UNIVERSITY SCHOOL

OF

INFORMATION AND COMMUNICATION TECHNOLOGY

Department Of Computer Science & Engineering

COURSE STRUCTURE

B. TECH
COMPUTER SCIENCE AND ENGINEERING
Specialization: Cyber Security

2022-2026

GAUTAM BUDDHA UNIVERSITY
GAUTAM BUDH NAGAR, GREATER NOIDA
UP (INDIA)

SEMESTER I

S.No	Course Code	Course Name	L-T-P	Credits
1	MA101	Engineering Mathematics-I	3-1-0	4
2	PH102	Engineering Physics	3-1-0	4
3	EE102	Basic Electrical Engineering	3-1-0	4
4	ME101	Engineering Mechanics	3-1-0	4
5	ES101	Environmental Studies	3-1-0	4
6	PH104	Engineering Physics Lab	0-0-2	1
7	EE104	Basic Electrical Engineering Lab	0-0-2	1
8	EN151	Language Lab	0-0-2	1
9	ME102	Workshop Practice	1-0-2	2
10	GP	General Proficiency	Non Credit	
Total Credits			**25**	
Total Contact Hours			**16-5-8=29**	

SEMESTER II

S.No	Course Code	Course Name	L-T-P	Credits
1	CS101	Fundamentals of Computer Programming	3-1-0	4
2	CC102	Introduction to Cyber Security	2-0-0	2
3	MA102	Engineering Mathematics-II	3-1-0	4
4	EC101	Basic Electronics Engineering	3-1-0	4
5	CS102	Computer Organization & Architecture	3-1-0	4
6	EN101	English Proficiency	2-0-0	2
7	CE103	Engineering Graphics	1-0-2	2
8	CS181	Computer Programming Lab	0-0-2	1
9	CC182	Cyber Security Lab	0-0-2	1
10	EC181	Basic Electronics Engineering Lab	0-0-2	1
11	GP	General Proficiency	Non Credit	
Total Credits			**25**	
Total Contact Hours			**17-4-8=29**	

SEMESTER III

Sr.No	Course Code	Courses	L-T-P	Credits
1	CC201	Internet Technology	3-0-0	3
2	CC203	Operating Systems	3-0-0	3
3	CC205	Data Structure & Algorithms	3-0-0	3
4	CC207	Introduction to Python	3-0-0	3
5	CC209	Information Retrieval Systems	3-0-0	3
6	MA201	Engineering Mathematics-III	3-1-0	4
7	CC281	Internet Technology Lab	0-0-3	2
8	CC283	Data Structure & Algorithms Lab	0-0-3	2
9	CC285	Python Programming Lab	0-0-3	2
10	GP	General Proficiency	Non Credit	
Total Credits			**25**	
Total Contact Hours			**18-1-9=28**	

SEMESTER IV

Sr.No	Course Code	Courses	L-T-P	Credits
1	CC202	Software Engineering	3-0-0	3
2	CC204	Database Management System	3-0-0	3
3	CC206	Java Programming	3-0-0	3
4	CC208	Artificial Intelligence	3-0-0	3
5	CC210	Information Theory & Coding	3-0-0	3
6	CC212	Theory of Automata	3-1-0	4
7	CC282	Database Management System Lab	0-0-3	2
8	CC284	Java Programming Lab	0-0-3	2
9	CC286	Information Theory & Coding Lab	0-0-3	2
10	GP	General Proficiency	Non Credit	
Total Credits			**25**	
Total Contact Hours			**18-1-9=28**	

SEMESTER V

Sr.No	Course Code	Courses	L-T-P	Credits
1	CC301	Compiler Design	3-1-0	4
2	CC303	Soft Computing Techniques	3-0-0	3
3	CC305	Analysis & Design of Algorithms	3-0-0	3
4	CC307	Cryptography & Data Privacy	3-0-0	3
5	CC309	Machine Learning	3-0-0	3
6		Elective I	3-0-0	3
7	CC381	Analysis& Design of Algorithms Lab	0-0-3	2
8	CC383	Cryptography & Data Privacy Lab	0-0-3	2
9	CC385	Machine Learning using Python Lab	0-0-3	2
10	GP	General Proficiency	Non Credit	
Total Credits				**25**
Total Contact Hours			**18-1-9=28**	

SEMESTER VI

Sr.No	Course Code	Courses	L-T-P	Credits
1	CC302	Web Development using PHP	3-0-0	3
2	CC304	Network Defense for Cyber Security	3-0-0	3
3	CC306	Risk Management and Audit	3-1-0	4
4	CC308	Digital Forensic, Audit &Investigations	3-0-0	3
5	CC310	Data Privacy and Database Security	3-0-0	3
6		Elective 2	3-0-0	3
7	CC382	Web Development using PHP Lab	0-0-3	2
8	CC384	Network Defense for Cyber Security Lab	0-0-3	2
9	CC386	Data Privacy and Database Security Lab	0-0-3	2
10	GP	General Proficiency	Non Credit	
Total Credits				**25**
Total Contact Hours			**18-1-9=28**	

- Industrial training will be done after the third year during the summer break and it will be of minimum 4 weeks. It will be evaluated at the end of VII Semester.

SEMESTERVII

Sr.No	Course Code	Courses	L-T-P	Credits
1	MA401	**Modeling & Simulation**	3-1-0	4
2	CC401	Blockchain Technology	3-0-0	3
2	CC403	AI Enabled Cyber Security	2-0-0	2
3		Elective3	3-0-0	3
5		Elective4	3-0-0	3
6	CC481	AI Enabled Cyber Security Lab	0-0-3	2
7	CC491	Minor Project	0-0-10	5
8	CS 493	Industrial Training	0-0-6	3
9	GP	General Proficiency	Non Credit	
Total Credits				**25**
Total Contact Hours			**14-1-19=34**	

SEMESTER VIII

Sr.No	Course Code	Courses	L-T-P	Credits
1	CC490	Seminar	0-0-3	2
2	CS492	Major Project	0-0-16	8
3	CS494	Internship	0-0-30	15
4	GP	General Proficiency	Non Credit	
Total Credits				**25**
Total Contact Hours			**0-0-49=35**	

GRAND TOTAL OF CREDITS = 200

- In the **Seminar**, students need to study and present individually, on the latest research paper of their specialized area and It will be evaluated as per University Examination Rules.
- The **Internship** in Industry will be done by candidates individually during the 8th semester and it will be for 4-6 months. It will be evaluated as per University Examination Rules.

Minor and Major Project will be in a group and It will be evaluated as per University Examination Rules. USICT will provide a mentor/supervisor for industrial training, seminar, internship, minor and major projects.

ELECTIVES

S.No.	Course Code	Course Name	L	T	P	Credits	Types
1	CC311	Security Information and Event Management	3	0	0	3	E1
2	CC313	Intrusion Detection and Prevention System	3	0	0	3	E1
3	CC315	Cryptography	3	0	0	3	E1
4	CC317	Biometric System and Security	3	0	0	3	E1
5	CC319	Ethical Hacking	3	0	0	3	E2
6	CC312	Mobile Security	3	0	0	3	E2
7	CC314	**Cloud Architecture and Security**	3	0	0	3	E2
8	CC316	**Principle of Secure Coding**	3	0	0	3	E2
9	CC318	Information Warfare	3	0	0	3	E2
10	CC320	Social Network Security	3	0	0	3	E3
11	CC405	Physical Security of IT Infrastructure	3	0	0	3	E3
12	CC407	NISTA 800-53 Security Control	3	0	0	3	E3
13	CC409	Operating System Security	3	0	0	3	E3
14	CC411	Mobile and Wireless Network Security	3	0	0	3	E3
15	CC413	Enterprise Security and Management	3	0	0	3	E3
16	CC415	Malware Analysis	3	0	0	3	E4
17	CC417	Android Security Design and Internals	3	0	0	3	E4
18	CC419	Data and Database Management Security	3	0	0	3	E4
19	CC421	Web application and Penetration Testing	3	0	0	3	E4
20	CC423	Access Control and Identity Management Systems	3	0	0	3	E4

SEMESTER-I

SEMESTER-II

FUNDAMENTALS OF COMPUTER PROGRAMMING			
Course Code:	**CS101**	**Course Credits:**	**4**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**1U**	**Course Semester (U / P):**	**2U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 01**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 15**	**End Sem. Exam Hours:**	**3**

COURSE OBJECTIVES
Students will be able to:
1. Provide students with understanding of programming essentials and to learn preprogramming steps like writing algorithms, drawing flowcharts and pseudo codes.
2.Understand the structure, and learn the syntax and semantics of C programming
3.Know the variable declaration with different data types and learn using operators and different control structures like decision control, loop control and special cases..
4. Recognize the concept of pointers, declarations, initialization, operations on pointers and their usage
5.Analyse how to perform various FILE I/O.

COURSE OUTCOMES
At the end of the course the students should be able to:
1.Able to implement the algorithms and draw flowcharts for solving Mathematical and Engineering problems.
2.Students can write, compile and debug programs in C language and use different data types for writing the programs
3.Able to design programs connecting decision structures, loops and functions..
4.Understand the dynamic behavior of memory by the use of pointers..
5.Develop confidence for self-education and ability for life-long learning needed for Computer language.

UNIT I INTRODUCTION TO COMPUTER AND PROGRAMMING CONCEPTS

Definition, characteristic, generation of computers, basic components of a computer system, memory, input, output and storage units, high level language and low level language, Soft- ware: system software, application software, hardware, firmware, Operating System, compil- er, interpreter and assembler, linker, loader, debugger, IDE. Introduction to algorithm and flow chart; representation of algorithm using flow chart symbol, pseudo code, basic algorithm de- sign, characteristics of good algorithm, development of algorithm.

UNIT II INTRODUCTION TO C PROGRAMMING LANGUAGE

Introduction to C programming language , Declaring variables, preprocessor statements, arithmetic operators, programming style, keyboard input , relational operators, introduction, feature of C language, concepts, uses, basic program structure, simple data types, variables, constants, operators, comments, control flow statement :if, while, for, do-while, switch. bitwise operators, Pre defined and User defined data types, arrays, declaration and opera- tions on arrays, searching and sorting on arrays, types of sorting, 2D arrays, Passing 2D arrays to functions, structure, member accessing, structure and union, array of structures, func- tions, declaration and use of functions, parameter passing, recurssion .

UNIT IV FUNDAMENTALS OF POINTERS

Introduction to pointers, pointer notations in C, Declaration and usages of pointers, operations that can be performed on computers, use of pointers in programming exercises, parameter passing in pointers, call by value, call by references, array and characters using pointers, dynamic memory allocation

UNIT V FILE HANDLING IN C AND ENUM

Introduction to file handling, file operations in C , defining and opening in file, reading a file, closing a file, input output operations on file, counting: characters, tabs , spaces, file opening modes, error handling in input/output operations, Enumerated data types, use of Enum, declaration of Enum.

Text Books:

1. C Programming by Herbert Shield
2. C Programming Language 2nd Edition by Brian, W Kernighan Pearson Education.
3. Programming in ANSI C by E. Balagurusamy, Tata Mgraw Hill
4. C Puzzle Book: Puzzles For The C. Programming Language by Alan R Feuer Prentice HallGale
5. Expert C Programming: Deep C Secrets (s) by Peter Van Der Linden Dorling Kindersley

INTRODUCTION TO CYBER SECURITY			
Course Code:	**CC102**	**Course Credits:**	**2**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**1U**	**Course Semester (U / P):**	**2U**
No. of Lectures + Tutorials (Hrs/Week):	**02 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**30 + 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1. To prepare students with the technical knowledge and skills needed to protect and defend computer systems and networks.			
2. To develop graduates that can plan, implement, and monitor cyber security mechanisms to help ensure the protection of information technology assets.			
3. Analyze and resolve security issues in networks and computer systems to secure an IT infrastructure			
4. Evaluate and communicate the human role in security systems with an emphasis on ethics, social engineering vulnerabilities and training			
5. Interpret and forensically investigate security incident			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1. Follow a structured model in Security Systems Development Life Cycle (SDLC)			
2. Plan, implement and audit operating systems' security in a networked, multi-platform and cross platform environment			
3. Protect data and respond to threats that occur over the Internet			
4. Design and implement risk analysis, security policies, and damage assessment			
5. Detect attack methodology and combat hackers from intrusion or other suspicious attempts at connection to gain unauthorized access to a computer and its resources			

UNIT I CYBER SECURITY FUNDAMENTALS

Overview of cyber security and why it is important; Internet governance: challenges and constraints; cyber threats: cyber warfare, cybercrime, cyber terrorism, cyber espionage; Need for a comprehensive cyber security policy; Need for an international convention on cyber space; Identify trends in cyber security events and protection techniques;

UNIT-II CYBER SECURITY VULNERABILITIES

Categorize assets, risk, threat and vulnerability; Identify different types of vulnerabilities in a system; Vulnerability in software; Complex network architecture of organization; Open access to organizational data; Weak authentication; Determine the phase of a cyber-attack; Overview of cryptography; Deception; Denial of service filters; Ethical hacking

UNIT-III CYBERSPACE AND THE LAW

Computer Ethics and security policies; Cyber security regulations; Role of International Laws; Role of stakeholders (state and private sector) in cyber security; Components of cyber security framework; Cyber security standards; Indian cyber space; National cyber security policy;

UNIT-IV CYBER FORENSICS-overview- Why cyber forensics is important; Types of computer forensics; Objective of cyber security forensics investigators; How experts works; Stages of forensics investigation; Techniques and tools used by forensics experts; Advantages of cyber forensics; Incident handling;

UNIT-V SECURING WEB APPLICATIONS, SERVICES AND SERVER

Introduction; Basic security for HTTP applications and services; Basic security for SOAP (Simple Object Access Protocol)services; Identify management and Web Services; Authorization Patterns; Security Considerations and challenges;

Text Books:

1. Jon Friedman. Mark Bouchard, CISSP. Foreword by John P. Watters to. Cyber Threat Intelligence. Definitive GuideTM. 2015.
2. Scott Roberts, Rebekah Brown. Intelligence-Driven Incident Response: Outwitting the Adversary: O'Reilly 2017.
3. Bob Gourley, The Cyber Threat, Createspace Independent Pub 2014
4. Marjie T Britz, Computer Forensics and Cyber Crime: An Introduction, Pearson Education, 2nd Edition, 2008.
5. Cyberspace and the Law: Your Rights and Duties in the On-Line World By Edward Cavazos and Gavino Morin: MIT Press: 1994.

COMPUTER ORGANIZATION AND ARCHITECTURE			
Course Code:	**CS102**	**Course Credits:**	**4**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**1U**	**Course Semester (U / P):**	**2U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 01**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 15**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.Discuss the basic concepts and structure of computers.			
2.Understand concepts of register transfer logic and arithmetic operations.			
3.Explain different types of addressing modes and memory organization.			
4.Learn the different types of serial communication techniques.			
5.Summarize the Instruction execution stages.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Define different number systems, binary addition and subtraction, 2's complement representation and operations with this representation.			
2.Able to understand the theory and architecture of central processing unit			
3.Analyze some of the design issues in terms of speed, technology, cost, performance.			
4.Use appropriate tools to design verify and test the CPU architecture			
5 .Learn the concepts of parallel processing, pipelining and interprocessor communication.			

UNIT I Data representation and Logic circuits:

Number System, complements, fixed point representation, floating point representation, binary codes, and error detection codes. Logic gates, Boolean algebra, combinational circuits, flip flops, sequential circuits.

UNIT II Digital components and RTL:

Integrated circuits, decoders, multiplexers, registers, shift registers, binary counters, and memory unit. Register Transfer language, Register Transfer, Bus and memory transfers, Arithmetic Mircro operations, logic micro operations, shift micro operations, Arithmetic logic shift unit.

UNIT III Basic Processing Unit:

Instruction codes, Computer Registers, Computer instructions – Instruction cycle, Memory – Reference Instructions. Input – Output and Interrupt. STACK organization, Instruction formats, Addressing modes, DATA Transfer and manipulation, Program control, Reduced Instruction set computer.

UNIT IV Micro Programmed Control and Computer Arithmetic:

Micro program example, design of control unit, Hard-wired control. Micro programmed control unit Addition and subtraction, multiplication Algorithms, Division Algorithms, Floating – point Arithmetic operations. Decimal Arithmetic unit, Decimal Arithmetic operations.

UNIT V The Memory System and IOP:

Memory Hierarchy, Main memory, Auxiliary memory, Associative memory, Cache memory, Virtual memory. Peripheral Devices, Input-Output Interface, Asynchronous data transfer Modes of Transfer, Priority Interrupt, Direct memory Access.

Text Books:

1. Patterson, Computer Organisation and Design, Elsevier Pub. 2009
2. William Stalling, " Computer Organization", PHI
3. Vravice,Hamacher & Zaky, "Computer Organization", TMH
4. Mano," Computer System Architecture", PHI
5. John P Hays, " Computer Organization", McGraw Hill
6. Tannenbaum," Structured Computer Organization', PHI
7. P Pal chaudhry, ' Computer Organization & Design', PHI
8. Computer System Architecture, Morris Mano, 3rd Edition.
9. Computer organization – Carl Hamacher, Zvonks Vranesic, SafeaZaky, Vth Edition, McGraw Hill.

Reference Books:

1. Computer System Architecture, Naush Jotwani- 7MM.
2. Digital Electronics, James W Bignel, Robert Donovan, 5th Edition, Cengage Learning Publications.
3. Digital Design – Morris Mano, PHI, 3rd Edition, 2006.
4. Taub & Schilling: Digital integrated electronics McGraw-Hill
5. R P Jain : Digital Electronics, 4th Edition TMH.

COMPUTER PROGRAMMING LAB – I			
Course Code:	**CS181**	**Course Credits:**	**1**
Course Category:	**CC-P**	**Course (U / P)**	**U**
Course Year (U / P):	**1U**	**Course Semester (U / P):**	**2U**
No. of Labs:	**01(2 hrs)**		
Total No. of Lab (L + T):	**10 + 00**	**End Sem. Exam Hours:**	**2**

COURSE OBJECTIVES
1.Introduce students to the basic knowledge of programming fundamentals of C language.
2.Impart writing skill of C programming to the students and solving problems.
3.Impart the concepts like looping, array, functions, pointers, file, structure.
4.Write programs to print output on the screen as well as in the files..
5.Apply all the concepts that have been covered in the theory course.

COURSE OUTCOMES
At the end of the course the students should be able to:
1.Recognize and understand the syntax and construction of C programming code
2.Able to design and develop Computer programs, analyzes, and interprets the concept of pointers, declarations, initialization, operations on pointers and their usage.
3.Adequate to define data types and use them in simple data processing applications also he/she must be able to use the concept of array of structures.
4.Student must be able to define union and enumeration user defined data types.
5.Develop confidence for self-education and ability for life-long learning needed for Computer language.

LIST OF EXPERIMENTS

1. Write a program for the following:

   a) To find the reverse of a given number.

   b) Calculate factorial of a number using recursion.

2. Write a program to take marks of a student of 5 subjects as an input and print the grade. Also create the same program using switch.

   marks<40 = FAIL
   marks>=40 and <=59 =GOOD
   marks>=59 and <80
   =EXCELLENT marks>=80 =
   OUTSTANDING

3. Write a program to compute the length of a string using While Loop.
4. Write a program to print the following pattern: -

   a)
   ```
   *
   **
   ***
   ****
   *****
   ```

b)

```
       *
      * *
     * * *
    * * * *
```

c)

```
       0
      1 2
     3 4 5
    6  7 8 9
```

5. Write a program to compute and display the product of two matrices.

6. Write a program to illustrate the difference between call by value and call by reference.

7. Write a program to check whether a given string is palindrome or not.
8. Create a structure called STUDENT having name, reg no., class as its field. Compute the size of structure STUDENT.

9. Write a program to compute the length of a string using pointers.

10. Write a program to create a file, input data and display its content.

CYBER SECURITY LAB			
Course Code:	**CC182**	**Course Credits:**	**1**
Course Category:	**CC-P**	**Course (U / P)**	**U**
Course Year (U / P):	**1U**	**Course Semester (U / P):**	**2U**
No. of Labs (Hrs/Week):	**2 hrs.**	**Mid Sem. Exam Hours:**	
Total No. of Labs:	**10**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.Explain & Design computer science terminology related to coding, password protection, social engineering, and network security			
2.Learn & implement fundamentals of cryptography and its application to network security			
3.Develop & Understand network security threats, security services, and countermeasures			
4.Acquire & Design well known network security protocols such as IPSec, SSL, and WEP			
5.Acquire & Develop background on hash functions; authentication; firewalls; intrusion detection techniques.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Develop and implement a java interface for encryption and decryption algorithms i.e., AES, MD5 and RSA algorithm			
2.Design and develop a security architecture for an organization.			
3.Design operational and strategic cyber security strategies and policies			
4.Implement cyber security solutions and use of cyber security, information assurance, and cyber/computer forensics software/tools			
5.Comprehend and execute risk management processes, risk treatment methods, and key risk and performance indicators			

List of Experiments:

1. Study of different wireless network components and features of any one of the Mobile Security Apps.
2. Study of the features of firewall in providing network security and to set Firewall Security in windows
3. Study of steps to ensure Security of any one web browser (Mozilla Firefox/Google Chrome)
4. Study of System threat attacks - Denial of Service and Sniffing and Spoofing attacks
5. Study of Techniques used for Web Based Password Capturing.
6. Implementation of S-DES algorithm for data encryption
7. Implementation of Asymmetric Encryption Scheme – RSA.
8. Study of IP based Authentication.
9. To implement the simple substitution technique named Caesar cipher using C language.
10. To write a program to implement the hill cipher substitution techniques

SEMESTER-III

INTERNET TECHNOLOGY			
Course Code:	**CC201**	**Course Credits:**	**3**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**2U**	**Course Semester (U / P):**	**3U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**

COURSE OBJECTIVES
1.Present the basic web technology concepts for developing web applications.
2.Helps in computational thinking.
3.Understand of networking fundamentals.
4.Recognize the process of technology planning.
5.Interpret the paradigms of web page coding.

COURSE OUTCOMES
At the end of the course the students should be able to:
1.Have basic knowledge and understanding of core Internet technologies.
2.Apply Internet technology techniques for Web page design.
3.Learn various Browsing systems.
4.Work in JavaScript to create web pages effectively.
5.Process page Coding & Planning

UNIT I OVERVIEW OF INTERNET AND WEB

Introduction to internet, history of Internet and web, Internet services and accessibility, uses of internet, Internet standards, Internet protocols- IP, TCP,UDP and host names, web server, proxy server, fast ready connections on the web, web browsers, Netscape communication suite, Microsoft Internet explorer, firewalls, data security.

UNIT II WEB DESIGN

Key issues in web site design, introduction to HTML, SGML- DTD, DTD elements, attributes, outline of an HTML document, body section- headers, paragraphs, text formatting, linking, internal linking, embedding images, lists, tables, frames, other special tags and characters, head section- prologue, link, base, meta, script, style, XML, XHTML, structuring data, XML schema documents, document object model, security and management issues for creating a website.

UNIT III BROWSING SYSTEMS

Searching and web casting technique, popular web servers, basic features, bookmarks, cookies, progress indicators, customization of browsers, browsing tricks, next generation web browsing, search engines, architecture of search engines, search tools, web crawlers, types of crawlers, scalable web crawler, incremental crawler, parallel crawler, focused crawler, agent based crawler, case study of IE, counters, Internet chat, hardware and software requirements for Internet and web based applications, Internet and web technologies.

UNIT IV JAVASCRIPT

Introduction, Language elements, objects of JavaScript, other objects like data, math, string, regular expressions, and arrays.

UNIT V ACTIVE SERVER PAGES

Creating interactive applications using active server pages : client and server side script in C#, variables and constants, creating modules, creating objects from classes, ASP's object model, arrays, collections, control structures, using request and response objects, Integration with database.

Reference Books:

1. Raj Kamal, Internet and Web Technologies, TMH, 2005.
2. Monica D'Souza, Web publishing, TMH, 2001.
3. David Crowder and Rhonda Crowder, Web Design, IDG Books India, 2001.
4. Musciano C., HTML and XHTML the Definitive Guide, 6th edition, OReilly, 2006.
5. Deitel H., Deitel P., Internet and World Wide Web: How to Program, 4 edition, PHI.

OPERATING SYSTEM			
Course Code:	**CC203**	**Course Credits:**	**3**
Course Category:CC	**CC**	**Course (U / P)**	**U**
Course Year (U / P):U	**1U**	**Course Semester (U / P):**	**3U**
No. of Lectures + Tutorials (Hrs/Week):	**03+ 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):30	**45+ 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.Understand how Operating System is Important for Computer System.			
2.Make aware of different types of Operating System and their services.			
3.Learn different process scheduling algorithms and synchronization techniques to achieve better performance of a computer system			
4.Know virtual memory concepts and secondary memory management			
5.Understanding of Security & protection in Operating System			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Understand the different services provided by Operating System at different level			
2.Learn real life applications of Operating System in every field.			
3.Understands the use of different process scheduling algorithm and synchronization techniques to avoid deadlock.			
4.Learn different memory management techniques like paging, segmentation and demand paging etc.			
5.Perform implementation of protection mechanisms in operating system			

UNIT I INTRODUCTION TO OPERATING SYSTEM
Importance of operating systems, basic concepts and terminology about operating system, memory management, processor management, device management, information management functions.

UNIT II PROCESS MANAGEMENT
Elementary concept of process, job scheduler, process scheduling, operation on process, threads, overview, scheduling criteria, scheduling algorithms, algorithm ,deadlocks: system model, deadlock characterization, deadlocks prevention, deadlocks avoidance, deadlocks detection, recovery from deadlock.

UNIT III MEMORY & STORAGE MANAGEMENT
Basic Memory Management**:** Definition, Logical and Physical address map, Memory allocation: Contiguous Memory allocation, partition, Fragmentation, Compaction, Paging, Segmentation.

UNIT IV UNIX/LINUX OPERATING SYSTEM: Development Of Unix/Linux, Role & Function Of Kernel, System Calls, Elementary Linux command & Shell Programming, Directory Structure, System Administration.

UNIT V SECURITY & PROTECTION: Security Environment, Design Principles of Security, User authentication, Protection Mechanism: Protection Domain, Access Control List

Text Books:

[1]. Galvin, Wiley, Operating Systems Concepts, 8th edition, 2009.

[2]. James L Peterson, Operating Systems Concept, John Wiley & Sons Inc, the 6Rev edition, 2007.

Reference Books:

[3]. Deitel H. M., An Introduction to Operating Systems, Addison-Wesley,
1990. [4]. Stallings William, Operating Systems, PHI, New Delhi, 1997.
[5]. S. Tanenbaum Modern Operating Systems, Pearson Education, 3rd edition, 2007.
[6]. Nutt, Operating System, Pearson Education, 2009.
[7]. S. Tanenbaum, Distributed Operating Systems, Prentice Hall, 2nd edition, 2007.

DATA STRUCTURE AND ALGORITHMS			
Course Code:	**CC205**	**Course Credits:**	**3**
Course Category:	**CC**	**Course (U / P)**	U
Course Year (U / P):	**2U**	**Course Semester (U / P):**	3U
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.To emphasize the importance of appropriate data structure in developing and implementing efficient algorithms			
2.Understand basic data structures such as arrays, stacks, queues, hash tables and linked list			
3.To analyze the asymptotic performance of various algorithms			
4.Solve problems using graphs, trees and heaps			
5.Apply important algorithmic design paradigms and methods of analysis			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Define basic static and dynamic data structures and relevant standard algorithms for them.			
2.Select basic data structures and algorithms for autonomous realization of simple programs or program parts.			
3.Determine and demonstrate bugs in program, recognise needed basic operations with data structures			
4.Formulate new solutions for programming problems or improve existing code using learned algorithms and data structures			
5.Evaluate algorithms and data structures in terms of time and memory complexity of basic operations.			

UNIT I INTRODUCTION TO DATA STRUCTURES

Abstract data types, sequences as value definitions, data types in C, pointers in C, data structures and C, arrays in C, array as ADT, one dimensional array, Implementing one dimensional array, array as parameters, two dimensional array, structures in C, implementing structures, Unions in C, implementation of unions, structure parameters, allocation of storage and scope of variables, recursive definition and processes: factorial function, fibonacci sequence, recursion in C, efficiency of recursion, hashing: hash function, open hashing, closed hashing: linear probing, quadratic probing, double hashing, rehashing, extendible hashing.

UNIT II STACK, QUEUE AND LINKED LIST

Stack definition and examples, primitive operations, example -representing stacks in C, push and pop operation implementation, queue as ADT, C Implementation of queues, insert operation, priority queue, array implementation of priority queue, inserting and removing nodes from a list-linked implementation of stack, queue and priority queue, other list structures, circular lists: stack and queue as circular list - primitive operations on circular lists, header nodes, doubly linked lists, addition of long positive integers on circular and doubly linked list.

UNIT III TREES

Binary trees: operations on binary trees, applications of binary trees, binary tree representation, node representation of binary trees, implicit array representation of binary tree, binary tree traversal in C, threaded binary tree, representing list as binary tree, finding the Kth element, deleting an element, trees and their applications: C representation of trees, tree traversals, evaluating an expression tree,

UNIT IV SORTING AND SEARCHING

General background of sorting: efficiency considerations, notations, efficiency of sorting, exchange sorts: bubble sort; quick sort; selection sort; binary tree sort; heap sort, heap as a priority queue, sorting using a heap, heap sort procedure, insertion sorts: simple insertion, shell sort, address calculation sort, merge sort, radix sort, sequential search: indexed sequential search, binary search, interpolation search.

UNIT V GRAPHS

Application of graph, C representation of graphs, transitive closure, Warshall's algorithm, shortest path algorithm, linked representation of graphs, Dijkstra's algorithm, graph traversal, traversal methods for graphs, spanning forests, undirected graph and their traversals, depth first traversal, application of depth first traversal, efficiency of depth first traversal, breadth first traversal, minimum spanning tree, Kruskal's algorithm, round robin algorithm.

Text Books:

1. Aaron M. Tenenbaum, Yeedidyah Langsam, Moshe J. Augenstein, 'Data structures using C', Pearson Education, 2004 / PHI.
2. E. Balagurusamy, 'Programming in Ansi C', Second Edition, TMH, 2003.
3. Robert L. Kruse, Bruce P. Leung Clovis L.Tondo, 'Data Structures and Program Design in C', Pearson Education, 2000 / PHI.

INTRODUCTION TO PYTHON			
Course Code:	**CC207**	**Course Credits:**	**3**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**2U**	**Course Semester (U / P):**	**3U**
No. of Lectures + Tutorials (Hrs/Week):	**03**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.Master the fundamentals of writing Python scripts.			
2.Learn core Python scripting elements such as variables and flow control structures.			
3.Discover how to work with lists and sequence data.			
4.Write Python functions to facilitate code reuse.			
5.Use Python to read and write files.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Problem solving and programming capability.			
2.Explain basic principles of Python programming language			
3.Implement database and GUI applications.			
4.Implement object oriented concepts			
5.Define and demonstrate the use of built-in data structures “lists” and “dictionary”			

UNIT I PYTHON BASICS, CONDITIONAL &LOOPS

Installation of Python and python Notebook, Python Objects, Number & Booleans, Strings, Container objects, Mutability of objects, Operators - Arithmetic, Bitwise, comparison and Assignment operators, Operators Precedence and associativity. Conditions (If else, if-elif-else), Loops (While ,for), Break and Continue statements, Range Functions

UNIT II STRING OBJECTS AND LIST OBJECTS

String object basics, String methods, Splitting and Joining Strings, String format functions, list object basics, list methods, List as stack and Queues, List comprehensions,

UNIT III TUPLES, SET, DICTIONARIES & FUNCTIONS

Tuples, Sets, Dictionary Object basics, Dictionary Object methods, Dictionary View Objects. Functions basics, Parameter passing, Iterators, Generator functions, Lambda functions, Map, Reduce, filter functions

UNIT IV OOPS CONCEPTS & WORKING WITH FILES

OOPS basic concepts, creating classes and Objects, Inheritance, Multiple Inheritance, working with files, Reading and writing files, Buffered read and write, Other File methods

UNIT V MODULES, EXCEPTION HANDLING & DATABASE PROGRAMMING

Using Standard Module, Creating new modules, Exceptions Handling with Try-except, Creating, inserting and retrieving Table, Updating and deleting the data. **Data Ananlysis-**Numpy variable, Numpy manipulation, Scipy, Pandas intro. Descriptive analysis, Pandas Input-output, Pandas manipulation, Pandas groupby

Text Books:

1. Head First Python 2e: A Brain-Friendly Guide Paperback – Illustrated, 16 by Paul Barry, Oreilly
2. Python: The Complete Reference Paperback – 20 March 2018 by Martin C. Brown (Author), TMH Publication
3. Let Us Python by Yashavant Kanetkar , 1 January 2019, BPB publication
4. Python Programming, A modular approach , First Edition, By Pearson Publication by Taneja Sheetal and Kumar Naveen , 26 September 2017

INFORMATION RETRIEVAL SYSTEMS			
Course Code:	**CC209**	**Course Credits:**	**3**
Course Category:	**CC7**	**Course (U / P)**	**U**
Course Year (U / P):	**2U**	**Course Semester (U / P):**	**3U**
No. of Lectures + Tutorials (Hrs/Week):	**03**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.To understand the theoretical basis behind the standard models of IR (Boolean, Vector-space, Probabilistic and Logical models)			
2. To understand the difficulty of representing and retrieving documents, images, speech, etc.			
3.To understand the standard methods for Web indexing and retrieval			
4.To understand how techniques from natural language processing, artificial intelligence, human- computer interaction, and visualization integrate with IR			
5.To be familiar with various algorithms and systems			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Learn the theories and techniques behind Web search engines, E-commerce recommendation systems, etc.			
2.Get hands on project experience by developing real-world applications, such as intelligent tools for improving search accuracy from user feedback, email spam detection, recommendation system, or scientific literature organization and mining.			
3.Learn tools and techniques to do cutting-edge research in the area of information retrieval or text mining.			
4.be able to implement, run and test a standard IR system,			
5.Open the door to the amazing job opportunities in Search Technology and E-commerce companies such as Google, Microsoft, Yahoo!, and Amazon.			

UNIT I INFORMATION RETRIEVAL FUNDAMENTALS

Overview of IR Systems, Historical Perspectives, Basic Evaluation, Document Representation: Statistical Characteristics of Text, Basic Query Processing, Data Structure and File Organization for IR, examples of information retrieval, need of maintain the global information base, use of information for planning, reliability of information storage, redundancy in information storage, report on 21st Century intelligent System, role of intelligent system in e-governance.

UNIT II INFORMATION RETRIEVAL MODELS

Information retrieval using the Boolean model, dictionary and postings, dictionary-based approaches of information retrieval, list, adhoc information retrieval method, indexing, Scoring and term weighting, random vs sequential search methods, the content-based information retrieval system, consistency of retrieved information, accuracy, and precision of retrieved information.

UNIT III INTERNET BASED INFORMATION RETRIEVAL METHODS

Vector space retrieval, relevance feedback and query expansion, XML retrieval probabilistic information retrieval, language model for information retrieval, text classification and naïve bayes, web search basics, web crawling and indexes, evaluating information retrieval methods, concept of

UNIT IV AGENT BASED INFORMATION RETRIEVAL

Ontology based web agents, search for information in unstructured knowledge domains, intelligent adaptive information agents, designing of agent for information retrieval, incorporation of AI concepts for design of intelligent agent.Document and Term Clustering, Document Categorization, IR Systems and the WWW, PageRank and Hyperlink Analysis,

UNIT V INFORMATION RETRIEVAL TECHNIQUES

Search PersonalizationIR Systems and the WWW, Heterogeneous Information Sources, Intelligent Web Agents, Web Mining, and Its Applications, Intelligent Systems for finding Genes in DNA, using information content to evaluate semantic similarity in information taxonomy.

Textbook:

1. D. Grossman and O. Frieder,"Information Retrieval: Algorithms and Heuristics", Kluwer Academic Press.
2. Richard K. Belew, "Finding Out About: A Cognitive Perspective on Search Engine Technology and the WWW", Cambridge University Press, 2001.
3. C. J. van Rijsbergen , "Information Retrieval".

INTERNET TECHNOLOGY LAB			
Course Code:	**CC281**	**Course Credits:**	**2**
Course Category:	**CC-P**	**Course (U / P)**	**U**
Course Year (U / P):U	**2U**	**Course Semester (U / P):**	**3U**
No. of Labs	**1(3 hrs)**		
Total No. of Lab(L + T):10	**10+ 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.To design interactive web pages using Scripting languages.			
2.To learn server side programming using servlets and JSP.			
3.To develop web pages using XML/XSLT			
4.To develop dynamic web pages using different patforms			
5.Learn how to use XAMP Server			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Design simple web pages using markup languages like HTML and XHTML.			
2.Create dynamic web pages using DHTML and java script that is easy to navigate and use.			
3.Program server side web pages that have to process request from client side web pages.			
4.Represent web data using XML and develop web pages using JSP.			
5.Understand various web services and how these web services interact.			

List of Programs

1. Create a web page with the following using HTML.
   0. To embed an image map in a web page.
   1. To fix the hot spots.
   2. Show all the related information when the hot spots are clicked
2. Create a web page with all types of Cascading style sheets.
3. Client Side Scripts for Validating Web Form Controls using DHTML.
4. Installation of Apache Tomcat web server.
5. Write programs in Java using Servlets:
   0. To invoke servlets from HTML forms.
   1. Session Tracking.
6. Write programs in Java to create three-tier applications using JSP and Databases
   0. For conducting on-line examination.
   1. For displaying student mark list. Assume that student information is available in a database which has been stored in a database server.
7. Programs Using Xml – Schema – Xslt/Xsl.
8. Programs using DOM and SAX parsers.
9. Programs using AJAX.
10. Consider a case where we have two web Services- an airline service and a travel agent and the travel agent is searching for an airline. Implement this scenario using Web Services and Data base.

Software Required:

- Dream Weaver or Equivalent, MySQL or Equivalent, Apache Server, WAMP/XAMPP

DATA STRUCTURE AND ALGORITHMS LAB			
Course Code:	**CC283**	**Course Credits:**	**2**
Course Category:	**CC-P**	**Course (U / P)**	**U**
Course Year (U / P):	**2U**	**Course Semester (U / P):**	**3U**
No. of Labs (Hrs/Week):	**2(3 hrs)**		
Total No. of Labs:	**10**	**End Sem. Exam Hours:**	**3**
LAB OBJECTIVES			
1.Introduce the concept of data structures through ADT including List, Stack, Queues .			
2.To design and implement various data structure algorithms.			
3.To introduce various techniques for representation of the data in the real world.			
4.To develop application using data structure algorithms			
5.Compute the complexity of various algorithms.			
LAB OUTCOMES			
At the end of the course the students should be able to:			
1. Select appropriate data structures as applied to specified problem definition			
2.Implement operations like searching, insertion, and deletion, traversing mechanism etc. on various data structures.			
3.Students will be able to implement Linear and Non-Linear data structures.			
4. Implement appropriate sorting/searching technique for given problem.			
5. Design advance data structure using Non-Linear data structure			

List of Experiments:

1. Run time analysis of Fibonacci Series
2. Study and Application of various data Structure
3. Study and Implementation of Array Based Program
   a. Searching (Linear Search, Binary Search)
   b. Sorting (Bubble, Insertion, Selection, Quick, Merge etc)
   c. Merging
4. Implementation of Link List
   a. Creation of Singly link list, Doubly Linked list
   b. Concatenation of Link list
   c. Insertion and Deletion of node in link list
   d. Splitting the link list into two link list
5. Implementation of STACK and QUEUE with the help of
   a. Array
   b. Link List
6. Implementation of Binary Tree
7. Implementation of Binary Search Tree.
8. Write a program to simulate various traversing Technique
9. Representation and Implementation of Graph
   a. breadth First Search
   b. Prims Algorithm
   c. Kruskal’s Algorithms
10. Implementation of Hash Table

PYTHON PROGRAMMING LAB			
Course Code:	**CC285**	**Course Credits:**	**2**
Course Category:	**CC-L4**	**Course (U / P)**	**U**
Course Year (U / P):	**2U**	**Course Semester (U / P):**	**3U**
No. of Labs (Hrs/Week):	**3 hrs**	**Mid Sem. Exam Hours:**	
Total No. of Labs:	**10**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.To introduce students to use of Python programming to solve data analytics problems			
2.To elaborate students to statistical analysis using Python programming			
3.To describe various libraries required for data analytics			
4.To elaborate statistical analysis using Python			
5.To study special libraries in Python such as Numpy and Scipy			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Improve problem solving and programming capability			
2.Learn data analytics through python programming			
3.Underline the use of package			
4.Write simple Python programs for solving problems.			
5.Decompose a Python program into functions, lists etc.			

List of Experiments:

Write a program in python :

1. To print the largest/smallest of two numbers
2. To read two numbers x and n and print x^n (first write with the use of operator and then write with the help of inbuilt function
3. To input the value of x and n and print the sum of the series:
   a. $1+x+x^2+x^3+x^4+\ldots\ldots.x^n$
4. Write a program to compute distance between two points taking input from the user (Pythagorean Theorem)
5. Write a program to count the numbers of characters in the string and store them in a dictionary data structure
6. To print factorial of a number with and without using recursion
7. To tell the frequency of the most common word in a file or a given string
8. Write a function to find all duplicates in the list.
9. Write a program to perform addition and multiplication of two square matrices
10. To read from a text file and print each word separated by # symbol, example #vipin # rai

SEMESTER-IV

SOFTWARE ENGINEERING			
Course Code:	**CC202**	**Course Credits:**	**3**
Course Category:CC	**CC**	**Course (U / P)**	**U**
Course Year (U / P):U	**2U**	**Course Semester (U / P):**	**4 U**
No. of Lectures + Tutorials (Hrs/Week):3	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):45	**45 + 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1. Help students to develop skills that will enable them to construct high quality software that is reliable, and that is reasonably easy to understand, modify and maintain.			
2. Foster an understanding of why these skills are important			
3.Provide an understanding of the working knowledge of the techniques for estimation, design, testing and quality management of large software development projects			
4.Study process models, software requirements, software design, software testing			
5.Help to study Software process/product metrics, risk management, quality management and UML diagrams			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Identify and apply appropriate software architectures and patterns to carry out high level design of a system and be able to critically compare alternative choices.			
2. Expertise and/or awareness of testing problems and will be able to develop a simple testing report			
3.Translate end-user requirements into system and software requirements, using e.g. UML, and structure the requirements in a Software Requirements Document (SRD).			
4. Analyze various software engineering models and apply methods for design and development of software projects			
5 .Proficiently apply standards, CASE tools and techniques for engineering software projects			

UNIT I SOFTWAREENGINEERING

Introduction to software engineering: definitions, role of software engineering, planning a software project, defining the problem, developing a solution strategy, planning the development process, software engineering process paradigms, principles of software engineering, software engineering activities, Software Development Life Cycle (SDLC) Models: Water Fall Model, Prototype Model, Spiral Model, Evolutionary Development Models, Iterative Enhancement Models, Software Quality Frameworks, ISO 9000 Models, SEI-CMM Model

UNIT II REQUIREMENT ANALYSIS AND DESIGN

Software Requirement Specification (SRS): Introduction, need of SRS, significance, characteristics of SRS, Structure of SRS, IEEE standards for SRS design, functional and non-functional requirements, Requirement gathering and analysis, requirement engineering and management, Decision Tables.

Software Quality Assurance (SQA): Verification and Validation, SQA Plans, Software Quality Frameworks, ISO 9000 Models, SEI-CMM Model.

UNIT III SOFTWARE DESIGN PROCESS

Software Design: Introduction, design process activities: architectural design, Abstract specification, Interface design, component design, data structure design, algorithm design modular approach, top-down design, bottom-up design, design methods: data-flow model: data flow diagram, entity-relation-attribute model: E-R diagram, structural model: structure charts, context diagrams, object models: use end Metrics: Various Size Oriented Measures: Halestead's Software Science, Function Point (FP) Based Measures, Cyclomatic Complexity Measures: Control Flow Graphs.

UNIT IV SOFTWARE TESTING

Testing Objectives, Unit Testing, Integration Testing, 8 Acceptance Testing, Regression Testing, Testing for Functionality and Testing for Performance, Top-Down and Bottom-Up Testing Strategies: Test Drivers and Test Stubs, Structural Testing (White Box Testing), Functional Testing (Black Box Testing), Test Data Suit Preparation, Alpha and Beta Testing of Products.Static Testing Strategies: Formal Technical Reviews (Peer Reviews), Walk Through, Code Inspection, Compliance with Design and Coding Standards.

UNIT V SOFTWARE MAINTENANCE

Need for Maintenance, Categories of Maintenance: Preventive, Corrective and Perfective Maintenance, Cost of Maintenance, Software Re-Engineering, Reverse Engineering. Software Configuration Management Activities, Change Control Process, Software Version Control, An Overview of CASE Tools. Estimation of Various Parameters such as Cost, Efforts, Schedule/Duration, Constructive Cost Models (COCOMO), Resource Allocation Models, Software Risk Analysis and Management.problem resolution, software maintenance from customers‟ perspective, maintenance standard: IEEE-1219, ISO-12207, Software Risk Analysis and Management.

Text Books:

1. Pankaj Jalote, An Integrated Approach to Software Engineering, Narosa Publishing House, New Delhi 1997.
2. Ian Sommerville, Software Engineering, Pearson Education, 2009.
3. Pressman Roger S., Software Engineering: Practitioner's Approach, McGraw-Hill Inc., 2004.
4. Software Engineering: Software Reliability, Testing and Quality Assurance, Nasib S. Gill, Khanna Book Publishing Co (P) Ltd., New Delhi, 2002.

DATABASE MANAGEMENT SYSTEM			
Course Code:	**CC204**	**Course Credits:**	**3**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**2U**	**Course Semester (U / P):**	**4U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.Describe the fundamental elements of relational database management systems			
2.Explain the basic concepts of relational data model, entity-relationship model, relational database design, relational algebra and SQL.			
3.Design ER-models to represent simple database application scenarios			
4.Convert the ER-model to relational tables, populate relational database and formulate SQL queries on data.			
5.Improve the database design by normalization.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1. Understanding of database concepts and thorough knowledge of database software's.			
2.Model an application's data requirements using ER diagrams			
3. Write SQL commands to create tables and query data in a relational DBMS			
4. Execute various advanced SQL queries related to transactions, concurrency			
5.Explain the principle of transaction management design.			

UNIT I DATABASE SYSTEM

Database system vs. file system, view of data, data abstraction, instances and schemas, data models, ER model, relational model, database languages, DDL, DML, database access for applications programs, database users and administrator, transaction management, data base system structure, storage manager, query processor, history of database systems, data base design and ER diagrams, beyond ER design entities, attributes and entity sets, relationships and relationship sets, additional features of ER model, concept design with the ER model, and conceptual design for large enterprises.

UNIT II RELATIONAL MODEL

Introduction to the relational model, integrity constraint over relations, enforcing integrity constraints, querying relational data, and logical database design, destroying /altering tables and views. relational algebra and calculus: relational algebra, selection and projection set operations, renaming, joins, division, relational calculus, tuple relational calculus, domain relational calculus, expressive power of algebra and calculus.

UNIT III BASIC SQL QUERY

Examples of basic SQL queries, nested queries, correlated nested queries set, comparison operators, aggregative operators, NULL values, comparison using null values, logical connectivity's, AND, OR and NOTR, impact on SQL constructs, outer joins, disallowing NULL values, complex integrity constraints in SQL triggers and active databases.

UNIT IV SCHEMA REFINEMENT

Problems caused by redundancy, decompositions, problem related to decomposition, reasoning about FDS, FIRST, SECOND, THIRD normal form, BCNF, fourth normal form, lossless join decomposition, dependency preserving decomposition, schema refinement in database design, multi valued dependencies.

UNIT V OVERVIEW OF TRANSACTION MANAGEMENT

ACID properties, transactions and schedules, concurrent execution of transaction, lock based concurrency control, performance locking, and transaction support in SQL, crash recovery, concurrency control, Serializability and recoverability, lock management, lock conversions, dealing with deadlocks, specialized locking techniques, concurrency without locking, crash recovery: ARIES, log, other recovery related structures, the write, ahead log protocol, check pointing, recovering from a system crash, media recovery, other approaches and interaction with concurrency control.

References Books:

1. Elmasri Navrate, Database Management System, Pearson Education, 2008.
2. Raghurama Krishnan, Johannes Gehrke, Database Management Systems, TMH, 3rd edition, 2008.
3. C. J. Date, Introduction to Database Systems, Pearson Education, 2009.
4. Silberschatz, Korth, Database System Concepts, McGraw hill, 5th edition, 2005.
5. Rob, Coronel & Thomson, Database Systems Design: Implementation and Management, 2009.

JAVA PROGRAMMING			
Course Code:	**CC206**	**Course Credits:**	**3**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**2U**	**Course Semester (U / P):**	**4U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.Teach principles of object-oriented programming paradigm including abstraction, encapsulation, inheritance, and polymorphism.			
2.Impart fundamentals of object-oriented programming in Java, including defining classes, invoking methods, using class libraries, etc.			
3.Familiarize the concepts of packages and interfaces			
4.Facilitate students in handling exceptions.			
5.Demonstrate the concept of event handling used in GUI.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Analyze the necessity for Object Oriented Programming paradigm over structured programming and become familiar with the fundamental concepts in OOP like encapsulation, Inheritance and Polymorphism			
2.Design and develop java programs, analyze, and interpret object-oriented data and report results			
3.Design an object-oriented system, AWT components and multithreaded processes as per needs and specifications.			
4.Participate and succeed in competitive examinations like GATE, Engineering services, recruitment interviews etc.			
5.Plan their career in java-based technologies like HADOOP etc.			

UNIT I OBJECT-ORIENTED PROGRAMING

Concept of object-oriented programming (OOP), benefits of OOP, application of OOP, Java history, Java features, Java streaming, Java and Internet, Java contribution to Internet: Java applets, security, portability; Java environment, Java library, Java program structure, Java program, Java Virtual Machine (JVM) architecture, Just In Time compiler (JIT), data type, variables and arrays, operators, control statements, object-oriented paradigms; abstraction, encapsulation, inheritance, polymorphism, Java class and OOP implementation

UNIT II DATA TYPE, OPERATORS AND CONTROL STATEMENT

Data types, Java keywords, identifiers, constants, variables, declaration and scope of the variable, symbolic constant, type casting, arithmetic operator, relational operator, logical operator, assignment operator, increment and decrement operator, conditional operator, bitwise operator, ?: operator, arithmetic expressions, expressions, type conversions in expressions, mathematical functions, more data types: arrays, strings, vectors, wrappers classes, program control statements: decision making and branching: if, if….else, else….if, else if ladder, switch, decision making and looping: while, do….while, for.

UNIT III CLASSES, OBJECTS AND METHODS

Java class libraries, class fundamentals, object, methods, adding variables, add methods, creating objects, accessing class members, constructors, methods overloading, static members, nesting of methods, inheritance: extending a class, overriding methods, final variables and methods, final classes, finalizer methods, abstract methods and classes, visibility control, exception handling fundamental.Interfaces, extending interfaces, implementing interfaces, interfaces references, accessing interface variable, creating queue interface, variable in interfaces, packages, finding a packages and classpath, package and member access, Java API package, system package, naming conventions, creating package, accessing a package, adding a class to a package, hiding classes,

UNIT V MULTITHREADING AND APPLET PROGRAMMING

Multithreading programming: creating threads, thread class and runnable interface extending the thread class, stopping and blocking a thread, life cycle of a thread, thread methods, thread exceptions, thread priority, synchronization, thread communication using notify(), wait(), and notify all(), applet programming : applet basic, applets architecture, a complete applet skeleton, building applets code, applets life cycle, creating a executable applet, designing a web page, applets tag, passing parameters to applets, applets and HTML.

Text Books:

1. Programming with JAVA, E. Balagurusawamy, Tata McGraw Hill, 1998.
2. JAVA Beginner‟s guide, Herbert Schildt, Tata McGraw Hill, 2007.
3. Java How to Program, Deitel & Deitel, Prentice-Hall, 1999.

ARTIFICIAL INTELLIGENCE			
Course Code:	**CC208**	**Course Credits:**	**2**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**2U**	**Course Semester (U / P):**	**4U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.Provide a strong foundation of fundamental concepts in Artificial Intelligence			
2.Enable the student to apply these techniques in applications which involve perception, reasoning and learning			
3.Provide a basic exposition to the goals and methods of Artificial Intelligence			
4.Explain the role of agents and how it is related to environment and the way of evaluating it and how agents can act by establishing goals.			
5.Learn the different machine learning techniques to design AI machine and enveloping applications for real world problems.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Understand the various searching techniques, constraint satisfaction problem and example problems- game playing techniques.			
2. Apply these techniques in applications which involve perception, reasoning and learning			
3.Acquire the knowledge of real world Knowledge representation			
4.Analyze and design a real world problem for implementation and understand the dynamic behavior of a system.			
5.To enable the student to apply these techniques in applications which involve perception, reasoning and learning			

UNIT 1 Introduction

Introduction to AI, Components of AI, Goals of AI, Types of AI, History of AI, Turing Test in AI, Advantages and Disadvantages of AI, Intelligence, Intelligent System, Role of IS, Comparison of various IS, Weak AI and Strong AI, Mind Body Problem in AI, Chinese Room Experiment in AI, Parallel and Distributed AI.

UNIT 2 Agents in AI

Intelligent Agents, Types of AI Agents, Simple Reflex Agent,Model-based reflex agent, Goal-based agents, Utility-based agent, Learning agent, Structure of an AI Agent, Agent Environment in AI, Examples of Agents, Knowledge Engineering, Knowledge Based System, Knowledge Engineering Techniques, Knowledge Engineering Principles, Knowledge Engineering Methodology.

UNIT 3 Searching Techniques and AI problems

Searching in AI, Search Algorithm Terminologies, Properties of Search Algorithms, Breadth-first search, Depth-first search, Best First Search, Tic-Tac Toe Problem, Water Jug problem, Chess Problem, Tower of Hanoi problem, Travelling Salesman problem, Monkey and Banana Problem, Magic Square.

UNIT 4 Knowledge Representation

Knowledge Representation Definition, Declarative Knowledge, Procedural knowledge, Meta Knowledge, Heuristic Knowledge, Structural Knowledge, Inheritable Knowledge, Inferential Knowledge, Relational Knowledge, Explicit Knowledge, Tacit Knowledge, Uncertain Knowledge, Knowledge Storage, Relation between Knowledge and Intelligence, AI knowledge cycle.

UNIT 5 AI Techniques and applications

Introduction to Machine Learning, Introduction to Deep Learning, Introduction to Expert system, Introduction to Natural Language Processing, AI in future, AI in social Media, AI in Entertainment and education, AI in drones, AI in Automated Computer support, AI in personalized shopping experience, surveillance, Ai in education, AI in healthcare, AI in E commerce.

Reference Books:

1. Artificial Intelligence, Elaine Reich: Tata Mcgraw Hill publishing house, 2008.
2. Artificial Intelligence, Ela Kumar, IK Publishing.
3. Artificial Intelligence, Peterson, TataMcGraw Hill, 2008.
4. Artificial Intelligence, Russel and Norvig, Pearson Printice Hall Publication, 2006.
5. Artificial Intelligence, Winston, PHI publication, 2006.
6. Artificial Intelligence- A modern approach (3rd Edition) By Stuart Russell & Peter Norvig.
7. Artificial Intelligence: The Basics By Kevin Warwick

INFORMATION THEORY & CODING			
Course Code:	**CC210**	**Course Credits:**	**3**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**2U**	**Course Semester (U / P):**	**4U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 15**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 15**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.Understand the differences between dependent and independent sources.			
2.Understand different source coding techniques.			
3.Understand information channels like joint probability matrix, binary symmetric channel, etc.			
4.Learn error control coding.			
5.Learn convolutional codes.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1. Explain concept of Dependent & Independent Source, measure of information, Entropy, Rate of information and Order of a source			
2. Represent the information using Shannon Encoding, Shannon Fano, Prefix and Huffman Encoding Algorithms			
3. Model the continuous and discrete communication channels using input, output and joint probabilities			
4. Determine a codeword comprising of the check bits computed using Linear Block codes, cyclic codes & convolutional codes			
5. Design the encoding and decoding circuits for Linear Block codes, cyclic codes, convolutional codes, BCH and Golay codes.			

UNIT I INFORMATION THEORY

Information Theory: Introduction, Measure of information, Information content of message, Average Information content of symbols in Long Independent sequences, Average Information content of symbols in Long dependent sequences, Markov Statistical Model for Information Sources, Entropy and Information rate of Mark off Sources

UNIT II SOURCE CODING

Source Coding: Encoding of the Source Output, Shannon's Encoding Algorithm, Shannon Fano Encoding Algorithm, Source coding theorem, Prefix Codes, Kraft McMillan Inequality property• KMI, Huffinan codes

UNIT III INFORMATION CHANNELS

Information Channels: Communication Channels, Discrete Communication channels Channel Matrix, Joint probability Matrix, Binary Symmetric Channel, System Entropies, Mutual Information, Channel Capacity, Channel Capacity of Binary Symmetric Channel

UNIT IV ERROR CONTROL CODING

Error Control Coding: Introduction, Examples of Error control coding, methods of Controlling Errors, Types of Errors, types of Codes, Linear Block Codes: matrix description of Linear Block Codes, Error detection & Correction capabilities ofLinear Block Codes, Single error correction Hamming code, Table lookup Decoding using Standard Array.

Binary Cyclic Codes: Algebraic Structure of Cyclic Codes, Encoding using an (n-k) Bit Shift register, Syndrome Calculation, Error Detection and Correction

UNIT V CONVOLUTION CODES

Convolution Codes: Convolution Encoder, Time domain approach, Transform domain approach, Code Tree, Trellis and State Diagram, The Viterbi Algorithm

TextBook:

1. Digital andAnalog Communication Systems, K. Sam Shanmugam, John Wtley India Pvt Ltd,

1996. 2 Digital Communication, Simon Haykin, John Wtley India Pvt Ltd, 2008.

Reference Books:

1. lTC and Cryptography, Ranjan Bose, TMH, II edition, 2007

2 Principles ofDigital Communication, J. Das, S.K.Mullick, P. K. Chatterjee, Wiley, 1986-Technology &Engineering

3. Digital Conummications- Fundamentals andApplications, Bernard Sklar, SecondEdition, Pearson Education, 2016, ISBN: 9780134724058.

4. Information Theory and Coding, HariBhat, Ganesh Rao, Cengage, 2017.

5. Error Correction Coding, Todd K Moon,Wiley Std. Edition, 2006

THEORY OF AUTOMATA			
Course Code:	**CC212**	**Course Credits:**	**4**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**2U**	**Course Semester (U / P):**	**4U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 15**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 15**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.Determine the various categories of automata (deterministic and nondeterministic finite state automata, and variants of Turing machines)			
2.Understand the various categories of languages and grammars in the Chomsky hierarchy			
3.Define the notions of computability and decidability			
4.Recognize to which class in the Chomsky hierarchy the language described (by a grammar or machine)			
5. Discover the problems reducible to/from well-known decidable/undecidable problems			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Model, compare and analyze different computational models using combinatorial methods.			
2.Apply rigorously formal mathematical methods to prove properties of languages, grammars and automata.			
3.Construct algorithms for different problems and argue formally about correctness on different restricted machine models of computation.			
4.Identify limitations of some computational models and possible methods of proving them.			
5.Have an overview of how the theoretical study in this course is applicable to and engineering application like designing the compilers.			

UNIT I

Introduction: Alphabets, Strings and Languages, Automata and Grammars, Deterministic finite Automata (DFA)-Formal Definition, Simplified notation: State transition graph, Transition table, Language of DFA, Nondeterministic finite Automata (NFA), NFA with epsilon transition, Language of NFA, Equivalence of NFA and DFA, Minimization of Finite Automata, Quotient Construction, Myhill- Nerode Theorem.

UNIT II

Regular expression (RE), Definition, Operators of regular expression and their precedence, Algebraic laws for Regular expressions, Kleen's Theorem, Regular expression to FA, DFA to Regular expression, Arden Theorem, Non Regular Languages, Pumping Lemma for regular Languages . Application of Pumping Lemma, Closure properties of Regular Languages, Decision properties of Regular Languages, FA with output: Moore and Mealy machine, Equivalence of Moore and Mealy Machine, Applications and Limitation of FA.

UNIT III

Context free grammar (CFG) and Context Free Languages (CFL): Definition, Examples, Derivation , Derivation trees, Ambiguity in Grammar, Inherent ambiguity, Ambiguous to Unambiguous CFG, Useless symbols, Simplification of CFGs, Normal forms for CFGs: CNF and GNF, Closure proper ties of CFLs, Decision Properties of CFLs: Emptiness, Finiteness and Membership, Pumping lemma for CFLs Cock-Younger-Kasami Algorithm, Application to Parsing.

UNIT IV

Push Down Automata (PDA): Description and definition, Instantaneous Description, Language of PDA, Acceptance by Final state, Acceptance by empty stack, Deterministic PDA, Equivalence of

PDA and CFG, CFG to PDA and PDA to CFG, Two stack PDA

UNIT V

Turing machines (TM): Basic model, definition and representation, Instantaneous Description, Language acceptance by TM, Variants of Turing Machine, TM as Computer of Integer functions, Universal TM, Church's Thesis, Recursive and recursively enumerable languages, Halting vs Looping, Introduction to Undecidability, Undecidable problems about TMs. Post correspondence problem (PCP), Modified PCP, Introduction to recursive function theory .

Text Books

1. Automata and Computability, Dexter C. Kozen, Springer Publishers, 2007.
2. Introduction to Automata Theory, Languages and Computation, Hopcroft, Motwani, and Ullman, Pearson Publishers, Third Edition, 2006.

Reference Books

1. Elements of the Theory of Computation, H. R. Lewis and C.H. Papadimitriou, Prentice Hall Publishers, 1981
2. Introduction to Languages and the Theory of Computation, John. C. Martin, Tata McGraw-Hill, 2003.
3. K.L.P. Mishra and N.Chandrasekaran, "Theory of Computer Science : Automata, Languages and Computation", PHI Learning Private Limited, Delhi India

DATABASE MANAGEMENT SYSTEM LAB			
Course Code:	**CC282**	**COURSE CREDITS:**	**2**
Course Category:	**CC-P**	**Course (U / P)**	**U**
Course Year (U / P):	**2U**	**Course Semester (U / P):**	**4U**
No. of Labs(Hrs/Week):	**2(3 hrs)**		
Total No. of Labs	**10**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1. Explain basic database concepts, applications, data models, schemas and instances.			
2.Demonstrate the use of constraints and relational algebra operations.			
3.Emphasize the importance of normalization in databases.			
4.Facilitate students in Database design			
5.Familiarize issues of concurrency control and transaction management.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Students get practical knowledge on designing and creating relational database systems.			
2.Understand various advanced queries execution such as relational constraints, joins, set operations, aggregate functions, trigger, views and embedded SQL.			
3.Design a commercial relational database system (Oracle, MySQL) by writing SQL using the system			
4.Use the basics of SQL and construct queries using SQL in database creation and interaction.			
5.Analyze and Select storage and recovery techniques of database system.			

List of Experiments:

1.Introduction to MySQL, an exercise of data types in MySQL & Data Definition Language Commands
2. Exercise on Data Manipulation Language and Transaction Control Commands

3. Exercise on Types of Data Constraints

4.Exercise on JOINS (Single-Table) Using Normalization

5. Exercise on JOINS (Multiple-Table) Using Normalization

6. Exercise on GROUP BY/ORDER BY Clause and Date Arithmetic

7. Exercise on different Functions (Aggregate, Math and String)

8. Exercise on different types of sub queries

9. Procedures

JAVA PROGRAMMING LAB			
Course Code:	**CC284**	**Course Credits:**	**2**
Course Category:	**CC-P**	**Course (U / P)**	**U**
Course Year (U / P):	**2U**	**Course Semester (U / P):**	**4U**
No. of Labs (Hrs/Week):	**02(3 hrs)**		
Total No. of Labs:	**10**	**End Sem. Exam Hours:**	**3**

COURSE OBJECTIVES
1. Prepare students to excel in Object Oriented programming and to succeed as a Java Developer through global rigorous education
2. Students learn an object-oriented way of solving problems using java.
3. Make the students write programs using multithreading concepts and handle exceptions.
4.Demonstrate the students to write programs that connect to a database and be able to perform various operations.
5.Make the students to create the Graphical User Interface using Applets, AWT Components & Swing Components.

COURSE OUTCOMES
At the end of the course the students should be able to:
1.To Understand OOP concepts and basics of Java programming.
2.Design and develop java programs, analyze, and interpret object-oriented data and report results.
3.Demonstrate an ability to design an object-oriented system, AWT components or multithreaded process as per needs and specifications.
4.To build files and establish database connections.
5.To visualize and work on laboratory and multidisciplinary tasks like console and windows applications both for standalone and Applets programs

1. Write a separate Java Code to implement each of the following:

   Class, Command Line Argument, how to enter value through keyboard
2. Write a separate Java Code to implement each of the following data types: Variable, Constant, Arrays, Strings, Vectors, Wrappers Classes, Type Casting

3. Write a separate Java Code to implement each of the following operators:

   Arithmetic operator, Relational operator, Logical operator, Assignment operator, Increment & Decrement operator, Conditional operator, Bitwise operator, ?: operator
4. Write a separate Java Code to implement each of the following control statements: Decision statement, Loops statement and Branch statements

5. Write a separate Java Code to implement each of the following sorting: Bubble Sort, Selection Sort, Insertion Sort, Merge Sort

6. Write a separate Java Code to implement each of the following:
   Class, Object, Constructors, Method, Method Overloading and Method Overriding

Final variable, final class, final method, abstract class, abstract method and concrete method

8. Write a separate Java Code to implement each of the following OOPs concepts: Abstraction, Polymorphism, Encapsulation, Inheritance

9. Write a separate Java Code to implement each of the following: Exception handling with Try, Catch, Throw, Throws, Finally Multiple catch statement with the following exceptions : ArithmeticException, ArrayOutOfBoundsException and ArrayStoreException

10. Write a separate Java Code to implement the following:

a) Interface

b) Packages and how to import them.

INFORMATION THEORY & CODING LAB			
Course Code:	**CC286**	**Course Credits:**	**2**
Course Category:	**CC-P**	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**5U**
No. of Labs (Hrs/Week):	**2(3 hrs)**	**Mid Sem. Exam Hours:**	
Total No. of Labs:	**10**	**End Sem. Exam Hours:**	**3**

COURSE OBJECTIVES
1.To study Fourier perspective; and extensions to wavelets,complexity, compression, and efficient coding of audio-visual information
2. To study Fourier perspective; and extensions to wavelets,complexity, compression, and efficient coding of audio-visual information
3. To implement to calculate the capacity of a communication channel, with and without noise; coding schemes, including error correcting and codes
4. To understand how discrete channels and measures of information generalise to their continuous forms
5. To study Fourier perspective; and extensions to wavelets,complexity, compression, and efficient coding of audio-visual information

COURSE OUTCOMES
At the end of the course the students should be able to:
1.Understands the fundamentals of coding theory
2.Understands concept of source coding
3. Understands channel coding theorem.
4. Students will demonstrate the error control coding
5. Students will demonstrate various codes

List of Experiments:

1. To revise and write programs for understanding variable scope, swapping integers by reference and checking the number even or odd using ternary operators in C/C++.
2. To revise and write a program for sorting integers numbers, and factorial using recursion, function overloading and inline function.
3. Develop a program to implement The algorithm of Encoding of messages.
4. Develop a program to Compute the Entropy in case of Discrete Algorithm.
5. Develop a program to Compute Entropy of 4 Parts of Message
6. To write a program to Find the Entropy of certain message.in C++
7. Develop and Implement Program to Compute the Capacity of Noiseless Binary Channel.
8. Can computing Binary Entropy Function (Channel Capacity) as follow:

   $$C = 1 - H(p)$$

   Write Program for BSC when px=0.1 find the Hp= 0.468 ~ 0.47 and Capacity= 0.53~0.531.
9. Can Computing BSC (Channel Capacity) in Private Case Study As Follow:

   $$I(X;Y) = H(Y) - H(Y|X)$$

   Write Program For BSC of Private Case Study To Compute Capacity.
10. Use an example to illustrate Shannon Fano algorithm.

SEMESTER-V

COMPILER DESIGN			
Course Code:	**CC301**	**Course Credits:**	**4**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**5U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 01**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 15**	**End Sem. Exam Hours:**	**3**

COURSE OBJECTIVES
1.Understand the basic principles of compiler design, its various constituent parts, algorithms and data structures required to be used in the compiler.
2.Find Out the relations between computer architecture and how its understanding is useful in design of a compiler.
3. Construct efficient algorithms for compilers.
4.Provide an understanding of the fundamental principles in compiler design.
5.Learn the process of translating a modern high-level-language to executable code required for compiler construction.

COURSE OUTCOMES
At the end of the course the students should be able to:
1.Acquire knowledge of different phases and passes of the compiler and also able to use the compiler tools like LEX, YACC, etc. Students will also be able to design different types of compiler tools to meet the requirements of the realistic constraints of compilers.
2.Understand the parser and its types i.e. Top-Down and Bottom-up parsers and construction of LL, SLR, CLR, and LALR parsing table.
3.Implement the compiler using syntax-directed translation method and get knowledge about the synthesized and inherited attributes.
4.Acquire knowledge about run time data structure like symbol table organization and different techniques used in that.
5.Analyse the target machine's run time environment, its instruction set for code generation and techniques used for code optimization.

UNIT I INTRODUCTION TO COMPILER

Introduction to compiler, phases and passes, bootstrapping, finite state machines and regular expressions and their applications to lexical analysis, optimization of DFA-based pattern matchers implementation of lexical analyzers, lexical-analyzer generator, LEX-compiler, formal grammars and their application to syntax analysis, BNF notation, ambiguity, YACC, syntactic specification of programming languages: Context free grammars, derivation and parse trees, capabilities of CFG.

UNIT II PARSING TECHNIQUE

Parsers, shift reduce parsing, operator precedence parsing, top down parsing, predictive parsers Automatic construction of efficient parsers: LR parsers, the canonical collection of LR(0) items, constructing SLR parsing tables, constructing canonical LR parsing tables, constructing LALR parsing tables, using ambiguous grammars, an automatic parser generator, implementation of LR parsing tables.

UNIT III SYNTAX-DIRECTED TRANSLATION

Syntax-directed translation schemes, implementation of syntax directed translators, intermediate code, postfix notation, parse trees & syntax trees, three address code, quadruple & triples, translation of assignment statements, boolean expressions, statements that alter the flow of control, postfix translation, translation with a top down parser, more about translation: array references in arithmetic expressions, procedures call, declarations and case statements.

UNIT IV SYMBOL TABLES

Data structure for symbols tables, representing scope information, run-time administration: implementation of simple stack allocation scheme, storage allocation in block structured language, Error detection & recovery: lexical phase errors, syntactic phase errors, semantic errors.

UNIT V CODE GENERATION

Design issues, the target language. addresses in the target code, basic blocks and flow graphs, optimization of basic blocks, code generator. code optimization: machine-independent optimizations, loop optimization, DAG representation of basic blocks, value numbers and algebraic laws, global data-flow analysis

Text Books:

1. Aho, Sethi & Ullman, "Compilers: Principles, Techniques and Tools”, Pearson Education
2. V Raghvan, “ Principles of Compiler Design”, TMH
3. Kenneth Louden,” Compiler Construction”, Cengage Learning.

SOFT COMPUTING TECHNIQUES			
Course Code:	**CC203**	**Course Credits:**	**3**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**4U**	**Course Semester (U / P):**	**5U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.Primary objective of this course is to provide an introduction to the basic principles, techniques, and applications of soft computing.			
2. Understanding of the basic areas of Soft Computing including Artificial Neural Networks, Fuzzy Logic and Genetic Algorithms.			
3.Provide the mathematical background for carrying out the optimization associated with neural network learning.			
4.Aim of this course is to develop some familiarity with current research problems and research methods in Soft Computing by working on a research or design project.			
5. Genetic algorithms, its applications and advances.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Apply basics of Fuzzy logic and neural networks..			
2.Discuss the ideas of fuzzy sets, fuzzy logic and use of heuristics based on human			
3. Describe with genetic algorithms and other random search procedures useful while seeking global optimum in self-learning situations			
4. Develop some familiarity with current research problems and research methods in Soft Computing Techniques			
5. experience Relate with neural networks that can learn from available examples and generalize to form appropriate rules for inference systems			

UNIT I INTRODUCTION

Introduction to Soft Computing; Definition, requirement, necessity and adequacy; various dialects of soft computing – Evolutionary Algorithms, Fuzzy Sets and Fuzzy Logic, Artificial Neural Networks - their suitability in Searching, optimization, decision matching and pattern related problems; potential areas of applications.

UNIT II FUZZY SETS AND FUZZY LOGIC

Introduction to fuzzy sets and fuzzy logic; difference between classical and fuzzy sets; chance vs fuzziness; limitations of fuzzy systems; typical shapes of membership functions and their usage; operations on fuzzy sets: compliment, intersection, union; combinations on operations, aggregation operation.

UNIT III FUZZY RELATIONS AND FUZZY SYSTEMS

Cartesian Product; Classical Relations and Fuzzy Relations; Cardinality, operations and properties of crisp and fuzzy relations; Composition of operations, Fuzzy cartesian product; The linguistic variables, Reasoning in fuzzy logic, Fuzzification and defuzzification; Mamdani and Sugano Fuzzy Inference Systems.

UNIT IV NEURAL NETWORK

Overview of biological neurons; McCulloch-Pitts model, Rosenblatt's Perceptron model, difference, capabilities and limitations; Model of generic computational neuron; Basic activation functions; Basic Learning laws of neurons; Single layer and multilayer architectures; Feedforward and feedback networks.

UNIT V LEARNING FUNDAMENTALS

Learning paradigms, supervised and unsupervised learning, reinforced learning; back propagation algorithm; Radial basis neurons, Generalized Regression Neural network, Probabilistic Neural Networks; Competitive learning; Self Organizing Features Map, Hopfield networks, associative memories, applications of artificial neural networks. Elasticity vs plasticity dilemma, preprocessing, post processing, early stopping.

UNIT VI EVOLUTIONARY ALGORITHMS

Problems suitable and not suitable for applying evolutionary algorithms; Various dialects of evolutionary Algorithms; Terminology of Genetic Algorithms; Canonical Genetic Algorithm; Common representations and related reproduction operators; premature convergence, schema theorem, minimal deceptive problem and Royal Road function; fitness function, Roulette wheel selection, Rank selection, Tournament Selection; termination criteria, survivor selection, population models; parallel implementations.

Text Books:

1. Artificial Neural Networks: An introduction to ANN Theory and Practice, Peteus J. Braspenning,

   PHI publication, 2005.
2. Fuzzy Logic: A spectrum of Theoretical and Practical issues, Paul P. Wang, pearson publication 2004.
3. An Introduction to Genetic Algorithms, Milanie Mitchell, MIT Press 1998.
4. A Genetic Algorithm Tutorial, Darrell Whitley.
5. Fuzzy Sets, Fuzzy logic, and Fuzzy Systems: Selected Papers- Lotfi Asker Zadeh, George J. Kilr, Bo yuan, 2005.
6. Foundations of Fuzzy logic and Soft Computing: 12th International Fuzzy conference proceeding, 2005.
7. Neural Networks Theory, Particia Melin, Oxford University press, 2003
8. Neural Networks Theory and Application, Oscar Castillo, Wiley Eastern publication
9. Genetic Algorithms in Search, Optimization and Machine Learning, David E Goldberg, Eddison-Wesley, 1988.

ANALYSIS & DESIGN OF ALGORITHMS			
Course Code:	**CC305**	**Course Credits:**	**3**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**5U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.Analyze the asymptotic performance of algorithms.			
2.Write rigorous correctness proofs for algorithms.			
3.Demonstrate a familiarity with major algorithms and data structures.			
4.Apply important algorithmic design paradigms and methods of analysis.			
5.Synthesize efficient algorithms in common engineering design situations.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Argue the correctness of algorithms using inductive proofs and invariant			
2.Explain the major graph algorithms and their analyses. Employ graphs to model engineering problems, when appropriate. Synthesize new graph algorithms and algorithms that employ graph computations as key components, and analyze them.			
3.Describe the divide-and-conquer paradigm and explain when an algorithmic design situation calls for it. Recite algorithms that employ this paradigm. Synthesize divide-and-conquer algorithms. Derive and solve recurrences describing the performance of divide-and-conquer algorithms.			
4.Define the dynamic-programming paradigm and explain when an algorithmic design situation calls for it. Recite algorithms that employ this paradigm. Synthesize dynamic-programming algorithms, and analyze them.			
5.Analyze worst-case running times of algorithms using asymptotic analysis.			

UNIT I BASIC CONCEPT OF ALGORITHMS

What is an algorithm, notion of algorithm, fundamentals of algorithmic solving, Mathematics for Algorithmic sets, Functions and Relations, Vectors and Matrices, linear Inequalities and Linear Equations, fundamentals of analysis framework, the efficient algorithm, Average, Best and Worst case analysis, asymptotic notation, Analyzing Control statement, Loop invariant and the correctness of the algorithm.

UNIT II MATHMATICAL ASPECTS AND ANALYSIS OF ALGORITHM

Mathematical analysis of non- recursive algorithm , mathematical analysis of recursive algorithm, example: fibonacci numbers, empirical analysis of algorithms, algorithm visualization.

UNIT III ANALYSIS OF SORTING AND SEARCHING ALGORITHM

Sorting Algorithms and Analysis: Bubble sort, Selection sort, Insertion sort,Shell sort Heap sort, Sorting in linear time: Bucket sort, Radix sort and Counting sort. sequential search and brute-force string matching, divide and conquer, merge sort, binary search, binary tree, traversal and related properties, depth first search and breadth forst search.

UNIT IV ALGORITHM TECHNIQUES

Transform and conquer, presorting, balanced search trees, avl trees, heaps and heap sort, dynamic programming, Warshall's and Floyd's algorithm, optimal binary search trees, greedy techniques, Prim's algorithm, Kruskal's algorithm, Dijkstra's algorithm, Huffman trees.

UNIT V ALGORITHM DESIGN METHODS

Backtracking, n-Queen's problem, Hamiltonian circuit problem, subset-sum problem, branch and bound, assignment problem, knapsack problem, traveling salesman problem.

Text Books:

1. Anany Levitin, "Introduction to the Design and Analysis of Algorithm", Pearson Education Asia, 2003

References Books:

2. T.H. Cormen, C.E. Leiserson, R. L. Rivest and C. Stein, "Introduction to Algorithm", PHI Pvt. Ltd., 2001

3. Sara Baase and Allen Van Gelder,"Computer Algorithms-Introduction to the Design and Analysis ", Pearson Education Asia, 2003

4. A. V. Aho, J.E. Hopcroft and J.D. Ullman, "the Design and Analysis of Computer Algorithms", Pearson Education Asia, 2003.

CRYPTOGRAPHY & DATA PRIVACY			
Course Code:	**CC307**	**Course Credits:**	**3**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**5U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 +00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.To understand the mathematics behind Cryptography.			
2.To understand the security concerns and vulnerabilities			
3. To familiarize with different types of cryptosystems			
4. To create an awareness for the design of various cryptographic primitives			
5.To analyze different types of attacks on various cryptosystems.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.To learn the importance of number theory in designing crypto systems;			
2.To design public and private key cryptosystems;			
3.To do cryptanalysis of various cryptosystems.			
4. To implement cryptographic algorithms			
5. To structure Privacy issues and able to resolve them.			

UNIT I

Introduction to Security:-Security Goals – Security services(Confidentiality, Integrity, Authentication, Non-repudiation,Access control) – Security Mechanisms (Encipherment, Data Integrity, Digital Signature, Authentication Exchange, Traffic Padding, Routing Control, Notarization, Access control) - Security Principles. Introduction to Cryptography:-Kerckhoff's Principle -Classification of Cryptosystems-Cryptanalytic attacks- Cipher Properties (Confusion, Diffusion).

UNIT II

Traditional Secret Key Ciphers:- Substitution Ciphers (mono alphabetic ciphers, poly alphabetic ciphers)-Transposition Ciphers-Stream and Block Ciphers. Modern Secret Key Ciphers:- Substitution Box-Permutation Box-Product Ciphers

UNIT III

Data Encryption Standard (DES) (Fiestel and Non-Fiestel Ciphers, Structure of DES, DES Attacks, 2-DES, 3-DES) - Advanced Encryption Standard (AES) (Structure, Analysis)-Cryptographic Hash Functions– Properties - Secure HashAlgorithm-Message Authentication Code (MAC).

UNIT IV

Public Key Cryptosystems (PKC): - Types of PKC –Trapdoor -one way functions -RSA Cryptosystem (Integer FactorisationTrapdoor, Key Generation, Encryption, Decryption) - El Gamal Cryptosystem (Discrete Logarithm Trapdoor, Key Generation, Encryption, Decryption) - Diffie-Hellman Key Exchange Protocol, Man in the Middle attack on Diffie-Hellman Protocol.

UNIT V

Digital Signature:-Signing – Verification - Digital signature forgery (Existential forgery, Selective forgery, Universal forgery) - RSA Digital Signature Scheme - ElGamal Signature Scheme - IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload-Intruders, Intrusion Detection, Distributed Denial of Service attacks

Text Books:

1. Behrouz A. Forouzan and Debdeep Mukhopadhyay, Cryptography & Network Security, Second Edition, Tata McGraw Hill, New Delhi, 2010

2. Douglas R. Stinson, “Cryptography: Theory and Practice”, Third Edition, CRC Press.

3. William Stallings, “Cryptography and Network Security – Principles and Practices”, Pearson Education, Fourth Edition, 2006.

Reference Books:

1. Atul Kahate, “Cryptography and Network Security”, 2nd Edition, Tata McGraw Hill, 2003.

2. Bernard Menezes, Network Security and Cryptography-Cengage Learning India, 2011

3. Bruce Schneier, “Applied Cryptography: Protocols, Algorthms, and Source Code in C”, Second Edition, John Wiley and Sons Inc, 2001.

4. Thomas Mowbray, “Cybersecurity : Managing Systems Conducting Testing, and Investigating Intrusions”, John Wiley, 2013

5. Wenbo Mao, “ Modern Cryptography- Theory & Practice”, Pearson Education, 2006.

MACHINE LEARNING			
Course Code:	**CC309**	**Course Credits:**	**3**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**4U**	**Course Semester (U / P):**	**5U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1. Explain Machine Learning concepts, classifications of Machine Learning and write simple programs using python.			
2.Describe Supervised Learning concepts.			
3.Describe unsupervised learning concepts and dimensionality reduction techniques			
4.Discuss simple Machine Learning applications in a range of real-world applications using Python programming			
5.To develop skills of using recent machine learning software for solving practical problems.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Recognize the characteristics of machine learning that make it useful to real-world problems.			
2.Characterize machine learning algorithms as supervised, semi-supervised, and unsupervised.			
3.Effectively use machine learning toolboxes.			
4.Understand the concept behind neural networks for learning non-linear functions.			
5.Figure out the algorithms for learning Bayesian networks			

Unit 1: Introduction – Well defined learning problems, Designing a Learning System, Issues in Machine Learning; THE CONCEPT LEARNING TASK - General-to-specific ordering of hypotheses, Find-S, List then eliminate algorithm, Candidate elimination algorithm, Inductive bias

Unit 2: Decision Tree Learning - Decision tree learning algorithm-Inductive bias- Issues in Decision tree learning; ARTIFICIAL NEURAL NETWORKS – Perceptrons, Gradient descent and the Delta rule,
Adaline,Multilayer networks, Derivation of backpropagation rule Backpropagation Algorithm Convergence, Generalization

Unit 3: Evaluating Hypotheses: Estimating Hypotheses Accuracy, Basics of sampling Theory, Comparing Learning Algorithms; **Bayesian Learning:** Bayes theorem, Concept learning, Bayes Optimal Classifier, Naïve Bayes classifier, Bayesian belief networks, EM algorithm;

Unit 4: Computational Learning Theory: Sample Complexity for Finite Hypothesis spaces, Sample Complexity for Infinite Hypothesis spaces, The Mistake Bound Model of Learning;
INSTANCE-BASED LEARNING – k-Nearest Neighbour Learning, Locally Weighted Regression, Radial basis function networks, Case-based learning

Unit 5: Genetic Algorithms: an illustrative example, Hypothesis space search, Genetic Programming, Models of Evolution and Learning; Learning first order rules-sequential covering algorithms- General to specific beam search-FOIL; REINFORCEMENT LEARNING - The Learning Task, Q Learning.

Text Books:

1. Tom M. Mitchell, ―Machine Learning, McGraw-Hill Education (India) Private Limited, 2013.
2. Ethem Alpaydin, ―Introduction to Machine Learning Press 2004.
3. Stephen Marsland, ―Machine Learning: An Algorithmic Perspective, CRC Press, 2009.Bishop, C., Pattern Recognition and Machine Learning. Berlin: Springer-Verlag.

ELECTIVE 1

SECURITY INFORMATION AND EVENT MANAGEMENT

Course Code:	**CS311**	**Course Credits:**	**3**
Course Category:	**E1**	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**5U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**

Pre requisites: Basic knowledge of cybersecurity concepts

COURSE OBJECTIVES

1. Understand when, where, how, and why to apply Intrusion Detection tools and techniques in order to improve the security posture of an enterprise.
2. Apply knowledge of the fundamentals and history of Intrusion Detection in order to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems
3. Analyze intrusion detection alerts and logs to distinguish attack types from false alarms

COURSE OUTCOMES

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

1. Build and design multi-tenancy SIEM Architecture.
2. Collect data / logs from any data sources (Cloud, Hybrid, On-Prem).
3. Leverage AI & ML (Machines Learning Models) for detection.
4. Build custom detection & analytics rules.
5. Build automation rules and playbooks for custom integration and/or response and remediation.

COURSE CONTENTS:

Unit 1: Introduction and Overview of SIEM: Overview and Key Aspects of SIEM Solutions
Architectural Design & RBAC: SIEM Solutions Models, Architecture Design (Single/Multi-tenancy) & RBAC, features of SIEM.

Unit 2:
Onboarding and Deployment Process, Data Collection, Normalization, Hunting & Analysis
Splunk- a SIEM software, alert status- types, IDS vs IPS, snort as an IPS, The history of Wi-Fi - the WLAN standard, Wireless vulnerability, Wireless vulnerabilities,

Unit 3: Detection Rules & Visualization, Threat Intelligence, Threat Intelligence vs. Threat Hunting
Threat Intelligence Lifecycle, Types of Threat Intelligence

Unit 4: Threat Detection: Detecting compromised user credentials, Tracking system changes, Detecting unusual behavior on privileged accounts, Secure cloud-based applications, Phishing detection, Monitoring loads and uptimes, Automation & SOAR, Query-based SIEM

Unit 5: Introduction, Risk Management, Communication, InfoSec Governance, InfoSec Policy Management, Decision making, Security & Usability, Security Culture, Compliance, Changing the Culture, Case Study

Text Books:

1. *Security Information and Event Management (SIEM) - O'Reilly*

2. *Information Security Policies, Procedures, and Standards - A Practitioner's Reference* by Douglas Landoll. CRC Press, 2016 ISBN: 1482-24589-2
3. *The Corporate Culture Survival Guide* by Edgar H. Schein. Jossey-Bass Press, 2009 ISBN: 0470-29371-3.

Reference Books:

1. Applied Network Security by Arthur Salmon, Warun Levesque, Michael McLafferty

INTRUSION DETECTION AND PREVENTION SYSTEMS

Course Code:	**CC313**	**Course Credits:**	**3**
Course Category:	**E1**	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**5U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**

COURSE OBJECTIVES

1. Understand when, where, how, and why to apply Intrusion Detection tools and techniques in order to improve the security posture of an enterprise.
2. Apply knowledge of the fundamentals and history of Intrusion Detection in order to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems
3. Analyze intrusion detection alerts and logs to distinguish attack types from false alarms

COURSE OUTCOMES

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

1. Explain the fundamental concepts of Network Protocol Analysis and demonstrate the skill to capture and analyze network packets.
2. Use various protocol analyzers and Network Intrusion Detection Systems as security tools to detect network attacks and troubleshoot network problems.
3. To know the intrusion detection and prevention policies

UNIT-I

History of Intrusion detection, Audit, Concept and definition , Internal and external threats to data, attacks, Need and types of IDS, Information sources Host based information sources, Network based information sources.

UNIT-II

Intrusion Prevention Systems, Network IDs protocol based IDs ,Hybrid IDs, Analysis schemes, thinking about intrusion. A model for intrusion analysis , techniques Responses requirement of responses, types of responses mapping responses to policy Vulnerability analysis, credential analysis non credential analysis

UNIT-III

Introduction to Snort, Snort Installation Scenarios, Installing Snort, Running Snort on Multiple Network Interfaces,Snort Command Line Options. Step-By-Step Procedure to Compile and Install Snort Location of Snort Files, Snort Modes Snort Alert Modes

UNIT-IV

Working with Snort Rules, Rule Headers, Rule Options, The Snort Configuration File etc. Plugins, Preprocessors and Output Modules, Using Snort with MySQL

UNIT-V

Using ACID and Snort Snarf with Snort, Agent development for intrusion detection, Architecture models of IDs and IPs.

TEXT BOOKS:

1. Rafeeq Rehman : “ Intrusion Detection with SNORT, Apache, MySQL, PHP and ACID,” 1st Edition, Prentice Hall , 2003.

REFERENCES:

1.Christopher Kruegel,Fredrik Valeur, Giovanni Vigna: “Intrusion Detection and Correlation Challenges and Solutions”, 1st Edition, Springer, 2005.

2.Carl Endorf, Eugene Schultz and Jim Mellander “ Intrusion Detection & Prevention”, 1st Edition, Tata McGraw-Hill, 2004.

3.Stephen Northcutt, Judy Novak : “Network Intrusion Detection”, 3rd Edition, New Riders Publishing, 2002.

4.T. Fahringer, R. Prodan, “A Text book on Grid Application Development and Computing Environment”. 6th Edition, KhannaPublihsers, 2012.

CRYPTOGRAPHY

Course Code:	**CC315**	**Course Credits:**	**3**
Course Category:	E1	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**5U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**

COURSE OBJECTIVES

1. Explain the objectives of information security
2. Explain the importance and application of each of confidentiality, integrity, authentication and availability
3. Understand various cries and understand the current legal issues towards information security.
4. Cryptographic algorithms.
5. Understand the basic categories of threats to computers and networks
6. Describe the public-key cryptosystem.

COURSE OUTCOMES

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

1. Students will be able to understand basic cryptographic algorithms, message and web authentication and security issues.
2. Ability to identify information system requirements for both of them such as client and server.

UNIT –I Attacks on Computers and Computer Security: Introduction, The need for security, Security approaches, Principles of security, Types of Security attacks, Security services, Security Mechanisms, A model for Network Security

Cryptography: Concepts and Techniques: Introduction, plain text and cipher text, substitution techniques, transposition techniques, encryption and decryption, symmetric and asymmetric key cryptography, stenography, key range and key size, possible types of attacks.

UNIT – II Symmetric key Ciphers: Block Cipher principles & Algorithms(DES, AES, Blowfish), Differential and Linear Crypt analysis, Block cipher modes of operation, Stream ciphers, RC4,Location and placement of encryption function, Key distribution

Asymmetric key Ciphers: Principles of public key cryp to systems, Algorithms(RSA, Diffie-Hellman, ECC), Key Distribution.

UNIT – III Message Authentication Algorithms and Hash Functions: Authentication requirements, Functions, Message authentication codes, Hash Functions, Secure hash algorithm, Whirlpool, HMAC, CMAC, Digital signatures, knapsack algorithm

Authentication Applications: Kerberos, X.509 Authentication Service, Public – Key Infrastructure, Biometric Authentication.

UNIT – IV EMail Security: Pretty Good Privacy, S/MIME IP Security: IP security overview, IP Security architecture, Authentication Header, Encapsulating security payload, Combining security associations, key management.

UNIT – V Web Security: Web security considerations, Secure Socket Layer and Transport Layer Security, Secure electronic transaction

Intruders, virus and Firewalls: Intruders, Intrusion detection, password management, virus and related threats, Countermeasures, Firewall design principles, types of firewalls

Case Studies on Cryptography and security: Secure Inter-branch Payment Transactions, Cross site Scripting Vulnerability, Virtual Elections

TEXT BOOKS:

1. Cryptography and Network Security : William Stallings, Pearson Education,4"‘ Edition
2. Cryptography and Network Security : Atul Kahate, Mc Graw Hill Edition

REFERENCE BOOKS

1. Cryptography and Network Security: C K Shyamala, N Harin i, Dr T R Padmanabhan, Wiley India, 1”
2. Cryptography and Network Security : Forouzan Mukhopadhyay, MC Graw Hill, 2"” Edition
3. Information Security, Principles and Practice: Mark Stamp, Wiley India.
4. Principles of Computer Security: WM.Arthur Conklin, Greg White, TMH
5. Introduction to Network Security: Neal Krawetz, CENGAGE Learning

BIOMETRIC SYSTEM SECURITY

CourseCode:	CC317	CourseCredits:	3
CourseCategory:CC	E1	Course(U/P)	U
CourseYear(U/P):U	3U	CourseSemester(U/P):	5U
No.ofLectures+Tutorials(Hrs/Week):	03+00	MidSem.ExamHours:	1
TotalNo.ofLectures(L+ T):30	45+00	EndSem.ExamHours:	3
COURSE OBJECTIVES			
1.To provide students with understanding of biometrics.			
2.Make awareness of different types of biometrics devices.			
3.Learn different process equipment and their working.			
4.Understanding of Security and standards applied to security.			
5.To understand attacks in security from malicious attackers.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Demonstrate knowledge of the basic physical and biological science and engineering Principles underlying biometric systems.			
2.Understand And analyze biometric systems at the component level and be able to analyze And design basic biometric system applications.			
3.Be able to work effectively in teams and express their work and ideas orally and in writing..			
4.Identify the sociological and acceptance issues associated with the design and Implementation of biometric systems.			
5.UnderstandvariousBiometricsecurityissues.			

UNIT I INTRODUCTION TO BIOMETRICS

Introduction- benefits of biometrics over traditional authentication systems -benefits of biometrics in identification systems-selecting a biometric for a system –Applications - Key biometric terms and processes-biometric matching methods-Accuracy In Biometric systems.

UNIT II PHYSIOLOGICAL BIOMETRIC TECHNOLOGIES

Physiological Biometric Technologies: Fingerprints - Technical description –characteristics - Competing technologies-strengths, weaknesses, deployment- Facialscan-Technical description-characteristics weaknesses-deployment - Iris scan - Technical description – characteristics - strengths – weaknesses –deployment-Retinal Vascular Pattern

UNIT III MEMORY & STORAGE MANAGEMENT

Technical description – characteristics - strengths – weaknesses – deployment - Hand scan - Technical description-characteristics - strengths – weaknesses deployment – DNA biometrics. Behavioral BiometricTechnologies:HandprintBiometrics -DNABiometrics.

UNIT IV SIGNATURE AND HANDWRITING TECHNOLOGY

Signature and handwriting technology - Technical description – classification – keyboard / key stroke dynamics- Voice – data acquisition - feature extraction - characteristics - strengths – weaknesses-deployment.

UNIT V MULTIBIOMETRICS

Multi biometrics and multi factor biometrics - two-factor authentication with passwords - tickets and tokens–executive decision-implementation plan.

TextBooks:

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi : “Biometrics -Identity verification in a network”, 1st Edition,WileyEastern,2002.
2. JohnChirilloandScottBlaul:“ImplementingBiometricSecurity”,1stEdition,WileyEasternPublication,2005

References:

[1.]JohnBerger:“BiometricsforNetworkSecurity”,1stEdition,Prentice Hall,2022

[2].JamesLPeterson,OperatingSystemsConcept,JohnWiley&SonsInc,the6Revedition,2007.
[3]. Deitel H. M., An Introduction to Operating Systems,PHI,NewAddisonWesley, 1990.
[4]. Stallings William, OperatingSystems,Delhi,1997.
[5]. S. Tanenbaum Modern Operating Systems, Pearson Education,3rd edition, 2007.
[6]. Nutt, Operating System, Pearson Education,2009.
[7].S.Tanenbaum,DistributedOperatingSystems,PrenticeHall,2ndedition,2007.

ETHICAL HACKING			
CourseCode:	**CC319**	**CourseCredits:**	**3**
CourseCategory:CC	**E1**	**Course(U /P)**	**U**
CourseYear(U/P):U	**3U**	**CourseSemester(U/P):**	**5U**
No.ofLectures+Tutorials(Hrs/Week):	**03+00**	**MidSem. ExamHours:**	**1**
TotalNo. ofLectures(L+T):30	**45+00**	**EndSem.ExamHours:**	**3**
COURSEOBJECTIVES			
1.To exploretheconceptsofsecuritytestingandtheknowledgerequiredtoprotectagainstthe hacker and attackers.			
2.Tounderstandreconnaissanceandthe publicly available tools used to gather information on Potential targets			
3.To discover the scanning techniques used to identify network systems open ports.			
4.To identify network system vulnerabilities and confirm their exploitability.			
5.To explore techniques for identifying web application vulnerabilities andattacks			
COURSEOUTCOMES			
At the end of the course the students should be able to:			
1.Understand the different terms of ethical hacking.			
2.Learn real life applications of network and security.			
3.Understands the use of different vulnerabilities and loop holes in the network.			
4.Learn different security hacking techniques like phishing, bruteforce etc.			
5.Perform implementation of protection mechanism in network.			

UNIT I INTRODUCTION TO ETHICAL HACKING

Introduction to Hacking – Important Terminologies,Penetration Test, VulnerabilityAssessmentsversusPenetrationTest,Pre-Engagement,RulesofEngagement,PenetrationTestingMethodologies OSSTMM,NIST,OWASP,CategoriesofPenetration Test, Types of Penetration Tests – Vulnerability Assessment Summary,Reports.

UNIT II INFORMATIONGATHERINGANDSCANNING

Information Gathering Techniques – Active Information Gathering, Passive Information Gathering,SourcesofInformationGathering,TracingtheLocation,Traceroute,ICMPTraceroute,TCPTraceroute, Usage, UDP Traceroute – Enumerating and Fingerprinting the Webservers , TargetEnumerationandPort ScanningTechniques,AdvancedFirewall/IDSEvadingTechniques

UNIT III NETWORKATTACKS

VulnerabilityDataResources–ExploitDatabases,NetworkSniffing,TypesofSniffing,MITMAttacks, Denial of Service Attacks,Hijacking Session with MITM Attack, SSL Strip: Stripping HTTPSTraffic,DNSSpoofing,ARPSpoofingAttackOverviewofBruteForceAttacks,TraditionalBruteForceAttackingSMTP, AttackingSQL Servers,Testingfor WeakAuthentication.

UNIT IV EXPLOITATION

IntroductiontoMetasploit,ReconnaissancewithMetasploit,PortScanning with Metasploit Compromising a Windows Host with Metasploit, Client Side Exploitation Methods,E–Mails with Malicious Attachments, Creating a Custom Executable, Creating a Backdoor with SET, PDF Hacking–Social Engineering Toolkit, Browser Exploitation, Hashing Algorithms.

UNIT V WIRELESS AND WEB HACKING:

Wireless Hacking – Introducing Aircrack, Network Using Aircracking, Causing Denialof Service on the Original AP, Web Hacking, Attacking the Authentication, BruteForce and Dictionary Attacks,Types of Authentication, Log-In ProtectionMechanisms,Captcha ValidationFlaw

TextBook-

1. **loch,“Ethical Hacking and Penetration Testing Guide”, CRCPress,2014.**

ReferenceBookBooks:

1.RafayBas:

1. KevinBeaver,“EthicalHackingforDummies”,SixthEdition, Wiley,2018.

2. JonErickson,“Hacking:TheArtofExploitation”,SecondEdition,Rogunix,2007.

ANALYSIS & DESIGN OF ALGORITHMS LAB			
Course Code:	CC381	Course Credits:	2
Course Category:	CC-P	Course (U / P)	U
Course Year (U / P):U	3U	Course Semester (U / P):	5U
No. of Lectures + Tutorials (Hrs/Week):	02(3 hrs)		
Total No. of Labs:	10	End Sem. Exam Hours:	3
COURSE OBJECTIVES			
1.Write sorting programs using Divide-and-Conquer techniques.			
2. Implement to find the minimum cost spanning tree and shortest path using different Greedy techniques			
3. Construct DFS, BFS programs and topological ordering using Decrease-and-Conquer technique			
4. Implement knapsack, travelling salesperson			
5.Design different searching & sorting techniques and finding the complexities.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Demonstrate Quick sort and Merge sort and calculate the time required to sort the elements.			
2.Implement the topological ordering of vertices, travelling salesman problem and Knapsack problem			
3.Construct programs to check graph is connected or not using BFS and DFS methods			
4.Implement programs on divide and conquer, decrease and conquer			
5.Experiment finding the minimum cost of spanning tree using Prim’s algorithms and shortest path using Dijkstra’ algorithm			

PRACTICALS

(Note: Use any programming tools like C/Java/Python to execute.) 1.Sort
a given set of elements :
(a)using the Quick sort method and also analyse it’s runtime complexity for different inputs.
(b)using merge sort method and also analyse it’s runtime complexity for different inputs.

2. Write a program to obtain the topological ordering of vertices in a given digraph.

3. Implement travelling salesman problem.
4.Implement the knapsack problem (0/1).
5. Print all the nodes reachable from a given starting node in a digraph using BFS method.
6.Check whether a given graph is connected or not using DFS method.
7. Write a program to implement binary search using divide and conquer
technique 8.Write a program to implement insertion sort using decrease and conquer
technique
9 . Find minimum cost spanning tree of a given undirected path using a Prim’s algorithm.
10. From a given vertex in a weighted connected graph, find shortest paths to other vertices using Dijkstra’s algorithm.

CRYPTOGRAPHY & DATA PRIVACY LAB			
Course Code:	**CC383**	**Course Credits:**	**2**
Course Category:	**CC-P**	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**5U**
No. of Labs (Hrs/Week):	**2(3 hrs)**	**Mid Sem. Exam Hours:**	
Total No. of Labs:	**10**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.To learn different commands for implementing encryption and decryption.			
2.To understand the implementation of Caesar cipher.			
3.To understand the encryption and decryption for XOR operation.			
4.To understand the working of wireless audit on a router.			
5. To demonstrate intrusion detection system.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Apply encryption and decryption on any input.			
2.Generate random numbers within a range.			
3.Apply an RSA algorithm with different values of p and q.			
4.Apply snort tool.			
5. Design New policies related to privacy methods			

List of Experiments:

1. To understand and illustrate the different commands used to implement encryption and decryption.
2. Write an encryption and decryption program for Caesar cipher.
3. Write a program in which encryption and decryption is done in one program without input.
4. Write a program in C++ to generate Pseudo Random numbers in a range.
5. Write a program in C++ for XOR Encryption and Decryption.
6. Write a program in C++ for Vernam Cipher.
7. Write a program in C++ for the RSA algorithm taking p and q randomly.
8. Working with KfSensor Tool for Creating And Monitoring Honeypot.
9. Working with NetStumbler to Perform Wireless Audit On Router.
10. Working with Snort Tool to Demonstrate Intrusion Detection Syste

MACHINE LEARNING USING PYTHON LAB			
Course Code:	**CC385**	**Course Credits:**	**2**
Course Category:	**CC-P**	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**5U**
No. of Labs (Hrs/Week):	**2(3 hrs)**	**Mid Sem. Exam Hours:**	
Total No. of Labs:	**10**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.To understand the basic concepts and techniques of Machine Learning through python programming.			
2.To develop skills of using recent machine learning packages for solving practical problems.			
3.To gain experience of doing independent study and research			
4.To understand the methods using in machine learning			
5. To demonstrate real time applications using python			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Familiarize Python			
2.Able to generate, analyze and interpret data using Python.			
3. Use Python to design and implement classifiers for machine learning applications.			
4.Implement an end to end Machine Learning System			
5. Design new programs related to machine learning methods			

List of Experiments:

1. Write a python program to compute Central Tendency Measures: Mean, Median, Mode Measure of Dispersion: Variance, Standard Deviation
2. Study of Python Basic Libraries such as Statistics, Math, Numpy and Scipy
3. Study of Python Libraries for ML application such as Pandas and Matplotlib
4. Write a Python program to implement Simple Linear Regression
5. Implementation of Multiple Linear Regression for House Price Prediction using sklearn
6. Implementation of Decision tree using sklearn and its parameter tuning
7. Implementation of KNN using sklearn
8. Implementation of Logistic Regression using sklearn
9. Implementation of K-Means Clustering
10. Performance analysis of Classification Algorithms on a specific dataset (Mini Project)

SEMESTER-VI

WEB DEVELOPMENT USING PHP			
Course Code:	**CC302**	**Course Credits:**	**3**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**6U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1. Describe the fundamentals of the web.			
2. Introduce the creation of static webpage using HTML			
3. Describe the function of JavaScript as a dynamic webpage creating tool			
4. Outline the principles behind using MySQL as a backend DBMS with PHP			
5.Describe the importance of CSS in web development			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Learn and use DHTML and AJAX. Learn the basics of JQuery.			
2. Learn about the major vulnerabilities facing web sites and some simple ways to reduce their likelihood			
3.Use a MySQL database with PHP to create database applications			
4.Design HTML pages and use basic JavaScript code to enhance the pages			
5.Develop a complete market-ready database-driven website with PHP and JavaScript and go through the basic phases of the software life cycle			

UNIT I INTRODUCTION

Internet Standards, Introduction to WWW, WWW Architecture, client and server, web server, web application basic pieces, working of a website, Internet Protocols, Overview of HTTP, HTTP request – response, Generations of dynamic web pages, Frontend and backend web development, web content management systems: Wordpress, Joomla, web development life cycle, Guidelines for Indian Government websites.

UNIT II BASICS OF HTML,CSS, JAVASCRIPT

HTML and HTML5: Introduction, TML Tags, Formatting and Fonts, Commenting Code, Anchors, Backgrounds, Images, Hyperlinks, Lists, Tables, Frames, HTML Forms. Cascading Style Sheet (CSS): Introduction, Basics of CSS, style types. JavaScript: Introduction, variables, operators, conditionals, looping and validation. Introduction to Jquery, Ajax and XML.

UNIT III INTRODUCTION TO PHP

PHP structure: basic syntax, variables, operators, multiline commands. Expression and control flow in PHP, PHP dynamic linking. PHP functions and Objects, PHP arrays, Practical PHP: Date and time functions, file handling, system calls. Accessing and manipulating databases using PHP, Error handling in PHP, generating images with PHP. Cookies, sessions and authentication.

UNIT IV INTRODUCTION TO FRAMEWORK

Introduction of MVC pattern models, MVC works, Configuration Codelgniter, setting up Codelgniter with apache, Environment eg. Enable mod_rewrite, Fetching data, saving and updating data, Deleting data, user defined function in model, Data Validation, controller function, interacting with views, controller variables and parameters, Redirection, Getting post data, working with configuration layout, creating custom layout, Element and helpers, storing data in cake session, Reading a session data, Delete data from session

UNIT V MYSQL - Databases, Tables, Columns, MySQL Data Type, SELECT, UPDATE and DELETE Statements,PHP and MySQL: Connecting from PHP to MySQL Database, Executing SQL Queries from PHP.

Text Books:

1. **Learning PHP, MySQL & JavaScript with JQUERY, CSS & HTML5: Robin Nixon (O'Reilly)**
2. Learning Web Design: A Beginner's Guide to (X)HTML, Style Sheets and Web Graphics: Jennifer Niederst Robbins (O'Reilly).

NETWORK DEFENSE FOR CYBER SECURITY			
Course Code:	**CC304**	**Course Credits:**	**3**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**6U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.Determine the various levels of a cybersecurity evaluation			
2.Recognize the various types of cyber-threats			
3.Acquire the skills needed to conduct a hands-on cybersecurity assessment			
4.Use the learned techniques to defend IT assets against cyber-threats			
5.Understand the network, system, and application risks and how to manage them			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Securing an IT infrastructure, examining and resolving security risks in networks and computer systems.			
2.Creating, testing, and evaluating secure application software.			
3. Developing policies and procedures for managing security risks in organizations.			
4.Identify network, system, and application vulnerabilities and implement the strongest possible security countermeasure			
5. Understand techniques used by hackers to penetrate computer networks and systems			

UNIT I
Network security and its working, what can be done with network security, advantages and disadvantages of network security, why do we need network security, Future scope for network security

UNIT II
Data security & why it is important, its considerations, types of data security controls, Cryptography, cryptography techniques and tools, Network security, working and need of cyber security

UNIT III
Phishing, its need and tools, Basics of cyber security, network topology, Algorithms and Cryptography, HTTP methods, authentication methods, security technologies

UNIT IV
Security architecture, email security gateways, network monitoring tools, network analysis, types of Ddos attacks, different protocols for network defense with cyber security

UNIT V Case studies and research articles related to network defense for cyber security.

Text Books:

1. Practical Malware Analysis. The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski,July 2017

2. The Code Book. The Science of Secrecy from Ancient Egypt to Quantum Cryptography by simon Singh,August 2016

Reference Books

1. Cyberwar. The Next Threat to National Security & What to Do About It by Richard A. Clarke, Robert Knake.

2. The Web Application Hacker's Handbook Finding and Exploiting Security Flaws by Dafydd Stuttard,August 2018

3. Open Source Intelligence Techniques. Resources for Searching and Analyzing Online Information by Michael Bazzell.

RISK MANAGEMENT & AUDIT			
Course Code:	**CC306**	**Course Credits:**	**4**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**6U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 15**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 15**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.To identify the IT Audit Process			
2.To analyse the risk assessment and IT Governance,			
3. To introduce Audit life Cycle			
4. To describe IT Audit standards & regulations			
5. Identify and analyze controls within the IT security framework			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Explain the role of IT Audit function within an organization			
2. Explain the audit process and the tasks within an Audit Area			
3. Understand risk methods and procedures in an audit perspective			
4.Understand risk management process and control practices in an audit contex			
5. students will learn the life cycle of auditing different IT systems including the operation system, database, computer network etc			

UNIT I

Investigates the principles of information systems audit, IT audit tools, audit procedures to help in detection and prevention of security breaches and fraud. Examines the solutions that can be used to prevent information loss or costly business interruptions, the role of information technology governance in business organizations, reporting requirements, and industry standards for IT Governance.

UNIT II

Risk and its management,Risk management framework,principles, Umbrella methodology for the management of risk,Types and sources of risk,Risk and the economic environment ,Corporate governance and organizational structure,External reporting and accounting Section ,The risk management process,A risk management framework ,Risk measurement tools and techniques

UNIT III

Identifying and assessing interest rate risk,Evaluating interest rate risk ,Managing interest rate risk,Interest rate risk management Instruments:short term,Interest rate risk management Instruments :longer term,Other risk issues,Treasury operational risk and controls,External risk reporting

UNIT IV

Risk assessment:risk analysis and evaluation,IT Audit Planning and Managing the IT Audit Function - Management of IT Auditing - Developing the IT Audit Plan,Auditing IT Governance Controls - Information Security Governance - Auditing IT Governance - IT Outsourcing

UNIT V Risk responses and risk treatment Introduction to risk treatment and risk response, the 4Ts, risk control techniques (PCDD), control of selected hazard risks, introduction to monitoring and review, insurance and risk transfer, business continuity planning (BCP)

Text Books:

1. Fundanentals of Information & Management Auditing,Christopher,wright,IT Governance Publishing,April 2016
2. Risk Management ,Macmillan foundation

Reference Books:

1.Auditing Risk Based Approach by Johnstone, Gramling, Rittenberg, Cengage September

2018 2.Risk-Based Auditing,Phil Grifiths,October 2018
3.Auditor's Risk Management Guide: Integrating Auditing and Erm ,by Paul J. Sobel ,January 2017

DIGITAL FORENSICS, AUDIT, & INVESTIGATIONS			
Course Code:	**CC308**	**Course Credits:**	**3**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**6U**
No. of Lectures + Tutorials (Hrs/Week):	**03 +00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.Overview of digital investigation and digital evidence			
2.To identify data Acquisition of physical storage devices			
3.To analyse file carving & documententation			
4.To examine Time, registry & password recovery			
5.To determine Email & database forensics			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Students will explain and properly document the process of digital forensics analysis.			
2.Students will gain an understanding of the tradeoffs and differences between various forensic tools.			
3.Students will understand the inner workings of file systems.			
4.Students will be able to create disk images, recover deleted files and extract hidden information.			
5.Students will be introduced to the current research in computer forensics. This will encourage them to define research problems and develop effective solutions.			

Unit I

Foundations of Digital Forensics, Digital Evidence, Increasing Awareness of Digital Evidence, Digital Forensics: Past, Present, and Future, Principles of Digital Forensics, Challenging Aspects of Digital Evidence, Following the Cyber trail. Language of Computer Crime Investigation, The Role of Computers in Crime.

Unit II

Conducting Digital Investigations-Digital Investigation Process Models, scaffolding for Digital Investigations, Applying the Scientific Method in Digital Investigations, Investigative Scenario: Security Breach. Handling a Digital Crime Scene- Published Guidelines for Handling Digital Crime Scenes, Fundamental Principles, Authorization

Unit III

Investigative Reconstruction with Digital Evidence- Equivocal Forensic Analysis, Victimology,Crime Scene Characteristics, Threshold Assessments. Axes to Pathological Criminals and Other Unintended Consequences, Modus Operandi, Technology and Modus Operandi, Motive and Technology, Current Technologies.

Unit IV

Digital Evidence as Alibi- Investigating an Alibi, Time as Alibi, Location as Alibi. ApplyingForensic Science to Computers- Preparation, Survey, Documentation, Preservation, Examination and Analysis, Reconstruction, Reporting.

Unit V Applying Forensic Science to Networks- reparation and Authorization, Identification,Documentation, Collection, and Preservation, Filtering and Data Reduction, Class/Individual Characteristics and Evaluation of Source, Evidence Recovery, Investigative Reconstruction, Reporting Results.

Text Books:

1. Digital evidence and computer crime: forensic science, computers and the Internet. Academic Press.Casey, E. (2011).

2. Computer forensics: computer crime scene investigation. Jones and Bartlett Publishers. Vacca, J. R. (2010).

Reference Books:

1. Computer forensics: incident response essentials.Pearson Education.Kruse II, W. G., & Heiser, J. G. (2001).

2. Nelson, B., Phillips, A., & Steuart, C. (2014). Guide to computer forensics and investigations. Cengage Learning.

3. Solomon, M. G., Rudolph, K., Tittel, E., Broom, N., & Barrett, D. (2011) Computer forensics jumpstart. John Wiley & Sons

DATA PRIVACY & DATABASE SECURITY			
Course Code:	**CC310**	**Course Credits:**	**3**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**6U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.To understand the fundamentals of security, and how it relates to information systems.			
2To identify risks and vulnerabilities in operating systems from a database perspective.			
3.To learn good password policies, and techniques to secure passwords in an organization			
4. To learn and implement administration policies for users.			
5.To understand the various database security models and their advantages or disadvantages.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Identify between authorized & unauthorized data observation.			
2.Examine unauthorized data modification.			
3.Ensure the data confidentiality.			
4.Identify security threats in database systems.			
5.Design and Implement secure database systems.			

UNIT I

Introduction:Introduction to Databases Security Problems in Databases Security Controls Conclusions,Security Models -l:Introduction Access Matrix Model Take-Grant Model Acten Model PN Model Hartson and Hsiao's Model Fernandez's Model Bussolati and Martella's Model for Distributed databases

UNIT II

Security Models -2:Bell and LaPadula's Model Biba's Model Dion's Model Sea View Model Jajodia and Sandhu's Model The Lattice Model for the Flow Control conclusion

UNIT III

Security Mechanisms:Introduction User ldcntification fit authentication Memory Protection Resource Protection Control Flow Mechanisms Isolation Security Functionalities in some Operating Systems Trusted Computer System Evaluation Criteria

UNIT IV

Security Software Design:Introduction A Methodological Approach to Security Software Design Secure Operating System Design Secure DBMS Design Security Packages Database Security Design

UNIT V

Statistical Database Protection & Intrusion Detection Systems: lntroduction, Statistics Concepts and Definitions Types of Attacks Inference Controls evaluation Criteria for Control Comparison. Introduction IDES System RETISS System ASES System Discovery

Text Books:

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

Reference Books:

1. Database security by alfred basta, melissa zgola, CENGAGE learning.
2. Data and Applications Security and Privacy by Pierangela Samarati,22 June 2015
3. Protecting Privacy in Data Release: 57 (Advances in Information Security)by Giovanni Livraga 9 October 2016

ELECTIVE 2

MOBILE SECURITY			
CourseCode:	**CC312**	**CourseCredits:**	**3**
CourseCategory:CC	**CC**	**Course(U /P)**	**U**
CourseYear(U/P):U	**3U**	**CourseSemester(U/P):**	**6U**
No.ofLectures+Tutorials(Hrs/Week):	**03+00**	**MidSem. ExamHours:**	**1**
TotalNo. ofLectures(L+T):30	**45+00**	**EndSem.ExamHours:**	**3**
COURSEOBJECTIVES			
1. To explore the concepts of security testing and the knowledge required to protect against the hacker and attackers.			
2. To understand reconnaissance and the publicly available tools used to gather information on potential targets			
3. To discover the scanning techniques used to identify network systems open ports.			
4. To identify network system vulnerabilities and confirm their exploitability			
5. To explore techniques for identifying web application vulnerabilities and attacks			
COURSE OUTCOMES			
1.To explore the concepts of security testing and the knowledge required to protect against the hacker and attackers.			
2.To understand and reconnaissance and the publicly available tools used to gather information on potential targets			
3.To discover the scanning techniques used to identify network systems open ports.			
4.To identify network system vulnerabilities and confirm their exploitability			
5.To explore techniques for identifying web application vulnerabilities and attacks			

UNIT I

Introduction to Mobile Security – Important Terminologies, Mobile Application Threat Model, Android SecurityMechanism, Security Issues in Wireless and Mobile Communications, Security Requirements in Wireless andMobile Communications, Security for Mobile Applications, Advantages and Disadvantages of Application – levelSecurity.

UNIT II

Security of Device, Network, and Server Levels: Mobile Devices Security Requirements, MobileWirelessnetworklevelSecurity,ServerLevelSecurity.ApplicationLevelSecurityinWirelessNetworks: Application of WLANs, Wireless Threats, Some Vulnerabilities and Attack Methods overWLANs, Security for 1G Wi-Fi Applications, Security for 2G Wi-Fi Applications, Recent SecuritySchemesforWi-FiApplications

UNIT III

Application Level Security in Cellular Networks: Generations of Cellular Networks, Security Issuesand Attacks in cellular networks, GSM Security for applications, GPRS Security for applications,UMTS security for applications, Security of UMTS Networks, 3G security for applications, Some ofSecurityandauthenticationSolutions.

UNIT IV

Application Level Security in MANETs: MANETs, Some applications of MANETs, MANET Features, SecurityChallengesinMANETs,SecurityAttacksonMANETs,ExternalThreatsforMANETapplications,InternalthreatsforMANET Applications, Some of the Security Solutions. Ubiquitous Computing, Need for NovelSecurity Schemes for UC, Security Challenges for UC,and Security Attacks on UC networks, Some of the security solutions for UC.

UNIT V

Data Center Operations - Security challenge, implement “Five Principal Characteristics of Cloud Computing, Datacenter Security Recommendations Encryption for Confidentiality and Integrity, Encrypting data at rest, Key Management Life cycle,Emerging Trends in Mobile Security,Cloud Encryption Standards.

TextBooks:

1. PallapaVenkataram,SatishBabu:“WirelessandMobileNetworkSecurity”,1stEdition,TataMcGrawHill,2010.
2. FrankAdelstein,K.S.Gupta:“FundamentalsofMobileandPervasiveComputing”,1stEdition,TataMcGrawHill2005.

Cloud Architecture and Security			
CourseCode:	**CC314**	**CourseCredits:**	**3**
CourseCategory:CC	**CC**	**Course(U /P)**	**U**
CourseYear(U/P):U	**3U**	**CourseSemester(U/P):**	**6U**
No.ofLectures+Tutorials(Hrs/Week):	**03+00**	**MidSem. ExamHours:**	**1**
TotalNo. ofLectures(L+T):30	**45+00**	**EndSem.ExamHours:**	**3**
COURSE OBJECTIVES			
1.To explore the concepts of cloud and security testing .			
2. To understand reconnaissance and the publicly available tools used to gather information on potential targets			
3. To discover the could computing techniques used to identify network systems open ports.			
4. To learn service management using cloud			
5. To explore cloud security techniques for identifying- vulnerabilities and attacks on the cloud			
COURSE OUTCOMES			
1.To explore the concepts of cloud and security testing .			
2. To understand reconnaissance and the publicly available tools used to gather information on potential targets			
3. To discover the could computing techniques used to identify network systems open ports.			
4. To learn service management using cloud			
5. To explore cloud security techniques for identifying- vulnerabilities and attacks on the cloud			

Unit 1 Overview of Computing Paradigm - Recent trends in Computing, Grid Computing, Cluster Computing, Distributed Computing, Utility Computing, Cloud Computing. Evolution of cloud computing, Business driver for adopting cloud computing

Unit 2 Introduction to Cloud Computing- Cloud Computing (NIST Model), Introduction to Cloud Computing, History of Cloud Computing, Cloud service providers, Properties, Characteristics & Disadvantages, Pros and Cons of Cloud Computing, Benefits of Cloud Computing, Cloud computing vs. Cluster computing vs. Grid computing, Role of Open Standards

Unit 3 Cloud Computing Architecture- Cloud computing stack, Comparison with traditional computing architecture (client/server), Services provided at various levels, How Cloud Computing Works, Role of Networks in Cloud computing, protocols used, Role of Web services Service Models (XaaS)- Infrastructure as a Service(IaaS), Platform as a Service(PaaS), software as a Service(SaaS), Deployment Models- Public cloud, Private cloud, Hybrid cloud, Community cloud

Unit 4 Infrastructure as a Service(IaaS) - Introduction to IaaS: IaaS definition, Introduction to virtualization, Different approaches to virtualization, Hypervisors, Machine Image, Virtual Machine(VM), Resource Virtualization: Server, , storage, Network-Virtual Machine(resource) provisioning and manageability, storage as a service, Data storage in cloud computing(storage as a service) -Examples Amazon EC2- Renting, EC2 Compute Unit, Platform and Storage, pricing, customers Eucalyptus

Platform as a Service(PaaS) - Introduction to PaaS, What is PaaS, Service Oriented Architecture (SOA), Cloud Platform and Management- Computation, Storage, Examples- Google App Engine, Microsoft Azure, SalesForce.com's Force.com platform

Software as a Service(PaaS) - Introduction to SaaS: Web services, Web 2.0, Web OS, Case Study on SaaS

Unit 5 Service Management in Cloud Computing- Service Level Agreements(SLAs), Billing & Accounting, Comparing Scaling Hardware: Traditional vs. Cloud, Economics of scaling: Benefitting enormously, Managing Data-

Looking at Data, Scalability & Cloud Services, Database & Data Stores in Cloud, Large Scale Data Processing

Cloud Security - Infrastructure Security, Network level security, Host level security, Application level security, Data security and Storage, Data privacy and security Issues, Jurisdictional issues raised by Data location, Identity & Access Management, Access Control, Trust, Reputation, Risk, Authentication in cloud computing, Client access in cloud, Cloud contracting Model, Commercial and business considerations

Case Study on Open Source & Commercial Clouds -Eucalyptus, Microsoft Azure, Amazon EC2

Reference Books

- *Cloud Computing Bible,* Barrie Sosinsky*, Wiley-India,* 2010
- *Cloud Computing: Principles and Paradigms,* Editors: Rajkumar Buyya, James Broberg, Andrzej M. Goscinski*, Wile,* 2011
- *Cloud Computing: Principles, Systems and Applications, Editors:* Nikos Antonopoulos, Lee Gillam*, Springer,* 2012
- *Cloud Security: A Comprehensive Guide to Secure Cloud Computing,* Ronald L. Krutz, Russell Dean Vines*, Wiley-India,* 2010

Principles of Secure Coding			
CourseCode:	CC314	CourseCredits:	3
CourseCategory:CC	CC	Course(U /P)	U
CourseYear(U/P):U	3U	CourseSemester(U/P):	6U
No.ofLectures+Tutorials(Hrs/Week):	03+00	MidSem. ExamHours:	1
TotalNo. ofLectures(L+T):30	45+00	EndSem.ExamHours:	3
COURSE OBJECTIVES			
1.To describe how to use techniques that mimic formal methods to improve the robustness and security of programs.			
2. To Differentiate between robust programming and secure programming and generalize from philosophies of "what to watch out for" and "where to look" to specific situations.			
3. to compare and contrast formal, informal, and ad hoc programming methods.			
4. To Explain the issues that can arise from fragile programming.			
5. To explain what can go wrong in fragile code and be able to write a robust version of fragile code			
COURSE OUTCOMES			
1. To describe how to use techniques that mimic formal methods to improve the robustness and security of programs.			
2. To Differentiate between robust programming and secure programming and generalize from philosophies of "what to watch out for" and "where to look" to specific situations.			
3. to compare and contrast formal, informal, and ad hoc programming methods.			
4. To Explain the issues that can arise from fragile programming.			
5. To explain what can go wrong in fragile code and be able to write a robust version of fragile code			

Unit 1 Introduction
the key concepts in secure programming including typical problems and procedures. Differentiate between robust programming and secure programming and generalize from philosophies of "what to watch out for" and "where to look" to specific situations.

Unit 2- Secure Programming Philosophy

Introduction, The Philosophy of Secure Programming, Defining Secure Programming, Robust vs. Secure Programming, Security Policies and Procedures, Secure Programming General Philosophy, Checking Design and Implementation, Where to Look for Vulnerabilities.

Unit 2 Secure Programming Design Principles
Introduction, Secure Programming Design Principles Overview, Principle of Least Privilege, Fail-Safe Defaults, Principle of Economy of Mechanism, Principle of Complete Mediation, Separation of Privilege Principle, Principle of Open Design, Principle of Least Common Mechanism, Principle of Least Astonishment, Secure Programming Design Principles Summary,

Unit 3 Robust Programming
Introduction, Robust Programming Overview, Robust Programming Basic Principles, An Example Of Fragile Code, Error Handling1, Cohesion, New Interfaces, and Token Generation, Token Generation and Interpretation, Creating and Deleting a Queue, Adding and Removing Elements to a Queue.

Unit 4- Methods for Robustness

Methods for Robustness Overview, Methods Overview: Formal, Informal, and Ad Hoc Methods, Overview of Formal Methods, Login Program Example, Incorporating Hierarchical Decomposition Methodology, Login Program: Authenticating a User, Login Program: Preconditions and Postconditions.

Text books

1. Engineering Safe and Secure Software Systems (Artech House Information Security and Privacy), by C. Warren Axelrod (Buy here) ...
2. The Software Vulnerability Guide (Programming Series) by Herbert H. Thompson and Scott G. ...
3. Secure Coding: Principles and Practices by Mark G. Graff and Kenneth R.

INFORMATION WARFARE			
CourseCode:	CC318	CourseCredits:	3
CourseCategory:CC	E2	Course(U/P)	U
CourseYear(U/P):U	3U	CourseSemester(U/P):	6U
No.ofLectures+Tutorials(Hrs/Week):	03+00	MidSem.ExamHours:	1
TotalNo.of Lectures(L+T):30	45+00	EndSem.ExamHours:	3

COURSE OBJECTIVES

1. Explain the theory of data, information and knowledge as they pertain to information warfare.
2. Apply strategies of using information as a weapon and a target.
3. Apply the principles of offensive and defensive information warfare for a given context.
4. Demonstrate appropriate techniques to gather intelligence from a variety of sources to support a position / objective.
5. Discuss the social, legal and ethical implications of information warfare.

COURSE OUTCOMES

At the end of thecourse the students should beable to:

1. Evaluate contemporary information warfare concepts for their application in a corporate environment.
2. Understand and describe how tapping into the emotional component of an idea can spark a revolt.
3. Outline the different types of means and methods used in digital influence & manipulation operations.
4. Examine and propose how influence operations focus on manipulating the psychology of targets through strategic communication.
5. Analyze different case studies on past adversarial IO campaigns to determine how informational power is created and leveraged.

UNIT I INTRODUCTION TO INFORMATION WARFARE

The nature of information, data, and knowledge, The use of information as a weapon, The concept of information as a target, Corporate espionage, Information Assurance, Attack strategies, Swarming as an attack strategy, National, criminal, and military information warfare.

UNIT II CYBER TERRORISM

Social, legal and ethical aspects of information warfare including Terrorism Acts, Cyberterrorism, Contemporary issues in Information Warfare, e.g. Individual Information Warfare, Critical Infrastructure Protection.

UNIT III THE INFORMATION WARFARE ARSENAL AND TACTICS OF TERRORISTS AND ROGUES

The Terrorist profile, the dark world of the cyber underground, new tools of terrorism, information warfare, Arsenal and Tactics of private companies.

UNIT IV ROLE OF CYBER IN MILITARY DOCTRINE

Russian Federation, FEP ,Information wars, RF Military Policy, Art of Misdirection China Military Doctrine ,Anti-access Strategies , 36 Stratagems , US Military Doctrine

UNIT V RUSSIAN FEDERATION : INFORMATION WARFARE FRAMEWORK

Russian Government Policy, Laws and Amendments, Government Structures, Russian Military of Defence ,Administrative Changes, Electronic Warfare Troops , Military Units , Russian Federation Ministry of Communications and Mass Communications US Department of Defence Cyber Command and Organizational.

Text Books:

1. Inside Cyber Warfare: Mapping the Cyber Underworld by Jeffrey Carr, 2nd edition, O,Reilly
2. Cyberdeterrence and Cyberwar by Martin C. Libicki.

ReferenceBooks:

1. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.
2. Information Warfare and Security by Dorothy F. Denning, Addison Wesley.
3. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform.
4. Data Privacy Principles and Practice by Natraj Venkataramanan and Ashwin Shriram, CRC Press.
5. Information Security Governance, Guidance for Information Security Managers by W. KragBrothy, 1st Edition, Wiley Publication.

Social Network Security			
CourseCode:	**CC320**	**CourseCredits:**	**3**
CourseCategory:CC	**E2**	**Course(U/P)**	**U**
CourseYear(U/P):U	**3U**	**CourseSemester(U/P):**	**6U**
No.ofLectures+Tutorials(Hrs/Week):	**03+00**	**MidSem.ExamHours:**	**1**
TotalNo.of Lectures(L+T):30	**45+00**	**EndSem.ExamHours:**	**3**

COURSEOBJECTIVES
1. Understand the basic terminologies related to cyber security and current cyber security threat landscape.
2. Understanding about the Cyber warfare and necessity to strengthen the cyber security of end user machine, critical IT and national critical infrastructure.
3. Able to appreciate various privacy and security concerns on online Social media.
4. Understand the reporting procedure of inappropriate content, underlying legal aspects and best practices for the use of Social media platforms.
5.Understanding of security&protectionin Social media.

COURSE OUTCOMES
Attheendofthecoursethestudentsshouldbeableto:
1. Understand the aspects related to personal data privacy and security.
2. Get insight into the Data Protection Bill,2019 and data privacy and security issues related to Social media platforms.
3. Analyse and evaluate existing legal framework and laws on cyber security.
4. Will be able to use basic tools and technologies to protect their devices.
5. Understand the basic security aspects related to Computer and Mobiles.

UNIT I SOCIAL MEDIA OVERVIEW

Introduction to Social networks. Types of Social media, Social media platforms, Social media monitoring, Hashtag, Viral content, Social media marketing, Social media privacy, Challenges, opportunities and pitfalls in online social network,

UNIT II SECURITY ISSUES IN SOCIAL MEDIA

Security issues related to social media, Flagging and reporting of inappropriate content, Laws regarding posting of inappropriate content, Best practices for the use of Social media, Case studies.

UNIT III DATA PRIVACY AND DATA SECURITY

Defining data, meta-data, big data, nonpersonal data. Data protection, Data privacy and data security, Personal Data Protection Bill and its compliance, Data protection principles, Big data security issues and challenges, Data protection regulations of other countries- General Data Protection Regulations(GDPR),2016 Personal Information Protection and Electronic Documents Act (PIPEDA)., Social media- data privacy and security issues.

UNIT IV SEMANTIC TECHNOLOGY FOR SOCIAL NETWORK ANALYSIS

Introduction To Ontology Based Knowledge Representation – Ontology Languages for the Semantic Web – Rdf and Owl – Modeling Social Network Data – Network Data Representation, Ontological Representation of Social Individuals and Relationships -Aggregating and Reasoning With Social Network Data – Advanced Representations**.**

UNIT V DIGITAL DEVICES SECURITY , TOOLS AND TECHNOLOGIES FOR CYBER SECURITY

End Point device and Mobile phone security, Password policy, Security patch management, Data backup, Downloading and management of third party software, Device security policy, Cyber Security best practices, Significance of host firewall and Ant-virus, Management of host firewall and Anti-virus, Wi-Fi security,Configuration of basic security policy and permissions.

ReferenceBooks:

1. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd.
2. Information Warfare and Security by Dorothy F. Denning, Addison Wesley.
3. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform.
4. Data Privacy Principles and Practice by Natraj Venkataramanan and Ashwin Shriram, CRC Press.
5. Information Security Governance, Guidance for Information Security Managers by W. KragBrothy, 1st Edition, Wiley Publication.

WEB DEVELOPMENT USING PHP LAB			
Course Code:	**CC382**	**Course Credits:**	**2**
Course Category:	**CC-P**	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**6U**
No. of Labs (Hrs/Week):	**02(3 hrs)**		
Total No. of Labs:	**10**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1. Understand best technologies for solving web client/server problems using PHP			
2. Analyse & design real time web applications			
3. Use PHP for dynamic effects and to validate form input entry			
4.Analyze & Develop to Use appropriate client-side or Server-side applications			
5. To develop and deploy real time web applications in web servers and in the cloud			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1. Develop a dynamic webpage by the use of java script and DHTML.			
2. Write a well formed / valid XML document using PHP			
3. Connect a java program to a DBMS and perform insert, update and delete operations on DBMS table using PHP.			
4. Draft a server side application called Servlet to catch form data sent from client, process it and store it on database using PHP			
5. Create a server side application to catch form data sent from client and store it on database using PHP			

List of Experiments:

1. Basic HTML Tags,Table Tags,List Tags,Image Tags, Forms .
2. Implement forms using HTML,FRAMES,CSS.
3. Install the following on local machine
   - Apache web server
   - Tomcat application server locally,
   - Install MySQL
   - PHP and configure it to work with Apache web server and MySQL
4. To create an email id for receive and send pictures, documents .
5. To create a simple web file to demonstrate the use of different tags.
6. To create an html web with different types of frames such as floating frame, navigation frame & mixed frame.
7. Write a PHP program to store current date-time in a COOKIE and display the ‘Last visited on’ date- time on the web page upon reopening of the same page.
8. Write a PHP program to store page views count in SESSION, to increment the count on each refresh, and to show the count on web page.
9. Create a XHTML form with Name, Address Line 1, Address Line 2, and E-mail text fields. On submitting, store the values in MySQL table.Retrieve and display the data based on Name.
10. Using PHP and MySQL, develop a program to accept book information viz. Accession number, title, authors, edition and publisher from a web page and store the information in a database and to search for a book with the title specified by the user and to display the search results with proper headings.

NETWORK DEFENSE FOR CYBER SECURITY LAB			
Course Code:	**CC384**	**Course Credits:**	**2**
Course Category:	**CC-P**	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**6U**
No. of Labs (Hrs/Week):	**2(3 hrs)**	**Mid Sem. Exam Hours:**	
Total No. of Labs:	**10**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.Exhibit knowledge to secure corrupted systems, protect personal data, and secure computer networks in an Organization.			
2. Practice with an expertise in academics to design and implement security solutions			
3. Understand key terms and concepts in Cryptography, Governance and Compliance.			
4. Develop cyber security strategies and policies			
5. Understand principles of web security and to guarantee a secure network by monitoring and analyzing the nature of attacks through cyber/computer forensics software/tools.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Measure the performance and troubleshoot cyber security systems.			
2. Implement cyber security solutions and use of cyber security, information assurance, and cyber/computer forensics software/tools			
3. Comprehend and execute risk management processes, risk treatment methods, and key risk and performance indicators			
4. Design and develop a security architecture for an organization.			
5.Design operational and strategic cyber security strategies and policies.			

List of Experiments:

1. Study of different wireless network components and features of any one of the Mobile Security Apps.
2. To understand different concepts related to commands, software used for implementing and the background of cyber security.
3. Study of the features of firewalls in providing network security and to set Firewall Security in windows.
4. Steps to ensure Security of any one web browser (Mozilla Firefox/Google Chrome).
5. Study of different types of vulnerabilities for hacking websites / Web Applications.
6. Analysis of the Security Vulnerabilities of E-commerce services.
7. Analysis the security vulnerabilities of E-Mail Applications
8. To develop some method for securing the confidential information of an organization.
9. To understand the need and applications where network defense is must and to be implemented as soon as possible.
10. To understand the future scope of network defense.

DATA PRIVACY & DATABASE SECURITY LAB			
Course Code:	**CC386**	**Course Credits:**	**2**
Course Category:	**CC-P**	**Course (U / P)**	**U**
Course Year (U / P):	**3U**	**Course Semester (U / P):**	**6U**
No. of Labs (Hrs/Week):	**2(3 hrs)**	**Mid Sem. Exam Hours:**	
Total No. of Labs:	**10**	**End Sem. Exam Hours:**	**3**

COURSE OBJECTIVES
1.To provide a good foundation in mathematics, sciences and engineering fundamentals required to solve engineering problems
2. To provide analytical and problem solving skills to design algorithms, other hardware / software systems
3.To facilitate graduates to get familiarized with the art software / hardware tools, imbibing creativity and innovation
4. To inculcate professional ethics, inter-personal skills to work in a multi-cultural team.
5. To facilitate & learn employment skills in industry and / or to pursue postgraduate studies with an appreciation for lifelong learning

COURSE OUTCOMES
At the end of the course the students should be able to:
1.An ability to apply knowledge of mathematics, science and engineering to develop and analyze computing systems
2.An ability to apply knowledge of mathematics, science and engineering to develop and analyze computing systems
3.An ability to perform experiments to analyze and interpret data for different applications.
4. An ability to design, implement and evaluate computer-based systems, processes, components or programs to meet desired needs within realistic constraints of time and space.
5. An ability to use current techniques, skills and modern engineering tools necessary to practice as an IT professional.

List of Experiments:

1. Introduction of Cryptool Software
2. To understand steps and concepts to generate digital signatures.
3. To understand the concepts of hash value and steps to generate hash value.
4. To generate HMAC values using CrypTool.
5. Write a program for Diffie Hellman Key Exchange.
6. Write a program for the RSA algorithm by inputting the value of two prime numbers.
7. To understand the data discovery and classification for security with a single program.
8. To work with intrusion prevention and detection systems.
9. To understand the concept of data loss prevention.
10. To implement some new method with which data can be secured using previous study

SEMESTER-VI

BLOCKCHAIN TECHNOLOGY			
Course Code:	**CC401**	**Course Credits:**	**3**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**4U**	**Course Semester (U / P):**	**7U**
No. of Lectures + Tutorials (Hrs/Week):	**03 +00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**

COURSE OBJECTIVES
1. To understand the technology behind blockchain
2. Explain distributed Consensus, and Consensus in Bitcoin
3. Discuss Permissioned Blockchain, and Hyperledger Fabric
4. To comprehend the issues related to blockchain
5. To study the real-world applications of blockchain

COURSE OUTCOMES
At the end of the course the students should be able to:
1. Describe the basic concept of Blockchain, Crypto Primitives, Bitcoin Basics
2. Identify the area in which they can apply permission or permission less blockchain.
3. Apply Block chaining concept in various applications.
4.Design and implement new ways of using blockchain for applications other than cryptocurrency
5. Recognize the underlying technology of transactions, blocks, proof-of-work, and consensus building

UNIT I
Introduction to Blockchain: What is Blockchain, Public Ledgers, Blockchain as Public Ledgers, Bitcoin, Blockchain 2.0, Smart Contracts, Block in a Blockchain, Transactions, Distributed Consensus, The Chain and the Longest Chain, Cryptocurrency to Blockchain 2.0, Permissioned Model of Blockchain

UNIT II
Basic Crypto Primitives: Cryptographic Hash Function, Properties of a hash function, Hash pointer and Merkle tree, Digital Signature, Public Key Cryptography, A basic cryptocurrency.
Bitcoin Basics: Creation of coins, Payments and double spending, FORTH – the precursor for Bitcoin scripting, Bitcoin Scripts, Bitcoin P2P Network, Transaction in Bitcoin Network, Block Mining, Block propagation and block relay.

UNIT III
Distributed Consensus: Why Consensus, Distributed consensus in open environments, Consensus in a Bitcoin network.
Consensus in Bitcoin: Bitcoin Consensus, Proof of Work (PoW) – basic introduction, Hashcash PoW, Bitcoin PoW, Attacks on PoW and the monopoly problem, Proof of Stake, Proof of Burn and Proof of Elapsed Time. The life of a Bitcoin Miner, Mining Difficulty, Mining Pool.

UNIT IV
Permissioned Blockchain: Permissioned model and use cases, Design issues for Permissioned blockchains, Execute contracts, State machine replication, Consensus models for permissioned blockchain, Distributed consensus in closed environment, Paxos, RAFT Consensus, Byzantine general problem.Blockchain Components and Concepts: Actors in a Blockchain, Components in Blockchain design, Ledger in Blockchain.

UNIT V

Hyperledger Fabric – Transaction Flow: Fabric Architecture, Transaction flow in Fabric.
Hyperledger Fabric Details: Ordering Services, Channels in Fabric, Fabric Peer and Certificate Authority.
Fabric – Membership and Identity Management: Organization and Consortium Network, Membership Service Provide, Transaction Signing.

Text Books

1. Nitin Gaur, Luc Desrosiers, Venkatraman Ramakrishna, Petr Novotny, Salman Baset, Anthony O'Dowd.Hands-On Blockchain with Hyperledger: Building decentralized applications with Hyperledger Fabric and Composer. Packt Publishing Ltd.
2. Bellaj Badr, Richard Horrocks, Xun (Brian) Wu. Blockchain By Example: A developer's guide to creating decentralized applications using Bitcoin, Ethereum, and Hyperledger. Packt Publishing Ltd, 2018.

Reference Books

1. Vikram Dhillon, David Metcalf, Max Hooper. Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You. Apress.
2. Mayukh Mukhopadhyay Ethereum Smart Contract Development: Build blockchain-based decentralized applications using solidity. Packt Publishing Ltd.

AI ENABLED CYBER SECURITY			
Course Code:	**CC403**	**Course Credits:**	**3**
Course Category:	**CC**	**Course (U / P)**	**U**
Course Year (U / P):	**4U**	**Course Semester (U / P):**	**7U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1. To Analyze and improving cybersecurity posture			
2. To understand AI & CS systems are being trained to identify malware, execute pattern recognition			
3. To study better Vulnerability Management			
4. To understand the concepts of AI by Adversaries			
5. AI enabled cyber security.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Insight into the main methods used in artificial intelligence (AI) and Cyber security			
2.Students are able to gain knowledge AI and CS important for cybersecurity			
3.Students will able to use CS/ML Security in today lives.			
4.Students will be able to explain CS/ML Used in Security.			
5. knowledge of the historical development of the field of Cyber Security enabled AI.			

UNIT I Fundamentals of Cyber Security & AI

Identity, authentication, confidentiality, privacy, anonymity, availability and integrity,deep learning fundamentals from a security perspective.fundamentals of AI and how AI can solve problems in the cyber security space,Examples of companies using AI for Security, such as Cylance and FireEye.

UNIT II Secure Web

Security using AI techniques for injection using regular expressions,identifying patterns and matching with existing scores,Vulnerability measures,statistical patterns and Bayesian statistics,statistical distributions

UNIT III Cyber Security Threat

Web Application Security**,**Injection,Broken authentication,Sensitive data exposure,XML External Entities (XXE),Broken access control,Security misconfigurationCross-Site Scripting (XSS),Insecure deserialization,Using components with known vulnerabilitiesInsufficient logging and monitoring.

UNIT IV Securing Infrastructure

Security issues in systems,secure software design, secure programming, and security testing, covering security analysis as well as the secure development of software-based systems both on architectural level and system level

UNIT V Impact of AI on Cyber Security

Threat hunting in memory, file system and network data,cyber threat hunting and digital investigation, introductory analysis of malicious programs.,KNN (K - Nearest Neighbours) for threat visualisers,Isolation forest for anomaly detection,LSTM for multi-vector correlation DBSCAN for riskware detection and fraudLSTM (Autoencoder) for endpoint protection

Text Books:

1. Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies
Alessandro Parisi , 1st edition (2 August 2019)

2. AI-Enabled Threat Detection and Security Analysis,by Hadis Karimipour (Editor), Farnaz Derakhshan 3 August 2021

Reference Books:

1. Cyber Security Incident Response Guide. – Alan J White,
2. Cybersecurity – Attack and Defense Strategies: Counter Modern Threats and Employ State-of-the-Art Tools and Techniques to Protect Your Organization Against Cybercriminals. – Yuri Diogenes, Erdal Ozkaya,August 2019
3. Cybersecurity: An Essential Guide to Computer and Cyber Security for Beginners, Including Ethical Hacking, Risk Assessment, Social Engineering, Attack and Defense Strategies, and Cyberwarfare. – Latest Edition

ELECTIVE 3

PHYSICAL SECURITY OF IT INFRASTRUCTURE			
Course Code:	CC405	Course Credits:	3
Course Category:	E3	Course (U / P)	U
Course Year (U / P):	4U	Course Semester (U / P):	7U
No. of Lectures + Tutorials (Hrs/Week):	03 + 00	Mid Sem. Exam Hours:	1
Total No. of Lectures (L + T):	45 + 00	End Sem. Exam Hours:	3
COURSE OBJECTIVES			
1. To understand physical security threats			
2. Understand different disasters and recovery			
3. To understand securing of infrastructure			
4. Understand data encryption and cryptography			
5. Understanding assessments and audit			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1. To apply knowledge to access physical threats and security			
2. Implement how measure risk and avoid disaters			
3. Solve and implement data encryption			
4. Secure the infrastructure from attacks and have countermeasures			
5. Apply assessments and audits			

UNIT 1 Physical security essential

Overview , Physical Security Threats, Physical Security Prevention and Mitigation Measures, Recovery from Physical Security, Breaches,Threat Assessment, Planning, and Plan Implementation, Example: A Corporate Physical Security Policy,Integration of Physical and Logical Security, Physical Security Checklist

UNIT 2 Disaster Recovery and Biometrics

Measuring Risk and Avoiding disaster , The business assessment (BIA), Biometric system architecture ,Using biometric systems , cyber warfare model , foundation of security

UNIT 3 Securing the infrastructure

Communication security goals , attacks and countermeasures , Infrastructure weakness : DAC , MAC, and RBAC , Strengthening the infrastructure : authentication systems

UNIT 4 Data Encryption

Need for cryptography , mathematical prelude to cryptography , classical cryptography , modern symmetric ciphers , algebraic structure , Elliptic curve cryptosystems , TDEA Block cipher

UNIT 5 Assessments and Audit

Assessing vulnerabilities and Risk : penetration testing and vulnerability assessments , Risk management : Quantitative risk measurements , Advance data encryption , RSA cryptosystems

Text Books :

1. Cyber Security and IT Infrastructure Protection by John Vacca
2. Information Technology Infrastructure And Its Management By Trivedi, Munesh

Reference Book:

1. Cyber-Physical Security Protecting Critical Infrastructure at the State and Local Level 2021
2. Critical Infrastructure Security and Resilience Theories, Methods, Tools and Technologies 2019

NISTA800-53 (Security control)			
Course Code:	**CC407**	**Course Credits:**	**3**
Course Category:	**E3**	**Course (U / P)**	**U**
Course Year (U / P):	**4U**	**Course Semester (U / P):**	**7U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1 Understanding Security control			
2 To learn the fundamentals			
3 To understand the different security and privacy assessment procedures			
4 To learn 800-53			
5 To learn 800-53 controls			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1 Able to analyze different security controls			
2 Able to clarify the fundamentals			
3 Able to understand other assessment procedures			
4 Able to define 800-53			
5 Able to know various controls of 800-53			

UNIT I Introduction to Security Control

Introduction to security control, Physical control, Technical control, Administrative control

UNIT II Fundamentals

Assessments within the system development life cycle, control structure and organization, Building an effective assurance case, and Assessment procedures: assessment objects, methods, and objectives

UNIT III Security and Privacy Assessment Procedures

Access control, Awareness and training, Audit and Accountability, Assessment, authorization and monitoring, comfiguration management , contingency planning, identification and authentication

UNIT IV Getting to know 800-53

Introduction, Risk management framework, How NIST explains 800-53, To Rev5 and Beyond

UNIT V Understanding 800-53 controls

Control Families, Anatomy of a control, Control Selection, Common, System and Hybrid controls, Organization defined variables, System Security Plan, Control Assessment, POA&M

Text Book

1. **Internet Security Control System Paperback – Import, 16 September 2010**

   by Benny Benyamin Nasution (Author), Asad I Khan (Author), Bala S Srinivasan (Author)

Reference Book

1. **Force, J. T. (2017).** ***Security and privacy controls for information systems and organizations*** **(No. NIST Special Publication (SP) 800-53 Rev. 5 (Draft)). National Institute of Standards and Technology.**
2. Tariq, M. I., Tayyaba, S., Ashraf, M. W., Rasheed, H., & Khan, F. (2016). Analysis of NIST SP 800-53 rev. 3 controls effectiveness for cloud computing. *computing*, *3*(4).

OPERATING SYSTEM SECURITY			
Course Code:	CC409	Course Credits:	3
Course Category:	E3	Course (U / P)	U
Course Year (U / P):	4U	Course Semester (U / P):	7U
No. of Lectures + Tutorials (Hrs/Week):	03 + 00	Mid Sem. Exam Hours:	1
Total No. of Lectures (L + T):	45 + 00	End Sem. Exam Hours:	3
COURSE OBJECTIVES			
1. To identify and assess current and anticipated security risks and vulnerabilities			
2. To monitor, evaluate and test security conditions and environment			
3. To develop an organizational security plan that provides for periodic reviews of security policies and procedures			
4. To Implement security plan and monitor solutions			
5. To understand Respond to any breach of security and adjust organizational security plan accordingly			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1. Monitors and corrects performance: Distinguishes trends, predicts impacts on system operations, diagnoses systems performance, and corrects malfunctions			
2. Detect and protect systems from malicious softwares			
3. Implement firewall on different OS			
4. Evaluate tools and technologies for use in protecting the network and individual network systems			
5. Implement knowledge taken from case studies			

UNIT 1 Operating Systems Security
What Is Operating System and Network Security? ,Operating Systems and Security,Computer Networks and Security Careers in Information Security,Why Security Is NecessaryProtecting Information and Resources ,Ensuring Privacy ,Facilitating WorkflowAddressing Security Holes or Software Bugs Compensating for Human Error or Neglect ,Cost Factors ,Types of Attacks ,Hardening your systems

UNIT 2 Viruses, Worms, and Malicious Software
How Viruses, Worms, and Trojan Horses Spread , Virus , worms, trojan horse , typical methods used by malicious software , protecting an OS from malicious software , Different Encryption methods , different authentication methods , Attacks on encryption and authentications

UNIT 3 Account based security
Account Naming and Security Policies ,Creating User Accounts :Windows 2000 Professional and Windows XP Professional ,Windows 2000 Server and Windows Server 2003 ,Red Hat Linux 9x ,NetWare 6.x,Mac OS X ,Setting Account Policies and Configuring Logon Security

UNIT 4 Firewalls and Border security
An Overview ofTCP UDP and IP ,Understanding Transmission Control Protocol (TCP) ,Understanding User Datagram Protocol (UDI) , Understanding How the Internet Protocol (IP) Works ,How IP Addressing Works ,Using a Subnet Mask ,Creating Subnetworks
Border and Firewall Security ,Packet Filtering ,Network Address Translation (NAT)

UNIT 5 Case studies

Case Study Solaris Trusted Extensions :Glenn Faden and Christoph Schuba, Sun Microsystems, Inc , Trusted Extensions Access Control, Solaris Compatibility , Trusted Extensions Mediation , Process Rights Management (Privileges) , Privilege Bracketing and Relinquishing,Controlling Privilege Escalation,Assigned Privileges and Safeguards , Role-based Access Control (RBAC) ,RBAC Authorizations ,Rights Profiles , Users and Roles ,Converting the Superuser to a Role ,Trusted Extensions Networking, Trusted Extensions Multilevel Services ,Trusted Extensions Administration
Case Study: Building a Secure Operating System for Linux ,Linux Security Modules.,

Text Book :

1. Guide to Operating systems security - Michel (2004)
2. Operating Systems Security (Synthesis Lectures on Information Security, Privacy, and Trust) - Trent Jaeger (2008)

Reference Books :

1. Guide to Operating Systems - Michael Walters (2006)
2. Modern operating systems 4e - Tanenbaum

Mobile and Wireless Network Security			
Course Code:	**CC 411**	**Course Credits:**	**3**
Course Category:CC	**E3**	**Course (U / P)**	**U**
Course Year (U / P):U	**4U**	**Course Semester (U / P):**	**7U**
No. of Lectures + Tutorials (Hrs/Week):	**03+ 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):30	**45+ 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1. To Understand the security implications inherent in wireless devices, as compared to their wired counterparts			
2. Understand the unique attack vectors faced by wireless networks and required wireless-specific security strategies to mitigate attacks.			
3. Learn fundamentals of wireless exploitation techniques, and gain hands-on experience attacking wireless networks and devices via laboratory experiments			
4. Understand the use of cryptographic primitives in specific wireless applications, including: 802.11, GSM, RFID, and Bluetooth.			
5. Understand techniques to secure wireless devices and networks.			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1 Familiarize with the issues and technologies involved in designing a wireless and mobile system that is robust against various attacks.			
2. Gain knowledge and understanding of the various ways in which wireless networks can be attacked and tradeoffs in protecting networks			
3. Have a broad knowledge of the state-of-the-art and open problems			
4. Learn various security issues involved in cloud computing.			
5. Learn various security issues related to GPRS and 3G. Explain the design of a data center and storage requirements.			

UNIT I Introduction

Security Issues in Mobile Communication: Mobile Communication History, Security – Wired Vs Wireless, Security Issues in Wireless and Mobile Communications, Security Requirements in Wireless and Mobile Communications, Security for Mobile Applications, Advantages and Disadvantages of Application – level Security.

UNIT II Network devices

Security of Device, Network, and Server Levels: Mobile Devices Security Requirements, Mobile Wireless network level Security, Server Level Security. Application Level Security in Wireless Networks: Application of WLANs, Wireless Threats, Some Vulnerabilities and Attach Methods over WLANs, Security for 1G Wi-Fi Applications, Security for 2G Wi-Fi Applications, Recent Security Schemes for Wi-Fi Applications

UNIT III Applications Level Security

Application Level Security in Cellular Networks: Generations of Cellular Networks, Security Issues and attacks in cellular networks, GSM Security for applications, GPRS Security for applications, UMTS security for applications, 3G security for applications, Some of Security and authentication Solutions.

UNIT IV Application Level Security in MANETs

Application Level Security in MANETs: MANETs, Some applications of MANETs, MANET Features, Security Challenges in MANETs, Security Attacks on MANETs, External Threats for MANET applications, Internal threats for MANET Applications, Some of the Security Solutions.

Ubiquitous Computing, Need for Novel Security Schemes for UC, Security Challenges for UC, and Security Attacks on UC networks, some of the security solutions for UC. Advantages of Cloud computing.

UNIT V Security Challenges

Data Center Operations - Security challenge, implement "Five Principal Characteristics of Cloud Computing, Data center Security Recommendations Encryption for Confidentiality and Integrity,Encrypting data at rest, Key Management Lifecycle, Cloud Encryption Standards.

Text Books:

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

2. Frank Adelstein, K.S.Gupta : "Fundamentals of Mobile and Pervasive Computing", 1st Edition, Tata McGraw Hill 2005.

Reference Book:

1. Randall k. Nichols, Panos C. Lekkas : "Wireless Security Models,Threats and Solutions", 1st Edition, Tata McGraw Hill, 2006.
2. Bruce Potter and Bob Fleck : "802.11 Security" , 1st Edition, SPD O'REILLY 2005.

3. James Kempf: "Guide to Wireless Network Security, Springer. Wireless Internet Security – Architecture and Protocols", 1st Edition, Cambridge University Press, 2008.

Enterprise Security and Management			
Course Code:	**CC413**	**Course Credits:**	**3**
Course Category:CC	**E3**	**Course (U / P)**	**U**
Course Year (U / P):U	**4U**	**Course Semester (U / P):**	**7U**
No. of Lectures + Tutorials (Hrs/Week):	**03+ 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):30	**45+ 00**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1. Apply ethical frameworks to analyze problems and evaluate alternative solutions			
2.Create and manage technology policies and procedures for an organization with an understanding of the regulatory environment			
3.Interpret and manage IT governance policies and Design appropriate security architecture with an understanding of the technology			
4.Create and deploy enterprise solutions in support of organizational goals			
5.Plan and implement projects related to infrastructure, security, software development or data analysis			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Understand ethical frameworks to analyze problems and evaluate alternative solutions			
2.Create and manage technology policies and procedures for an organization with an understanding of the regulatory environment			
3.: Interpret and manage IT governance policies.			
4. Develop appropriate data management technologies			
5. Create and deploy enterprise solutions in support of organizational goals			

UNIT I Intro to Information Security & Computer Networks
CIA triad: Confidentiality, Integrity, Availability, RMIAS model, Information Security knowledge areas, Cyber Security industry, certifications, and careers Cryptography, Introduction to Networking Security protocols Threats Authentication and Authorization Access Controls Security Vulnerabilities Security Tools — Penetration testing, etc.

UNIT II IT Security Governance ,Risk Management and Business Continuity Planning
Four types of policies Develop and manage security policies Perform risk management for IT security Threat identification and classification Incident Management, IT security business continuity planning IT security disaster recovery planning.

UNIT III Laws, Investigations and Ethics
Types of computer crime Privacy and the law Computer forensics Information security professional’s code of ethics Intellectual property law

UNIT IV Physical Security and Software Development Security

Physical security domain Physical safeguards, Software development lifecycle Security design reviews Best practices in software engineering

UNIT V IT Security Enterprise Solutions, Network Security architecture and design

Network security in context Protecting TCP/IP networks Virtual Private Networks IPSec Overview of Cloud Securit, Defining the trusted computing base System security assurance concepts Confidentiality and Integrity models

Text Books:

[1]. Brian Allen, Rachelle Loyear ,Enterprise Security Risk Management: Concepts and Applications

Reference Books:

[2]. Brian Allen, The Manager’s Guide to Enterprise Security Risk Management: Essentials of Risk-Based Security

[3]. Aaron Woody, Enterprise Security: A Data-Centric Approach to Securing the Enterprise

ELECTIVE 4

Malware analysis			
CourseCode:	**CC415**	**CourseCredits:**	**3**
CourseCategory:CC	**E4**	**Course(U/P)**	**U**
CourseYear(U/P):U	**4U**	**CourseSemester(U/P):**	**7U**
No.ofLectures+Tutorials(Hrs/Week):	**03+00**	**MidSem.ExamHours:**	**1**
TotalNo.of Lectures(L+T):30	**45+00**	**EndSem.ExamHours:**	**3**
COURSEOBJECTIVES			
1. To recognize the types of malware through analysis methods.			
2. To learn basic and advanced malware analysis techniques.			
3.To learn basic malware functionality.			
4. To practice the android malware analysis techniques.			
5. To practice malware analysis techniques for real world applications.			
COURSEOUTCOMES			
At the end of the course the students should be able to:			
1. .Identify various malwares and understand the behavior of malwares in real world applications			
2. Implement different malware analysis techniques			
3. .Analyze the malware behavior in windows and android.			
4. Understand the purpose of malware analysis.			
5. Identify the various tools for malware analysis			

UNIT-1 INTRODUCTION
Malware Analysis Introduction What is Malware?, Types of Malware, The goal of Malware analysis, Malware Analysis Methodology, What is Malware Analysis?, Basic Techniques for Malware Analysis, General Rules for Malware Analysis, Lab Setup for Malware Analysis

UNIT II Basic Analysis
Basic Analysis Antivirus Scanning, Hashing, Finding Strings, Packed and Obfuscated Malware, Portable Executables File Format, Linked Library and Functions, Static Analysis in Practice, The PE File Headers and Section

UNIT III Malware Analysis in Virtual Machine
The Structure of Virtual Machine, Creating Malware Analysis Machine, Using Malware Analysis Machine, Risk of Virtual Machine for Malware Analysis.

UNIT IV Basic Dynamic Analysis
Malware Sandboxes, Monitoring with Process Manager, Viewing Process with Process Explorer, Comparing Registry Snapshot, Faking a Network, Packet Sniffing with Wireshark, Using INetSim

UNIT V Malware Functionality
Malware Behaviour: Downloaders and Launchers, Backdoors, Credential Stealers, Persistence Mechanism, Privilege Escalation

Testbook:
Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software 1st Edition

Reference Books:

- Practical malware analysis The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig ISBN-10: 159327-290-1, ISBN-13: 978-1-59327-290-6, 2012
- Computer viruses: from theory to applications by Filiol, Eric Springer Science & Business Media, 2006
- Android Malware by Xuxian Jiang and Yajin Zhou, Springer ISBN 978-1-4614-7393-0, 2005

- Hacking exposed™ malware & rootkits: malware & rootkits security secrets & Solutions by Michael Davis, Sean Bodmer, Aaron Lemasters, McGraw-Hill, ISBN: 978-0-07-159119-5, 2010
- Windows Malware Analysis Essentials by Victor Marak, Packt Publishing, 2012.

ANDROIDS SECURITY DESIGN & INTERNALS

Course Code:	**CC 417**	**Course Credits:**	**3**
Course Category:	**E4**	**Course (U / P)**	**U**
Course Year (U / P):	**4U**	**Course Semester (U / P):**	**7U**
No. of Lectures + Tutorials (Hrs/Week):	**03 + 00**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45 + 00**	**End Sem. Exam Hours:**	**3**

COURSE OBJECTIVES

1. To identify and assess overview of Android's architecture and security model.
2. To monitor, evaluate and test security conditions and environment
3. To develop code signing and details how Android's application installation and management process works.
4. To Implement Android security plan and monitor solutions
5. To understand Respond to device security and adjust organizational security plan accordingly

COURSE OUTCOMES

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

1.
2. Detect and protect systems from malicious softwares
3. Implement Android devices.
4. Evaluate tools and technologies for use in protecting the network and individual network systems
5. Implement knowledge on device security

UNIT1- Android's Security Model

Android's Architecture, Linux Kernel, Native Userspace, Dalvik VM, Java Runtime Libraries, . System Services, Inter-Process Communication ,Binde, Android Framework Libraries, Applications, Android's Security

Model,Application Sandboxing, Permissions, IPC,Code Signing and Platform Keys,Multi-User Support ,SELinux,System Updates,Verified Boot

UNIT 2 - Permissions

The Nature of Permissions ,Requesting Permissions ,Permission Management, Permission Protection Levels, Permission Assignment,Contents in Detail Permission Enforcement,Kernel-Level Enforcement, Native Daemon-Level Enforcement, Framework-Level Enforcement ,System Permissions,Signature Permissions,Development Permissions, Shared User ID,Custom Permissions,Public and Private Components, Activity and Service Permissions Broadcast Permissions, Content Provider Permissions, Static Provider Permissions,Dynamic Provider Permissions,Pending Intents

UNIT-3 Package Management

Android Application Package Format,Code Signing, Java Code Signing,Android Code Signing . APK Install Process, Location of Application Packages and Data, Active Components,Installing a Local Package, Updating a Package,Installing Encrypted APKs, Forward Locking,Android 4.1 Forward Locking Implementation,Encrypted Apps and Google Play,Package Verification, Android Support for Package Verification, Google Play Implementation,

UNIT-4 Device Security

Controlling OS Boot-Up and Installation, Bootloader, Recovery,Verified Boot,dm-verity Overview Android Implementation, Enabling Verified Boot,Disk Encryption,Cipher Mode, Key Derivation . . Disk Encryption Password, Changing the Disk Encryption Password,Enabling Encryption, Booting an Encrypted Device, Screen Security,Lock Screen Implementation, Keyguard Unlock Methods ,Brute-Force Attack Protection,Contents in Detail Secure USB Debugging,ADB Overview,The Need for Secure ADB,Securing ADB, Secure ADB Implementation,ADB Authentication Keys, Verifying the Host Key Fingerprint,Android Backup,Android Backup Overview, Backup File Format, Backup Encryption, Controlling Backup Scope

UNIT - 5 Online Account Management

Android Account Management Overview,Account Management Implementation, AccountManagerService and AccountManager, Authenticator Modules,The Authenticator Module Cache, AccountManagerService Operations and Permissions,The Accounts Database . Multi-User Support,Adding an Authenticator Module, Google Accounts Support, The Google Login Service,Google Services Authentication and Authorization Google Play Services

Data and Database Management Security			
Course Code:	**CC419**	**Course Credits:**	**3**
Course Category:	**E4**	**Course (U / P)**	**U**
Course Year (U / P):	**4U**	**Course Semester (U / P):**	**7U**
No. of Lectures + Tutorials (Hrs/Week):	**03 +0+0**	**Mid Sem. Exam Hours:**	**1**
Total No. of Lectures (L + T):	**45**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1. To study the different models involved in database security			
2. To understand the security issues and solution for database			
3. To study application in real time world to protect the database and information			
4. Solve complex problems in a team of database work			
5. Identify security threats in database systems			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1. Avoid unauthorized data observation			
2. Ensure the data confidentiality			
3. Prove that data integrity is preserved			
4. Design and Implement secure database systems			
5. Avoid unauthorized data modification			

UNIT I INTRODUCTION TO DATABASE

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

UNIT II SECURITY ISSUES

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

UNIT III OUTSOURCED DATABASE AND SECURITY REQUIREMENTS

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

UNIT IV PRIVACY PRESERVING DATA MINING

Privacy-Preserving Data Mining – Introduction - Randomization method: Privacy Quantification, Attacks on Randomization, Multiplicative Perturbations, Data Swapping - KAnonymity framework – Distributed Privacy-Preserving Data Mining.

UNIT V DATABASE WATERMARKING

Database Watermarking – Basic Watermarking Process - Discrete Data, Multimedia, and Relational Data – Attacks on Watermarking - Single Bit Watermarking, Multi bit Waterm

Reference Books

1. Michael Gertz and Sushil Jajodia (Editors), Handbook of Database Security: Applications and Trends , ISBN-10: 0387485325. Springer, 2007

2. Osama S. Faragallah, El-Sayed M. El-Rabaie, Fathi E. Abd El-Samie, Ahmed I. Sallam, and Hala S. El-Sayed, Multilevel Security for Relational Databases by; ISBN 978-1-4822- 0539-8. CRC Press, 2014.

3. Bhavani Thuraisingham, Database and Applications Security: Integrating Information Security and Data Management, CRC Press, Taylor & Francis Group, 2

Web Application and Penetration Testing			
CourseCode:	**CC421**	**CourseCredits:**	**3**
CourseCategory:CC	**E4**	**Course(U/P)**	**U**
CourseYear(U/P):U	**4U**	**CourseSemester(U/P):**	**7U**
No.ofLectures+Tutorials(Hrs/Week):	**03+00**	**MidSem.ExamHours:**	**1**
TotalNo.of Lectures(L+T):30	**45+00**	**EndSem.ExamHours:**	**3**

COURSEOBJECTIVES

1.Understand how move beyond push-button scanning to professional, thorough, high-value web application penetration testing.

2.Understand how to assess a web application's security posture and convincingly demonstrate the business impact should attackers exploit discovered vulnerabilities.

3.Gives novice students the information and skills to become expert penetration testers with practice, and fills in all the foundational gaps for individuals with some penetration testing background.

4.Focuses heavily on in-depth, hands-on labs to ensure that students can immediately apply all they learn

5. Perform two complete web penetration tests, one during the five sections of course instruction, and the other during the Capture the Flag exercise.

COURSEOUTCOMES

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

1. Apply the knowledge of the internet and related internet concepts that are vital in understanding web application development and analyze the insights of internet programming to implement complete application over the web.

2. Understand, analyze and apply the role of markup languages like HTML, DHTML, and XML in the workings of the web and web applications.

3. Use web application development software tools i.e. XML, Apache Tomcat etc. and identifies the environments currently available on the market to design web sites.

4. Understand and exploit insecure deserialization vulnerabilities with ysoserial and similar tools.

5.Manually discover and exploit Cross-Site Request Forgery (CSRF) attacks. Manually discover and exploit Server-Side Request Forgery (SSRF) attacks. Use the Browser Exploitation Framework (BeEF) to hook victim browsers, attack client software and the network, and evaluate the potential impact that XSS flaws have within an application

UNIT 1 Introduction and Information Gathering

Overview of the web from a penetration tester's perspective, Web application assessment methodologies, the penetration tester's toolkit, Interception proxies, Proxying SSL through Burp Suite Pro and Zed Attack Proxenos reconnaissance, Virtual host discovery, Open-source intelligence (OSINT), The HTTP protocol, Secure Sockets Layer (SSL) configurations and weaknesses, Target discovery and profiling, Configuration flaws

UNIT II Content Discovery, Authentication, and Session Testing

Logging and monitoring, learning tools to spider a website, Analysing website content, Brute forcing unlinked files and directories via ZAP and fluff, Web authentication mechanisms, Fuzzing with Burp Intruder, Username harvesting and password guessing, Burp sequencer, Session management and attacks, Authentication and authorization bypass, Mutillidae

UNIT III Injection

HTTP response security controls, Command injection, Directory traversal, Local File Inclusion (LFI), Remote File Inclusion (RFI), Insecure deserialization, SQL injection, Blind SQL injection, Error-based SQL injection, Exploiting SQL injection, SQL injection tools: sqlmap

UNIT IV XSS, SSRF, and XXE:
Cross-Site Scripting (XSS), Browser Exploitation Framework (BeEF), AJAX, XML and JSON, Document Object Model (DOM), API attacks, Data attacks, REST and SOAP, Server-Side Request Forgery (SSRF**),** XML Eternal Entity (XXE)

UNIT V CSRF, Logic Flaws and Advanced Tools:
Cross-Site Request Forgery (CSRF), Logic attacks, Python for web app penetration testing, WP Scan, Exploit DB, BurpSuite Pro scanner, Nuclei, Metasploit, **when** tools fail, Business of Penetration Testing:

TextBooks:

1. [Xavier, C, " Web Technology and Design" , New Age International
2. Ivan Bayross," HTML, DHTML, Java Script, Perl & CGI", BPB Publication
3. Bhave, "Programming with Java", Pearson Education
4. Herbert Schieldt, "The Complete Reference:Java", TMH.

ReferenceBooks:

1. Hans Bergsten, "Java Server Pages", SPD O'Reilly
2. Margaret Levine Young, "The Complete Reference Internet", TMH
3. Naughton, Schildt, "The Complete Reference JAVA2", TMH 9. Balagurusamy E, "Programming in JAVA", TMH

ACCESS CONTROL AND IDENTITY MANAGEMENT SYSTEM			
CourseCode:	**CC423**	**CourseCredits:**	**3**
CourseCategory:CC	**E4**	**Course(U/P)**	**4**
CourseYear(U/P):U	**4U**	**CourseSemester(U/P):**	**7U**
No.ofLectures+Tutorials(Hrs/Week):	**03+00**	**MidSem.ExamHours:**	**1**
TotalNo.of Lectures(L+T):30	**45+00**	**EndSem.ExamHours:**	**3**
COURSEOBJECTIVES			
1. Compute tasks with security contexts.			
2. Different classifications of identity management system. Various models for Trust paradigms.			
3. Discretionary access model and Access Matrix Model.			
4. Classify all the active entities of a protection system.			
5. Compute tasks with security contexts.			
COURSEOUTCOMES			
At the end of the course the students should be able to:			
1. Analyze to compute tasks with security contexts.			
2. Categorize the identity management system in to different classes.			
3. Measure the different elements of Trust paradigms for various models.			
4. Compare and contrast between Discretionary access model and Access Matrix Model.			
5. Categorize all the active entities of a protection system.			

Unit 1: Access control: Introduction , Attenuation of privileges ,Trust and Assurance, Confinement problem, Security design principles, Identity Management models, local, Network, federal, global web identity ,XNS approach for global Web identity, Centralized enterprise level Identity Management

Unit2: Elements of trust paradigms in computing, Third party approach to identity trust, Kerberos, Explicit third-party authentication paradigm, PKI approach to trust establishment, Attribute certificates, generalized web of trust models, Examples

Unit3: Mandatory access control, comparing information flow in BLP and BIBA models, Combining the BLP and BIBA models ,Chinese wall problem.

Unit4: Discretionary access control and Access matrix model, definitions, Safety problem, the take grant protection model, Schematic protection model,SPM rules and operations, Attenuating, Applications

Unit5: Role based accesscontrol,HierarchicalAccessControl,Mappingofamandatorypolicy to RABC, Mapping discretionary control to RBAC, RBAC flow analysis, Separation of Duty in RBAC, RBAC consistency properties, The privileges perspective of separation of duties ,Functional specification for RBAC.

Text Book:
1. Messoud Benantar “Access Control System: Security, Identity
2. Management and Trust Models”, Springer, 2009

Reference Book
1. Elena Ferrari and M. Tamer A-zsu,” Access Control in Data Management
2. System,” Morgan & Claypool Publisher, 2010.

AI ENABLED CYBER SECURITY LAB			
Course Code:	**CC481**	**Course Credits:**	**2**
Course Category:	**CC-P**	**Course (U / P)**	**U**
Course Year (U / P):	**4U**	**Course Semester (U / P):**	**7U**
No. of Labs (Hrs/Week):	**2(3 hrs)**	**Mid Sem. Exam Hours:**	
Total No. of Labs:	**10**	**End Sem. Exam Hours:**	**3**
COURSE OBJECTIVES			
1.To incorporate an assessment of the security requirements for AI systems in public procurement policies.			
2.To address the skills shortage and uneven distribution of talents and professionals			
3.To ensure a degree of operational control over AI systems by developing and monitoring practices			
4.To enhance AI reliability and reproducibility by using techniques such as Randomisation, Noise Prevention, Defensive Distillation, Ensemble Learning.			
5.To plan secure logs related to the development/coding of the system,			
COURSE OUTCOMES			
At the end of the course the students should be able to:			
1.Propose the full auditability of models at time/point of failure to organizations			
2. Demonstrate due diligence when testing the technology, before releasing it, preferably including the actual test suites			
3. Devise new methods to allow for system audits other than openly pushing dataset, such as restricting audits			
4.Access cyber-secure pedigrees for all software libraries linked to that code.			
5. Execute & strengthen AI security as it relates to maintaining accountability across intelligent systems.			

List of Experiments:

1. To study the different frameworks that are available in cyber security along with their benefits and limitations.
2. To study those applications of artificial intelligence where cyber security is a mandatory concept.
3. To study the concepts of cyber threat identification.
4. To implement cyber threat identification.
5. To automate threat hunting.
6. To automatically recognize patterns in the data for cyber security.
7. To develop an AI based antivirus software.
8. To implement Email monitoring.
9. To study the ways to fight with different threats using AI.
10. To study the future AI