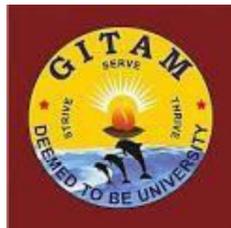# GANDHI INSTITUTE OF TECHNOLOGY AND MANAGEMENT (GITAM)
(Deemed to be University)
VISAKHAPATNAM * HYDERABAD * BENGALURU

Accredited by NAAC with A$^+$ Grade

REGULATIONS AND SYLLABUS

OF

M.Tech. Cyber Forensics and Information Security

(w.e.f. 2019-20 admitted batch)

Vision and Mission of University

Vision
To become a global leader in higher education.

Mission

*To impart futuristic and comprehensive
education of global standards
with high sense of discipline and
social relevance in a serene and
invigorating environment.*

Vision and Mission of Department

Vision

*Excel in computer science and engineering education with
international standards for global employment and
research.*

Mission

- *Create an excellent academic ambience that promotes
  innovation and research.*

- *Impart quality education through well designed
  curriculum experiential learning in tune with the
  changing needs of the industry.*

- *Collaborate with world class academic institutions and
  software industries for mutual benefit.*

- *Produce competent and socially committed graduates
  having creative skills and ethical values.*

Program Educational Objectives of M. Tech. Computer Science and Engineering are:

- PEO1: Apply the knowledge gained in the areas of research and development
- PEO2: Develop and use IT tools for the benefit of society
- PEO3: Work effectively as part of a team with strong moral and ethical values

Program Educational Objectives of M. Tech. Data Science are:

- PEO1: Develop competent professionals who can develop novel techniques and tools for data analysis
- PEO2: Enhance their technical skills to be easily absorbed in industry
- PEO3: Produce highly skilled engineers who can work for a sustainable society

Program Educational Objectives of M. Tech. Cyber Forensics and Information Security are:

- PEO1: Develop highly secure and scalable algorithms to provide better security among the various software used.
- PEO2: Promote leadership abilities along with team work for a just and secure technical society
- PEO3: Engage in lifelong learning

Program Outcomes:

At the end of the program a student is expected to have:

1. An understanding of the theoretical foundations and the limits of computing.

2. An ability to adapt existing models, techniques, algorithms, data structures, etc. for efficiently solving problems.

3. An ability to design, develop and evaluate new computer based systems for novel applications which meet the desired needs of industry and society.

4. Understanding and ability to use advanced computing techniques and tools.

5. An ability to undertake original research at the cutting edge of computer science & its related areas.

6. An ability to function effectively individually or as a part of a team to accomplish a stated goal.

7. An understanding of professional and ethical responsibility.

8. An ability to communicate effectively with a wide range of audience.

9. An ability to learn independently and engage in life-long learning.

10. An understanding of the impact of IT related solutions in an economic, social and environment context.

Program Specific Outcomes:

Upon successful completion of the program the students should be able to:

1. identify, formulate and provide efficient solutions to higher engineering problems.

2. design and develop software/hardware solutions for multidisciplinary and transdisciplinary problems.

3. handle research problems.

M.Tech in Cyber Forensics & Information Security(CF&IS)

REGULATIONS

(w.e.f. 2019-20 admitted batch)

1. ADMISSION

Admission into M.Tech. in Cyber Forensics & Information Security program of GITAM (Deemed to be University) is governed by GITAM admission regulations.

2. ELIGIBILITY CRITERIA

2.1 A pass in B.E./B.Tech./AMIE in any branch of Engineering or its equivalent orMCA/M.Sc.

2.2 Admissions into M.Tech. will be based on the following:

- Score obtained in GAT (PG), if conducted.

- Performance in Qualifying Examination /Interview.

- CandidateswithvalidGATEscoreshallbeexemptedfromappearingforGAT(PG).

2.3 The actual weightage to be given to the above items will be decided by the authorities at the time of admissions.

3. CHOICE BASED CREDIT SYSTEM

3.1 Choice Based Credit System (CBCS) was introduced with effect from 2015-16 admitted batch and revised with effect from academic year 2019-20 in order topromote:

- Student centered Learning

- Activity based learning

- Cafeteria approach

- Learning at their own pace

- Interdisciplinary learning

3.2 Learning objectives and outcomes are outlined for each course to enable a student to know what he/she will be able to do at the end of the program.

4. STRUCTURE OF THEPROGRAM

4.1 The Program Consists of

i) Core Courses (compulsory) which give exposure to a student in core subjects related area.

ii) Program Electives.

iii) Open Electives

iv) Mandatory and Audit Courses

4.2 Each course is assigned a certain number of credits depending upon the number of contact hours (lectures/tutorials/practical) per week.

4.3 In general, credits are assigned to the courses based on the following contact hours per week per semester.
- One credit for each Lecture / Tutorial hour per week.
- One credit for two hours of Practical per week.

The curriculum of the four semesters M.Tech. program is designed to have a total of 68 credits for the award of M.Tech. Degree

5. MEDIUM OF INSTRUCTION

The medium of instruction (including examinations and project reports) shall be English.

6. REGISTRATION

Every student has to register for the courses in each semester at the time specified in the academic calendar.

7. ATTENDANCE REQUIREMENTS

7.1 A student whose attendance is less than 75% in all the courses put together in any semester will not be permitted to attend the semester-end examination and he/she will not be allowed to register for subsequent semester of study. He/she has to repeat the semester along with his/her juniors.

7.2 However, the Vice-Chancellor on the recommendation of the Principal / Director of the Institute/School may condone the shortage of attendance to the students whose attendance is between 65%and74%ongenuinegroundsandonpaymentofprescribedfee.

8. EVALUATION

8.1 The assessment of the student's performance in a theory course shall be based on two components: Continuous Evaluation (40marks) and semester-end examination(60marks).

8.2 A student has to secure a minimum of 40% in any theory course in the two components (ref. 8.1) put together to be declared to have passed the course, subject to the condition that the student must have secured a minimum of 24 marks out of 60 marks (i.e. 40%) in the theory component at the semester-end examination.

8.3 Practical/ Project Work/ Viva voce/ Seminar etc. course is completely assessed under Continuous Evaluation for a maximum of 100 marks, and a student has to obtain a minimum of 40% to secure Pass Grade. Details of Assessment Procedure are furnished below in Table1.

8.4 Audit courses are assessed through continuous evaluation for satisfactory or not satisfactory only. No credits will be assigned.

Table 1: Assessment Procedure

S.No.	Component of Assessment	Marks Allotted	Type of Assessment	Scheme of Evaluation
1	Theory Courses	40	Continuous Evaluation	i) Thirty (30) marks for mid Semester examinations. Three mid examinations shall be conducted for 15 marks each; performance in best two shall be taken into consideration. ii) Ten (10) marks for Quizzes, Assignments and Presentations.
		60	Semester-end Examination	iii) Sixty (60) marks for Semester-end examinations
	Total	100		

2	Practical Courses	100	Continuous Evaluation	i) Fifty (50) marks for regularity and performance, records and oral presentations in the laboratory. Weightage for each component shall be announced at the beginning of the semester. ii) Ten (10) marks for case studies. iii) Forty (40) marks for two tests of 20 marks each (one at the mid-term and the other towards the end of the semester) conducted by the concerned lab teacher.
3	Technical Seminar (II Semester)	100	Continuous Evaluation	Through five periodic seminars of 20 marks each
4	Project Work (III Semester)	100	Continuous Evaluation	i) Forty (40) marks for periodic assessment on originality, innovation, sincerity and progress of the work, assessed by the project supervisor. ii) Thirty (30) marks for mid-term evaluation for defending the project, before a panel of examiners. iii) Thirty (30) marks for final report presentation and viva-voce, by a panel of examiners*.
5	Project Work (IV Semester)	50	Continuous Evaluation	i) Twenty (20) marks for periodic assessment on originality innovation, sincerity and progress of the work, assessed by the project supervisor. ii) Fifteen (15) marks for mid-term evaluation for defending the project, before a panel of examiners*. iii) Fifteen (15) marks for interim report presentation and viva-voce.
		50	Semester-end Examination	Fifty (50) marks for final project report and viva-voce examination assessed by external examiners.
	Total	100		

6	Audit Courses	100	Continuous Evaluation	Audit courses are assessed for PASS or FAIL only. No credits will be assigned to these courses. If a student secures a minimum of 40 out of 100 marks during continuous evaluation, he / she will be declared PASS, else FAIL. PASS grade is necessary to be eligible to get the degree

Panel of Examiners shall be appointed by the concerned Head of the Department

9. PROVISION FOR ANSWER BOOK VERIFICATION AND CHALLENGEEVALUATION

9.1 If a student is not satisfied with his/her grade, the student can apply for answer book verification on payment of prescribed fee for each course within one week after announcement of results.

9.2 After verification, if a student is not satisfied with revaluation marks/grade, he/she can apply for challenge valuation within one week after announcement of answer book verification result or two weeks after the announcement of results, which will be valued by two examiners i.e., one Internal and one External examiner in the presence of the student on payment of prescribed fee. The challenge valuation fee will be returned, if the student is successful in the appeal by securing a better grade.

10. SUPPLEMENTARY AND SPECIALEXAMINATIONS

10.1 The odd semester supplementary examinations will be conducted after conducting regular even semester examinations during April/May.

10.2 The even semester supplementary examinations will be conducted after conducting regular odd semester examinations during October/November.

10.3 A student who has secured 'F' Grade in Project work shall have to improve his/her work and reappear for viva-voce after satisfactory completion of work approved by panel of examiners.

10.4 A student who has completed period of study and has "F" grade in final semester courses is eligible to appear for special examination.

11. MASSIVE OPEN ONLINE COURSES(MOOCs)

Greater flexibility to choose variety of courses is provided through Massive Open Online Courses (**MOOCs**) during the period of study. Students without any backlog courses up to first semester are permitted to register for MOOCs in second semester up to a maximum of 6 credits from program elective / open elective/audit courses. However, the Departmental Committee (DC) of the respective campuses has to approve the courses under MOOCs. The grade equivalency will be decided by the respective Board of Studies (BoS).

12. GRADING SYSTEM

12.1 Based on the student performance during a given semester, a final letter grade will be awarded at the end of the semester in each course. The letter grades and

S.No.	Grade	Grade Points	Absolute Marks
1	O (outstanding)	10	90 and above
2	A+ (Excellent)	9	80 to 89
3	A (Very Good)	8	70 to 79
4	B+ (Good)	7	60 to 69
5	B (Above Average)	6	50 to 59
6	C (Average)	5	45 to 49
7	P (Pass)	4	40 to 44
8	F (Fail)	0	Less than 40
9	Ab (Absent)	0	-

Table 2: Grades and Grade Points

12.2 A student who earns a minimum of 4 grade points (P grade) in a course is declared to have successfully completed the course, and is deemed to have earned the credits assigned to that course, subject to securing a GPA of 5.0 for a Pass in the semester.

13. GRADE POINT AVERAGE

13.1 A Grade Point Average (GPA) for the semester will be calculated according to the formula:

$$GPA = \frac{\Sigma \, [C \times G]}{\Sigma \, C}$$

where, C = number of credits for the course,

G = grade points obtained by the student in the course.

13.2 The Cumulative Grade Point Average (CGPA), is calculated using the above formula considering the grades obtained in all the courses, in all the semesters up to that particular semester.

13.3 CGPA required for classification of class after the successful completion of the program is shown in Table3.

Class	CGPA Required
First Class with Distinction	≥ 8.0*
First Class	≥ 6.5
Second Class	≥ 5.5
Pass Class	> 5.0

Table 3: CGPA required for Award of Class

* In addition to the required CGPA of 8.0 or more, the student must have necessarily passed all the courses of every semester in the first attempt.

14. ELIGIBILITY FOR AWARD OF THE M.Tech. DEGREE

14.1 Duration of the program: A student is ordinarily expected to complete the M.Tech. Program in four semesters of two years. However, a student may complete the program in not more than four years including study period.

14.2 However, the above regulation may be relaxed by the Vice-Chancellor in individual cases for cogent and sufficient reasons.

14.3 A student shall be eligible for award of the M.Tech. Degree if he / she fulfills all the following conditions.

   a) Registered and successfully completed all the courses and project works.

   b) Successfully acquired the minimum required credits as specified in the curriculum corresponding to the branch of his/her study with in the stipulated period.

   c) Has no dues to the Institute, Hostels, Libraries, NCC / NSS etc ,and

   d) No disciplinary action is pending against him /her.

15. DISCRETIONARYPOWER

Notwithstanding anything contained in the above sections, the Vice Chancellor may review all exceptional cases, and give his decision, which will be final and binding.

M. Tech in Cyber Forensics and Information Security
Effective from academic year 2019-20 admitted batch

Semester I

S.no.	Course Code	Course Title	Category	L	T	P	C	Remarks
1	19ECS701	Advanced Data Structures	PC	3	0	0	3	Common to CFIS/CSE/DS
2	19ECS705	Algorithms and Analysis	PC	3	0	0	3	Common to CFIS/CSE/DS
3	19ECS707	Number Theory and Cryptography	PC	3	0	0	3	
4	19ECS7XX	Program Elective I	PE	3	0	0	3	
5	19ECS7XX	Program Elective II	PE	3	0	0	3	
6	19EMC741	Research Methodology And IPR	MC	2	0	0	2	
7	19ECS721	Advanced Data Structures Laboratory	PC	0	0	4	2	Common to CFIS/CSE/DS
8	19ECS729	Ethical Hacking Laboratory	PC	0	0	4	2	CEH training is must
9	19EAC7XX	Audit Course I	AC	2	0	0	0	
						Total Credits: 21		

Semester II

S.no.	Course Code	Course Title	Category	L	T	P	C	Remarks
1	19ECS704	Pragmatics of Information Security	PC	3	0	0	3	
2	19ECS7XX	Program Elective III	PE	3	0	0	3	
3	19ECS7XX	Program Elective IV	PE	3	0	0	3	
4	19ECS7XX	Program Elective V	PE	3	0	0	3	
5	19EOE7XX	Open Elective	OE	3	0	0	3	
6	19ECS726	Pragmatics of Information Security Laboratory	PC	0	0	4	2	
7	19ECS724	Digital Forensics Laboratory	PC	0	0	4	2	
8	19ECS792	Technical Paper Writing	PW	0	0	4	2	Common to CFIS/CSE/DS
9	19EAC7XX	Audit Course II	AC	2	0	0	0	
						Total Credits: 21		

Semester III

S.no.	Course Code	Course Title	Category	L	T	P	C	Remarks
1	19ECS891	Project Work I	PW	0	0	26	13	
						Total Credits: 13		

Semester IV

S.no.	Course Code	Course Title	Category	L	T	P	C	Remarks
1	19ECS892	Project Work II	PW	0	0	26	13	
						Total Credits: 13		

Number of Credits

Semester	I	II	III	IV	Total
Credits	21	21	13	13	**68**

Programme Elective I

S.no.	Course Code	Course Title	Category	L	T	P	C	Remarks
1	19ECS741	Machine Learning	PE	2	0	2	3	Common to CFIS/CSE/DS
2	19ECS764	Secure Coding	PE	2	0	2	3	
4	19ECS778	Internet Technologies and Cyber Laws	PE	2	0	2	3	

Programme Elective II

S.no.	Course Code	Course Title	Category	L	T	P	C	Remarks
1	19ECS757	Malware Analysis and Reverse Engineering	PE	2	0	2	3	
2	19ECS759	Ethical Hacking	PE	2	0	2	3	
3	19ECS761	Data Encryption and Compression	PE	2	0	2	3	
4	19ECS777	Agile Software Development	PE	2	0	2	3	Common to CFIS/CSE/DS

Programme Elective III

S.no.	Course Code	Course Title	Category	L	T	P	C	Remarks
1	19ECS760	Steganography and Digital Watermarking	PE	2	0	2	3	
2	19ECS782	Intrusion Detection and Prevention System	PE	2	0	2	3	
3	19ECS744	Secure Software Design and Enterprise Computing	PE	2	0	2	3	
4	19ECS780	Web Application Security	PE	2	0	2	3	

Programme Elective IV

S.no.	Course Code	Course Title	Category	L	T	P	C	Remarks
1	19ECS766	Biometrics	PE	2	0	2	3	
2	19ECS752	Digital Forensics	PE	2	0	2	3	
3	19ECS786	Cloud Security	PE	2	0	2	3	

Programme Elective V

S.no.	Course Code	Course Title	Category	L	T	P	C	Remarks
1	19ECS768	Security Assessment and Risk Analysis	PE	2	0	2	3	
2	19ECS784	Mobile application security	PE	2	0	2	3	
3	19ECS772	Data Security and Access Control	PE	2	0	2	3	Common to CFIS/CSE/DS
4	19ECS785	Block Chain Technology	PE	2	0	2	3	Common to CFIS/DS

AUDIT COURSE I and II

S. no	Course Code	Course Name	Category	L	T	P	C	Remarks
1	19EAC741	English for Research Paper Writing	AC	2	0	0	0	Common to ALL
2	19EAC742	Disaster Management	AC	2	0	0	0	Common to ALL
3	19EAC744	Value Education	AC	2	0	0	0	Common to ALL
4	19EAC745	Constitution of India	AC	2	0	0	0	Common to ALL
5	19EAC746	Pedagogy Studies	AC	2	0	0	0	Common to ALL
6	19EAC747	Stress Management by Yoga	AC	2	0	0	0	Common to ALL
7	19EAC748	Personality Development through life Enlightenment Skills	AC	2	0	0	0	Common to ALL
8	19EAC750	Developing Soft Skills and Personality	AC	2	0	0	0	Common to ALL

OPEN ELECTIVE

S. No	Course Code	Course Name	Category	L	T	P	C	Remarks
1.	19EOE742	Business Analytics	OE	3	0	0	3	Common to ALL
2.	19EOE746	Operations Research	OE	3	0	0	3	Common to ALL
3.	19EOE748	Cost Management of Engineering Projects	OE	3	0	0	3	Common to ALL

`

19ECS701: ADVANCED DATA STRUCTURES

                                                                    L T P C
                                                                    3 0 0 3

This course provide an overall idea of to design, implement and to perform various operations like search, insert, delete etc., operations on the complex data structures. As a part string matching techniques and text data compression algorithms were also considered

Course Objectives:
- Learn to choose appropriate data structures, understand the ADT/libraries, and use it to design algorithms for a specific problem.
- Understand the necessary mathematical abstraction to solve problems.
- Familiarize with advanced paradigms and data structure used to solve algorithmic problems.
- Analyze efficiency and proof of correctness of various algorithms.

Unit I   9L
Dictionaries: Definition, Dictionary Abstract Data Type, Implementation of Dictionaries.
Hashing: Review of Hashing, Hash Function, Collision Resolution Techniques in Hashing, Separate Chaining, Open Addressing, Linear Probing, Quadratic Probing, Double Hashing, Rehashing, Extendible Hashing.
Learning Outcomes
After completion of this unit the student will be able to
- define ADT understand hashing (L1)
- design and implement a hash function with the above collision resolution techniques(L6)

Unit II   9L
Skip Lists: Need for Randomizing Data Structures and Algorithms, Search and Update Operations on Skip Lists, Probabilistic Analysis of Skip Lists, Deterministic Skip Lists
Learning Outcomes
After completion of this unit, the student will be able to
- create and perform operations like insert, delete and search operations on skipped lists (L6)
- differentiate between singly linked list/ doubly linked list and skip list with respect to space complexity and time complexity to perform search, insert and delete operations. (L2)

Unit III   9L
Trees: Binary Search Trees, AVL Trees, Red Black Trees, 2-3 Trees, B-Trees, Splay Trees
Learning Outcomes
After completion of this unit, the student will be able to
- organize data in a hierarchy form / non-linear way (L4)
- perform search, insert and delete operations in the above data structures. (L4)

Unit IV   9L
Text Processing: Sting Operations, Brute-Force Pattern Matching, The Boyer-Moore Algorithm, The Knuth- Morris-Pratt Algorithm, Standard Tries, Compressed Tries, Suffix Tries, The Huffman Coding Algorithm, The Longest Common Subsequence
Problem (LCS), Applying Dynamic Programming to the LCS Problem.
Learning Outcomes
After completion of this unit, the student will be able to
- perform various string handling and string-matching algorithms mainly considering similarity and identity in to account. (L6)
- understand various text data compression techniques (L2)

Unit V   6L
Computational Geometry: One Dimensional Range Searching, Two-Dimensional Range Searching, constructing a Priority Search Tree, Searching a Priority Search Tree, Priority Range Trees, Quad trees, k-D Trees.

Learning Outcomes

After completion of this unit, the student will be able to

- distinguish between one dimensional range search and two-dimensional range search (l2)
- understand the database management query concepts in this domain(L2)

Text Book(s):

1. Mark Allen Weiss, Data Structures and Algorithm Analysis in C++, 2nd Edition, Pearson, 2004.
2. M T Goodrich, Roberto Tamassia, Algorithm Design, John Wiley, 2002.

Course Outcomes:

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

- understand the implementation of symbol table using hashing techniques. (L2)
- develop and analyze algorithms for red-black trees, b-trees and splay trees. (L3)
- develop algorithms for text processing applications. (L5)
- identify suitable data structures and develop algorithms for computational geometry problems. (L4)

19ECS705: ALGORITHMS AND ANALYSIS

L T P C
3 0 0 3

The course is concentrated on the study and development of algorithms for solving practical problems efficiently, and the theoretical analysis of their behavior. It involves algorithm design techniques, methods for analyzing the performance of corresponding algorithms and improving their efficiency, and to provide performance guarantees.

Course Objectives:
- Introduce the advanced methods of designing and analyzing algorithms.
- Identify an appropriate algorithm and implement it for a specific problem.
- Understand different classes of problems concerning their computation difficulties.
- Solve problems using dynamic programming, network flow algorithms, graph algorithms and approximation algorithms.
- Analyze recent developments in the area of algorithmic design.

Unit I 6 L
Sorting: Review of various sorting algorithms, topological sorting
Graph**:** Definitions and Elementary Algorithms: Shortest path by BFS, shortest path in edge weighted case (Dijkastra's), depth-first search and computation of strongly connected components, emphasis on correctness proof of the algorithm and time/space analysis.
Learning Outcomes
After completion of this unit the student will be able to
- describe different sorting algorithms and their time complexity(L2)
- apply various graph traversal algorithms to find shortest paths(L3)
- outline the difference between BFS and DFS algorithms(L4)
- review the correctness of algorithm time and space analysis(L2)

Unit II 8 L
Matroids: Introduction to greedy paradigm, algorithm to compute a maximum weight maximal independent set. Application to MST.
Graph Matching: Algorithm to compute maximum matching. Characterization of maximum matching by augmenting paths, Edmond's Blossom algorithm to compute augmenting path.
Learning Outcomes
After completion of this unit the student will be able to
- calculate the maximum matching in graph related problems(L3)
- compute algorithms for maximum weight and maximal independent set. (L3)
- apply MST for real world problems(L3)
- discover augmenting paths in graphs using various algorithms(L3)

Unit III 9 L
Flow-Networks: Maxflow-mincut theorem, Ford-Fulkerson Method to compute maximum flow, Edmond- Karp maximum-flow algorithm.
Matrix Computations**:** Strassen's algorithm and introduction to divide and conquer paradigm, inverse of a triangular matrix.
Learning Outcomes
After completion of this unit the student will be able to
- solve network flow problems using network flow algorithms(L3)
- implement divide and conquer paradigm for matrix multiplication(L3)
- analyze how efficiency can be achieved by matrix computation algorithms(L4)

Unit IV 10 L
Shortest Path in Graphs: Floyd-Warshall algorithm and introduction to dynamic programming paradigm.

More examples of dynamic programming.
Modulo Representation of integers/polynomials: Chinese Remainder Theorem, Conversion between base- representation and modulo-representation. Application: Interpolation problem.

Learning Outcomes:
After completion of this unit the student will be able to
- practice more examples on dynamic programming(L3)
- determine shortest paths in a graph using dynamic programming(L5)
- assess various representations of data(L5)
- develop algorithms for interpolation problems(L6)

Unit V   **9 L**
Linear Programming: Geometry of the feasibility region and Simplex algorithm
NP-completeness: Examples, proof of NP-hardness and NP-completeness. One or more of the following topicsbasedontimeandinterest.Approximationalgorithms,RandomizedAlgorithms,InteriorPointMethod.

Learning Outcomes
After completion of this unit, the student will be able to
- explain linear programming concepts(L2)
- examine NP-hardness and NP-completeness problems (L4)
- illustrate approximation algorithms(L4)
- analyze randomized algorithms(L4)

Text Book(s):
1. Cormen, Leiserson, Rivest, Stein, "Introduction to Algorithms", Tata Mcgraw Hill Publishers.
2. Aho, Hopcroft, Ullman, "The Design and Analysis of Computer Algorithms", Pearson Education.
3. Kleinberg and Tardos, "Algorithm Design", Pearson Education.

Course Outcomes:
After completion of the course, students would be able to:
- analyze the complexity/performance of different algorithms. (L4)
- determine appropriate algorithm that is suitable for solving a particular set of problems. (L3)
- explain more complex algorithms and proofs in written form (L3)
- categorize different problems in various classes according to their complexity. (L4)
- design and analyze techniques for algorithms and ways to approach NP-complete problems (L6)
- apply techniques to solve new problems that may arise in various applications (L3)

19ECS707: NUMBER THEORY AND CRYPTOGRAPHY

L	T	P	C
3	0	0	3

The emphasis of the course is on the application of the number theory in the design of cryptographic algorithms. The course will start with the notion of time complexity and with several elementary number theoretic algorithms. Putting them together we will see how we can design several cryptographic algorithms. As a part of cryptanalysis, we will study several attacks on these algorithms as well as their remedies. We will also study recent developments in elliptic curve cryptography and the use digital signatures and its variations for authentication.

Course Objectives:

- This course purpose is to introduce the arithmetic topics, both ancient and very modern, which have been at the center of interest in applications, especially in cryptography.
- For this reason, we take an algorithmic approach, emphasizing estimates of the efficiency of the techniques that arise from the theory.
- Enable the student to learn basic knowledge in cryptographic various algorithms.
- Demonstrate the handling of variety of threats during transmission of information over network and also how to overcome it.
- Train the student to convert algorithm logic into any programming language code.

Unit I   8L
Topics in elementary number theory: O and Ω notations, time estimates for doing arithmetic, divisibility and the Euclidean algorithm. Congruence's: Definitions and properties, linear congruencies, residue classes, Euler's phi function, Fermat's Little Theorem, Chinese Remainder Theorem, Applications to factoring, finite fields, quadratic residues and Reciprocity: Quadratic residues, Legendre symbol, Jacobi symbol.

Learning Outcomes:
After completion of this unit, the student will be able to
- Identify how number theory is related to and used in cryptography. (L3)
- Learn basic Algebra and Discrete Mathematics. (L1)
- Know to find the greatest common divisor of two numbers (which is an incredibly important problem by itself), but its extended version also gives an efficient way to solve Diophantine equations and compute modular inverses. (L1)
- Understand the Chinese remainder theorem which gives a unique solution to simultaneous linear congruence's with co-prime moduli. (L2)

Unit II   8L
Simple Cryptosystems: Enciphering Matrices – Block ciphers Principles –Data Encryption Standard (DES) –The Strength of DES– Differential & Linear Crypt analysis–Block Cipher Design principles.

Learning Outcomes:
After completion of this unit, the student will be able to
- Learn the environment that led to the development of the Data Encryption Standard (DES). (L1)
- Identifying, describing, and explaining the purpose of each stage of the DES algorithm. (L3)
- Explaining why the input and output permutation in DES do not improve the security. (L2)
- Enumerating the weaknesses of the DES algorithm. (L1)
- Comparing and contrasting the protection provided by 3DES as compared to 2DES. (L2)
- Defining what a Feistel structure is and why it is important to the design of encryption techniques. (L1)

Unit III   **10L**

Public Key Cryptosystems: The idea of public key cryptography, The Diffie–Hellman Key Agreement Protocol. RSA Cryptosystem, Bit security of RSA, ElGamal Encryption, Discrete Logarithm, Knapsack problem, Zero-Knowledge Protocols from Cryptography to Communication Security - Oblivious Transfer.

Learning Outcomes:

After completion of this unit, the student will be able to

- defining key expressions and terminology including multiplicative inverse, relatively prime, and the totient function. (L1)
- describing the steps required to perform the RSA (rivest, shamir, and adleman) encryption algorithm. (L2)
- performing the RSA algorithm on a given number by hand. (L3)
- using the RSA algorithm to encrypt and decrypt data. (L3)
- describing a key exchange algorithm or protocol (e.g. Diffie Hellman). (L2)
- design and implement a new unbreakable cryptosystem. (L6)
- blend the existing cryptographic algorithms with the existing communication protocols. (L6)
- analyze and application of cryptography for secures ecommerce and other secret transactions. (L4)

Unit IV   **8L**

Primality and Factoring: Pseudo primes, the rho (γ) method, Format factorization and factor bases, the continued fraction method, the quadratic seieve method.

Learning Outcomes:

After completion of this unit, the student will be able to

- understand the concept of way to attack RSA would be to try to factor the public modulus. (L2)
- apply the Modern Algorithms: Quadratic Sieve, Number field Sieve. (L3)
- learn Complexity of Trial Division. (L1)

Unit V   **8L**

Number Theory and Algebraic Geometry: Elliptic curves, basic facts, elliptic curve cryptosystems, elliptic curve primality test – elliptic curve factorization.

Learning Outcomes:

After completion of this unit, the student will be able to

- identify the approach to public-key cryptography is based on the algebraic structure of elliptic curves over finite fields. (L3)
- learn examples of elliptic curves over the field of real numbers. (L1)
- learn about the elliptic curve discrete logarithm problem, which is the cornerstone of much of present-day elliptic curve cryptography. (L1)

Text Book(s):

1. Neal Koblitz, A Course in Number Theory and Cryptography, 2/e, Springer,2002.
2. William Stallings, Cryptography and Network Security, 5/e, Pearson education,2010.
3. R. P. Feynman, Feynman lectures on computation, 1stEdition, Penguin Books,1996.
4. Gennady P. Berman, Gary D. Doolen, Ronnie Mainiri&ValdmisItriFrinovich, Introduction to quantum computers, 1stEdition, World Scientific, Singapore,1998
5. Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography, Principles and Protocols,2ndEdition, CRC Press,2014.

Course Outcomes:

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

- find the greatest common divisor of two numbers (which is an incredibly important problem by itself), but its extended version also gives an efficient way to solve Diophantine equations and compute modular inverses. (L1)
- identifying, describing, and explaining the purpose of each stage of the DES algorithm. (L3)
- analyze and application of cryptography for secures ecommerce and other secret transactions. (L4)
- apply the Modern Algorithms: Quadratic Sieve, Number field Sieve. (L3)
- he approach to public-key cryptography is based on the algebraic structure of elliptic curves over finite fields.(L6)

19EMC741: RESEARCH METHODOLOGY AND IPR

	L	T	P	C
	2	0	0	2

This course introduces the student, to the fundamentals of research, research process, technical writing and intellectual property rights. Students will be able to use this knowledge to gain interest in their subject area and pursue their career in research.

Course Objectives

- To familiarize the meaning, objectives and sources of research
- To acquaint the student with the importance and methods of literature review/research ethics
- To impart the knowledge of technical writing for preparing reports, presentations, research proposals, conference/journal publications
- To introduce the terminology and process of obtaining intellectual property rights
- To expose the intricacies in the process of obtaining patent rights

Unit I   5L

Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem. Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations

Learning Outcomes
After the completion of this unit, the student will be able to
- define the meaning of a research problem (L1)
- list the different sources of research problem (L2)
- enumerate the different criteria of good research and list the different errors in selecting research problem (L2)
- contrast the different approaches of research (L3)
- compare the different methods for data collection and analysis (L5)

Unit II   5L

Effective literature studies approaches, analysis Plagiarism, Research ethics

Learning Outcomes
After the completion of this unit, the student will be able to
- list and elaborate the different steps of the research process (L1)
- explain the importance of carrying out an effective literature review (L2)
- identify the research gaps from literature review (L5)
- describe the ethical principles to be following during research process and authorship (L2)
- define the terminology and list the methods to avoid being accused of plagiarism (L1)
- list the different types of research misconduct (L2)

Unit III   5L

Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee

Learning Outcomes
After the completion of this unit, the student will be able to

- list the attributes, reasons and guidelines for effective technical writing (L1)
- contrast between conference paper, technical presentation and journal paper (L3)
- choose a particular research contribution for patenting or journal publication (L4)
- describe the terminology related to citation, citation index, h-index etc (L2)

Unit IV   5L
Nature of Intellectual Property: Patents, Designs, Trademarks and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development.
International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT.
Learning Outcomes
After the completion of this unit, the student will be able to
- describe the codes and standards in building intellectual property rights(L2)
- list the subject, importance and requirements for of patentability(L1)
- explain the process of patenting and commercialization in academia(L2)
- enumerate the procedure for application preparation, filing and grant of Patents(L2)

Unit V   8L
Patent Rights: Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications. **New Developments in IPR**: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.
Learning Outcomes
After the completion of this unit, the student will be able to
- explain the scope of patent rights(L2)
- describe the process for licensing and transfer of technology(L2)
- identify the sources of patent information and databases(L1)
- elaborate the administration of patent system(L2)
- describe the new developments in IPR in computer software, biological systems etc(L3)

Text Book(s):
1. Stuart Melville and Wayne Goddard, "Research methodology: an introduction for Science and engineering students", Tata Mcgraw Hill India, 2013.
2. Ranjit Kumar, "Research Methodology: A Step by Step Guide for beginners", 2/e, Prentice Hall of India, 2013.

References:

1. Halbert, "Resisting Intellectual Property", Taylor and Francis Limited, 2007.
2. Mayall, "Industrial Design", McGraw Hill, 1992.
3. Niebel, "Product Design", McGraw Hill, 1974.
4. Asimov, "Introduction to Design", Prentice Hall, 1962.
5. Robert P. Merges, Peter S. Menell, Mark A. Lemley, "Intellectual Property in New Technological Age", 2016
6. T. Ramappa, "Intellectual Property Rights Under WTO", S. Chand Publishers, 2008

19ECS721: ADVANCED DATA STRUCTURES LABORATORY

L T P C
0 0 4 2

1. Develop programs for
   a. Heap Sort
   b. Merge Sort
   c. Quick sort by taking random element as pivot
   d. Selection

2. Program to perform insertion, deletion and search operations on the following:
   a. Single Linked List b. Doubly Linked List c. Circular Linked List

3. Implement the functions of a dictionary using Hashing.

4. Implement hash tables with linear probing and double hashing. Demonstration of inserting and deleting elements.

5. Skip list: Implementations and operations.

6. Develop a program to perform insertion, deletion and search operations on the following Trees
   a. Binary Search Tree
   b. B-Trees
   c. AVL Tree
   d. Red Black Trees

7. Implement the code for the following problems using Dynamic Programming:
   a. Matrix Chain Multiplication Problem.
   b. String matching algorithm.

19ECS729: ETHICAL HACKING LABORATORY

L T P C
0 0 4 2

1. To learn about hacking tools and skills

2. To study about "Footprinting and Reconnaissance".
   Domain Name Information, Finding IP Address, Finding Hosting Company, IP Address Ranges.

3. To study about Fingerprinting.
   Port Scanning, Ping Sweep, DNS Enumeration

4. To study about system Hacking.
   TCP/IP Hijacking, Trojan Attacks, Trojan Information, Email Hijacking, Social Engineering, Inserting Viruses in a User System, Password Hacking, Dictionary Attack, Hybrid Dictionary Attack, Brute-Force Attack, Rainbow Tables

5. To study about Wireless Hacking.
   Kismet, NetStumbler, Wired Equivalent Privacy, WEPcrack, Aircrack-ng, Wireless DoS Attacks

6. To learn about Sniffing tools.

7. To study about Mobile Hacking.

8. To study about performing DOS Attacks on Cloud Network.

9. To study various cryptography tools.

10. To study Web Application Hacking

19ECS741: MACHINE LEARNING

LT P C
2 0 2 3

Machine Learning is the science of making machines think intelligently without being explicitly programmed. Machine learning is pervasive in everyday life today. This course is designed to enable students get in-depth understanding of different machine learning techniques including deep learning and reinforcement learning and apply them on real-life data.

Course Objectives:
- Understand the fundamental concepts of Supervised learning.
- Explore descriptive problem solving through unsupervised learning strategies.
- Acquire skills in developing as well as evaluating different machine learning models.
- Demonstrate the application of different deep learning methodologies.
- Gain an understanding of concepts like Reinforcement Learning and Active Learning.

Unit I   **10L**

Supervised Learning (Regression/Classification): Basic methods: Distance-based methods, Nearest-Neighbors, Decision Trees, Naive Bayes, Linear models: Linear Regression, Logistic Regression, Support Vector Machines, Nonlinearity and Kernel Methods, Beyond Binary Classification: Multi-class

Learning Outcomes

After completion of this unit, the student will be able to
- explain the concept of machine learning and their applications to different real-world datasets. (L2)
- demonstrate the working of different supervised learning algorithms and assess their suitability to a given problem. (L3)
- extend a binary classification problem to solve a multi-class classification problem. (L3)

Unit II   **7L**

Unsupervised Learning: Clustering: K-means, Dimensionality Reduction: PCA and kernel PCA, Generative Models (Gaussian Mixture Models and Hidden Markov Models)

Learning Outcomes

After completion of this unit, the student will be able to:
- demonstrate the working of different dimensionality reduction techniques on high-dimensional datasets (L3)
- illustrate the working of Generative Models mathematically. (L3)

Unit III   **6L**

Evaluating Machine Learning algorithms, Model Selection, Ensemble Methods (Boosting, Bagging, Random Forests)

Learning Outcomes

After completion of this unit, the student will be able to:
- interpret ensemble models as a function of different weak classifiers. (L3)
- compare the performances of different classification models. (L4)

Unit IV   **9L**

Modeling Sequence/Time-Series Data, Deep Learning (Deep generative models, Deep Boltzmann Machines, Deep auto-encoders, Applications of Deep Networks) and Feature Representation Learning

Learning Outcomes

After completion of this unit, the student will be able to:
- understand the methods for handling time series and sequence data. (L2)
- demonstrate the working of different deep learning approaches on complex data. (L3)

Unit V   **9L**

Scalable Machine Learning (Online and Distributed Learning) Semi-supervised Learning, Active Learning, Reinforcement Learning, Inference in Graphical Models, Introduction to Bayesian Learning and Inference

Learning Outcomes

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

- apply reinforcement learning approach to applications like bioinformatics and personalized recommendation. (L3)
- analyses the working of Active Learning approach on complex data. (L4)

Text Book(s)

1. Kevin Murphy, Machine Learning: A Probabilistic Perspective, MIT Press, 2012.
2. Trevor Hastie, Robert Tibshirani, Jerome Friedman, The Elements of Statistical Learning, Springer 2009
3. Jiawei Han, Micheline Kamber, Jian Pei, Data Mining: Concepts and Techniques, 3/e, Morgan Kaufmann, 2011.
4. Christopher Bishop, Pattern Recognition and Machine Learning, Springer, 2007.

Course Outcomes:

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

- relate knowledge about application of machine learning techniques to real world problems. (L3)
- apply deep learning methodologies to applications such as image recognition, video tagging etc.(L3)
- generate suitable unsupervised learning approaches to descriptive machine learning models. (L4)
- utilize supervised learning approaches to perform predictive modeling of data. (L3)
- assess different machine learning algorithms based on performance evaluation measures. (L5)

19ECS764: SECURE CODING

L T P C
2 0 2 3

This course aims to provide an understanding of the various security attacks and knowledge to recognize and remove common coding errors that lead to vulnerabilities. It gives an outline of the techniques for developing a secure application.

Course Objectives:

- Understand the most frequent programming errors leading to software vulnerabilities.
- Identify and analyze security problems in software.
- Understand and protect against security threats and software vulnerabilities.
- Effectively apply their knowledge to the construction of secure software systems

Unit I   **9L**

Safe Initialization: Sanitizing the Environment, Restricting Privileges on Windows, Dropping Privileges in set UID Programs, Limiting Risk with Privilege Separation, Managing File Descriptors Safely, creating a Child Process Securely, Executing External Programs Securely, Executing External Programs Securely, Disabling Memory Dumps in the Event of a Crash.

Learning Outcomes:

After completing this Unit, students will be able to

- analyze the security policies and flaws(L4)
- interpret the security problems occur in software(L2)
- classify the vulnerabilities(L2)

Unit II   **7L**

Access Control:Understanding the Unix Access Control Model, Understanding the Windows Access Control Model, Determining Whether a User Has Access to a File on Unix, Determining Whether a Directory Is Secure, Erasing Files Securely ,Accessing File Information Securely, Restricting Access Permissions for New Files on Unix, Locking Files, Synchronizing Resource Access Across Processes on Unix, Synchronizing Resource Access Across Processes on Windows, Creating Files for Temporary Use, Restricting Filesystem Access on Unix, Restricting Filesystem and Network Access on FreeBSD.

Learning Outcomes:

After completion of this unit, the student will be able to.

- analyze the bugs that can occur in program and try to solve them(L4)
- able to identify the string errors and rectify them(L3)

Unit III   **8L**

Input Validation: Understanding Basic Data Validation Techniques, Preventing Attacks on Formatting Functions, Preventing Buffer Overflows, Using the SafeStr Library, Preventing Integer Coercion and Wrap-Around Problems, Using Environment Variables Securely, Validating Filenames and Paths, Evaluating URL Encodings, Validating Email Addresses, Preventing Cross-Site Scripting, Preventing SQL Injection Attacks, Detecting Illegal UTF-8 Characters, Preventing File Descriptor Overflows When Using select( )

Learning Outcomes:

After completion of this unit, the student will be able to

- analyze the different vulnerabilities related to inter data(L4)
- handle the input and validate them(L2)

Unit IV   **8L**

Symmetric Cryptography Fundamentals: Representing Keys for Use in Cryptographic Algorithms, Generating Random Symmetric Keys, Representing Binary Keys (or Other Raw Data) as Hexadecimal, Turning ASCII Hex Keys (or Other ASCII Hex Data) into Binary, Performing Base64 Encoding, Performing Base64 Decoding, Representing Keys (or Other Binary Data) as English Text, Text Keys to Binary Keys, Using Salts, Nonces, and Initialization Vectors, Deriving Symmetric Keys from a Password, Algorithmically Generating Symmetric Keys from One Base Secret, Encrypting in a Single Reduced Character Set, Managing Key Material Securely, Timing Cryptographic Primitives

Learning Outcomes:

After completion of this unit, the student will be able to

- understand Memory Forensics and Volatility (L2)
- find artifacts in Process Memory(L1)

Unit V   **10L**

Anti-Tampering: Understanding the Problem of Software Protection, Detecting Modification, Obfuscating Code, Performing Bit and Byte Obfuscation, Performing Constant Transforms on Variables, Merging Scalar Variables, Splitting Variables, Disguising Boolean Values, Using Function Pointers, Restructuring Arrays, Hiding Strings, Detecting Debuggers, Detecting Unix Debuggers, Detecting Windows Debuggers, Detecting SoftICE, Countering Disassembly, Using Self-Modifying Code.

Learning Outcomes:

After completing this Unit, students will be able to

- develop web applications and validate them(L3)
- understand the concept of maintaining session state(L2)

Text Book(s)

1. John Viega and Matt Messier, Secure Programming Cookbook for C and C++, O'Reilly Publication,2003.

Course Outcomes:

After completion of course, students would be able to:

- write secure programs and various risk in the software. (L5)
- describe various possible security attacks(L4)
- classify various errors that lead to vulnerabilities(L2)
- real time software and vulnerabilities associated with them. (L6)

19ECS778: INTERNET TECHNOLOGIES AND CYBERLAWS

L T P C
2 0 2 3

This course provides an overview of various crimes encountered in the internet era and the laws that prevent the cyber crimes and discusses upon copyright issues, taxation policies and digital signatures to protect the content over the internet.

Course Objectives
- Learn about various types of cyber attacks
- Understand the concepts related to contracts and IPR in internet
- Familiarize about copyright issues, taxation, and their protection
- Analyze about digital signature and its needs.

Unit I   7L
Crimes of this millennium, checks and balances against arbitrary arrests, concept of cyber crime and the IT act, hacking, teenage web vandals, cyber fraud and cyber cheating, virus on the internet, other IT act offences, network service providers, criminal justice in India and implications.
Learning outcomes
After completion of this unit the student will be able to
- Tabulate various cybercrimes(L1)
- Infer on criminal justice over cybercrimes(L2)

Unit II   7L
Contracts in the InfoTech world, click wrap and shrink wrap contracts, contract formation under the Indian context, contract formation on the internet, terms and conditions of the contract, jurisdiction and information technology act, foreign judgments in India, IPR disputes, misuse of the law of jurisdiction, jurisdictional disputes with respect to the internet in USA.
Learning outcomes
After completion of this unit the student will be able to
- Understand the concept and terms in digital contracts(L2)
- Analyze IPR and its implications(L4)

Unit III   9L
Concept of domain name and reply to cyber squatters, meta-tagging, copyright ownership and assignment, license of copyright, copyright term and respect for foreign works, copyright infringement remedies and offences, copyright protection of content on the internet, computers software piracy.
Learning outcomes
After completion of this unit the student will be able to
- Understand the concepts of copyright(L2)
- Analyze the implications related to copyright protection(L4)

Unit IV   9L
Concept of permanent Establishment, PE in cross border E-Commerce, the modeled nations, model tax treaty, law of double taxation avoidance agreements, tax Agents of non-residents

under the income tax act and the relevance to E-Commerce, impact of the internet on customs duties, taxation policies in India.

Learning outcomes

After completion of this unit the student will be able to

- Learn the concept of Permanent Establishment(L1)
- Understand laws of taxation in ecommerce and its impact(L2)

Unit V   **10L**

Digital signatures, digital signature certificate, certifying authorities and liability in the event of digital signature compromise, status of electronic records as evidence, proving digital signatures, proof of electronic agreements, proving electronic messages, goods and services, consumer complaint, defect in goods and deficiency in services, restrictive and unfair trade, practices, reliefs under CPA, consumer forums, jurisdictions and implications on cyber consumers in India.

Learning outcomes

After completion of this unit the student will be able to

- Understand the details of digital signatures(L2)
- Analyze the practices in ecommerce pertaining to agreements, jurisdictions in cyber world(L4)

Text Book(s):

1. Vivek Sood, Cyberlaw Simplified, Tata McGrawHll, 2001.
2. Godbole, Information Systems Security, Wiley, 2008.
3. Merkov, Breithaupt, Information Security, Prentice Hall of India HI, 2005.
4. Yadav, Foundations of Information Technology, 3/e, New Age, 2006.

Course outcomes

After completion of this unit the student will be able to

- Distinguish various cyber crimes
- Understand about implementation of digital contracts, copyrights and taxation in ecommerce.
- Outline about digital signatures, agreements related to cyber consumers.

19ECS757: MALWARE ANALYSIS AND REVERSE ENGINEERING

L T P C
2 0 2 3

The course will provide an overview of malware research, intelligence gathering related to malware, and provide basic skills required to analyze and dis-assemble malicious programs. Students will explore the tools required to analysis and do reverse engineering of malicious code, learn malware Forensics techniques, how malware functions, and will perform live analysis and reverse engineering exercises.

Course Objectives:
- Learn fundamentals and Classification of Malware
- Introduce Tools and Techniques of malware analysis
- Enable to Identify malware through behavioural and Code analysis
- Describe Malware Forensics

Unit I   **9L**
Introduction: The goals of malware analysis, malware analysis techniques, types of malware, general rules for malware analysis.
Basic Static Techniques: antivirus scanning, hashing, finding strings, packed and obfuscated malware, portable executable file format, linked libraries and functions, dynamically linked functions with dependency walker, static analysis in practice, PE file headers and sections.
Malware Analysis in Virtual Machines: the structure of a virtual machine, creating malware analysis machine, configuring VMware, using malware analysis machine, risks of using vmware for malware analysis.
Dynamic Analysis:Sandboxes - using a malware sandbox, sandbox drawbacks. Running malware, monitoring with process monitor, viewing processes with process explorer, comparing registry snapshots with regshot, using ApateDNS, monitoring with netcat, packet sniffing with wireshark, using INetSim
Basic Dynamic Tools in Practice.
Learning Outcomes:
After completion of this unit, the student will be able to
- understand goals of malware analysis(L1)
- compare malware analysis techniques(L2)
- identify malware analysis. (L1)

Unit II   **7L**
Advanced Static Analysis: x86 Disassembly - levels of abstraction, reverse-engineering, x86 architecture.
IDA PRO 87: loading an executable, IDA pro interface, using cross-references, analyzing functions, using graphing options, enhancing disassembly, extending IDA with plug-ins.
Recognizing C Code Constructs in Assembly: global vs. local variables, disassembling arithmetic operations, recognizing if statements, recognizing loops, understanding function call conventions, analyzing switch statements, disassembling arrays, identifying structs, analyzing linked list traversal.
Analyzing Malicious Windows Programs: windows API, windows registry, networking APIS, following running malware, kernel vs. user mode, the native API.
Learning Outcomes:
After completion of this unit, the student will be able to
- review C code constructs (L2)
- compare various statis analysis methods. (L2)
- understand how x86 and IDA PRO 87 is implemented (L6)

Unit III   **8L**

Advanced Dynamic Analysis: Debugging -source-level vs. assembly-level debuggers, kernel vs. user-mode debugging, using a debugger, exceptions, modifying execution with a debugger. OLLYDBG: loading malware, OllyDbg interface, memory map, viewing threads and stacks, executing code, breakpoints, loading DLLs, tracing, exception handling, patching analyzing shellcode, plug-ins, scriptable debugging.
Kernel Debugging WithWinDbg: drivers and kernel code, setting up kernel debugging, using WingDbg, Microsoft symbols, rootkits, loading drivers, kernel issues for windows.

Learning Outcomes:
After completion of this unit, the student will be able to
- develop debuggers with WinDbg(L3)
- trace issues in different interfaces (L2)

Unit IV   **8L**
Malware Functionality: Malware behavior – downloaders and launchers, Reverse Shell, RATs, Botnets, Credential stealers, persistence mechanism, privilege escalation, user mode rootkits.
Covert Malware Launching: Launchers, process injection, process replacement, hook injection, detours, APC injection.
Data Encoding: Goals of analyzing encoding algorithms, simple ciphers, common cryptographic algorithms, custom encoding, decoding.
Malware Focused Network Signatures: Network countermeasures, safely investigate on attackers online, content-based network countermeasures, combining static and dynamic analysis techniques, attacker's perspective.

Learning Outcomes:
After completion of this unit, the student will be able to
- record the experience of malware behavior by covert malware launching, data encoding and malware network signatures (L1)
- evaluate cryptographic algorithms. (L5)

Unit V   **10L**
Anti-Reverse Engineering: Anti–Disassembly: Understanding anti-disassembly, defeating disassembly algorithms, anti-disassembly techniques, obscuring flow control, thwarting stack-frame analysis.
Anti-Debugging: Windows debugger detection, identifying debugger behavior, interfering with debugger functionality, debugger vulnerabilities.
Anti-Virtual Machine Techniques: VMware artifacts, vulnerable instructions.

Learning Outcomes:
After completion of this unit, the student will be able to
- identify anti disassembly techniquesL1)
- explain anti debugger behavior and functions. (L4)
- understand vulnerable instructions (L2)

Text Book(s)
1.   Michael Sikorski, Andrew Honig, Practical Malware Analysis: The Hands On Guide to Dissecting Malicious Software, William Pollock, 2012

Course Outcomes:
After completion of this course, the student will be able to
- apply malware analysis methodology and technology (L3)
- implement advanced static and dynamic malware analysis(L3)
- make use of Memory Forensics and Volatility (L3)
- find Artifacts in Process Memory Identify known anti-reverse engineering techniques(L1)
- apply DNS Server Process and Reverse IP Process(L3)

19ECS759: ETHICAL HACKING

```
L  T  P  C
2  0  2  3
```

This course provides an overall idea of various ethical hacking techniques. It also provides various reverse engineering technique.Exploitation techniques for Linux and windows operating systems are also provided.

Course Objectives:
- Learn the grey hat way of hacking.
- Understand the red team and purple team operations.
- Familiarize with Linux exploitation techniques.
- Implement windows exploitation techniques.

Unit I   **8L**
Introduction to grey hat hacking: Know your Enemy, the grey hat way, Evolution of cyber law, C Programming Language, computer memory, Assembly language basics, Debugging with gdb
Introduction to reverse engineering: Code Annotation, Collaborative Analysis, Dynamic Analysis
Learning Outcomes
After completion of this unit the student will be able to
- understand Grey hat hacking (L1)
- design and implement reverse engineering techniques(L6)

Unit II   **10L**
Red team Operations: Objectives, Scope, Time, Audience, Overcoming Limitations, Understanding Threads, Attack frameworks, Testing Environment, Adaptive testing.
Purple Teaming: Introduction, Blue team operations, Purple team operations, Purple team optimization.
Bug Bounty Programs: History of Vulnerability Disclosure, Bug crowd, earning a living finding bugs, incident response, Gaining Access - Capturing Password Hashes, Using Winexe, Using WMI, WinRM
Learning Outcomes
After completion of this unit the student will be able to
- Explain various red team and purple team operation (L4)
- Identify bug bounty programs (L3)

Unit III   **8L**
Linux Exploits: Stack operations and function-calling procedures, Buffer Overflows, Local Buffer overflow Exploits, Exploit Development process. Format String Exploits, Memory protection schemes.
Learning Outcomes
After completion of this unit the student will be able to
- understand Linux exploitation techniques (L1)
- use buffer overflow attack techniques(L3)

Unit IV   **8L**
Windows Exploits; Compiling and debugging windows programs, Writing Windows, Exploits, understanding structured Exception handling, Understanding and bypassing windows memory protections.

Learning Outcomes

After completion of this unit the student will be able to
- use windows exploitation techniques (L3)
- Implement windows memory protection bypass techniques(L4)

Unit V   **8L**

Web application exploitation: The Evolution of cross site scripting, Framework Vulnerabilities
Malware analysis: Dissecting Mobile Malware, The android platform, The IOS Platform.
Dissecting ransomware, . Dissecting ransomlock, WannaCry. Introduction to honeypots.

Learning Outcomes

After completion of this unit the student will be able to
- understand malware analysis (L1)
- design and implement Web application exploitation (L6)

Text Books:

1.   Allen Harper, Gray Hat Hacking: The Ethical Hacker's Handbook, Mc Graw Hill Education ,5th Edition.

Course Outcomes:

After completion of this course, the student will be able to
- understand Grey hat hacking techniques. (L2)
- Differentiate red team and purple team operations. (L4)
- Implement Linux and Windows exploitation. (L6)
- Implement malware analysis on various platforms (L6)

19ECS761: DATA ENCRYPTION AND COMPRESSION

<div align="right">

L T P C
2 0 2 3

</div>

The emphasis of the course is processing of encryption and compression in the design of cryptographic algorithms. The course will start with encryption is the process of encoding messages or information in such a way that only authorized parties can read it. And compression, source coding, or bit-rate reduction involves encoding information using fewer bits than the original representation. As a part of cryptanalysis we will study several attacks on these algorithms as well as their remedies. We will also study recent developments in Entropy encoding and differential encoding techniques.

Course Objectives:
- The objective of this course is to introduce to the students the fundamentals of data compression, data encryption and data security.
- Students will be able to distinguish among various types of Data Compression and Encryption techniques/algorithms for text, images.
- Enable the student to learn basic knowledge in cryptographic various algorithms.
- Demonstrate the handling of variety of threats during transmission of information over network and also how to overcome it.
- Describe and apply various techniques for text compression and also evaluate performance of the coding techniques.

Unit I   **6L**

Introduction to Security: Need for security, Security approaches, Principles of security, Types of attacks. Encryption Techniques: Plaintext, Cipher text, Substitution & Transposition techniques, Encryption & Decryption, Types of attacks, Key range & Size.

Learning Outcomes:
After completion of this unit the student will be able to
- learn why network need security and its approaches. (L1)
- learn to protect a computer system from security threats and also ethical issues related to computer and network security. (L1)
- finding differentiates between substitution and transposition techniques and also different types of cryptography. (L2)

Unit II   **9L**

Symmetric & Asymmetric Key Cryptography: Algorithm types & Modes, DES, IDEA, Differential & Linear Cryptanalysis, RSA, Symmetric & Asymmetric key together, Digital signature, Knapsack algorithm. User Authentication Mechanism: Authentication basics, Passwords, Authentication tokens, Certificate based & Biometric authentication, Firewall.

Learning Outcomes:
After completion of this unit the student will be able to
- learn the environment that led to the development of the Data Encryption Standard (DES). (L6)
- identifying, describing, and explaining the purpose of each stage of the DES algorithm. (L3)
- enumerating the weaknesses of the DES algorithm. (L4)
- finding methods that provide the goals of integrity, authentication and non-repudiation. (L1)

Unit III   **9L**

Case Studies of Cryptography: Denial of service attacks, IP spoofing attacks, Secure inter branch payment transactions, Conventional Encryption and Message Confidentiality, Conventional

Encryption Principles, Conventional Encryption Algorithms, Location of Encryption Devices, Key Distribution.

Public Key Cryptography and Message Authentication: Approaches to Message Authentication, SHA-1, MD5, Public-Key Cryptography Principles, RSA, Digital, Signatures, Key Management.

Learning Outcomes:

After completion of this unit the student will be able to

- learn the requirement in a public key cryptography is a secure algorithm. (L1)
- know the MD5 sum collection in the presence of witnesses. (L1)
- practices and procedures to be followed in carrying out technical and administrative aspects of key management, both automated and manual. (L3)

Unit IV   **7L**

Introduction: Need for data compression, Fundamental concept of data compression & coding, Communication model, Compression ratio, Requirements of data compression, Classification.

Methods of Data Compression: Data compression - Loss less & Lossy.

Learning Outcomes:

After completion of this unit the student will be able to

- describe and apply various techniques for text compression and also evaluate performance of the coding techniques. (L2)
- define and classify compression and also explain its performance parameters. (L1)

Unit V   **11L**

Entropy encoding: Repetitive character encoding, Run length encoding, Zero/Blank encoding.

Statistical encoding: Huffman, Arithmetic & Lempel-Ziv coding; Source encoding - Vector quantization (Simple vector quantization & with error term).

Differential encoding: Predictive coding, Differential pulse code modulation, Delta modulation, Adaptive differential pulse code modulation.

Transform based coding: Discrete cosine transform & JPEG standards, Fractal compression.

Recent trends in encryption and data compression techniques.

Learning Outcomes:

After completion of this unit the student will be able to

- understand need for text compression, types of redundancies and their model to apply coding. (L2)
- examine the given situation to choose the appropriate compression technique by evaluating the performance. (L4)
- conclude on encoded outputs using entropy technique with given the different probability sets. (L5)
- draw and explain different image compression standards. (L2)

Text Book(s)

1. B. Forouzan, Cryptography and Network Security, McGraw-Hill.
2. Nelson, The Data Compression Book, BPB.
3. Atul Kahate, Cryptography & Network Security, TMH

Course Outcomes:

After completion of this course, the students would be able to

- provide security of the data over the network. (L4)
- do research in the emerging areas of cryptography and network security. (L6)
- implement various networking protocols. (L3)
- protect any network from the threats in the world.(L5)

19ECS777: AGILE SOFTWARE DEVELOPMENT

LT P C
2 0 2 3

In software development, agile software development practices are highly effective when deployed in a collaborative, people-centered organizational culture. Students will learn agile development principles and techniques covering the entire software development process from problem conception through development, testing and deployment

Course Objectives

- To understand the agile concept and its importance in software development
- To acquire complete knowledge on Xtreme programming
- To know complete modeling of agile process on XP environment.
- To assess and predict the future development potentiality linked with agile policies.
- To apply the agile knowledge to RUP, and FDD and to extend it to other integrated tools.

8L

UNIT I
Introduction: The Agile manifesto, Agile methods, XP: Extreme Programming, DSDM, SCRUM, feature- Driven Development, modelling misconceptions, agile modelling, tools of misconceptions, updating agile models.

Learning Outcomes:
After completion of this unit, the student will be able to

- What is Agile?(L1)
- Classify different agile methods for software development(L2)
- Describe the origins and motivations of the Agile Manifesto(L3)
- Analyze what scrum methodology is?(L4)
- Construct different agile models(L6)

UNIT II   8L
Extreme Programming: Introduction, core XP values, the twelve XP practices, about extreme programming, planning XP projects, test first coding, making pair programming work.

Learning Outcomes:
After completion of this unit, the student will be able to

- Define core XP values(L1)
- Explain the twelve XP practices(L2)
- Identify different XP projects(L4)
- Justify extreme programming(L5)
- Construct test first coding and pair programming(L6)

UNIT III   8L
Agile Modelling and XP: Introduction, the fit, common practices, modelling specific practices, XP objections to agile modelling, agile modelling and planning XP projects, XP implementation phase.

Learning Outcomes:
After completion of this unit, the student will be able to

- HowAgile Modeling enables developers to develop customized software(L1)
- Illustrate common practices and specific practices(L3)
- Apply XP objections to agile modeling(L4)
- Distinguish agile modelling and planning XP projects(L5)

- Create XP implementation phase(L6)

UNIT IV   **8L**
Feature-Driven Development: Introduction, incremental software development, Regaining Control,The motivation behind FDD, planning an iterative project, architecture centric, FDD and XP.
Learning Outcomes:
After completion of this unit, the student will be able to
- Define Feature-Driven Development(L1)
- Demonstrate incremental software development(L2)
- Apply regaining control techniques(L3)
- Appraise the motivation behind FDD(L5)
- Modify iterative project and architecture centric(L6)

UNIT V   **10L**
Agile Methods with RUP and PRINCE2 and Tools and Obstacles: Agile modelling and RUP, FDD and RUP, agile methods and prince2, tools to help with agile development, Eclipse, An agile IDE, obstacles to agile software development, management intransigence, the failed project syndrome, contractual difficulties, familiarity with agility.
Learning Outcomes:
After completion of this unit, the student will be able to
- Recall agile modelling and RUP, FDD(L1)
- Explain prince2, tools and obstacles to agile software development(L2)
- Identify tools to help with agile development(L3)
- Estimate the failed project syndrome and contractual difficulties(L4)
- ConstructAgile methods with RUP and PRINCE2(L5)

Text Book(s):
1. John Hunt, Agile Software Construction,1st Edition, Springer,2005
2. Craig Larman, Agile and Iterative Development: A Manager's Guide, Addison-Wesley, Pearson Education – 2004.
3. Pearson, Robert C. Martin, Juli, James Shore, Chromatic 2013, The Art OfAgile Development, O'Reilly Media.
4. Elisabeth Hendrickson, Agile Testing, Quality Tree Software Inc 2008.

Course Outcomes:
After completion of this course, the student will be able to
- use agile methods in various development environments
- apply Xtreme programming in XP projects confidently.
- design and model agile methods in XP environments.
- develop abilities on Future Driven Development with iterative projects visualize applications with RUP and PRINCE2 like tools by agile methods

19ECS704: PRAGMATICS OF INFORMATION SECURITY

LT P C
2 0 2 3

The goal of this course is to provide an up-to-date survey of developments in computer security. Central problems that confront security designers and security administrators include defining the threats to computer and network systems, evaluating the relative risks of these threats, and developing cost-effective and user-friendly countermeasures.

Course Objectives

- Deep understanding of various basic principles and examines their application in specific areas of computer security.
- Demonstrates various issues relating to authentication and access control.
- Design approaches to meet specific computer security requirements.
- An understanding of the current status and future direction of technology in information security.

Unit I   8L

Overview: Computer Security Concepts, Requirements, Architecture, Trends.
Strategy Perimeter Security: Firewalls, Intrusion Detection, Intrusion Prevention systems, Honeypots.
Case Study: Readings, Intrusion and intrusion detection by John McHugh.

Learning Outcomes:

After Completion of this unit the student will be able to

- describe the key security requirements of confidentiality, integrity, and availability.(L2)
- understand the types of security threats and attacks that must be dealt with different categories of computer and network assets. (L2)
- distinguish among various types of intruder behavior patterns. (L2)
- understand the basic principles of and requirements for intrusion detection and prevention systems. (L2)
- describe the purpose of honey pots. (L2)

Unit II   9L

User Authentication: Password, Password-based, token based, Biometric, Remote User authentication. Access Control: Principles, Access Rights, Discretionary Access Control, Unix File Access Control, Role Based Access Control Internet Authentication.
Applications: Kerberos, X.509, PKI, Federated Identity Management.

Learning Outcomes:

After Completion of this unit the student will be able to

- discuss the four general means of authenticating a user's identity. (L6)
- present an overview of token-based user authentication and issues involved and the approaches for remote user authentication. (L5)
- explain how access control fits into the broader context that includes authentication, authorization, and audit. (L2)
- describe the Principle concepts of UNIX file access control model and role-based access control. (L2)
- summarize the basic operation of Kerberos. (L2)
- compare the functionality of Kerberos version 4, version 5 and function of X.509 certificates. (L2)

Unit III   8L

Cryptographic Tools: Confidentiality with symmetric encryption, Message Authentication & Hash Functions, Digital Signatures, Random Numbers. Symmetric Encryption and Message. Confidentiality: DES, AES, Stream Ciphers, Cipher Block Modes of Operation, Key Distribution.

Learning Outcomes:

After Completion of this unit the student will be able to

- explain the basic operation of symmetric block encryption algorithms. (L2)
- compare and contrast block encryption and stream encryption. (L4)
- discuss the use of secure hash functions for message authentication. (L6)
- describe the structure and function of DES and AES. (L2)
- distinguish among the major block cipher modes of operation. (L4)
- discuss the issues involved in key distribution. (L2)

Unit IV   **8L**

Internet Security Protocols: SSL, TLS, IPSEC, S/ MIME. Public Key Cryptography and Message. Authentication: Secure Hash Functions, HMAC, RSA, Diffie Hellman Algorithms.

Case Study: Readings, Programming Satan's Computer Ross Anderson and Roger Needham.

Learning Outcomes:

After Completion of this unit the student will be able to

- understand the functionality of S/MIME and the security threats it addresses. (L2)
- explain the key components of SSL. (L5)
- discuss the use of HTTPS. (L6)
- understand the operation of SHA-1 and SHA-2. (L2)
- present an overview of the use of HMAC for message authentication. (L2)
- describe the RSA algorithm and Diffie-Hellman algorithm. (L2)

Unit V   **9L**

Malicious Software: Types of Malware, Viruses & Counter Measures, Worms, Bots.

Root kits Software Security: Buffer Overflows, Stack overflows, Defense, Other overflow attacks

Case Study: Readings, Smashing The Stack for Fun and Profit, Aleph One
http://www.phrack.com/issues.html?issue=49&id=14#article

earning Outcomes:

After Completion of this unit the student will be able to

- describe three broad mechanisms malware uses to propagate. (L2)
- understand the basic operation of viruses, worms, and Trojans. (L2)
- describe four broad categories of malware payloads. (L4)
- understand the different threats posed by bots, spyware, and root kits. (L2)
- describe some malware countermeasure elements. (L4)
- describe three locations for malware detection mechanisms. (L4)

Text Book(s):

1. William Stalling, Lawrie Brown, Computer Security: Principles and Practice, Pearson, 3rd Edition, 2010

Course Outcomes:

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

- distinguish among various types of intruder behavior patterns(L4)
- describe the key security requirements of confidentiality, integrity, and availability(L1)
- explain how access control fits into the broader context that includes authentication, authorization, and audit(L5)
- describe the structure and function of DES and AES. (L2)
- describe four broad categories of malware payloads. (L4)

19ECS726: PRAGMATICS OF INFORMATION SECURITY LABORATORY

L T P C
0 0 4 2

The following programs should be implemented preferably on platform Windows/Unix using

C language (for 1-5) and other standard utilities available with UNIX systems (for 6-15) :-

1. Implement the encryption and decryption of 8-bit data using Simplified DES Algorithm (created by Prof. Edward Schaefer) in C

2. Write a program to break the above DES coding

3. Implement Linear Congruential Algorithm to generate 5 pseudo-random numbers in C

4. Implement Rabin-Miller Primality Testing Algorithm in C

5. Implement the Euclid Algorithm to generate the GCD of an array of 10 integers in C

6. a) Implement RSA algorithm for encryption and decryption in C

    b) In an RSA System, the public key of a given user is e=31, n=3599. Write a program to find private key of the User.

7. Configure a mail agent to support Digital Certificates, send a mail and verify the correctness of this system using the configured parameters.

8. Configure SSH (Secure Shell) and send/receive a file on this connection to verify the correctness of this system using the configured parameters.

9. Configure S/MIME and show email-authentication.

10. Implement encryption and decryption with open SSL.

11. Implement Using IP TABLES on Linux and setting the filtering rules.

12. Implementation of proxy based security protocols in C or C++ with features like confidentiality, integrity and authentication

19ECS724: DIGITAL FORENSICS LABORATORY

L T P C
0 0 4 2

The following exercises have to be performed using various software tools/utilities mentioned Software Tools:

1. Cyber Check 4.0 – Academic Version

2. Cyber Check Suite

3. Mobile Check

4. Network Session Analyser

5. Win-LiFT

6. True Imager

7. True Traveller

8. Photo Examiner Ver1.1

9. CDR Analyzer

Forensics Exercises:

I) DiskForensics:

1. Identify digital evidences

2. Acquire the evidence

3. Authenticate the evidence

4. Preserve the evidence

5. Analyze the evidence

6. Report the findings

II) Network Forensics:

- Intrusion detection

- Logging (the best way to track down a hacker is to keep vast records of activity on a network with the help of an intrusion detection system)

- Correlating intrusion detection and logging

III) Device Forensics:

1. PDA

2. Mobile phone

3. Digital Music

4. Printer Forensics

5. Scanner Forensics

19ECS792: TECHNICAL PAPER WRITING

L T P C
0 0 4 2

Each student shall survey a technical topic related to a chosen specialization and prepare/submit a report in a specified format. Each student has to prepare a power point presentation on a selected technical topic with a novelty and get it evaluated by the faculty assigned for this purpose.

19ECS760: STEGANOGRAPHY AND DIGITAL WATERMARKING

L T P C
2 0 2 3

Information Hiding plays a very important role in providing of security to information and copy right protection. It consists of two parts: Digital Steganography and Digital Watermarking. Steganography is the art of information hiding in objects or images. It is a field with a rich heritage, and an area of rapid current development. Watermarking provides a copyright protection of video and audio products against multimedia pirates. Like probability theory, information and coding theory, signal processing procedures used for embedding of additional information into cover objects can be completely described by computer programs. Therefore, this course is especially useful for students specialized in computer science.

Course Objectives:
- To learn about steganography methods of hiding data
- To learn about steganography Algorithm and Techniques
- To learn about the watermarking models, applications and tools
- To learn about watermark security and authentication

Unit I   7L
Introduction: Overview of Information Hiding, Steganography and Watermarking. Importance of Digital Watermarking and Steganography. Applications and Properties of Steganography and Watermarking. Evaluating and Testing Steganographic Systems.
Learning Outcomes:
After completion of this unit the student will be able to
- Understand the techniques of information hiding(L2).
- Apply Digital Watermarking and Steganography(L3).

Unit II   7L
Models of Watermarking: Notation, Communications, Communication-Based Models of Watermarking, Geometric Models of Watermarking, Modeling Watermark Detection by Correlation
Basic Message Coding: Mapping Messages into Message Vectors, Error Correction Coding, Detecting Multi symbol Watermarks.
Learning Outcomes:
After completion of this unit the student will be able to
- Classify Models of Watermarking. (L2)
- Analyze how error correction coding works. (L4)

Unit III   8L
Watermarking with Side Information: Informed Embedding, Watermarking Using Side Information, Dirty-Paper Codes.
Practical Dirty-Paper Codes: Practical Considerations for Dirty-Paper Codes, Approaches to Dirty-Paper Code Design, Implementing DM with a Simple Lattice Code, Typical Tricks in Implementing Lattice Codes, Coding with Better Lattices, Making Lattice Codes Survive Valumetric Scaling.
Analyzing Errors: Message Errors, False Positive Errors, False Negative Errors, ROC Curves, Interpolation Along One or Both Axes, The Effect of Whitening on Error Rates, Analysis of Normalized Correlation.
Learning Outcomes:
After completion of this unit the student will be able to
- Understand information embedding. (L3)
- Identify and implement practical dirty-paper codes. (L3)

- Recognize various message errors (L4)

Unit IV   **6L**
Perceptual Models: Evaluating Perceptual Impact of Watermarks, 8.2 General Form of a Perceptual Model, Watson's DCT-Based Visual Model, Perceptual Model for Audio, Perceptually Adaptive Watermarking.
Learning Outcomes:
After completion of this unit, the student will be able to
- Choose Perceptual Models for visual media and audio. (L5)
- Evaluate impact of watermarks(L3)

Unit V   **14L**
Steganography: Steganographic Communication, Notation and Terminology, Information-Theoretic Foundations of Steganography, Practical Steganographic Methods, Masking Embedding as Natural Processing, Minimizing the Embedding Impact.
Steganalysis:Steganalysis Scenarios, LSB Embedding and the Histogram Attack, Sample Pairs Analysis, Blind Steganalysis of JPEG Images Using Calibration, Blind Steganalysis in the Spatial Domain
Learning Outcomes:
After completion of this unit the student will be able to
- make use of different steganalysis techniques for embedding(L3)
- understand different type of steganography methods of hiding data(L2)

Text Book(s)
1. Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, Ton Kalker, Digital Watermarking and Steganography, Margan Kaufmann Publishers, 2nd Edition, 2008.
2. Neil F. Johnson, Zoran Duric, SushilJajodia, Information Hiding: Steganography and Watermarking - Attacks and Counter measures, Springer, 2012.
3. Stefan Katzenbeisser, Fabien A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking, 2016.

Course Outcomes:
After completion of this course, the student will be able to
- understand different type of steganography methods of hiding data(L2)
- understand public key steganography and apply the steganography algorithm(L2)
- make use of different steganography techniques(L3)
- apply different tools(L3)
- make use of different steganography techniques for embedding(L3)
- apply different techniques and tools of watermarking (L3)

19ECS782: INTRUSION DETECTION AND PREVENTION SYSTEM

L T P C
2 0 2 3

This course covers the fundamentals of intrusion detection and prevention techniques. Course will explore the difference between IDS and IPS. This course covers how to detect attacks using neural networks, artificial intelligence. In this course we will discuss how to use machine learning techniques in intrusion detection. This course provides an overall idea on wireless intrusion detection system.

Course Objectives:
- Familiarize the students with the network security and intrusion detection and prevention techniques.
- Enable the students to master the knowledge about intrusion detection and prevention in the context of real-life applications.
- Demonstrate various tools for Intrusion Detection Mechanisms.
- To prepare the students for understanding, evaluating critically, and assimilating new knowledge and emerging technology in network security Understand the necessary mathematical abstraction to solve problems.
- Understand wireless intrusion detection techniques to protect from threats.

Unit I   **9L**
Outlier Detection: Introduction, Basics of Outlier Detection, Data Labels, Application Domains., Clustering-Based Outlier Detection Techniques, Statistical-Based Approaches.
Network Traffic Monitoring and Analysis: Introduction, Intrusion Detection Analysis, Computational IDS Tools,
Learning Outcomes:
After completion of this unit, the student will be able to.
- How components in different layers inter-operate in the intrusion detection and prevention system. (L2)
- Summarize network traffic monitoring and analysis. (L2)

Unit II   **7L**
Using Routers and Honeypots in Combination for Collecting Internet Worm Attacks: Definition and History of Honeypots, Types of Threats, The Value of Honeypots, Honeypot Types Based on Interaction Level., Notable Honeypots, Honeypot Implementation Steps.
Attack Severity–Based Honeynet Management Framework: Formal Foundation, Mathematical Background, Framework Details, Algorithm Implementation.
Learning Outcomes:
After completion of this unit, the student will be able to.
- Classify various types of threats based on their behavior. (L2)
- Analyze how mathematical back ground used to design frame work and design an algorithm. (L4)

Unit III   **8L**
Intrusion Detection Systems for Critical Infrastructure: Intrusion Detection and Prevention Systems (IDPS), Intrusion Detection and Prevention System for Industrial Control Systems.
Cyber Security of Smart Grid Infrastructure: Smart Grid Infrastructures, Security Issues of a Cyber-Physical Smart Grid, Security Requirements of a Smart Grid,
Learning Outcomes:

- Apply intrusion detection technique for real world applications. (L3)
- Identify security issues of a cybersecurity and security requirements. (L3)

Unit IV   **8L**
New Unknown Attack Detection with the Neural Network–Based IDS: Intrusion Detection System Definition, Neural Networks, Input Data for the Detection of Attacks, The Proposal of the New IDS Architecture.
Artificial Intelligence– Based Intrusion Detection Techniques: Intrusion Detection in Wired Networks, Applications of Artificial Intelligence in Intrusion Detection, Challenges in IPv6 Networks, Application of Artificial Intelligence in Other Environments.

Learning Outcomes:
After completion of this unit, the student will be able to
- Choose Neural Network- Based intrusion detection technique to detect unknown attacks. (L5)
- Utilize Artificial intelligence-based intrusion detection techniques in Wired networks. (L3)

Unit V   **10L**
Applications of Machine Learning in Intrusion Detection: Machine Learning in Intrusion Detection, Challenges and Limitations, Potential Countermeasures
Introduction to Wireless Intrusion Detection Systems: Wireless Intrusion Detection Systems, Threat Identification, Intrusion Detection, Alert Correlation, Evaluation

Learning Outcomes:
After completion of this unit, the student will be able to
- Adapt machine learning algorithms to detect attacks. (L6)
- Analyze Wireless IDS and detect threats in wireless IDS. (L4)

Text Book(s)
1. Al-Sakib Khan Pathan, The State of the Art in Intrusion Prevention and Detection, CRC Press.

Course Outcomes:
After completion of this course, the student will be able to
- Illustrate the operational characteristics and the various functions performed by the intrusion detection and prevention system. And how to utilize various IDS tools to Network Traffic Monitoring and Analysis. (L2)
- Make use of routers and honeypots for collecting warm attacks in networks. Design Honeypot management framework. (L3)
- Analyze how to protect critical infra structure from attacks using Intrusion detection system and how to provide security for smart gird infrastructure. (L4)
- Adapt new technologies like neural networks and AI and design new techniques to detect unknown attacks in wired networks. (L6)
- Apply knowledge of machine learning in system and network protection. Optimize performance of detection systems by employing various machine learning techniques. (L3)

19ECS744: SECURE SOFTWARE DESIGN AND ENTERPRISE COMPUTING

L T P C
2 0 2 3

This course provides an overall idea of design, development and implementation methods of secure software as well as deployment, integration and testing processes. It is used for ensuring that software functions as intended and it is free of design defects and implementation flaws.

Course Objectives:

- Learn about need for computer security, vulnerability, database security, attacks and threats.
- Build a secure system from requirements analysis, design and coding to testing.
- Methodologies and tools to design and implement a secure software.
- Identifying the deployment, integration and validating that each security requirement has been implemented
- Auditing the critical applications and maintain the software securely.

Unit I   **8L**
Security in Software Systems: Need for Computer Security, Vulnerability and Attacks, Various Security Attacks, Computer Security, Counter External Threats, Security Programming, Database Security, Security Standards.
Learning Outcomes
After completion of this unit the student will be able to
- Remember the vulnerability, attacks and threats to software. (L1)
- Understand the need for computer and database security. (L2)

Unit II   **7L**
Architecting Secure Software Systems: Building Secured Systems, Security Requirements Analysis, Threat Modeling, Security Design, Security Coding, Safe Programming, Security Review, Generating the Executable, Security Testing.
Learning Outcomes
After completion of this unit the student will be able to
- Understand the architecture of secure software design. (L2)
- Differentiate the security in design and coding. (L2)

Unit III   **9L**
Design Activities: Security Tiers, Requirements and Specifications, Design and Architecture, Deployment and Operations Planning.
Implementation Activities: Stress the Positive and Strike the Balance, Security Mechanisms and Controls, Code Reuse, Coding Resources, Implementing Security Tiers, Code Reviews.
Learning Outcomes
After completion of this unit the student will be able to
- Apply the secure design and implementation activities. (L3)
- Create security specification for design and architecture. (L6)

Unit IV   **9L**
Deployment and Integration: How Does Deployment Relate to Confluence, A Road Map, Advanced Topics in Deployment, integrating with the Security Operations Infrastructure, Third-Generation

Log Analysis Tools, Retro fitting Legacy and Third-Party Components. Testing Activities: Security Testing, Tools of the Trade, Security Bug Life Cycle.

Learning Outcomes

After completion of this unit the student will be able to

- Analysis the developed software using tools and techniques. (L4)
- Integration of third-party components if it is needed. (L4)

Unit V   **8L**

Operating Software Securely: Adjusting Security Thresholds, Dealing with IDS in Operations, Identifying Critical Applications, CSIRT Utilization.

Maintaining Software Securely: Common Pitfalls, Maintaining Software Securely Relate to Confluence, learning from History, Evolving Threats, The Security Patch, Maintaining Software Securely Fit into Security SDLCs.

Learning Outcomes

After completion of this unit the student will be able to

- Evaluate and identify the common pitfalls.   (L5)
- Maintain the software to recover from attack. (L5)

Text Book(s):

1. Asoke K. Talukder, ManishChaitanya, Architecting Secure Software Systems, CRC Press.
2. Kenneth R. VanWyk, Mark G. Graff, Enterprise Software Security, Addison Wisley.

Course Outcomes:

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

- Differentiate between various software vulnerabilities, attacks and threats.
- Interrelate security, software design and development process.
- Methods and tools to design and implement a secure software.
- Identify software process vulnerabilities for an organization
- Monitor resources consumption in a software

19ECS780: WEB APPLICATION SECURITY

L T P C
2 0 2 3

This course offers extensive knowledge for every web developer and web application engineer.A participant will discover important principles of modern web security, and learn about current security best practices. This course also explores the Open Web Application Security Project (OWASP) top 10 2017 which is essential to organizations and IT pros for better managing the emerging impact of application security risks.

Course Objectives:

- Recognize common web application security vulnerabilities and how to determine if they are present in web applications(L1).
- Recognize web application design assumptions and how to exploit them(L1).
- Be familiar with the capabilities of various Browser Proxies(L2).
- Be prepared to detect SQL Injection Vulnerabilities(L3).)
- Be prepared to detect Cross-Site Scripting (XSS) Vulnerabilities(L4).
- Be prepared to test web application security(L5).

Unit I   **7L**
Web Application (In)security: The Evolution of Web Applications, Common Web Application Functions, Benefits of Web Applications, Web Application Security. Core Defense Mechanisms: Handling User Access Authentication, Session Management, Access Control, Handling User Input, Varieties of Input Approaches to Input Handling, Boundary Validation. Multistep Validation and Canonicalization: Handling Attackers, Handling Errors, Maintaining Audit Logs, Alerting Administrators, Reacting to Attacks.
Learning Outcomes
After completion of this unit the student will be able to
- Understand common web app security vulnerabilities(L2).
- Best practices to mitigate vulnerabilities(L3).

Unit II   **8L**
Web Application Technologies: The HTTP Protocol, HTTP Requests, HTTP Responses, HTTP Methods, URLs, REST, HTTP Headers, Cookies, Status Codes, HTTPS, HTTP Proxies, HTTP Authentication, Web Functionality, Server-Side Functionality, Client-Side Functionality, State and Sessions, Encoding Schemes, URL Encoding, Unicode Encoding, HTML Encoding, Base64 Encoding, Hex Encoding, Remoting and Serialization Frameworks.
Learning Outcomes
After completion of this unit the student will be able to
- Understand the basic aspects of HTTP(L2)
- The client-server structure, combined with the ability to simply add headers, allows HTTP to advance along with the extended capabilities of the Web(L3)

Unit III   **8L**

Mapping the Application: Enumerating Content and Functionality, Web Spidering, User Directed Spidering, Discovering Hidden Content, Application Pages Versus Functional Paths, Discovering Hidden Parameters, Analyzing the Application, Identifying Entry Points for User Input, Identifying Server-Side Technologies, Identifying Server-Side Functionality, Mapping the Attack Surface.

Learning Outcomes

After completion of this unit the student will be able to

- Enumerate application's content and functionality(L3).
- Some is hidden, requiring guesswork and luck to discover(L1).
- Examine every aspect of behavior, security mechanisms, and technologies(L2).
- Determine attack surface and vulnerabilities(L4).

Unit IV   **10L**

Attacking Authentication: Authentication Technologies, Design Flaws in Authentication Mechanisms, Bad Passwords, Brute-Forcible Login, Verbose Failure Messages, Vulnerable Transmission of Credentials, Password Change, Functionality, Forgotten Password Functionality, "Remember Me" Functionality, User Impersonation, Functionality Incomplete, Validation of Credentials, Nonunique Usernames, Predictable Usernames, Predictable Initial Passwords, Insecure Distribution of Credentials. Attacking Access Controls: Common Vulnerabilities, Completely Unprotected, Functionality Identifier-Based Functions, Multistage Functions, Static Files, Platform Misconfiguration, Insecure Access Control Methods.

Learning Outcomes

After completion of this unit the student will be able to

- Authentication also lies at the heart of an application's protection against malicious attack(L1).
- Know Front line of defense(L2).
- What could an attacker achieve if he were to target our authentication mechanism(L5).

Unit V   **9L**

Attacking Data Stores: Injecting into Interpreted Contexts, Bypassing a Login, Injecting into SQL, Exploiting a Basic Vulnerability Injecting into Different Statement Types, Finding SQL Injection Bugs, Fingerprinting the Database, The UNION Operator, Extracting Useful Data, Extracting Data with UNION, Bypassing Filters, Second-Order SQL Injection, Advanced Exploitation Beyond SQL Injection: Escalating the Database Attack, Using SQL Exploitation Tools, SQL Syntax and Error Reference, Preventing SQL Injection.

Learning Outcomes

After completion of this unit the student will be able to

- Understand web applications use a database(L2).
- How to exploiting a basic Vulnerability(L6).

Text Book(s):

1. The Web Application Hacker's Handbook: Finding and Exploiting Security DefyddStuttard, Marcus Pinto Wiley Publishing,Second Edition.
2. Professional Pen Testing for Web application, Andres Andreu, Wrox Press
3. Carlos Serrao, Vicente Aguilera, Fabio Cerullo, Web Application Security, Springer, 1st Edition
4. Joel Scambray, Vincent Liu, Caleb Sima ,"Hacking exposed", McGraw-Hill; 3rd Edition, 2010

5. Web Security Privacy and Commerce,OReilly 2ndEdition, 2011
6. Software Security Theory Programming and Practice, Richard sinn, Cengage LearningDatabase Security and Auditing, Hassan, Cengage Learning

Course Outcomes:
After completion of this course, the student will be able to
- Underlying security principles of the web (L1).
- Overview of concrete threats against web applications(L2).
- Insights into common attacks and countermeasures(L3).
- Current best practices for secure web applications(L4).
- Capacity to perform a security assessment, penetration and defense of web systems(L5).

19ECS766: BIOMETRICS

The course is designed to enable the student to apply biometric principles and practices for the secure real time systems, scientific and business applications. This course lays the foundation both for developing program logic and for writing programs in to diagnose the biometric and cyber problems and to build the system with advance solution to solve problem with cyber ethics.

Course Objectives:

- familiarize the student to understand the basics of Biometrics and its functionalities
- enable the student to understand the role of biometric in the organization build program
- explain the context of Biometric Applications
- demonstrate the handle to learn to develop applications with biometric security
- train the student to design of biometric recognition for the organization

Unit I   **6L**

Introduction and Definitions of bio-metrics, Traditional authenticated methods and technologies.

Learning Outcomes:

After completion of this unit the student will be able to

- understand basics of Biometrics(L2).
- list the traditional methods (L1).
- Interpret the technologies of biometrics(L2)

Unit II   **9L**

Bio-metric technologies: Fingerprint, Face, Iris, Hand Geometry Gait Recognition, Ear, Voice, Palm print, On-Line Signature Verification, 3D Face Recognition, Dental Identification and DNA.

Learning Outcomes:

After completion of this unit, the student will be able to

- understand fingerprint, face, iris(L2).
- analyze 3DFace Recognition (L4).
- understand DNA(L2).

Unit III   **5L**

The law and the use of multi bio-metrics systems.

Learning Outcomes:

After completion of this unit, the student will be able to

- analyze law of biometric systems (L4).
- make use of the multi-biometric systems(L3).

Unit IV   **10L**

Statistical measurement of Bio-metric. Bio-metrics in Government Sector and Commercial Sector.

Learning Outcomes:

After completion of this unit, the student will be able to

- understand the government sector and commercial sector for biometrics (L2).
- Apply the statistical measurement of biometric (L3).
- make use statistical measurements in biometric (L3).

Unit V   **12L**

Case Studies of bio-metric system, Bio-metric Transaction. Bio-metric System Vulnerabilities.

Recent trends in Bio-metric technologies and applications in various domains. Case study of 3D face recognition and DNA matching

Learning Outcomes:

After completion of this unit, the student will be able to

- develop programs biometric system (L6).
- understand recent trends in biometric technologies(L2)

Text Book(s):

1. Paul Reid, Biometrics for network security, Hand book of Pearson.
2. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer Verlag, 2003.
3. A.K. Jain, R. Bolle, S. Pankanti (Eds.), BIOMETRICS: Personal Identification in Networked Society, Kluwer Academic Publishers,1999.
4. J. Wayman, A.K. Jain, D. Maltoni, and D. Maio (Eds.), Biometric Systems: Technology, Design and Performance Evaluation, Springer,2004.
5. Anil Jain, Arun A. Ross, Karthik Nanda kumar, Introduction to biometric, Springer,2011.
6. J. Wayman, A. K. Jain, D. Maltoni, and D. Maio, Biometric Systems: Technology, Design and PerformanceEvaluation

Course Outcomes:

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

- identify the various Biometric technologies. (L3)
- understand DNA(L2).
- analyze law of biometric systems (L34.
- understand the government sector and commercial sector for biometrics (L2).
- understand recent trends in biometric technologies(L2)

19ECS752: DIGITAL FORENSICS

<div align="right">

L T P C
2 0 2 3

</div>

The course is designed to enable the student to understand underlying principles and many of the techniques associated with the digital forensic practices and cybercrime, investigate attacks, handling evidences. Student can have a sneak review of Computer Forensics, Network Forensics, And Mobile Forensics.

Course Objectives:

- Familiarize the student about digital and computer forensics.
- Enable the student to learn analysis of crime scene.
- Manage and present evidences
- Demonstrate investigation process with case study.

Unit I   10L

Digital Forensics Science: Forensics science, computer forensics, and digital forensics. Use of Computer Forensics in Law Enforcement, Computer Forensics Assistance to Human Resources/ Employment Proceedings, Computer Forensics Services, Benefits of Professional Forensics Methodology Steps Taken by Computer Forensics Specialists, Types of computer forensic technology, Types of computer forensic systems, case studies.

Learning Outcomes:

After completion of this unit the student will be able to

- understand basics of digital forensics (L1)
- differentiate the types of forensic technologies (L4)

Unit II   10L

Computer Forensics Evidence and Capture: Data Recovery, Role of data backup in data recovery, Hiding and Recovering Hidden Data. Evidence collection and Data seizure: why collecting evidence? Types of evidence, Rules of evidence, Methods of collection of evidence, Reconstruction of evidence, Parts of gathering evidence, Seizure data evidence.

Learning Outcomes:

After completion of this unit, the student will be able to

- explain the capture of digital evidence (L4)
- understand the techniques for reconstructing evidences (L1)

Unit III   10L

Duplication and Preservation of Digital Evidence: Preserving the Digital crime scene, Computer Evidence Processing Steps, Legal Aspects of Collecting and Preserving Computer Forensic Evidence, Computer Image Verification and Authentication: Special Needs of Evidential Authentication, Practical Considerations, computer Forensics Analysis: Discovery of Electronic Evidence, Identification of Data,
Reconstructing Past Events, Networks: A Technical Approach, Tools Needed for Intrusion Response to the Destruction of Data.

Learning Outcomes

After completion of this unit the student will be able to

- illustrate duplication and preservation of digital evidence. (L3)
- reconstruct past events and networks (L2)

Unit IV   10L

Countermeasures: Information Warfare :: Fighting Against Macro Threats: Defensive Strategies for Governments and Industry Groups: What Industry Groups Have Done to Prepare for Information

Warfare , Strategic Diplomacy and Information Warfare ,The Role of International Organizations , The Role of Global Military Alliances , Marshall Law and Cyberspace ,The Super Cyber Protection Agencies , The Information Warfare Arsenal and Tactics of Terrorists and Rogues, The Information Warfare Arsenal and Tactics of Private Companies , The Information Warfare Arsenal of the Future: Email Wiretaps Like Carnivore Can Steal Sensitive Correspondence , IW Weapons of the Future.

Learning Outcomes

After completion of this unit the student will be able to
- Understand various strategies for information warfare(L1)
- develop countermeasure models (L3)

Unit V   **10L**

Advanced Computer Forensics: Advanced Encryption: The Need to Conceal, Advanced Hacking, Advanced Tracker Hackers, Computer Forensics Resources.
Mobile Forensics: mobile forensics techniques, mobile forensics tools.
Legal Aspects of Digital Forensics: IT Act 2000, amendment of IT Act 2008.

Learning Outcomes

After completion of this unit the student will be able to
- Understand advanced hacking tools (L1)
- develop mobile forensics (L3)

Text Book(s)

1. Computer Forensics computer crime scene investigation, second edition, John R.Vacca, John Sammons
2. The Basics of Digital Forensics, Elsevier. John Vacca, Computer Forensics: Computer Crime Scene Investigation, Laxmi Publications

Course Outcomes

After completion of this course, the student will be able to
- understand the basics of digital forensics. (L2)
- Implement the capture, duplication, and preservation of digital evidence. (L4)
- Analyze the digital evidence to find the digital artifacts. (L6)
- Understand the legal aspects of the digital forensics (L3)

19ECS786: CLOUD SECURITY

LT P C
2 0 2 3

Cloud computing infrastructure have become a mainstay of the IT industry, opening the possibility for on-demand, highly elastic and infinite compute power with scalability and supporting the delivery of mission-critical secure enterprise applications and services. This course provides the ground-up coverage on the high-level concepts of cloud landscape, architectural principles, techniques, design patterns and real-world best practices applied to Cloud service providers and consumers and delivering secure Cloud based services

Course Objectives:

- Cloud computing and architectural principles with primary focus on security techniques and security design
- Deep dive on Security architecture, Technological Influences and best practices
- Current security standards, protocols, and best practices intended for delivering Cloud based enterprise IT services
- Architectural and design approaches to designing secure cloud services
- Applying industry security standards, regulatory mandates, audit policies and compliance requirements
- Survey on Cloud vendor security implementations, compliance and autonomic protection mechanisms

Unit I   **10L**

Cloud Computing Fundamentals: Essential Characteristics, Architectural Influences, Technological Influences, Operational Influences, Out sourcing.
Cloud Computing Architecture: Cloud Delivery Models, Cloud Deployment Models, Expected Benefits
Learning Outcomes
After completion of this unit, the student will be able to
- Understand what is Cloud computing
- Architectural and Technological Influences of Cloud Computing
- Understand the Cloud deployment models and Scope of Control

Unit II   **7L**

Cloud Computing Software Security Fundamentals :Cloud Information Security Objectives, Cloud Security Services, Relevant Cloud Security Design Principles, Secure Cloud Software Requirements, Approaches to Cloud Software Requirements Engineering, Cloud Security Policy Implementation, Secure Cloud Software Testing, Cloud Computing and Business Continuity Planning/Disaster Recovery, Redundancy Provided by the Cloud, Secure Remote Access, Integration into Normal Business Processes
Learning Outcomes
After completion of this unit, the student will be able to
- Developing secure software is based on applying the secure software design principles that form the fundamental basis for software assurance.
- Understand the cloud security services, cloud security principles, secure software requirements, and testing concepts.
- Understand the cloud business continuity planning, disaster recovery, redundancy, and secure remote access.

Unit III   **6L**
Cloud Computing Risk Issues: The CIA Triad, Privacy and Compliance Risks, Threats to Infrastructure, Data, and Access Control, Cloud Service Provider Risks
Learning Outcomes

After completion of this unit, the student will be able to
- Understand the cloud computing risks, threats privacy assurance and compliance regulations
- Understand the "traditional" concepts of data, identity, and access management (IAM) risks, and how those risks and threats may be unique to cloud service providers (CSPs)

Unit IV   **9L**

Cloud Computing Security Challenges: Security Policy Implementation, Policy Types, Computer Security Incident Response Team (CSIRT), Virtualization Security Management, VM Security Recommendations, VM-Specific Security Techniques

Learning Outcomes

After completion of this unit, the student will be able to
- identify the management challenges, opportunities and security posture of the organization it relates to the virtualization perimeter.
- to understand and make security policy and computer intrusion detection and response implementation techniques and dive deeply into virtualization security management issues

Unit V   **9L**

Cloud Computing Security Architecture: Architectural Considerations, General Issues, Trusted Cloud Computing, Secure Execution Environments and Communications, Microarchitectures, Identity Management and Access Control, Identity Management, Access Control, Autonomic Security

Learning Outcomes

After completion of this unit, the student will be able to
- understand the important cloud computing security architectural issues, including trusted cloud computing, secure execution environments, and micro architectures.
- understand and identify the identity management and access control and develops the concepts of autonomic systems and autonomic protection mechanisms.

Text Book(s)
1. Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, 2010, Wiley Publishing, Inc

Course Outcomes:

After successful completion of the course, the student will be able to
- understand fundamentals of cloud computing architectures based on current standards, protocols, and best practices intended for delivering Cloud based enterprise IT services and business applications.
- Identify the known threats, risks, vulnerabilities and privacy issues associated with Cloud and evolve appropriate safeguards and countermeasures
- Design Cloud security architectures that assures secure isolation of compute, network and storage infrastructures, comprehensive data protection, end-to-end identity and access management, monitoring and auditing processes and compliance with industry and regulatory mandates.
- Cloud computing security guidelines set forth by ISO, NIST, ENISA and Cloud Security Alliance (CSA)
- Prepares for Cloud Security - CBK Certifications from Cloud Security Alliance (CSA) and Policies.

19ECS768: SECURITY ASSESSMENT AND RISK ANALYSIS

L	T	P	C
2	0	2	3

The course is designed to enable the student achieve the analytical tools to understand and analyze complex risk and security issues and developments, as well as the ability to plan and implement strategic processes in organizations and companies. The purpose of the course is to train students through critical reflection and professional insights, to identify opportunities for change in the complex and risky environments in which they operate and to put these reflections into action.

Course Objectives:

- Student will acquire theoretical and empirical knowledge about security policy, risk analysis and organizations in a changing world. Enable the student to perform vulnerability analysis.
- Student will acquire skills to analyze complex risk and security issues and developments, as well as the ability to plan and implement strategic processes in organizations and private companies.
- Students will acquire competences to translate knowledge about the political field of risk and security into risk analysis and strategies and to identify socially, politically and economically sustainable solutions and opportunities for public organizations and private companies.

Unit I   9L

Security Basics: Information Security (INFOSEC) Overview: critical information characteristics – availability information states – processing security countermeasures education, training and awareness, critical information characteristics – confidentiality critical information characteristics – integrity, information states – storage, information states – transmission, security counter measures policy, procedures and practices, threats, vulnerabilities.

Learning Outcomes:
After completion of this unit the student will be able to
- Describe the critical information characteristics (L1)
- Understand the security counter measures(L1)
- Identify the threats and vulnerabilities (L1)
- Explain Confidentiality, Integrity and Availability(L2)

Unit II   9L

Threats to and Vulnerabilities of Systems: definition of terms (e.g., threats, vulnerabilities, risk), major categories of threats (e.g., fraud, Hostile Intelligence Service (HOIS), malicious logic, hackers, environmental and technological hazards, disgruntled employees, careless employees, HUMINT, and monitoring), threat impact areas, Countermeasures: assessments (e.g., surveys, inspections), Concepts of Risk Management: consequences (e.g., corrective action, risk assessment), cost/benefit analysis of controls, implementation of cost effective controls, monitoring the efficiency and effectiveness of controls (e.g., unauthorized or inadvertent disclosure of information), threat and vulnerability assessment).

Learning Outcomes:

After completion of this unit, the student will be able to
- understand major categories of threats. (L1)
- identify threat impact areas(L2).
- implement cost effective controls, monitoring the efficiency and effectiveness of controls (L3).

Unit III   9L

Security Planning: Directives and procedures for policy mechanism, Risk Management: acceptance of risk (accreditation), corrective actions information identification, risk analysis and/or vulnerability assessment components, risk analysis results evaluation, roles and responsibilities of all the players in the risk analysis process, Contingency Planning/Disaster Recovery: agency response procedures and continuity of operations, contingency plan components, determination of backup requirements, development of plans for recovery actions after a disruptive event, development of procedures for offsite processing, emergency destruction procedures, guidelines for determining critical and essential workload, team member responsibilities in responding to an emergency situation.

Learning Outcomes:
After completion of this unit, the student will be able to
- explain directives and procedures for policy mechanism (L4).
- understand the procedures for offsite processing, emergency destruction (L1).
- explain roles and responsibilities of all the players in the risk analysis process (L4).

Unit IV   **9L**

POLICIES AND PROCEDURES: Physical Security Measures: alarms, building construction, cabling, communications center, environmental controls (humidity and air conditioning), filtered power, physical access control systems (key cards, locks and alarms), Personnel Security Practices and Procedures: access authorization/verification (need to know), contractors, employee clearances, position sensitivity, security training and awareness, systems maintenance personnel, Administrative Security Procedural Controls: attribution, copyright protection and licensing , Auditing and Monitoring: conducting security reviews, effectiveness of security programs, investigation of security breaches, privacy review of accountability controls, review of audit trails and logs

Learning Outcomes:
After completion of this unit, the student will be able to
- understand physical security measures (L1)
- employ personnel security practices and procedures(L3)
- explain administrative security procedural controls (L3)

Unit V   **6L**
Operations Security (OPSEC): OPSEC surveys/OPSEC planning INFOSEC: computer security – audit, cryptography encryption (e.g., point to point, network, link), cryptography key management (to include electronic key), cryptography strength (e.g., complexity, secrecy, characteristics of the key) Case study of threat and vulnerability assessment.
Learning Outcomes:
After completion of this unit, the student will be able to
- understand OPSEC surveys and OPSEC planning (L1)
- explain cryptographic encryption and key management (L3)
- outline cryptography strength (L3)

Text Book(s)
1. Whitman&Mattord, Principles of Incident Response and Disaster Recovery, Course Technology ISBN:141883663X
2. http://www.cnss.gov/Assets/pdf/nstissi_4011.pdf(Web Link)

Course Outcomes
After completion of course, students would be able to:
- understand the security counter measures(L1)
- implement cost effective controls, monitoring the efficiency and effectiveness of controls (L3).
- employ personnel security practices and procedures(L3).

19ECS784:MOBILE APPLICATION SECURITY

L T P C
2 0 2 3

This course provides an overall idea of defensive security mechanisms in mobile applications. Along with defensive techniques it also provides the offensive methods for the exploit the mobile application. It provides the techniques for mobile operating systems like iOS, Android, and Windows Mobile OS

Course Objectives:
- Learn the evolution of mobile application and its security.
- Understand IOS Applications and its security
- Familiarize android applications and its security.
- Analyze the mobile application security in windows mobile OS,IOS and Android.

Unit I   7L
Mobile Application security: Introduction to mobile application in security, The evolution of mobile applications, Mobile application security,
Analyzing IOS Applications: security Model, Understanding IOS Applications, Jail Breaking, data protection API, IOS Key chain, Touch ID, Reverse Engineering IOS binaries.
Learning Outcomes
After completion of this unit the student will be able to
- understand mobile application security (L1)
- Analysing IOS application (L3)

Unit II   9L
Attacking IOS Applications: Introduction to transport security, identifying insecure storage, Patching IOS Applications with HOPPER, Attacking IOS Runtime, inter process communication, Attacking using injection
IOS Applications Security: IOS implementation Insecurities, Disclosing Personally Identifiable Information, Data Leaks, Memory Corruption, Protecting Data, Avoiding Injection Vulnerabilities, Securing Your Application with binary protections
Learning Outcomes
After completion of this unit the student will be able to
- Practice attacking the IOS Applications. (L3)
- Explain IOS application security techniques(L4)

Unit III   8L
Analyzing Android Applications: Creating Android Environment. Understanding Android Applications, Understanding Security Model, Reverse-Engineering Applications.
Attacking Android Applications
Exposing Security Model Quirks, Attacking Application Components, accessing storage and logging, Misusing Insecure Communications, Exploiting other vectors, Additional testing techniques.
Learning Outcomes
After completion of this unit the student will be able to
- Analyse android applications (L3)
- implement techniques to attack android applications (L6)

Unit IV   8L
Android Applications security: Reviewing pre-installed Applications, Exploiting Devices, infiltrating user data, Principle of least exposure, Essential Security Mechanisms, Advanced Security

Mechanisms, Slowing down a reverse engineer.
Learning Outcomes
After completion of this unit the student will be able to
- understand android application security (L1)
- analyse android application security (L4)

Unit V   **10L**
Analyzing windows Phone Applications: Understanding Security Model, Understanding Windows Phone 8.x Applications, Analyzing application Binaries.
Cross platform Applications: Introduction. Bridging Native Functionality, Exploring Phone Gap and Apache Cordova
Learning Outcomes
After completion of this unit the student will be able to
- analyse windows phone applications (L4)
- learn various cross platform application (L6)

Text Book

1. Dominic Chell, Tyrone Erasmus, The Mobile Application Hacker's Handbook, Wiley Publication ,1e

Course Outcomes:
After completion of this course, the student will be able to
- Understand evolution of mobile applications and its security. (L2)
- analyse IOS, Android and Windows mobile applications. (L3)
- Implement security methodologies in IOS, Android and Windows mobile applications. (L6)
- Understand various cross platform mobile applications (L3)

19ECS772: DATA SECURITY AND ACCESS CONTROL

```
            L  T  P  C
            2  0  2  3
```

The course provides fundamentals of data security and various access control techniques mechanisms that are introduced along with application areas of access control techniques. It also contains an RBAC and smart card technology that has great deal of attention for commercial and real time applications.

Course Objectives

- To narrate and evaluate the design principles of conventional discretionary and mandatory security techniques.
- To learn Different RBAC frameworks for modelling a secure system
- To know methods for assigning access to information in a company based on the individual's need for the information,
- To specify security administrator and enforce security policies that map naturally to the organization's structure.
- To utilize a technology that decreases the cost of network administration while improving the enforcement of network security policies.
- To understand reliable and quality data transmission using smart cards.

Unit I   5L

Introduction to Access Control, Purpose and fundamentals of access control, brief history.
Policies of Access Control, Models of Access Control, and Mechanisms, Discretionary Access Control(DAC), Non- Discretionary Access Control, Mandatory Access Control (MAC). Capabilities and Limitations of Access Control Mechanisms: Access Control List (ACL) and Limitations, Capability List and Limitations.

Learning Outcomes
After completion of this unit the student will be able to
- list the origins, history, and central concepts of access control (L1)
- review the technical realization and security of data (L2)
- compare principles of conventional discretionary and mandatory security techniques. (L2)
- identify access control policies, access control models, and access control mechanisms. (L1)

Unit II   8L

Role-Based Access Control (RBAC) and Limitations, Core RBAC, Hierarchical RBAC, Statically Constrained RBAC, Dynamically Constrained RBAC, Limitations of RBAC. Comparing RBAC to DAC and MAC Access control policy.

Learning Outcomes
After completion of this unit the student will be able to
- review popular forms of access controls in use today (L2)
- interpret the basic concepts of RBAC and its advantages for system, application, and network security(L3)
- compare security levels of different RBAC models. (L2)
- incorporate roles to users using RBAC(L6)

Unit III   8L

Biba's intrigity model, Clark-Wilson model, Domain type enforcement model, mapping the enterprise view to the system view, Role hierarchies- inheritance schemes, hierarchy structures and inheritance forms, using SoD in real system, Temporal Constraints in RBAC, MAC and DAC.

Integrating RBAC with enterprise IT infrastructures: RBAC for WFMSs, RBAC for UNIX and JAVA environments Case study: Multi-line Insurance Company.

Learning Outcomes

After completion of this unit the student will be able to

- describe the similarities and differences between roles and groups(L1)
- develop access control mechanisms and models (L3)
- illustrate the research concepts and associated prototypes that have been developed to integrate RBAC model concepts into existing enterprise IT infrastructures. (L3)
- trace the integration of the RBAC model into the Web applications (L2)

Unit IV 9L

Smart Card based Information Security, Smart card operating system-fundamentals, design and implantation principles, memory organization, smart card files, file management, atomic operation, smart card data transmission ATR, PPS Security techniques- user identification, smart card security, quality assurance and testing, smart card life cycle-5 phases, smart card terminals.

Learning Outcomes

After completion of this unit the student will be able to

- identify smart card applications like identification, financial, mobile phones (SIM), public transit, computer security, schools, and healthcare(L1)
- explain how Smart cards provide computing, portability and secure storage of data and value. (L4)
- understand the integration of smart cards into system to introduce security. (L2)
- construct preset permissions set by the card issuer. (L3)

Unit V 12L

Recent trends in Database security and access control mechanisms. Case study of Role-Based Access Control (RBAC) systems, Recent Trends related to data security management, vulnerabilities in different DBMS.

Learning Outcomes

After completion of this unit the student will be able to

- record the experience of a real company in its transition from conventional access control methods to RBAC. (L1)
- develop prototypes to integrate the RBAC model into the various enterprise technologies. (L3)
- evaluate the benefits and costs of RBAC from the vantage point of a software end user. (L5)
- report insights related to delegated administration and other functionalities afforded RBAC users. (L2)

Text Book(s):
1. David F. Ferraiolo, D. Richard Kuhn, Ramaswamy Chandramouli, Role Based Access Control, Artech House, 2003.
2. http://www.smartcard.co.uk/tutorials/sct-itsc.pdf : Smart Card Tutorial.

Course Outcomes:

After completion of course, students would be able to:

- understand and implement classical models. (L2)

- analyse the data, identify the problems, and choose the relevant models (L4)
- assess the strengths and weaknesses of various access control models and to analyse their behaviour. (L5)
- assign security levels are assigned to users, with subjects acting on behalf of users and objects. (L3)
- Use of a common mechanism for a wide variety of purposes. (L3)

19ECS785: BLOCK CHAIN TECHNOLOGY

	L	T	P	C
	2	0	2	3

To really be aware of what is special about Bitcoin, we need to understand how it works at a technical level. Bitcoin truly is a new technology and we can only get so far by explaining it through simple analogies to past technologies. Cryptography is a deep academic research field utilizing many advanced mathematical techniques that are notoriously subtle and complicated to understand. Fortunately, Bitcoin only relies on a handful of relatively simple and well-known cryptographic constructions. Here specifically we will study cryptographic hashes and digital signatures, two primitives that prove to be very useful for building cryptocurrencies and Bitcoin mining Strategies.

Course Objectives

- Gain knowledge on Block Chain Fundamentals and Working Principle
- Understand the basic concept of Cryptographic Hash Functions, Hash Pointers
- Learn Elliptic Curve Digital Signature Algorithm.
- Get an insight into the working of the Bitcoin network, wallet, Bitcoin mining and distributed consensus for reliability.
- Gain knowledge about Bitcoin storage, Transaction and Usage
- Be familiar with Bitcoin Mining Hardware, Pools, strategies and basics of Anonymity.

UNIT I   **8 L**

Block Chain Fundamentals: Tracing Blockchain's Origin, Revolutionizing the Traditional Business Network, How Blockchain Works, What Makes a Blockchain Suitable for Business?
Introduction to Cryptography: Cryptographic Hash Functions, SHA256, Hash Pointers and Data Structures, Merkle tree.
Learning Outcomes:
After completion of this unit, the student will be able to
- Learn Block chain Fundamentals and Working Principle.
- Apply Cryptographic Hash Functions.
- Implement Merkle Tree

UNIT II   **8 L**

Digital Signatures: Elliptic Curve Digital Signature Algorithm (ECDSA), Public Keys as Identities, A Simple Crypto currency.
Learning Outcomes:
After completion of this unit, the student will be able to
- Implement Elliptic Curve Digital Signature Algorithm.
- Learn Simple Crypto currency like Goofy Coin, Scrooge Coin.

UNIT III   **10 L**

Centralization vs. Decentralization, Distributed Consensus, Consensus without identity using a block chain, Incentives and proof of work.
Mechanics of Bitcoin: Bitcoin transactions, Bitcoin Scripts, Applications of Bitcoin scripts, Bitcoin blocks, The Bitcoin network.
Learning Outcomes:
After completion of this unit, the student will be able to
- Work on Bitcoin network, wallet
- Learn Bitcoin mining and distributed consensus for reliability
- Use Bitcoin Transaction and applications

UNIT IV   **8 L**

Storage of and Usage of Bitcoins: Simple Local Storage, Hot and Cold Storage, Splitting and Sharing Keys, Online Wallets and Exchanges, Payment Services, Transaction Fees, Currency Exchange Markets.

Learning Outcomes:

After completion of this unit, the student will be able to

- Learn Types of Bitcoin Storage
- Use Bitcoin Payment Services and Currency Exchange Markets.
- Able to do mining job in Bitcoin transaction.

UNIT V   **8 L**

Bitcoin Mining: The Task of Bitcoin miners, Mining Hardware, Mining pools, Mining incentives and strategies.

Bitcoin and Anonymity: Anonymity Basics, Mixing, Zerocoin and Zerocash

Learning Outcomes:

After completion of this unit, the student will be able to

- Learn Mining Hardware and Pools
- Design Bitcoin Mining strategies

Text Book(s):

1. Manav Gupta, BlockChain for dummies, 2nd IBM Limited Edition, Published by John Wiley & Sons, Inc, 2018.
2. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, Bitcoin and Cryptocurrency Technologies, 2016.
3. Melanie Swan ,Blockchain: Blueprint for a New Economy, O'Reilly Media, 1/e, 2015.
4. Andreas M. Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain, O'Reilly Media, 2/e, 2017.

Course Outcomes:

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

- learn Block chain Fundamentals and Working Principle.
- apply Cryptographic Hash Functions, Hash Pointers.
- implement Elliptic Curve Digital Signature Algorithm.
- work on Bitcoin network, wallet, Bitcoin mining and distributed consensus for reliability.
- use Bitcoin Transaction, Payment Services and Exchange Market Services.
- design Bitcoin Mining Hardware, Pools and strategies.

19EAC741: ENGLISH FOR RESEARCH PAPER WRITING

	L	T	P	C
	2	0	0	0

This course introduces the student, to the different aspects of research paper writing including planning, preparation, layout, literature review write-up etc. Specifically, the perspective and style of writing in different sections of a research paper is highlighted. Students will be exposed to English language skills relevant to research paper writing.

Course Objectives:
- To write clearly, concisely and carefully by keeping the structure of the paper in mind.
- To use standard phrases in English and further improve his command over it.
- To write with no redundancy, no ambiguity and increase the readability of the paper.
- To plan and organize his paper by following a logical buildup towards a proper conclusion.
- To decide what to include in various parts of the paper.
- To write a suitable title and an abstract in order to attract the attention of the reader.
- To identify the correct style and correct tense.
- To retain the scientific value of the paper by using minimum number of words.

Unit I   5L
Planning and Preparation, Word Order, breaking up long sentences, Structuring Paragraphs and Sentences, Being Concise and Removing Redundancy, Avoiding Ambiguity and Vagueness.

Learning Outcomes:
After the completion of this unit, the student will be able to
- To know the expectations of various journals and referees (L2)
- To know the typical structure of a paper (L3)
- Learn to put words in a sentence in the correct order (L4)
- To write short and clear sentences from the very beginning of the paper (L4)
- To increase the readability of the paper by making it easy to read and 100% clear (L4)
- Learn to be concise without losing any important content (L4)
- To avoid some typical grammar mistakes made in research papers (L4)

Unit II   5L
Clarifying Who Did What, Highlighting Your Findings, Hedging and Criticizing, Paraphrasing and Plagiarism, Sections of a Paper, Abstracts, Introduction.

Learning Outcomes:
After the completion of this unit, the student will be able to
- Learn to make useful contribution worth recommending for publication (L4)
- Learn good use of language to make readers notice the key findings (L4)
- Learn to anticipate or predict possible objections to the claims made in the paper(L5)
- To understand what is plagiarism, and how to paraphrase other people's work (L4)
- Learn to attract the right kind of readers with a suitable title(L3)
- Learn to sell the abstract to potential readers by attracting their curiosity (L2)

Unit III   **6L**

Review of the Literature, Methods, Results, Discussion, Conclusions, The Final Check. key skills are needed when writing a Title, key skills are needed when writing an Abstract, key skills are needed when writing an Introduction, skills needed when writing a Review of the Literature.

Learning Outcomes:

After the completion of this unit, the student will be able to

- have a deep knowledge about everything that has been previously written on the topic and decide   what is important to know in Introduction. (L3)
- Learn to provide the right amount of literature regarding the sequence of events leading up to the current situation in the Literature review(L4)

Unit IV   **6L**

Writing Skills: skills are needed when writing the Methods, skills needed when writing the Results, skills are needed when writing the Discussion, skills are needed when writing the Conclusions.

Learning Outcomes:

After the completion of this unit, the student will be able to

- Learn to describe the materials used in experiments and/or the methods used to carry out the research (L2)
- The key skill is in reporting the results simply and clearly (L3)
- Learn to structure the Discussion and satisfy the typical requirements of the referees (L4)
- Learn to provide a clear and high-impact take-home message in the conclusion (L5)

Unit V   **6L**

Good Paper Writing: Useful phrases, how to ensure paper is as good as it could possibly be the first- time submission.

Learning Outcomes:

After the completion of this unit, the student will be able to

- Learn various lists of frequently used phrases that have a general acceptance in all disciplines and use in specific sections of the paper (L3)
- Learn various kinds of things one should look for when doing the final check (L3)

Text Book(s**):**
1. Goldbort R, Writing for Science, Yale University Press, 2006
2. Day R, How to Write and Publish a Scientific Paper, Cambridge University Press, 2006
3. Highman N, Handbook of Writing for the Mathematical Sciences, SIAM, Highman, 1998.

References:
1. Adrian Wallwork, English for Writing Research Papers, Springer New York Dordrecht Heidelberg London, 2011.

Course Outcomes:

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

- Frame the structure of the paper precisely. (L2).
- Improve his command over English by using standard phrases. (L3).
- Avoid repetition and mistakes in the paper and increase its readability. (L3).
- Organize the paper logically towards a proper conclusion. (L4).
- Decide on the content to be included in various parts of the paper. (L5).
- Identify whether to use personal or impersonal style in the paper. (L5).
- Express the content in a clear and concise way. (L6).
- Attract the attention of the reader by providing a suitable title and an appropriate abstract. (L6).

19EAC742: DISASTER MANAGEMENT

L T P C
2 0 0 0

This course is intended to provide fundamental understanding of different aspects of Disaster Management. It will expose the students to the concept and functions of Disaster Management and to build competencies of Disaster Management professionals and development practitioners for effective supporting environment as put by the government in legislative manner. It would also provide basic knowledge, skills pertaining to Planning, Organizing and Decision-making process for Disaster Risk Reduction.

Course Objectives
- to provide students an exposure to disasters, their significance, types & Comprehensive understanding on the concurrence of Disasters and its management.
- to ensure that students begin to understand the relationship between vulnerability, disasters, disaster prevention, risk reduction and the basic understanding of the research methodology for risk reduction measures.
- equipped with knowledge, concepts, and principles, skills pertaining to Planning, Organizing, Decision-making and Problem solving methods for Disaster Management.
- to develop rudimentary ability to respond to their surroundings with potential disaster response in areas where they live, with due sensitivity.

Unit I   5L
Introduction Disaster: Definition, Factors and Significance; Difference Between Hazard and Disaster; Natural and Manmade Disasters: Difference, Nature, Types and Magnitude.
Learning Outcomes
After the completion of this unit, the student will be able to
- define the meaning, list the factors and mention the significance of disaster (L1)
- distinguish between hazard and disaster (L3)
- compare manmade and natural disaster (L3)
- list the types of disaster and describe their magnitude (L2)

Unit II   5L
Repercussions of Disasters and Hazards: Economic Damage, Loss of Human and Animal Life, Destruction of Ecosystem. Natural Disasters: Earthquakes, Volcanisms, Cyclones, Tsunamis, Floods, Droughts and Famines, Landslides and Avalanches, Man-made disaster: Nuclear Reactor Meltdown, Industrial Accidents, Oil Slicks and Spills, Outbreaks of Disease and Epidemics, War and Conflicts.
Learning Outcomes
After the completion of this unit, the student will be able to
- list the different repercussions of disasters and hazards(L1)
- describe the characteristics of natural disasters and the magnitude of their losses(L2)
- describe the characteristics of man-made disasters and the magnitude of their losses(L2)
- elaborate the outbreaks of diseases and epidemics after disasters (L3)

Unit III   **6L**
Disaster Prone Areas in India Study of Seismic Zones; Areas Prone to Floods and Droughts, Landslides and Avalanches; Areas Prone to Cyclonic and Coastal Hazards with Special Reference to Tsunami; Post-Disaster Diseases and Epidemics.
Learning Outcomes
After the completion of this unit, the student will be able to
* describe the seismic zones and their characteristics(L2)
* identify the areas prone to floods and droughts(L1)
* distinguish between landslides and avalanches(L3)
* identify areas prone to cyclonic and costal hazards(L4)
* enumerate the post disaster diseases and epidemics(L2)

Unit IV   **6L**
Disaster Preparedness and Management Preparedness: Monitoring of Phenomena Triggering a Disaster or Hazard; Evaluation of Risk: Application of Remote Sensing, Data from Meteorological and Other Agencies, media reports: governmental and Community Preparedness.
Learning Outcomes
After the completion of this unit, the student will be able to
* describe the monitoring of phenomena triggering a disaster/hazard(L2)
* evaluate the risk with the use of remote sensing and meteorological data(L5)
* list the governmental and community measures for disaster preparedness(L2)

Unit V   **6L**
Risk Assessment Disaster Risk: Concept and Elements, Disaster Risk Reduction, Global and National Disaster Risk Situation. Techniques of Risk Assessment, Global Co-Operation in Risk Assessment and Warning, People's Participation in Risk Assessment. Strategies for Survival.
Learning Outcomes
After the completion of this unit, the student will be able to
* define and list the elements of disaster risk(L1)
* enumerate the measures for risk reduction(L2)
* apply the techniques of risk assessment (L4)
* identify the means of people's participation in risk assessment(L2)

Text Book(s):

1.   R. Nishith, Singh A.K., Disaster Management in India: Perspectives, issues and strategies, New Royal Book Company., 2008.
2.   Sahni, Pardeep, Disaster Mitigation Experiences and Reflections, Prentice Hall of India, New Delhi., 2012
3.   Goel S. L., Disaster Administration and Management Text and Case Studies", Deep and Deep Publication, 2007.

Course Outcomes

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

- Identify management activities in pre, during and post phases of Disasters. (L1)
- Plan disaster management activities and specify measure for risk reduction(L4)
- apply risk assessment techniques in real life disaster scenarios(L4)

19EAC744: VALUE EDUCATION

	L	T	P	C
	2	0	0	0

This course is intended to expose the student to the need for human values and methods to cultivate them for leading an ethical life with good moral conduct. Students taking this course will be able to experience a change in personal and professional behavior with these ethical principles guiding him throughout life

Course Objectives
- to expose the student to need for values, ethics, self-development and standards
- to make the student understand the meaning of different values including duty, devotion, self-reliance etc.
- to imbibe the different behavioral competencies in students for leading an ethical and happy life
- to expose the student to different characteristic attributes and competencies for leading a successful, ethical and happy profession life.

Unit I   7L
Values and self-development –social values and individual attitudes. Work ethics, Indian vision of humanism. Moral and non- moral valuation. Standards and principles. Value judgements
Learning Outcomes
After the completion of this unit, the student will be able to
- define the social values and individual attitudes for self development(L1)
- describe the Indian vision of humanism(L2)
- distinguish between moral and non-moral acts(L3)
- list the standards and value principles for moral conduct (L2)

Unit II   7L
Importance of cultivation of values. Sense of duty. Devotion, self-reliance. Confidence, concentration. Truthfulness, cleanliness. Honesty, humanity. Power of faith, national unity. Patriotism, love for nature, discipline.
Learning Outcomes
After the completion of this unit, the student will be able to
- describe the importance of cultivating values(L2)
- list the different traits of self-developed individual(L1)
- explain the need for loving nature/country/humanity(L2)

Unit III   7L
Personality and Behaviour Development - Soul and Scientific attitude. Positive Thinking. Integrity and discipline. Punctuality, Love and Kindness. Avoid fault Thinking. Free from anger, Dignity of labour. Universal brotherhood and religious tolerance. True friendship. Happiness Vs suffering, love for truth. Aware of self-destructive habits. Association and Cooperation. Doing best for saving nature.
Learning Outcomes
After the completion of this unit, the student will be able to
- describe the benefits of positivie thinking, integrity and discipline(L2)
- list the different methods for avoiding fault finding, anger(L1)
- explain the methods to overcome suffering, religious intolerance, self-destructive habits(L2)

Unit IV   7L

Character and Competence –Holy books vs Blind faith. Self-management and Good health. Science of reincarnation. Equality, Nonviolence, Humility, Role of Women. All religions and same message. Mind your Mind, Self-control. Honesty, Studying effectively.

Learning Outcomes

After the completion of this unit, the student will be able to

- describe the science of reincarnation(L2)
- explain the relation between self-management and good health(L1)
- elaborate the role of different religions in reaching the common goal(L3)
- list the different techniques for mind-control to improve personality and studies(L1)

Text Book(s):

1. Chakroborty S.K., "Values and ethics for organizations: Theory and Practice", Oxford University Press, 1998.

Course Outcomes

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

- describe the need for human values and methods for self development (L2)
- elaborate the different traits and benefits of a self-developed individual (L1)
- list the different attributes of self-developed individual (L1)
- elaborate the role and scope of books/faith/health/religions in character building and competence development(L3)

19EAC745: CONSTITUTION OF INDIA

L	**T**	**P**	**C**
2	**0**	**0**	**0**

This course is intended to expose the student to the philosophy of Indian constitution. Students will be able to understand their fundamental rights/duties and governance structure. Students also appreciate the role of election commission in establishing a democratic society.

Course Objectives
- to familiarize the student about the need for a constitution
- to make the student understand the role of constitution in a democratic society
- to acquaint the student with key constitutional features and fundamental rights of a citizen
- to impart the organs of governance and local administration hierarchy and their responsibilities
- to familiarize the student with the role, responsibilities and administration hierarchy of election commission

Unit I   5L
History of Making of the Indian Constitution: History Drafting Committee, (Composition & Working). **Philosophy of the Indian Constitution**: Preamble, Salient Features
Learning Outcomes
After the completion of this unit, the student will be able to
- list the outline of drafting committee and their roles in the making of Indian constitution (L1)
- describe the need and role of a constitution in a democratic society(L2)
- elaborate the salient features of Indian constitution(L3)

Unit II   5L
Contours of Constitutional Rights & Duties: Fundamental Rights, Right to Equality, Right to Freedom, Right against Exploitation, Right to Freedom of Religion, Cultural and Educational Rights, Right to Constitutional Remedies, Directive Principles of State Policy, Fundamental Duties.
Learning Outcomes
After the completion of this unit, the student will be able to
- list the fundamental rights of a citizen(L1)
- explain the intricacies in the different rights(L2)
- elaborate the fundamental duties of a citizen(L3)
- describe the principles of state policy(L2)

Unit III   6L
Organs of Governance: Parliament, Composition, Qualifications and Disqualifications, Powers and Functions, Executive, President, Governor, Council of Ministers, Judiciary, Appointment and Transfer of Judges, Qualifications, Powers and Functions
Learning Outcomes
After the completion of this unit, the student will be able to
- present the hierarchy of governance (L2)
- list the role/responsibilities/powers of different organs of governance(L1)
- elaborate the guidelines for appointment/transfer of judges(L2)

Unit IV   6L
Local Administration: District's Administration head: Role and Importance, Municipalities: Introduction, Mayor and role of Elected Representative, CEO of Municipal Corporation. Panchayat raj: Introduction, PRI: ZilaPachayat. Elected officials and their roles, CEO

ZilaPachayat: Position and role. Block level: Organizational Hierarchy (Different departments), Village level: Role of Elected and Appointed officials, Importance of grass root democracy.

Learning Outcomes

After the completion of this unit, the student will be able to

- describe the administrative organizational hierarchy of municipalities and panchayats(L2)
- appreciate the role/responsibilities/powers of mayor, CEO, elected officials(L3)
- appreciate the importance of grass root democracy(L3)

Unit V   **6L**

Election Commission: Election Commission: Role and Functioning. Chief Election Commissioner and Election Commissioners. State Election Commission: Role and Functioning. Institute and Bodies for the welfare of SC/ST/OBC and women.

Learning Outcomes

After the completion of this unit, the student will be able to

- describe the administrative hierarchy of election commission(L2)
- elaborate the roles/responsibilities/powers of election commissioners at different levels of hierarchy(L3)
- outline the welfare activities of SC/ST/OBC/Women by different bodies(L3)

Text Book(s):

1. The Constitution of India, 1950 (Bare Act), Government Publication.
2. S. N. Busi, Dr. B. R. Ambedkar, Framing of Indian Constitution, 1/e, 2015.
3. M. P. Jain, Indian Constitution Law, 7/e, Lexis Nexis, 2014.
4. D.D. Basu, Introduction to the Constitution of India, Lexis Nexis, 2015.

Course Outcomes

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

- describe the philosophy and salient features of Indian constitution(L2)
- list the constitutional rights and duties of a citizen(L1)
- elaborate the central and local administrative hierarchy and their roles(L2)
- describe the roles/responsibilities/powers of different governing and administrative bodies(L2)
- explain the structure/functioning and power of election commission(L2)

19EAC746: PEDAGOGY STUDIES

	L	T	P	C
	2	0	0	0

This course is aimed to familiarizing the student with pedagogical principles, practices and methodologies. This course is intended for students interested in pursuing a career in teaching and research.

Course Objectives
- to familiarize the student about the need for pedagogy studies, background and conceptual framework
- to expose the student to pedagogical practices in formal/informal classrooms
- to acquaint the student with type of curriculum and guidance materials for effective pedagogy
- to familiarize the student with classroom practices and curriculum assessment procedures
- to make the student understand the effect of undertaking research on teaching quality

Unit I   5L
Introduction and Methodology: Aims and rationale, Policy background, Conceptual framework and terminology, Theories of learning, Curriculum, Teacher education. Conceptual framework, Research questions. Overview of methodology and Searching.
Learning Outcomes
After the completion of this unit, the student will be able to
- define the aim and rationale behind teacher education(L1)
- classify the different theories of learning (L1)
- elaborate the need and role of curriculum, teacher education (L1)

Unit II   5L
Thematic overview: Pedagogical practices are being used by teachers in formal and informal classrooms in developing countries. Curriculum, Teacher education.
Learning Outcomes
After the completion of this unit, the student will be able to
- describe the different pedagogical practices used by teachers in formal and informal classrooms(L1)
- explain the pedagogical practices employed in developing countries (L1)
- enumerate the duties of faculty in terms of teaching, research, consultancy, administration (L1)

Unit III   6L
Evidence on the effectiveness of pedagogical practices, Methodology for the in depth stage: quality assessment of included studies. How can teacher education (curriculum and practicum) and the school curriculum and guidance materials best support effective pedagogy? Theory of change. Strength and nature of the body of evidence for effective pedagogical practices. Pedagogic theory and pedagogical approaches. Teachers' attitudes and beliefs and Pedagogic strategies.
Learning Outcomes
After the completion of this unit, the student will be able to
- list the measures for effective pedagogy(L1)
- identify the different documentation required to formalize curriculum implementation and quality assessment(L1)
- describe the teachers attitudes and beliefs in pedagogic strategies(L2)

Unit IV   **6L**

Professional development: alignment with classroom practices and follow-up support, Peer support, Support from the head teacher and the community. Curriculum and assessment, Barriers to learning: limited resources and large class sizes.

Learning Outcomes

After the completion of this unit, the student will be able to

- define the organizational hierarchy in a school administration system(L1)
- list the different barriers to learning(L3)
- enumerate the methods to overcome limited resources and handle large class sizes(L3)
- describe the follow-up support and peer-support in classroom practices(L2)

Unit V   **6L**

Research gaps and future directions: Research design, Contexts, Pedagogy, Teacher education, Curriculum and assessment, Dissemination and research impact.

Learning Outcomes

After the completion of this unit, the student will be able to

- explain the need for and role of research in teaching profession(L2)
- list the different research activities to be taken up by teachers(L1)
- describe the impact of research on teaching quality and learning process(L2)

Text Book(s):

1. Ackers J, Hardman F, Classroom interaction in Kenyan primary schools, Compare, 31 (2): 245-261, 2001
2. Agrawal M, Curricular reform in schools: The importance of evaluation, Journal of Curriculum Studies, 36 (3): 361-379, 2004.
3. Akyeampong K, Teacher training in Ghana - does it count? Multi-site teacher education research project (MUSTER) country report 1. London: DFID., 2003.
4. Akyeampong K, Lussier K, Pryor J, Westbrook J, Improving teaching and learning of basic maths and reading in Africa: Does teacher preparation count? International Journal Educational Development, 33 (3): 272–282., 2013.
5. Alexander RJ, Culture and pedagogy: International comparisons in primary education. Oxford and Boston: Blackwell., 2001.
6. Chavan M, Read India: A mass scale, rapid, 'Learning to Read' campaign., 2003.

Course Outcomes

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

- describe the theories of learning and conceptual framework of pedagogy(L2)
- explain the pedagogical practices used by teachers in formal and informal classrooms(L2)
- visualize the administrative hierarchy of schools and colleges and define the role(L3)
- appreciate the need for research and define the future direction of teaching career(L3)
- describe the impact of curriculum and assessment on the teaching learning process of a student(L3)

19EAC747: STRESS MANAGEMENT BY YOGA

L	**T**	**P**	**C**
2	**0**	**0**	**0**

This course is aimed to familiarize the student with basic principles of yoga and different physical/mental practices for managing mind and body. This course helps the student in managing stress during education, home and workplace. Further, principles learnt in this course help in building overall personality for a stress-free, happy and independent life.

Course Objectives
- to familiarize the student about eight parts of yoga and their significance
- to expose the student to the importance and meaning of Yam and Niyam
- to make the student understand the meaning and importance of yogic principles including Ahimsa, Satya, Astheyaetc
- to introduce the different yogic poses with a knowledge of their benefits for mind and body
- to familiarize the effect of different types of breathing techniques in concept and in activity

Unit I   **9L**
Definitions of Eight parts of yoga (Ashtanga).
Learning Outcomes
After the completion of this unit, the student will be able to
- list the eight parts of yoga (L1)
- describe the effects of different parts of yoga on mind and body(L2)
- elaborate the importance of yoga in stress management and personality development(L3)

Unit II   **9L**
Yam and Niyam.
Do`s and Don't's in life.
   i) Ahinsa, satya, astheya, bramhacharya and aparigraha
   ii) Shaucha, santosh, tapa, swadhyay, ishwarpranidhan.
Learning Outcomes
After the completion of this unit, the student will be able to
- elaborate the importance of Yam and Niyam(L2)
- describe the meaning and significance of Ahinsa, satya, astheyaetc(L2)
- explain the need for shaucha, santosh, tapa, swadhyay in leading a healthy and fruitful life(L3)

Unit III   **9L**
Asan and Pranayam
   i) Various yog poses and their benefits for mind & body
   ii) Regularization of breathing techniques and its Effects-Types of pranayam.
Learning Outcomes
After the completion of this unit, the student will be able to
- demonstrate the different physical asanas and explain their physical and phychological effects(L4)
- demonstrate the different breathing techniques and describe their physical and mental effects (L4)
- distinguish between different types of pranayamam(L5)

Text Book(s):
1. Janardan, Yogic Asanas for Group Tarining-Part-I, Swami Yogabhyasi Mandal, Nagpur
2. Swami Vivekananda, "Rajayoga or conquering the Internal Nature", Advaita Ashrama, Kolkata

Course Outcomes

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

- describe the eight parts of yoga and their significance(L1)
- explain the the importance and meaning of Yam and Niyam(L2)
- define the meaning and importance of yogic principles including Ahimsa, Satya, Astheyaetc(L1)
- demonstrate the different yogic poses and explain their benefits for mind and body(L4)
- demonstrate the different types of breathing techniques and explain their physical and mental benefits(L5)

19EAC748: PERSONALITY DEVELOPMENT THROUGH LIFE ENLIGHTENMENT SKILLS

	L	T	P	C
	2	0	0	0

This course is aimed to familiarize the student with life enlightenment skills for personality development. This course helps the student in building his holistic personality through human values, ethics and spiritual attributes.

Course Objectives
- to familiarize the student to good personality traits through moral stories
- to make the student understand the goal of human life and importance of good personality in reaching the goal
- to expose the student to the study of Shrimad-Bhagwad-Geeta for developing his/her personality and achieve the highest goal in life
- to familiarize the student to leadership skills for driving nation and mankind to peace and prosperity
- to expose the role of Neetishatakam for developing versatile personality of students.

Unit I   9L
Neetisatakam-Holistic development of personality
Verses- 19,20,21,22 (wisdom)
Verses- 29,31,32 (pride & heroism)
Verses- 26,28,63,65 (virtue)
Verses- 52,53,59 (dont's)
Verses- 71,73,75,78 (do's).
Learning Outcomes
After the completion of this unit, the student will be able to
- describe the moral stories illustrating the traits of good personality(L2)
- define the meaning and importance of wisdom, pride, heroism, virtue etc(L1)
- identify do and donts in life from the foundations of human morals/ethics(L5)

Unit II   9L
Approach to day to day work and duties.
Shrimad BhagwadGeeta: Chapter 2-Verses 41, 47,48,
Chapter 3-Verses 13, 21, 27, 35, Chapter 6-Verses 5,13,17, 23, 35,
Chapter 18-Verses 45, 46, 48.
Learning Outcomes
After the completion of this unit, the student will be able to
- describe the characteristics and principles of bhakti yogam, jnana yogam and karma yogam(L1)
- identify the use of different yogic characteristics in different activities of daily life/duties(L4)
- apply the use of yogic principles for leading a stress-free, happy and fruitful life with good developed personality(L4)

Unit III   **9L**

Statements of basic knowledge.
Shrimad BhagwadGeeta: Chapter2-Verses 56, 62, 68
Chapter 12 -Verses 13, 14, 15, 16,17, 18
Personality of Role model. Shrimad BhagwadGeeta:
Chapter2-Verses 17, Chapter 3-Verses 36,37,42,
Chapter 4-Verses 18, 38,39
Chapter18 – Verses 37,38,63

Learning Outcomes

After the completion of this unit, the student will be able to

- list the characteristics of role model proposed by verses of bhagavadgita(L1)
- explain the methods for obtaining life enlightenment through the practice of four yoga appropriately (L2)
- describe the characteristics of karma yogi/jnana yogi for developing leadership personality (L2)

Text Book(s):

1. Swami Swarupananda, "Srimad Bhagavad Gita", Advaita Ashram (Publication Department), Kolkata
2. P. Gopinath, Bhartrihari's Three Satakam (Niti-Sringar-vairagya), Rashtriya Sanskrit Sansthanam, New Delhi.

Course Outcomes

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

- List the different parables of neethisathakam and identify their morals(L1)
- enumerate the different traits of human personality for life enlightenment(L2)
- describe the leadership attributes for driving nation and mankind to peace and prosperity(L2)
- explain the applicability of different types of yoga to day-to-day work and duties resulting in responsible personality (L2)

19EAC750: DEVELOPING SOFT SKILLS AND PERSONALITY

	L	T	P	C
	3	0	0	0

Soft skills comprise pleasant and appealing personality traits as self-confidence, positive attitude, emotional intelligence, social grace, flexibility, friendliness and effective communication skills. The course aims to cause a basic awareness within the students about the significance of soft skills in professional and inter-personal communications and facilitate an all-round development of personality.

Course Objectives
- to familiarize the student to the criteria for self assessment and significance of self-discipline
- to expose the student to attitudes, mindsets, values and beliefs
- to acquaint the student to plan career and goals through constructive thinking
- to enable the student to overcome barriers for active listening and persuasive speaking
- to familiarize the skill of conducting meetings, writing minutes and involving in active group discussions

Unit I   **8L**
Self-Assessment; Identifying Strength & Limitations; Habits, Will-Power and Drives; Developing Self-Esteem and Building Self-Confidence, Significance of Self-Discipline
Learning Outcomes
After the completion of this unit, the student will be able to
- identify strengths & limitations through self-assessment(L3)
- list the attributes of personalities will good will-power and self-drives(L1)
- describe the reasons for building self-esteem and self-confidence(L2)
- explain the significance of self discipline(L2)

Unit II   **8L**
Understanding Perceptions, Attitudes, and Personality Types: Mind-Set: Growth and Fixed; Values and Beliefs
Learning Outcomes
After the completion of this unit, the student will be able to
- define the characteristics of different perceptions, attitudes and personality types(L1)
- distinguish between fixed and growing mindsets(L3)
- define the importance and meaning of values and beliefs(L2)

Unit III   **8L**
Motivation and Achieving Excellence; Self-Actualisation Need; Goal Setting, Life and Career Planning; Constructive Thinking
Learning Outcomes
After the completion of this unit, the student will be able to
- describe the need for having high motivation and achieving excellence(L2)
- define the need for self-actualization(L1)
- plan the life and career goals based on self assessment(L4)
- explain the attributes of constructive thinking(L2)

Unit IV   **8L**
Communicating Clearly: Understanding and Overcoming barriers; Active Listening; Persuasive Speaking and Presentation Skills.
Learning Outcomes
After the completion of this unit, the student will be able to

- self-assess the barriers for communicating clearly (L4)
- list the attributes of active listening(L1)
- describe the minimal aspects of effective presentation(L2)
- organize ideas resulting a persuasive talk(L3)

Unit V   **8L**
Conducting Meetings, Writing Minutes, Sending Memos and Notices; Netiquette: Effective E-mail Communication; Telephone Etiquette; Body Language in Group Discussion and Interview.
Learning Outcomes
After the completion of this unit, the student will be able to
- describe the format and structure of writing meeting minutes(L2)
- identify the essential components of memos and notices(L3)
- explain the principles of effective email communication(L2)
- list the basic etiquette of telephone conversation(L1)
- describe the effective body traits during group discussion and interviews(L2)

Text Book(s):
1. Dorch, Patricia. What Are Soft Skills? New York: Execu Dress Publisher, 2013.
2. Kamin, Maxine. Soft Skills Revolution: A Guide for Connecting with Compassion for Trainers, Teams, and Leaders. Washington, DC: Pfeiffer & Company, 2013.
3. Klaus, Peggy, Jane Rohman& Molly Hamaker. The Hard Truth about Soft Skills. London: HarperCollins E-books, 2007.
4. Petes S. J., Francis. Soft Skills and Professional Communication. New Delhi: Tata McGraw-Hill Education, 2011.
5. Stein, Steven J. & Howard E. Book. The EQ Edge: Emotional Intelligence and Your Success. Canada: Wiley & Sons, 2006.

Course Outcomes
After successful completion of the course, the student will be able to
- carry out self assessment and describe the significance of self-discipline(L4)
- define, classify and compare attitudes, mindsets, values and beliefs(L3)
- plan career and goals through constructive thinking and personal assessment(L4)
- overcome barriers for active listening and persuasive speaking (L5)
- conduct meetings, write minutes and involve in active group discussions(L3)

19EOE742: BUSINESS ANALYTICS

	L	T	P	C
	3	0	0	3

This course introduces students to the science of business analytics. The goal is to provide students with the foundation needed to apply data analytics to real-world challenges they confront daily in their professional lives. Students will learn to identify the ideal analytic tool for their specific needs; understand valid and reliable ways to collect, analyze, and visualize data; and utilize data in decision making for managing agencies, organizations or clients in their workspace

Course Objectives
- To familiarize the scope, process and advantages of business analytics
- To acquaint the student with the modeling and problem solving skills in business analytics
- To impart the organization and management of business analytics
- To introduce the forecasting models and techniques used in analytics
- To expose the formulation and decision strategies used in business analytics

Unit I   8L
Business analytics: Overview of Business analytics, Scope of Business analytics, Business Analytics Process, Relationship of Business Analytics Process and organisation, competitive advantages of Business Analytics. Statistical Tools: Statistical Notation, Descriptive Statistical methods, Review of probability distribution and data modelling, sampling and estimation methods overview
Learning Outcomes
After the completion of this unit, the student will be able to
- define the scope and process of business analytics (L1)
- choose an organizational structure to implement a business analytics process (L4)
- describe the statistical tools and methods used for data modeling and analysis (L2)
- identify the sampling and estimation requirements for data analysis (L1)

Unit II   8L
Trendiness and Regression Analysis: Modeling Relationships and Trends in Data,simple Linear Regression. Important Resources, Business Analytics Personnel, Data and models for Business analytics, problem solving, Visualizing and Exploring Data, Business Analytics Technology.
Learning Outcomes
After the completion of this unit, the student will be able to
- identify the relationships and trends in data (L1)
- utilize linear regression methods for identifying data relationships (L4)
- list the types of data and their models used for business analytics (L1)
- describe the methods for visualization and exploration of data (L2)

Unit III   8L
Organization Structures of Business analytics: Team management, Management Issues, Designing Information Policy, Outsourcing, Ensuring Data Quality, measuring contribution of Business analytics, Managing Changes. Descriptive Analytics, predictive analytics, predicative Modelling, Predictive analytics analysis, Data Mining, Data Mining Methodologies, Prescriptive analytics and its step in the business analytics Process, Prescriptive Modelling, nonlinear Optimization.
Learning Outcomes
After the completion of this unit, the student will be able to

- describe the management issues in the organization structures (L2)
- define the designing information policy and its usage (L1)
- list the methods for ensuring data quality measuring contribution (L1)
- explain the use of data mining methodologies for predictive analytics analysis (L3)
- describe the use of prescriptive analytics methods in business analytics process (L2)

Unit IV   **10L**
Forecasting Techniques: Qualitative and Judgmental Forecasting, Statistical Forecasting Models, Forecasting Models for Stationary Time Series, Forecasting Models for Time Series with a Linear Trend, Forecasting Time Series with Seasonality, Regression Forecasting with Casual Variables, Selecting Appropriate Forecasting Models. Monte Carlo Simulation and Risk Analysis: Monte Carle Simulation Using Analytic Solver Platform, New-Product Development Model, Newsvendor Model, Overbooking Model, Cash Budget Model.
Learning Outcomes
After the completion of this unit, the student will be able to
- classify and describe the use of forecasting models (L3)
- model the use of regression forecasting with casual variables (L5)
- identify the appropriate forecasting model for a given data (L5)
- explain the use of monte carlo simulation for forecasting and identify the involved risk (L2)

Unit V   **8L**
Decision Analysis: Formulating Decision Problems, Decision Strategies with the withoutOutcome Probabilities, Decision Trees, The Value of Information, Utility and Decision Making.
Learning Outcomes
After the completion of this unit, the student will be able to
- formulate decision problems (L2)
- list the decision strategies with and without probabilities (L1)
- use the decision trees for analysis (L4)
- describe the value of information, utility and its use in decision making (L4)

Text Book(s):
1. Marc J. Schniederjans, Dara G.Schniederjans, Christopher M. Starkey,Business analytics Principles, Concepts, and Applications Pearson FT Press, 2014.
2. James Evans, Business Analytics, Pearson Education, 2013.

Course Outcomes
Upon successful completion of the course, the student will be able to
- define thescope, process and advantages of business analytics (L1)
- explain the modeling and problem solving skills in business analytics (L2)
- describe the organization and management of business analytics (L3)
- utilize the forecasting models and techniques used in analytics (L4)
- enumerate and utilize the formulation and decision strategies (L2)

19EOE746: OPERATIONS RESEARCH

	L	T	P	C
	3	0	0	3

Optimization problems arise in all walks of human activity- particularly in engineering, business, finance and economics. The simplest optimization problems are linear in nature which may be subject to a set of linear constraints. This course will equip the student with the expertise to mathematically model real life optimization problems as Linear Programming (Optimization) Problems and subsequently educate the student to solve these models with the help of the available methods.

Course Objectives
- to impart knowledge on developing mathematical formulation for linear programming and transportation problem
- to familiarize the student in the construction of the required activities in an efficient manner to complete it on or before a specified time limit and at the minimum cost.
- to expose the development of mathematical model for interactive decision-making situations, where two or more competitors are involved under conditions of conflict and competition.
- to illustrate PERT and CPM techniques for planning and implementing projects.
- To impart the knowledge of formulating and analysis of real life problems using advanced tools and techniques for resource optimization
- to provide frameworks for analyzing waiting lines using advanced queuing theory concepts

Unit I   8L
Optimization Techniques, Model Formulation, models, General L.R Formulation, Simplex Techniques, Sensitivity Analysis, Inventory Control Models
Learning Outcomes
After completing this unit, the student will be able to
- identify and develop operational research models from the verbal description of the real system. **[L4]**
- understand the classification systems of effective Inventory control models**[L2]**

Unit II   8L
Formulation of a LPP - Graphical solution revised simplex method - duality theory - dual simplex method - sensitivity analysis - parametric programming
Learning Outcomes
After completing this unit, the student will be able to
- translate a real-world problem, given in words, into a mathematical formulation. **[L2]**
- utilize the mathematical tools that are needed to solve optimization problems. **[L2]**

Unit III   8L
Nonlinear programming problem - Kuhn-Tucker conditions min cost flow problem - max flow problem - CPM/PERT
Learning Outcomes
After completing this unit, the student will be able to
- describe the need and origin of the optimization methods**[L2]**
- classify optimization problems to suitably choose the method needed to solve the particular type of problem**[L3]**

Unit IV   8L

Scheduling and sequencing - single server and multiple server models - deterministic inventory models - Probabilistic inventory control models - Geometric Programming.

Learning Outcomes

After completing this unit, the student will be able to
- choose linear programming problems to suitably choose the method needed to solve the particular type of problem**[L1]**
- identify industrial problems involved in inventory, MRP and scheduling**[L2]**

Unit V   **8L**
Competitive Models, Single and Multi-channel Problems, Sequencing Models, Dynamic Programming, Flow in Networks, Elementary Graph Theory, Game Theory Simulation

Learning Outcomes
After completing this unit, the student will be able to
- identify the values, objectives, attributes, decisions, uncertainties, consequences, and trade-offs in a real decision problem**[L2]**
- Apply the models to incorporate rational decision-making process in real life situations.**[L3]**
- Analyze various modeling alternatives & select appropriate modeling techniques for a given situation.. **[L3]**

Text Book(s):
1. H.A. Taha, Operations Research, An Introduction, Prentice Hall of India, 2008
2. H.M. Wagner, Principles of Operations Research, Prentice Hall of India, Delhi, 1982.
3. J.C. Pant, Introduction to Optimization: Operations Research, Jain Brothers, 2008
4. Hitler Libermann Operations Research: McGraw Hill Publishers, 2009
5. Pannerselvam, Operations Research: Prentice Hall of India, 2010
6. Harvey M Wagner, Principles of Operations Research: Prentice Hall of India, 2010

Course Outcomes
After the successful completion of the course, the students will be able to:
- Understand the basic concepts of different advanced models of operations research and their applications. (L2)
- Solve linear programming problems using appropriate techniques and optimization solvers, interpret the results obtained and translate solutions into directives for action. (L4)
- Apply the models to incorporate rational decision-making process in real life situations. (L4)
- Analyze various modeling alternatives & select appropriate modeling techniques for a given situation. (L3)
- Validate output from model to check feasibility of implementations. (L5)
- Create innovative modeling frameworks for a given situation.(L6)
- Conduct and interpret post-optimal and sensitivity analysis and explain the primal-dual relationship.(L3)

19EOE748: COST MANAGEMENT OF ENGINEERING PROJECTS

L	T	P	C
3	0	0	3

This course will equip the student with the expertise to mathematically model engineering projects and use effective methods and techniques to plan and execute engineering activities.

Course Objectives
- to introduce the basic principles of strategic cost management and the related terminology
- to familiarize the project planning and execution process involving technical/nontechnical activities
- to acquaint the student with detailed engineering activities and their cost management analysis
- to impart the knowledge of cost analysis and profit planning of engineering projects
- to familiarize the quantitative techniques for optimization of budget allocation

Unit I   8L

Introduction and Overview of the Strategic Cost Management Process, Cost concepts in decision-making; Relevant cost, Differential cost, Incremental cost and Opportunity cost. Objectives of a Costing System; Inventory valuation; Creation of a Database for operational control; Provision of data for Decision-Making.

Learning Outcomes
After the completion of this unit, the student will be able to
- describe the cost concepts in decision making(L2)
- define the various costs involved in the cost management process(L2)
- list the objectives of cost control(L2)
- identify the different fields of a database for operational control(L2)

Unit II   8L

Project: meaning, Different types, why to manage, cost overruns centres, various stages of project execution: conception to commissioning. Project execution as conglomeration of technical and nontechnical activities.

Learning Outcomes
After the completion of this unit, the student will be able to
- define the meaning of a project and list the different types(L2)
- identify the measures to manage cost overruns(L2)
- describe the various stages of project execution from conception to commissioning(L2)
- plan the proper order of technical/nontechnical activities as part of project execution(L2)

Unit III   8L

Detailed Engineering activities. Pre project execution main clearances and documents Project team: Role of each member. Importance Project site: Data required with significance. Project contracts. Types and contents. Project execution Project cost control. Bar charts and Network diagram. Project commissioning: mechanical and process.

Learning Outcomes
After the completion of this unit, the student will be able to
- identify the different clearance norms required in the pre-project execution phase(L2)
- describe the hierarchy of project team and identify the role of each member(L2)
- list the different contents of project contracts(L2)
- present the project cost control and planning through bar charts, network diagrams etc(L2)

Unit IV   8L

Cost Behavior and Profit Planning Marginal Costing; Distinction between Marginal Costing andAbsorption Costing; Break-even Analysis, Cost-Volume-Profit Analysis. Various decision-making problems. Standard Costing and Variance Analysis. Pricing strategies: Pareto Analysis. Target costing, Life Cycle Costing. Costing of service sector. Just-in-time approach, Material Requirement Planning, Enterprise Resource Planning, Total Quality Management and Theory of constraints. Activity-Based Cost Management, Bench Marking; Balanced Score Card and Value-Chain Analysis.

Learning Outcomes

After the completion of this unit, the student will be able to

- describe the cost behavior and profit planning(L2)
- distinguish between marginal costing and absorption costing(L2)
- analyze the variance of standard costing(L2)
- analyze the pricing strategies in project costing(L2)
- identify the quality measures satisfying the appropriate constraints(L2)

Unit V   **10L**

Budgetary Control; Flexible Budgets; Performance budgets; Zero-based budgets. Measurement of Divisional profitability pricing decisions including transfer pricing. Quantitative techniques for cost management, Linear Programming, PERT/CPM, Transportation problems, Assignment problems, Simulation, Learning Curve Theory

Learning Outcomes

After the completion of this unit, the student will be able to

- define and compare the different budgeting strategies(L2)
- model the cost management as a linear programming problem(L2)
- measure the divisional profitability and decide the appropriate pricing(L2)

Text Book(s):

1. Charles T. Horngren, Srikant M. Datar, George Foster, Cost Accounting A Managerial Emphasis, Prentice Hall of India, New Delhi, 2006.

References:

1. Charles T. Horngren, George Foster, Advanced Management Accounting, Greenwood Publishing, 2001.
2. Robert S Kaplan, Anthony A. Alkinson, Management & Cost Accounting, 1998.
3. Ashish K. Bhattacharya, Principles & Practices of Cost Accounting, Wheeler Publisher, 2004.
4. N.D. Vohra, Quantitative Techniques in Management, Tata McGraw Hill Book, 2006.

Course Outcomes

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

- list the basic principles of strategic cost management and define the related terminology(L1)
- plan the project execution process involving technical/nontechnical activities(L4)
- describe the detailed engineering activities and their cost management analysis(L2)
- carry out the cost analysis and profit planning of engineering projects(L5)
- utilize quantitative techniques for optimization of budget allocation(L6)

19ECS891: PROJECT WORK I

L T P C
0 0 26 13

Each student is required to submit a report of first part of project work i.e. about the problem definition, literature review and methodology to be adopted including experiments and tests to be performed on topic of project as per the guidelines decided by the department. The project work is to be evaluated through Presentations and Viva-Voce during the semester end.

19ECS892: PROJECT WORK II

L T P C
0 0 26 13

Each student is required to submit a detailed project report about the work on topic of project as per the guidelines decided by the department. The project work is to be evaluated through Presentations and Viva-Voce during the semester and Final evaluation will be done at the end of semester as per the guidelines decided by the department from time to time. The candidate shall present/publish one paper in national/international conference/seminar/journal of repute. However candidate may visit research labs/institutions with the due permission of chairperson on recommendation of supervisor concerned.