

WIRELESS AD-HOC NETWORKS [As per Choice Based Credit System (CBCS) scheme] (Effective from the academic year 2016 -2017) SEMESTER – I			
Subject Code	16LNI251 / 16SCE421 / 16SCN11	IA Marks	20
Number of Lecture Hours/Week	04	Exam Marks	80
Total Number of Lecture Hours	50	Exam Hours	03
CREDITS – 04			
Course objectives: This course will enable students to			
<ul style="list-style-type: none"> • Explain fundamental principles of Ad-hoc Networks • Discuss a comprehensive understanding of Ad-hoc network protocols • Outline current and emerging trends in Ad-hoc Wireless Networks. • Analyze energy management in ad-hoc wireless networks. 			
Module -1			Teaching Hours
Ad-hoc Wireless Networks Introduction, Issues in Ad-hoc Wireless Networks, Ad-hoc Wireless Internet; MAC Protocols for Ad-hoc Wireless Networks: Introduction, Issues in Designing a MAC Protocol, Design Goals of MAC Protocols, Classification of MAC protocols, Contention-Based Protocols, Contention-Based Protocols with Reservation Mechanisms, Contention-Based Protocols with Scheduling Mechanisms, MAC Protocols that Use Directional Antennas.			10Hours
Module -2			
Routing Protocols for Ad-hoc Wireless Networks Introduction, Issues in Designing a Routing Protocol for Ad-hoc Wireless Networks; Classification of Routing Protocols; Table Driven Routing Protocols; On-Demand Routing Protocols, Hybrid Routing Protocols, Hierarchical Routing Protocols and Power-Aware Routing Protocols.			10 Hours
Module – 3			
Multicast Routing in Ad-hoc Wireless Networks Introduction, Issues in Designing a Multicast Routing Protocol, Operation of Multicast Routing Protocols, An Architecture Reference Model for Multicast Routing Protocols, Classifications of Multicast Routing Protocols, Tree-Based Multicast Routing Protocols and Mesh-Based Multicast Routing Protocols.			10 Hours
Module-4			
Transport Layer and Security Protocols for Ad-hoc Networks: Introduction, Issues in Designing a Transport Layer Protocol; Design Goals of a Transport Layer Protocol; Classification of Transport Layer Solutions; TCP over Transport Layer Solutions; Other Transport Layer Protocols for Ad-hoc Networks; Security in Ad-hoc Wireless Networks, Issues and Challenges in Security Provisioning, Network Security Attacks, Key Management and Secure Touting Ad-hoc Wireless Networks.			10 Hours
Module-5			
Quality of Service and Energy Management in Ad-hoc Wireless Networks: Introduction, Issues and Challenges in Providing QoS in Ad-hoc Wireless Networks, Classification of QoS Solutions, MAC Layer Solutions, Network Layer Solutions; Energy Management in Ad-hoc Wireless Networks: Introduction, Need for Energy Management in Ad-hoc Wireless Networks, Classification of Energy Management Schemes, Battery Management Schemes, Transmission Management Schemes, System Power Management Schemes.			10 Hours
Course outcomes:			
The students shall able to:			
<ul style="list-style-type: none"> • Design their own wireless network • Evaluate the existing network and improve its quality of service • Choose appropriate protocol for various applications • Examine security measures present at different level 			

- Analyze energy consumption and management

Question paper pattern:

The question paper will have ten questions.

There will be 2 questions from each module.

Each question will have questions covering all the topics under a module.

The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. C. Siva Ram Murthy & B. S. Manoj: Ad-hoc Wireless Networks, 2nd Edition, Pearson Education, 2011

Reference Books:

1. Ozan K. Tonguz and Gianguigi Ferrari: Ad-hoc Wireless Networks, John Wiley, 2007.
2. Xiuzhen Cheng, Xiao Hung, Ding-Zhu Du: Ad-hoc Wireless Networking, Kluwer Academic Publishers, 2004.
3. C.K. Toh: Ad-hoc Mobile Wireless Networks- Protocols and Systems, Pearson Education, 2002

ADVANCES IN COMPUTER NETWORKS
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)

SEMESTER – I

Subject Code	16SCN12/16SCS22	IA Marks	20
Number of Lecture Hours/Week	04	Exam Marks	80
Total Number of Lecture Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Discuss with the basics of Computer Networks.
- Compare various Network architectures.
- Discuss fundamental protocols.
- Define and analyze network traffic, congestion, controlling and resource allocation.

Module 1	Teaching Hours
<p>Foundation: Building a Network, Requirements, Perspectives, Scalable Connectivity, Cost-Effective Resource sharing, Support for Common Services, Manageability, Protocol layering, Performance, Bandwidth and Latency, Delay X Bandwidth Product, Perspectives on Connecting, Classes of Links, Reliable Transmission, Stop-and-Wait , Sliding Window, Concurrent Logical Channels. T1: Chapter 1.1, 1.2, 1.5.1, 1.5.2., 2.1, 2.5 T2: Chapter 4</p>	10 Hours
<p>Module 2</p> <p>Internetworking I: Switching and Bridging, Datagram's, Virtual Circuit Switching, Source Routing, Bridges and LAN Switches, Basic Internetworking (IP), What is an Internetwork?, Service Model, Global Addresses, Datagram Forwarding in IP, sub netting and classless addressing, Address Translation (ARP), Host Configuration (DHCP), Error Reporting (ICMP), Virtual Networks and Tunnels. T1: Chapter 3.1, 3.2,</p>	10 Hours
<p>Module 3</p> <p>Internetworking- II: Network as a Graph, Distance Vector (RIP), Link State (OSPF), Metrics, The Global Internet, Routing Areas, Routing among Autonomous systems (BGP), IP Version 6 (IPv6), Mobility and Mobile IP T1: Chapter 3.3, 4.1.1,4.1.3 T2:Chapter 13.1 to 13.18 , Ch 18.</p>	10 Hours
<p>Module 4</p> <p>End-to-End Protocols: Simple Demultiplexer (UDP), Reliable Byte Stream(TCP), End-to-End Issues, Segment Format, Connecting Establishment and Termination, Sliding Window Revisited, Triggering Transmission, Adaptive Retransmission, Record Boundaries, TCP Extensions, Queuing Disciplines, FIFO, Fair Queuing, TCP Congestion Control, Additive Increase/ Multiplicative Decrease, Slow Start, Fast Retransmit and Fast Recovery T1: Chapter 5.1, 5.2.1 to 5.2.8, 6.2, 6.3</p>	10 Hours
<p>Module 5</p> <p>Congestion Control and Resource Allocation Congestion-Avoidance Mechanisms, DEC bit, Random Early Detection (RED), Source-Based Congestion Avoidance. The Domain Name System (DNS), Electronic Mail (SMTP,POP,IMAP,MIME), World Wide Web (HTTP), Network Management (SNMP) T1: Chapter 6.4 T2: Chapter 23.1 to 23.16, Chapter 24, Chapter 25, Chapter 27.1 to 27.8</p>	10 Hours
Course Outcomes	
The students should be able to:	

- List and classify network services, protocols and architectures, explain why they are layered.
- Choose key Internet applications and their protocols, and apply to develop their own applications (e.g. Client Server applications, Web Services) using the sockets API.
- Explain develop effective communication mechanisms using techniques like connection establishment, queuing theory, recovery Etc.
- Explain various congestion control techniques.

Question paper pattern:

The question paper will have ten questions.

There will be 2 questions from each module.

Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. Larry Peterson and Bruce S Davis “Computer Networks :A System Approach” 5th Edition , Elsevier -2014.
2. Douglas E Comer, “Internetworking with TCP/IP, Principles, Protocols and Architecture” 6th Edition, PHI – 2014.

Reference Books:

1. Uyles Black, “Computer Networks, Protocols , Standards and Inte rfaces” 2 nd Edition - PHI.
2. Behrouz A Forouzan, “TCP /IP Protocol Suite” 4 th Edition – Tata McGraw-Hill.

INFORMATION AND NETWORK SECURITY [As per Choice Based Credit System (CBCS) scheme] (Effective from the academic year 2016 -2017) SEMESTER – I			
Subject Code	16LNI12/16SCN13/16SCS253	IA Marks	20
Number of Lecture Hours/Week	04	Exam Marks	80
Total Number of Lecture Hours	50	Exam Hours	03
CREDITS – 04			
Course objectives: This course will enable students to			
<ul style="list-style-type: none"> • Explain standard algorithms used to provide confidentiality, integrity and authenticity. • Distinguish key distribution and management schemes. • Deploy encryption techniques to secure data in transit across data networks • Implement security applications in the field of Information technology 			
Module 1			Teaching Hours
Classical Encryption Techniques Symmetric Cipher Model, Cryptography, Cryptanalysis and Brute-Force Attack, Substitution Techniques, Caesar Cipher, Mono-alphabetic Cipher, Playfair Cipher, Hill Cipher, Poly alphabetic Cipher, One Time Pad. Block Ciphers and the data encryption standard: Traditional block Cipher structure, stream Ciphers and block Ciphers, Motivation for the feistel Cipher structure, the feistel Cipher, The data encryption standard, DES encryption, DES decryption, A DES example, results, the avalanche effect, the strength of DES, the use of 56-Bit Keys, the nature of the DES algorithm, timing attacks, Block cipher design principles, number of rounds, design of function F, key schedule algorithm			10 Hours
Module 2			
Public-Key Cryptography and RSA: Principles of public-key cryptosystems. Public-key cryptosystems. Applications for public-key cryptosystems, requirements for public-key cryptosystems. Public-key cryptanalysis. The RSA algorithm, description of the algorithm, computational aspects, the security of RSA. Other Public-Key Cryptosystems: Diffie-hellman key exchange, The algorithm, key exchange protocols, man in the middle attack, Elgamal Cryptographic systems, Elliptic curve arithmetic, abelian groups, elliptic curves over real numbers, elliptic curves over Z_p , elliptic curves over $GF(2^m)$, Elliptic curve cryptography, Analog of Diffie-hellman key exchange, Elliptic curve encryption/ decryption, security of Elliptic curve cryptography, Pseudorandom number generation based on an asymmetric cipher, PRNG based on RSA.			10 Hours
Module 3			
Key Management and Distribution: Symmetric key distribution using Symmetric encryption, A key distribution scenario, Hierarchical key control, session key lifetime, a transparent key control scheme, Decentralized key control, controlling key usage, Symmetric key distribution using asymmetric encryption, simple secret key distribution, secret key distribution with confidentiality and authentication, A hybrid scheme, distribution of public keys, public announcement of public keys, publicly available directory, public key authority, public keys certificates, X-509 certificates. Certificates, X-509 version 3, public key infrastructure. User Authentication: Remote user Authentication principles, Mutual Authentication, one way Authentication, remote user Authentication using Symmetric encryption, Mutual Authentication, one way Authentication, Kerberos, Motivation , Kerberos version 4, Kerberos version 5, Remote user Authentication using Asymmetric encryption, Mutual Authentication, one way Authentication, federated identity management, identity management, identity federation, personal identity verification.			10 Hours
Module 4			
Wireless network security: Wireless security, Wireless network threats, Wireless			10 Hours

<p>network measures, mobile device security, security threats, mobile device security strategy, IEEE 802.11 Wireless LAN overview, the Wi-Fi alliance, IEEE 802 protocol architecture. Security, IEEE 802.11i services, IEEE 802.11i phases of operation, discovery phase, Authentication phase, key management phase, protected data transfer phase, the IEEE 802.11i pseudorandom function. Web Security Considerations: Web Security Threats, Web Traffic Security Approaches. Secure Sockets Layer: SSL Architecture, SSL Record Protocol, Change Cipher Spec Protocol, Alert Protocol, and shake Protocol, Cryptographic Computations. Transport Layer Security: Version Number, Message Authentication Code, Pseudorandom Functions, Alert Codes, Cipher Suites, Client Certificate Types, Certificate Verify and Finished Messages, Cryptographic Computations, and Padding. HTTPS Connection Initiation, Connection Closure. Secure Shell(SSH) Transport Layer Protocol, User Authentication Protocol, Connection Protocol</p>	
<p>Module 5</p>	
<p>Electronic Mail Security: Pretty good privacy, notation, operational; description, S/MIME, RFC5322, Multipurpose internet mail extensions, S/MIME functionality, S/MIME messages, S/MIME certificate processing, enhanced security services, Domain keys identified mail, internet mail architecture, E-Mail threats, DKIM strategy, DKIM functional flow. IP Security: IP Security overview, applications of IPsec, benefits of IPsec, Routing applications, IPsec documents, IPsec services, transport and tunnel modes, IP Security policy, Security associations, Security associations database, Security policy database, IP traffic processing, Encapsulating Security payload, ESP format, encryption and authentication algorithms, Padding, Anti replay service, transport and tunnel modes, combining security associations, authentication plus confidentiality, basic combinations of security associations, internet key exchange, key determinations protocol, header and payload formats, cryptographic suits.</p>	<p>10 Hours</p>
<p>Course Outcomes</p>	
<p>The students should be able to:</p> <ul style="list-style-type: none"> • Analyze the vulnerabilities in any computing system and hence be able to design a security solution. • Identify the security issues in the network and resolve it. • Evaluate security mechanisms using rigorous approaches, including theoretical. 	
<p>Question paper pattern: The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.</p>	
<p>Text Books: 1. William Stallings, Cryptography and Network Security, Pearson 6th edition.</p>	
<p>Reference Books: 1. V K Pachghare: Cryptography and Information Security.</p>	

PROBABILITY STATISTICS AND QUEUING THEORY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – I

Subject Code	16LNI14 / 16SCN14/16SCS14/ 16SSE14 / 16SIT14 /16SCE14 / 16SFC14	IA Marks	20
Number of Lecture Hours/Week	04	Exam Marks	80
Total Number of Lecture Hours	50	Exam Hours	03

CREDITS – 04

Course objectives: This course will enable students to

- Develop analytical capability and to impart knowledge of Probability, Statistics and Queuing.
- Apply above concepts in Engineering and Technology.
- Acquire knowledge of Hypothesis testing and Queuing methods and their applications so as to enable them to apply them for solving real world problems

Module 1	Teaching Hours
Axioms of probability, Conditional probability, Total probability, Baye's theorem, Discrete Random variable, Probability mass function, Continuous Random variable. Probability density function, Cumulative Distribution Function, and its properties, Two-dimensional Random variables, Joint pdf / cdf and their properties	10 Hours

Module 2	Teaching Hours
Probability Distributions / Discrete distributions: Binomial, Poisson Geometric and Hyper-geometric distributions and their properties. Continuous distributions: Uniform, Normal, exponential distributions and their properties.	10 Hours

Module 3	Teaching Hours
Random Processes: Classification, Methods of description, Special classes, Average values of Random Processes, Analytical representation of Random Process, Autocorrelation Function, Cross-correlation function and their properties, Ergodicity, Poisson process, Markov Process, Markov chain.	10 Hours

Module 4	Teaching Hours
Testing Hypothesis: Testing of Hypothesis: Formulation of Null hypothesis, critical region, level of significance, errors in testing, Tests of significance for Large and Small Samples, t-distribution, its properties and uses, F-distribution, its properties and uses, Chi-square distribution, its properties and uses, χ^2 – test for goodness of fit, χ^2 test for Independence	10 Hours

Module 5	Teaching Hours
Symbolic Representation of a Queuing Model, Poisson Queue system, Little Law, Types of Stochastic Processes, Birth-Death Process, The M/M/1 Queuing System, The M/M/s Queuing System, The M/M/s Queuing with Finite buffers.	10 Hours

Course Outcomes

The students should be able to:

- Demonstrate use of probability and characterize probability models using probability mass (density) functions & cumulative distribution functions.
- Explain the techniques of developing discrete & continuous probability distributions and its applications.
- Describe a random process in terms of its mean and correlation functions.
- Outline methods of Hypothesis testing for goodness of fit.
- Define the terminology & nomenclature appropriate queuing theory and also distinguish various queuing models.

Question paper pattern:

The question paper will have ten questions.

There will be 2 questions from each module.

Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. Probability, Statistics and Queuing Theory, V. Sundarapandian, Eastern Economy Edition, PHI Learning Pvt. Ltd, 2009.

Reference Books:

1. Probability & Statistics with Reliability, Queuing and Computer Applications, 2nd Edition by Kishor. S. Trivedi , Prentice Hall of India ,2004.
2. Probability, Statistics and Random Processes, 1st Edition by P Kausalya, Pearson Education, 2013.

INTERNET OF THINGS [As per Choice Based Credit System (CBCS) scheme] (Effective from the academic year 2016 -2017) SEMESTER – I			
Subject Code	16LNI253 /16SCE253 / 16SCN151 /16SCS24 /16SIT251 /16SSE421	IA Marks	20
Number of Lecture Hours/Week	03	Exam Marks	80
Total Number of Lecture Hours	40	Exam Hours	03
CREDITS – 03			
Course objectives: This course will enable students to <ul style="list-style-type: none"> • Define and explain basic issues, policy and challenges in the IoT • Illustrate Mechanism and Key Technologies in IoT • Explain the Standard of the IoT • Explain resources in the IoT and deploy of resources into business • Demonstrate data analytics for IoT 			
Module -1			Teaching Hours
What is The Internet of Things? Overview and Motivations, Examples of Applications, IPV6 Role, Areas of Development and Standardization, Scope of the Present Investigation. Internet of Things Definitions and frameworks-IoT Definitions, IoT Frameworks, Basic Nodal Capabilities. Internet of Things Application Examples- Overview, Smart Metering/Advanced Metering Infrastructure-Health/Body Area Networks, City Automation, Automotive Applications, Home Automation, Smart Cards, Tracking, Over-The-Air-Passive Surveillance/Ring of Steel, Control Application Examples, Myriad Other Applications.			8 Hours
Module -2			8 Hours
Fundamental IoT Mechanism and Key Technologies-Identification of IoT Object and Services, Structural Aspects of the IoT, Key IoT Technologies. Evolving IoT Standards- Overview and Approaches, IETF IPV6 Routing Protocol for RPL Roll, Constrained Application Protocol, Representational State Transfer, ETSI M2M, Third Generation Partnership Project Service Requirements for Machine-Type Communications, CENELEC, IETF IPv6 Over Lowpower WPAN, Zigbee IP(ZIP), IPSO			8 Hours
Module – 3			8 Hours
Layer ½ Connectivity: Wireless Technologies for the IoT-WPAN Technologies for IoT/M2M, Cellular and Mobile Network Technologies for IoT/M2M, Layer 3 Connectivity :IPv6 Technologies for the IoT: Overview and Motivations. Address Capabilities, IPv6 Protocol Overview, IPv6 Tunneling, IPsec in IPv6, Header Compression Schemes, Quality of Service in IPv6, Migration Strategies to IPv6.			8 Hours
Module-4			8 Hours
Case Studies illustrating IoT Design-Introduction, Home Automation, Cities, Environment, Agriculture, Productivity Applications.			8 Hours
Module-5			8 Hours
Data Analytics for IoT – Introduction, Apache Hadoop, Using Hadoop MapReduce for Batch Data Analysis, Apache Oozie, Apache Spark, Apache Storm, Using Apache Storm for Real-time Data Analysis, Structural Health Monitoring Case Study.			8 Hours
Course outcomes:			
At the end of this course the students will be able to: <ul style="list-style-type: none"> • Develop schemes for the applications of IOT in real time scenarios • Manage the Internet resources • Model the Internet of things to business 			

- Understand the practical knowledge through different case studies
- Understand data sets received through IoT devices and tools used for analysis

Question paper pattern:

The question paper will have ten questions.

There will be 2 questions from each module.

Each question will have questions covering all the topics under a module.

The students will have to answer 5 full questions, selecting one full question from each module.

Text Books:

1. Daniel Minoli, "Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications", Wiley, 2013.
2. Arshdeep Bahga, Vijay Madisetti, "Internet of Things: A Hands on Approach" Universities Press., 2015

Reference Books:

1. Michael Miller, "The Internet of Things", First Edition, Pearson, 2015.
2. Claire Rowland, Elizabeth Goodman et.al., "Designing Connected Products", First Edition, O'Reilly, 2015.

SOCIAL NETWORK ANALYSIS [As per Choice Based Credit System (CBCS) scheme] (Effective from the academic year 2016 -2017) SEMESTER – I			
Subject Code	16SCN152 / 16SIT252/	IA Marks	20
Number of Lecture Hours/Week	03	Exam Marks	80
Total Number of Lecture Hours	40	Exam Hours	03
CREDITS – 03			
Course objectives: This course will enable students to			
<ul style="list-style-type: none"> The learning objective of the course Social Network Analysis is to discuss essential knowledge of network analysis applicable to real world data, with examples from today's most popular social networks. 			
Module 1			Teaching Hours
Introduction to social network analysis and Descriptive network analysis: Introduction to new science of networks. Networks examples. Graph theory basics. Statistical network properties. Degree distribution, clustering coefficient. Frequent patterns. Network motifs. Cliques and k-cores.			8 Hours
Module 2			
Network structure, Node centralities and ranking on network: Nodes and edges, network diameter and average path length. Node centrality metrics: degree, closeness and betweenness centrality. Eigenvector centrality and PageRank. Algorithm HITS.			8 Hours
Module 3			
Network communities and Affiliation networks: Networks communities. Graph partitioning and cut metrics. Edge betweenness. Modularity clustering. Affiliation network and bipartite graphs. 1-mode projections. Recommendation systems.			8 Hours
Module 4			
Information and influence propagation on networks and Network visualization: Social Diffusion. Basic cascade model. Influence maximization. Most influential nodes in network. Network visualization and graph layouts. Graph sampling. Low - dimensional projections			8 Hours
Module 5			
Social media mining and SNA in real world: FB/VK and Twitter analysis: Natural language processing and sentiment mining. Properties of large social networks: friends, connections, likes, re-tweets.			8 Hours
Course Outcomes			
The students should be able to:			
<ul style="list-style-type: none"> Define notation and terminology used in network science. Demonstrate, summarize and compare networks. Explain basic principles behind network analysis algorithms. Analyzing real world network. 			
Question paper pattern:			
The question paper will have ten questions.			
There will be 2 questions from each module.			
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.			
Text Books:			
<ol style="list-style-type: none"> David Easley and John Kleinberg. "Networks, Crowds, and Markets: Reasoning About a Highly Connected World." Cambridge University Press 2010. Eric Kolaczyk, Gabor Csardi. "Statistical Analysis of Network Data with R (Use R)". Springer, 2014. 			

3. Stanley Wasserman and Katherine Faust. "Social Network Analysis. Methods and Applications." Cambridge University Press, 1994.

Reference Books:

1. NIL

MULTI-CORE ARCHITECTURE AND PROGRAMMING
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER - I

Subject Code	16SCE24 / 16SCN153	IA Marks	20
Number of Lecture Hours/Week	03	Exam Marks	80
Total Number of Lecture Hours	40	Exam Hours	03

CREDITS - 03

Course objectives: This course will enable students to

- Define technologies of multicore architecture and performance measures
- Demonstrate problems related to multiprocessing
- Illustrate windows threading, posix threads, openmp programming
- Analyze the common problems in parallel programming

Module -1	Teaching Hours
------------------	-----------------------

Introduction to Multi-core Architecture Motivation for Concurrency in software, Parallel Computing Platforms, Parallel Computing in Microprocessors, Differentiating Multi-core Architectures from Hyper- Threading Technology, Multi-threading on Single-Core versus Multi-Core Platforms Understanding Performance, Amdahl's Law, Growing Returns: Gustafson's Law. System Overview of Threading : Defining Threads, System View of Threads, Threading above the Operating System, Threads inside the OS, Threads inside the Hardware, What Happens When a Thread Is Created, Application Programming Models and Threading, Virtual Environment: VMs and Platforms, Runtime Virtualization, System Virtualization.	8 Hours
--	----------------

Module -2	
------------------	--

Fundamental Concepts of Parallel Programming :Designing for Threads, Task Decomposition, Data Decomposition, Data Flow Decomposition, Implications of Different Decompositions, Challenges You'll Face, Parallel Programming Patterns, A Motivating Problem: Error Diffusion, Analysis of the Error Diffusion Algorithm, An Alternate Approach: Parallel Error Diffusion, Other Alternatives. Threading and Parallel Programming Constructs: Synchronization, Critical Sections, Deadlock, Synchronization Primitives, Semaphores, Locks, Condition Variables, Messages, Flow Control- based Concepts, Fence, Barrier, Implementation-dependent Threading Features	8 Hours
--	----------------

Module – 3	
-------------------	--

Threading APIs :Threading APIs for Microsoft Windows, Win32/MFC Thread APIs, Threading APIs for Microsoft. NET Framework, Creating Threads, Managing Threads, Thread Pools, Thread Synchronization, POSIX Threads, Creating Threads, Managing Threads, Thread Synchronization, Signaling, Compilation and Linking.	8 Hours
--	----------------

Module-4	
-----------------	--

OpenMP: A Portable Solution for Threading : Challenges in Threading a Loop, Loop-carried Dependence, Data-race Conditions, Managing Shared and Private Data, Loop Scheduling and Portioning, Effective Use of Reductions, Minimizing Threading Overhead, Work-sharing Sections, Performance-oriented Programming, Using Barrier and No wait, Interleaving Single-thread and Multi-thread Execution, Data Copy-in and Copy-out, Protecting Updates of Shared Variables, Intel Task queuing Extension to OpenMP, OpenMP Library Functions, OpenMP Environment Variables, Compilation, Debugging, performance	8 Hours
--	----------------

Module-5	
-----------------	--

Solutions to Common Parallel Programming Problems : Too Many Threads, Data Races, Deadlocks, and Live Locks, Deadlock, Heavily Contended Locks, Priority Inversion, Solutions for Heavily Contended Locks, Non-blocking Algorithms, ABA Problem, Cache	8 Hours
--	----------------

<p>Line Ping-ponging, Memory Reclamation Problem, Recommendations, Thread-safe Functions and Libraries, Memory Issues, Bandwidth, Working in the Cache, Memory Contention, Cache-related Issues, False Sharing, Memory Consistency, Current IA-32 Architecture, Itanium Architecture, High-level Languages, Avoiding Pipeline Stalls on IA-32, Data Organization for High Performance.</p>	
<p>Course outcomes:</p>	
<p>The students shall be able to:</p> <ul style="list-style-type: none"> • Identify the limitations of ILP and the need for multicore architectures • Define fundamental concepts of parallel programming and its design issues • Solve the issues related to multiprocessing and suggest solutions • Make out the salient features of different multicore architectures and how they exploit parallelism • Demonstrate the role of OpenMP and programming concept 	
<p>Question paper pattern: The question paper will have ten questions. There will be 2 questions from each module. Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.</p>	
<p>Text Books:</p> <ol style="list-style-type: none"> 1. Multicore Programming , Increased Performance through Software Multi-threading by Shameem Akhter and Jason Roberts , Intel Press , 2006 	
<p>Reference Books: NIL</p>	

SOFT COMPUTING [As per Choice Based Credit System (CBCS) scheme] (Effective from the academic year 2016 -2017) SEMESTER – I			
Subject Code	16SSE41 / 16SCS254 / 16SCN154	IA Marks	20
Number of Lecture Hours/Week	03	Exam Marks	80
Total Number of Lecture Hours	40	Exam Hours	03
CREDITS – 03			
Course objectives: This course will enable students to			
<ul style="list-style-type: none"> • Explain key aspects of soft computing. • Identify the components and building block hypothesis of Genetic algorithm. • Analyze Neuro Fuzzy modeling and control. • Evaluate machine learning through Support vector machines. 			
Module 1			Teaching Hours
Introduction to Soft computing: Neural networks, Fuzzy logic, Genetic algorithms, Hybrid systems and its applications. Fundamental concept of ANN, Evolution, basic Model of ANN, Terminologies used in ANN, MP model, Hebb model.			8 Hours
Module 2			
Perceptron Network: Adaptive linear neuron, Multiple adaptive linear neurons, Back propagation Network (Theory, Architecture, Algorithm for training, learning factors, testing and applications of all the above NN models).			8 Hours
Module 3			
Introduction to classical sets and fuzzy sets: Classical relations and fuzzy relations, Membership functions.			8 Hours
Module 4			
Defuzzification: Fuzzy decision making, and applications.			8 Hours
Module 5			
Genetic algorithms: Introduction, Basic operations, Traditional algorithms, Simple GA General genetic algorithms, The schema theorem, Genetic programming, applications.			8 Hours
Course Outcomes			
The students should be able to:			
<ul style="list-style-type: none"> • Implement machine learning through neural networks. • Design Genetic Algorithm to solve the optimization problem. • Develop a Fuzzy expert system. • Model Neuro Fuzzy system for clustering and classification. 			
Question paper pattern:			
The question paper will have ten questions.			
There will be 2 questions from each module.			
Each question will have questions covering all the topics under a module. The students will have to answer 5 full questions, selecting one full question from each module.			
Text Books:			
1. Principles of Soft computing, Shivanandam, Deepa S. N, Wiley India, ISBN 13: 788126527410, 2011			
Reference Books:			
1. Neuro-fuzzy and soft computing, J.S.R. JANG, C.T. SUN, E. MIZUTANI, Phi (EEE edition), 2012.			

COMPUTER NETWORKS AND INFORMATION SECURITY LABORATORY
[As per Choice Based Credit System (CBCS) scheme]
(Effective from the academic year 2016 -2017)
SEMESTER – I

Subject Code	16SCN16	IA Marks	20
Number of Lecture Hours/Week	01+03	Exam Marks	80
Total Number of Lecture Hours	50	Exam Hours	03

CREDITS – 02

Course objectives: This course will enable students to

- Demonste Concepts of fundamental protocols.
- Illustrate internetworking concepts.
- Implement concepts in congestion control and error detections.
- Evaluate fundamentals of Cryptography through practical implementation.
- Implement standard algorithms used to provide confidentiality, integrity and authenticity.
- Design security applications in the field of Information technology.

PART – A Computer Network LABORATORY WORK

Note:

Implement the following using C/C++ or equivalent with LINUX/Windows environment:

1. Write a program to transfer the contents of a requested file from server to the client using TCP/IP Sockets (using TCP/IP Socket programming).
2. Write a program to archive Traffic management at Flow level by implementing Closed Loop Control technique. (Leaky Bucket Algorithm)
3. Write a program to implement dynamic routing strategy in finding optimal path for data transmission. (Bellman ford algorithm).
4. Write a program to implement Link State Routing (Dijkstra Algorithm).
5. Write a program for implementing the error detection technique while data transfer in unreliable network code using CRC (16-bits) Technique.
6. Write a program for providing security for transfer of data in the network. (RSA Algorithm)
7. Write a program for encrypting 64 bit playing text using DES algorithm.

Simulation Programs using OPNET /NS2/NS3 or any other equivalent software

8. Simulate a 3 node point to point network with duplex links between them. Set the Queue size and vary the bandwidth and find the number of packets dropped.
9. Simulate a four-node point-to-point network, and connect the links as follows: n0->n2, n1->n2 and n2->n3. Apply TCP agent changing the parameters and determine the number of packets sent/received by TCP/UDP

PART – B INSLABORATORY WORK

2. Consider a file with composite data, substitute the content and transpose the ciphers.
3. Consider an alphanumeric data, encrypt and Decrypt the data using advanced encryption standards and verify for the correctness.
4. Apply the RSA algorithm on a text file to produce cipher text file.
5. Develop a mechanism to setup a security channel using Diffie-Hellman Key Exchange between client and server
6. Implementation of Message Authentication Code using cryptography VMAC function.
7. Implement secure hash algorithm for Data Integrity. Implement MD5 and SHA-1 algorithm, which accepts a string input, and produce a fixed size number - 128 bits for MD5; 160 bits for SHA-1, this number is a hash of the input. Show that a small change

- in the input results in a substantial change in the output
- Using any simulation tool: demonstrate packet filtering firewalls, create the ACL, create VLAN (Sub-netting).

Course Outcomes

The students should be able to:

- Apply key Internet applications and their protocols, and ability to develop their own applications (e.g. Client Server applications, Web Services) using the sockets API.
- Design and evaluate application layer protocol
- Analyze the vulnerabilities in any computing system and hence be able to design a security solution.
- Identify the security issues in the network and resolve it.
- Evaluate security mechanisms using rigorous approaches, including theoretical.

Conduction of Practical Examination:

- All laboratory experiments (nos) are to be included for practical examination.
- Students are allowed to pick one experiment from **each part and execute both**
- Strictly follow the instructions as printed on the cover page of answer script for breakup of marks
- PART –A:** Procedure + Conduction + Viva: **10 + 20 +10 (40)**
- PART –B:** Procedure + Conduction + Viva: **10 + 20 +10 (40)**
- Change of experiment is allowed only once and marks allotted to the procedure part to be made zero.**

SEMINAR [As per Choice Based Credit System (CBCS) scheme] (Effective from the academic year 2016 -2017) SEMESTER – I			
Subject Code	16SCE17 / 16SCN17 / 16LNI17 / 16SIT17 / 16SSE17 / 16SCS17 / 16SFC17	IA Marks	100
Number of Lecture Hours/Week	----	Exam Marks	-
Total Number of Lecture Hours	----	Exam Hours	-
CREDITS – 01			
Course objectives: This course will enable students to			
<ul style="list-style-type: none"> • Motivate the students to read technical article • Discover recent technology developments 			
Descriptions			
<p>The students should read a recent technical article (try to narrow down the topic as much as possible) from any of the leading reputed and refereed journals like:</p> <ol style="list-style-type: none"> 1. IEEE Transactions, journals, magazines, etc. 2. ACM Transactions, journals, magazines, SIG series, etc. 3. Springer 4. Elsevier publications etc <p>In the area of (to name few and not limited to)</p> <ul style="list-style-type: none"> • Web Technology • Cloud Computing • Artificial Intelligent • Networking • Security • Data mining 			
Course Outcomes			
<p>The students should be able to:</p> <ul style="list-style-type: none"> • Conduct survey on recent technologies • Infer and interpret the information from the survey conducted • Motivated towards research 			
Conduction:			
<p>The students have to present at least ONE technical seminar on the selected topic and submit a report for internal evaluation.</p>			
<p>Marks Distribution: Literature Survey + Presentation (PPT) + Report + Question & Answer + Paper: 20 + 30 + 30 + 20 (100).</p>			