hours	**Total Hours**	: 39 Hours
L–T–P-J	: 3–0–0-0		

Course Learning Objectives:

This Course will enable students to:

1. **Give** insights into the Cyber-incident, Cyber-crime, Cyber-Physical systems and Cybersecurity.
2. **Recognize** the basic programming to detect and protect the systems from cyber threats.
3. **Understand** the design and development framework for IDS and IPS.
4. **Deploy** the Cloud infrastructure using different methods from the scratch.
5. **Apply** and map theoretical knowledge of Cybersecurity to assess risk and vulnerability of a given system.

Teaching-Learning Process

1. ***Lecture method*** along with traditional lecture method, different *type of teaching methods* may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *incorporating* brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and roleplaying.
3. Showing ***Video/animation*** films to explain functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the ***different ways to solve*** the same problem and encourage the students to come up with their own creative ways to solve them.

MODULE 1: Cybersecurity Foundation	**10Hrs**
Modern Computing Trends, Application Threat Vectors, Cyber space, Cyber-attacks on business: Attacker profiles, Cyber-attack Life-cycle (CAL), High-profile Cybersecurity attacks, Advanced Persistent Threats (APTs), Types of malwares, vulnerabilities, and exploits: Spamming and Phishing attacks, Bot and Botnets, Zero Trust Design principles and Architecture: Perimeter-based network security strategies: Demilitarized security zone, Next Generation Firewall (NGFW) and Traps.	
MODULE 2: Network Security Fundamentals	**7Hrs**
Identification of common enterprise network devices: Topologies: Protocols in OSI and TCP model layers: Ports and packet filtering procedures: Routed versus Routing protocols: DNS, FQDN, and IoT: Structure and fields of an IP header, IPV4 and IPV6 addressing, Subnet mask, DHCP and Network Address Translation (NAT), Endpoint and network security technologies like SSH, SSL, and TLS.	
MODULE 3: Cloud Security Fundamentals	**8Hrs**
Cloud computing service, deployment, and shared responsibility models: cloud native technologies- virtual machines, containers and orchestration, and serverless computing: Cloud native security- Kubernetes security, DevOps, and DevSecOps- Security challenges like visibility, governance, and compliance: East-West and North-South traffic protection methods: Layers and capabilities in a Secure Access Service Edge (SASE).	
MODULE 4: Security Operations Fundamentals	**7Hrs**
Key elements of Security Operations (SecOps), SecOps processes: Log forwarding: Security Information and Event Management (SIEM), Security Analysis tools: Security Operations Center (SOC) Engineering: Security Orchestration, Automation, and Response (SOAR) for SecOps: Threat Intelligence: Vulnerability Profiles to secure Endpoints.	
MODULE 5: Modern Tools and Use Cases in Cyber Security	**7Hrs**
AutoFocus: Mindmeld: Cortex XDR: Cortex XSOAR: Cortex Data Lake: Normalization of Enterprise Security data with advanced Artificial Intelligence (AI) and Machine Learning (ML):	
Reconnaissance Attacks: Mindmeld for threat intelligence gathering and response: Prisma Access architecture: Four pillars of Prisma Cloud: Next Generation Firewall to use Dynamic Block Lists.	

Course Outcome	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Summarize the fundamental concept of cybersecurity to design zero-trust and perimeter-centric robust security system.	L2
2	Apply the basic concept of network security and packet filtering techniques to protect end nodes in a public network.	L3
3	Summarize the fundamental concept of cloud security to develop a robust and secure cloud-centric application.	L3
4	Apply the knowledge of Security Operations (SecOps) utilizing Log forwarding, SIEM, SOAR to assess end-point vulnerabilities.	L3
5	Make use of different cyber security tools and techniques like AutoFocus, Mindmeld, Cortex XDR, Cortex XSOAR, Cortex Data Lake to detect and prevent cyber security threats.	L3

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	2	2			1				1			1	2	1
CO2	2	1			2				1			2	2	2
CO3	2	1			1							1	2	1
CO4	2	2			2				1			2	2	2
CO5	2	1			3							1	2	1

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Palo Alto Networks Cybersecurity Survival Guide Fundamental Principles & Best Practices, Fifth Edition, 2020.
2. Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Nina Godbole and Sumit Belapure, Wiley, First Edition, 2011.

E-Resources:

1. https://onlinecourses.swayam2.ac.in/cec23_cs16/preview
2. https://onlinecourses.swayam2.ac.in/nou23_ge65/preview
3. Introduction to Cyber Security - Course (swayam2.ac.in)
4. https://www.coursera.org/learn/introduction-to-cybersecurity-foundations/

****

EMBEDDED SYSTEM DESIGN

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – IV

Subject Code	: 22CY2405	**Credits**	: 04
Hours / Week	: 03 Hours	**Total Hours**	: 39(Th) + 26(P) Hours
L–T–P-J	: 3–0–2-0		

Course Learning Objectives:

This Course will enable students to:

1. **Understand** the fundamental concepts of embedded system design.
2. Gain **knowledge** of various hardware and software components used in embedded systems.
3. **Develop** skills to design and implement embedded systems for different applications.
4. Learn to **analyze** and optimize the performance of embedded systems.
5. **Enhance** problem-solving and critical thinking abilities in the context of embedded system design.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes.

1. ***Interactive Lectures:*** Engage students through discussions, case studies, and real-life examples.
2. ***Hands-on Projects:*** Assign practical projects to students to enhance their understanding and application of concepts.
3. ***Group Discussions:*** Encourage collaborative learning and problem-solving through group discussions and brainstorming sessions.
4. ***Case Studies:*** Analyze real-world embedded system designs to understand their challenges and solutions.
5. ***Simulations and Virtual Labs:*** Use simulation tools and virtual labs to provide a virtual hands-on experience.
6. ***Guest Lectures:*** Invite industry experts to share their experiences and provide insights into real-world embedded system design practices.
7. ***Online Forums:*** Establish an online platform for students to discuss and share their ideas and questions related to the course.
8. ***Demonstrations:*** Conduct live demonstrations of embedded system prototypes to showcase practical implementations.
9. ***Assignments and Assessments:*** Assign regular assignments and assessments to evaluate students' understanding and progress.

Industry Visits: Organize visits to embedded system manufacturing companies to expose students to real-world applications.

UNIT – I	05 Hours

INTRODUCTION TO EMBEDDED SYSTEMS

Introduction: What is an Embedded System, Embedded Systems VS. General Computing Systems, History of Embedded Systems, Classification of Embedded Systems, Major Application Areas of Embedded Systems, Purpose of Embedded Systems, Wearable Devices—The Innovative Bonding of Lifestyle with Embedded Technologies ***(Text Book-3: Chapter 1)***

Characteristics and Quality Attributes of Embedded Systems: Characteristics of an Embedded System, Quality Attributes of Embedded Systems ***(Text Book-3: Chapter 3)***

Embedded Systems—Application- and Domain-Specific: Washing Machine—Application-Specific Embedded System, Automotive–Domain Specific Examples of Embedded System ***(Text Book-3: Chapter 4)***

UNIT – II	10 Hours

EMBEDDED SYSTEM HARDWARE DESIGN

Embedded System Core: General Purpose and Domain Specific Processors, Application Specific c Integrated Circuits (ASICs), Programmable Logic Devices (PLDs), Commercial off-the-shelf Components (COTS)

(Text Book 3: Chapter 2.1)

Memory: Overview on Various Types of memory sub systems used in Embedded systems and their selection

(Text Book 3: Chapter 2.2)

Sensors and Actuators: interfacing of LEDs, 7-segment LED Displays, Piezo Buzzer, Stepper Motor, Relays, Optocouplers, Matrix keyboard, Push button switches, Programmable Peripheral Interface Device (e.g. 8255 PPI), etc. with the I/O subsystem of the embedded system

(Text Book 3: Chapter 2.3)

Communication Interface: I2C, SPI, CAN, UART,1-wire, parallel bus, etc. RS-232C, RS-485, Parallel Port, USB, IEEE 1394, Infrared (IrDA), Bluetooth, Wi-Fi, ZigBee, GPRS, etc.

(Text Book 3: Chapter 2.4)

Other System Components: Reset Circuit, Brown-out protection circuit, Oscillator Unit, Real-Time Clock (RTC), Analog to Digital Converter (ADC), Timers and Watchdog Timer unit

(Text Book 3: Chapter 2.6)

Arm Cortex Mx Processor family Overview: Features, Architecture, Memory System, Exception and Interrupts, Low Power Features ***(Text Book 1: Chapter 3)***

UNIT – III	10 Hours
EMBEDDED SYSTEM SOFTWARE DESIGN	
Programming Concepts and Embedded Programming in C: High -Level Language C programming, C program elements (compiler build stages, macros, functions, Bitwise Operations, Looping constructs, Pointers and AAPCS) ***(Reference Book 2: Chapter 5.1 to 5.6)*** **Embedded Firmware Design and Development:** Embedded Firmware Design Approaches ***(Text Book 3: Chapter 9.1)***	
UNIT – IV	**10 Hours**
REAL-TIME OPERATING SYSTEMS	
Operating System Basics: The Kernel, Types of Operating Systems, Tasks, Process and Threads ***(Text Book 3: Chapter 10.1, 10.2, 10.3)*** **Thread Management:** Introduction to RTOS, Function pointers, Thread Management, Semaphores, Thread Synchronization, Process Management, Dynamic loading and linking ***(Text Book 2: Chapter 3)*** **Time Management:** Cooperation, blocking semaphores, First In First Out Queue, Thread sleeping, Deadlocks, Monitors, Fixed Scheduling ***(Text Book 2: Chapter 4)*** **Real-time Systems:** Data Acquisition Systems, Priority scheduler, Debouncing a switch, Running event threads as high priority main threads, Available RTOS ***(Text Book 2: Chapter 5)***	

UNIT – V	04 Hours
EMBEDDED SYSTEM TESTING AND DEBUGGING	
Integration and Testing of Embedded Hardware and Firmware: Integration of Hardware and Firmware, Board Bring up ***(Text Book 3: Chapter 12),*** Tools used for testing and debugging**:** ***(Text Book 3: Chapter 13)***	

Course Outcome	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	**Apply** knowledge of embedded system design principles to solve real-world problems.	Apply - Level 4
2	**Design** and implement embedded systems using appropriate hardware and software components.	Synthesis - Level 5
3	**Analyze** and evaluate the performance of embedded systems through testing and debugging techniques.	Analyze - Level 4
4	**Demonstrate** effective teamwork and communication skills in the development of embedded system projects.	Apply - Level 4
5	**Critically assess** the ethical and societal implications of embedded system design.	Evaluate - Level 6

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)												PSOs		
	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3
CO1	3	3	3								2	2	3	3	
CO2	3	3	3		3	2	2	1	3			2	3	3	
CO3	3	3	1		3							2	3	2	
CO4	3	3	3		3	2							3	3	
CO5						3	3	3							3

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Joseph Yiu," The Definitive Guide to ARM® Cortex®-M3 and Cortex®-M4 Processors", 3rd Edition, Newnes, 2013
2. Jonathan Valvano," Embedded Systems: Real-Time Operating Systems for ARM Cortex-M Microcontrollers", 2nd Edition, CreateSpace Independent Pub, 2012.
3. K.V. Shibu," Introduction to Embedded Systems", 2nd Edition, McGraw Hill Education, 2017.

REFERENCE BOOKS:

1. James K. Peckol, "Embedded Systems: A Contemporary Design Tool", Wiley, 2009.
2. Raj Kamal, "Embedded Systems- Architecture, Programming and Design", 3rd Edition, McGraw Hill Education, 2017.

E-Resources:

1. MOOC Course: "Introduction to Embedded Systems" by University of California, Irvine (Link: [www.coursera.org/embedded-systems])
2. Website: Embedded.com (Link: [www.embedded.com])
3. Online Tutorial: "Embedded Systems Tutorial" by Tutorials point (Link: [www.tutorialspoint.com/embedded_system])
4. ARM Procedure Call Standard (AAPCS) Standard documentation (Link: https://developer.arm.com/documentation/dui0041/c/ARM-Procedure-Call- Standard)

Activity Based Learning (Suggested Activities in Class)

1. **Project-based Learning:** Assign a semester-long project where students design and implement an embedded system for a specific application.
2. **Hackathons:** Organize hackathons where students work in teams to solve a given problem using embedded system design techniques.
3. **Guest Speaker Series:** Invite professionals from the industry to share their experiences and projects related to embedded system design.
4. **Case Studies:** Provide students with real-world case studies of successful embedded system designs and ask them to analyze and present their findings.
5. **Prototyping Sessions:** Conduct hands-on sessions where students build and test small-scale embedded system prototypes using development boards and sensors.

LABORATORY EXPERIMENTS

Total Contact Hours: 26

1. Introduction to Microcontrollers: Familiarize students with microcontroller architecture and programming.
2. C as implemented in Assembly: Modify and compile a C program and observe the assembly listing and the map file.
3. General purpose I/O Lab: Implement a simple C program to read from and write to IO pins in the microcontroller.
4. Interrupt Handling: Understand interrupt handling and implement interrupt-driven tasks.
5. Analog-to-Digital Conversion: Learn how to perform analog-to-digital conversion using microcontrollers
6. Timer Lab Exercise: Signal Generator with precision Timing and Buffering
7. PWM Generation: Generate Pulse Width Modulation signals for controlling motor speed.
8. Communication Protocols: Implement I2C or SPI communication protocols between microcontrollers
9. Wireless Communication: Implement wireless communication between two or more embedded systems.
10. Power Management Techniques: Design power-efficient embedded systems using sleep modes and power management techniques
11. Real-Time Operating Systems: Implement a simple real-time task scheduler on a microcontroller.
12. System Debugging and Testing: Learn techniques for debugging and testing embedded systems.
13. Embedded System Project: Design and implement a complete embedded system project, integrating various hardware and software components.

COMPUTER ORGANIZATION AND ARCHITECTURE

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – IV

Course Code	: 22CY2406	**Credits**	: 03
Hours / Week	: 03 Hours	**Total Hours**	: 39 Hours
L–T–P-J	: 3–0–0-0		

Course Learning Objectives:

This Course will enable students to:

1. **Understand** the Architecture and programming of ARM microprocessor.
2. **Develop** program using Arm instruction set and appreciate the advanced features provided in the ARM
3. **Understand** the exception handling techniques.
4. **Study in** detail the concept of instruction level parallelism and concepts of pipelining.
5. **Understand** various cache memory mapping techniques and memory Organization.

Teaching-Learning Process

7. ***Lecture method*** along with traditional lecture method, different *type of teaching methods* may be adopted to develop the course outcomes.
8. ***Interactive Teaching:*** *incorporating* brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and roleplaying.
9. Showing ***Video/animation*** films to explain functioning of various concepts.
10. Encourage ***Collaborative*** (Group Learning) Learning in the class.
11. To make ***Critical thinking***, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
12. Showing the ***different ways to solve*** the same problem and encourage the students to come up with their own creative ways to solve them.

UNIT – I	05 Hours
An Overview of Computing Systems: History of Computers, The Computing Device, **The ARM7TDMI Programmers' Model:** Introduction, Data types, Processor Modes, Registers, Program Status Registers, The vector Table. **Assembler Rules and Directives:** Structure of Assembly Language Modules, Registers, Directives and Macros. **Loads, Stores and Addressing:** LODS and STORES instructions, Operand Addressing, ENDIANNES ***Text Book-1: 1.1 to 1.3; 2.1 to 2.6 ; 4; 5.3, 5.4, 5.5***	
UNIT – II	**05 Hours**
Constants and Literal Pools: The ARM Rotation Scheme, Loading Constants and address into Registers **Logic and Arithmetic:** Flags and their Use, Compare instructions, Data Processing Instructions **Loops and Branches:** Branching, Looping, Conditional Execution, Straight-Line Coding **Subroutines and Stacks:** Stack, Subroutines, Passing parameters to subroutines, The ARM APCS. ***(Text Book-1: 6.1 to 6.4; 7.1 to 7.4; 8.2 to 8.6; 10.1 to 10.5***	
UNIT – III	**05 Hours**
Mixing C and Assembly Language: Inline Assembler Embedded Assembler, Calling Between C and Assembly. **Exception Handling:** Interrupts, Error Conditions, Processor Exception Sequence, The Vector Table, Exception Handlers, Exception Priorities, Procedures for Handling Exceptions. ***(Text Book-1: 11.1 to 11.8; 14.1 to 14.4***	
UNIT – IV	**12 Hours**
Pipelining: Basic and Intermediate Concepts Introduction, The Major Hurdle of Pipelining, How Pipelining Implemented, What makes Pipelining hard to Implement, Extending the MIPS Pipeline to Handle Multicycle Operations, The MIPS R4000 Pipeline, Crosscutting Issues. ***Text Book-2: C.1 to C.7***	

UNIT – V	12 Hours
Memory Hierarchy: Introduction, Cache Performance, Six basic cache Optimizations, Virtual Memory, Protection andexamples of Virtual Memory, Fallacies and Pitfalls. ***Text Book-2: B.1 to B.6***	

Course Outcome	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	**Apply** knowledge of the internal architecture and organization of ARM microprocessors to utilize their components and functionalities.	L3
2	**Apply** the instruction set of ARM Microprocessor by writing Assembly language programs.	L3
3	**Analyze and compare** the various exception handling techniques.	L4
4	**Examine** the concept of instruction-level parallelism and **analyze** the principles of Pipelining techniques.	L4
5	**Compare** and C**ontrast** memory hierarchy and its impact on computer cost/performance.	L4

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	3		2										2	
CO2	3		3		1								2	
CO3	3	3	1										2	
CO4	3	3	1										2	
CO5	3	3	1										2	

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Lo**

TEXT BOOKS:

1. William Hohl, "ARM Assembly Language", 2nd Edition, CRC Press, 2009.
2. John L Hennessy, David A Patterson, "Computer Architecture, A Quantitative Approach", 5th Edition, Morgan Kaufmann publishers, 2012.

REFERENCE BOOKS:

1. David A Patterson, John L Hennessy, "Computer Organization and Design", 4th Edition, Morgan Kaufmann publishers, 2010.
2. Steve Furber, "ARM System-on-chip Architecture", 2nd Edition, Pearson Publications, 2000.
3. Carl Hamacher, Zvonko Vranesic, Safwat Zaky, "Computer Organization", 5th Edition, Tata McGraw Hill, 2002.

E-Resources:

1. https://www.udemy.com/topic/arm-cortex-m/
2. https://www.edx.org/school/armeducation
3. https://onlinecourses.nptel.ac.in/noc22_cs93/preview

Activity Based Learning (Suggested Activities in Class)

1. Mini project implementation using Assembly Language Programming.
2. Demonstration of solution to a problem through programming.

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING

Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

Automata Theory & Compiler Design

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – V

Subject Code	: 23CY3501	**Credits**	: 04
Hours / Week	: 03 Hours	**Total Hours**	: 52(Th)+26(T) Hours
L–T–P–S	: 3–2–0–0		

Course Learning Objectives:

This course will enable students to:

- To provide an understanding of automata, grammars, language translators.
- To know the various techniques used in compiler construction.
- To be aware of the process of semantic analysis.
- To analyze the code optimization & code generation techniques

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

- ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
- ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
- Show ***Video/animation*** films to explain the functioning of various concepts.
- Encourage ***Collaborative*** (Group Learning) Learning in the class.
- To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
- Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**10Hours**

Formal Language and Regular Expressions: Languages, Definition Languages regular expressions, Finite Automata – DFA, NFA. Conversion of regular expression to NFA, NFA to DFA. Context Free grammars and parsing, derivation, parse trees, Application of Finite Automata

UNIT – II	**12 Hours**

Introduction To Compiler, Phases of Compilation, ambiguity LL(K) grammars and LL(1) parsing Bottom up parsing handle pruning LR Grammar Parsing, LALRparsing, parsing ambiguous grammars, YACC programming specification.

Semantics: Syntax directed translation, S-attributed and L-attributed grammars

UNIT – III	**10 Hours**
Intermediate code – abstract syntax tree, translation of simple statements and control flow statements. **Context Sensitive features** – Chomsky hierarchy of languages and recognizers, type checking, type conversions, equivalence of type expressions, overloading of functions and operations.	
UNIT – IV	**08 Hours**
Run time storage: Storage organization, storage allocation strategies scope access to nonlocal names, **Code optimization**: Principal sources of optimization, optimization of basic blocks, peephole optimization	
UNIT – V	**08 Hours**
Code generation: Machine dependent code generation, object code forms, generic code generation algorithm, Register allocation and assignment. Using DAG representation of Block.	
Course Outcomes: At the end of the course the student will be able to: ● Explain the necessity and types of different language translators in use. ● Apply the techniques and design different components (phases) of a compiler. ● Ability to implement practical aspects of automata theory. ● Use the tools Lex, Yacc in compiler construction	

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

SECURITY ENGINEERING AND PROJECT MANAGEMENT

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – V

Subject Code	: 23CY3502	**Credits**	:03
Hours / Week	: 03 Hours	**Total Hours**	: 39 Hours
L–T–P–S	: 3–0–0–0		

Course Learning Objectives:

This course will enable students to:

1. Students will **understand** the importance of identifying and engaging with the security project sponsor, learning to effectively communicate and manage stakeholder expectations throughout the project lifecycle.
2. Students will learn to **identify** the project's critical path and manage it effectively to ensure the project stays on schedule and meets its deadlines.
3. **Develop and document** the processes and methodologies to be followed throughout the project lifecycle.
4. Students will **identify and understand** the key skills required for successfully executing a wireless security project, including technical, analytical, and project management skills.
5. Students will **develop and apply** methods for measuring and evaluating software security to ensure robust protection against vulnerabilities and threats.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT-I **07 Hours**

Introduction to Software Engineering:
The nature of Software, The unique nature of WebApps, Software Engineering, The software Process, the software Engineering practice, The software myths, How it all starts
Textbook 1: Chapter 1: 1.1 to 1.7
Process Models:
A generic process model, Process assessment and improvement, Prescriptive process models, Waterfall model, Incremental process models, Evolutionary process models, Concurrent models, Specialized process models.

Textbook 1: Chapter 2: 2.1 to 2.4

UNIT – II	**08 Hours**

Defining the Security Project:
Defining the Security Problem, Network Security and the CIA, Defining Potential Security Project Solutions, Applying Security Project Constraints, Identifying the Security Project Sponsor.
(Text book 2: chapter 2)

UNIT – III	**08 Hours**

Security and project management:
Project scope, Project plan, Resources, estimating nature and duration of required resources**,** Project and product risk, Measuring software security, Governance and security – Adopting an enterprise software security framework – Security and project management – Maturity of Practice.
(Text Book-3: chapter 7)

UNIT – IV	**08 Hours**

Agile Development:
What is Agility? Agility and the cost of change. What is an agile Process? Extreme Programming (XP), Other Agile Process Models, A tool set for Agile process.
DevOps Fundamentals: Introduction to DevOps, Evolution from Agile to DevOps, Key principles and benefits of DevOps
(Textbook 1: Chapter 3: 3.1 to 3.6, Chapter 4: 4.1 to 4.3)

UNIT – V	**08 Hours**

Wireless Security Project Plan*:*
Types of Wireless Network Components and Devices, Wireless Technologies, Types of Threats, Assessment, Wireless Security Project Parameters, Scope, Schedule, Budget, Key Skills Needed.
(Text Book-2: chapter 12)

Course Outcomes:

At the end of the course the student will be able to:

• Explain the activities involved in software engineering and analyze the role of various process models
• Explain the significance of network security and apply the CIA (Confidentiality, Integrity, Availability) triad to real-world scenarios.
• Explain and implement governance models and enterprise software security frameworks.
• **Explain** various software testing methods and to understand the importance of agile methodology and DevOps
• **Define** key parameters for planning a wireless security project, including scope, schedule, and budget.

TEXT BOOKS:

1. Roger S. Pressman: Software Engineering-A Practitioners approach, 7th Edition, Tata McGraw Hill.
2. 2.S Snedaker - IT Security Project Management Handbook-Syngress.
3. 3.Julia H. Allen - Software Security Engineering_ A Guide for Project Managers_ A Guide for Project Managers (SEI Series in Software Engineering)-Addison-Wesley Professional (2008).
4. Bob Hughes, Mike Cotterell, Rajib Mall: Software Project Management, 6th Edition, McGraw Hill Education, 2018.

REFERENCE BOOKS:

1. Pankaj Jalote: An Integrated Approach to Software Engineering, Wiley India.
2. Software Engineering, by Ian Sommerville 10th edition, Pearson global edition
3. Software Engineering, an Engineering approach-JamesF. Peters, Witold Percy, John Wiley

E-Resources:

1. https://onlinecourses.nptel.ac.in/noc20_cs68/preview
2. https://www.youtube.com/watch?v=WxkP5KR_Emk&list=PLrjkTql3jnm9b5nr-ggx7Pt1G4UAHeFlJ
3. http://elearning.vtu.ac.in/econtent/CSE.php
4. http://elearning.vtu.ac.in/econtent/courses/video/CSE/15CS42.html
   https://nptel.ac.in/courses/128/106/128106012/ (DevOps)

Activity Based Learning (Suggested Activities in Class)

1. Demonstration of solution to a problem using different process models like V model.
2. Real world problem solving and its cost estimation using COCOMO models.
3. Project management activity- Project scheduling using Tools for near real time projects.

4. Testing activity-Writing Test case & Test plan for the real time projects.

****

OPERATING SYSTEMS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – V

Subject Code	: 23CY3503	**Credits**:	04
Hours / Week:03 Hours		**Total Hours** :	45(Th)+30(P) Hours
L–T–P–S	:3–0–2–0		

Course Learning Objectives:

This course will enable students to:

To understand the basic concepts and functions of operating systems.

To understand Processes and Threads

To analyze Scheduling algorithms.

To understand the concept of Deadlocks.

To analyze various Memory and Virtual memory management, File system and storage techniques.

To discuss the goals and principles of protection in a modern computer system.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

Lecture method means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.

Interactive Teaching: *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.

Show ***Video/animation*** films to explain the functioning of various concepts.

Encourage ***Collaborative*** (Group Learning) Learning in the class.

To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.

Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**10 Hours**

OS Overview and System Structure

Introduction to operating systems, System structures: What operating systems do?; Computer System organization; Computer System architecture; Operating System structure; Operating System operations; Process management; Memory management; Storage management; Protection and Security; Distributed system; Computing environments.

Operating System Services: User - Operating System interface; System calls; Types of system calls; System programs; Operating system design and implementation; Operating System structure; Virtual machines.

UNIT – II	**12 Hours**
Process Management: Process Management: Process concept; Process scheduling; Operations on processes. Multi-threaded Programming: Overview; Multithreading models; Threading issues. Process Scheduling: Basic concepts; Scheduling Criteria; Scheduling Algorithms	
UNIT – III	**10 Hours**
Process Coordination Process Synchronization: The critical section problem; Peterson's solution; Synchronization hardware; Semaphores; Classical problems of synchronization; Monitors. Deadlocks: Deadlocks; System model; Deadlock characterization; Methods for handling deadlocks; Deadlock prevention; Deadlock avoidance; Deadlock detection and recovery from deadlock.	
UNIT – IV	**10 Hours**
Memory Management Memory Management Strategies: Background; Swapping; Contiguous memory allocation; Paging; Structure of page table; Segmentation. Virtual Memory Management: Background; Demand paging; Copy-on-write; Page replacement; Allocation of frames; Thrashing	
UNIT – V	**10 Hours**
File System and Secondary Storage Structure File System, Implementation of File System: File system: File concept; Access methods; Directory structure; File system mounting; File sharing. Protection: Implementing File system: File system structure; File system implementation; Directory implementation; Allocation methods; Free space management. Mass storage structures; Disk structure; Disk attachment; Disk scheduling; Disk management; Swap space management. Protection and Security: Protection: Goals of protection, Principles of protection, System Security: The Security Problem, Program Threats, System and Network Threats.	

Course Outcomes:

At the end of the course the student will be able to:

1. **Summarize** basic concepts of operating systems and identify its variants.
2. **Apply** FIFO, SJF, SRT, Priority, Round Robin algorithms to solve process scheduling.
3. **Summarize** process coordination and apply Banker's algorithm to prevent inter-process deadlock.
4. **Distinguish** contiguous and virtual memory management.
5. **Apply** the page replacement algorithms to detect page fault appear in virtual memory.
6. **Apply** FCFS, SSTF, SCAN, C-SCAN, Look and C-Look algorithms to solve I/O scheduling.

Table: Mapping Levels of COs to POs / PSOs														
COs	**Program Outcomes (POs)**												**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	2											2		2
CO2	2	2	2	2								2		2
CO3	2	2	2	2								2		2
CO4	2	2	2	1								2		2
CO5	2	2	2	2								2		2
CO6	2	2	2	2								2		2

1: Poor (Low) **2: Moderate (Medium)** **3: Substantial (High)**

TEXT BOOKS:

1. Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, Operating System Principles 8th edition, Wiley India, 2010.

REFERENCES:

1. Operating Systems-Internals and Design Principles, William Stallings, 6th Edition, Pearson Education, 2009.
2. Operating Systems: A Modern Perspective, Gary J. Nutt, Addison-Wesley, 1997.

E-Resource:

1. https://onlinecourses.nptel.ac.in/noc24_cs80/preview
2. https://onlinecourses.nptel.ac.in/noc24_cs108/preview
3. https://www.coursera.org/learn/codio-intro-to-operating-systems-2-memory-management
4. Modern Operating Systems by Andrew S. Tanenbaum - Known for its comprehensive coverage of modern operating systems principles and design.
5. Operating System Fundamentals - Course (nptel.ac.in)
6. Introduction to Operating Systems - Course (nptel.ac.in)
7. Intro to Operating Systems 1: Virtualization | Coursera
8. Intro to Operating Systems 3: Concurrency | Coursera
9. Intro to Operating Systems 2: Memory Management | Coursera

Activity Based Learning (Suggested Activities in Class)

1. Implementing Operating System concepts by doing Mini projects.
2. Case study to compare various Operating Systems and their performance.
3. Present real-world case studies or problems related to operating systems design and performance optimization, encouraging students to apply theoretical knowledge to

analyze and propose solutions.

LABORATORY EXPERIMENTS

Total Contact Hours: 26

1. Write a C program to create a new process that exec a new program using system calls fork(), execlp() & wait().
2. Write a C program to display PID and PPID using system calls getpid () & getppid ().
3. Write a C program using I/O system calls open(), read() & write() to copy contents of one file to another file.
4. Write a C program to implement multithreaded program using pthreads.
5. Write C program to simulate the following CPU scheduling algorithms.
   . FCFS b) SJF c) Priority d) Round Robin
2. Write a C program to simulate producer-consumer problem using semaphores.
3. Write a C program to simulate Banker's algorithm for the purpose of deadlock avoidance.
4. Write a C program to simulate deadlock detection.
5. Write a C program to simulate paging technique of memory management.
6. Write a C program to simulate page replacement algorithms.
   . FIFO b) LRU c) LFU
2. Write a C program to simulate the following file organization techniques,
   . Single level directory b) Two level directory
2. Write a C program to simulate the following file allocation strategies,
   . Sequential b) Indexed

Open-ended experiments

1. Write a program to simulate dynamic memory allocation using malloc() and free().
2. Set up and manage virtual machines using VirtualBox or VMware.
3. Write a program to navigate and manipulate file directories.

****

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

CRYPTOGRAPHY AND NETWORK SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – V

Subject Code :	23CY3504	**Credits**	:	04
Hours / Week :	03 Hours	**Total Hours**	:	42(Th)+26(P) Hours
L–T–P–S :	3–0–2–0			

Course Learning Objectives:

This course will enable students to:

1. Understand OSI security architecture and classical encryption techniques.
2. Acquire fundamental knowledge on the concepts of finite fields and number theory.
3. Understand various block cipher and stream cipher models.
4. Describe the principles of public key cryptosystems, hash functions and digital signature.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**07 Hours**
Overview: Services, Mechanisms and attacks, the OSI security architecture, Network security model. Classical Encryption Techniques: Symmetric cipher model, Substitution Techniques, Transposition Techniques, Steganography.	
UNIT – II	**09 Hours**
Finite Fields and Number Theory: Groups, Rings, Fields, Modular Arithmetic, Euclid's Algorithm, Finite Fields, Polynomial Arithmetic, Prime Numbers, Fermat's and Euler's Theorem, Testing for Primality, The Chinese Remainder Theorem, Discrete Logarithms. Block Cipher principles, Data Encryption Standard (DES), Triple DES, Block Cipher Modes of Operation, Advanced Encryption Standard (AES).	
UNIT – III	**09 Hours**

Public key cryptography: Principles of public key cryptosystems, The RSA algorithm, El Gamal Cryptosystem, Elliptic Curve Arithmetic, ECC. Symmetric Key Agreement: Diffie Hellman Key exchange, Key management and Distributions. Hash function, SHA, MAC, Authentication requirement, Authentication function, Security of MAC, HMAC, CMAC.

UNIT – IV	**08 Hours**
Digital signature: EI Gamal, Schnorr, DSS. Authentication applications, One way Authentication, Mutual Authentication, Kerberos, X.509 Authentication services.	
UNIT – V	**09 Hours**
Electronic Mail security, PGP, S/MIME, IP security, Web Security, System Security, Intruders, Malicious software, viruses, Firewalls.	

Course Outcome	**Description**	**Bloom's Taxonomy Level**
At the end of the course the student will be able to:		
1	**Analyze** the concepts of services, mechanisms, and attacks within the OSI security architecture and network security model and **Evaluate** the classical encryption techniques like substitution techniques, transposition techniques, and steganography.	L5
2	**Analyze** advanced mathematical concepts and cryptographic algorithms, such as modular arithmetic, finite fields, and block cipher principles, to solve complex problems in information security and encryption.	L4
3	**Evaluate** the security and efficiency public key cryptosystems like RSA, ElGamal, and Elliptic Curve Cryptography (ECC) and **Make use of** key distribution principles to establish session key between two keys.	L5
4	**Apply** cryptographic hash functions, such as SHA, to ensure data integrity in practical scenarios, and implement Message Authentication Codes (MAC), including HMAC and CMAC, to achieve data authentication in secure communication systems.	L3
5	**Analyze** different digital signature algorithms such as ElGamal, Schnorr, and DSS (Digital Signature Standard).	L4
6	**Analyze** the effectiveness of various security measures, including PGP, S/MIME, IP security, Web Security, System Security, Intruders, Malicious software, viruses, and Firewalls, in protecting electronic communication and information systems.	L4

Table: Mapping Levels of COs to POs / PSOs														
COs	**Program Outcomes (POs)**												**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	3	3	3										2	1
CO2	3	2	1		2			1				2	2	2
CO3	3	3	3		2			1				2	2	2
CO4	3	1	1		2			1				2	2	2
CO5	3	2	1		2			1				2	2	2
CO6	3	1						1s				2	2	1

3: Substantial (High) 2: Moderate (Medium) 1: Poor (Low)

TEXT BOOKS:

1. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson, 8thEdition, 2019, ISBN: 9780135764039,0135764033.

REFERENCE BOOKS:

1. BehrouzA.Foruzan, Cryptography and Network Security, Tata McGraw Hill 2007.
2. C K Shyamala, N Harini and Dr. T R Padmanabhan: Cryptography and Network Security, Wiley India Pvt.Ltd
3. Cryptography and Network Security: Atul Kahate, Mc Graw Hill, 3rd Edition.

E-Resources:

1. https://onlinecourses.swayam2.ac.in/cec24_cs16/preview
2. https://www.coursera.org/learn/crypto
3. https://www.coursera.org/learn/cryptography
4. https://www.coursera.org/specializations/applied-crypto

LABORATORY EXPERIMENTS

Total Contact Hours: 26

1. Implement Ceaser cipher using C program.
2. Write a C program to implement transposition cipher.
3. Write a C program that contains a string(char pointer) with a value \Hello World'. The programs should XOR each character in this string with 0 and display the result.
4. Write a C program to implement the Euclid Algorithm to generate the GCD.
5. Write a program to perform encryption and decryption using the following algorithms:
   . Ceaser Cipher
   i. Substitution Cipher
   ii. Hill Cipher
2. Write a Java program to implement the DES algorithm logic.
3. Write a C/JAVA program to implement the Blowfish algorithm logic.
4. Write a C/JAVA program to implement the Rijndael algorithm logic.

5. Write a Java program to implement RSA Algorithm.
6. Implement the Diffie-Hellman Key Exchange mechanism using HTML and JavaScript.

open-ended experiments

1. Write a C program to implement the signature scheme - Digital Signature Standard.
2. To calculate the message digest of a text using the SHA-1 algorithm in Java.
3. Write a program to implement Rail fence Cipher technique

****

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

SECURITY OPERATIONS AND CYBER DEFENSE

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – V

Subject Code	:	23CY3505	**Credits**	:	03
Hours / Week	:	03 Hours	**Total Hours**	:	39 Hours
L–T–P–S	:	3–0–0–0			

Course Learning Objectives:

This course will enable students to:

1. Understand the role and functions of a Security Operations Centre (SOC) in an organization's cybersecurity strategy.
2. Analyze various types of cyber threats and attack vectors, and their implications for security operations.
3. Apply techniques and tools for threat detection, incident response, and threat intelligence.
4. Evaluate the effectiveness of different security operation strategies and frameworks.
5. Design a security operations plan that includes incident response, threat management, and continuous monitoring.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**10 Hours**

SECURITY OPERATIONS AND CHALLENGES IN MODERN DAY:
Introduction, Security Breaches, Common Security Threats: Malware, Phishing, Spear Phishing, Man in the Middle (MitM), Trojans, Ransomware, Denial-of-Service Attack, Distributed Denial-of-Service Attack (DDoS), Attacks on IoT Devices, Data Breaches.
Security Challenges in Modern Day: Cloud Computing, Social Media, Smart Phones, General Data Protection Regulations (GDPR), Attacks Based on Machine Learning and AI, Attacks against Cryptocurrencies and Blockchain Systems, Switching to DevOps, and DevSecOps, Biometric Authentication, File-based and File-less Malware.
(Text Book-1: Chapter 1, 1.1 to 1.4).

UNIT – II	**08 Hours**
ADVANCED PERSISTENT THREAT (APT) AND CYBER DEFENCE MECHANISMS: Introduction to APT attacks, How an APT attack works, Some Instances of APTs, Characteristics of APTs. **Preventive Measures**: Identify the Threats, Cyber Defence Mechanisms & Cybercrimes, Observe All Stakeholders, Usage of Two-Factor Authentication, Auditing, Credit Sign-Off Policy, Protect Vital Data, Risk Assessments, Cybercrime, Risk Factors, Threat Modelling, Role of a Threat Analyst. ***(Text Book-1: Chapter 1, 1.5 to 1.9).***	
UNIT – III	**08 Hours**
CYBER-PHYSICAL SYSTEMS: Introduction, Background Knowledge of CPS, Application Areas of Cyber-Physical System (CPS), Philosophical Issues of CPS, Principle of CPS Operation, Architecture of CPS Layers, Security Threats of CPS, Attacks on CPS, Attacks and Its Consequences, Adversaries Characteristics. ***(Text Book-1: Chapter 3, 3.1 to 3.11).***	
UNIT – IV	**07 Hours**
SECURITY THREAT ANALYSIS AND CYBERWARFARE ASSOCIATED TECHNOLOGIES Introduction, Survivability Network Architecture, SONET and Self-Healing Ring Transportation, Single-Access and Multi-Access Optical Network Ring Architecture, Optical Network Ring Architecture, Channel Demand Routing Ring Architecture, Cyberwar – A New Weapon of Mass Effect, Cyberthreat Intelligence, Countermeasures. ***(Text Book-1 Chapter 2: 2.1 to 2.5, Text Book-2 Chapter 2: 1 to 4***)	
UNIT – V	**06 Hours**
CYBER DEFENCE AND CRITICAL NATIONAL INFRASTRUCTURE (CNI) Introduction, Cyber Operations as a Domain of Warfare, CNI Case Studies in the Energy and Healthcare Sector, Ukraine Power Grid, CNI Attacks Through ICS, SCADA Systems, Cyber Weapons, and Evolution in the Digital Age. ***(Text Book- 2: Chapter 1***)	

Course Outcomes:

At the end of the course the student will be able to:

1. Analyze common security threats like malware, phishing, ransomware, attacks on IoT devices and AI-based attacks, to develop effective strategies for mitigating these threats.
2. Apply appropriate cyber defense mechanisms to mitigate the risks associated with Advanced Persistent Threat (APT) attacks by identifying the threats, performing risk assessments, and implementing two-factor authentication, auditing, and data protection strategies.
3. Analyze the architecture and operation of Cyber-Physical Systems (CPS) to identify and evaluate potential security threats and vulnerabilities.
4. Evaluate survivable network architectures, including SONET and self-healing ring technologies, to ensure robust and resilient communication networks in the context of cyberwarfare and security threats.
5. Analyze the vulnerabilities and threats associated with critical national infrastructure (CNI) in sectors such as energy and healthcare.

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	3	3	2		1				2	2		2	3	
CO2	3	3	2		1				2	2		2	3	
CO3	3	2	1		1				2	2		2	3	
CO4	3	1			1				2	2		2	3	
CO5	2	1	3		1				2	2		2	3	

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Gautam Kumar, Dinesh Kumar Saini, and Nguyen Ha Huy Cuong, "Cyber Defense Mechanisms Security, Privacy, and Challenges", CRC Press, 2021.
2. Hamid Jahankhani, Stefan Kendzierskyj, Nishan Chelvachandran, and Jaime Ibarra, "Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity", Advanced Sciences and Technologies for Security Applications, Springer, 2020.

REFERENCE BOOKS:

1. The Security Operations Center: Building, Operating, and Maintaining your SOC" by Joseph Muniz and Gary McIntyre
2. "Blue Team Handbook: Incident Response Edition" by Don Murdoch
3. "Cybersecurity Ops with bash: Attack, Defend, and Analyze from the Command Line" by Paul Troncone and Carl Albing
4. Various online resources, industry reports, and current articles on cyber defense and security operations

E-Resources:

1. https://www.coursera.org/learn/in-the-trenches-security-operations-center
2. https://www.udemy.com/course/cyber-security-operations-center-csoc-soc-analyst/
3. https://www.udemy.com/course/cyber-security-operations-and-technology-solutions/

Activity Based Learning (Suggested Activities in Class)

1. Modern tools in Security Operation and Cyber Defence.
2. Practical demonstration of cyber defence using various modern tools like firewalls and honeypots.

****

ESS SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – V

Subject Code	:	23CY3506	**Credits**	:	03
Hours / Week	:	03 Hours	**Total Hours**	:	39 Hours
L–T–P–S	:	3–0–0–0			

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**08 Hours**
Security Issues in Mobile Communication: Mobile Communication History, Security – Wired Vs Wireless, Security Issues in Wireless and Mobile Communications, Security Requirements in Wireless and Mobile Communications, Security for Mobile Applications, Advantages and Disadvantages of Application – level Security. (***Text Book-1: Chapter 1: 1.1 to 1.6).***	
UNIT – II	**08 Hours**

Security of Device, Network, and Server Levels: Mobile Devices Security Requirements, Mobile Wireless network level Security, Server Level Security. ***(Text Book-1: Chapter 2: 2.1 to 2.3)***
Application-Level Security in Wireless Networks: Application of WLANs, Wireless Threats, Some Vulnerabilities and Attach Methods over WLANs, Security for 1G Wi-Fi Applications, Security for 2G Wi- Fi Applications, Recent Security Schemes for Wi-Fi Applications.
(Text Book-1: Chapter 3: 3.1 to 3.6).

UNIT – III	**08 Hours**

Application-Level Security in Cellular Networks: Generations of Cellular Networks, Security Issues and attacks in cellular networks, GSM Security for applications, GPRS Security for applications, UMTS security for applications, 3G security for applications, Some of Security
and authentication Solutions. ***(Text Book-1: Chapter 4: 4.1 to 4.7)***

UNIT – IV	**08 Hours**

Application-Level Security in MANETs: MANETs, Some applications of MANETs, MANET Features, Security Challenges in MANETs, Security Attacks on MANETs, External Threats for MANET applications, Internal threats for MANET Applications, Some of the Security Solutions.
(Text Book-1: Chapter 5: 5.1 to 5.8)

Application-Level Security in Ubiquitous Networks: Ubiquitous Computing, Need for Novel Security Schemes for UC, Security Challenges for UC, and Security Attacks on UC networks, Some of the security solutions for UC. ***(Text Book-1: Chapter 6: 6.1 to 6.5)***

UNIT – V	**07 Hours**

Application-Level Security: Introduction, Some of the Heterogeneous Wireless Network, Heterogeneous Network Application in Disaster Management, Security Problems and Attacks in Heterogeneous Wireless Networks, Some Security Solutions for Heterogeneous Wireless Networks. ***(Text Book-1: Chapter 7: 7.1 to 7.5)***

Course Outcomes:

At the end of the course the student will be able to:

1. **Analyze** security requirements and issues in wireless and mobile communications, comparing and contrasting these with wired communication security, and **evaluate** the advantages and disadvantages of application-level security for mobile applications.
2. **Evaluate** application-level security in wireless networks, identifying vulnerabilities, threats, and security schemes for various generations of Wi-Fi applications.
3. **Identify** common security issues and attacks, and **apply** appropriate security and authentication solutions for GSM, GPRS, UMTS, and 3G applications.
4. **Analyze** and **evaluate** the security challenges and threats in Mobile Ad-hoc Networks (MANETs) and Ubiquitous Computing (UC) environments, and propose appropriate security solutions to mitigate these threats.
5. **Analyze** and address security challenges in heterogeneous wireless networks by understanding their applications in disaster management, identifying potential security threats and attacks.

TEXT BOOKS:

1. Pallapa Venkataram, Satish Babu: “Wireless and Mobile Network Security”, 1st Edition, Tata McGraw Hill,2010.

REFERENCE BOOKS:

a. Frank Adelstein, K.S.Gupta : "Fundamentals of Mobile and Pervasive Computing", 1st Edition, Tata McGraw Hill 2005.
b. KavehPahlavan and Prashant Krishnamurthy, "Principles of Wireless Networks", Prentice Hall, 2006.
c. Randall k. Nichols, Panos C. Lekkas : "Wireless Security Models, Threats and Solutions", 1st Edition, Tata McGraw Hill, 2006.

E-Resources:

1. https://www.udemy.com/course/wireless-security/?couponCode=IND21PM
2. https://www.udemy.com/course/learn-wireless-security-from-scratch-2021/?couponCode =IND21PM
3. https://iisecurity.in/courses/wireless-security-course
4. https://www.coursera.org/learn/sscp-4th-ed-course-6

Activity Based Learning (Suggested Activities in Class)

1. Database designing and data extraction using group discussion.
2. Collaborative Activity is minor project development with a team of 4 students.

****

SECURE CODING

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – V

Subject Code	:	23CY3507	**Credits**	:	03
Hours / Week	:	03 Hours	**Total Hours**	:	39 Hours
L–T–P–S	:	3–0–0–0			

Course Learning Objectives:

This course will enable students to:

1. Understand the secure software development lifecycle (SDLC) and best practices in secure coding.
2. Identify and define security requirements for software projects.
3. Recognize common software vulnerabilities and implement preventive measures.
4. Apply secure coding standards and practices during software development and maintenance.
5. Conduct security code analysis and review to ensure robust and secure applications.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**08 Hours**
Secure software development life-cycle: Software development life cycle (Microsoft, McAfee, OWASP etc), development team, Quality and Security, Application Guidelines, (ISC) 2 Ten best practices of secure software development, Security principles, Security Standards Three pillars of software security, Seven Touch points of software security, Security Methodologies, Security Framework, Security Models	

UNIT – II	**08 Hours**
Secure Software Requirements: Introduction, Objective, Sources, Types of Security Requirements, Requirements Engineering for Secure Software, Concepts of Misuse and Abuse, SQUARE Process Model, SQUARE Sample Outputs, Requirements Elicitation and Prioritization, Object Modeling, Threat Modeling	

UNIT – III	**08 Hours**
Secure Software Implementation, : Introduction to Software Vulnerability and Preventive/ Defensive techniques , Vulnerability description, types, Vulnerability Databases, OWASP top 10, NVD, CWE, Common Software Vulnerabilities and Controls, Defensive Coding Practices—Concepts and Techniques :Buffer Overrun, Format String Problems, Integer Overflow, and Injection flaws : SQL Injection, Command Injection, Failure to Handle Errors, Cross Site Scripting, Broken Authentication and Session Management, Magic URLs, Insecure De-serialization	

UNIT – IV	**08 Hours**
Secure Coding Standards: Memory Management, Exception management, Development tools, IDEs tools, Versioning tools, Networking tools, Coding in the cube: Functions, procedures and code blocks, Structuring for Validation, Structured Programming, Debugging, Coding and applying security requirements during maintenance,	

UNIT – V	**07 Hours**

Security code analysis and review: Code review with a tool (fortify, coverty etc.) Code analysis Securing Server, Database, Network and their secure configuration, Firewalls. Case Study: Recent Software vulnerabilities due to insecure programming and how to prevent them during design and implementation.

Course Outcomes:

At the end of the course the student will be able to:

1. Describe and implement secure software development lifecycle practices.
2. Analyze and specify security requirements for software projects.
3. Identify common software vulnerabilities and apply appropriate defensive techniques.
4. Implement secure coding standards and practices in software development.
5. Perform security code analysis and review, and secure configuration of servers, databases, and networks

TEXT BOOKS:

1. Paul, M. (2016). Official (ISC) 2 Guide to the CSSLP. CRC Press.
2. SEACORD, R. (2013). Secure Coding in C and C++ (2 nd Edition). SEI Series in Software Engineering.
3. Howard, Michael, David LeBlanc, and John Viega. "24 Deadly Sins of Software Security.
4. Programming Flaws and How to Fix Them (2010). McGraw-Hill Education.

REFERENCE BOOKS:

1. Ransome, J., & Misra, A. (2018). Core software security: Security at the source. CRC press.
2. Bishop, M. (2019). Computer Security (2 nd Edition). Addison-Wesley Professional.
3. McGraw, G. (2006). Software security: building security in (Vol. 1). Addison- Wesley Professional
4. John Veiga, Gary Mc Graw,"Building Secure Software: How to Avoid Security Problems the Right
5. Way", Addison-Wesley Professional Computing Series, 2001.

E-Resources:

1. https://owasp.org/
2. https://nvd.nist.gov/
3. https://www.microsoft.com/en-us/securityengineering/sdl/

Activity Based Learning (Suggested Activities in Class)

1. Secure Code Review and Analysis
2. Secure Coding Hackathon

****

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

BIG DATA

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – V

Subject Code	:	23CY3508	**Credits**	:	03
Hours / Week	:	03 Hours	**Total Hours**	:	39 Hours
L–T–P–S	:	3–0–0–0			

Course Learning Objectives:

This course will enable students to:

1. **Develop** a comprehensive understanding of the key concepts, principles, and technologies underlying Big Data.
2. **Gain** proficiency in using major Big Data platforms and tools such as Hadoop, Spark, and NoSQL databases.
3. **Develop** the skills to perform data analysis on large datasets using statistical and machine learning methods, and visualize Big Data insights using tools like Tableau, Power BI, or custom visualization techniques.
4. **Understand** how to optimize performance for Big Data applications, including the use of parallel and distributed computing techniques.
5. **Gain** practical experience by applying Big Data techniques to solve real-world problems in various domains such as finance, healthcare, and social media.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**08 Hours**

Introduction to the World of Big Data: Understanding Big Data, Evolution of Big Data, Failure of Traditional Database in Handling Big Data, 3Vs of Big Data, Sources of Big Data, Different Types of Data, Big Data Infrastructure, Big Data Life Cycle, Big Data Technology, Big Data Applications. ***(T1: Chapter 1)***

UNIT – II	**08 Hours**

Big Data Storage Concepts:

Cluster Computing, Distribution Models, Distributed File System, Relational and Non-Relational Databases ,Scaling Up and Scaling Out Storage.

NoSQL Database:

Introduction to NoSQL, Why NoSQL, CAP Theorem, ACID, BASE 56, Schemeless Databases, NoSQL (Not Only SQL), Migrating from RDBMS to NoSQL.

(T1: Chapter 2 and Chapter 3)

UNIT – III	**08 Hours**
Processing, Management Concepts, and Cloud Computing: ***Part I: Big Data Processing and Management Concepts***-Data Processing, Shared Everything Architecture, Shared-Nothing Architecture, Batch Processing, Real-Time Data Processing Parallel Computing, Distributed Computing, Big Data Virtualization, ***Part II: Managing and Processing Big Data in Cloud Computing*** - Introduction, Cloud Computing Types, Cloud Services, Cloud Storage, Cloud Architecture **(T1: Chapter 4)**	
UNIT – IV	**08 Hours**
Driving Big Data with Hadoop Tools and Technologies: Apache Hadoop, Hadoop Storage, Hadoop Computation, Hadoop 2.0, HBASE, Apache Cassandra, SQOOP, Flume, Apache Avro, Apache Pig, Apache Mahout, Apache Oozie, Apache Hive, Hive Architecture, Hadoop Distributions ***(T1: Chapter 5)***	
UNIT – V	**07 Hours**
Big Data Analytics with Machine Learning: Introduction to Machine Learning, Machine Learning Use Cases, Types of Machine Learning **Big Data Visualization:** Introduction to Big Data Visualization, Conventional Data Visualization Techniques, ***Tableau*** -Bar Chart in Tableau, Line Chart, Pie Chart, Bubble Chart, Box Plot, Tableau Use Cases, ***Installing R and Getting Ready***-Data Structures in R, Importing Data from a File, Importing Data from a Delimited Text File, Control Structures in R, Basic Graphs in R. ***(T1: Chapter7 and Chapter 10)***	
Course Outcomes: At the end of the course the student will be able to: 1. **Analyze** complex big data sets to identify patterns and trends. 2. **Design** effective data models to optimize storage and retrieval of big data. 3. **Formulate** strategies for managing and securing large-scale data infrastructures. 4. **Evaluate** the performance of different big data tools and technologies. 5. **Analyze** the advanced algorithms to process and extract valuable insights from big data.	

TEXT BOOKS:

1. Balamurugan Balusamy, Nandhini Abirami. R, "Big Data - Concepts, Technology, and Architecture",
   Wiley Publications, first edition -2021, ISBN 978-1-119-70182-8.

Reference Books:

1. The Lazy-Programmer "Big Data, MapReduce, Hadoop, and Spark with Python Master Big Data Analytics and Data Wrangling with MapReduce Fundamentals using Hadoop, Spark, and Python".
2. Vince Reynolds, "Big Data for Beginners"

E-Resources:

1. https://www.ibm.com/topics/endpoint-security
2. https://www.coursera.org/articles/endpoint-security
3. https://skillsforall.com/course/endpoint-security?courseLang=en-US
4. https://www.sans.org/cyber-security-courses/security-essentials-network-endpoint-cloud/

Activity Based Learning (Suggested Activities in Class)

1. ***Case Study Analysis:*** Students analyze real-world case studies of companies that have
2. ***Group Project on Big Data Infrastructure:*** In groups, students design a big data infrastructure for a hypothetical company, including data storage, processing, and analysis components.
3. ***Hands-on Lab with Big Data Technologies:*** Students use tools like Hadoop, Spark, or NoSQL databases to perform data processing and analysis tasks.
4. ***Data Visualization Exercise:*** Students create visualizations from a large dataset using tools like Tableau or Power BI.
5. ***Data Cleaning and Preprocessing Workshop:*** Students work on cleaning and preprocessing a messy dataset to prepare it for analysis.

****

DATABASE SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – V

Course Code	: 23CY3509	**Credits**	: 03
Hours / Week	: 03 Hours	**Total Hours**	: 39 Hours
L–T–P-J	: 3–0–0-0		

Course Learning Objectives:

This Course will enable students to:

1. To study the different models involved in database security and their applications in real time world to protect the database and information associated with them.

UNIT – I	**09Hours**
Introduction Introduction to Databases Security Problems in Databases Security Controls Conclusions Security Models - Introduction Access Matrix Model Take-Grant Model Acten Model PN Model Hartson and Hsiao's Model Fernandez's Model Bussolati and Martella's Model for Distributed databases	

UNIT – II	**09 Hours**
Security Models - Bell and LaPadula's Model Biba's Model Dion's Model Sea View Model Jajodia and Sandhu's Model The Lattice Model for the Flow Control conclusion Security Mechanisms Introduction User Identification/Authentication Memory Protection Resource Protection Control Flow Mechanisms Isolation Security Functionalities in Some Operating Systems Trusted Computer System Evaluation	

UNIT – III	**08 Hours**
Security Software Design Introduction A Methodological Approach to Security Software Design Secure Operating System Design Secure DBMS Design Security Packages Database Security Design Statistical Database Protection & Intrusion Detection Systems Introduction Statistics Concepts and Definitions Types of Attacks Inference Controls evaluation Criteria for Control Comparison .Introduction IDES System RETISS System ASES System Discovery	

UNIT – IV	**7 Hours**
Models For The Protection Of New Generation Database Systems -1 Introduction A Model for the Protection of Frame Based Systems A Model for the Protection of Object Oriented Systems SORION Model for the Protection of Object-Oriented Databases	

UNIT – V	**10 Hours**
Models For The Protection Of New Generation Database Systems -2 A Model for the Protection of New Generation Database Systems: the Orion Model Jajodia and Kogan's Model A Model for the Protection of Active Databases Conclusions	

Course Outcome	**Description**	**Bloom's Taxonomy Level**

At the end of the course the student will be able to:		
1	Avoid unauthorized data observation and unauthorized data modification.	L3
2	Ensure the data confidentiality and prove that the data integrity is preserved.	L3
3	Prove that, only authorized user has access to the data.	L4
4	Identify security threats in database systems	L4
5	Solve Complex Problems in a Team of database works.	L4

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	3		2										2	
CO2	3		3		1								2	
CO3	3	3	1										2	
CO4	3	3	1										2	
CO5	3	3	1										2	

3: Substantial (High) 2: Moderate (Medium) 1: Poor (Low)

TEXT BOOKS:

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

REFERENCE BOOK:

1. Database security by alfred basta, melissa zgola, CENGAGE learning

INTRODUCTION TO IPR AND REGISTRATION

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER V

Course Code	:	23CY3510	**Credits**	:	02
Hours / Week	:	01 Hours	**Total Hours**	:	26 Hours
L T P	:	1 0 2 0			

Course Learning Objectives:

This Course will enable students to:

1. To understand the concepts IPR
2. To understand Trademarks, Trade Secretes and GI of goods.
3. To understand Copyrights, Patents and Industrial Designs.
4. To learn about how to manage IP rights and legal aspects.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only traditional lecture method, but different *type of teaching methods* may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt the* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher order Thinking questions in the class.
6. Adopt ***Problem Based Learning***, which fosters students' Analytical skills, develop thinking skills such as the ability to evaluate, generalize, and analyse information rather than simply recall it.
0. Show the ***different ways to solve*** the same problem and encourage the students to come up with their own creative ways to solve them.
0. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the students' understanding.

UNIT I	04 Hours

INTRODUCTION TO IPR:

Introduction to Intellectual Property Rights, types of intellectual property, importance of intellectual property rights, Evolution of IP acts and treaties, Agencies responsible for IPR registrations, Role and value of IP in international commerce, Issues affecting IP internationally.

UNIT II	07 Hours

Trade Marks:

Purpose and function of trademarks, Acquisition of trade mark rights, transfer of rights, Selecting and evaluating trademark, registration of trademarks, claims.

Trade Secrets: Trade secret law, determination of trade secret status, liability for misappropriation of trade secrets, trade secret litigation.

UNIT III	07 Hours

COPYRIGHTS:

Fundamentals Of Copyright Law, Originality of Material, Right of Reproduction, Right to Perform the Work Publicly, Copyright Ownership Issues, Notice of Copyright.

PATENTS: Foundation of Patent Law, Patent Searching Process, Basic Criteria of Patentability Industrial Designs: Kind of Protection Provided in Industrial Design. **Managing IP Rights:**

Acquiring IP Rights: letters of instruction, joint collaboration agreement, Protecting IP Rights: non- disclosure agreement, cease and desist letter, settlement memorandum. Transferring IP Rights: Assignment contract, license agreement, deed of assignment.

UNIT IV	08 Hours

DESIGN-
Meaning, Definition, Object, Registration of Design, Cancellation of Registration, International convention on design, functions of Design. Semiconductor Integrated circuits and layout design Act- 2000.

BASIC TENENTS OF INFORMATION TECHNOLOGY ACT-2000
IT Act – Introduction, E-Commerce and legal provisions E- Governance and legal provisions
Digital signature and Electronic Signature.

Course Outcome	Description	Level
At the end of the course the student will be able to:		
1	**Demonstrate** the basic concepts of IPR and their role and value internationally.	L2
2	**Interpret** trademark, their values and trade secrets for liability and litigations.	L3
3	**Devise** knowledge on copyrights, patents and how to manage and protect IP.	L3
4	**Examine** convention on design and basic information technology act.	L3

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	3	3	3	3	3							2		3
CO2	3	3	3	3	3	3			3		3	2		3
CO3	3	3	3	3	3	3			3		3	1		3
CO4	3	3	3	3	3	3			3		3	2		3

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Deborah Bouchoux ,"Intellectual Property: The Law of Trademarks, Copyrights, Patents, and Trade Secrets", 4th Edition, Delmar Cengage Learning.
0. Elizabeth Verkey," Intellectual Property: Law and Practice", 2015 Edition, Eastern Book Company

REFERENCE BOOKS:

1. Kompal Bansal , Parikshit Bansal, "Fundamentals of Intellectual Property for Engineers", 2014, BS Publications.
2. Prabuddha Ganguli," Intellectual property right - Unleashing the knowledge economy", Ganguli, 1st edition (1 July 2017), McGraw Hill Education.

E-Resources:

1. Inventing the Future: An introduction to Patents for small and medium sized Enterprises; WIPO publication No. 917. URL: www.wipo.int/ebookshop.
2. Looking Good : An Introduction to Industrial Designs for Small and Medium-sized Enterprises; WIPO publication No.498. URL: www.wipo.int/ebookshop.
3. Creative Expression: An Introduction to Copyright and Related Rights for Small and Medium-sized Enterprises; WIPO publication No. 918. URL: www.wipo.int/ebookshop
4. Making a Mark: An Introduction to Trademarks for Small and Medium-sized Enterprises; WIPO publication No. 900. URL: www.wipo.int/ebookshop

****

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

FULL STACK DEVELOPMENT

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – V

Course Code	:	23CY3511	**Credits**	:	03
Hours / Week	:	03 Hours	**Total Hours**	:	26 Hours
L–T–P–S	:	1–0–2–0			

Course Learning Objectives:

This course will enable students to:

1. To demonstrate the ability to design basic web pages using HTML and CSS
2. To utilize advanced CSS methods to design the web page, background and components.
3. To experiment with Bootstrap, Javascript and DOM for to create dynamic webpages.
4. To build web pages with the ReactJS and NodeJS as front end and back end.
5. To Model a complete web-page with mangoDB CRUD operations.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.

0. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.

0. Show ***Video/animation*** films to explain the functioning of various concepts.

0. Encourage ***Collaborative*** (Group Learning) Learning in the class.
0. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.

0. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**08 Hours**

Introduction to HTML: HTML syntax, HTML elements, HTML document structure, CSS selectors, properties, and values, Build your first web page, Semantics of HTML, Block and inline elements, Hyperlinks, Lists, Tables, Forms, Create a basic multi page website, Cascading effect, Advanced selectors, CSS resets, Positioning

UNIT – II	**08 Hours**

Introduction to CSS: CSS syntax , Cascading effect, Specificity, Combining and layering selectors, Backgrounds and gradients, CSS resets, The box model, positioning with floats, Creating a grid structure, Precise Positioning, Basic website clone.

UNIT – III	**08 Hours**

Bootstrap and JavaScript Basics: Introduction to Bootstrap, Bootstrap Basics, Bootstrap Grids, Bootstrap Themes, Bootstrap CSS, Bootstrap JS, Fundamentals Of JavaScript, Fundamentals of jQuery, Fundamentals of Ajax Development, Document Object Model, DOM Manipulation, DOM Events, JavaScript Libraries (jQuery and Underscore), Simple HTML CSS JavaScript Project with AJAX.

UNIT – IV	**08 Hours**
ReactJS and NodeJS Development: Introduction and Foundation, Node Projects, Working with shrink-wrap to lock the node modules versions, working with asynchronous programming, Building a HTTP Server with Node.JS using HTTP APIs, React Components, React State and Props, React Event Handling, Routing in React flux, Styling React.	

UNIT – V	**08 Hours**
MongoDB Development: Introduction to NoSQL databases, MongoDB A Database the Modern Web, CRUD Operations in MongoDB, Indexing and Aggregation, Replication and Sharding, Developing Java and Node JS Application with MongoDB. LAMP/WAMP/XAMP	

Table: Mapping Levels of COs to POs / PSOs

COs	**Program Outcomes (POs)**												**PSOs**		
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**	**3**
CO1	3	3	3		3				-						
CO2	3	3	3		3				-						
CO3	2	2	2		3	2			-		3	2	2	2	2
CO4	3	3	3		3	2			-		3	2	2	2	2
CO5	3	1	3		3	2			-		3	2	2	2	2

Text Books:

1. Riaz Ahmed-Full Stack Web Development For Beginners,2021
2. Chris Northwood - The Full Stack Developer: Your Essential Guide to the Everyday Skills
3. Edwin Ross Torres -Full Stack Web Development,2020

Reference Books:

1. Ahmed Bouchefra,- Full Stack Development with Angular and GraphQL, 2022
2. David Choi -Full-Stack React, TypeScript, and Node,2020.
3. Valerio De Sanctis-ASP.NET Core 5 and Angular,2021

E-Resources:

1.Manu Sharma, Full Stack Development with MongoDB, bpb publishers
2.Apress Modern Full-Stack Development by Zammetti

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

INOVATION AND ENTREPRENEURSHIP

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – VI

Subject Code	:	23CY3601	**Credits**	:	02
Hours / Week	:	02 Hours	**Total Hours**	:	39 Hours
L–T–P–S	:	2–0–0–0			

Course Learning Objectives:

This course will enable students to:

1. Identify and analyse the factors that contribute to the process of successfully launching an entrepreneurial venture and managing a new business.
2. Learn the entrepreneurial process from idea generation to implementation.
3. Acquaint with special problems of starting new ventures, finding products and services, which can support new enterprises, and raising capital.
4. Discuss how to start own business and also to work in or with small business or are involved with entrepreneurship.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**08 Hours**

OVERVIEW OF ENTREPRENEURSHIP: THE ENTREPRENEURIAL PERSPECTIVE:

Nature and Development of Entrepreneurship. Defining Manager, Entrepreneur, Entrepreneurship and Entrepreneurship. Key Elements of Entrepreneurship. Personality Characteristics of Successful Entrepreneurs. Common Myths about Entrepreneurs. Ethics and Social Responsibility of Entrepreneurs. Types of Start-Up Firms. Process of New Venture Creation. Role of Entrepreneurship in Economic Development. Emerging Trends and Issues in entership22. Case Study: Successful Entrepreneurs Narayana
Murthy Infosys.

UNIT – II	08 Hours

THE ENTREPRENEURIAL AND ENTREPRENEURIAL MIND:

The Entrepreneurial Process: Identify and Evaluate the Opportunity, develop a Business Plan, Determine the Resources Required, Manage the Enterprise. Managerial Versus Entrepreneurial Decision Making: Strategic Orientation, Commitment to Opportunity, Commitment of Resources, Control of Resources, Management Structure, Entrepreneurial Venturing inside a Corporation, Causes for Interest in Entrepreneurship, Climate for Entrepreneurship, Entrepreneurial Leadership Characteristics. Case study: How to develop effective Business Plan

UNIT – III	08 Hours

CREATIVITY AND BUSINESS IDEA:

Identify and Recognizing Opportunities: Observing Trends and Solving Problems. Creativity: Concept, Components and Types of Creativity, Stages of Creative Process. Sources of New Venture Ideas. Techniques for Generating Ideas. Stages of Analysing and Selecting the Best Ideas. Protecting the Idea: Intellectual Property Rights and its Components. Linking Creativity, Innovation and Entrepreneurship. Case study: Application of Design Thinking in New business ideas generation in particular sector (Health care, Water
Saving, Energy saving)

UNIT – IV	08 Hours

PREPARING THE PROPER ETHICAL AND LEGAL FOUNDATION:

Initial Ethical and Legal Issues Facing a New Firm, establishing a Strong Ethical Culture, choosing an attorney (Lawyer), Drafting a founder's agreement, Avoiding legal disputes, Choosing a form of business organization, Obtaining business licenses and permits, Choosing a Form of Business Ownership (Sole, Proprietorship, Partnership, Corporation & Limited Liability Company) Case study: Start-up Law A to Z IP https://techcrunch.com/2019/02/25/startup-law-a-to-z-intellectual-property/

UNIT – V	07 Hours

MANAGING EARLY GROWTH AND CHALLENGES:

Recruiting and Selecting Key Employees. Lenders and Investors. Funding Requirements: Sources of Personal Financing. Venture Capital. Commercial Banks. Sources of Debt Financing. Key Marketing Issues for New Ventures. Why marketing is critical for Entrepreneurs. Entrepreneurs face unique Marketing Challenges. Guerrilla Marketing. Business Growth: Nature of Business Growth, Planning for Growth, Reasons for Growth. Managing Growth: Knowing and Managing the Stages of Growth, Challenges of Growing a Firm. Strategies for Firms Growth: Internal and External Growth Strategies. Implications of Growth for the Firm and Entrepreneur. Entrepreneurial Skills and Strategies to Overcome Pressures On: Financial Resources (Financial Control, Managing Inventory and Maintaining Good Records). Human Resources, Management of Employees, Time Management. Case study: 9 ways to get startups funded https://www.quicksprout.com/how-to-get-your-startup-funded/

Course Outcome	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Demonstrate knowledge of the key elements of the entrepreneurial Process	L2
2	Employ strategies to generate new ideas for start-ups	L3
3	Outline how to protect IP legally	L2
4	Examine different ways of generating funding	L4
5	Explain organizing managing people, finance and customers	L2

TEXT BOOKS:

1. Barringer, Ireland, "Entrepreneurship: Successfully Learning New Ventures", Pearson, Latest Edition.
2. Hisrich, Peters, Shepherd, "Entrepreneurship", Mc Graw Hill, Sixth Edition.

E-Resources:

0. https://www.mygreatlearning.com/academy/learn-for-free/courses/entrepreneurial-management
0. https://www.careers360.com/courses/mba-in-entrepreneurship-management

****

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

CLOUD SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – VI

Subject Code	:	23CY3602	**Credits**	:	04
Hours / Week	:	03 Hours	**Total Hours**	:	39(Th) +26 (P)Hours
L–T–P–S	:	3–0–2–0			

Course Learning Objectives:

This course will enable students to:

1. Master cloud basics, architecture, and deployment models to improve how your organization manages its IT infrastructure and operations.
2. Master the essential principles and practices of securing cloud-based systems to safeguard data confidentiality, integrity, and availability.
3. Understand and address security risks in cloud computing environments.
4. Understand how to effectively secure cloud computing environments through principles of architecture, trusted methodologies, identity management, and access control.
5. Demonstrate cloud computing life cycle issues, standards, and security measures, and to develop incident response plans.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	08 Hours

Introduction & Cloud Computing Architecture: Cloud computing at a glance: Defining a cloud, A closer look, The cloud computing reference model, Characteristics and benefits Historical developments: Distributed systems, Virtualization, Web 2.0, Service oriented computing, Utility-oriented computing Building cloud computing environments: Application development, Infrastructure and system development, Computing platforms and technologies. The cloud reference model: Architecture, Infrastructure-and hardware-as-a service, Platform as a service, Software as a service .Types of clouds: Public, Private, Hybrid, Open Challenges: Cloud definition, Cloud interoperability and standards, Scalability and fault tolerance, Security, trust, and privacy, Organizational aspects.

UNIT – II	**08 Hours**
Virtualization: Introduction, Characteristics of Virtualized Environments, Taxonomy of Virtualization Techniques - Execution Virtualization, Other types of Virtualization, Virtualization and Cloud Computing, Pros and Cons of Virtualization, Technology Examples – Xen, VMware, Microsoft Hyper-V Cloud Computing Software Security Fundamentals: Cloud Information Security Objectives-Confidentiality, Integrity, and Availability, Confidentiality, Integrity, Availability, Cloud Security Services-Authentication, Authorization, Auditing, Accountability	
UNIT – III	**08 Hours**
Secure Cloud Software Requirement-Secure Development Practices, Approaches to Cloud Software Requirements Engineering, Cloud Security Policy Implementation, NIST 33 Security Principles, *Secure Cloud Software Testing***-**Testing for Security Quality Assurance, Cloud Penetration Testing, Regression Testing. **Cloud Computing Risk Issues and Security Challenges**: The CIA Triad, Privacy and Compliance Risks, Threats to Infrastructure, Data, and Access Control, Cloud Service Provider Risks, Cloud Computing Security Challenges**-**Security Policy Implementation, Computer Security Incident Response Team (CSIRT).	
UNIT – IV	**08 Hours**
Cloud Computing Security Architecture: Introduction, ***Architectural Considerations***- General Issues, Trusted Cloud Computing, Secure Execution Environments and Communications, Microarchitectures, ***Identity Management and Access Control***-Identity Management, Access Control, Autonomic Security	
UNIT – V	**07 Hours**
Cloud Computing Life Cycle Issues: Standards, The Distributed Management Task Force (DMTF), The International Organization for Standardization (ISO), The European Telecommunications Standards, The Organization for the Advancement of Structured, Storage Networking Industry Association (SNIA), Open Grid Forum (OGF), The Open Web Application Security Project (OWASP), Incident Response.	

Course Outcomes:

At the end of the course the student will be able to:

1. **Analyze** cloud computing fundamentals and architecture to optimize resource utilization and enhance organizational efficiency.
2. **Implement** cloud security measures effectively, including authentication, authorization, and auditing, to ensure confidentiality, integrity, and availability of data in cloud computing environments.
3. **Identify** cloud computing risks and security challenges, applying the CIA triad and privacy regulations. **Evaluate** threats to infrastructure, data, and access control, cloud service providers.
4. **Evaluate** cloud security principles, design secure environments and communications, integrate robust identity management, and enforce access controls for autonomic security.
5. **Assess** and **Analyze** cloud computing life cycle issues, standards from DMTF, ISO, ETSI, SNIA, OGF, and OWASP, and develop incident response plans.

Table: Mapping Levels of COs to POs / PSOs														
COs	**Program Outcomes (POs)**												**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	3	2			2							2	2	3
CO2	3		2		3							2	3	3
CO3	3	3	2		2							2	1	2
CO4	3	2			2							2	2	2
CO5	3	2	2		3			3				2	2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Rajkumar Buyya, Christian Vecchiola, S Tamarai Selvi "Mastering Cloud Computing Foundations And Applications Programming" , McGraw Hill Education, 2016.
2. Ronald L. Krutz, Russell Dean Vines “Cloud Security A Comprehensive Guide to Secure Cloud Computing” Wiley Publishing. INC.
3. Kai Hwang, Geoffrey C Fox, Jack J Dongarra, "Distributed and Cloud Computing - From Parallel Processing to the Internet of Things", Morgan Kaufman Publishing, 2012

.

REFERENCE BOOKS:

1.Sirisha Potluri et.al. “Cloud Security Techniques and Applications (Smart Computing Applications)”.
2.Chris Dotson, “Practical Cloud Security A Guide for Secure Design and Deployment”. O’Riley Publishing.

E-Resources:

1. National Institute of Standards and Technology (NIST) - Cloud Computing Security: https://www.nist.gov/topics/cloud-computing-security
2. OWASP Cloud Security Top 10: https://owasp.org/www-project-cloud-security-top-10/
3. SANS Institute - Cloud Security: https://www.sans.org/white-papers/cloud-security/
4. Coursera - "Cloud Security Basics" by Google Cloud: https://www.coursera.org/learn/cloud-security-basics
5. edX - "Cloud Computing Security" by University of Maryland: https://www.edx.org/professional- certificate/cloud-computing-security
6. Pluralsight - "Cloud Security" learning path: https://www.pluralsight.com/paths/cloud-security
7. Cybrary - "Cloud Security Fundamentals" course: https://www.cybrary.it/course/cloud-security- fundamentals/

Activity Based Learning (Suggested Activities in Class)

1. Cloud Security as a group Case study.
2. Collaborative Activity is minor project development with a team of 4 students.

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

LABORATORY EXPERIMENTS

Total Contact Hours: 26

1. Install Oracle Virtual box and create two VMs on your laptop/Desktop.
2. Test ping command to test the communication between the guest OS and Host OS
3. Use gcc to compile c-programs. Split the programs to different modules and create an application using make command
4. Find a procedure to transfer the files from one virtual machine to another virtual machine.
5. Establish an AWS account. Use the AWS Management Console to launch an EC2 instance and connect to it.
6. Launch an EC2 instance in AWS, install and configure CloudWatch and CloudTrail. Simulate an access event and perform basic log analysis to detect the activity.
7. Create a policy in AWS IAM that grants users access to only specific S3 buckets and restricts all other services.
8. Create a new IAM user named john_doe with programmatic access and console access. Attach the following policies to the user: a) AmazonS3ReadOnlyAccess (Read-only access to S3 buckets) b) AmazonEC2FullAccess (Full access to EC2 instances)
9. Use version control systems command to clone, commit, push, fetch, pull, checkout, reset, and delete repositories
10. Develop a Windows Azure Hello World application.
11. Launch GUI applications inside Docker Container & access them from the Docker Host system.
12. Demonstrate at least two methods to block access to ChatGPT (or similar AI services) on a system. Implement and verify the blocking using tools like the hosts file, firewall rules, DNS filtering, or proxy settings.

****

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

TOOLS AND TECHNIQUES FOR ETHICAL HACKING

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – VI

Subject Code :	23CY3603	**Credits** :	04
Hours / Week:	03 Hours	**Total Hours** :	39 (Th)+26(P)Hours
L–T–P–S:	3–0–2–0		

Course Learning Objectives:

This course will enable students to:

1. To understand and analyze Information security threats & countermeasures
2. To perform security auditing & testing
3. To understand issues relating to ethical hacking
4. To study & employ network defense measures
5. To understand penetration and security testing issues

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**08 Hours**

ETHICAL HACKING OVERVIEW & PENETRATION TESTING

Understanding the importance of security, Concept of ethical hacking and essential Terminologies Threat, Attack, Vulnerabilities, Target of Evaluation, Exploit. Phases involved in hacking. Penetration Test – Vulnerability Assessments versus Penetration Test – Pre-Engagement – Rules of Engagement - Penetration Testing Methodologies – OSSTMM – NIST – OWASP – Categories of Penetration Test – Types of Penetration Tests – Vulnerability Assessment Summary -Reports.

UNIT – II	**08 Hours**

FOOTPRINTING & PORT SCANNING

Foot printing - Introduction to foot printing, Understanding the information gathering methodology of the hackers, Tools used for the reconnaissance phase. Port Scanning - Introduction, using port scanning tools, ping sweeps, Scripting Enumeration-Introduction, Enumerating windows OS & Linux OS.

UNIT – III	**08 Hours**
SYSTEM HACKING8 cracking, Keystroke Loggers, Understanding Sniffers, Comprehending Active and Passive Sniffing, ARP Spoofing and Redirection, DNS and IP Sniffing, HTTPS Sniffing	
UNIT – IV	**08 Hours**
HACKING WEB SERVICES & SESSION HIJACKING Web application vulnerabilities, application coding errors, SQL injection into Back-end Databases, cross-site scripting, cross-site request forging, authentication bypass, web services and related flaws, protective http headers Understanding Session Hijacking, Phases involved in Session Hijacking, Types of Session Hijacking, Session Hijacking Tools.	
UNIT – V	**07 Hours**
HACKING WIRELESS NETWORKS Introduction to 802.11, Role of WEP, Cracking WEP Keys, Sniffing Traffic, Wireless DOS attacks, WLAN Scanners, WLAN Sniffers, Hacking Tools, Securing Wireless Networks.	

Course Outcomes:

At the end of the course the student will be able to:

1. **Outline** the influence of security, penetration testing and vulnerability assessment on ethical hacking.
2. **Make use of** port scanning tools like Nmap, OpenVAS and Nessus and ping sweeps such as Hping and Fping to identify open ports and ip addresses of an active host.
3. **Utilize** brute force, key logger, sniffing and spoofing techniques to assess the computational security of a system.
4. **Summarize** sql injection, cross-site scripting and session hijacking techniques to secure e-commerce-based web services.
5. **Perceive** network packets of WLAN using modern tools like WLAN Scanners and WLAN Sniffers.

Table: Mapping Levels of COs to POs / PSOs

COs	**Program Outcomes (POs)**												**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	3				3			3				2	3	3
CO2	3	3	2	2	3		2	3				2	2	3
CO3	3	3	2	2	3		2	3				2	2	2
CO4	3	2		1	2		2	3				2	2	2
CO5	3	2	1	1	3		1	3				2	2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Kimberly Graves, "Certified Ethical Hacker", Wiley India Pvt Ltd, 2010
2. Michael T. Simpson, "Hands-on Ethical Hacking & Network Defense", Course Technology, 2010

REFERENCE BOOKS:

1. Rajat Khare, "Network Security and Ethical Hacking", Luniver Press, 2006
2. Ramachandran V, BackTrack 5 Wireless Penetration Testing Beginner's Guide (3rd ed.). Packt
   Publishing, 2011
3. Thomas Mathew, "Ethical Hacking", OSB publishers, 2003

E-Resources:

1. https://onlinecourses.nptel.ac.in/noc24_cs94/preview
2. https://www.udemy.com/course/complete-ethical-hacking-bootcamp-zero-to-mastery/
3. https://www.coursera.org/projects/metasploit-for-beginners-ethical-penetration-testing
4. https://www.coursera.org/learn/kali-linux

Activity Based Learning (Suggested Activities in Class)

1. vulnerability scanning on a controlled network environment using tools like Nmap, OpenVAS, or Nessus.
2. Organize a Capture the Flag (CTF) competition where students solve various hacking challenges, including web exploitation, cryptography, reverse engineering, and forensics.
3. Create a phishing simulation where students design and execute a phishing campaign within ethical and controlled boundaries.
4. Role-play various social engineering scenarios where students must gather information through techniques like pretexting, baiting, or tailgating.
5. Analyze real-world hacking incidents, discussing the techniques used, the impact, and the countermeasures that could have been implemented.

LABORATORY EXPERIMENTS

Total Contact Hours: 26

1. Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup, ipconfig/ifconfig,ping to gather information about networks and domain registrars.
2. Download and install nmap. Use it with different options to scan open ports, perform OS fingerprinting, do a ping scan, tcp port scan and udp port scan.
3. Using Nmap scanner to perform port scanning of various forms like ACK, SYN, FIN, NULL, XMAS.
4. Using Nmap scanner perform the following ping scan like ping scan, don't ping, ack ping, syn ping,
   udp ping, icmp ping, icmp echo ping, arp ping for host discovery.
5. Study of packet sniffer tools like wireshark and tcpdump.
6. Use the Nessus tool to scan the network for vulnerabilities.
7. Detect ARP spoofing using open-source tool ARPWATCH.
8. Perform ARP Poisoning.
9. Session impersonation using Firefox and Tamper Data add-on.
10. Create a simple keylogger using python.

Open-Ended Experiments

1. Conduct research to identify potential zero-day vulnerabilities in a specific software or hardware system. Document the research methodology, tools used, and any findings. Discuss ethical considerations and responsible disclosure practices.
2. Perform a comprehensive penetration test on a simulated network.
3. Analyze and improve password security.

****

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

CYBER SECURITY ESSENTIALS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER -VI

Course Code	:	23OE0028	**Credits**	:	03
Hours/Week	:	03 Hours	**TotalHours**	:	39 Hours
L–T–P-J	:	3–0–0-0			

Course Learning Objectives:

This Course will enable students to:

1. Understand the foundational concepts of cybersecurity, including threat vectors, cryptography, and virtualization.
2. Explain attacker motivations and techniques used in cyber incidents and advanced threats.
3. Apply networking protocols and security mechanisms to protect enterprise networks and endpoints.
4. Understand security frameworks and deployment models in cloud computing environments.
5. Apply fundamental SecOps concepts, tools, and processes to assess and enhance system security.

Teaching-Learning Process

1. ***Lecture Method:*** Traditional lectures will be used to introduce fundamental concepts such as cryptography, DNS, network security, cloud models, and cybersecurity operations.
2. ***Interactive Teaching:*** Encourage active learning through brainstorming sessions, class discussions, group activities, real-world case studies, focused listening, formulating and answering cybersecurity-related questions.
3. ***Visual Aids:*** Use of videos, animations, and simulations to demonstrate cyber-attack scenarios, encryption processes, firewall mechanisms, and cloud security architecture.
4. ***Collaborative Learning:*** Students will participate in group-based activities like analyzing recent cyber incidents, exploring attacker tactics, and designing small security frameworks.
5. ***Critical Thinking Activities:*** Higher Order Thinking (HOT) questions will be posed during quizzes, scenario analysis, and hands-on exercises that involve network and cloud security problem-solving.
6. ***Multiple Solution Approaches:*** Encourage students to think creatively by exploring and presenting multiple methods to solve security challenges, simulate defense mechanisms, or build secure systems.

MODULE 1: Cybersecurity Foundation	**7Hrs**
Information Assurance Fundamentals, Modern Computing Trends, Application Threat Vectors, Basic Cryptography: Symmetric Encryption, Public Key Encryption, The Domain Name System (DNS), Firewalls, Virtualization.	
MODULE 2: Attacker Techniques and Motivations	**9Hrs**
How Hackers Cover Their Tracks (Antiforensics): How and Why Attackers Use Proxies, Tunneling Techniques, Fraud Techniques: Phishing, Smishing, Vishing, and Mobile Malicious Code, Advanced Persistent Threats (APTs), Bot and Botnets, Rogue Antivirus, Click Fraud, Threat Infrastructure, Cyber-attack Life-cycle (CAL), High-profile Cybersecurity attacks.	
MODULE 3: Network Security Fundamentals	**7Hrs**
Identification of common enterprise network devices, Topologies, Protocols in OSI and TCP model layers, Ports and packet filtering procedures: Routed versus Routing protocols, DNS, FQDN, and IoT, Structure and fields of an IP header, IPV4 and IPV6 addressing, Subnet mask, DHCP and Network Address Translation (NAT), SSH, SSL/TLS.	
MODULE 4: Cloud Security Fundamentals	**9Hrs**
Cloud deployment models, cloud computing service models, cloud native technologies, virtual machines, containers and orchestration, serverless computing, Cloud native security, Kubernetes security, DevOps, and DevSecOps- Security challenges like visibility, governance, and compliance: East-West and North-South traffic protection methods: Layers and capabilities in a Secure Access Service Edge (SASE).	
MODULE 5: Security Operations Fundamentals	**7Hrs**
Key elements of Security Operations (SecOps), SecOps processes: Log forwarding: Security Information and Event Management (SIEM), Security Analysis tools: Security Operations Center (SOC) Engineering: Security Orchestration, Automation, and Response (SOAR) for SecOps: Threat Intelligence: Vulnerability Profiles to secure Endpoints.	

Course Outcome	**Description**	**Bloom's Taxonomy Level**
At the end of the course the student will be able to:		
1	Summarize fundamental cybersecurity concepts such as encryption, DNS, firewalls, and virtual environments.	L2
2	Explain various attacker strategies, including phishing, botnets, and the cyber-attack lifecycle.	L2
3	Apply knowledge of network protocols, addressing, NAT, and secure communication techniques (SSH, SSL/TLS).	L3

4	Illustrate the use of cloud deployment models and describe challenges in cloud-native and DevSecOps environments.	L2
5	Apply security operations tools such as SIEM, SOAR, and threat intelligence to identify and respond to vulnerabilities.	L3

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	3											2	2	1
CO2	3	2										2	2	2
CO3	3	2	2		3							2	2	1
CO4	3		2		2							2	2	2
CO5		2	2	2	3				1	1		3	2	1

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Palo Alto Networks Cybersecurity Survival Guide Fundamental Principles & Best Practices, Fifth Edition, 2020.
2. Cyber Security Essentials, James Graham, Richard Howard and Ryan Olson, CRC Press.

E-Resources:

1. https://onlinecourses.swayam2.ac.in/cec23_cs16/preview
2. https://onlinecourses.swayam2.ac.in/nou23_ge65/preview
3. Introduction to Cyber Security - Course (swayam2.ac.in)
4. https://www.coursera.org/learn/introduction-to-cybersecurity-foundations/

****

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

NETWORK SECURITY ESSENTIALS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER- VI

Course Code	:	23OE0029	**Credits**	:	03
Hours / Week	:	03 Hours	**Total Hours**	:	39 Hours
L–T–P-J	:	3–0–0-0			

Course Learning Objectives:

This Course will enable students to:

1. Understand the foundational concepts of computer networks, OSI and TCP/IP models, and network security models.
2. Explore various security threats and cryptographic techniques for securing network communication.
3. Gain knowledge on authentication mechanisms, secure electronic mail protocols, and DNS security.
4. Analyse IP-level and transport-level security mechanisms such as IPSec, VPN, SSL, and TLS.
5. Evaluate system security techniques including intrusion detection, malware analysis, and firewall configurations.

Teaching-Learning Process

1. ***Lecture method:*** Use whiteboard/presentation-based sessions to introduce theoretical concepts.
2. ***Interactive sessions:*** Group discussions and Q&A on real-world cyber threats and attacks.
3. ***Hands-on labs:*** Simulate authentication, encryption, and firewall configurations using tools like Wireshark, OpenSSL, and VirtualBox.
4. ***Video demonstrations:*** Showcase animations on layered protocols, encryption methods, and real cyber incidents.
5. ***Case study analysis:*** Review recent cyberattacks and discuss how different models/techniques could prevent them.
6. ***Assignments and quizzes:*** Encourage critical thinking and real-time problem solving.

MODULE 1:	**10Hrs**
Overview of Network: Criteria, Network Topologies, Categories of Network. Overview of the Internet: History, Protocol and Standards, Layering Scenario: The OSI model, TCP/IP Protocol Suite, Comparison of the OSI and TCP/IP reference model. OSI Security Architecture, Security Attacks, Services and Mechanisms, A model for Network Security.	

MODULE 2:	**8Hrs**
Key distribution and User Authentication: Symmetric Key distribution, Kerberos, X.509 Certificate, Public-Key Infrastructure, Federated identity management. Electronic Mail Security: Internet Mail	

Architecture, E-mail Formats, E-mail Threats, S/MIME, Pretty Good Privacy (PGP), DNS Security, Domain Keys Identified Mail.	
MODULE 3:	**7Hrs**
IP Security (IPSec): IP Security Overview, IP Security Policy, Encapsulating Security Payload, Combining Security Associations, Internet Key Exchange, IPv4 and IPv6 Security. Virtual Private Network (VPN).	
MODULE 4:	**6Hrs**
Transport layer security: Web Security Considerations, Secure Socket Layer and Transport Layer Security, TLS Record Protocol, Change Cipher Spec Protocol, Handshake Protocol, Alert Protocol, HTTPS, Secure Shell (SSH).	
MODULE 5:	**8Hrs**
System Security: Intruders, Intrusion Detection, Password Management. Malicious Software: Types of Malicious Software, Viruses, Worms, Distributed Denial of Service Attacks. Firewalls: The Need for Firewalls, Firewall Characteristics, Types of Firewalls, Firewall Basing, Firewall Location and Configurations.	

Course Outcome	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Summarize the issues and challenges of Internet essentials to build secure computer network.	L2
2	Experiment with PGP, S/MIME and Domain Keys Identified Mail (DKIM) tools to assess secure email services over the Internet.	L3
3	Make use of key distribution principles to establish session key between two keys.	L3
4	Experiment with IPSec, SSL, TLS, SSH, IKE, HTTPS to inspect transport and IP layer security.	L3
5	Summarize the tools and techniques to assess intrusion detection and prevention in a given network.	L2

Table: Mapping Levels of COs to POs / PSOs														
COs	**Program Outcomes (POs)**												**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	3											2	2	2
CO2	3	2			3		3	2	2			3	2	2
CO3	3	2			3			2	2			3	2	2
CO4	3	2			3			2	2			3	2	2
CO5	3	2			1			1	2			3	2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Behrouz A. Forouzan, "Data Communications and Networking", Fourth Edition, McGraw-Hill.
2. William Stallings, "Network Security Essentials: Application and Standards", ISBN: 9789352866601, Pearson Education, 2016.

E-Resources:

1. Network Security | Coursera
2. Connect and Protect: Networks and Network Security | Coursera
3. Computer Networks and Network Security | Coursera
4. Network Security - Course

****

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

TELECOMMUNICATION SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – VI

Subject Code	:	23CY3604	**Credits**	:	03
Hours / Week	:	03 Hours	**Total Hours**	:	39 Hours
L–T–P–S	:	3–0–0–0			

Course Learning Objectives:

This course will enable students to:

1. **Identify** the basic components and functions of various telecommunication systems.
2. **Describe** the architecture and security mechanisms of mobile networks such as GSM, UMTS, LTE, and 5G**.**
3. **Explain** the functionality of the TCP/IP suite in the context of mobile networks.
4. **Identify** future challenges and opportunities in the field of telecommunication security**.**

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**08 Hours**

An Overview of Wireless Systems: Introduction, First- and Second-Generation Cellular Systems, Cellular Communications from 1G to 3G, Road Map for Higher Data Rate Capability in 3G, Wireless 4G Systems, Future Wireless Networks, Standardization Activities for Cellular Systems.
(***Text Book-1: Chapter 1: 1.1 to 1.7).***

Tele traffic Engineering: Introduction, Service Level, Traffic Usage, Call Capacity, Definitions of Terms, Data Collection, Office Engineering Considerations.
(***Text Book-2: Chapter 1: 2.1 to 2.10).***

UNIT – II	**08 Hours**
Fundamentals of Cellular Communications: Introduction, Cellular Systems, Hexagonal Cell Geometry, Cell Splitting, Adjacent Channel Interference (ACI), Segmentation. (***Text Book-1: Chapter 5: 5.1 to 5.3, 5.8 to 5.10).*** Multiple Access Techniques: Introduction, Narrowband Channelized Systems, Wideband Systems, Comparisons of FDMA, TDMA, and DS-CDMA, Random Access Methods. (***Text Book-1: Chapter 6: 6.1 to 6.5, 6.11).***	
UNIT – III	**08 Hours**
Wireless Application Protocol: Introduction, WAP and the World Wide Web (WWW), Introduction to Wireless Application Protocol, The WAP Programming Model, WAP Architecture, Traditional WAP Networking Environment, WAP Advantages and Disadvantages, Applications of WAP. (***Text Book-1: Chapter 18: 18.1 to 18.8)***	
UNIT – IV	**08 Hours**
Security in Wireless Systems: Introduction, Security and Privacy Needs of a Wireless System, Required Features for a Secured Wireless Communications System, Methods of Providing Privacy and Security in Wireless Systems, Wireless Security and Standards, IEEE 802.11 Security, Security in North American Cellular/PCS Systems, Security in GSM, GPRS, and UMTS, Data Security, Air Interface Support for Authentication Methods, Summary of Security in Current Wireless Systems. (***Text Book-1: Chapter 13: 13.1 to 13.11).***	
UNIT – V	**07 Hours**
Mobile Network and Transport Layer: Introduction, Concept of the TCP/IP Suite in Internet, Network Layer in the Internet, TCP/IP Suite, Transmission Control Protocol, Mobile IP (MIP) and Session Initiation Protocol (SIP), Internet Reference Model. (***Text Book-1: Chapter 14: 14.1 to 14.7)***	

Course Outcomes:

At the end of the course the student will be able to:

1. **Summarize** the progression of wireless systems and optimize the teletraffic networks.
2. **Analyze** and design cellular networks with considerations for cell geometry, interference, and segmentation and evaluate and compare multiple access techniques.
3. **Analyze** the WAP a
4. Architecture and its comparison with traditional web protocols
5. **Summarize** the security mechanisms in North American Cellular/PCS Systems, GSM, GPRS, and UMTS.
6. **Summarize** the operation of Transmission Control Protocol (TCP) and its importance in ensuring reliable communication.

TEXT BOOKS:

1. Vijay K. Garg: "WIRELESS COMMUNICATIONS AND NETWORKING", Elsevier Inc., 2007.

REFERENCE BOOKS:

1. Roger L. Freeman: "Telecommunication System Engineering", 4th Edition, John Wiley & Sons, Inc.,2004.
2. "Telecommunication Networks: Protocols, Modeling and Analysis" by Mischa Schwartz.
3. "Network Security Essentials: Applications and Standards" by William Stallings.
4. "Cryptography and Network Security: Principles and Practice" by William Stallings.
5. "Mobile and Wireless Networks Security and Privacy" by Man Ho Au and Raymond Choo.

E-Resources:

1. https://www.udemy.com/course/5g-4g-lte-3g-2g-cellular-mobile-communications-wireless
2. https://www.coursera.org/learn/business-considerations-for-5g-with-edge-iot-and-ai
3. https://www.coursera.org/learn/network-security-communications-sscp

****

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

APPLICATION SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER: VI

Subject Code	:	23CY3605	**Credits**	:	03
Hours / Week	:	03 Hours	**Total Hours**	:	39 Hours
L–T–P–S	:	3–0–0–0			

Course Learning Objectives:

This course will enable students to:

1. Understand the principles and practices of secure programming.
2. Identify and mitigate security risks in web applications.
3. Apply security measures to protect applications from common threats and attacks.
4. Explore advanced topics and applications of security in various contexts.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**06 Hours**

Introduction to Application Security

Overview of Application Security, Importance and Need for Application Security, - Secure Software Development Lifecycle (SDLC), Secure Requirements Gathering and Analysis, Secure Design Principles, Code Review and Testing for Security.

UNIT – II	**08 Hours**

WEB AND MOBILE APPLICATION SECURITY

INTRODUCTION, LET'S HACK A WEBSITE, HOW BROWSERS WORK, HOW THE INTERNET WORKS, HOW WEB SERVERS WORK, HOW PROGRAMMERS WORK, SESSION HIJACKING, INFORMATION LEAKS, ENCRYPTION, XML ATTACKS, DON'T BE AN ACCESSORY, DENIAL-OF-SERVICE ATTACKS, INJECTION ATTACKS, THIRD-PARTY CODE, CROSS-SITE SCRIPTING ATTACKS, CROSS-SITE REQUEST FORGERY ATTACKS, COMPROMISING AUTHENTICATION, MOBILE EXPLOITS AND MALWARE, IOS

SECURITY MODEL, ANDROID SECURITY MODEL, COMPARING PERMISSION MODELS, WI-FI SECURITY: EVIL TWIN, JASAGER, SSLSTRIP.

UNIT – III	**08 Hours**

PROMPT ENGINEERING SECURITY:

THE POWER OF PROMPT ENGINEERING, FINE-TUNING THE PROMPT WITH TECHNIQUES, PROMPTING FOR TEXT GENERATION, PROMPTING FOR QUESTION ANSWERING, PROMPTING FOR CODE GENERATION, EVALUATING AND TESTING PROMPTS, ETHICAL CONSIDERATIONS IN PROMPT ENGINEERING, SECURITY AND PRIVACY PRESERVING PROMPT ENGINEERING-ISSUES AND CHALLENGES.

UNIT – IV	**10 Hours**

SUPPLY CHAIN SECURITY

INTRODUCTION, BENEFITS OF INVESTING IN SUPPLY CHAIN SECURITY, SUPPLY CHAIN SECURITY MANAGEMENT, MEASURING THE VALUE CREATED BY SUPPLY CHAIN SECURITY, ISO 28000 AND SIX SIGMA, FIVE STEPS OF THE SIX SIGMA PROJECT (DMAIC), OVERVIEW OF CONTEMPORARY SUPPLY CHAIN SECURITY INITIATIVES, SUPPLY CHAIN SECURITY TECHNOLOGIES & THEIR APPLICATIONS: SMART CONTAINERS, TRACKING SYSTEMS, BAR CODE & RFID TAGS, INTRUSION DETECTION SENSORS, ACCESS POINTS, FENCING, IDENTITY MANAGEMENT SYSTEMS (IDMS), ELECTRONIC ACCESS CONTROL SYSTEM (EACS), VEHICLE
ELECTRONIC ACCESS CONTROL SYSTEM (VEACS), CONTAINER DETECTION AND SCREENING EQUIPMENT.

UNIT – V	**08 Hours**

API SECURITY

UNDERSTANDING APIS- GROWING THE API ECONOMY- SECURING APIS WITH TRADITIONAL APPROACHES- MODERN APPROACHES TO SECURING APIS- BENEFITTING FROM AN API SECURITY FRAMEWORK: AUTOMATING YOUR API SECURITY FRAMEWORK- DEVOPS AND DEVSECOPS.

Course Outcomes:

At the end of the course, the student will be able to:

1. Apply secure programming practices to develop robust and secure applications
2. Identify vulnerabilities and implement security measures in web applications
3. Understand and implement security throughout the software development lifecycle
4. Explore advanced topics and applications of security in various domains
5. Analyze and evaluate emerging trends and technologies in application security

TEXT BOOKS:

1. Web Application Hacker's Handbook: Finding and Exploiting Security Flaws by Dafydd Stuttard and Marcus Pinto.
2. API Security for Dummies by Emily Freeman, John Wiley & Sons Inc., 2020.
3. Supply Chain Security Management, Initiatives & Technologies, Thomas Miller, First Edition, 2010.
4. Prompt Engineering Playbook by GovTech Data Science & AI Division, 2023.

REFERENCE BOOKS:

1. "OWASP Testing Guide v4" by OWASP Foundation, 2014.
2. "**Mobile Application Security**: Protecting Mobile Devices and Their Applications" by Himanshu Dwivedi, Chris Clark, and David Thiel, 2012.
3. "**Building Secure and Reliable Systems**: Best Practices for Designing, Implementing, and Maintaining
Systems" by Heather Adkins, Betsy Beyer, Paul Blankinship, and Ana Oprea.
4. **Secure Coding:** Principles and Practices by Mark G. Graff and Kenneth R. van Wyk.

E-Resources:

1. OWASP (https://owasp.org/)
2. NIST (https://www.nist.gov/)
3. https://www.ncsc.gov.uk/collection/supply-chain-security
4. https://project.linuxfoundation.org/hubfs/CNCF_SSCP_v1.pdf
5. https://www.developer.tech.gov.sg/products/collections/data-science-and-artificial- intelligence/playbooks/prompt-engineering-playbook-beta-v3.pdf
6. https://terrorgum.com/tfox/books/security_engineering_a_guide_to_building_dependable_distributed_ systems.pdf
7. https://datasciencehorizons.com/pub/Mastering_Generative_AI_Prompt_Engineering_Data_Science_Horizons_v2.pdf
8. https://arxiv.org/pdf/2404.06001
9. https://www.cybertalk.org/wp-content/uploads/2024/04/The-cyber-security-professionals-guide-to- prompt-engineering .pdf
10. https://owasp.org/www-project-mobile-app-security/
11. https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2019/ITUPITA2018/ITU-ASP-CoE-Training-on-/Mobile%20Apps%20Security_fv.pdf
12. https://www.dhs.gov/sites/default/files/publications/2019_mobilesecurity_rd_programguide_vol3.pdf

Activity Based Learning (Suggested Activities in Class)

1. Hands-on coding exercises to implement secure programming practices
2. Web application vulnerability assessment and remediation exercises.
3. Case studies and group discussions on real-world security incidents and solutions

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

INTERNET OF THINGS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – VI

Subject Code	:	23CY3606	**Credits**	:	03
Hours / Week	:	03 Hours	**Total Hours**	:	39 Hours
L–T–P–S	:	3–0–0–0			

Course Learning Objectives:

This course will enable students to:

1. **Explain** the basic concepts of IoT M2M, and WSN.
2. **Apply** the ARM and CISCO-IRM Models for creating and designing IoT applications for the real-world problems.
3. **Develop** IoT Platforms and Applications using C++ and Python language with Arduino and Raspberry Pi.
4. **Differentiate** IoT, M2M and WSN to construct routing protocols.
5. **Demonstration** of cloud and Big Data-centric modern tools to store and aggregate the IoT Data.
6. **Summarize** IoT-centric security, privacy, and trust issues.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**07 Hours**

FUNDAMENTAL OF IOT:

The Internet of Things, Time for Convergence, Towards the IoT Universe, Internet of Things Vision, IoT Strategic Research and Innovation Directions, IoT Applications, Future Internet Technologies, Infrastructure, Networks and Communication, Hardware Design challenges, Software Development challenges, Security and Privacy challenges.

UNIT – II **07 Hours**

IoT AND M2M :

Introduction, Some Definitions, M2M Value Chains, IoT Value Chains, An emerging industrial structure for IoT, The international driven global value chain and global information monopolies. M2M to IoT-An Architectural Overview Building an architecture, Main design principles and needed capabilities, An IoTmarchitecture outline, Standards considerations. Merits and Demerits of M2M and IoT.

UNIT – III **07 Hours**

WIRELESS SENSOR NETWORKS AND IoT:

Network and Communication aspects, Topology and Coverage, Wireless medium access issues, MAC protocol, Routing protocols, Sensor deployment and Node discovery, Data aggregation and dissemination.

Introduction to Industrial IoT (IIoT) Systems:
The Various Industrial Revolutions, Role of Internet of Things (IoT) & Industrial Internet of Things (IIoT) in Industry, Industry 4.0 revolutions, Support System for Industry 4.0, Smart Factories..

UNIT – IV **07 Hours**

IIoT Data Monitoring & Control:
IoT Gate way, IoT Edge Systems and It's Programming, Cloud computing, Real Time Dashboard for Data Monitoring, Data Analytics and Predictive Maintenance with IIoT technology.

Cyber Physical Systems:
Next Generation Sensors, Collaborative Platform and Product Lifecycle Management, Augmented Reality and Virtual Reality, Artifical Intelligence, Big Data and Advanced Analysis.

UNIT – V **07 Hours**

Industrial IoT- Applications:
Healthcare, Power Plants, Inventory Management & Quality Control, Plant Safety and Security (Including AR and VR safety applications), Facility Management.

Case Studies of IIoT Systems: IIoT application development with Embedded PC based development boards, Development of mini-Project on new version of Operating systems and Edge development board. That project should also address to the current societal needs.

Course Outcomes:

At the end of the course the student will be able to:

1. **Make use of** IoT and its characteristics, ARM and CISCO-IRM models to **develop** IoT applications.
2. **Differentiate** IoT, M2M and WSN plaforms to construct novel routing protocols**.**
3. **Develop** IoT Platforms and Applications using C++ and Python language with Arduino Uno/Nano, ESP-32, and Raspberry Pi support and knowledge of theory and practice related to Industrial IoT Systems.
4. Ability to **identify**, formulate and solve engineering problems by using Industrial IoT.
5. Ability to **implement** real field problem by gained knowledge of Industrial applications with IoT capability.

Table: Mapping Levels of COs to POs / PSOs														
COs	**Program Outcomes (POs)**												**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**1**	**2**
CO1	3	2	3	1	2				2	1		2	3	
CO2	3	3	3	1	2				2	1		2	3	
CO3	3	3	1	1	2				2	1		3	3	
CO4	3	1	1	1	2				2	1		2	3	
CO5	2	1	1	1	1				2	1		2	3	

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. "Internet of Things: Principles and Paradigms" by Rajkumar Buyya, Amir Vahid Dastjerdi.
2. "Building the Internet of Things" by Maciej Kranz.
3. Industry 4.0: The Industrial Internet of Things Alasdair GilchristPublications: Apress
4. The Concept Industry 4.0 An Empirical Analysis of Technologies and Applications in Production Logistics Authors: Bartodziej, Christoph Jan Springer: Publication in the field of economic science.

0. Embedded System: Architecture, Programming and Design by Rajkamal, TMH3.
0. Dr. OvidiuVermesan, Dr. Peter Friess, "Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems", River Publisher

REFERENCE BOOKS:

1. "Internet of Things: A Hands-On Approach" by Arshdeep Bahga and Vijay Madisetti
2. IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things" by David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Rob Barton, Jerome Henry.

****

IMAGE PROCESSING AND DATA PRIVACY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – VI

Subject Code	:	23CY3607	**Credits**	:03
Hours / Week	:	03 Hours	**Total Hours**	: 39 Hours
L–T–P–S	:	3–0–0–0		

Course Learning Objectives:

This course will enable students to:

1. **Explain** the concept of image representation and formation.
2. **Apply** the principals of morphological processing**.**
3. **Differentiate** various reversible steganography techniques.
4. **Summarize** various quantum steganographic techniques.
5. **Get the idea** of digital media steganalysis.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**08 Hours**

Digital Image Representation: What is an image? Resolution and quantization, Image formats, Colour spaces, Images in Matlab, System Engineering and Vulnerability Evaluation; ***(Text Book-1: Chapter 1: 1.1 to 1.5)***

Digital Image Formation: How is an image formed? The mathematics of image formation, The engineering
of image formation; ***(Text Book-1: Chapter 2: 2.1 to 2.3)***

UNIT – II	08 Hours
Pixels: What is a pixel?, Operations upon pixels, Point-based operations on images, Pixel distributions: histograms, Technology: Passive and Active Cyber ISR; ***(Text Book-1: Chapter 5: 5.1 to 5.5)*** **Morphological processing:** Introduction, Binary images: foreground, background and connectedness, Structuring elements and neighbourhoods, Dilation and erosion, Effects and uses of erosion and dilation, Morphological opening and closing, Boundary extraction, Region filling; ***(Text Book-1: Chapter 8: 8.1 to 8.4, 8.7 to 8.11)***	

UNIT – III	08 Hours
Introduction to digital image steganography: Introduction, Applications of steganography, Challenges facing steganography, Steganographic approaches, Performance evaluation; ***(Text Book-2: Chapter 1: 1.1 to 1.5)*** **Reversible steganography techniques: A survey:** Introduction, Difference Expansion (DE) schemes, Histogram-Shifting (HS) schemes, Pixel-Value-Ordering (PVO) schemes, Dual-image-based schemes, Interpolation-based schemes ***(Text Book-2: Chapter 10: 10.1 to 10.6***)	

UNIT – IV	08 Hours
Quantum steganography: Introduction, —Information Security, Goals and tools of quantum steganography, Quantum steganography with depolarizing noise, Steganographic encoding in error syndromes, encoding in the binary symmetric channel, Encoding in the 5-qubit "perfect" code, Secrecy and security, Asymptotic rates in the noiseless case, Asymptotic rates in the noisy case. ***(Text Book-2 Chapter 11: 11.1 to 11.9***)	

UNIT – V	07 Hours
Digital media steganalysis: Introduction, Image steganalysis, Audio steganalysis, Video steganalysis, Text steganalysis, Mission Planning and Force Execution, Mission Assessment. ***(Text Book-2: Chapter 12: 12.1 to 12.5***)	

Course Outcomes:

At the end of the course the student will be able to:

1. **Explain** the fundamental concepts in computer vision and image processing.
2. **Describe** pre-processing of images before more complex tasks such as object detection, classification, or measurement using morphological processing.
3. **Analyze** and apply reversible steganography techniques.
4. **Describe** various quantum steganographic techniques.
5. **Explain** the concept of digital media steganalysis.

Table: Mapping Levels of COs to POs / PSOs														
COs	Program Outcomes (POs)												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	3	2	2		1				2	2		2	3	
CO2	3	2	2		1				2	2		2	3	
CO3	3	2	1		1				2	2		2	3	
CO4	3	1	1		1				2	2		2	3	
CO5	3	1	3		1				2	2		2	3	

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Chris Solomon and Toby Breckon (2011), "Fundamentals of Digital Image Processing", Wiley
2. Mahmoud Hassaballah (2020), "Digital Media Steganography (Principles, Algorithms, and Advances)",
   Elsevier

REFERENCE BOOKS:

1. Shraddha N. Zanjat (2023). "Introduction To Digital Image Processing", International Publication House.
2. Fabien A. P. Petitcolas and Stefan Katzenbeisser (2000) "Information Hiding Techniques for Steganography and Digital Watermaking", Artech House Books, DOI:10.1201/1079/43263.28.6.20001201/30373.5

E-Resources:

1. https://dl.ebooksworld.ir/motoman/Digital.Image.Processing.3rd.Edition.www.EBooksWorld.ir.pdf
2. https://homepages.inf.ed.ac.uk/rbf/CVonline/LOCAL_COPIES/TUDELFT/FIP2_3.pdf
3. http://www.cs.umsl.edu/~sanjiv/classes/cs5420/lectures/intro.pdf

Activity Based Learning (Suggested Activities in Class)

1. Image representation in Matlab, interaction and discussion.
2. Implementation of Stegnographic techniques using Matlab.

****

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING

Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

BLOCKCHAIN TECHNOLOGY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – VI

Subject Code	: 23CY3608	**Credits**	: 03
Hours / Week	: 03 Hours	**Total Hours**	: 39 Hours
L–T–P–S	: 3–0–0–0		

Course Learning Objectives:

This course will enable students to:

1. Learn the underlying principles and techniques associated with blockchain technologies.
2. Understand and describe how blockchain works.
3. Familiarize the Ethereum, smart contracts and related technologies, and solidity language.
4. Understand the application of blockchain in various domain.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**08 Hours**

Introduction to Blockchain: Distributed systems, P2P network Architecture of Blockchain, Generic elements of a blockchain: How blockchain works, Benefits, features, and limitations of blockchain How blockchain accumulates blocks, types of blockchain, Distributed ledger, Consensus Mechanisms-Proof of work, Proof of Stake, Proof of Authority, CAP theorem, Decentralization, Disintermediation, Ecosystem - Storage,
Communication and Computation.

UNIT – II	**08 Hours**
Cryptography and Smart Contracts: Symmetric cryptography (DES, AES), Asymmetric cryptography, Public and Private keys, Algorithms - RSA, Hash functions, SHA, SHA-256 Smart contracts - Benefits of Smart contracts, Solidity Programming-Types, Literals, Enums, write basic program using Solidity, Compile, verify and deploy.	
UNIT – III	**08 Hours**
Ethereum Blockchain: The Ethereum network, Ethereum Virtual Machine Execution Environment, Opcodes and their meaning, Structure of a Block, Genesis Block, Merkle tree, Geth, Transactions, Transaction receipts, Nonce, Gas - gasPrice, gasLimit, Ether, Mining, Wallets, Ethereum network (main net, test net), Metamask	
UNIT – IV	**08 Hours**
Ethereum Development: Infura, Web3.0 for Blockchain, Web3J -Java frontend, Creating Blockchain network and peering, Truffle - build contract, migrate and deploy, Ganache CLI	
UNIT – V	**07 Hours**
Hyperledger: Projects under Hyperledger, Hyperledger reference architecture, Hyperledger design principles, Hyperledger Fabric, Hyperledger Sawtooth, Case study: Blockchain in IoT	

Course Outcomes:

At the end of the course the student will be able to:

1. Outline the basic concepts of blockchain and cryptography, mining, merkle tree concepts used in blockchain to develop decentralized applications.
2. Use solidity programming for smart contract development in real world applications such as library management system, student management system, employee management system.
3. Implement Ethereum blockchain applications using geth, metamask, ganache, truffle blockchain tools.
4. Develop Block chain Application for IoT smart home, healthcare using hyperledger platform.
5. Adapt the advanced concepts of blockchain programming language and tools to develop complex blockchain application

TEXT BOOKS:

1. Mastering Blockchain, Third Edition, Published by Packt Publishing Ltd, Published 2020, Imran Bashir.
2. Solidity Programming Essentials, First Edition, Published by Packt Publishing Ltd, April 2018.
3. Blockchain for Dummies, Manav Gupta, IBM Limited Edition, John Wiley & Sons, Inc. 2017.

REFERENCE BOOKS:

1. Baxv Kevin Werbach, The Blockchain and the new architecture of Trust, MIT Press, 2018.
2. Joseph J. Bambara and Paul R. Allen, Blockchain – A practical guide to developing business, law, and technology solutions, McGraw Hill, 2018.

E-Resources:

1. https://www.coursera.org/specializations/blockchain.
2. https://www.coursera.org/learn/cryptocurrency.

****

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

CYBER ETHICS, PRIVACY & LEGAL ISSUES

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – VI

Subject Code	:	23CY3609	**Credits**	:	03
Hours / Week	:	03 Hours	**Total Hours**	:	39 Hours
L–T–P–S	:	3–0–0–0			

Course Learning Objectives:

This course will enable students to:

1. Deals with all the aspects of Cyber law as per Indian/IT act.
2. Covers overview of Cyber Ethics, Intellectual Property Right and Trademark Related laws with respect to Cyber Space.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**08 Hours**
Cyber Crimes Categories and kinds, Evolution of the IT Act, IT Act, 2000, various authorities under IT Act and their powers. Penalties & Offences, amendments	
UNIT – II	**08 Hours**
Case Laws on Cyber Space Jurisdiction and Jurisdiction issues under IT Act, E –commerce and Laws in India, Digital / Electronic Signature in Indian Laws	
UNIT – III	**07 Hours**
Intellectual Property Rights (IPR), Domain Names and Trademark Disputes, Copyright in Computer Programmes, Concept of Patent Right.	
UNIT – IV	**08 Hours**
Sensitive Personal Data or Information in Cyber Law, Cyber Law – An International Perspective.	

UNIT – V	**08 Hours**
Cyber Ethics and Code, Net Neutrality, Free speech and Censorship in Cyberspace, Intellectual Property in Cyberspace, Privacy Rights and Surveillance.	
Course Outcomes: At the end of the course the student will be able to: 1. Demonstrate a critical understanding of the Cyber law with respect to Indian IT/Act, Cyber Ethics and Intellectual Property Rights..	

Textbooks/ References

1. Sushma Arora, Raman Arora, Cyber Crimes & Laws, 4th Edition 2021, Publisher: Taxmann, ISBN-10: 9390712491
2. N S Nappinai, Technology Laws Decoded, 1st Edition, Publisher: Lexis Nexis, ISBN: 9789350359723
3. Suresh T. Vishwanathan, The Indian Cyber Law, Bharat Law House New Delhi
4. P.M. Bukshi and R.K. Suri, Guide to Cyber and E –Commerce Laws, Bharat Law House, New Delhi
5. Rodney D. Ryder, Guide to Cyber Laws; Wadhwa and Company, Nagpur
6. The Information Technology Act, 2000; Bare Act –Professional Book Publishers, New Delhi
7. Richard A.Spinello, Cyberethics: Morality and Law in Cyberspace: Morality and Law in Cyberspace, 7th Edition, Publisher: Jones & Bartlett Learning, 2020, ISBN-10: 1284184064

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

HARDWARE SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – VI

Subject Code	:	23CY3611	**Credits**	:	03
Hours / Week	:	03 Hours	**Total Hours**	:	39 Hours
L–T–P–S	:	3–0–0–0			

Course Learning Objectives:

This course will enable students to:

1. **Understanding** the hardware security principles, recognize the importance of hardware security in computing systems, and apply knowledge of hardware vulnerabilities and countermeasures to design and evaluate secure hardware systems.
2. **Explore** various countermeasures and mitigation techniques to prevent, detect, and mitigate hardware trojan attacks.
3. **Identify** and assess potential security risks and threats associated with hardware IP piracy, reverse engineering, and IP-based design methodologies.
4. **Understand** the challenges and opportunities associated with integrating nano-scale components into PCB designs for improved security and performance**.**
5. **Explore** countermeasures and defense mechanisms to mitigate system-level attacks and protect the integrity and confidentiality of hardware systems.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

7. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
8. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
9. Show ***Video/animation*** films to explain the functioning of various concepts.
10. Encourage ***Collaborative*** (Group Learning) Learning in the class.
11. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
12. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**08 Hours**

Hardware Security Principles and Random Number Generators:

Introduction to Hardware Security, Hardware Vulnerabilities, Countermeasures, Random Number Generators (RNGs) ***(Text Book-1: Chapter 1: 1.1 to 1.5, Text Book-2: chapter 5).***

UNIT – II	**08 Hours**
Hardware Trojans: Understanding SoC design flow and the nature of hardware Trojans, identifying hardware Trojans in FPGA designs, categorizing different types of hardware Trojans and implementing countermeasures. ***(Text Book-1: Chapter 5: 5.1 to Chapter 5.5.8).***	
UNIT – III	**07 Hours**
Hardware IP Piracy and Reverse Engineering: Understanding the concept of hardware IP and the associated security issues in IP-based SoC design, Addressing security concerns specific to FPGA designs. ***(Text Book-1: Chapter 7:7:1 to 7.7).***	
UNIT – IV	**08 Hours**
Side-Channel Attacks and PCB Security Challenges*:* Exploring various types of side-channel attacks, including power analysis, electromagnetic, fault injection, and timing attacks, Understanding security challenges and attack models for PCB, with practical experiments like bus snooping attacks**,** ***(Text Book-1: Chapter 8:8.1 to 8.6, Chapter 11:11.1.to 11.3).***	
UNIT – V	**08 Hours**
Countermeasures and Emerging Trends*:* Implementing hardware security primitives and obfuscation techniques, designing for security and evaluating trust in hardware systems, Exploring the latest trends in hardware attacks and protections, and understanding system-level attacks and countermeasures, ***(Text Book-1: Chapter 16:16:1 to 16.5).***	
<u>Course Outcomes:</u> At the end of the course the student will be able to: 4. Ability to analyse common hardware vulnerabilities, implement effective countermeasures, and apply theoretical knowledge of random number generators (RNGs) in practical settings. 5. Understanding the Hardware Trojans, including their detection and prevention in both SoC and FPGA designs. Students will gain practical experience through hands-on experiments, enhancing their ability to address hardware security challenges in real-world scenarios. 6. Students with the knowledge and skills to address security challenges in IP-based SoC design and FPGA- based systems, ensuring the integrity and confidentiality of hardware designs and intellectual property. 7. Students with know-how to create safe hardware primitives, investigate cutting-edge technologies to improve hardware security, and assess and mitigate security risks in hardware designs. 8. Students should be equipped with the knowledge and skills necessary to analyse, design, and implement secure hardware systems, as well as identify and mitigate various hardware-level security threats and vulnerabilities.	

TEXT BOOKS:

1. Hardware Security: Design, Threats, and Safeguards Debdeep Mukhopadhyay, Rajat Subhra Chakraborty
2. Hardware Security: A Hands-On Learning Approach" by Swarup Bhunia, Mark Tehranipoor, and Cliff Wang.

REFERENCE BOOKS:

1. Introduction to Hardware Security and Trust" by Mohammad Tehranipoor and Cliff Wang.
2. Principles of Hardware Security" by Wayne Burleson and Cynthia A. Pasquale

E-Resources:

1. https://www.coursera.org/learn/hardware-security
2. https://onlinecourses.nptel.ac.in/noc22_cs48/preview

****

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING

Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

UNIVERSAL HUMAN VALUES

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – VI

Subject Code	:	23CY3612	**Credits**	:	2
Hours / Week	:	03 Hours	**Total Hours**	:	26 Hours
L–T–P–S	:	1–0–2–0			

Course Learning Objectives:

This course will enable students to:

- Appreciate the essential complementarity between 'VALUES' and 'SKILLS' to ensure sustained happiness and prosperity which are the core aspirations of all human beings.
- Facilitate the development of a Holistic perspective among students towards life and profession as well as towards happiness and prosperity based on a correct understanding of the Human reality and the rest of existence. Such a holistic perspective forms the basis of Universal Human Values and movement towards value-based living in a natural way.
- Highlight plausible implications of such a Holistic understanding in terms of ethical human conduct, trustful and mutually fulfilling human behaviour and mutually enriching interaction with Nature.
- Provide a much-needed orientation input in value education to the young enquiring minds

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**04 Hours**

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

UNIT – II	**04 Hours**
Harmony in the Human Being : Understanding Human being as the Co-existence of the Self and the Body, Distinguishing between the Needs of the Self and the Body, The Body as an Instrument of the Self, Understanding Harmony in the Self, Harmony of the Self with the Body, Programme to ensure self-regulation and Healt	
UNIT – III	**03 Hours**
Harmony in the Family and Society : Harmony in the Family – the Basic Unit of Human Interaction, 'Trust' – the Foundational Value in Relationship, 'Respect' – as the Right Evaluation, Other Feelings, Justice in Human-to Human Relationship, Understanding Harmony in the Society, Vision for the Universal Human Order	
UNIT – IV	**04 Hours**
Harmony in the Nature/Existence : (3 hours) Understanding Harmony in the Nature, Interconnectedness, self-regulation and Mutual Fulfilment among the Four Orders of Nature, Realizing Existence as Co-existence at All Levels, The Holistic Perception of Harmony in Existence	
UNIT – V	**03 Hours**
Implications of the Holistic Understanding – a Look at Professional Ethics : Natural Acceptance of Human Values, Definitiveness of (Ethical) Human Conduct, A Basis for Humanistic Education, Humanistic Constitution and Universal Human Order, Competence in Professional Ethics Holistic Technologies, Production Systems and Management Models-Typical Case Studies, Strategies for Transition towards Value-based Life and Profession	

Course Outcomes:

At the end of the course the student will be able to:

1. They would become more responsible in life, and in handling problems with sustainable solutions, while keeping human relationships and human nature in mind.
2. They would have better critical ability.
3. They would also become sensitive to their commitment towards what they have understood (human values, human relationship and human society).
4. It is hoped that they would be able to apply what they have learnt to their own self in different day-to-day settings in real life, at least a beginning would be made in this direction.

Textbook and Teachers Manual

1. The Textbook A Foundation Course in Human Values and Professional Ethics, R R Gaur, R Asthana, G P Bagaria, 2nd Revised Edition, Excel Books, New Delhi, 2019. ISBN 978-93-87034- 47-1
2. The Teacher's Manual for A Foundation Course in Human Values and Professional Ethics, R R Gaur, R Asthana

Reference Books

1. Jeevan Vidya: Ek Parichaya, A Nagaraj, Jeevan Vidya Prakashan, Amar kantak, 1999.
2. Human Values, A.N. Tripathi, New Age Intl. Publishers, New Delhi, 2004.
3. The Story of Stuff (Book).
4. The Story of My Experiments with Truth - by Mohandas Karamchand Gandhi
5. Small is Beautiful - E. F Schumacher. 6. Slow is Beautiful - Cecile Andrews

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

RESEARCH WRITING

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – VI

Subject Code	:	23CY3613	**Credits**	:	2
Hours / Week	:	03 Hours	**Total Hours**	:	26 Hours
L–T–P–S	:	1–0–2–0			

Course Learning Objectives:

This course will enable students to:

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. ***Lecture method*** means it includes not only the traditional lecture method but a different *type of teaching method* that may be adopted to develop the course outcomes.
2. ***Interactive Teaching:*** *Adopt* ***Active learning*** that includes brainstorming, discussing, group work, focused listening, formulating questions, note-taking, annotating, and roleplaying.
3. Show ***Video/animation*** films to explain the functioning of various concepts.
4. Encourage ***Collaborative*** (Group Learning) Learning in the class.
5. To make ***Critical thinking***, ask at least three Higher-order Thinking questions in the class.
6. Discuss how every ***concept can be applied to the real world*** - and when that's possible, it helps improve the student's understanding.

UNIT – I	**04 Hours**

Fundamentals of Research Writing: Introduction to research writing - Knowing the details of research writing - Planning the purpose and material - Practicing for the audience and content delivery - Processing the steps, activities and outputs

UNIT – II	**04 Hours**

Different Methods in Research Writing: Nature and meaning of research methods - Types of research - pure and applied research - Types of communication research – Quantitative, Qualitative and Rhetorical - Questionnaire and observation methods - Data collection and data analysis - Thesis/Synopsis writing - Structure and importance

UNIT – III	**03 Hours**

Mechanics and Conventions of Research Writing :Research writing in broader spectrum - The tone -The language - Conventions of research – Evidence-based arguments - Thesis-driven analysis - Complexity and higher- order thinking

UNIT – IV	**04 Hours**

Components of Research Writing: Formatting a research paper – Title page – Abstract – Introduction – Methodology – Conclusion – Proof reading – Citing sources

UNIT – V	**03 Hours**
Effective Research Presentation: Introduction- Definition, meaning, purpose and method – Personal skill – Language skill – Content development – Gathering supporting evidence	

Course Outcomes:

At the end of the course the student will be able to:

1. Understand and can create effective research writing documents for end-users.
2. Follow writing process and strategies to produce clear, high-quality research papers in a multitude of technical writing genres.
3. Apply professional research writing conventions of clean and clear design, style, and layout of written materials.
4. Analyze research documents appropriately with citing resources.
5. Present research paper clearly, concisely and effectively.

REFERENCES

1. Work book for Advanced Research and Writing by Dr. L. Kavitha Nair, EFL, SRMIST, KTR.
2. Introducing Research Methodology: A Beginner's Guide to Doing a Research Project - Uwe Flick
3. Research Design: Qualitative, Quantitative and Mixed Methods Approaches - J. David Creswell and John W. Creswell
4. The Craft of Research - Gregory G. Colomb, Joseph M. Williams, and Wayne C Booth
5. Foundations of Behavioral Research - Fred N. Kerlinge
6. Technical Writing Style by – Dan Jones, Sam Dragga
7. Handbook of Technical Writing by – Walter. E.ollu
8. Technical Writing Process by – Kieran Morgan and Sanja Spejic

ONLINE RESOURCES

1. https://www.freelancewriting.com/copywriting/what-is-technical-writing/
2. https://web.mit.edu/me-ugoffice/communication/technical-writing.pdf
3. https://www.nitorinfotech.com/blog/best-practices-for-technical-writing

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

RISK ASSESSMENT AND SECURITY AUDIT

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VII

Course Code	:	23CY4701	**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To equip students with the knowledge and practical skills required to identify, assess, and audit security risks in information systems using industry-recognized standards and methodologies.

Course Objectives:

This course will enable students to:

1. To understand the fundamentals of risk assessment and security auditing
2. To analyse threats, vulnerabilities, and risk evaluation techniques
3. To learn audit processes, standards, and compliance requirements
4. To apply tools and techniques for security assessment and auditing
5. To develop reporting and mitigation strategies based on audit findings

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. Lecture sessions combined with demonstrations of risk assessment and auditing techniques.
2. Case study analysis based on real-world audit scenarios and security breaches.
3. Hands-on exposure to auditing tools and vulnerability assessment methods.
4. Group discussions and collaborative audit exercises to enhance analytical skills.
5. Scenario-based problem solving and report writing to develop practical auditing skills.

MODULE – I	**09 Hours**

Fundamentals of Risk Assessment - Risk concepts, threat and vulnerability, asset identification, risk management process, qualitative and quantitative risk analysis, risk evaluation techniques, risk matrix, likelihood and impact analysis.

MODULE – II	**09 Hours**

Threat Modeling and Vulnerability Assessment - Threat modeling concepts, STRIDE and DREAD models, vulnerability identification, vulnerability scanning tools, penetration testing basics, attack surface analysis, CVSS scoring, risk prioritization.

MODULE – III	**09 Hours**

Security Audit Standards and Frameworks - NIST guidelines, ISO/IEC 27001 standards, ISO/IEC 27005, COBIT framework, audit principles, audit lifecycle, compliance requirements.

MODULE – IV	**09 Hours**

Security Audit Process and Tools - Audit planning, audit scope and objectives, data collection techniques, checklist-based auditing, vulnerability scanners, configuration review tools, log analysis, audit documentation, evidence collection.

MODULE – V	09 Hours
Reporting, Compliance and Case Studies -Audit reporting techniques, risk communication, remediation strategies, compliance auditing, legal and ethical issues, case studies of security audits, best practices in audit management.	

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Understand risk assessment concepts, threats, and vulnerabilities.	L2
2	Perform systematic risk analysis using standard methodologies .	L3
3	Apply security audit frameworks and standards such as NIST and ISO/IEC 27001.	L3
4	Conduct security audits and interpret findings	L4
5	Recommend mitigation strategies and prepare audit reports.	L5

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

	Program Outcomes (POs)											PSOs	
COS	1	2	3	4	5	6	7	8	9	10	11	1	2
CO-1	3	2										3	2
CO-2	3	3	2	2								3	2
CO-3	2	3	3	2	1							2	3
CO-4	2	2	3	3	2							3	3
CO-5	2	2	2	3	3	2						2	3

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. *Information Security Risk Assessment Toolkit* – Joshua Feldman
2. *Security Risk Assessment Handbook* – Douglas Landoll

REFERENCE BOOKS:

1. *The Basics of IT Audit* – Stephen D. Gantz
2. *Information Security Policies and Procedures* – Thomas Peltier

E-RESOURCES:

RECOMMENDED TOOLS

- Vulnerability Assessment Tools: Nessus, OpenVAS, Qualys
- Network Scanning Tools: Nmap, Netcat
- Packet Analysis Tools: Wireshark, tcpdump
- Log Analysis and SIEM Tools: Splunk, ELK Stack (Elasticsearch, Logstash, Kibana)
- Risk Assessment Tools: OCTAVE, FAIR model tools

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

CRYPTOGRAPHY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VII

Course Code	:	23OE0053	**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

To create awareness of cryptographic techniques and enable students to understand and apply fundamental concepts for securing digital information and communication in real-world systems.

Course Objectives:

This course will enable students to:

1. Introduce basic concepts of cryptography and its role in information security.
2. Explain fundamental encryption techniques used in modern digital systems.
3. Illustrate applications of cryptographic methods in real-world scenarios.
4. Develop understanding of authentication, data integrity, and secure communication.
5. Create awareness about common security threats and protection mechanisms.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

1. **Lecture method** along with presentation-based teaching to explain cryptographic concepts.
2. **Interactive Teaching:** brainstorming, discussions, and case studies on real-world security scenarios.
3. **Showing video/animation films** to demonstrate encryption, hashing, and secure communication.
4. **Encourage Collaborative (Group Learning) learning** through mini-projects and problem-solving.
5. To **develop critical thinking, asking higher order thinking questions** through quizzes and case-based analysis.
6. **Demonstrating multiple approaches** to solve security problems and encouraging innovative solutions.

MODULE – I: Introduction to Cryptography	**10 Hours**

Introduction to cryptography: security goals, basic terminology. Classical cryptography: Caesar cipher, substitution cipher, limitations and cryptanalysis. Need for modern cryptography. Overview of cryptography in real-world systems (messaging apps, banking, internet security).

Applications: Secure messaging systems, Password protection, Data privacy in online platforms

AI Integration: Data privacy in AI applications, Secure handling of user data

Authentic Intelligence: Risks of weak security practices, Awareness of data protection

MODULE – II: Symmetric Key Cryptography	**08 Hours**

Concept of symmetric key encryption, block ciphers, Data Encryption Standard (DES), Advanced Encryption Standard (AES), modes of operation. Applications in real-world systems.

Applications: File and disk encryption, Wi-Fi security, Data protection in devices

AI Integration: Protecting AI datasets, Secure storage of model data

Authentic Intelligence: Choosing secure encryption methods, Avoiding weak configurations

MODULE – III: Public Key Cryptography	**09 Hours**
Asymmetric cryptography, public and private keys, RSA, Diffie-Hellman key exchange, digital certificates, secure communication. **Applications:** Secure web browsing, Online banking, Secure communication systems **AI Integration:** Secure communication in distributed AI, Cloud-based AI security **Authentic Intelligence:** Trust in digital communication, Ethical use of cryptographic systems	
MODULE – IV: Hashing & Digital Signatures	**09 Hours**
Cryptographic hash functions (SHA-256), password hashing, MAC, digital signatures, authentication vs authorization. **Applications:** Secure login systems, Data integrity verification, Digital document authentication **AI Integration:** Data integrity in AI pipelines, Secure authentication in AI systems **Authentic Intelligence:** Preventing data tampering, Responsible authentication practices	
MODULE – V: Cryptography in Practice & Security Attacks	**09 Hours**
SSL/TLS, cryptography in blockchain and cloud systems. Common attacks: phishing, replay attacks, Man-in-the-Middle attacks. Case studies of data breaches. **Applications:** Secure web communication (HTTPS), Cloud security, Cybersecurity awareness **AI Integration:** AI-based threat detection, Secure AI communication **Authentic Intelligence:** Awareness of cyber threats, Responsible digital behavior	

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Explain fundamental concepts of cryptography, classical encryption techniques, and their role in securing information.	L2
2	Describe and apply symmetric key cryptographic techniques such as AES and modes of operation in real-world scenarios.	L3
3	Explain and apply public key cryptography concepts including RSA, Diffie-Hellman, and digital certificates for secure communication.	L3
4	Analyze hashing techniques and digital signatures for ensuring data integrity and authentication.	L3
5	Evaluate cryptographic applications in real-world systems and analyze common security threats with appropriate protection mechanisms.	L5

Table: Mapping Levels of COs to POs / PSOs													
COs	**Program Outcomes (POs)**											**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**
	Engineering knowledge	Problem analysis	Design/ Development of Solutions	Conduct investigations of complex problems	tool usage	The engineer and society	Ethics	team work	Communication	Project management and finance	Life-long learning	Programming & core computing skills	Cybersecurity & data protection skills
CO1	3	2	-	-	-	-	-	-	-	-	1	2	2
CO2	3	2	2	-	2	-	-	-	-	-	1	3	2
CO3	3	3	2	1	2	-	-	-	-	-	1	3	3
CO4	3	2	3	2	2	-	-	-	-	-	1	3	3
CO5	2	3	2	2	2	1	1	-	-	-	2	2	3

Mapping Levels of COs to POs / PSOs

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. William Stallings, Cryptography and Network Security, Pearson
2. Behrouz A. Forouzan, Cryptography and Network Security, McGraw Hill.

REFERENCE BOOKS:

1. Jonathan Katz & Yehuda Lindell, Introduction to Modern Cryptography
2. Christof Paar & Jan Pelzl, Understanding Cryptography
3. Bruce Schneier, Applied Cryptography.

RECOMMENDED TOOLS

- Python
- hashlib
- PyCryptodome
- Jupyter Notebook

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

DIGITAL FORENSICS

[Open Elective - Applicable to All Engineering Branches]

SEMESTER - VII (As per CBCS Scheme)

Course Code	:	23OE0054	**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L-T-P-J	:	3-0-0-0	**CIE+SEE**	**:**	60+40 Marks

Eligible Branches: Civil Engineering | Mechanical Engineering | Electrical & Electronics Engineering | Electronics & Communication Engineering | Information Science Engineering | Biotechnology | Aerospace Engineering | Industrial Engineering | All other B.E. / B.Tech programs

Prerequisite: Basic Computer Operation & Internet Usage. No prior programming or cybersecurity knowledge required.

Course Vision: To develop awareness, investigative thinking, and practical skills in digital forensics among engineering students of all disciplines — enabling them to identify, preserve, and analyze digital evidence from computers, mobile devices, and networks, and apply forensic principles responsibly in their professional and academic domains.

Course Objectives: This course will enable students:

1. To understand the digital forensics lifecycle, legal framework, and ethical responsibilities in investigating digital evidence across engineering and professional environments.
2. To identify and analyze digital evidence from computers, storage devices, and file systems using accessible forensic tools without requiring programming expertise.
3. To investigate digital artifacts from email, social media, mobile devices, and IoT systems relevant to engineering industries.
4. To understand network-based evidence, cybercrime investigation techniques, and the role of digital forensics in industrial control systems and critical infrastructure.
5. To document forensic findings, produce professional investigation reports, and apply digital forensic awareness in engineering project and workplace contexts.

Teaching-Learning Process (General Instructions)

These are sample pedagogical methods where the teacher can use to accelerate the attainment of the various course outcomes. Since this is an open elective for all engineering branches, methods are designed to be inclusive and accessible without programming prerequisites:

1. **Lecture method** along with traditional lecture method, different type of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and roleplaying.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them.

MODULE - I: Introduction to Digital Forensics	**09 Hours**

Topics:

What is Digital Forensics: Definition, scope, goals, and importance in the digital age; Difference between digital forensics, cybersecurity, and cyber law; Categories of digital evidence: structured, unstructured, and volatile data. Digital Forensics Lifecycle: Identification, preservation, collection, examination, analysis, and presentation of evidence. Legal & Ethical Framework: Indian IT Act 2000 and its amendments; Evidence Act provisions for electronic records; Chain of custody: definition, importance, and documentation; Admissibility of digital evidence in Indian courts.

AI Integration:

Discussion of how AI is changing the landscape of digital evidence in engineering contexts; Introduction to using AI assistants (ChatGPT, Claude) for legal research and forensic report drafting.

Authentic Intelligence:

Understanding the boundaries between forensic investigation and invasion of privacy; Ethical obligations when discovering colleague misconduct through digital evidence;

MODULE - II: Computer & Storage Media Forensics	**09 Hours**

Topics:

Computer Hardware Basics for Forensics: Storage devices: HDD, SSD, USB drives, SD cards, optical media; How data is stored and why deleted files are recoverable; Disk partitions, file systems, and data organization (FAT32, NTFS, ext4) - conceptual overview without programming. File System Forensics (Tool-Based): Understanding file metadata: created, modified, accessed timestamps (MAC times); Hidden files, file extensions, and disguised file types; Deleted file recovery concepts: unallocated space and file carving; Slack space and steganography: hiding data inside innocent-looking files. Practical Forensic Imaging: What is a forensic image and why is it needed; Write blockers: purpose and usage; Introduction to forensic imaging tools: FTK Imager (GUI-based), Recuva; Hash verification: MD5 and SHA-256 for evidence integrity

AI Integration:

Using AI-assisted tools (Autopsy plugins) for automated file classification and metadata extraction.

Authentic Intelligence:

Privacy implications of full-disk forensic imaging in engineering workplace investigations.

MODULE - III : Email, Social Media, & Mobile Forensics	**09 Hours**

Topics:

Email Forensics: Structure of an email: headers, body, attachments; Tracing email origin using email header analysis (GUI tools); Email spoofing and phishing identification; Recovering deleted emails from mail clients and web-based services; Email evidence in harassment, fraud, and intellectual property cases. Social Media Forensics: Digital footprint: what data social media platforms retain; Open Source Intelligence (OSINT): ethically gathering public information. Mobile Device Forensics: Smartphone data categories: call logs, SMS, contacts, app data, GPS history, photos; Types of mobile forensic acquisition: manual, logical, and physical (conceptual); Tools: MSAB XRY (overview), Cellebrite

(overview), Android/iOS data extraction using Oxygen Forensics; Mobile evidence in accident reconstruction and workplace incident investigations.

AI Integration:

Machine learning-based phishing email detection from header and content patterns; AI-assisted mobile data analysis.

Authentic Intelligence:

Legal boundaries of collecting social media evidence without a court order; Ethical risks of OSINT: the line between public information gathering and stalking.

MODULE - IV: Network Forensics & Cybercrime Investigation	**09 Hours**

Topics:

Network Forensics Basics: What is network traffic and why it matters for investigations; IP addresses, MAC addresses, and how devices are identified on a network; Introduction to packet capture: what Wireshark shows (GUI walkthrough - no coding required); Log files as forensic evidence: web server logs, firewall logs, router logs; Identifying suspicious network activity: unauthorized access, data exfiltration, DDoS patterns. Cybercrime Investigation Techniques: Incident response lifecycle: detect, contain, eradicate, recover, document; Types of malware and their behaviour: viruses, ransomware, spyware, trojans; Ransomware attack investigation: timeline reconstruction and evidence collection; Social engineering and phishing investigation workflow; Dark Web Awareness: What the dark web is and its relevance to cybercrime investigations; How stolen engineering data and intellectual property appears on dark web markets; Responsible awareness without participation.

AI Integration:

AI-based network traffic anomaly detection.

Authentic Intelligence:

Ethical obligations when discovering a cyberattack in progress within an organization.

MODULE - V: Forensic Reporting & Ethics	**09 Hours**

Topics:

Forensic Investigation Reporting: Structure of a professional digital forensic investigation report: executive summary, methodology, findings, conclusions, recommendations; Chain of custody documentation: forms, logs, and evidence bags; How to present technical findings to non-technical stakeholders (management, legal teams, courts); Common mistakes in forensic reports and their legal consequences. Anti-Forensics Awareness: What anti-forensics means: file wiping, encryption, steganography, log deletion; Why anti-forensics matters for investigators: knowing what evidence may have been destroyed; Introduction to detection approaches (tool-level, not programming-level). Ethical and Professional Responsibilities: Professional ethics for engineers encountering digital evidence; Whistleblower protection and legal obligations for reporting cybercrime discovered at work; Intellectual property protection for engineers: safeguarding project files, designs, and research data.

AI Integration:

AI and deepfake detection tools; Automated forensic report generation using AI writing assistants.

Authentic Intelligence:

Transparency obligations when AI tools are used to generate or support forensic findings.

Course Outcomes		
Course Outcomes (COs)	**Description**	**Bloom's Taxonomy Level**
At the end of the course the student will be able to:		
1	Explain the digital forensics lifecycle, legal framework, chain of custody principles, and ethical responsibilities associated with handling digital evidence in engineering and professional environments.	**L2**
2	Identify and recover digital artifacts from computers, storage media, and file systems using GUI-based forensic tools, and document findings with proper evidence integrity verification.	**L3**
3	Investigate digital evidence from email, social media, and mobile devices, relevant to engineering industry incident scenarios.	**L3**
4	Analyze network logs and cybercrime incident patterns to reconstruct attack timelines and support incident response in engineering environments.	**L4**
5	Explain the process of forensic report writing, identify common anti-forensic techniques	**L2**

Table: Mapping Levels of COs to POs / PSOs

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

3: Substantial (High) 2: Moderate (Medium) 1: Poor (Low)

TEXT BOOKS:

1. Digital Forensics and Incident Response - Gerard Johansen, Packt Publishing, 2nd Edition, 2020.
2. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics - John Sammons, Syngress (Elsevier), 2nd Edition, 2014.

REFERENCE BOOKS:

1. Cybercrime and Digital Forensics: An Introduction - Thomas J. Holt, Adam M. Bossler & Kathryn C. Seigfried-Spellar, Routledge, 3rd Edition, 2022.
2. Digital Evidence and Computer Crime - Eoghan Casey, Academic Press (Elsevier), 3rd Edition, 2011.
3. Guide to Computer Forensics and Investigations - Bill Nelson, Amelia Phillips & Christopher Steuart, Cengage Learning, 6th Edition, 2019.

RECOMMENDED TOOLS (GUI-Based - No Programming Required):

Forensic Imaging: FTK Imager (free GUI tool), Recuva (deleted file recovery), Autopsy (open-source GUI forensic platform)
Mobile Forensics: Oxygen Forensic Detective (educational trial), Android Backup Extractor, iExplorer (iOS)
Network Analysis: Wireshark (GUI packet capture and analysis), NetworkMiner (GUI-based network forensics)
Report Writing Aids: Autopsy report export, Forensic case report templates, Microsoft Word / Google Docs
AI Assistants: ChatGPT, Claude, Copilot (for report drafting, legal research, and case summarization)

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

VULNERABILITY MANAGEMENT AND PENETRATION TESTING

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER–VII

Subject Code	:	23CY4703	**Credits**	:	03
Hours / Week	:	03 Hours	**Total Hours**	:	45 Hours
L–T–P–J	:	3–0–0–0			

Course Learning Objectives:

This Course will enable students to:

1. Understand the evolving tools, tactics and procedures used by cybercriminals to breach networks.
2. Discuss implications of common vulnerabilities and recommend ways to rectify or mitigate.
3. More complex vulnerabilities are sought which cannot be found by automated scanners and the effectiveness of the security measures taken at the technical, organizational and personnel level is checked.
4. Understand the legal aspects, industry ethics and the approaches and methodologies used when performing a penetration test.
5. Be able to use the appropriate penetration testing tools for a given scenario and understand their output.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes.

1. Lecture method means it includes not only traditional lecture method, but different type of teaching methods may be adopted to develop the course outcomes.
2. Interactive Teaching: Adopt the Active learning that includes brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and roleplaying.
3. Show Video/animation films to explain functioning of various concepts.
4. Encourage Collaborative (Group Learning) Learning in the class.
5. To make Critical thinking, ask at least three Higher order Thinking questions in the class.
6. Adopt Problem Based Learning, which fosters students' Analytical skills, develop thinking skills such as the ability to evaluate, generalize, and analyse information rather than simply recall it.
7. Show the different ways to solve the same problem and encourage the students to come up with their own creative ways to solve them.

Discuss how every concept can be applied to the real world - and when that's possible, it helps improve the students' understanding.

Course Outcome	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Summarize the significance of risk, security and vulnerability assessment.	L2
2	Appl penetration testing strategies for diagnosing security of web application using OWASP standards.	L3
3	Identify the types of vulnerability assessment policies to evaluate system security.	L3
4	Apply modern tools and techniques like Metasploit, RouterSploit, Backdoor, remote access to gather active and passive information of a system.	L3
5	Apply web application security concepts to design application portfolio for reducing risk and vulnerabilities.	L3

MODULE 1:Vulnerability Management Governance	**9Hrs**
Vulnerability Management Governance: Security basics, Identification, Authentication, Authorization, Auditing, Accounting, Non–repudiation, Vulnerability, Threats, Exposure, Risk, Safeguards, Attack vectors. Understanding the need for security assessments: Types of security tests: Security testing, Vulnerability assessment versus penetration testing, Security assessment, Security audit.	
MODULE 2: Penetration testing standard	**9Hrs**
Penetration testing standards, Penetration testing lifecycle, industry standard, Open Web Application Security Project (OWASP) testing guide. Security Assessment Prerequisites: Target scoping and planning, gathering requirements: checklist of test requirements, time frame and testing hours, Identifying stakeholders,MITTRE Framwork	
MODULE 3:Types of vulnerability assessment	**9Hrs**
Types of vulnerability assessment: based on location, based on knowledge about environment/ infrastructure, Announced and Unannounced Automated Testing, Manual Testing Estimating the resources and deliverables, preparing a test plan, Getting approval and signing NDAs, Confidentiality and Nondisclosure Agreements.	

MODULE 4:Information Gathering	9Hrs
Information Gathering: Passive information gathering, Active information gathering. Enumeration: Enumeration Services. Gaining Network Access: Gaining remote access, cracking passwords, Creating backdoors using Backdoor Factory, Exploiting remote services using Metasploit, Hacking embedded devices using RouterSploit, Social engineering using SET.	
MODULE 5: Assessing Web Application Security	9Hrs
Assessing Web Application Security: Importance of web application security testing, Application profiling, Common web application security testing tools, Authentication, Authorization, Session management, Input validation, Security misconfiguration.	

Table: Mapping Levels of COs to POs / PSOs

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

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Sagar Rahalkar, Network Vulnerability Assessment, Packt Publishing Inc, 2018.

REFERENCE BOOKS:

1. Abhishek Singh, Baibhav Singh and Hirosh Joseph, Vulnerability Analysis and De□ense □or the Internet, Springer Publishing Inc, 2008.
2. Wil Allsopp, Unauthorized Access: Physical Penetration Testing For IT Security, Wiley Publishing Inc, 2009.
3. Kimberly Graves, Vulnerability Analysis and De□ense □or the Internet, Wiley Publishing Inc.; 2007.
4. Shakeel Ali and Tedi Heriyanto, Backtrack -4: Assuring security by penetration testing", PACKT Publishing; 2011

****

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

ENDPOINT SECURITY
[As per Choice Based Credit System (CBCS) scheme]
SEMESTER -VII

Course Code	:	23CY4704	**Credits**	:	03
Hours / Week	:	3	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:
To develop skilled professionals who can protect endpoint devices using modern security practices, ensuring confidentiality, integrity, and availability while proactively defending against evolving cyber threats.

Course Objectives:
This course will enable students:
1. To understand the fundamental concepts of network security, including various security controls used to protect network resources.
2. To understand the fundamentals of endpoint security frameworks, including Endpoint Protection Platforms (EPP) and Endpoint Detection & Response (EDR) solutions.
3. To understand outbreak control mechanisms and the importance of quarantining infected endpoints to limit the spread of malware.
4. To understand wired network scanning methods for identifying unauthorized devices, open ports, and vulnerabilities in LAN environments.
5. To identify and disable unnecessary user accounts to reduce the system attack surface.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:
1. **Lecture method** along with traditional lecture method, different type of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and roleplaying.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**09 Hours**

Fundamental Elements of Network Security

Topics:
Network Security Controls, Network Security Protocols, Network Security Perimeter Appliances. Access Control: Terminology, Principles, and Access Control Systems: Administrative Access Control, Physical Access Controls, and Technical Access Controls.

Applications:
Secure online transactions (encryption, authentication), Fraud detection systems, Protect patient records (HIPAA-like compliance), Secure medical devices and hospital networks.

AI Integration: Uses behavior analysis for user authentication, Identifies suspicious login patterns,Enhances encryption management, Prevents data leakage using intelligent monitoring.

Authentic Intelligence: Refers to trustworthy, reliable, and explainable intelligence in security systems , Ensures decisions are accurate, transparent, and secure
Combines AI, trust, and ethics in cybersecurity.

Courses Relevant to this Module:
https://www.netacad.com/

MODULE – II	**09 Hours**

Endpoint Security Framework

Topics: Endpoint Protection Platforms (EPP), Endpoint Detection & Response (EDR) solutions, antimalware, retrospective security, Indication of Compromise (IOC), antivirus, dynamic file analysis, and endpoint-sourced telemetry

Applications. Prevents malware attacks on endpoints (laptops, desktops, servers), Secures enterprise devices from ransomware and viruses, detects advanced and unknown threats Used in personal and enterprise systems.

AI Integration: Identifies unknown threats (zero-day attacks), Automates threat prevention and blocking, Reduces reliance on signature-based detection

Authentic Intelligence: Uses verified and trusted detection methods, ensures minimal false positives**,** Maintains consistent endpoint protection.

Authentic Intelligence: Uses verified and trusted detection methods, Ensures minimal false positives , Maintains consistent endpoint protection.

Courses Relevant to this Module:
https://www.coursera.org/

MODULE – III	**09 Hours**

Endpoint Security Configuration and Protection Strategies

Topics: Configure and verify outbreak control and quarantines to limit infection, uses and importance of a multifactor authentication (MFA) strategy, endpoint posture assessment solutions, and endpoint patching strategy.

Applications: Definition of endpoint security, Importance in modern IT infrastructure, hardening operating systems, Disabling unnecessary services and ports, Secure baseline configurations.

AI Integration. Faster threat detection and response, Reduced human effort and errors Improved accuracy and efficiency, Scalable security solutions.

Authentic Intelligence: Dependency on skilled professionals, Integration complexity, managing AI trust and transparency. .

Courses Relevant to this Module:
https://www.cybrary.it

MODULE – IV	**09 Hours**

Wireless Network Security

Topics: Disable SSID Broadcasting, Monitoring Wireless Network Traffic, Defending Against WPA Cracking: Passphrases, Client Settings, Passphrase Complexity, Additional Controls, Detecting Rogue Access Points, and Wireless Scanning: Wired Network Scanning, and SNMP Polling.

Applications:

Prevents casual users from easily discovering the network, reduces unauthorized connection attempts, Useful in offices, enterprises, and restricted environments, Adds an initial layer of obscurity (not a complete security solution).

AI Integration: Faster and real-time decision-making, reduced human effort, High accuracy in detecting threats, Predictive and proactive capabilities.

Authentic Intelligence: Balanced Decision-Making: Combines speed of AI with judgment of humans, Reduced False Positives: Humans filter alerts before action, Context-Aware Security: AI identifies threats; humans evaluate business impact, Continuous Learning: AI improves from human feedback.

Courses Relevant to this Module:
https://owasp.org/

MODULE – V	**09 Hours**

Securing Network Servers and Windows Security

Topics: Before hardening servers, hardening web servers, and hardening email servers: Recommendations include Microsoft Baseline Security Analyzer (MBSA), setting up BIOS password, auditing the Windows Registry, User and password management, disabling unnecessary user accounts, configuring user authentication, and configuring Windows Firewall.

Applications: Hiding SSID reduces casual discovery of the network, Adds a basic layer of security (not strong alone), Used in corporate and restricted environments.

AI Integration: Real-time threat detection, Reduced human intervention, Improved accuracy and efficiency, Predictive and proactive security.

Authentic Intelligence: Proactive, accurate, and context-aware security , Robust protection across general servers, web servers, and email servers

Courses Relevant to this Module:
https://thehackernews.com/

Course Outcome

Course Outcomes (COs)	**Description**	**Bloom's Taxonomy Level**
At the end of the course the student will be able to:		
1	Explain network security controls and their role in protecting network infrastructure.	L2
2	Explain Endpoint Protection Platforms (EPP) and their role in preventing endpoint threats.	L2
3	Explain outbreak control mechanisms and the importance of quarantining the infected.	L2
4	Illustrates techniques for securing wireless networks, including disabling SSID broadcasting and controlling network visibility.	L2
5	Explain the importance of server hardening before deployment to ensure secure system configurations.	L2

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	2	1	2	2	3	1			2	2		2	2
CO2	2	1	2	2	3	1			2	2		2	2
CO3	2	1	2	2	3	1			2	2		2	2
CO4	2	1	2	2	3	1			2	2		2	2
CO5	2	1	2	2	3	1			2	2		2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Mark Kadrich, "Endpoint Security", Addison-Wesley — 1st ed .ISBN 0-321-43695-4
2. Axel Buecker, Alisson Campos, Peter Cutler, Andy Hu, Garreth Jeremiah, Toshiki Matsui, Michal Zarakowski, Endpoint Security and Compliance Management, IBM Red Books, 2012.

REFERENCE BOOKS:

1. Andrew Avanessian, The Endpoint Security Paradox, 2016.

E-Resources:

1. https://www.ibm.com/topics/endpoint-security
2. https://www.coursera.org/articles/endpoint-security
3. https://skillsforall.com/course/endpoint-security?courseLang=en-US
4. https://www.sans.org/cyber-security-courses/security-essentials-network-endpoint-cloud/

Mini Projects

Students will design practical auditing/compliance-based systems such as:

- Antivirus Scanner Simulation
- Password Strength Checker
- USB Device Monitoring System
- Basic Firewall Rule Simulator
- Keylogger Detection Tool

Students should demonstrate the following:

- Risk analysis
- Tool usage
- Compliance mapping
- Report generation

Recommended Tools

- Microsoft Defender Antivirus
- Symantec Endpoint Protection
- McAfee Endpoint Security

Activity Based Learning (Suggested Activities in Class)

1. **Interactive Quizzes and Games:** Create interactive quizzes or games related to endpoint security concepts, terminology, and best practices. This can make learning more engaging and help reinforce key concepts in a fun and interactive way.
2. **Role-Playing Scenarios:** Divide students into groups and assign them different roles such as IT administrators, employees, and attackers. Create scenarios where they have to respond to security incidents like phishing emails or malware infections.
3. **Case Study Analysis:** Provide case studies of real-world endpoint security breaches or successful defense strategies. Have students analyze the cases in groups, identify key issues, and propose solutions
or preventive measures.
4. **Group Projects:** Assign group projects where students have to design and present comprehensive endpoint
security plans for fictional organizations or scenarios. This encourages collaboration, critical thinking, and
practical application of concepts learned in class.

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

IOT AND IIOT SECURITY

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER – VII

Subject Code	: 23CY4705	**Credits**	: 03
Hours / Week	: 03 Hours	**Total Hours**	: 45 Hours
L–T–P–S	: 3–0–0–0		

Course Learning Objectives:

This course will enable students to:

1. To understand IoT and IIoT architectures and security requirements.
2. To learn vulnerabilities and threat models in IoT environments.
3. To analyze attacks on IoT devices, networks, and industrial systems.
4. To apply security mechanisms including authentication, encryption, and secure communication.
5. To design secure IoT/IIoT systems for real-world applications.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. Use lecture methods with diagrams to explain IoT architectures and security concepts.
2. Demonstrate real-world IoT attacks and vulnerabilities.
3. Encourage hands-on activities using network and IoT security tools.
4. Use case studies of IoT and industrial cyber-attacks.
5. Promote mini-projects on secure IoT system design.

UNIT – I	09 Hours

IoT & IIoT Fundamentals and Security Requirements

Topics: IoT architecture, IIoT systems, sensors and actuators, communication layers, IoT protocols (MQTT, CoAP, HTTP), industrial IoT overview, security requirements (confidentiality, integrity, availability), threat surface.

Applications: Smart homes, industrial automation, healthcare systems, environmental monitoring

UNIT – II	09 Hours

IoT/IIoT Vulnerabilities and Threat Models

Topics:

Device vulnerabilities, firmware attacks, network threats (DoS, MITM, spoofing), botnets (Mirai), industrial threats (SCADA/ICS), attack vectors and threat modeling.

Applications:
Security testing of IoT devices, industrial network protection, intrusion scenarios.

UNIT – III	09 Hours

Cryptography and Secure Communication

Topics:
Lightweight cryptography, encryption techniques, authentication mechanisms, key management, secure communication protocols (TLS, DTLS), secure MQTT/CoAP.

Applications:
Secure data transmission, device authentication, secure messaging systems.

UNIT – IV	09 Hours

Network and System Security for IoT

Topics:
Network security mechanisms, firewalls, IDS/IPS for IoT, secure routing, access control, device hardening, firmware security, patch management.

Applications:
Smart network protection, intrusion detection systems, secure IoT deployment.

UNIT – V	09 Hours

Industrial IoT Security and Emerging Trends

Topics:
SCADA and ICS security, industrial communication protocols, risk assessment, secure architecture design, blockchain (overview), case studies (Stuxnet, industrial attacks).

Applications:
Industrial automation security, critical infrastructure protection, smart manufacturing.

Course Outcomes:

At the end of the course the student will be able to:

1. Describe IoT and IIoT architectures and security requirements
2. Explain vulnerabilities and threat models in IoT systems
3. Analyze attacks on IoT and industrial systems
4. Apply security mechanisms for protecting IoT systems
5. Develop secure IoT/IIoT systems for real-world applications

Table: Mapping Levels of COs to POs / PSOs													
COs	**Program Outcomes (POs)**											**PSOs**	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**1**	**2**
CO1	3	2	1	-	-	-	-	-	-	-	1	2	2
CO2	3	3	2	1	-	-	-	-	-	-	1	2	3
CO3	3	3	2	2	2	-	-	-	1	1	1	2	3
CO4	2	3	3	2	3	1	1	2	2	1	1	2	3
CO5	2	3	3	2	3	2	1	2	2	1	1	2	3

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Sudip Misra, Anandarup Mukherjee, Arijit Roy, “Introduction to IoT”, Cambridge University Press 2021.
2. David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Robert Barton, Jerome Henry,"IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things”, 1st Edition, Pearson Education
(Cisco Press Indian Reprint). (ISBN: 978- 9386873743)

REFERENCE BOOKS:

1. Vijay Madisetti and ArshdeepBahga, “Internet of Things (A Hands-on-Approach)”, 1st Edition, VPT, 2014. (ISBN: 978-8173719547)
2. Raj Kamal, “Internet of Things: Architecture and Design Principles”, 1st Edition, McGraw Hill Education, 2017.
(ISBN: 978-9352605224)

E-Resources:

1. https://www.cisco.com/c/en/us/solutions/internet-of-things/
2. https://www.sap.com/india/products/scm/industry-4-0/what-is-iiot.html
3. https://www.hivemq.com/mqtt/

RECOMMENDED TOOLS

- **Programming Languages:** Embedded C, Python
- **Development Platforms:** ESP32, Arduino, Raspberry Pi
- **IoT Communication Tools:** MQTT Broker (Mosquitto), Node-RED
- **Network Analysis Tools:** Wireshark, Scapy
- **IoT Security Tools:** Nmap, Metasploit Framework
- **Firmware Analysis Tools:** Binwalk
- **Simulation Tools (Optional):** Cisco Packet Tracer, NS3
- **Cloud Platforms (Optional):** ThingSpeak, AWS IoT Core
- **Development Environments:** Arduino IDE, Thonny IDE, Jupyter Notebook
- **Version Control:** Git, GitHub

Table: Mapping Levels of COs to POs / PSOs													
COs	**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PSO1**	**PSO2**
CO1	2	2	1	-	-	-	-	-	-	-	1	2	2
CO2	2	2	1	-	1	-	-	-	-	-	1	2	2
CO3	3	2	2	1	1	2	1	-	2	1	1	2	2
CO4	3	2	1	1	1	2	1	-	2	1	1	2	2
CO5	3	3	2	1	1	2	1	-	2	1	1	2	2
3: Substantial (High) 2: Moderate (Medium) 1: Poor (Low)													

Course Outcomes		
Course Outcomes (COs)	**Description**	**Bloom's Taxonomy Level**
At the end of the course the student will be able to:		
1	Identify and explain the fundamentals of digital forensics, disk structures, file systems, and legal frameworks governing forensic investigations.	**L2**
2	Apply disk acquisition techniques using write blockers and forensic imaging tools to acquire and verify evidence from various storage media.	**L3**
3	Analyze Windows and Linux file system artifacts—including registry entries, prefetch files, NTFS metadata, and logs—to reconstruct user activity timelines.	**L4**
4	Acquire and analyze volatile memory using forensic tools to detect running malware, network artifacts, and code injection techniques.	**L4**
5	Evaluate anti-forensic techniques, produce professional forensic investigation reports, and apply emerging forensic methodologies in cloud and containerized environments.	**L5**

TEXT BOOKS:

1. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory – Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters, Wiley, 1st Edition, 2014.
2. File System Forensic Analysis – Brian Carrier, Addison-Wesley, 1st Edition, 2005.

REFERENCE BOOKS:

1. Incident Response & Computer Forensics – Jason Luttgens, Matthew Pepe, Kevin Mandia, McGraw-Hill, 3rd Edition, 2014.
2. Digital Forensics with Open Source Tools – Cory Altheide & Harlan Carvey, Syngress, 1st Edition, 2011.

RECOMMENDED TOOLS:

Disk Forensics: Autopsy, The Sleuth Kit (TSK), FTK Imager, Guymager, TestDisk/PhotoRec
Memory Forensics: Volatility 3, Rekall, WinPmem, DumpIt, LiME
Timeline & Artifact Analysis: Log2Timeline/Plaso, RegRipper, Shellbags Explorer, PECmd, LECmd
Forensic Platforms: SIFT Workstation, CAINE (Computer Aided Investigative Environment), REMnux
Scripting & Automation: Python (python-evtx, pytsk3, libewf), Jupyter Notebook
AI Assistants: GitHub Copilot, ChatGPT, Claude

S.No	Exercise Title	Aim / Objective	Tools	CO
1	Disk Structure Exploration	Examine MBR/GPT structures and partition tables on a forensic disk image using The Sleuth Kit.	Autopsy / Kali Linux	CO1
2	File System Analysis	Analyze FAT32 and NTFS file systems: identify clusters, inodes, and slack space using Autopsy.	Autopsy / Kali Linux	CO1
3	Forensic Imaging	Acquire a forensic image of a USB drive using FTK Imager and verify integrity with MD5/SHA-256 hashes.	Autopsy / Kali Linux	CO2
4	dd-based Acquisition	Create a bit-stream image using dd/dcfldd and compare with FTK Imager output using hash verification.	Autopsy / Kali Linux	CO2
5	NTFS Artifact Examination	Parse MFT entries and extract MACB timestamps using Python (pytsk3) and Autopsy.	Autopsy / Kali Linux	CO3
6	Windows Registry Forensics	Extract forensic artifacts from registry hives using RegRipper: UserAssist, MRU, ShimCache.	Autopsy / Kali Linux	CO3
7	Memory Acquisition	Acquire a live memory dump using DumpIt/WinPmem and verify dump integrity.	WinPmem / DumpIt	CO4
8	Process & Network Analysis	Use Volatility 3 to enumerate running processes, network connections, and command-line arguments from a memory image.	Volatility 3	CO4
9	Forensic Report Writing	Conduct a complete forensic investigation on a provided disk/memory image and produce a professional investigation report with chain of custody documentation.	Autopsy, Volatility, Plaso	CO5

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

Operating Systems Security

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VII

Course Code	:	23CY4706	**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:

Examine prior research that defines the requirements of a secure operating system and explores implemented systems that effectively enforce security, in order to better understand how to balance functionality and security of the operating system.

Course Objectives:

This course will enable students:

- Outline the models of protection and techniques to enforce security in operating systems.
- Describe the impact of security features and access control mechanisms used in secure operating systems.
- Summarizes a variety of ways that commercial operating systems have been extended with security features by using case studies.
- Apply OS security principles in practical scenarios.
- Explore virtualization and advanced OS security techniques.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:

- **Lecture method** along with traditional lecture method, different type of teaching methods may be adopted to develop the course outcomes.
- **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and roleplaying.
- Showing **Video/animation** films to explain functioning of various concepts.
- Encourage **Collaborative** (Group Learning) Learning in the class.
- To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
- Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**09 Hours**

Operating System Resource Security and Protection

Access and Flow Control – Introduction, Preliminaries, The access Matrix Model, Implementation of Access Matrix, Safety in the Access Matrix Model, Advanced Models of Protection, Case Studies: The UNIX operating System, The Hydra Kernel, Amoeba

Applications: File permissions and user access control in systems like UNIX operating system. Process isolation and memory protection. Role-Based Access Control (RBAC) for managing user privileges. Preventing unauthorized data access.

AI Integration: AI models learn normal access patterns and detect unusual behavior (e.g., insider threats). AI can adjust permissions in real time based on context (location, time, device). Machine learning can generate and optimize access control rules from usage data.

Authentic Intelligence: Critical decisions (like privilege escalation) require human approval alongside AI suggestions. Humans verify AI-generated access policies to avoid over-restriction or vulnerabilities

MODULE – II	**09 Hours**

Access Control Fundamentals

Secure Operating Systems, Security Goals, Trust Model, Threat Model, Protection System, Lampson's Access Matrix, Mandatory Protection Systems, Reference Monitor, Secure Operating System Definition, Assessment Criteria, Multics History, The Multics System, Multics Security, Multics Vulnerability Analysis.

Applications: Access control frameworks used in enterprise systems and cloud platforms like Microsoft Azure. Role-Based and Attribute-Based Access Control (RBAC/ABAC). Secure OS principles guide sandboxing, privilege separation, and isolation. Reference monitor concept used in secure kernels and hypervisors

AI Integration: Intelligent Threat Modelling. Adaptive Trust Models. Smart Reference Monitor

Authentic Intelligence: Risk-Aware Decision Making. Ethical and Fair Access Control

MODULE – III	**09 Hours**

Security in Ordinary Operating Systems, Verifiable Security Goals, Security Kernels

System Histories, UNIX Security, Windows Security, Information Flow, Information Flow Secrecy Models, Information Flow Integrity Models, The Security Kernel, Secure communications processor.

Applications: Minimal trusted computing base (TCB) using security kernels. Used in high-assurance systems like Gemini Secure Operating System. Verifiable security goals applied in certified systems. Ensures correctness of security mechanisms in critical applications

AI Integration: Intelligent Information Flow Monitoring. Automated Verification. AI identifies malware and suspicious processes in operating systems.

Authentic Intelligence: Experts validate AI-based verification of security kernels and OS models. Maintains balance between usability and strict security.

MODULE – IV	**09 Hours**

Securing Commercial Operating Systems, Case Studies

Retrofitting Security into a Commercial OS, History of Retrofitting Commercial OS's, Commercial Era, Microkernel Era, UNIX Era, Case Study1: Solaris Trusted Extensions, Case Study2: Building a Secure Operating System for Linux.

Applications: Enterprise Operating System Security. Retrofitting Security in Legacy Systems. Cloud and Virtualization Security.

AI Integration: Intelligent Retrofitting Analysis. Automated Vulnerability Detection. Adaptive Security Controls.

Authentic Intelligence: Security professionals validate AI recommendations before applying changes to critical systems. Humans ensure compliance and correctness of AI-generated policies.

MODULE – V	**09 Hours**

Secure Testing, Tools & Best Practices

Capability System Fundamentals, Capability Security, Challenges in Secure Capability Systems, Building Secure Capability Systems, Separation Kernels, VAX VMM Security Kernel, Security in Other Virtual Machine Systems.

Applications: Secure Resource Management (Capability Systems). Virtual Machine Security. High-Assurance Systems.
AI Integration: Intelligent Capability Management. VM Behaviour Analysis. Automated Security Policy Enforcement.
Authentic Intelligence: Explainable Virtualization Security. Risk-Aware System Management

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	**Identify** and explain operating system security preliminaries including access and flow control, the access matrix model used in UNIX Operating System, Hydra Kernel, and Amoeba Distributed Operating System.	L2
2	**Outline** the fundamentals of access control in secure operating systems, including security goals, trust and threat models, and protection mechanisms using Lampson's Access Matrix and the Reference Monitor in the Multics Operating System.	L2
3	**Utilize** protection mechanisms, information flow models, and security kernels in systems such as UNIX, Microsoft Windows for achieving verifiable security goals.	L3
4	**Apply** operating system security principles to analyze and evaluate methods for retrofitting security into commercial operating systems through case studies such as Solaris Trusted Extensions and secure implementations in Linux.	L3
5	**Make Use of** capability-based security principles and virtual machine protection mechanisms to analyse secure capability systems and security kernels in virtualized environments such as VAX VMM Security Kernel.	L3

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	2	2	1	-	-	-	-	-	-	-	-	1	2
CO2	2	2	1	-	-	-	-	-	-	-	-	1	2
CO3	3	3	1	-	-	-	-	-	-	-	-	1	2
CO4	3	2	2	-	-	-	-	-	-	-	-	1	2
CO5	3	2	1	-	-	-	-	-	-	-	-	1	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

6. Mukesh Singhal and Niranjan Shivaratri, Advanced Concepts in Operating Systems, McGraw-Hill, 2011
7. Trent Jaeger, Operating System Security, Morgan & Claypool Publishers, 2008.

REFERENCE BOOKS:

2. Michael J. Palmer, "Guide To Operating Systems Security", 1st Edition, Cengage Learning, 2004.
3. Gerard Blokdyk, "Security-focused operating system: Master the Art of Design Patterns", CreateSpace Independent Publishing Platform, 2017.

RECOMMENDED TOOLS: Python, Java, Flask, Django, SQLite, MySQL, Scikit-learn, pgmpy, File Handling APIs, Basic VM simulation tools / datasets

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

BIG DATA SECURITY
[As per Choice Based Credit System (CBCS) scheme]
SEMESTER - VII

Course Code	:	23CY4709	**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:
To develop a strong foundation in securing big data systems by integrating cybersecurity principles, distributed architectures, and artificial intelligence techniques, enabling students to design intelligent, scalable, and secure data-driven infrastructures.

Course Objectives:
This course will enable students:
1. Understand big data architectures along with their security challenges.
2. Apply cryptographic and security protocols in big data environments.
3. Analyse and evaluate security performance metrics such as latency, trust, reliability, and energy efficiency.
4. Design secure big data processing systems using modern frameworks like Hadoop and Spark.
5. Integrate AI techniques for threat detection, anomaly detection, and intelligent security decision-making.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:
1. **Lecture method** along with traditional lecture method, different type of teaching methods may be adopted to develop the course outcomes.
2. **Interactive Teaching:** incorporating brainstorming, discussing, group work, focused listening, formulating questions, notetaking, annotating, and roleplaying.
3. Showing **Video/animation** films to explain functioning of various concepts.
4. Encourage **Collaborative** (Group Learning) Learning in the class.
5. To make **Critical thinking**, asking Higher order Thinking questions in the class in the form of Quiz and writing programs with complex solutions.
6. Showing the **different ways to solve** the same problem and encourage the students to come up with their own creative ways to solve them

MODULE – I	**09 Hours**

Fundamentals of Big Data and Security
Topics: Introduction to Cloud Computing and Big Data, Cloud Service Models: IaaS, PaaS, SaaS, Big Data Characteristics (5Vs), IoT and Big Data Integration, Security Challenges in Cloud and Big Data, Privacy, Trust, and Risk Management, Internet of Everything (IoE).
Applications: Classification and regression problems in real-world scenarios, predictive analytics in healthcare and finance, feature engineering for improving model performance.
AI Integration: AI in cloud resource monitoring, intelligent risk prediction models, AI-driven data classification for security.
Authentic Intelligence: Understanding well-posed learning problems and their real-world constraints, challenges in designing efficient learning systems, limitations of deep learning models, risks associated with poor feature selection and sampling bias, ethical considerations and responsible deployment of AI systems.

MODULE – II	**09 Hours**

Big Data and IoT Architecture with Security Models
Topics: Big Data Architecture and Ecosystem, IoT Architecture and Layers, Cisco IoT Reference Model, Functional, Information, and Deployment Views, Security Architecture in IoT and Big Data, Blockchain for Data Integrity.

Applications: house price prediction systems, medical diagnosis systems, fault detection in machines, financial risk prediction.
AI Integration: Implementation of supervised learning algorithms using Scikit-learn, training and evaluating models using real-world datasets.
Authentic Intelligence: AI-based architecture optimization, predictive maintenance using IoT data, Blockchain + AI for secure transactions.

MODULE – III	**09 Hours**

Cryptography and Security Protocols for Cloud & Big Data
Topics: Conventional Cryptography (Symmetric & Asymmetric), Secure Communication Protocols, Authentication and Key Management, Security in Wireless Sensor Networks (WSN), Security in IoT and Cyber-Physical Systems (CPS), Data Encryption in Cloud Storage.
Applications: customer segmentation in business analytics, anomaly detection in network traffic, pattern discovery in industrial data.
AI Integration: Implementing clustering and dimensionality reduction techniques using Scikit-learn, visualization of clusters using Python tools.
Authentic Intelligence: Risks of misinterpreting clusters, responsible interpretation of patterns discovered from data.

Relevant Online Resources (Relevant to this Module):
1. **Accelerating Clustering Algorithms to Achieve the Highest Performance**
https://www.coursera.org/learn/ml-clustering-and-retrieval?utm_source

MODULE – IV	**09 Hours**

Secure Big Data Processing (Hadoop & Spark)
Topics: Big Data Storage and Processing, Apache Hadoop Ecosystem (HDFS, MapReduce), Apache Spark Architecture, Security in Hadoop (Kerberos, HDFS Security), Spark Security Mechanisms, Data Integrity and Access Control.
Applications: Large-scale data analytics, fraud detection systems, social media data processing.
AI Integration: implementation of graphical models and ensemble techniques using Scikit-learn, use of bagging and boosting methods, model evaluation with Out-of-Bag score.
Authentic Intelligence: limitations of graphical and ensemble models, overfitting risks in boosting, interpretability challenges, and importance of responsible model selection.

Relevant Online Resources (Relevant to this Module):
1. **AI Models on Distributed Platforms and Secure ML Pipelines**
https://www.coursera.org/learn/harden-ai-secure-your-ml-pipelines-?utm_source

MODULE – V	**09 Hours**

AI-Based Big Data Security
Topics: AI in Cybersecurity, Machine Learning for Threat Detection, Anomaly Detection Techniques, Risk-Based Authentication Systems.
Security Analytics and Predictive Models, Trust and Reputation Systems, Intrusion Detection Systems (IDS), Autonomous Security Response Systems.
Applications: Intrusion Detection Systems (IDS), fraud detection in financial systems, cloud security monitoring systems.
AI Integration: use of Grid Search and Random Search for hyperparameter tuning, implementation of validation techniques and performance metrics, application of optimization algorithms and regularization methods using Scikit-learn.
Authentic Intelligence: Understanding overfitting and underfitting, bias-variance tradeoff, limitations of optimization methods, and importance of selecting appropriate validation and regularization techniques.

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Apply cryptographic protocols to secure Big Data, IoT, and Cyber-Physical Systems.	L2
2	Analyze and evaluate security mechanisms using metrics like latency, trust, reliability, and availability.	L3
3	Design and implement secure Big Data processing systems using Hadoop and Spark.	L3
4	Develop cloud security architectures incorporating authentication, access control, and data protection.	L3
5	Apply AI-based techniques for threat detection, anomaly detection, and intelligent security management.	L5

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	2	2	1	-	-	-	-	-	-	-	1	2	2
CO2	2	2	1	-	-	-	-	-	-	-	1	2	2
CO3	3	2	1	1	1	2	1	-	2	1	1	2	2
CO4	3	2	1	1	1	2	1	-	2	1	1	2	2
CO5	3	2	1	1	1	2	1	-	2	1	1	2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Cloud Security: A Comprehensive Guide to Secure Cloud Computing – Ronald L. Krutz & Russell Dean Vines,
Wiley, 1st Edition, 2010.
2. Big Data: A Revolution That Will Transform How We Live, Work, and Think – Viktor Mayer-Schönberger &
Kenneth Cukier, Houghton Mifflin Harcourt, 2013.

REFERENCE BOOKS:

1. Data Security in Cloud Computing – Rajeev Kanth, CRC Press, 2019.
2. Hadoop: The Definitive Guide – Tom White, O'Reilly Media, 4th Edition, 2015.

RECOMMENDED TOOLS:

1. AWS Free Tier, Google Cloud Platform (GCP), Microsoft Azure — for hands-on cloud service model exploration (IaaS/PaaS/SaaS)
2. OpenStack — for private cloud setup and experimentation
3. Apache Hadoop (HDFS, MapReduce) — for distributed storage and batch processing
4. OpenSSL — for implementing AES, RSA, digital certificates, and TLS/mTLS
5. Wireshark — for network traffic capture and protocol analysis
6. Kerberos — for authentication in Hadoop clusters

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

DISK AND MEMORY FORENSICS

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VII

Course Code	:	23CY4708	**Credits**	:	3
Hours / Week	:	3	**Total Hours**	:	45
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision: To develop the ability to investigate, analyze, and reconstruct digital evidence from storage media and volatile memory by integrating forensic methodologies, investigative tools, and responsible handling of digital artifacts in real-world cybersecurity scenarios.

Course Objectives: This course will enable students:

1. To understand the fundamentals of digital forensics, file systems, and disk structures.
2. To acquire, preserve, and analyze disk images using forensic tools and techniques.
3. To perform volatile memory acquisition and analyze memory dumps for forensic evidence.
4. To investigate artifacts in file systems, registries, and operating system structures.
5. To apply anti-forensic detection techniques and present forensic findings in professional reports.

Teaching-Learning Process (General Instructions)

These are sample pedagogical methods where the teacher can use to accelerate the attainment of the various course outcomes:

Lecture method: Along with traditional lecture method, different types of teaching methods may be adopted to develop the course outcomes.

Interactive Teaching: Incorporating brainstorming, CTF (Capture The Flag) challenges, case study discussions, group analysis of forensic scenarios, and notetaking.

Demonstrations: Live forensic tool demos (Autopsy, Volatility, FTK Imager) to explain forensic workflows and artifact examination.

Collaborative Learning: Encourage group investigation of forensic case studies and simulated incident response scenarios.

Critical Thinking: Higher-order questions in the form of case-based quizzes; students write forensic investigation reports from provided disk or memory images.

Problem Solving: Showing different forensic approaches to the same artifact type and encouraging students to validate and compare findings independently.

MODULE – I: Foundations of Digital Forensics & Disk Structures	**09 Hours**

Topics:

Introduction to Digital Forensics: Scope, goals, and legal framework; Types of digital evidence; Chain of custody and evidence integrity. Disk Fundamentals: Physical disk structure (platters, sectors, tracks, cylinders); Logical vs. Physical disk addressing; MBR, GPT partition tables; File allocation: FAT12/16/32, NTFS, ext2/3/4 file systems; Slack space, unallocated space, and deleted file recovery concepts.

Applications:

Understanding how evidence is structured on storage media; Identifying file system artifacts in cybercrime investigations; Legal and procedural guidelines for forensic investigations; Preservation of evidence for court admissibility.

AI Integration:

Introduction to Python-based forensic scripting for disk analysis.

Authentic Intelligence:

Understanding the legal and ethical boundaries of digital investigations; Risks of evidence contamination and chain of custody violations.

MODULE – II: Disk Acquisition & Imaging Techniques	**09 Hours**

Topics:

Disk Acquisition Fundamentals: Write blockers (hardware and software); Forensic imaging formats: RAW/DD, E01 (Expert Witness), AFF; Bit-by-bit imaging vs. logical acquisition; Hashing for integrity verification: MD5, SHA-1, SHA-256. Imaging Tools and Techniques: FTK Imager, dd/dcfldd, Guymager.

Applications:

Acquiring forensic images in incident response scenarios; Verifying the integrity of acquired evidence; Handling encrypted storage in law enforcement investigations; Creating verified forensic duplicates for analysis without altering originals.

AI Integration:

Automated hash verification workflows using Python; Scripting acquisition pipelines with dcfldd and Python wrappers; Using AI-assisted anomaly detection in imaging metadata; Integrating FTK Imager and Guymager into automated forensic pipelines.

Authentic Intelligence:

Risks of evidence alteration during acquisition; Challenges posed by encryption and anti-forensic countermeasures; Ethical considerations in acquiring data from personal devices.

MODULE – III: File System Forensics & Artifact Analysis	**09 Hours**

Topics:

NTFS Forensics: Master File Table (MFT), $LogFile, $UsnJrnl; Alternate Data Streams (ADS); NTFS timestamps (MACB times) and timeline analysis. Windows Artifact Investigation: Registry forensics: hives, keys, and forensic artifacts (UserAssist, MRU, ShimCache, AmCache); Prefetch files, LNK files, Jump Lists, Shellbags. Linux File System Forensics: ext4 journal analysis; inode examination; Bash history, cron jobs, and log analysis (/var/log/).

Applications:

Reconstructing user activity timelines from Windows artifacts; Identifying recently accessed files, installed programs, and USB device history.

AI Integration:

Python scripting for MFT parsing and timeline generation; AI-assisted correlation of artifacts across multiple evidence sources.

Authentic Intelligence:

Privacy implications of forensic access to user activity data. Limitations of automated artifact correlation tools. Validating forensic findings through corroboration of multiple artifact sources.

MODULE – IV : Memory Forensics & Volatile Data Analysis	**09 Hours**

Topics:

Memory Acquisition: Importance of volatile data; Memory acquisition tools: WinPmem, DumpIt, LiME (Linux Memory Extractor); Memory acquisition from live systems and virtual machines (VMware, VirtualBox snapshots). Memory Analysis with Volatility Framework: Process analysis: pslist, pstree, cmdline, dlllist

Applications:

Extracting running process information and detecting malware in memory.

AI Integration:

Automated Volatility plugin pipelines using Python scripting; AI-assisted malware classification from memory artifacts; Using YARA rules integrated with Volatility for pattern matching.

Authentic Intelligence:

Risks of false positives in memory-based malware detection; Privacy implications of full memory acquisition (passwords, personal data exposure).

MODULE – V : Anti-Forensics, Reporting & Case Management	**09 Hours**

Topics:

Anti-Forensics Techniques and Detection: Data hiding: steganography, ADS, slack space abuse; File wiping and secure deletion tools: BleachBit, Eraser, Cipher; Timestamp manipulation and metadata scrubbing; Encryption and obfuscation in malware. Forensic Reporting: Structure of a forensic investigation report; Chain of custody documentation.

Applications:

Producing court-admissible forensic reports; Managing multi-source evidence in complex investigations.

AI Integration:

AI-driven detection of steganographic content in files; Automated report generation using forensic case management tools.

Authentic Intelligence:

Risk of bias in AI-assisted forensic conclusions used in legal proceedings; Accuracy and completeness requirements for court-admissible evidence.

Course Outcomes		
Course Outcomes (COs)	**Description**	**Bloom's Taxonomy Level**
At the end of the course the student will be able to:		
1	Identify the fundamentals of digital forensics, disk structures, file systems, and legal frameworks governing forensic investigations.	**L2**
2	Apply disk acquisition techniques using write blockers and forensic imaging tools to acquire and verify evidence from various storage media.	**L3**
3	Analyze Windows and Linux file system artifacts—including registry entries, prefetch files, NTFS metadata, and logs—to reconstruct user activity timelines.	**L4**
4	Acquire and analyze volatile memory using forensic tools to detect running malware, network artifacts, and code injection techniques.	**L4**
5	Evaluate anti-forensic techniques, produce professional forensic investigation reports, and apply emerging forensic methodologies in cloud and containerized environments.	**L5**

Table: Mapping Levels of COs to POs / PSOs

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

3: Substantial (High) 2: Moderate (Medium) 1: Poor (Low)

TEXT BOOKS:

1. The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory – Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters, Wiley, 1st Edition, 2014.
2. File System Forensic Analysis – Brian Carrier, Addison-Wesley, 1st Edition, 2005.

REFERENCE BOOKS:

1. Incident Response & Computer Forensics – Jason Luttgens, Matthew Pepe, Kevin Mandia, McGraw-Hill, 3rd Edition, 2014.
2. Digital Forensics with Open Source Tools – Cory Altheide & Harlan Carvey, Syngress, 1st Edition, 2011.

RECOMMENDED TOOLS:

Disk Forensics: Autopsy, The Sleuth Kit (TSK), FTK Imager, Guymager, TestDisk/PhotoRec
Memory Forensics: Volatility 3, Rekall, WinPmem, DumpIt, LiME
Timeline & Artifact Analysis: Log2Timeline/Plaso, RegRipper, Shellbags Explorer, PECmd, LECmd
Forensic Platforms: SIFT Workstation, CAINE (Computer Aided Investigative Environment), REMnux
Scripting & Automation: Python (python-evtx, pytsk3, libewf), Jupyter Notebook
AI Assistants: GitHub Copilot, ChatGPT, Claude

S.No	Exercise Title	Aim / Objective	Tools	CO
1	Disk Structure Exploration	Examine MBR/GPT structures and partition tables on a forensic disk image using The Sleuth Kit.	Autopsy / Kali Linux	CO1
2	File System Analysis	Analyze FAT32 and NTFS file systems: identify clusters, inodes, and slack space using Autopsy.	Autopsy / Kali Linux	CO1
3	Forensic Imaging	Acquire a forensic image of a USB drive using FTK Imager and verify integrity with MD5/SHA-256 hashes.	Autopsy / Kali Linux	CO2
4	dd-based Acquisition	Create a bit-stream image using dd/dcfldd and compare with FTK Imager output using hash verification.	Autopsy / Kali Linux	CO2
5	NTFS Artifact Examination	Parse MFT entries and extract MACB timestamps using Python (pytsk3) and Autopsy.	Autopsy / Kali Linux	CO3
6	Windows Registry Forensics	Extract forensic artifacts from registry hives using RegRipper: UserAssist, MRU, ShimCache.	Autopsy / Kali Linux	CO3
7	Memory Acquisition	Acquire a live memory dump using DumpIt/WinPmem and verify dump integrity.	WinPmem / DumpIt	CO4
8	Process & Network Analysis	Use Volatility 3 to enumerate running processes, network connections, and command-line arguments from a memory image.	Volatility 3	CO4

9	Forensic Report Writing	Conduct a complete forensic investigation on a provided disk/memory image and produce a professional investigation report with chain of custody documentation.	Autopsy, Volatility, Plaso	CO5

3: Substantial (High) 2: Moderate (Medium) 1: Poor (Low)

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

QUANTUM CRYPTOGRAPHY
[As per Choice Based Credit System (CBCS) scheme]
SEMESTER -VII

Course Code	:	23CY4707	**Credits**	:	03
Hours / Week	:	03	**Total Hours**	:	45+30
L–T–P–J	:	3–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:
To develop the ability to understand, design, and analyze secure communication systems using principles of quantum mechanics and cryptography for next-generation cyber security applications.

Course Objectives:
This course will enable students:
1. To summarize the fundamental concepts of quantum mechanics and cryptography.
2. To understand quantum key distribution and quantum communication protocols.
3. To apply post-quantum cryptographic techniques for secure systems.
4. To analyze quantum algorithms and their impact on classical cryptography.
5. To evaluate security, performance, and implementation challenges in quantum cryptography.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods, where teacher can use to accelerate the attainment of the various course outcomes:
1. Lecture method along with traditional lecture delivery may be adopted to explain quantum and cryptographic concepts effectively.
2. Interactive Teaching: incorporating brainstorming, discussions, group work, and problem-solving on quantum protocols.
3. Showing video/animation films to visualize quantum states, qubits, and cryptographic protocols.
4. Encourage Collaborative (Group Learning) through case studies and protocol analysis tasks.
5. Demonstrations using quantum simulators and cryptographic tools.
6. To develop critical thinking through quizzes and complex problem-solving related to quantum security.

MODULE – I	**09 Hours**

Foundations of Quantum Computing and Cryptography

Topics: Basics of Quantum Mechanics, Qubits, Superposition, Entanglement, Quantum Gates, Classical vs Quantum Cryptography, Limitations of Classical Cryptography.
Applications: Secure communication systems, quantum computing foundations, cryptographic system design.
AI Integration: Simulation of quantum circuits using Python-based tools, introduction to Qiskit for modeling qubits and gates.
Authentic Intelligence: Understanding physical constraints of quantum systems, challenges in implementing real-world quantum systems, risks of classical cryptographic vulnerabilities.

NVIDIA DLI Courses (Relevant to this Module):
1. Accelerating End-to-End Data Science Workflows (8 hrs) | Path: Data Science Training - Accelerated Data Science Foundations
https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-01+V2
2. Best Practices in Feature Engineering for Tabular Data With GPU Acceleration (2 hrs) | Path: Accelerated Data Science Foundations
https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-06+V1

MODULE – II	**09 Hours**
Quantum Key Distribution (QKD) **Topics:** BB84 Protocol, E91 Protocol, Quantum Key Exchange, Security of QKD, No-Cloning Theorem, Photon Polarization Techniques. **Applications:** Secure key exchange in communication systems, defense and financial sector encryption. **AI Integration:** Simulation of QKD protocols using Qiskit, analysis of quantum communication channels. **Authentic Intelligence:** Practical limitations such as noise, distance constraints, and implementation challenges in QKD systems.	
MODULE – III	**09 Hours**
Quantum Cryptographic Protocols **Topics:** Quantum Teleportation, Quantum Secret Sharing, Quantum Digital Signatures, Quantum Authentication Protocols. **Applications:** Secure communication networks, identity verification systems, next-gen secure protocols. **AI Integration:** Modeling and simulation of quantum protocols, analysis of protocol efficiency. **Authentic Intelligence:** Risks in protocol design, implementation challenges, and scalability issues.	
NVIDIA DLI Free Courses (Relevant to this Module): 1. **Accelerating Clustering Algorithms to Achieve the Highest Performance** (2 hrs) | Path: Data Science Training – Accelerated Data Science Foundations https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-04+V1	
MODULE – IV	**09 Hours**
Post-Quantum Cryptography **Topics:** Introduction to Post-Quantum Cryptography, Lattice-based Cryptography, Hash-based Cryptography, Code-based Cryptography, Multivariate Cryptography. **Applications:** Future-proof encryption systems resistant to quantum attacks, secure internet communications. **AI Integration:** Performance evaluation of post-quantum algorithms, comparison with classical cryptography using Python tools. **Authentic Intelligence:** Trade-offs between security and efficiency, computational overhead, and adoption challenges.	
NVIDIA DLI Courses (Relevant to this Module): 1. **Exploring Adversarial Machine Learning** (8 hrs) | Path: Deep Learning Training – AI Security Engineering & Federated ML https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+S-DS-03+V1	
MODULE – V	**09 Hours**
Quantum Attacks, Security and Implementation Challenges **Topics:** Shor's Algorithm, Grover's Algorithm, Quantum Attacks on RSA and AES, Security Analysis, Implementation Challenges, Quantum Hardware Limitations. **Applications:** Cryptanalysis, cybersecurity risk assessment, secure system design. **AI Integration:** Simulation of quantum attacks, performance evaluation of cryptographic systems. **Authentic Intelligence:** Real-world limitations of quantum computing, ethical implications, and security risks.	
NVIDIA DLI Free Courses (Relevant to this Module): 1. **Accelerate Data Science Workflows with Zero Code Changes** (1 hr) | Path: Data Science Training – Data Preparation for Model Training https://learn.nvidia.com/courses/course-detail?course_id=course-v1:DLI+T-DS-03+V1	

Course Outcome

Course Outcomes (COs)	Description	Bloom's Taxonomy Level
At the end of the course the student will be able to:		
1	Recall basic concepts of quantum computing and cryptography.	L2
2	Describe quantum principles and cryptographic techniques.	L3
3	Apply quantum cryptographic protocols and QKD techniques.	L3
4	Analyze post-quantum cryptographic methods and quantum attacks.	L3
5	Evaluate security and performance of quantum cryptographic systems.	L5

Mapping Levels of COs to POs / PSOs

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)											PSOs	
	1	2	3	4	5	6	7	8	9	10	11	1	2
CO1	1	1	1	-	-	-	-	-	-	-	1	2	2
CO2	2	2	1	-	-	-	-	-	-	-	1	2	2
CO3	3	2	1	1	1	2	1	-	2	1	1	2	2
CO4	3	2	1	1	1	2	1	-	2	1	1	2	2
CO5	3	2	1	1	1	2	1	-	2	1	1	2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. Quantum Computation and Quantum Information – Michael A. Nielsen & Isaac L. Chuang, Cambridge University Press, 10th Anniversary Edition, 2010.
2. Quantum Cryptography and Secret-Key Distillation – Gilles Van Assche, Cambridge University Press, 1st Edition,2006.

REFERENCE BOOKS:

1. Post-Quantum Cryptography – Daniel J. Bernstein, Johannes Buchmann & Erik Dahmen, Springer, 1st Edition,
   2009.
2. An Introduction to Quantum Computing – Phillip Kaye, Raymond Laflamme & Michele Mosca, Oxford University Press, 1st Edition, 2007.

RECOMMENDED TOOLS

Programming: Python (NumPy, Qiskit, Cirq) – Google Colab/ Jupyter Notebook/Visual Studio
Quantum Platforms: IBM Quantum Experience, Microsoft Azure Quantum
Simulation: Qiskit Aer Simulator, Cirq Simulator
Cryptographic Tools: OpenSSL, PQCrypto Libraries
Visualization: Matplotlib, Plotly
AI Assistants: GitHub Copilot, ChatGPT, Claude

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING
Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

EMBEDDED SYSTEM SECURITY

SEMESTER – VII

Subject Code	:	23CY4710	**Credits**	:	03
Hours / Week	:	03 Hours	**Total Hours**	:	45 Hours
L–T–P–S	:	3–0–0–0			

Course Learning Objectives:

This course will enable students to:

1. Understand the fundamentals of embedded system security, threats, vulnerabilities, and secure design principles.
2. Analyze secure boot, firmware integrity, authentication, and authorization mechanisms in embedded systems.
3. Apply secure communication, testing, and risk assessment techniques in embedded and IoT systems.
4. Design secure embedded applications using Raspberry Pi, Python, and Embedded C programming.

Teaching-Learning Process (General Instructions)

These are sample new pedagogical methods that teachers can use to accelerate the attainment of the various course outcomes.

1. Lecture method includes conventional classroom teaching along with modern interactive teaching methods.
2. Adopt active learning methodologies such as brainstorming, discussions, group activities, and focused problem-solving sessions.
3. Use videos, animations, and demonstrations to explain embedded security concepts and attacks.
4. Encourage collaborative and project-based learning approaches.
5. Discuss real-world embedded security applications and industry case studies.
6. Conduct practical demonstrations using Raspberry Pi, Python, and Embedded C programming.

UNIT – I	09 Hours

Introduction to Embedded System Security:

Fundamentals of embedded systems and their security challenges, Overview of different security threats and attack vectors in embedded systems, Side channel and Covert channel Attacks, Security engineering principles and secure development methodologies, Secure coding practices and vulnerability mitigation techniques in embedded systems.

UNIT – II	09 Hours

Secure Boot and Firmware Security:

Importance of secure boot and firmware integrity in embedded systems, Chain of trust and secure boot process, Bootloader design for secure boot implementation, Trusted Platform Module (TPM) and hardware root of trust, Hardware-based secure boot solutions, Secure firmware storage and secure Over-The-Air (OTA) firmware update mechanisms.

UNIT – III	09 Hours

Embedded System Authentication and Secure Communication:
Authentication mechanisms and access control protocols for embedded systems, Public Key Infrastructure (PKI) and digital certificates in embedded systems, Role-Based Access Control (RBAC) and privilege escalation prevention techniques, Secure communication protocols including TLS/DTLS and MQTT security, Secure data transfer mechanisms in embedded and IoT systems.

UNIT – IV	09 Hours

Embedded System Security Testing and Evaluation:
Threat modeling and risk assessment techniques, Vulnerability assessment and penetration testing in embedded systems, Secure code review and static analysis methods, Dynamic security testing and fuzz testing techniques, Incident response and handling in embedded systems, Security testing using Python with Raspberry Pi and Embedded C programming.

UNIT – V	09 Hours

Embedded System Security Case Studies and Emerging Trends:
Case studies in embedded system vulnerabilities and exploits, Secure embedded system design and implementation case studies, Automotive and Industrial IoT security basics, AI-enabled embedded security and TinyML security concepts, Hardware trojans and Physical Unclonable Functions (PUFs), Future trends and industry perspectives in embedded system security.

Course Outcomes:

At the end of the course the student will be able to:

1. Explain the fundamentals of embedded system security, security threats, attack vectors, and secure design principles.
2. Analyze vulnerabilities, firmware protection techniques, authentication mechanisms, and secure boot processes in embedded systems.
3. Develop secure embedded applications using Raspberry Pi, Python, and Embedded C programming with secure communication mechanisms.
4. Evaluate embedded systems using threat modeling, penetration testing, and security analysis techniques.
5. Design secure embedded and IoT-based systems using modern embedded security technologies and best practices.

Table: Mapping Levels of COs to POs / PSOs

COs	Program Outcomes (POs)												PSOs	
	1	2	3	4	5	6	7	8	9	10	11	12	1	2
CO1	3	3	1	1	1	-	-	-	-	-	-	1	2	3
CO2	3	3	2	2	1	-	-	-	-	-	-	1	2	2
CO3	3	2	3	2	3	-	-	-	1	1	-	1	2	3
CO4	2	3	2	3	2	-	-	-	1	1	-	1	2	2
CO5	3	3	3	2	2	-	1	-	1	1	-	2	2	2

3: Substantial (High) **2: Moderate (Medium)** **1: Poor (Low)**

TEXT BOOKS:

1. David Kleidermacher and Mike Kleidermacher, Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development, Newnes/Elsevier, 2012.
2. William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson Education, 2017.
3. Tammy Noergaard, Embedded Systems Architecture: A Comprehensive Guide for Engineers and Programmers, Elsevier, 2013.

REFERENCE BOOKS:

1. Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley.

2. Jean-Philippe Aumasson, Serious Cryptography, No Starch Press, 2018.

3. Qing Li and Caroline Yao, Real-Time Concepts for Embedded Systems, CMP Books.

DAYANANDA SAGAR UNIVERSITY
SCHOOL OF ENGINEERING

Devarakaggalahalli, Harohalli, Kanakapura Road, Bengaluru South District, Karnataka – 562 112

Leadership, Policy & Authentic Intelligence

[As per Choice Based Credit System (CBCS) scheme]

SEMESTER - VII

Course Code	:	23CY4803	**Credits**	:	02
Hours / Week	:	02	**Total Hours**	:	30
L–T–P–J	:	2–0–0–0	**CIE+SEE**	:	60+40 Marks

Course Vision:
To create awareness of cryptographic techniques and enable students to understand and apply fundamental concepts for securing digital information and communication in real-world systems.

Course Vision

This condensed 2-credit version of LPAI retains the full conceptual scope of the original 5-unit course while compressing delivery into 10 weeks and 30 contact hours. The three core lenses — technical leadership, technology policy, and AI ethics — are preserved and integrated from the outset, with a streamlined capstone replacing the extended Unit 5 sprint.

Course Objectives

Students will:

- Understand the fundamentals of engineering and society leadership
- Apply tools of AI ethics, policy
- Develop governance frameworks
- Analyze ethical, societal, and reliability issues in AI systems

Course Outcomes (CO)

CO	Outcome
CO1	Apply authentic intelligence, systems thinking, and leadership models in socio-technical contexts. (Module 1)
CO2	Demonstrate communication and teamwork skills for presenting technical ideas to stakeholders. (Module 1)
CO3	Implement AI policy frameworks and governance principles in real-world scenarios. (Module 2)

CO	Outcome
CO4	Apply ethical principles to address bias, fairness, and accountability in AI systems. (Module 2)
CO5	Develop solutions using leadership, policy, and ethical considerations for real-world challenges. (Module 3)

Broad Course Description

This course introduces students to the rapidly evolving field of AI and ethics .It covers foundational concepts such as Policy, regulatory, and governance. Students will gain hands-on experience in analyzing, comparing various other regulatory on AI applications . The course integrates NVIDIA DLI resources to expose students to Trustworthy AI workflows in deep learning series. Ethical concerns such as bias, hallucination, and responsible AI deployment are also emphasized.

Detailed Course Syllabus

The course consists of three modules. Each module integrates:

- Core topics on leadership.
- Governance, policy and ethics
- Case study
- Authentic Intelligence reflection

Course Modules

Module 1:· Foundations + Leadership 10 hours | Weeks 1–4

Topics covered

• What is authentic intelligence? Beyond artificial intelligence

• Engineering in society: roles, responsibilities, and power

• Systems thinking for engineers — feedback loops and stakeholder mapping

• History of technology governance and the leadership–policy–AI nexus

• Leadership models: transformational, servant, and distributed

- Decision-making under uncertainty and high-stakes environments
- Managing diverse, interdisciplinary teams
- Communicating technical ideas to non-technical stakeholders
- Ethical leadership: when to dissent, when to escalate

Teaching methods
- Socratic seminar and concept mapping (Week 1)
- Guest talk: industry or government practitioner (Week 2)
- Leadership style self-assessment and small group case discussion (Week 3)

Project deliverable
Deliverable Project brief (individual) 1-page problem framing with stakeholder map Format Individual · 1 page
Due End of Week 4
Weight 15% of final grade

Module 2 · Policy, Governance & AI Ethics
10 hours | Weeks 5–7

Topics covered

- How policy is made: legislative, regulatory, and standards processes
- Key frameworks: EU AI Act, India's DPDP Act 2023, IEEE standards
- Engineers as policy actors: testimony, consultation, design advocacy
- Comparative case: Aadhaar — governance lessons for engineers
- Public interest technology and responsible innovation
- Ethical theories applied to AI: consequentialism, deontology, virtue ethics
- Bias, fairness, and representation in algorithmic systems
- Authentic intelligence: human judgment augmented by AI
- Accountability gaps: who is responsible when AI fails?
- Designing for human dignity, autonomy, and informed consent

Teaching methods

- Policy memo writing workshop and India AI regulatory landscape mapping (Week 5)
- Mock regulatory hearing and comparative analysis paired activity (Week 6)
- Ethics case carousel (3 cases, 3 groups) and bias detection exercise (Week 7)
- AI ethics canvas workshop and Socratic philosophical dialogue (Week 7)

Project deliverable
Deliverable Policy & ethics brief (team) — 2-page governance recommendation + 1-page ethics audit card
Format Team · 3 pages total + verbal debrief
Due End of Week 7
Weight 20% of final grade

Unit 3 · Capstone: Integrated Design

Challenge 10 hours | Weeks 8–10

Topics covered

- Revisiting your Unit 1 problem brief — what has changed?
- Integrating leadership, policy, and ethics into one design response
- Stakeholder consultation and co-design methods
- Prototyping governance structures and technical safeguards
- Writing for public audiences: op-eds and policy explainers
- Structuring a policy pitch for decision-makers
- Visual communication: slides, infographics, and data stories
- Structured peer review and iteration under time pressure

Teaching methods

- Problem reframing workshop and capstone kick-off Q&A (Week 8)
- Co-design simulation and structured peer consultation (Week 9)
- Pitch rehearsal and writing workshop (Week 9)

- Structured peer review with instructor micro-consultations (Week 10)
- Public showcase with external jury panel: industry, policy, and academia (Week 10)

Project deliverable

Deliverable Capstone portfolio (team) — 6-page written portfolio + 8-minute pitch to external Jury.

Individual component

300-word individual reflection submitted alongside the team portfolio

Due End of Week 10 (final showcase)

Weight 50% capstone + 15% individual reflection

10-Week Detailed Schedule

Each week = 3 contact hours. Total: 30 hours across 10 weeks.

Wk	Topic	Methods & notes
1	What is authentic intelligence?	Icebreaker: 'AI decision you made today' · Concept mapping · Short provocation reading · Course overview: the leadership–policy–AI triangle
2	Systems thinking & the technology–society interface	Guest speaker: policy or industry practitioner · Stakeholder mapping workshop · Feedback loops and power mapping
3	Leadership models & self-awareness	Leadership style self-assessment · Small group case discussion · Cases: engineering leaders who shaped policy (Grace Hopper, Sundar Pichai)
4	Decision-making, teams & communication	Role-play simulation: high-stakes engineering decision · Peer feedback · When to dissent: ethical leadership and escalation · Project brief due

Module 1 · Foundations + Leadership (Weeks 1–4)

Wk	Topic	Methods & notes
5	How policy is made	Policy memo writing workshop · Mapping India's AI regulatory landscape · Regulatory bodies vs. standards organizations (IEEE, ISO, BIS)
6	Comparative governance & public interest tech	Mock regulatory hearing · Comparative analysis: EU AI Act, US, India, China · Case: Aadhaar — governance lessons for engineers
7	AI ethics: frameworks, bias & human dignity	Ethics case carousel (3 cases, 3 groups) Bias detection hands-on exercise · AI ethics canvas workshop · Socratic dialogue: where should humans always decide? · Policy & ethics brief due

Module 2 · Policy, Governance & AI Ethics (Weeks 5–7)

Wk	Topic	Methods & notes
8	Capstone launch & stakeholder consultation	Problem reframing workshop · Team formation or reconfirmation · Capstone kick-off Q&A · Co-design simulation · Draft capstone outline due (1 page)
9	Public communication & peer review	Writing workshop: op-ed drafting · Pitch rehearsal in pairs · Structured peer review of capstone drafts · Instructor micro-consultations · Full capstone draft due
10	Final showcase & course reflection	Final capstone presentations (8 min + 5 min Q&A per team) · External jury panel: industry/policy/academia · Individual reflection · Course close

Module 3 · Capstone (Weeks 8–10)

DLI Resources as Case Studies

These are resources you can analyse to understand how authentic intelligence principles play out in practice.

Case Study 1 — Deloitte + DLI (enterprise AI governance at scale) NVIDIA collaborated with Deloitte to shape a DLI curriculum customised to the needs of AI professionals and projects, enabling Deloitte to tap into

the power of their own NVIDIA DGX system to explore novel AI use cases. NVIDIA This is a case study in how a major consulting firm institutionalised AI literacy as a governance function — connecting technical training directly to client-facing AI deployments in regulated industry

Case Study 2 — Booz Allen Hamilton + US Air Force DLI teamed with Booz Allen Hamilton to train employees and government personnel, including members of the U.S. Air Force, providing hands-on training for data scientists to solve challenging problems in healthcare, cybersecurity and defence. NVIDIA Newsroom This illustrates authentic intelligence in high-stakes, mission-critical settings where explainability and accountability are non-negotiable — the military context demands AI that can be audited and overridden by humans.

Case Study 3 — KENET University Faculty Training (Global South capacity building) The Fundamentals of Deep Learning course provided faculty from different KENET member universities a great opportunity to get up-to-date training. NVIDIA KENET is Kenya's national research and education network. This is a case study in authentic intelligence as inclusion — building AI capacity in African universities so that the Global South participates in defining how AI works, not just consuming AI built elsewhere.

Case Study 4 — Generative AI Teaching Kit with Dartmouth (academic-industry co-creation) The Generative AI Teaching Kit, co-developed with Assistant Professor Sam Raymond from Dartmouth College, explores practical implementation of Generative AI through LLMs, diffusion models, multimodal architectures, distributed training, and accelerating inference. NVIDIA Developer The co-development model itself is a case study — when universities co-author industry training content, it creates a feedback loop where academic critical thinking (including ethics and bias analysis) shapes what engineers learn to build.

Case Study 5 — NeMo Guardrails as governance in code the inclusion of NeMo Guardrails in the Generative AI Teaching Kit curriculum is a case study in authentic intelligence by design. Rather than treating safety as a policy document, NeMo Guardrails allows developers to write topical rails, dialogue flows, and output filters in configuration — making ethical constraints enforceable at the inference layer. Analysing how Guardrails works, what it can and cannot prevent, and who controls the rail definitions is a rigorous case study in the limits and possibilities of technical AI governance.

Assessment Framework

All assessments are project-based. No written exams. Work builds progressively toward the capstone.

Assessment	Unit	Format	Marks
Project brief	U1	Individual · 1 page	20
Policy & ethics brief	U2	Team · 2 pages	10
Capstone pitch	U3	Team · 8-min pitch + 6-page portfolio	40
Any one of the DLI Certification from NVIDIA DLI certificate to be recognized and considered for assessment with 50% weightage			
Individual reflection	U3	Individual · 200 words	30

Assessment principles

- Each assessment is scaffolded — the project brief frames the policy brief, which frames the capstone.
- Team assessments use a peer contribution rubric; individual grades may be adjusted by ±10% based on peer feedback.
- The capstone is assessed by an external jury using a shared rubric covering technical rigour, policy coherence, and ethical consistency.

Teaching Strategies

Four evidence-based strategies selected for the compressed format. Each is designed to maximise engagement within 3-hour weekly sessions.

Think-Pair-Share

Activate thinking before full group discussion. Give students 60–90 seconds of silent thinking, 2 minutes of pair discussion, then invite pairs to share. Cold-call pairs rather than volunteers to reduce bias. Use a timer to keep it tight.

Socratic Seminar

Assign shared text or prompt in advance. Open with one big question that has no single right answer. Facilitate: redirect questions, do not answer them. Students build on, challenge, or

question each other. Close with a written exit ticket. Arrange seating in a circle and norm: speak to the group, not just the teacher.

Jigsaw Activity

Divide complex content into 3–4 chunks. Assign each student to an expert group to study their chunk. Regroup so each new team has one expert per chunk; each expert teaches their piece. Keep expert groups small (3–5) and provide a clear 'what to teach' checklist.

Gallery Walk

Post work or prompts around the room. Students rotate in pairs (2–3 minutes per station), leaving a sticky note or written comment at each. Debrief by asking what patterns or surprises came up. Use a signal — bell or music — to rotate, and assign roles: reader, writer, timekeeper.

Assessment Scheme

Definitions

1. **"Internal Assessment"** refers to the Continuous Internal Assessment (CIA). The weightage of this component is **60%**. It includes:
    a. One **Mid Semester Examination (MSE)** (Descriptive-based),
    b. Six **Continuous Assessment Tool (CAT)**: Quiz, Project based learning, Reflection Note on Guest Lecture, Industrial visit, E-course certification, Building models,
    Group discussion, Case study, Seminar, or Open Book Assignment
    c. One **AI-powered Assignment (APA):** Use of AI tools for problem-solving while simultaneously developing Authentic Intelligence through critical evaluation, ethical reasoning, and responsible decision-making.
2. **"External Assessment"** refers to the Semester End Examinations (SEE). The weightage of this component is **40%**. At the end of semester, the final examination is conducted to evaluate student's performance.

- If any theory course ***consists of Mini project component***, then the total marks of ***10 (Ten marks)*** shall be evaluated for that mini project and hence there is no APA for such courses.
- If any theory course ***does not consist of mini project***, then APA is mandatory awarded for **10 marks**.

Recommended Tools

- Programming: Python
- Visualization: Transformers, Lang Chain
- Platforms: NVIDIA DLI, Google Collab
- AI Tools: CUDA, RAPIDS

Additional Resources

1. NVIDIA Learning Resources
    - NVIDIA Deep Learning Institute (DLI)
    - Generative AI Learning Path

2. Recommended:
    - Getting Started with Deep Learning
    - Accelerating Data Science Workflows
    - CUDA Python Fundamental