Course Name	**ADVANCED ALGORITHM DESIGN AND ANALYSIS**
Course Code	**CSN501**
Credits	**03**
LTP	**3 0 0**
Pre-requisites	**UG level course in Algorithm design and Analysis**

Total no. of Lectures : 42

COURSE OBJECTIVE
1. In this course, students will be introduced to methods of designing and analyzing algorithms. They will gain the ability to analyze best case, average case and worst-case running time of algorithms and advanced algorithmic problems.
2. The students will be familiarized with basic paradigms and data structures used to solve algorithmic problems.
3. The course should give the students an understanding of different classes of problems with reference to their computation difficulties and introduce the students with the recent developments in the area of algorithm design.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Overview Algorithm concepts, asymptotic efficiency of algorithms, asymptotic notations and their properties, Recurrence equations and method of solving recurrences, Searching using hash tables, open addressing using linear probing, Medians and order statistics.	**(03)**
Dynamic Programming Deterministic & probabilistic, greedy algorithms, amortized analysis.	**(05)**
Advanced Data Structures B trees, B+ trees, data structures for disjoint sets.	**(05)**
Advanced Graph Algorithms Breadth First and Depth First Search, minimum spanning trees, shortest path algorithms: single source and all pair, max flow problem and its solutions.	**(06)**
Linear Programming Standard and Slack forms, Formulating problems as linear programs, simplex algorithm, representation of polynomials, DFT and FFT.	**(06)**
String Matching Rabin Karp algorithm, String matching with finite automaton, Knuth-Morris-Pratt algorithm.	**(06)**
NP-Completeness Concepts Polynomial time verification, NP-completeness and reducibility, showing problems to be NP-complete like Clique problem, vertex cover problem etc.	**(06)**
Approximate Algorithms Approximate algorithms for vertex cover problem, traveling sales person problem, sum-subset problem.	**(05)**

COURSE OUTCOME
1. Demonstrate use different computational models (e.g., divide-and-conquer), to analyze the complexity/performance of different algorithms
2. Understand the difference between the lower and upper bounds of various problems and their importance in deciding the optimality of an algorithm
3. Demonstrate use of various techniques for efficient algorithm design (divide-and-conquer, greedy, and dynamic algorithms) and be able to apply them while designing algorithms
4. Augment various data structures (trees and arrays) to support specific application
5. To understand various advanced design and analysis techniques such as greedy algorithms, dynamic

programming
6. Gain insight to the concepts of tractable and intractable problems and the classes P, NP and NP-complete problems

REFERENCE(s):
1. Cormen, Leiserson, Rivest, Stein, “Introduction to Algorithms”, Prentice Hall of India.
2. Horowitz, Sahini, “Fundamentals of algorithms”, University Press.
3. Brassard, Bratley, “Fundamentals of algorithms”, Prentice Hall of India.
4. Knuth, “The Art of Computer Programming”, Vol. I-III, Pearson Education.
5. Kleinberg and Tardos, “Algorithm Design”, Pearson Addison-Wesley

Course Name	**ADVANCED COMPUTER NETWORKS**
Course Code	**CSN502**
Credits	**03**
LTP	**3 0 0**
Pre-requisites	**Basic UG course in Computer Networks**

Total no. of Lectures: 42

COURSE OBJECTIVE
1. To provide a deeper insight into the advanced topics of computer networks and to provide a complex survey of crucial protocols in computer networks (routing, IPv6, quality of service, etc.).
2. Develop an understanding of the underlying structure of networks and how they operate.
3. To be able to explain basic networking concepts by studying client/server architecture, network scalability, geographical scope, the Internet and intranets

LECTURE WITH BREAKUP	**NO. OF LECTURES**
INTRODUCTION Overview of computer networks, seven-layer architecture, TCP/IP suite of protocols.	**(02)**
MEDIUM ACCESS MAC protocols for high-speed LANS, MANs, and wireless LANs. (For example, FDDI, DQDB, HIPPI, Gigabit Ethernet, Wireless Ethernet, etc.), CSMA/CD, CSMA/CA, Simple performance models; WAN access methods - PPP.	**(06)**
INTERNETWORKING AND ROUTING Packet Switching, The Internetworking Problem, Internet Routing Architecture: Internet Service Providers and Peering Border Gateway Protocol (BGP), Border Gateway Protocol (continued), BGP instability, Fair queuing, Wireless TCP, The IP/TCP split connections, Scaling IP, Routers: Forwarding and Routing, The IP forwarding path, Unicast Internet routing: Intra and Inter domain routing, Internet Routing-in-the-wild, Router Design and Implementation, Security problems with Internet Architecture, IPV6, Mobile IP.	**(08)**
RESOURCE MANAGEMENT End-to-End Congestion Control, Router-Assisted Congestion Control: Active Queue Management, Fair Queuing and Variants, Modeling and Measurement: Packet Trains, TCP Congestion Control Impediments, Adaptive Network Applications, QoS: Why QoS; Basic Models and Architecture, Mechanisms and Properties, Modeling and Measurement: Traffic Self-Similarity.	**(08)**
GROUP COMMUNICATION Multicast Routing and Transport, IP Multicasting: Multicast routing protocols, address assignments, session discovery, Multicasting in mobile networks.	**(05)**

TRANSPORT LAYER PROTOCOL TCP protocol dynamics, TCP extensions for high-speed networks, transaction-oriented applications. Other new options in TCP, Application protocols for email, ftp, web, DNS.	**(05)**
WIRELESS NETWORKS Wireless LAN architecture, Mobile IP, Broadcast file system, Agent technology, Satellite technology.	**(04)**
SECURITY Network security at various layers. Secure-HTTP, SSL, Transport Layer security, ESP, Authentication header, Key distribution protocols. Digital signatures, digital certificates.	**(04)**

COURSE OUTCOME
1. Students will be able to analyze the behavior of even complex computer networks and propose their topology as well as solutions to particular problems
2. Identify features and benefits of the IPv6 network protocol and become able to design and implement an IPv6 network.
3. Students will also be able to design and build an Ethernet network by designing the subnet structure and configuring the routers to service that network
4. Be able to demonstrate skills for network management and systems administration.

REFERENCE(s):
1. Computer Networking, A Top-Down Approach Featuring the Internet - J. Kurose and K. Ross, 3rd Ed. (Pearson).
2. Computer Networks, A Systems Approach - L. Peterson and B. Davie, 3rd Ed. (Elsevier)
3. Andrew Tanenbaum. Computer Networks, PHI
4. W. R. Stevens. TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the Unix Domain Protocols, Addison Wesley, 1996.
5. W. Stallings, Cryptography and Network Security: Principles and Practice, 2nd ed, Prentice Hall, 1998.
6. E. Perkins, B. Woolf, and S. R. Alpert. Mobile IP: Design Principles and Practices, Addison Wesley, 1997.
7. Articles in various journals and conference proceedings.

Course Name	**ADVANCED TOPICS IN DATABASE SYSTEMS**
Course Code	**CSN506**
Credits	**0 3**
LTP	**3 0 0**
Pre-requisites	**Background and knowledge of relational database management systems**

Total no. of Lectures: 42

COURSE OBJECTIVE
1. To learn Database Management Systems (DBMSs) features such as indexing structures, concurrency control, recovery control, transactional models, and query optimization.
2. To learn advanced topics of databases like object-oriented, parallel and distributed databases
3. To implement the concepts of decision-support models in various database applications
4. To learn state-of-art techniques in database systems for research as well as practical work.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
REVIEW OF RELATIONAL DATA MODEL AND RELATIONAL DATABASE CONSTRAINTS Relational model concepts; Relational model constraints and relational database schemas; Update operations, transactions and dealing with constraint violations.	**(04)**
OBJECT AND OBJECT-RELATIONAL DATABASES Overview of Object-Oriented Concepts, complex objects; Object model of ODMG, Object definition Language ODL; Object Query Language OQL; Conceptual design of Object database. Overview of object relational features of SQL; Object-relational features of Oracle; Implementation and related issues for extended type systems, The nested relational model.	**10**

ENHANCED DATA MODELS FOR ADVANCED APPLICATIONS Active database concepts and triggers; Temporal, Spatial, and Deductive Databases, Mobile databases; Multimedia databases; Geographical Information Systems; Genome data management, XML Databases, Real-time Databases	**10**
PARALLEL AND DISTRIBUTED DATABASES Architectures for parallel databases; Parallel query evaluation; Parallelizing individual operations; Parallel query optimizations; Introduction to distributed databases – architectures; Storing data in a Distributed DBMS; Distributed catalog management; Distributed Query processing; Updating distributed data; Distributed transactions; Distributed Concurrency control and Recovery.	**10**
DECISION SUPPORT SYSTEMS Introduction to decision support, Decision Making systems- modeling and Analysis, Decision support system development.	**10**

COURSE OUTCOME
After completion of course, students would be able to:
1. Analyze the advanced concepts along with their application areas
2. Implement applications based on decision support systems
3. Implement advanced concepts of databases to resolve various research issues
4. Design efficient algorithms to solve various database problems
5. Design recovery protocols for distributed databases and parallel database architectures

REFERENCE(s):
1. Abraham Silberschatz, Henry F. Korth, S. Sudarshan: Database System Concepts, 6th Edition, McGrawHill,2010.
2. Raghu Ramakrishnan and Johannes Gehrke: Database Management Systems, 3rd Edition,McGraw-Hill,2003
3. Elmasri and Navathe: Fundamentals of Database Systems, Pearson Education, 2007. Connolly and Begg: Database Systems, 4th Edition, Pearson Publications, 2005.

Course Name	**ADVANCED COMPUTER ARCHITECTURE**
Course Code	**CSN509**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**Basic undergraduate course in Computer Architecture**

Total no. of Lectures: 42

COURSE OBJECTIVES:
1. To provide students with a broad understanding of current and emerging trends in computer architecture and
2. To study architectures exploiting instruction-level parallelism (ILP), and multiprocessors and multicomputer.
3. To inculcate knowledge about the latest commercial processors (e.g., Pentium Processors, ARM architectures)

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Introduction to Parallel Processing: Parallelism in uniprocessor system; parallel computer structure, architectural classification schemes.	**(05)**
Memory management and organization: Memory hierarchy, Virtual memory system, memory allocation and management, cache memory management. Mapping and management techniques, memory replacement policies.	**(10)**

Pipelining and Vector Architecture: Instruction and arithmetic pipelines design, linear and non-linear pipeline pipeline processors, superscalar and superpipeline design.	**(08)**
SIMD array architecture: SIMD array processors, SIMD interconnection network, Associative array processors.	**(07)**
MIMD multiprocessor and multicomputers: Multiprocessor architecture (loosely coupled, tightly coupled), interconnection networks, cache coherence and synchronization mechanism multiprocessor operating systems, exploiting concurrency.	**(08)**
Review of modern processors Pentium Processor: IA 32 and P6 micro architectures, ARM Processor.	**(04)**

COURSE OUTCOME:
At the end of the course students will be able to:
1. Demonstrate the advanced concepts of computer architecture.
2. Investigate modern design structures of Pipelined and Multiprocessors systems.
3. Understand the interaction amongst architecture, applications and technology.

TEXTBOOK:
1. **Advanced Computer Architectures - A Design space approach**, Dezso Sima, Terence Fountain, Peter Kacsuk, Pearson Education 1997.
REFERENCES:
1. K Hwang, **Advanced Computer Architecture**, Tata McGraw-Hill Education, 2003
2. David E. Culler, Jaswider Pal, **Parallel computer Architecture**, Gulf Professional Publishing, 1999
3. John L. Hennessy and David A. Patterson, **Computer Architecture: A Quantitative Approach**, Third Edition, Morgan Kaufmann, May 2002.
4. High-performance Computer Architecture, by Harold Stone Addison Wesley (1993) 3rd ed.
5. Parallel Computer Architecture: A Hardware/Software Approach David Culler and J.P. Singh with Anoop Gupta, Morgan Kaufmann (August 1998).

Course Name	**BUSINESS INTELLIGENCE**
Course No.	**CSN513**
Credits	**03**
L T P	**3-0-0**
Pre-requisites	

Total Number of Lectures:42

COURSE OBJECTIVE
1. The objective of this course is to aware students of the business intelligence, potential of today's data rich environment.
2. The objectives of this course are to provide students with comprehensive and in-depth knowledge of BI principles and techniques by introducing the relationship between managerial and technological perspectives.
3. The objective is also to enable students to have in depth knowledge of data capture, cleansing, validation, storage and analysis

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Introduction to Business Intelligence Introduction to digital data and its types – structured, semi-structured and unstructured, Introduction to OLTP and OLAP (MOLAP, ROLAP, HOLAP), BI Definitions & Concepts, BI	**(10)**

Framework, Data Warehousing concepts and its role in BI, BI Infrastructure Components – BI Process, BI Technology, BI Roles & Responsibilities, Business Applications of BI, BI best practices	
Basics of Data Integration (Extraction Transformation Loading) Concepts of data integration, needs and advantages of using data integration, introduction to common data integration approaches, Meta data - types and sources, Introduction to data quality, data profiling concepts and applications, introduction to ETL using Kettle	**(12)**
Introduction to Multi-Dimensional Data Modeling Introduction to data and dimension modeling, multidimensional data model, ER Modeling vs. multi dimensional modeling, concepts of dimensions, facts, cubes, attribute, hierarchies, star and snowflake schema, introduction to business metrics and KPIs, creating cubes using Microsoft Excel	**(10)**
Basics of Enterprise Reporting A typical enterprise, Malcolm Baldrige - quality performance framework, balanced scorecard, enterprise dashboard, balanced scorecard vs. enterprise dashboard, enterprise reporting using MS Access / MS Excel, best practices in the design of enterprise dashboards	**(10)**

COURSE OUTCOME
After completion of course, students would be able to:
1. Describe the components of a Enterprise data warehouse, Model the relational database required for an enterprise data warehouse.
2. To extract, cleanse, consolidated, and transform heterogeneous data into a single enterprise data warehouse and analyze data to generate information and knowledge that lead to informed decisions for businesses.
3. To perform "what-if" analysis in real time and will also be able to show how ERP business intelligence can be derived from data warehouses. Student will also be able to create standard reports for business users and derive insightful trends using data mining techniques.

TEXTBOOK(s):
1. Fundamentals of Business Intelligence by R. N. Parsad and Seema Acharya, Wiley
REFERENCE(s):
1. Business Intelligence by David Loshin
2. Business intelligence for the enterprise by Mike Biere
3. Business intelligence roadmap by Larissa Terpeluk Moss, Shaku Atre
4. An introduction to Building the Data Warehouse – IBM
5. Business Intelligence For Dummies – Swain Scheps
6. Successful Business Intelligence: Secrets to making Killer BI Applications by Cindi Howson Information dashboard design by Stephen Few

Course Name	**DESIGN OF EXPERIMENTS & RESEARCH METHODOLOGY**
Course Code	**CSN520**
Credits	**03**
LTP	**3 0 0**
Pre-requisites	**Mathematical concepts**

Total no. of Lectures: 42

COURSE OBJECTIVE
1. To understand some basic concepts of research and its methodologies
2. To select and define appropriate research problem and goals
3. To design methodology for conduct of scientific methods and validation mechanisms
4. To prepare a project proposal and write technical findings and reports

LECTURE WITH BREAKUP	NO. OF LECTURES
IDENTIFYING AND DEFINING RESEARCH PROBLEM Locating, Analyzing, stating and evaluating problem, technique in defining a problem	**(04)**
REVIEWING LITERATURE Need, Sources-Primary and Secondary, Purposes/scope of Review, Steps in conducting review	**(04)**
METHOD OF RESEARCH Research designs: Research design in case of exploratory research studies, research design in case of descriptive studies, Experimental Research and case study	**(04)**
PROCEDURE FOR WRITING A RESEARCH PROPOSAL Purpose, types and components of research proposal	**(05)**
PROCEDURE FOR WRITING A RESEARCH REPORT AND RESEARCH PAPER Audiences and types of research reports, Format of Research report and journal. Strategies for evaluating research, disseminating and utilizing research- An Overview, Guidelines for writing research paper	**(05)**
PROBABILITY DISTRIBUTIONS Discrete probability distribution, Continuous uniform distribution, Normal distribution, Areas under the normal curve, t-distribution, F-distribution, Chi-square distribution	**(06)**
SAMPLE ESTIMATION PROBLEMS Point estimation, Interval estimation, the estimation of mean, the estimation of Variances, Estimation of proportions	**(07)**
HYPOTHESIS Basic concepts concerning testing of hypothesis, procedure for hypothesis testing, important parametric tests: z-test, t-test, chi-squared test, F-test	**(07)**

COURSE OUTCOME	
Students who complete this course will learn:	
1.	To understand principles of research and underlying principles of research processes and methods
2.	To organize and conduct research in a scientific manner
3.	To understand statistical methods to formulate hypotheses
4.	To acquire effective technical writing skills

TEXTBOOK(s):
1. Probability and Statistics for Engineers and scientists, Walpole, Myers, Myers and Ye, 8th ed Pearson Education
2. Research methodology- methods and techniques, C.R. Kothari New Age International publisher
REFERENCE(s):
1. Adrian Wallwork ,English for writing research papers, Springer;
2. Charles X Ling, Quang Yang, Crafting your research Future , Morgan & claypool Publishers;

Course Name	**SPECIAL TOPICS IN SOFT COMPUTING**
Course Code	**CSN522**
Credits	**03**
LTP	**3 0 0**
Pre-requisites	**Artificial Intelligence**

Total no. of Lectures: 42

COURSE OBJECTIVE
1. Introduce students to soft computing concepts and techniques and foster their abilities in designing.
2. Implementing soft computing based solutions for real-world problems.
3. To give students knowledge of non-traditional technologies namely of fundamentals of artificial neural networks, fuzzy sets and fuzzy logic and genetic algorithms.

LECTURE WITH BREAKUP	NO. OF LECTURES
ISUUES IN EXPERT SYSTEMS Knowledge representation, planning and acting in real world, semantic networks, predicate calculus, structural/casual networks, inference control, theorem proving, deduction, truth maintenance, planning, case study of one or more examples from Natural Language Processing, question answering, vision, expert systems	**(10)**
ARTIFICIAL NEURAL NETWORKS Concepts of Artificial Neural Networks and its basic mathematical model, simple perceptron, Feed-Forward Multilayer perceptron, Hopfield network, Self organizing network and recurrent network. **FUZZY LOGIC SYSTEM AND GENETIC ALGORITHM** Fuzzy logic, Fuzzification, Inferencing and defuzzification, Fuzzy Knowledge and rule bases, Fuzzy modeling and Control schemes, Genetic algorithm and detail algorithmic steps, Adjustment of free parameters, Search techniques like tabu search and ant-colony for solving optimization problems, Optimization techniques: PSO(Particle Swarm Optimization), ACO(Ant-colony Optimization), BVO(Binary Vector Optimization).	**(10)** **(12)**
APPLICATIONS GA application to power system optimization problem, Identification and control of linear and nonlinear dynamic systems, stability analysis of Fuzzy control systems	**(10)**

COURSE OUTCOME
Student will learn to:
1. Identify and describe soft computing techniques and their roles in building intelligent machines
2. Apply fuzzy logic and reasoning to handle uncertainty and solve engineering problems
3. Apply genetic algorithms to combinatorial optimization problems
4. Apply neural networks to pattern classification and regression problems
5. Evaluate and compare solutions by various soft computing approaches for a given problem.

REFERENCE(s):
1. S. Russel and P. Norvig, “Artificial Intelligence: A Modern Approach”, Prentice Hall.
2. David.E. Goldberg, ”Genetic Algorithms in search, optimization and Machine Learning”, Pearson Education India
3. Elaine Rich, Kevin Knight, “Artificial Intelligence”, Mc-Raw Hill.
4. Kosko.B. “Neural Networks and Fuzzy Systems”, Prentice Hall of India Pvt. Ltd., 1994.

Course Name	**FOUNDATIONS OF INFORMATION SECURITY**
Course Code	**CSN550**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**Basic Concepts of Computer Science**

Total no. of Lectures: 42

Course Objectives
1. To provide an understanding of principal concepts, major issues, technologies, and basic approaches in information security.
2. Master the key concepts of information security and how they “work.”
3. Develop a “security mindset:” learn how to critically analyze situations of computer and network usage from a security perspective, identifying the salient issues, viewpoints, and trade-offs.

4. To provide the ability to examine and analyze real-life security cases.

LECTURE WITH BREAKUP	NO. OF LECTURES
Introduction: Security mindset, Computer Security Concepts (CIA), Threats, Attacks, and Assets	**(05)**
Software Security: Vulnerabilities and protections, malware, program analysis	**(05)**
Practical Cryptography: Encryption, authentication, hashing, symmetric and asymmetric cryptography, Digital Signatures and Certificates	**(08)**
Network Security: Network security issues, Sniffing, IP spoofing, Common threats, E-Mail security, IPSec, SSL, PGP, Intruders, Virus, Worms, Firewalls-need and features of firewall, Types of firewall, Intruder Detection Systems.	**(10)**
Cyber Security: Cyber Crime and security, Security tools, Introduction to Digital Forensic, OS fingerprinting, TCP/IP stack masking, Social Engineering.	**(08)**
Applications and special topics: Web application Security, Privacy and Anonymity, public policy	**(06)**
Laboratory: The lab work will be based on the setting up of network firewalls, Intruder Detection systems, security and performance analysis of basic cryptography algorithms and digital signature algorithms, tcpdump.	

COURSE OUTCOMES:
1. Evaluate vulnerability of an information system and establish a plan for risk management.
2. Demonstrate basic principles of Web application security
3. Evaluate the authentication and encryption needs of an information system.
4. Demonstrate how to secure a network
5. Evaluate a company's security policies and procedures

TEXTBOOK:
1. **Computer Security: Principles and Practice**, William Stallings; Lawrie Brown
REFERENCES:
1. Introduction to Computer Security, 2004 Matt Bishop, Addison-Wesley, ISBN 0-321-24744-
2. Buchmann J. A., Introduction to Cryptography, Springer Verlag (2001).
3. Stallings William, Cryptography and Network Security, Pearson Education (2006).
4. Schneier Bruce, Applied Cryptography, John Wiley and Sons (1996).
5. Britz M., Computer Forensic and cyber crime, Upper Saddle River, Prentice Hall (2003).

Course Name	**COMPUTATIONAL THEORY AND CRYPTOGRAPHY**
Course Code	**CSN551**
Credits	**03**
L T P	**3 0 0**
Pre-requisite	**Basic Concepts of Computer Science & Algorithms**

Total no. of Lectures: 42

COURSE OBJECTIVES
1. Provide an introduction to basic number theory and computational aspects with focus on applications in cryptography.
2. Understand basic design principals of symmetric and asymmetric cryptography and other indicators of a systems security;
3. Learn how many standard cryptanalytic attacks work and thereby how to avoid common design flaws;
4. Specify how cryptographic tools are applied to achieve privacy and authentication
5. To understand hash functions and existing techniques like AES, RSA, and Discrete Log.
6. To emphasize algorithmic complexity and understand security vs performance trade off.

LECTURE WITH BREAKUP	NO. OF LECTURES
Foundations Substitution Ciphers and Transposition Cipher, Block cipher, Stream cipher.	**(04)**
Cryptographic Protocols Introduction to Protocols, Communications using Symmetric Cryptography, One-Way Functions, Communications using Public-Key Cryptography, Digital Signatures, Digital Signatures with Encryption, Random and Pseudo-Random Sequence Generation, Basic Protocols: Key Exchange, Authentication, Authentication And Key Exchange, Multiple-Key Public-Key Cryptography.	**(08)**
Cryptographic Techniques **Key Length & Management:** Symmetric Key Length, Public-Key Key Length, Comparing Symmetric And Public-Key Key Length, **,** Generating Keys, Nonlinear Keyspaces, Transferring Keys, Verifying Keys, UPDATING KEYS, Storing Keys, Backup Keys.	**(10)**
Cryptographic Algorithms Mathematical Theory, Number Theory, Factoring, Prime Number Generation, Discrete Logarithms in a Finite Field, **Data Encryption Standard:** Description of DES, Security of DES, Differential And Linear Cryptanalysis, Design Criteria, DES Variants, DES modes of operation, Other Stream Ciphers and One-Way Hash Functions RC4, One-Way Hash Functions, MD5, Secure Hash Algorithm (SHA), Message Authentication Codes	**(08)**
Public-Key Algorithms Background, RSA, Elliptic Curve Cryptosystems, Digital Signature Algorithm, Key-Exchange Algorithms: DIFFIE-HELLMAN	**(08)**
Implementations Pretty Good Privacy (PGP), Smart Cards	**(04)**

COURSE OUTCOMES
1. Students should be able to apply the basic rules of public key and symmetric encryption for practical cryptographic problems.
2. Be able to demonstrate the design and use of hash functions, digital signatures, and key distribution with a wide range of key types.
3. Be able to understand the current popular techniques of AES and RSA, digital signatures and key establishment protocols.
4. Given a problem in cryptography, be able to design an algorithm to implement the solution to that problem.

TEXTBOOK:
1. **Applied Cryptography protocols, algorithms, and source code in C**, Second Edition, **Bruce Schneier**, John Wiley & Sons, 1996.
REFRENCE
1. Handbook of Applied Cryptography, by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, CRC Press ISBN: 0-8493-8523-7 , October 1996.

Course Name	**:**	**DIGITAL IMAGE PROCESSING**
Course Code	**:**	**CSN553**
Credits	**:**	**03**
LTP	**:**	**3 0 0**
Pre-requisite	**:**	**Basic knowledge of Mathematics**

Total no. of Lectures: 42

COURSE OBJECTIVES
1. To cover the basic theory and algorithms that are widely used in digital image processing.
2. Expose students to current technologies and issues that are specific to image processing systems.
3. Develop hands-on experience in using computers to process images.
4. Familiarize with MATLAB Image Processing Toolbox

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Introduction and Fundamental to Digital Image Processing Origin of Digital Image Processing, Fundamental steps in Digital Image Processing, Components of Digital Image Processing System, Image sensing and acquisition, Image sampling, quantization and representation, Basic relationship between pixels.	**(07)**
Image Enhancement in the Spatial Domain & Frequency domain Background, Basic grey level transformation, Histogram processing, Basics of Spatial filtering, Smoothing and Sharpening spatial filters, Introduction to Fourier Transform and the Frequency Domain, Discrete Fourier Transform, Smoothing and Sharpening Frequency – Domain filters.	**(08)**
ImageRestoration Image Degradation/Restoration Process, Noise models, restoration in presence of noise, Inverse filtering, Minimum Mean Square Filtering, Geometric menu filter, Geometric transformations.	**(07)**
Color Image Processing Color Fundamentals, Color models, Basis of full color image processing, Color ransformations.	**(05)**
ImageCompression Fundamentals, Image compression models, Error free compression, Lossy compression.	**(05)**
ImageSegmentation Detection of Discontinuities, Edge linking and boundary detection, Threshold, Region oriented segmentation.	**(05)**
Representation, Description and Recognition Representation-chain codes, polygonal approximation and skeletons, Boundary descriptors-simple descriptors, shape numbers, Regional descriptors-simple, topological descriptors, Pattern and Pattern classes-Recognition based on matching techniques.	**(03)**
Recognition Pattern and pattern classes, Decision –Theoretic Methods.	**(02)**

COURSE OUTCOMES
At the end of the course student should be able to:
1. Have a clear impression of the breadth and practical scope of digital image processing and have arrived at a level of understanding that is the foundation for most of the work currently underway in this field.
2. Implement basic image processing algorithms using different tools such as MATLAB.
3. Explore advanced topics of Digital Image Processing
4. Make a positive professional contribution in the field of Digital Image Processing

TEXTBOOK:
1. Digital Image processing By Rafael C. Gonzalez and Richard E. Woods - Pearson Education
REFERENCES:
1. Digital Image Processing by A.K. Jain, 1995, PHI
2. Digital Image processing (An algorithmic approach) By Madhuri A. Joshi - PHI

Course name	**SYSTEM SECURITY**
Course No.	**CSN554**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**: Operating systems, network architecture, network security**

Total no. of Lectures: 42

COURSE OBJECTIVES
1. To learn various aspects of security problems in computing, programs along with safe design methods in general-purpose operating systems
2. Formulate basic skills in security of networked operating systems and learn various phases of security administration like planning, risk analysis, physical security and policies
3. To develop skills necessary to help organizations design, test, and implement well-planned Information Security measures as well as solve information security problems.
4. Apply machine learning and data mining techniques to solve cyber security based systems

LECTURE WITH BREAKUP	NO. OF LECTURES
Security Problem in Computing Attacks , The Meaning of Computer Security , Computer Criminals , Methods of Defense , Concepts and Terminology, Security Models, Implementation of Mechanisms, Operating system vulnerabilities, Software Security.	**(08)**
Program Security Secure Programs, Nonmalicious Program Errors, Viruses and Other Malicious Code, Targeted Malicious Code, Controls against Program Threats .	**(05)**
Protection in General-Purpose Operating Systems Protected Objects and Methods of Protection, Memory and Address Protection, Control of Access to General Objects, File Protection Mechanisms, User Authentication.	**(06)**
Designing Trusted Operating Systems Introduction to a Trusted System, Security Policies, Models of Security, Trusted Operating System Design, Assurance in Trusted Operating Systems	**(05)**
Database and Data Mining Security Introduction to Databases, Security Requirements, Reliability and Integrity, Sensitive Data, Inference, Multilevel Databases, Proposals for Multilevel Security , Data Mining .	**(06)**
Network and OS Hardening	**(06)**

Hardening of various networks, Operating system hardening at various levels.	
Administering Security Security Planning, Risk Analysis, Organizational Security Policies, Physical Security.	**(06)**

COURSE OUTCOMES
After completion of course, students would b able to:
1. Logically analyze social, professional, and security issues related to computing and programs
2. Analyze a protected and trusted general-purpose operating system
3. Demonstrate understanding of key security domain concepts including physical security, computer application security, user support
4. Analyze various security planning techniques and utilize the same for risk analysis
5. Provide secure information in networked and computer systems by applying a layered security policy
6. Apply industry standard security practices to solve a variety of business and technical problems

TEXTBOOK:
1. C.P. Pfleeger, S. Pfleeger and S. Ware, **Security in Computing** (3rd edition), Prentice-Hall, 2002
REFERENCES:
1. D. Gollmann, Computer Security, John Wiley & Sons, 1999
2. M. Bishop, Computer Security: Art and Science, Addison-Wesley, 2002.

Course Name	**E-PRIVACY: PRIVACY AND TRUST IN THE ELECTRONIC SOCIETY**
Course Code	**CSN555**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**: Foundations of Information Security**

Total no. of Lectures: 42

COURSE OBJECTIVES
1. Gain an in-depth look into privacy laws and regulations as well as into technologies for achieving privacy in an electronic world.
2. Differentiate clearly between security and privacy and understand the tradeoffs.
3. Understand various trust metrics, designs and trust models
4. Understand Privacy Laws of various countries
5. Understand DRM and its applicability for wide range of applications

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Introduction Privacy and Security Issues in a Digital World, Privacy Principles and Policies, Authentication and Privacy, Data Mining, Privacy on the Web, E-mail Security, Impacts on Emerging Technologies. Privacy in the Law , Ethical Aspects of Information Security and Privacy	**(08)**
Data and System Security Authorization and Access Control , Role-Based Access Control , Database Security Trust Management , Trusted Platforms , Strong Authentication with Physical Unclonable Functions	**(08)**
Privacy Enhancing Privacy-Preserving Data Mining, Statistical Database Security, Different Search Strategies on Encrypted Data Compared, Client-Server Trade-Offs in Secure Computation , Federated Identity Management , Accountable Anonymous Communication	**(09)**
Digital Asset Protection An Introduction to Digital Rights Management Systems , Copy Protection Systems	

Forensic Watermarking in Digital Rights Management , Person-Based and Domain-Based Digital Rights Management , Digital Rights Management Interoperability , DRM for Protecting Personal Content	**(10)**
Enhancing Privacy for Digital Rights Management Privacy Policies , RFID and Privacy , Malicious Software in Ubiquitous Computing	**(07)**

COURSE OUTCOMES
1. Will be able to draft Privacy Policy for Institute/Organizations
2. Critically analyze and evaluate Privacy laws of various countries
3. Evaluate and design trust models for various IT applications
4. Understand the implications of Privacy and Security

TEXT BOOK
1. **Security, Privacy and Trust in Modern Data Management** By Milan Petkovic, Willem Jonker, Springer, ISBN: 978-3-540-69860-9
REFERENCE BOOK
1. Security in Computing, Prentice Hall, Charles P. Pfleeger , Shari Lawrence Pfleeger

Course name	**:**	**CYBER CRIMES & RELATED IT LAWS**
Course Code		**CSN556**
Credits		**03**
LTP		**3 0 0**
Pre-Requisite	**:**	**Network security**

Total no. of Lectures: 42

Course Objectives
1. Examine how the online world has borne new crimes and law enforcement response.
2. Investigate how the computer has become both a target of attack and a tool for criminal activity
3. Analyze the usage of internet as a tool of crime in cyber space
4. Explore through various case studies the number of emerging cybercrimes (cyber-stalking, hacking, and attacks to critical infrastructure), and also explores how old crimes are affected in new mediums
5. Gain insights to application of IT Laws for different types of cyber crimes

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Information Technology Law Digital and Electronic signatures, Penalties, Compensation & Adjudication, Offences, Liability of Intermediaries, Real World Cases, Sample documentation.	**(05)**
Use of internet in cybercrime How does the Internet work, Email, Web Browsers, Configuring an FTP Server, Configuring a DNS Server, Configuring a Web Server.	**(05)**
Types of Cyber Crimes Cyber Vandalism (Hacking), Cyber Stalking, Denial of Service, Attack, Dissemination of Offensive Material, Internet Frauds, Theft of Telecommunication services, Software Piracy, Dissemination of Viruses & worms, Phishing, Cell Phone cloning, Cyber Terrorism. **Real World Cyber Crime Investigations** Hacker Methodology, Malicious code, Basics of Cyber Crime Investigation, Investigating Emails, Investigating Server Logs, Password Breaking, Investigating Intellectual Property Crimes, Investigating Financial Crimes, Investigating Digital Signature Crimes, Legal Issues, Sample Documentation, Guidelines for Real World Investigations, Source code theft case, Cyber Sabotage case, Lottery fraud case, Accounting fraud case, Digital Signature Fraud	**(08)** **(10)**

case, Investigation Guidelines	
IT Act 2000 & IT Amendment Act 2008 Introduction, Digital Signature, Secure Electronic records and secure digital signatures, Digital Signature Certificates, Offences covered under IT Act 2000, Major Amendments in IT Act	**(08)**
Case Studies on International Cyber Crime Law India, Australia, Canada, Japan, Malaysia, Singapore, United Kingdom (UK), United States of America (USA).	**(06)**

COURSE OUTCOMES
After completion of the course, students would be able to:
1. Analyze various types of cyber crime and formulate real world cyber crime investigations
2. Understand the unique challenges posed to law enforcement agents, policy makers and prosecutors
3. Ability to find solutions in cyber crime investigations, evidence and applicable law for real world case studies
4. Analyze the software tools and methods currently available for finding illegal activities on computer disks and in computer networks.
5. Analyze the criminal activity on the Internet and propose available tools to prevent such activity.

TEXTBOOK:
1. Handbook of Cyber Laws, by Vakul Sharma ,Macmillan.
REFRENCES:
1. Articles in various journals and conference proceedings.

Course Name	**RECENT TRENDS IN INFORMATION TECHNOLOGY**
Course Code	**CSN557**
Credits	**03**
L T P	**3 0 0**
Pre-requisite	**Basics of Engineering profession and technologies**

Total no. of Lectures: 42

COURSE OBJECTIVES
1. Identify & examine latest trends and future challenges in information technology
2. Gain an understanding about latest mobile and wireless communication technologies and their wide range of applications
3. Appreciate and understand the changing programming paradigms, software platforms, Internet technologies and high performance computing infrastructures
4. Understand the techniques and methodologies available for performing big data analysis

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Mobile & Wireless Technologies Mobile Applications (M-Business, M-Government, M-Life, Positional Apps), Platforms to Support Mobile Applications: Mobile IP , Wireless Networks: Wireless PANs (Sensor Networks, Bluetooth, UWB), Wireless LANs (Wi-Fi, 802.11a to n), Wireless Local Loops and Free Space Optics , Cellular networks: from 1 to 5G Networks , Satellite communications and Deep Space Networking, Security, Integration, and Management Issues, VOIP & Broadband Networks	**(10)**
Software Technologies Object- and aspect-oriented software development, component-based software development, situation-aware and adaptive software, middleware, service-oriented	**(08)**

architecture and secure software engineering, Cloud Computing, Virtualization, Agile development, Dynamic language use, Case Studies	
High Performance Computing Infrastructures Parallel Architectures, Multi Cores, Graphical Processing Units, Clusters, Grid Computing, Cloud Computing.	**(06)**
Internet Technologies Emergence of Social networks & Blogs, Internet telephony, Skype and other P2P software's, IPTV, IP Gaming, Digital Rights Management, Web API's for e-commerce, etc, SaaS, SOA, OSS use/development, Web 2.0 and beyond.	**(08)**
Big Data Analysis Dimensions, Key technologies used in manipulating, storing, and analyzing big data, Hadoop and related tools that provide SQL-like access to unstructured data: Pig and Hive.	**(10)**

COURSE OUTCOMES
1. Analyze the upcoming trends of Information Technology in various domains like wireless and mobile networks, software technologies, high performance computing etc.
2. Apply technologies in different use cases to solve complex problems with the use of advanced technologies
3. Get familiar with various current domains of information technology to carry out projects and research work

TEXT BOOK
1. Mobile Communications, Joschen Schiller, Pearson Education
REFERENCE BOOK
2. C.P. Pfleeger, S. Pfleeger and S. Ware, Security in Computing (3rd edition), Prentice-Hall, 2002

Course Name	**HUMAN ASPECTS OF INFORMATION SECURITY**
Course Code	**CSN558**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**Information security, IT laws**

Total no. of Lectures: 42

COURSE OBJECTIVES
1. To learn various aspects of human knowledge as well as approaches to design security mechanisms.
2. To strengthen and improve the overall capabilities of the information security systems by realizing the human aspects as a major link to security.
3. To understand various authentication mechanism, guidelines, and strategies for the design of a secure system
4. To understand the legal, IT and policy level issues in Privacy
5. To understand the role of social media on security issues

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Psychological Acceptability Revisited Passwords, Patching, Configuration, Product: Human Factors, Policies, and Security Mechanisms, Process: Applying Human Factors Knowledge and User-Centered Approaches to Security Design, Panorama: Understanding the Importance of the Environment, Designing Systems That People Will Trust**:** The Trust-Risk Relationship, The Time-Course of Trust, Models of Trust, Trust Designs	**(09)** **(06)**

Authentication Mechanisms Authentication Mechanisms, Quality Criteria, Environmental Considerations, Graphical Passwords, Usable Biometrics, Biometrics and Public Technology: The ATM Example, Cryptographic Smart Cards	**(10)**
Secure Systems Guidelines and Strategies for Secure Interaction Design, Fighting Phishing at the User Interface: Introduction, Attack Techniques, Defenses; Sanitization and Usability: The Remembrance of Data Passed Study, Moving Forward: A Plan for Clean Computing,Usable PKI, Simple Desktop Security with Chameleon	**(12)**
Privacy and Anonymity Systems Privacy Issues and Human-Computer Interaction, A User-Centric Privacy Space Framework, Privacy Policies and Privacy Preferences: The Platform for Privacy Preferences (P3P), Privacy Analysis for the Casual User with Bugnosis: Cookies, Web Bugs, and User Tracking, Graphic Identity, Users Are Not the Enemy: Users Lack Security Knowledge, Security Needs User-Centered Design, Motivating Users, Users and Password Behavior	**(05)**
Social Media Applications, Impact on society, Case studies on Behavioural aspects e.g. Use of media in business.	

COURSE OUTCOMES
After completion of course, students would be able to:
1. Identify various human knowledge factors and user- centric approaches to design a secure information communication system
2. Define the concepts and definition of the information systems and differentiate between several types of information system
3. Identify the threats to information security and show how to protect information recourses
4. Design authentication mechanisms and strategies for secure system
5. Define the legal, IT and policy level issues in Privacy and Anonymity systems
6. Define the role of social media on security issues

TEXTBOOK:
1. Security and Usability: Designing Secure Systems that People Can Useby Lorrie Cranor and Simson Garfinkel
REFERENCES:
1. Research Papers

Course Name	**SECURITY ENGINEERING**
Course Code	**CSN559**
Credits	**03**
LPT	**3 0 0**
Pre-requisites	**Software Engineering, System Security/Network Security**

Total no. of Lectures: 42

COURSE OBJECTIVES:
1. Overview of software practice and software reliability process
2. Describe the implementing operational profiles
3. Describe the risk management process, grounding knowledge of software security and various kinds of security tests ,cases and various kinds of knowledge in software security
4. Understand the reliability and availability objectives, strategies for software reliability and understand the UML diagrams fir security and analyze the model for security.
5. Demonstrate the case-studies using Java and .NET technology and using software reliability models

LECTURE WITH BREAKUP	NO. OF LECTURES
Vulnerabilities and Attacks, Countermeasures, **Problem, Process, and Product** Problems of software practitioners: approach through software reliability engineering, experience with SRE, SRE process, defining the product, Testing acquired software, reliability concepts, software and hardware reliability. **Implementing Operational Profiles** Developing, identifying, crating, reviewing the operation, concurrence rate, occurrence probabilities, applying operation profiles	**(6)**
Software Security Engineering Pillar I: Risk Management, Risk Management Framework (RMF) Pillar II: Software Security best practices, code review, architectural risk analysis, predictive testing, risk based security test, abuse cases, security requirements, security operations. Pillar III: Software security knowledge, prescriptive knowledge, diagnostic knowledge, historical knowledge, software security knowledge architecture. Code review tools.	**(10)**
Engineering "Just Right" Reliability Defining "failure" for the product - Choosing a common measure for all associated systems. - Setting system failure intensity objectives -Determining user needs for reliability and availability. Overall reliability and availability objectives, common failure intensity objective, developed software failure intensity objectives. - Engineering software reliability strategies, Preparing for TestExecuting Test, Guiding Test, Deploying SRE	**(9)**
Using UML for Security: UML diagrams for security requirement -security business process- physical security - security critical interaction - security state. Analyzing Model**:** Notation - formal semantics - security analysis - important security opportunities. Model based security engineering with UML: UML sec profile- Design principles for secure systems - Applying security patterns Tool support for UML Sec: Extending UML CASE TOOLS with analysis tools - Automated tools for UML SEC.	**(9)**
Case Studies Case Study: JAVA Technology, Case Study: The .NET Framework, Web Services Security, Deployment and Configuration Various Security/ Reliability models followed in the industries: Architecture based software reliability models, Software reliability growth models (SRGMs), Exponential Failure class models etc.	**(8)**

COURSE OUTCOME:
At the end of the course students will be able to:
1. Explain the problem of software practitioner and software reliability engineering, software and hardware reliability
2. Explain the Developing, identifying, crating, reviewing the operation, concurrence rate, occurrence probabilities, applying operation profiles
3. Explain the risk management framework, software security, risk based security and risk based approaches for security and code review tools
4. Explore the reliability and availability objectives, and deploying SRE, UML diagrams for security requirement, formal semantics and security analysis.
5. Explain the case using programming languages, and various software reliability models.

TEXTBOOK:
1. **Security Engineering by Ross Anderson**, Wiley
REFERENCES:
1. John Musa D, Software Reliability Engineering, 2nd. Ed. Tata McGraw-Hill, 2005 (Covers Units I, II and III)
2. Jan Jurjens, Secure Systems Development with UML, Springer; 2004 (Covers Unit IV and V)
3. Gary McGraw, "Software Security, Building Security In", 2006, Addison Wisely.
4. Michael Howard, David C. LeBlanc, Writing Secure Code,2nd edition, Microsoft Press
5. Michael Howard, Steve Lipner, The Security Development Lifecycle, Microsoft Press.

Course name	**INFORMATION WARFARE**
Course Code	**CSN560**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**Foundations of Information Security**

Total no. of Lectures: 42

COURSE OBJECTIVES:
1. Gain an understanding of the threats to information resources, including military and economic espionage, communications eavesdropping, computer break-ins, denial-of-service, and disruption of information flow
2. Learn about countermeasures, including authentication, encryption, auditing, monitoring, intrusion detection, and firewalls, and the limitations of those countermeasures.
3. Learn about cyberspace law, information warfare and the military, and intelligence in the information age.
4. Gain knowledge of computer crime, police and forensic methods, and the legal requirements for collecting evidence.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Introduction Nature of information warfare, including computer crime and information terrorism; Threats to information resources, including military and economic espionage, communications eavesdropping, computer break-ins, Terrorism and Internet, Ten Information management Trends, Infrastructures of Information Warfare.	**(10)**
Cyber Attacks Denial-of- service, destruction and modification of data, distortion and fabrication of information, forgery, control and disruption of information flow, electronic bombs, perception management	**(9)**
Defending against Cyber attacks and Cyber Terrorism Countermeasures, including authentication, encryption, auditing, monitoring, intrusion detection, and firewalls, and the limitations of those countermeasures.	**(08)**
Legal Aspects Cyberspace law and law enforcement, information warfare and the military, and intelligence in the information age. Information warfare policy and ethical issues.	**(08)**
Extensive Case Studies	**(07)**

COURSE OUTCOME:
1. Recognize the various hard (technology) and soft (people) elements that make up the spectrum between reactive and proactive Computer Network Information Operations

2. Distinguish the basic approaches to offensive digital operations against data, systems and hardware
3. Describe the unique issues relating to open source intelligence gathering in cyberspace
4. Explain the human factors associated with attacking and defending computer systems
5. Contrast the influence available from messages propagated through cyberspace with that available through more traditional means
6. Differentiate the various information threats and vulnerabilities necessary to conduct a threat assessment

TEXT BOOK:
1. Cyber warfare and cyber terrorism, By Lech Janczewski, Andrew M. Colarik
REFERENCE BOOKS:
1. Inside Cyber Warfare, Mapping the Cyber Underworld, By Jeffrey Carr, O'Reilly Media, December 2009
2. Cyber War: The Next Threat to National Security and What to Do About It, Richard A. Clarke, Robert Knake, ISBN13: 9780061962233

Course name	**INTRUSION DETECTION & PREVENTION SYSTEMS**
Course Code	**CSN561**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**Foundations of Information Security, Network Security**

Total no. of Lectures: 42

COURSE OBJECTIVES:
1. Describe the importance of ethical conduct in using computer network system.
2. Explain fundamental concepts of Network Protocol Analysis.
3. Demonstrate the skill to capture and analyze network packets.
4. Use various protocol analyzers and NIDS as security tools to detect network attack and troubleshoot network problems.
5. Evaluate and demonstrate the use of network analysis and NIDS (network intrusion detection system) tools such as Snort, and Sniffer

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Network Attacks Attack Taxonomies, Probes , IPSweep and PortSweep, NMap, Privilege Escalation Attacks, Buffer, Overflow Attacks, Misconfiguration Attacks, Race condition Attacks, Man in the Middle Attacks, Social Engineering Attacks, Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks	**(05)**
Detection Approaches for DoS and DDoS Attacks Prevention and Response for DoS and DDoS Attacks, Examples of DoS and DDoS Attacks, Worms Attacks, Modeling and Analysis of Worm Behaviors, Detection and Monitoring of Worm Attacks, Worms Containment, Examples of Well Known Worm Attacks, Routing Attacks, OSPF Attacks, BGP Attacks	**(05)**

Detection Approaches Misuse Detection, Pattern Matching, Rule based Techniques, State based Techniques, Techniques based on Data Mining, Anomaly Detection, Advanced Statistical Models , Rule based Techniques, Biological Models, Learning Models, Specification based Detection, Hybrid Detection, Data Collection, Data Collection for Host Based IDSs, Audit Logs, System Call Sequences, Data Collection for Network Based IDSs, SNMP, Packets, Limitations of Network Based IDSs, Data Collection for Application Based IDSs, Data Collection for Application Integrated IDSs, Hybrid Data Collection	**(06)**
Theoretical Foundation of Detection Applications of Classifiers: Taxonomy of Anomaly Detection Systems, Fuzzy Logic in Anomaly Detection, Bayes Theory, Bayes Theory in Anomaly Detection, Artificial Neural Networks, Processing Elements, Connections, Network Architectures, Learning Process, Artificial Neural Networks in Anomaly Detection, Support Vector Machine in Anomaly Detection	**(06)**
Evolutionary Computation Evolutionary Computation in Anomaly Detection, Association Rules, Clustering, Comparative Study of Anomaly Detection Techniques	**(04)**
Evaluation Criteria Accuracy, False Positive and Negative, Confusion Matrix, Precision, Recall, and FMeasure, ROC Curves, The BaseRate Fallacy, Performance, Completeness, Timely Response, Adaptation and Cost Sensitivity, Intrusion Tolerance and Attack Resistance, Redundant and Fault Tolerance Design, Obstructing Methods, Test, Evaluation and Data Sets	**(06)**
Intrusion Response Response Types, Various theories and approaches, Survivability and Intrusion Tolerance	**(04)**
Case Studies Examples of Commercial and Open Source IDSs, Snort Intrusion Detection System, Ethereal Application Network Protocol Analyzer, Multi Router Traffic Grapher (MRTG)	**(06)**

COURSE OUTCOME:
1. Explain the fundamental concepts of Network Protocol Analysis and demonstrate the skill to capture and analyze network packets.
2. Use various protocol analyzers such as Ethereal , WildPackets, TCPDump, WinDump, Dsniff and Sniffit, etc to understand IPpackets in depth
3. Use Network Intrusion Detection Systems as security tools to detect network attacks and troubleshoot network problems.
4. Demonstrate the skill to penetrate service vulnerability

TEXT BOOK:
1. **Network Intrusion Detection and Prevention: Concepts and Techniques**, By Ali A. Ghorbani
REFERENCE BOOKS:
1. Intrusion Detection Systems, Advances in Information Security, Vol. 38, Pietro, Roberto; Mancini, Luigi V. (Eds.), 2008, Springer
2. Recent advances in intrusion detection: 4th international symposium, RAID , By Wenke Lee, Ludovic Me, Andreas Wespi, Springer

Course Name	**ETHICAL HACKING & INCIDENT HANDLING**
Course Code	**CSN562**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**Computer Networks/ Windows/Linux**

Total no. of Lectures: 42

COURSE OBJECTIVES
1. To learn the common hacking ways that hackers use so that students can proactively test their company networks and systems to discover any vulnerability
2. To learn the best practices of handling security incidences so that they can bring back the system online in the shortest possible timelines
3. To be able to appreciate the role of ethics and policies in handling Computing and Networking Infrastructure

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Incident Handling and Computer Forensics Introduction to Incident handling process, Steps for preparing and dealing with a computer security incidents: preparation, detection, containment, eradication, recovery and follow-up. Case Studies for identifying computer attackers and suggestive steps to improve the chances of catching and prosecuting attackers.	**(10)**
Discovering Network and Systems Details Passive profiling and Active scanning, Various hacker techniques, obscure attackers sources and intentions, locate weak DMZ systems and unsecured modem pools, mapping firewall, penetrate wireless LANs and evade intrusion detection systems, Live demonstrations and hands-on.	**(10)**
Penetrating the Targeted Penetration phase, Various attack techniques, its vulnerability, various tools to exploit them and how to harden the system against these attacks : buffer overflow, vulnerability exploitations, password cracking, format string attack, Web server and SQL server attacks, Web application attacks, SQL injection, cross-site scripting, IP spoofing, session hijacking, denial of service.	**(10)**
Owning the Victim Occupation phase of hacker attacks, installing sniffers and backdoors, apply RootKits, establish covert channels, manipulate log files, and deploy stenography, Extensive live demonstrations and hands-on exercises.	**(09)**
Impact on Business Case studies based financial losses, loss of reputation	**(03)**

COURSE OUTCOMES
1. Student should be able to plan, create and utilize their system in order to prevent, detect and respond to attacks.
2. Be able to defend a computer against a variety of different types of security attacks using a number of hands-on techniques
3. Be able to defend a LAN against a variety of different types of security attacks using a number of hands-on techniques

TEXT BOOK:
1. Chained Exploits: Advanced Hacking Attacks from Start to Finish, Andrew Whitaker, Keatron Evans , Jack B. Voth
REFERENCE BOOKS:

1. Hacker Techniques, Tools, and Incident Handling, by Sean-Philip Oriyano, Michael Gregg English ISBN: 0763791830, 2010

Course name	**NETWORK SECURITY**
Course Code	**CSN571**
Credits	**3**
LTP	**3 0 0**
Pre-requisite	**Computer Networks and Foundations of Information Security**

Total no. of Lectures: 42

COURSE OBJECTIVES
1. Investigation of core security technologies and security policies to mitigate risks.
2. Gain an understanding of network perimeter security design principles
3. Gain an understanding of free/ commercial security tools and their applications and develop the security solution for a given application/scenario. 4. Ability to review procedures for installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices. 5. Knowledge of the technologies that underpin the deployment and maintenance of a secure network.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Packet Filtering How Packet Filtering Works, TCP and UDP Ports, TCP's Three-way Handshake, Router as a Packet Filter, An Alternative Packet Filter: IP Chains, Egress Filtering, Industry standard protocols: working of router protocol, how they work and how to drive them.	**(05)**
Stateful & Proxy Firewalls Working of Stateful Firewall, The Concept of State, Stateful Filtering and Stateful Inspection, Fundamentals of Proxying, Pros and Cons of Proxy Firewalls, Types of Proxies, Tools for Proxying	**(05)**
Security Policy Firewalls Are Policy, How to Develop Policy, Perimeter Considerations	**(02)**
Virtual Private Networks VPN Basics, Advantages and Disadvantages of VPNs, IPSec Basics	**(03)**
Network Intrusion Detection & Prevention Systems Network Intrusion Detection Basics, the Roles of Network IDS in a Perimeter Defense, IDS Sensor Placement, IPS, IPS Limitations, NIPS, Host-Based Intrusion Prevention Systems, Case Studies	**(04)**
Host Hardening & Defense Components The Need for Host Hardening, Removing, Disabling or Limiting Access of Unnecessary Programs or Data and Configuration Files, Controlling User and Privileges, hardening hosts and the Perimeter, Antivirus Software, Host-Based Firewalls, Host-Based Intrusion Detection, Challenges of Host Defense Components, Preventing TCP/UDP exploits from DoS attacks.	**(08)**
Designing a Secure Network Perimeter The Role of a Router, The Router as a Perimeter & Security Device, Router Hardening, Fundamentals of Secure Perimeter Design, Gathering Design Requirements, Design Elements for Perimeter Security, Separating Resources, Security Zones, Common Design Elements, VLAN-Based Separation	**(07)**
	(04)

Maintaining a Security Perimeter System and Network Monitoring, Incident Response, Accommodating Change	
Network Log Analysis The Importance of Network Log Files, Log Analysis Basics, Analyzing Router Logs, Analyzing Network Firewall Logs, Analyzing Host-Based Firewall and IDS Logs	**(04)**

COURSE OUTCOMES
1. Explain fundamental concepts of network vulnerabilities and attacks.
2. Demonstrate the skill to penetrate service vulnerability.
3. Implement, monitor and maintain a secure network consisting of enterprise level routers and switches
4. Understand the role of AAA and IPSec in securing networks.
5. Understand how to design and implement firewall technologies that complement network policies in securing the perimeter of a network
6. Learn to design/develop/ implement the security solution for a given application.

TEXTBOOK:
1. Inside Network Perimeter Security, Second Edition, Stephen Northcutt; Lenny Zeltser; Scott Winters; Karen Kent; Ronald W. Ritchey, Sams
REFERENCES:
1. Network Perimeter Security: Building Defense In-Depth ,Cliff Riggs, Proteris Group, Waterbury, Vermont, USA
2. W. Stallings, Network Security Essentials (3rd Edition), Prentice-Hall, 2007
3. W. R. Stevens, TCP/IP Illustrated, Vol. 1: The Protocols, Addison-Wesley, 1993
4. D. E. Comer, Internetworking with TCP/IP, Vol.1 (4th Edition), Prentice Hall, 2000
5. R. Oppliger, Internet and Intranet Security (2nd edition), Artech House, 2002
6. W. R. Cheswick and S.M. Bellovin, Firewalls and Internet security (2nd edition), Addison-Wesley, 2003.

Course name	**INFORMATION SECURITY AUDIT AND SECURITY MANAGEMENT**
Course Code	**CSN572**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**Basics of Information Security**

Total no. of Lectures: 42

COURSE OBJECTIVES
1. To provide students with an understanding of information security management and an ability to critically evaluate technologies available for implementing security in systems.
2. To provide students with an understanding of information security auditing and an ability to critically evaluate audit methodologies and approaches for implementing security audits.
3. To enable students to find innovative solutions to security and audit problems in information systems.
4. To provide the theoretical and practical skills for security management.
5. To ensure that students have a basic understanding of the legal, regulatory requirements, and international standards requirements, pertaining to computer security and audit in different nations.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Introduction Introduction to Information Security Management, Introduction to Management Concepts, The Information Security Life Cycle	**(04)**

Security Plan Security Plan, Security Policy, Business Continuity Planning	**(04)**
7Drafting Security Policies **Drafting Security policies, Report writing, Human behavior**	**(04)**
Security Analysis Security Risk Management, Continual Security: Integrated Fault-Event Analysis and Response Framework (IFEAR), Active Security Assessment, System Availability	**(06)**
Security Design Background to the standards, Use of the standards Certification process, Overview of ISO 27001, Summary of changes from BS 7799-2:2002 ISO 27000 series in future Integration with other management systems, Record control Management responsibility The PDCA cycle: Scope definition, Risk assessment, Risk treatment plan, The statement of applicability Monitor & review the ISMS, Maintain the ISMS, control areas ISO 27001 & CobiT ISO 27001, ITIL & ISO 20000 PCI Data security Procedure	**(14)**
Security Implementation Security Solutions, Common Criteria's for implementations	**(04)**
Security Review Security Review through Security Audit, Privacy Rights, Information Technology, and HIPAA	**(06)**

COURSE OUTCOMES
1. Identify information systems threats, vulnerabilities, risks and controls
2. Design and Implement Information Security Policies and define technical controls
3. Ability to conduct a practical investigative task in a real world scenario eg: audit university computer lab
4. Audit/test controls on data integrity in end-user applications e.g. databases/spreadsheets/websites
5. Detection of network security attacks and configuration of protective mechanisms e.g. firewalls
6. Be able to develop a comprehensive security policy for any organization

TEXTBOOK:
1. **Information Security Management: Concepts and Practice**, Bel G. Raggad, Pace University, Pleasantville, New York, USA, **ISBN:** 9781420078541, CRC Press Online.
REFERENCE:
1. Information Security Based on ISO27001/ISO 17799: A Management Guide by A Calder, Van Haren Publishing (19 July 2006).

Course Name	**INTERNET SECURITY**
Course Code	**CSN574**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**Basic Understanding of Computer Networks and Operating systems**

Total no. of Lectures: 42

COURSE OBJECTIVES
1. To understand the layered perspective of Internet Security wrt wide applications.
2. To learn the logical and physical placement of security primitives and design architectures to enable complete framework to provide Internet Security.

3. Identify the impact of a layered defense on the performance of the network.
4. Discuss the objectives of access control methods and describe how the available methods are implemented in the defense of a network

LECTURE WITH BREAKUP	**No. OF LECTURES**
Network Security Practice: Authentication applications, Kerberos, X.509 Directory Authentication Service, Electronic Mail Security; SSL, S/MIME,IP Security Architecture, Combining Security Associations, Key Management, Web Security; Web Security Requirements, Secure Sockets Layer and Transport Layer Security, Secure Electronic Transaction(SET), System Security: Intruders, Viruses and Related Threats, Types of Viruses, Trusted Systems.	**(10)**
E-Mail And Internet Security: PGP and PEM, Firewalls, Types of Firewalls, Firewall Configuration, Firewall Design Principles, Classical attacks on the Internet, IP Spoofing attacks.	**(06)**
Mathematical Background Probability and Learning from a Bayesian Perspective, Parameter Estimation from Data, Mixture Models and the Expectation Maximization Algorithm, Graphical Models, Classification, Clustering, Markov Chains and information Theory.	**(07)**
Web Graphs Internet and Web Graphs, Generative Models for the Web Graph and Other Networks, Applications.	**(05)**
Secure Protocols For Financial Security Overview of electronic payment, Forward secure digital signatures, On-Line e-cash, Auctions, Micropayments, Off-Line e-cash, Brands' e-cash schemes, Brands' ecash schemes, Electronic voting schemes, Probabilistic Micropayments, NetBill and NetCheque, Security arguments for blind signatures, Group blind signatures, Identification protocols, Fair exchange and contract signing.	**(08)**
COMMERCE ON THE WEB: Models And Applications Introduction, Customer Data on the Web, Automated Recommender Systems, Networks and Recommendations, Web Path Analysis for Purchase Prediction.	**(06)**

COURSE OUTCOMES
1. The students should be able to configure routers and ACLs, firewalls, implement IPSec and VPNs
2. To be able to apply mathematical techniques and design modeling techniques for various Internet traffic and security based problems
3. Design and develop secure solutions for Internet based applications

TEXTBOOKS:
1. Modeling the Internet and the Web: Probabilistic Methods and Algorithms, **Published Online:** 11 Sep 2003, Pierre Baldi, Paolo Frasconi, Padhraic Smyth, **Print ISBN:** 9780470849064, **Online ISBN:** 9780470867990
REFERENCES:
1. Donal O'Mahony and Michael A. Peirce, Hitesh Tewari, Electronic Payment Systems for E-Commerce, Artech House, 2001.
2. Behrouz A. Forouzen, Data Communication and Networking, TMH Press.
3. Mostafa Hashem Sherif, Protocols for Secure Electronic Commerce, 2nd Edition, CRC Press, 2003.
4. A.Tanenbaum: Computer Networks, 3rd ed. Prentice Hall, 1996 (PHI 1997).

Course Name	**INTERNETWORKING ARCHITECTURE AND PROTOCOLS**

Course Code	**CSN575**
Credits	**03**
L T P	**3 0 0**
Pre- requisite	**Operating System & Data communication and network fundamentals**

Total no. of Lectures: 42

COURSE OBJECTIVES
1. To gain the understanding of the concepts and techniques used to model and implement communications between processes residing on independent host computers.
2. Examine the conceptual framework for specifying a computer network i.e. the network architecture,
3. Investigate the set of rules and procedures that mediate the exchange of information between two communicating processes i.e. the network protocols.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Internet Essentials: Naming, Addressing, and Routing Names and Addresses: Hierarchical and Flat, Intra-domain Topology and Routing, Inter-domain Routing, Router Design: Technologies and Trends, Multi-homing and Multi-path	**06**
Network Resource Management Assets and IP Management, Patch Management and Dashboard in Network security with practical examples and case studies	**06**
Network Measurement and Operations Troubleshooting and Fault Detection, Measurement Techniques, Strategies, and Pitfalls. Measurement Continued: Strategies, Pitfalls, Platforms, Traffic Monitoring and Routing Behavior, Traffic Estimation and Engineering, Evaluation Strategies: Simulation, Emulation, etc.	**(08)**
Network Security and Unwanted Traffic Denial of Service: Attacks and Defenses, Application-level Attacks: Resource Exhaustion, Click Fraud, Network Anomaly Detection and Routing Security	**06**
Advanced Topics P2P and Overlay Systems, Congestion Control, Longest Prefix Matching, Routing and Multicast, Future Internet Design	**(06)**
Management Functions & Protocols SNMP & management functions provided through MIBs, CLI, syslog, Netconf and YANG, Netflow and IPFIX, Fault, Configuration, Accounting, Performance, Security (FCAPS) reference model, OAM&P (Operations Administration Maintenance & Provisioning), management lifecycle, management processes and organization, service level agreements, service level monitoring and performance measurement, service level assurance	**10**

COURSE OUTCOMES
1. The student should be able to program security protocols
2. Testing of protocols and networks using network simulator against known standards
3. Design solutions to manage computer networks efficiently and effectively
4. Perform measurements for network traffic and Internet traffic case studies by using different tools and techniques

TEXTBOOK:
1. J. F. Kurose and K. W. Ross, **Computer Networking**, 5th ed., Pearson. ISBN: 0-13-607967-9
REFERENCES:
2. D. E. Comer, Internetworking with TCP/IP, Vol. 1: Principles, Protocols, and Architectures, Prentice Hall
3. W. R. Stevens, TCP/IP Illustrated, Vol. 1: The Protocols, Addison-Wesley.

4. W. R. Stevens, UNIX Network Programming, Prentice Hall

Course Name	**DATABASE SECURITY AND PRIVACY**
Course Code	**CSN576**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**Database Management System, Network Security**

Total no. of Lectures: 42

COURSE OBJECTIVES:
1. An overview of the Database System and Information Security
2. Students will learn the different types of Access control methods and Access Control and for XML and the database security concepts including features, access matrix model and security in DB2.
3. To have a clear understanding of the various types of SQL database attacks
4. Learn about the Risks and Threats in today's Database System and database privacy

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Introduction to Database System and Information Security Basic Database Objects, Categories, Schema, Queries and Views, Cryptographic Basics, Symmetric Encryption, Asymmetric Encryption, Message Digest / Hash.	**(6)**
Access Control: Role-Based Access Control: Grant and Revoking privileges, Discretionary Access Control, Mandatory Access Control , Statistical DB security	**(8)**
Database Security: Database Security, Database protection Requirements, User Types for DBMS including Security Features, Data Repositories for DBMS Including Security, Access Matrix Model , Security in DB2, Database Privileges.	**(8)**
Access control for XML: Basic XML concepts, DTD, XML schema, XQuery, Problems for access control for XML documents.	**(5)**
SQL Database Attacks Database Vulnerabilities Attack, Buffer over flow, SQL injection, Statistical Database Attacks, Aggregation and Inference Direct Attacks, Indirect and Tracker Attacks, SQL Injection through web application	**(6)**
Risks and Threats in Today Database System Threats and Internal Database Protection, Web Application and Database Protection	**(5)**
Database Privacy: Database Privacy Issues, Identity privacy,Ethical Implications of Database Privacy, Security and privacy issues in digital world.	**(4)**

COURSE OUTCOME:
At the end of the course students will be able to:
1. Explain the meaning of database objects, schema, query, views, Basics of cryptography, security and privacy for Internet applications
2. Explore Methods of protection, access control, Security features and data repositories, security in DB2 and database privileges
3. Explain the different types of database attacks
4. Explore the risks and threat in today database system and the issues and impact of database privacy in digital world

TEXT BOOK
1. Michael Gertz, Sushil Jajodia , "Handbook of Database Security, Applications and Trends", ISBN: 78-0-387-48532-4 (Print) 978-0-387-48533-1 (Online)
REFERENCE BOOK
1. Milan Petkovic, Willem Jonker , "Security, Privacy, and Trust in Modern Data Management", ISBN: 978-

3-540-69860-9 (Print) 978-3-540-69861-6 (Online)

Course name	**Critical Infrastructure Protection and Disaster Recovery**
Course Code	**CSN577**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**Foundations of Information Security**

Total no. of Lectures: 42

COURSE OBJECTIVES
1. Identify and describe the various components and their functions of the Critical Infrastructure Competency Model, relating to cyber security and the protection of information infrastructures.
2. Describe the elements of risk analysis as it pertains to the protection of information infrastructures.
3. Describe the various measures/mitigation and countermeasure strategies utilized to protect information infrastructures.
4. Investigate the design and implementation of strategies and systems for protecting critical information assets.
5. Students will learn about backup and recovery theory, including backup methods, planning, and key terminology.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Introduction Asset Identification, Critical Asset Identification , Tangible/Physical Assets, Intangible/Logical Assets, Asset Valuation, Baseline Creation , Understanding Asset, Ranking in Incident Response vs. Disaster Recovery	(02)
Introduction to Risk Management Overview of the Risk Management Process, Risk, Risk Assessment Process, Risk Management, Residual Risk, Risk Control and Acceptance	(02)
Threats Threats, Environmental/Natural Threat, Human Threats: Error, The Insider , Sabotage, Social Engineering; Hardware/Software Failure; Attacks: Software Attacks, Viruses, , Worms, Backdoors and Trapdoors, Denial of Service; Theft, Threat Analysis, Threat Assessment	(03)
Vulnerabilities Vulnerability Analysis, Vulnerability Management, Network Vulnerabilities, Technical Vulnerabilities	(02)
Planning for Organizational Readiness Contingency , Planning Process, Beginning the CP Process, Elements to Begin , Contingency Planning Policy , Business Impact Analysis, Business Impact Analysis Data Collection, Budget Planning for BIA, Incident Response Budgeting, Disaster Recovery Budgeting, Business Continuity Budgeting, Crisis Management Budgeting	(03)
Incident Response Preparing for Incident Response, Incident Response Policy, Building the Security Incident Response Team, Incident Response Planning: During the Incident, After the Incident, Before the Incident; Assembling and Maintaining the Final Incident Response Plan, Detecting Incidents, Incident Decision Making, Reaction, Recovery from Incidents	(06)
Contingency Strategies for Business Resumption Planning Data and Application Resumption, Site Resumption Strategies: Exclusive Site Resumption	(03)

Strategies, Shared Site Resumption Strategies , Service Agreements	
Disaster Recovery Disaster Classifications, Forming the Disaster Recovery Team, Disaster Planning Functions, Technical Contingency Planning Considerations, Resumption Phase, Restoration Phase, Facing Key Challenges, Training the DR Team and the Users, Disaster Response Phase,	(03)
Business Continuity Elements of Business Continuity, The Business Continuity Team, Business Continuity Policy and Plan Functions, Creating an Effective BC Plan/Policy, Implementing the BC Plan, Continuous Improvement of the BC Process, Maintaining the BC Plan, Simulation Exercise, Sample Business Continuity Plans,	(06)
Crisis Management Crisis Management in the Organization, Preparing for Crisis Management, Post crisis Trauma, Getting People Back to Work	(04)
Critical infrastructure Sector-level Approaches Develop an advanced understanding of and practical familiarity with the international critical infrastructure protection and resilience incident management framework through selected case studies: National Incident Management System (Cert-IN), National Response Framework and Critical Infrastructure Support, 9/11 Attacks, Madrid/London Transit Bombings, Hurricane Katrina California Wildfires, Mumbai Attack, Cyber Threats and Incidents	(08)

COURSE OUTCOMES
1. Demonstrate an understanding of the partnership and network building roles and responsibilities of all critical infrastructure partners.
2. Describe the various methods of collecting analyzing and disseminating information (information sharing) amongst critical infrastructure partners.
3. Develop the knowledge required to analyze IT infrastructures and develop efficient plans for deploying system redundancy and disaster recovery technologies to meet business needs.
4. Research mandatory business continuance requirements and data protection requirements for various industries and service providers.
5. Research various network technologies and topologies for system redundancy, resilience and high availability.

TEXTBOOK:
1. **Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation**, Ted G Lewis, Wiley-Inter Science, 2006
REFERENCES:
1. Pamela A. Collins and Ryan K. Baggett, Homeland Security and Critical Infrastructure Protection, Praeger Security International, 2009
2. Critical Information Infrastructures Resilience and Protection, Maitland Hyslop, Springer, ISBN: 0387718613

Course name	**OPERATING SYSTEM AND WEB APPLICATION SECURITY**
Course Code	**CSN578**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	

Total no. of Lectures: 42

COURSE OBJECTIVES:

1. To gain an understanding of how to reduce the risk to the organization posed by web applications.
2. To educate students in secure design and development practices with respect to OS and Web.
3. To identify methods to eliminate risks and to prevent damage to the organization.
4. Gain an understanding of how to harden hosts using best practices.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Introduction: Web Application Basics	**(03)**
Web Application Security Fundamentals	**(03)**
Threat Modeling	**(03)**
Threats and Countermeasures WASC Threat Classes, OWASP Top 10 Web Application Security Vulnerabilities, Attacks and Solutions - Fixing Common Web Application Vulnerabilities	**(06)**
Operating System Security: User Authentication, Application authentication OS security issues when interacting with Networking protocols: HTTP, DHCP, DNS, Active Directory, Secure Telnet, Secure ftp, Linux Security Essentials **Web Security:** Sources of Attacks: Internal, External. Types of attacks: Denial of Service (DOS), TCP/IP insecurity, Eavesdropping, Sniffing/Snooping/Wiretapping. Tools of use: Ethereal, Wireshark, Etherpeek, Packet Spoofing, Replay, Message Integrity, Phreaking **Enterprise Security Best Practices** LAB: Trace a DOS attack, Utilize tools to create packet spoofing, identify networking protocols for security attacks	**(07)** **(07)** **(04)**
Building Secure Data Access	**(03)**
Securing Your Network	**(02)**
Securing Your Web and Application Server and Web Services	**(02)**
Application Security Testing	**(02)**

COURSE OUTCOME:
At the end of the course students will be able to:
1. Recognize and implement techniques to deal with web client and server vulnerabilities.
2. Find solutions to potential problems with state-based attacks.
3. Implement techniques for testing web applications for security issues.
4. Design solutions to obtain secure computer networks and implement security policies.

TEXT BOOK:
1. Web application vulnerabilities: detect, exploit, prevent, By Michael Cross, Steven Palme
REFERENCES:
1. Improving Web application security: threats and countermeasures, By J. D. Meier, Microsoft Corporation
2. Hacking Web services: Shreeraj Shah, Thomson

Course Name	**COMPUTER CRIME INVESTIGATION AND FORENSICS**
Course Code	**CSN579**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**Network Security**

Total no. of Lectures: 42

COURSE OBJECTIVES:
1. To provide students with technical skills and competencies in the field of forensic computing
2. To protect the computer system during the forensic examination from any possible alteration, damage, data corruption, or virus introduction
3. Understand how information is stored and used on digital devices
4. To utilize the computer forensic technology and tools to digital data collection, recovery, preservation and analysis
5. To provide a clear understanding of the principles, procedures, technologies and the legal ramifications of investigator's work.
6. To gain insight into the legal measures for different types of misuse with the help of different case studies

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Introduction Types of computer crime, history, surveys, statistics and global connections Aspects of Cyber Warfare and Cyber Terrorism, Dynamic, Human and Technical Aspects of Cyber Warfare and Cyber Terrorism, Identification, Authorization and Access Control	**(07)**
Social Engineering: Spam, Phishing and Pharming	**(04)**
Malware: The types, effects and investigations, DoS and Distributed DoS: The causes, mechanisms, case studies and counter-measures.	**(07)**
Network Crimes: Hacking methodologies via the Internet and attacks to other networks	**(04)**
Computer Forensics & Investigations: Preparation of Investigation, Procedures, Understanding Data Recovery, Data Acquisition, Processing Crime & Incident scenes, Current Computer Forensic tools, Computer Forensic Analysis & Validations, recovery Graphic Files, Network Forensics, Email Investigations, Mobile Device Forensics	**(10)**
Legal Measures Computer Misuse, Criminal Damage, Software Piracy, Forgery, Investigative Powers	**(04)**
Case Studies: Investigations into hacking, cases and PC misuse, Investigations, Incident Handling and Forensic Examination, The Future: The expansion of the Internet, unsuitable material Identity Theft and Fraud	**(06)**

COURSE OUTCOME:
At the end of the course students will be able to:
1. Demonstrate use of use of computer forensics tools and appropriate skills and knowledge to perform investigations
2. Analyze digital devices to establish user activity
3. Research the development of new devices and technologies and how current digital forensics methods will apply to them.
4. Gain insight knowledge to understand attack profiles, investigation tools and techniques
5. Gain ability to perform Critical analysis of data to identify evidence
6. Be able to trace malicious internet activity and analyze email trails;

TEXTBOOK:
1. **Cyber Warfare and Cyber Terrorism** , Andrew Colarik and Lech Janczewski, editors Dorothy E. Denning, ISBN13: 9781591409915.
REFERENCE BOOK:

1. Information Warfare and Security, Addison-Wesley, 1999, Hedley & Aplin,
2. Blackstone's Statutes on IT and E-Commerce, Oxford University Press, C. Stoll, The Cuckoo's Egg, Pan Book Publishers.
3. **Computer Forensics and Investigations**, Nelson, Phillips Enfinger, Steuart, CENGAGE Learning.

Course Name	**BIOMETRIC SECURITY**
Course Code	**CSN580**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**Digital Image Processing**

Total no. of Lectures: 42

COURSE OBJECTIVES:
1. Cover a broad range of approaches to biometrics reflecting both fundamental principles and the current state-of-the-art practices.
2. To develop an understanding of the fundamental components common to all biometric systems.
3. To develop the student's ability to design, implement, test and evaluate biometric systems that conform to international standards.
4. To develop the students ability to carry out research in biometrics

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Biometrics Introduction Benefits of biometrics over traditional authentication systems, benefits of biometrics in identification systems, comparison of various biometric traits, selecting a biometric for system, Applications. Key biometric terms and processes, biometric verification and identification, how biometric matching works, Accuracy in biometric systems, Metrics for evaluating biometric systems: FAR, FRR, ERR etc.	**(07)**
Physiological Biometric Technologies Fingerprints: Technical description, characteristics, Competing technologies, strengths, weaknesses and deployment. Facial scan: Technical description, characteristics, weaknesses and deployment. Iris scan: Technical description, characteristics, strengths, weaknesses and deployment. Retina vascular pattern: Technical description, characteristics, strengths, weaknesses and deployment. Hand scan: Technical description, characteristics, strengths, weaknesses and deployment.	**(15)**
Behavioral Biometric Technologies Handprint Biometrics, Signature and handwriting technology: Technical description, classification, keyboard /keystroke dynamics, Voice: data acquisition, feature extraction, characteristics, strengths, weaknesses, deployment	**(10)**
Multi biometrics Multi-modal biometric Systems: Face and Hand geometry, Fingerprint and iris recognition etc, Multimodal fusion techniques- score fusion, z-norm fusion etc., Normalization techniques	**(05)**

Biometric Security Modals Sensor level security, database security, template security techniques, Channel level security, various remedial solutions available.	**(05)**

COURSE OUTCOME:
At the end of this course Students will be able to:
1. Modern biometric technologies and the generic components of a biometric system.
2. Pattern recognition and feature extraction in biometrics, Voice and face recognition systems.
3. Select the most appropriate biometric for a given application.
4. Work with signal and image acquisition systems, Deploying biometric systems.
5. Defend proposed biometric systems for a given real world problem and analyze its security aspects.

TEXT BOOK:
1. Anil K. Jain, Michigan State University, USA, Patrick Flynn University of Notre Dame, USA, Arun A. Ross West Virginia University, USA , "**Handbook of Biometrics**", 2008.
REFERENCES:
1. Implementing Biometric Security (Wiley Red Books)by John Chirillo, Scott Blaul.
2. Anil K. Jain Michigan State University, E. Lansing, Michigan and Ruud Bolle and Sharath Pankanti IBM, T.J. Watson Research Center Yorktown Heights, New York Kluwer Academic ," Biometrics Personal Identification in Networked Society", 2002 Kluwer Academic Publishers New York, Boston, Dordrecht, London, Moscow.
3. Articles in various journals and conference proceedings.

Course Name	**CLOUD COMPUTING & SECURITY**
Course Code	**CSN581**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**FOUNDATIONS OF INFORMATION SECURITY**

Total no. of Lectures: 42

COURSE OBJECTIVES:
1. An overview of the concepts, processes, and best practices needed to successfully secure information within Cloud infrastructures.
2. Students will learn the basic Cloud types and delivery models and develop an understanding of the risk and compliance responsibilities and Challenges for each Cloud type and service delivery model.
3. The student will also learn how to apply trust-based security model to real-world security problems.
4. The course provides guidance for building private Clouds and a lab exercise where the student will implement a public cloud using a 3rd party provider's interface

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Introduction to Cloud Computing Online Social Networks and Applications, Cloud introduction and overview, Different clouds, Risks, Novel applications of cloud computing	**(03)**
Cloud Computing Architecture Requirements, Introduction Cloud computing architecture, On Demand Computing Virtualization at the infrastructure level, Security in Cloud computing environments, CPU Virtualization, A discussion on Hypervisors Storage Virtualization Cloud Computing Defined, The SPI Framework for Cloud Computing, The Traditional Software Model, The Cloud Services Delivery Model	**(07)**
Cloud Deployment Models Key Drivers to Adopting the Cloud, The Impact of Cloud Computing on Users, Governance in the Cloud, Barriers to Cloud Computing Adoption in the Enterprise	
Security Issues in Cloud Computing Infrastructure Security, Infrastructure Security: The Network Level, The Host Level, The Application Level, Data Security and Storage, Aspects of Data Security, Data Security Mitigation Provider Data and Its Security,	**(07)**
Identity and Access Management	

Trust Boundaries and IAM, IAM Challenges, Relevant IAM Standards and Protocols for Cloud Services, IAM Practices in the Cloud, Cloud Authorization Management	**(05)**
Security Management in the Cloud Security Management Standards, Security Management in the Cloud, Availability Management: SaaS, PaaS, IaaS	**(05)**
Privacy Issues Privacy Issues, Data Life Cycle, Key Privacy Concerns in the Cloud, Protecting Privacy, Changes to Privacy Risk Management and Compliance in Relation to Cloud Computing, Legal and Regulatory Implications, U.S. Laws and Regulations, International Laws and Regulations	**(08)**
Audit and Compliance Internal Policy Compliance, Governance, Risk, and Compliance (GRC), Regulatory/External Compliance, Cloud Security Alliance, Auditing the Cloud for Compliance, Security-As-a-[Cloud]	**(07)**

COURSE OUTCOME:
1. Identify security aspects of each cloud model
2. Develop a risk-management strategy for moving to the Cloud
3. Implement a public cloud instance using a public cloud service provider
4. Apply trust-based security model to different layers in the infrastructure stack
5. Distinguish between cloud providers and 3rd party managed service providers

TEXTBOOK:
1. Cloud Computing Explained: Implementation Handbook for Enterprises, John Rhoton, Publication Date: November 2, 2009
REFERENCES:
1. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice), Tim Mather, ISBN-10: 0596802765,O'Reilly Media, September 2009
2. Cloud Application Architectures: Building Applications and Infrastructure in the Cloud, Publisher: O'Reilly Media; 1 edition (April 10, 2009), ISBN-10: 0596156367, ISBN-13: 978-0596156367
3. Cloud Computing Bible by Barrie Sosinsky (Jan 11, 2011), Wiley Publication, ISBN-10: 0470903562
4. Introduction to Cloud Computing by Timothy Chou (Dec 27, 2010)

Course name	**PUBLIC KEY INFRASTRUCTURE AND TRUST MANAGEMENT**
Course Code	**CSN582**
Credits	**03**
LTP	**3 0 0**
Pre-requisite :	**Cryptography And Network Security, Computer Networks**

Total no. of Lectures: 42

COURSE OBJECTIVES:
1. PKI Infrastructure is an in-depth, hands-on treatment of the Trusted security Manager solution.
2. To manage the digital keys and certificates that make up the digital identities required to transparently automate all security-related processes in an organization.
3. To provide students a thorough knowledge of the Entrust PKI components
4. To provide knowledge of dealing with PKI components, PKI-enabled services, certificate management
5. To brief about various trust models used for PKI-based security
6. To make students learn to plan, install, configure and manage their own infrastructure in labs

LECTURE WITH BREAKUP	**NO. OF**

	LECTURES
The Concept of an Infrastructure. Pervasive Substrate., Application Enabler, Secure Sign-On, End-User Transparency, Comprehensive Security, Business Drivers, Public-Key Infrastructure Defined, Certification Authority, Certificate Repository, Certificate Revocation, Key Backup and Recovery, Automatic Key Update, Key History, Cross-Certification, Support for Non-repudiation, Time Stamping, Client Software.	**(04)**
Core PKI Services: Authentication, Integrity, and Confidentiality. Authentication, Integrity, Confidentiality, Mechanisms, Authentication, Integrity, Confidentiality, Operational Considerations, Performance, Online versus Offline Operation, Commonality of Underlying Algorithms, Entity Naming.	**(04)**
PKI-Enabled Services. Secure Communication, Secure Time Stamping, Notarization, Non-repudiation, Connection with Other Services, Need for Secure Data Archive, Complexity of This Service, The Human Factor ,Privilege Management, Authentication and Authorization, Authorization Authorities, Delegation, Connection with the PKI, Privacy, Mechanisms Required to Create PKI-Enabled Services, Digital Signatures, Hashes, MACs, and Ciphers	**(07)**
Certificates and Certification Certificates, Digital Certificate, Certificate Structure and Semantics, Alternative Certificate Formats, Certificate Policies, Object Identifiers, Policy Authorities, Certification Authority, Registration Authority	**(04)**
Key and Certificate Management Key/Certificate Life-Cycle Management, Initialization Phase, Issued Phase, Cancellation Phase	**(05)**
Certificate Revocation. Periodic Publication Mechanisms, Certificate Revocation Lists (CRLs), Complete CRLs, Certification Authority, Revocation Lists (CARLs), End-Entity Public-Key Certification Revocation Lists (EPRLs), CRL Distribution Points. Redirect CRLs, Delta and Indirect Delta CRLs, Indirect CRLs, Certificate Revocation Trees (CRTs), Online Query Mechanisms, Online Certificate Status Protocol (OCSP), Simple Certificate Validation Protocol (SCVP), Other Revocation Options, Performance, Scalability, and Timeliness	**(05)**
Trust Models Strict Hierarchy of Certification Authorities, Loose Hierarchy of Certification Authorities, Policy-Based Hierarchies, Distributed Trust Architecture, Mesh Configuration, Hub-and-Spoke Configuration, Four-Corner Trust Model, Web Model, User-Centric Trust, Cross-Certification, Entity Naming, Certificate Path Processing, Path Construction, Path Validation, Trust Anchor Considerations,	**(05)**
Multiple Certificates per Entity. Multiple Key Pairs, Key Pair Uses, Relationship between Key Pairs and Certificates, Real-World Difficulties, Independent Certificate Management, Support for Non-repudiation.	**(04)**
Electronic Signature Legislation and Considerations Electronic Signature Legislation. E-Sign, Digital Signatures in Context, The Significance of Electronic Signature Initiatives, Legal Considerations for PKIs, CA Requirements, Roles and Responsibilities., Private Enterprise PKIs.	**(04)**

COURSE OUTCOME:
After completion of course, students would be able to:
1. Demonstrate how the processes of encryption and digital signatures help fulfil an organization's data

security requirements
2. Describe the basic architecture of public key infrastructure and trust management , including the function of the various applications and processes
3. Analyze and define the certification process
4. Design secure protocols with the help of various trust models like four-corner, web-odel, user-centric model etc.
5. Perform both the usual and the more advanced tasks related to management of PKI infrastructure
6. Customize the roles, policy and groups of the end-users

TEXT BOOK:
1. **Understanding PKI: concepts, standards, and deployment considerations**, By Carlisle Adams, Steve Lloyd, Addison Wesley
REFERENCES:
1. Public key infrastructure: building trusted applications and Web services, By John R. Vacca

Course Name	**MOBILE AND WIRELESS NETWORK SECURITY**
Course Code	**CSN583**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**Network Security, Cryptographic Technique, Mobile Communication, Computer Networks**

Total no. of Lectures: 42

COURSE OBJECTIVES:
1. To learn why wireless is different with perspective of designing security schemes.
2. Learn security requirement and analyze compatible solutions for wireless environment.
3. Creatively analyze mobile and wireless networks for threats and distinct attacks
4. Learn security design aspects in different wireless environment MANET, WLAN, VANET, WiMAX, GSM/CDMA etc.
5. Explain the vulnerabilities introduced into an infrastructure by wireless and cellular technologies.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Introduction to Mobile and Wireless Networks Mobile cellular networks : Advanced Generations: 1G onwards, IEEE wireless networks : IEEE 802.11, IEEE 802.15, IEEE 802.16, Mobile Internet networks : Macro mobility, Micro mobility, Personal mobility, MANET networks	**(05)**
Vulnerabilities of wired and wireless networks The Threat Landscape, Wireless Insecurity, Wireless Network Attacks, Passive vs. Active Attacks, Man-in-the-Middle Attacks, Rogue Access Points and Client Attacks, Denial of Service (DoS)Attacks	**(04)**
Fundamental Security Mechanisms Basics on Security, Secure communication protocols and VPN implementation, Authentication, Access control, SSID, Protocol and MAC Address Filtering, Virtual LAN's (VLAN's) and Network Segmentation, AP Isolation and Guest Networks, Securing the Upper Layers, Wireless Intrusion Detection and Prevention Systems (WIDS/WIPS): Kismet, AirDefense, Kismet IDS (Demo), Rogue AP Detection, Intrusion Forensics	**(06)**
Wi-Fi security Dedicated architectures Hot spot architecture : captive portals, Wireless intrusion detection system(WIDS), Wireless honeypots	**(04)**
Bluetooth Security Bluetooth technical specification, Bluetooth security, Hacking BlueTooth: BlueSnarfing, BlueBugging and BlueJacking, BlueTooth Hacking Tools, BTScanner (Demo)	**(05)**
Wi-Fi Security Attacks on wireless networks, security in the IEEE 802..11 standard, Security in 802.1x,	**(05)**

Security in WEP, WPA, 802.11i, Authentication in wireless networks, Layer 3 security mechanisms	
Security in Mobile Telecommunication Networks Signaling, security in the GSM, GPRS security, 3G/4G security	**(04)**
Security of Downloadable Applications Opening the handset, security policy, The implementation of a security policy, Execution environments for active contents, Validation of active contents, Detection of attacks	**(05)**
Wireless Sensor Network Security Introduction, Attacks on wireless sensor network and counter-measures, Preventive mechanism : authentication and traffic, Case study : centralized and passive intruder detection	**(04)**

COURSE OUTCOME:
1. Architect a secure wireless network infrastructure for their organization, including strong encryption and centralized authentication;
2. Understand the hacker threat and the major techniques hackers use against wireless networks;
3. Use various hacking and vulnerability assessment tools to assess the security of wireless networks, including cracking WEP and WPA security;
4. Identify (and fix) vulnerabilities and mis-configurations in wireless network technologies;

TEXTBOOK(s)
1. Wireless and Mobile Network Security-Security basics, Security in On-the-shelf and emerging technologies,Hakima Chaouchi, Maryline Maknavicius, ISBN: 9781848211179, June 2009, Hardback,
REFERENCE(s)
1. Mobile and Wireless Network Security and Privacy, Springer, ISBN: 0387710574, edition 2007.

Course name	**DATA SCIENCE AND BIG DATA ANALYTICS**
Course Code	**CSN584**
Credits	**03**
LTP	**3 0 0**
Pre-requisite	**Foundations Of Information Security**

Total no. of Lectures: 42

COURSE OBJECTIVES:
1. Gain a foundation level understanding on big data and the state of the practice of analytics.
2. Introduces Data Analytics Lifecycle to address industry challenges that leverage big data.
3. Provides grounding in basic and advanced analytic methods and an introduction to big data analytics technology and tools, including MapReduce and Hadoop.
4. Provide a practical opportunity to apply methods and tools to help investigate a big data analytics real world problem.

LECTURE WITH BREAKUP	**NO. OF LECTURES**
Introduction to Big Data Analytics Overview of big data, the state of practice of analytics, the Data Scientist role, and big data analytics in industry verticals.	**(05)**
Overview of Data Analytics Lifecycle Phases of a typical analytics lifecycle – discovery, data preparation, model planning, model building, communicating results and findings, and operationalizing, Critical activities in each phase of the lifecycle.	**(06)**
Initial Analysis of the Data Introduction to R programming, initial exploration and analysis of the data using R, and basic visualization using R.	**(05)**
Advanced Analytics and Statistical Modeling for Big Data Theory and Methods Core methods used by a Data Scientist, including candidate selection using the Naïve Bayesian	**(08)**

Classifier, categorization using K-means clustering and association rules, predictive modeling using decision trees, linear and logistic regression, and time-series analysis, and text analysis.	
Advanced Analytics and Statistical Modeling for Big Data – Technology and Tools Analytic tools for unstructured data, including MapReduce and the Hadoop ecosystem. It also details in-database analytics with SQL extensions and other advanced SQL techniques and MADlib functions for in-database analytics.	**(07)**
Concluding and Operationalizing an Analytics Project Identifying the core deliverables and creating them for key stakeholders and others. Key points using visualization methods.	**(05)**
Big Data Analytics Lifecycle Lab Practical application of learning to a big data analytics challenge in the context of the data analytics lifecycle.	**(06)**

COURSE OUTCOME:
1. Explain the phases and activities of the data analytics lifecycle and identify the main activities and deliverables.
2. Select and execute appropriate advanced analytic methods for candidate selection, categorization, and predictive modeling.
3. Explore and make an initial analysis of the data, using R and help in creation of initial hypotheses regarding potential relationships within the data that can then be explored using more advanced analytic methods.
4. Students will have the knowledge and practical experience to immediately participate effectively in big data and other analytics projects.

TEXT BOOK:
1. **Analytics in Practice**, by Soumendra Mohanty, Tata Mcgraw hill Education(2011), IsBn-13:-9780070707061
REFERENCE BOOKS:
2. **Agile Analytics: A value Driven approach to Business intelligence and Data Warehousing,** by Ken w. Collier, Pearson Education (2012), ISBN-13:- 9788131786826.
3. MapReduce Design Patterns, by Donald Miner, O'Reilly (2012), ISBN- 13:-9789350239810