VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

CURRICULUM AND SYLLABI

(2020-2021)

M.Tech (CSE) - Specialisation in Information Security

School of Computer Science and Engineering

M.Tech (CSE) - Specialisation in Information Security

CURRICULUM AND SYLLABUS

(2020-2021 Admitted Students)

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

VISION STATEMENT OF VELLORE INSTITUTE OF TECHNOLOGY

Transforming life through excellence in education and research.

MISSION STATEMENT OF VELLORE INSTITUTE OF TECHNOLOGY

World class Education: Excellence in education, grounded in ethics and critical thinking, for improvement of life.

Cutting edge Research: An innovation ecosystem to extend knowledge and solve critical problems.

Impactful People: Happy, accountable, caring and effective workforce and students.

Rewarding Co-creations: Active collaboration with national & international industries & universities for productivity and economic development.

Service to Society: Service to the region and world through knowledge and compassion.

VISION STATEMENT OF THE SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

To be a world-renowned centre of education, research and service in computing and allied domains.

MISSION STATEMENT OF THE SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

- To offer computing education programs with the goal that the students become technically competent and develop lifelong learning skill.
- To undertake path-breaking research that creates new computing technologies and solutions for industry and society at large.
- To foster vibrant outreach programs for industry, research organizations, academia and society.

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

M.Tech (CSE) - Specialization in Information Security

PROGRAMME EDUCATIONAL OBJECTIVES (PEOs)

1. Graduates will be engineering professionals who will engage in technology development and deployment with social awareness and responsibility.

2. Graduates will function as successful practising engineer / researcher / teacher / entrepreneur in the chosen domain of study.

3. Graduates will have holistic approach addressing technological, societal, economic and sustainability dimensions of problems and contribute to economic growth of the country.

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

M. Tech Computer Science and Engineering
Specialization in Information Security

PROGRAMME OUTCOMES (POs)

PO_1 Having an ability to apply mathematics and science in engineering applications

PO_2 Having an ability to design a component or a product applying all the relevant standards and with realistic constraints

PO_3 Having an ability to design and conduct experiments, as well as to analyze and interpret data

PO_4 Having an ability to use techniques, skills and modern engineering tools necessary for engineering practice

PO_5 Having problem solving ability- solving social issues and engineering problems

PO_6 Having adaptive thinking and adaptability

PO_7 Having a clear understanding of professional and ethical responsibility

PO_8 Having a good cognitive load management [discriminate and filter the available data] skills

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

School of Computer Science and Engineering

M.Tech(CSE) - Specialization in Information Security

PROGRAMME SPECIFIC OUTCOMES (PSOs)

1. The ability to design and develop computer programs/computer-based systems in the advanced level of areas including algorithms design and analysis, networking, operating systems design etc.

2. The ability to investigate and analyze using appropriate methodologies as well as security principles and apply ethically acceptable security solutions to mitigate cyber security threats.

3. Ability to bring out the capabilities for research and development in contemporary issues and to exhibit the outcomes as technical report.

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

M. Tech Computer Science and Engineering
Specialization in Information Security

CREDIT STRUCTURE

Category-wise Credit distribution

Category	Credits
University Core (UC)	**27**
Programme Core (PC)	**20**
Programme Elective (PE)	**17**
University Elective (UE)	**06**
Bridge Course (BC)	-
Total Credits	**70**

VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

CURRICULUM

M.Tech.-CSE (Spl. in Information Security) - (2020)

Programme Core	Programme Elective	University Core	University Elective	Total Credits
20	17	27	6	70

Course Code	Course Title	Course Type	L	T	P	J	C
PROGRAMME CORE							
CIS5001	Cryptosystems	ETL	2	0	2	0	3
CSE5001	Algorithms: Design and Implementation	ETL	2	0	2	0	3
CSE5002	Operating Systems and Virtualization	ETL	2	0	2	0	3
CSE5003	Database Systems: Design and Implementation	ETLP	2	0	2	4	4
CSE5004	Computer Networks	ETL	2	0	2	0	3
CSE6002	Information Security Foundations	ETP	3	0	0	4	4
Course Code	**Course Title**	**Course Type**	**L**	**T**	**P**	**J**	**C**
PROGRAMME ELECTIVE							
CIS6001	Cyber Attacks Detection and Prevention Systems	ETLP	2	0	2	4	4
CIS6002	Malware Analysis	ETLP	2	0	2	4	4
CIS6003	Penetration Testing and Vulnerability Assessment	ETLP	2	0	2	4	4
CIS6004	Wireless and Mobile Network Security	ETP	2	0	0	4	3
CIS6005	Multimedia Security	ETP	2	0	0	4	3
CIS6006	Cloud Security and Analytics	ETP	2	0	0	4	3
CIS6007	Secure Software Systems	ETP	2	0	0	4	3
CIS6008	Digital Forensics	ETLP	2	0	2	4	4
CIS6009	Trusted Network Systems	ETP	2	0	0	4	3
CIS6010	Critical Infrastructure Protection	ETP	2	0	0	4	3
CIS6011	Risk Detection, Management and Mitigation	ETP	2	0	0	4	3
CIS6012	Computer Security Audit and Assurance	ETP	2	0	0	4	3
CIS6013	Web Application Security	ETLP	2	0	2	4	4
Course Code	**Course Title**	**Course Type**	**L**	**T**	**P**	**J**	**C**
UNIVERSITY CORE							
CSE6099	Masters Thesis	PJT	0	0	0	0	16
MAT5002	Mathematics for Computer Engineering	TH	3	0	0	0	3
SET5001	Science, Engineering and Technology Project - I	PJT	0	0	0	0	2
SET5002	Science, Engineering and Technology Project - II	PJT	0	0	0	0	2
EFL5097	English and Foreign Language	CDB	0	0	0	0	2
ENG5001 - Fundamentals of Communication Skills - LO							
ENG5002 - Professional and Communication Skills - LO							
FRE5001 - Francais fonctionnel - TH							
GER5001 - Deutsch fuer Anfaenger - TH							
STS6777	Soft Skills M.Tech.	CDB	0	0	0	0	2
STS5001 - Essentials of Business Etiquettes - SS							
STS5001 - Essentials of Business Etiquette and Problem Solving - SS							

Course Code	Course Title	Course Type	L	T	P	J	C
STS5002 - Preparing for Industry - SS							
STS5102 - Programming and Problem Solving Skills - SS							
Course Code	**Course Title**	**Course Type**	**L**	**T**	**P**	**J**	**C**
BRIDGE COURSE							
Course Code	**Course Title**	**Course Type**	**L**	**T**	**P**	**J**	**C**
NON CREDIT COURSE							

CIS5001	CRYPTOSYSTEMS	L	T	P	J	C
		2	0	2	0	3
Pre-requisite		**Syllabus version**				
		1.0				

Course Objectives:

1. To provide an in-depth understanding of cryptography theories, algorithms and systems.
2. To provide necessary approaches and techniques to develop protection mechanisms in order to secure computer networks.

Expected Course Outcome:

1. Analyze and model the Symmetric cryptographic algorithms for information security.
2. Model the Public Key cryptosystems.
3. Apply the Integrity standards for information systems.
4. Identify the authentication schemes for membership authorization.
5. Understand how to apply access control techniques to authenticate the data.
6. Analyze the Cryptanalysis techniques.

Module:1	**Introduction to Wireless Sensor Networks**	**4 hours**

Introduction, Applications of Wireless Sensor Networks, WSN Standards, IEEE 802.15.4, Zigbee. Network Architectures and Protocol Stack – Network architectures for WSN, classification of WSN, protocol stack for WSN.

Module:2	**Wireless Transmission Technology and Systems**	**4 hours**

Wireless Transmission Technology and Systems – Radio Technology, Available Wireless Technologies.
Wireless Sensor Technology - Sensor Node Technology, Hardware and Software, Sensor Taxonomy, WN Operating Environment

Module:3	**Medium Access Control Protocols for Wireless Sensor Networks**	**5 hours**

Fundamentals of MAC Protocols, MAC Protocols for WSNs, Contention-Based protocols: Power Aware Multi-Access with Signaling - Data-Gathering MAC, Contention-Free Protocols: Low-Energy Adaptive Clustering Hierarchy, B-MAC, S-MAC. Dissemination Protocol for Large Sensor Network.

Module:4	**Deployment and Configuration**	**6 hours**

Target tracking, Localization and Positioning, Coverage and Connectivity, Single-hop and Multi-hop Localization, Self-Configuring Localization Systems.
Routing Protocols and Data Management for Wireless Sensor Networks - Routing Challenges and Design Issues in Wireless Sensor Networks, Routing Strategies in Wireless Sensor Networks, Routing protocols: data centric, hierarchical, location based energy efficient routing etc. Querying, Data Dissemination and Gathering.

Module:5	**Energy Efficiency and Power control**	**3 hours**

Need for energy efficiency and power control in WSN, passive power conservation mechanisms, active power conservation mechanisms		
Module:6	**Operating Systems For Wireless Sensor Networks**	**3 hours**
Operating System Design Issues, TinyOS, Contiki – Task management, Protothreads, Memory and IO management		
Module:7	**Sensor Network Platforms And Tools**	**3 hours**
Sensor Node Hardware – Tmote, Micaz, Programming Challenges, Node-level Software Platforms, Node-level Simulators, State-centric Programming.		
Module:8	**Recent trends**	**2 hours**
	Total Lecture hours:	**30 hours**

Text Book(s)	
1.	
Reference Books	
1.	Kazem Sohraby, Daniel Minoli, Taieb Znati, "Wireless Sensor Networks, Technology, Protocols and Applications", Wiley, 2007
2.	Holger Karl, Andreas Willig, "Protocols And Architectures for Wireless Sensor Networks", John Wiley, 2005.
3.	Jun Zheng, Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", Wiley, 2009.
4.	Ian F. Akyildiz, Mehmet Can Vuran, "Wireless Sensor Networks", Wiley, 2010
5.	Ibrahiem M. M. El Emary, S. Ramakrishnan, "Wireless Sensor Networks: From Theory to Applications", CRC Press Taylor & Francis Group, 2013
Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar	
Mode of assessment:	

Recommended by Board of Studies	**13-05-2016**		
Approved by Academic Council	**41**	**Date**	**17-06-2016**

CSE5001	ALGORITHMS: DESIGN AND IMPLEMENTATION	L	T	P	J	C
		2	0	2	0	3
Pre-requisite	**NIL**					**Syllabus version**
						1.0

Course Objectives:

1. To focus on the design of algorithms in various domains

2.To provide a foundation for designing efficient algorithms.

3.To provide familiarity with main thrusts of working algorithms-sufficient to gives context for formulating and seeking known solutions to an algorithmic problem.

Expected Course Outcome:

1. Solve a problem using Algorithms and design techniques
2. Solve complexities of problems in various domains
3. Implement algorithm, compare their performance characteristics, and estimate their potential effectiveness in applications
4. Solve optimization problems using simplex algorithm
5. Designing approximate algorithms for graph theoretical problems
6. Application of appropriate search algorithms for graphs and trees
7. Application of computational geometry method on optimization problems

Module:1	**Introduction**	**5 hours**
Algorithm design techniques : Divide and Conquer, Brute force, Greedy, Dynamic Programming. Time complexity (asymptotic notation, recurrence relations)		
Module:2	**Network Flows**	**5 hours**
Maximum Flows, Min-cost Flows, Max-Flow Min-Cut Theorem, Cycle Canceling Algorithms, Strongly Polynomial-time Analysis, Minimum Cuts without Flows		
Module:3	Tractable and Intractable Problems	**3 hours**
Class complexity: P, NP, NP-Hard, NP-Complete Approximation Algorithms		
Module:4	Approximation Algorithms	**3 hours**
Limits to Approximability, Vertex Cover problem, Set cover problem, Euclidean TSP		
Module:5	Search Algorithms for Graphs and Trees	**4 hours**
Limits to Approximability, Vertex Cover problem, Set cover problem, Euclidean TSP		
Module:6	Computational Geometry	**4 hours**
Line Segments, Convex hull finding algorithms		
Module:7	Linear Programming	**2 hours**
Representing problems-shortest paths, maximum flow ,and minimum-cost flow as linear programming problems. Simplex algorithm		

Module:8	Recent Trends	**2 hours**
	Total Lecture hours:	**30 hours**

Text Book(s)

Reference Books

1. Cormen, Leiserson, Rivest and Stein, Introduction to Algorithms, 3rd edition, McGraw-Hill, 2009.
2. J.Kleinberg and E.Tardos. Algorithm Design, Pearson Education, 2009.
3. E.Horowitz,S.Sahni,S.Rajasekaran,FundamentalsofComputerAlgorithms,2nd edition,Universities Press,2011.
4. Ravindra K.Ahuja, ThomasL. Magnanti, and JamesB.Orlin, Network Flows: Theory, Algorithms, and Applications, Pearson Education,2014.
5. GeorgeT.Heineman, GaryPollice,StanleySelkow,Algorithms in a nutshell,O'ReillyMedia, 2nd edition, 2016.

Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar

List of Challenging Experiments (Indicative)

1.	Implementation of algorithms for problems that can be solved by one or more of the following strategies : Divide and Conquer, Brute force, Greedy, Dynamic Programming.	2 hours
2.	Implementation of Ford Fulkerson method, Edmonds-Karp algorithm for finding maximum flow in a flow network and applying them for solving typical problems such as railway network flow, maximum bipartite matching	2 hours
3.	Implementation of Dinics strongly polynomial algorithm for computing them maximum flow in a flow network and applying it for solving typical problems	2 hours
4.	Implementation of push-relabel algorithm of Goldberg and Tarjan for finding maximum flow in a flow network and applying it for solving typical problems	2 hours
5.	Applying linear programming for solving maximum flow problem	2 Hours
6.	Applying network flow algorithms for baseball elimination and airline scheduling	2 Hours
7.	Given a flow network G=(V,E,s,t) ,where V is the vertex set, E is the edge set ,s and t are source and destination. An edge of the flow network is called critical if a decrease in the flow over that edge results in a decrease in the total flow of the flow network. An edge of the flow network is called a bottleneck edge if an increase in the flow over that edge results in an increase in the total flow of the flow network. Assume that you are using to compute the maximum flow of the network. (a) Write a program(any language)to identify all the critical edges. (b) Write a program (any language)to identify all bottleneck edges in the network.	3 Hours

8.	Implementation of solution techniques for the minimum-cost flow problem	2 hours
9.	Design a polynomial time algorithm to compute the solution of a linear programming problem in two dimensions. Your algorithm should convert each constrain to f the problem, into a planar region. Use that algorithm to compute the solution of the following problem. Implement your algorithm in any programming language. A manufacturer of furniture makes two products: chairs and tables. Processing of these products is done on two machines M1 and M2. A chair requires 2hours on machine M1and 6hours on machine M2. A table requires5 hours on machine M1and no time on machine M2.There are 16 hours of time per day available on machine M1and30 hours on machine M2. Profits gained by manufacturer from a chair and a table are Rs.1and Rs.5 respectively. The problem is to maximize the profit for the manufacturer.	2 hours
10.	Implementation of algorithms for the vertex cover problem, set cover problem, TSP	2 hours
11.	Implementation of search algorithms for graphs and trees: fundamental algorithms, Dijkstras algorithm	2 hours
12.	Consider the problem of barricading sleeping tigers by a fence of shortest length. Forest officials have tranquilized each tiger. Suggest an algorithm for the purpose. You are allowed to assume any information required for your algorithm. Implement your algorithm in any programming language (using convex hull)	3 hours
13.	A simple polygon is defined as a flat shape consisting of straight non-intersecting line segments or sides that are joined pairwise tofromaclosedpath.Letp1,p2,....,pn be a set of points in the two dimensional plane. (a) Write a program to find the simple polygon of P. (b) Write a program (linear time) to convert that the simple polygon of P to a Convex Hull.	3 hours
	Total Laboratory Hours	**30 hours**

Mode of assessment:			
Recommended by Board of Studies	**13.05.2016**		
Approved by Academic Council	41	**Date**	**17.06.2016**

CSE5002	OPERATING SYSTEMS AND VIRTUALIZATION	L	T	P	J	C
		2	0	2	0	3
Pre-requisite	**NIL**			**Syllabus version**		
				1.0		

Course Objectives:

1. To introduces Virtualization, operating systems fundamental concepts and its technologies
2. To provides skills to write programs that interact with operating systems components such as Processes, Thread, Memory during concurrent execution
3. To provide the skills and knowledge necessary to implement, provisioning and administer server and desktop virtualization

Expected Course Outcome:

1. Study operating system layers and kernel architectures
2. Design various techniques for process management
3. Construct various address translation mechanism
4. Perform process threading and synchronization
5. Study various methods of virtualization and perform desktop and server virtualization
6. Classify the light-weight virtual machines with dockers and containers
7. Develop programs related to the simulations of operating systems and virtualization concepts

Module:1	**Introduction**	**2 hours**

Computer system architecture a layered view with interfaces – Glenford Myer, Monolithic Linux Hybrid Windows10 kernels Layered architecture of operating system and core function a lists

Module:2	**Process**	**4 hours**

Introduction, Process Operations, States, Context switching, Data Structures (Process Control Block(PCB),Process Scheduling: Multi-Level Feedback Queue, Multi-processor Scheduling, Deadlocks and its detection

Module:3	**Memory**	**4 hours**

Introduction, Address Spaces, Memory API, Address Translation, Paging-Faster Translations (TLB), Smaller Tables. Virtual Memory System inx86

Module:4	**Concurrency**	**6 hours**

Introduction, Thread Models, Thread API, Building Evaluating a Lock, Test And Set, Two phase lock, Classical problems handling using semaphore. Persistence- File Organization: The i-node, Crash Consistency file security.

Module:5	**Virtual Machines**	**2 hours**

Process and System VMs Taxonomy of VMs

Module:6	**Types of Virtualization**	**4 hours**

Hardware Emulation, Full Virtualization with binary translation, Hardware assisted, Operating System Virtualization, OS assisted /Para virtualization.			
Module:7	**Hypervisor**		**7 hours**
Type 1, Type 2, Para virtualization, Server Virtualization, Desktop Virtualization, Overview VM portability-Clones, Templates, Snapshots, OVF, Hotand Cold Cloning Protecting Increasing Availability, Light Weight Virtual machine: Container /Docker			
Module:8	**Recent Trends**		**1 hours**
	Total Lecture hours:	**30 hours**	

Text Book(s)

1. Thomas Anderson, Michael Dahlin, Operating Systems: Principles and Practice, Second Edition, Recursive Books,2014
2. Matthew Portnoy, Virtualization Essentials, John Wiley Sons Inc; 2nd Edition, 2016

Reference Books

1. William Stallings, Operating Systems: Internals and Design Principles, 8thEdition
2. A.Silberschatz and P.Galvin. Operating System Concepts. Eight Edition, John Wiley Sons, 2008
3. Smith, Nair, Virtual Machines: Versatile Platforms for Systems and Processes, Morgan Kaufmann Publishers(2005)
4. Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar

Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar

List of Challenging Experiments (Indicative)		
1.	Study of Basic Linux Commands	2 hours
2.	Shell Programming (I/O, Decision making, Looping, Multi-level branching)	2 hours
3.	Crating child process using fork() system call, Orphan and Zombie process creation	2 hours
4.	Simulation of CPU scheduling algorithms (FCFS, SJF, Priority and Round Robin)	2hours
5.	Simulation of Banker s algorithm to check weather given system is in safe state or not. Also check whether addition resource requested can be granted immediately	4 hours
6.	Parallel Thread management using pthread library. Implement a data parallelism using multi-threading	4 hours
7.	Dynamic memory allocation algorithms - First-fit, Best-fit, Worst-fit algorithms	2 hours
8.	Page Replacement Algorithms FIFO, LRU and Optimal	4 hours
9.	Virtualization Setup: Type-1, Type-2 Hypervisor	4 hours
10.	Implementation of OS / Server Virtualization	4 hours
	Total Laboratory Hours	**30 hours**

Mode of assessment: ***Project/Activity***			
Recommended by Board of Studies	**13.05.2016**		
Approved by Academic Council	**41**	**Date**	**17.06.2016**

CSE5003	DATABASE SYSTEMS: DESIGN AND IMPLEMENTATION	L	T	P	J	C
		2	0	2	4	4
Pre-requisite	**NIL**	**Syllabus version**				
		1.0				

Course Objectives:

1. To emphasize the underlying principles of Relational Database Management System.
2. To model and design advanced data models to handle threat issues and counter measures.
3. To implement and maintain the structured, semi-structured and unstructured data in an efficient database system using emerging trends.

Expected Course Outcome:

1. Design and implement database depending on the business requirements and considering various design issues.
2. Select and construct appropriate parallel and distributed database architecture and formulate the cost of queries accordingly.
3. Understand the requirements of data and transaction management in mobile and spatial database and differentiate those with RDBMS.
4. Categorize and design the structured, semi-structured and unstructured databases.
5. Characterize the database threats and its counter measures.
6. Review cloud, streaming and graph databases.
7. Comprehend, design and query the database management system.

Module:1	**Relational Model**	**6 hours**

Database System Architecture–EER Modeling-Indexing–Normalization–Query processing and optimization – Transaction Processing

Module:2	**Parallel Databases**	**4 hours**

Architecture, Data partitioning strategy, Interquery and Intraquery Parallelism –Parallel Query Optimization

Module:3	**Distributed Databases**	**5 hours**

Features – Distributed Database Architecture –Fragmentation –Replication- Distributed Query Processing – Distributed Transactions Processing

Module:4	**Spatial and Mobile Databases**	**3 hours**

Spatial databases-Type of spatial data–Indexing in spatial databases, Mobile Databases– Transaction Model in MDS

Module:5	**SemiStructured Databases**	**4 hours**

Semi Structured databases – XML –Schema-DTD- XPath- XQuery, Semantic Web –RDF–RDFS

Module:6	**Database Security**	**3 hours**

Introduction to Database Security Issues–Security Models–Different Threats to databases– Counter

measures to deal with these problems		
Module:7	**Emerging Technologies**	**3 hours**
Cloud databases – Streaming Databases - Graph Databases-New SQL		
Module:8	**Recent Trends**	**2 hours**
	Total Lecture hours:	**30 hours**

Text Book(s)

1. AviSilberschatz,HankKorth,andS.Sudarshan,"DatabaseSystemConcepts",6thEd..McGraw Hill, 2010.
2. Ramez Elmasri B.Navathe: "Fundamentals of database systems", 7th edition, Addison Wesley,2014

Reference Books

1.S.K.Singh, "Database Systems: Concepts, Design Applications", 2nd edition, Pearson education, 2011.

2. Joe Fawcett, Danny Ayers, Liam R. E. Quin: "Beginning XML", Wiley India Private Limited5th Edition, 2012.

3. Thomas M. Connolly and Carolyn Begg "Database Systems: A Practical Approach to Design, Implementation, and Management", 6th edition, Pearson India, 2015.

Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar

List of Challenging Experiments (Indicative)

1.	Model any given scenario into ER/EER Model using any tool ERD Plus, ER Win, Oracle SQL developer)	1 hours
2.	Creating applications with RDBMS Table creation with constraints, alter schema, insert values, aggregate functions, simple and complex queries with joins PLSQL-PROCEDURES, CURSORS, FUNCTIONS, TRIGGERS	3 hours
3.	Partition a given database based on the type of query and compares the execution speed of the query with/without parallelism.	3 hours
4.	Create an XML document and validate it against an XML Schema/DTD. Use XQuery to query and view the contents of the database.	2hours
5.	Consider an application in which the results of football games are to be represented in XML,DTD and Xquery. For each game, we want to be able to represent the two teams involved ,which one was playing at home, which players scored goals(some of which may have been penalties)and the time when each was scored, and which players were shown yellow or red cards. You might use some attributes. You can check your solutions with the online demo of the Zorba XQueryengine4.	3 hours
6.	To implement parallel join and parallel sort algorithms to get marks from different colleges of the university and publish10 ranks for each discipline.	2 hours

7.	Create a distributed database scenario, insert values, fragment the database and query the database.	
8.	Consider a schema that contains the following table with the key underlined: Employee (Eno, Ename, Desg, Dno). Assume that we horizontally fragment the table as follows: Employee1(Eno; Ename; Desg;Dno), where 1¡= Dno ¡=10 Employee2(Eno;Ename; Desg; Dno), where 11 ¡= Dno ¡=20 Employee3 (Eno;Ename; Desg;Dno),where21¡=Dno¡=30In addition, assume we have 4 sites that contain the following fragments:Site1hasEmployee1Site2hasEmployee2Site3has Employee2andEmployee3Site4hasEmployee1Implementatleast5suitablequeries onEmployeefragments.Addrelationsto the database as per your requirements.	3 hours
9.	Download a spatial dataset based on any specific theme (containing layer information) from Quantum GIS and import it into Postgres SQL(PostGIS) and Query and view the database.	2 hours
10.	To investigation of some spatial analysis techniques using Toxic Release Inventory (www.epa.gov/triexplorer/) data for Massachusetts from the Environmental Protection Agency (EPA),which indicate the magnitude of the releases of toxic core chemicals into land, water and air ata site in the state. Note that these TRI locations were geo coded from a list of addresses provided by the EPA	3 hours
11.	Use sample datasets from health care domain, Visualize and interpret the results	3 hours
12.	Import the Hubway data intoNeo4jandconfigureNeo4j.Then, answer the following questions using the Cypher Query Language: a) List top 10 stations with most outbound trips (Show station name and number of trips) b) List top 10 stations with most inbound trips (Show station name and number of trips) c) List top 5 routes with most trips (Show starting station name, ending station name and number of trips) (4) List the hour number (for example 13 means 1pm -2pm) and number of trips which start from the station" B.U.Central" d)List the hour number(forexample13means1pm-2pm)and number of trips which end at the station "B.U. Central"	2 hours
	Total Laboratory Hours	**30 hours**

Mode of assessment: ***Project/Activity***			
Recommended by Board of Studies	**13.05.2016**		
Approved by Academic Council	**41**	**Date**	**17.06.2016**

CSE5004	COMPUTER NETWORKS	L	T	P	J	C
		2	0	2	0	3
Pre-requisite	**Nil**			**Syllabus version**		
				1.0		

Course Objectives:

1. Learn the division of network functionalities into layers.
2. Be familiar with the components required to build different types of networks and protocol
3. Understand the basic knowledge of software defined networks.

Expected Course Outcome:

1. Explore the basics of Computer Networks and various protocols.
2. Summarize the simple network management protocol components.
3. Interpret the characteristics of SDN controllers and their implications to learn the board aspects of security, overlay and network model.
4. Elaborate network function virtualization and network virtualization
5. Acquire the knowledge of SDN network security and network design implications of QoE/QoS.

Module:1	**Introduction**	**6 hours**

Network models, Addressing: Classful and Classless, Routing Protocols: unicast, multicast, Congestion control, Host configuration: DHCP, DNS.

Module:2	**Network Management**	**4 hours**

SNMP : Management Components, SMI, MIB, Configuration Management – Fault management – Performance Management – Accounting Management, Case studies.

Module:3	**Software Defined Networks**	**5 hours**

SDN Data plane, Control Plane, Application Plane. SDN security attack vectors and SDN Harderning, Overlay model and network model for cloud computing.

Module:4	**Network Functions Virtualization**	**3 hours**

Concepts, Benefits, requirements, Reference architecture, Management, Functionality and Infrastructure

Module:5	**Network Virtualization**	**4 hours**

Virtual LAN, Virtual Private Networks: IPSEC, MPLS, Network Virtualization Architecture and Benefits

Module:6	**Security**	**2 hours**

Security requirements, Threats to SDN, SDN security, NFV Security and its techniques

Module:7	**Network Design Implications of QoS and QoE**	**4 hours**

QoS Architectural Framework, SLA, IP Performance metrics, QoE: Strategies, Measurements, QoE/QoS Mapping models

Module:8	**RECENT TRENDS**		**2 hours**
	Total Lecture hours:	**30 hours**	

Text Book(s)

Reference Books

1. William Stallings, "Data and Computer Communication", Sixth Edition, Pearson Education, 2000.
2. Behrouz A. Forouzan, "TCP/IP Protocol Suite",Tata McGraw Hill edition, Fourth Edition. 2015.
3. William Stallings, "Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud" Pearson,2015
4. James F. Kuross, Keith W. Ross, "Computer Networking, A Top-Down Approach Featuring the Internet", Third Edition, Addison Wesley, 2004.
5. Andrew S. Tanenbaum, "Computer Networks", Fourth Edition, 2003.
6. Forouzan, A. Behrouz. "Data Communications & Networking (sie)". Tata McGraw-Hill Education, 2006.
7. Peterson and Bruce S. Davie Larry L.,"Computer Networks – A Systems approach" - , Morgan Kaufmann Publishers, Elsevier, 5th edition, 2012.

Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar

List of Challenging Experiments (Indicative)

1.	Study of different types of Network cables and Practically implement the cross-wired cable and straight through cable using crimping tool.	2 hours
2.	Study of Network Devices in Detail.	2 hours
3.	Study of network IP.	2 hours
4.	Web NMS (SNMP based)	2 hours
5.	Network Simulators	2 hours
6.	Implementation of routing protocols in MANETs	2 hours
7.	Network trouble shooting	2 hours
8.	Programs using network packet tracers	2 hours
9.	SDN Applications and Use Cases	2 hours
10.	Network Virtualization and Slicing	2 hours
11.	Network Function Virtualization (NFV)	2 hours
	Total Laboratory Hours	**22 hours**

Mode of assessment:

Recommended by Board of Studies	**13.05.2016**		
Approved by Academic Council	**No. xx**	**Date**	**17.06.2016**

CSE6002	INFORMATION SECURITY FOUNDATIONS	L	T	P	J	C
		3	0	0	4	4

Pre-requisite		Syllabus version
		1.0

Course Objectives:

1. To assess the current security landscape, including the nature of the threat, the general status of common vulnerabilities, and the likely consequences of security failures at network, server and application levels in CIA triad.
2. To justify the need for appropriate strategies and processes for disaster recovery and fault tolerance and propose how to implement them successfully.
3. To appraise the current information auditing, assurance, and computer forensics systems and procedures.

Expected Course Outcome:

1. Identify various vulnerabilities of computers network systems as well as the different modes of attack.
2. Explore and design techniques to prevent security attacks.
3. Identify the security solutions for servers like DNS, DHCP, WINS, Remote Access, NAT.
4. Explore the emerging security solutions for Web and Email using Firewall, SSL, TLS, SETand IPSec.
5. Develop the disaster recovery and fault tolerance systems.
6. Identify the need of information auditing, forensics security and RFID security.

Module:1	Information Security Fundamental	7 hours

Importance of Computer and Network Security CIAAN (Confidentiality, Integrity, Availability, Authentication, Non-Repudiation) - Business Needs -Threats and Countermeasures Attackers Policies and Standards - Legal, Ethical and Professional Issues Authentication, Authorization and Access Control Authentication Overview Credentials Protocols - Best practices for secure authentication -Services RADIUS (Remote Authentication Dial-In User Service), TACACS (Terminal Access Controller Access Control System), LDAP (Lightweight Directory Access Protocol); Authorization and Access Control - Access control model - Implementation on Windows - Implementation on Unix -Single Sign on

Module:2	Network Security	6 hours

VSecuring Network Transmission - Analyzing Security Requirements for Network Traffic - Defining Network Perimeters -Data Transmission Protection Protocols;

Module:3	Server Security	7 hours

Server Roles and Security Server Roles and Baselines - Securing Network Infrastructure Servers DNS. DHCP, WINS, Remote Access Servers, NAT servers Securing Domain Controllers - Securing File and Print Servers -Securing Application Servers

Module:4	Application Security	6 hours

Web Browser Security - Email Security Firewall VPN - Transport Layer Security (TLS) Handshake Protocol Alert Message Protocol Chan

Module:5	**Disaster Recovery and Fault Tolerance**	**6 hours**
Planning for the Worst -Creating a Backup Strategy -Designing for Fault Tolerance Antivirus Software Antivirus Features Typical signature - ByteStreams Checksums - Custom Check- sums - Cryptographic Hashes Advanced Signatures - Fuzzy Hashing - Graph-Based Hashes for Executable Files		
Module:6	**Information Auditing, Forensics Security and Assurance**	**7 hours**
Managing Updates - Auditing and Logging - Secure Remote Administration - Intrusion Detec- tion - Detection and Prevention -Honeypots, Honeynets and Padded Cell Systems -Scanning and Analysis Tools - Biometric Access Controls Forensics -Incident Response Procedures		
Module:7	**Other Security(Optical Network Security RFID Security)**	**4 hours**
Introduction Protection in SONET/SDH (Synchronous Optical Network/Synchronous Digital Hierarchy) - Protection in IP Networks Optical Layer Protection Schemes RFID (Radio Frequency Identification Device) Architecture, Standards, Applications RFID Challenges RFID Protections		
Module:8	**RECENT TRENDS**	**2 hours**
	Total Lecture hours:	**45 hours**

Text Book(s)

1. Cole, Eric, Rachelle Reese, Ronald L. Krutz, and James Conley. Network Security Fundamentals. United Kingdom: Wiley, John Sons, 2008. (ISBN No.: 978-0-470-10192-6).

2. Joshi, James, Bruce S. Davie, and Saurabh Bagchi. Network Security: Know It All. United States: Morgan Kaufmann Publishers In, 2008. (ISBN No.: 978-0-12-374463-0).

Reference Books

1. Peltier, Thomas R. Information Security Fundamentals. 2nd ed. CRC Press. Boca Raton, FL: Auerbach Publications, 2014. (ISBN No.: 978-1-4398-1063-7) (R1)
2. Vacca, John R., ed. Network and System Security. United States: Syngress Media,U.S., 2010. (ISBN No. : 978-1-59749-535-6) (R2)
3. Vacca, John R. Computer and Information Security Handbook. 2nd ed. San Francisco, CA: Morgan Kaufmann Publishers In, 2013. (ISBN No.: 978-0- 12-394397-2)
4. Ciampa, Mark. Security+ Guide to Network Security Fundamentals. 4th ed. Boston, MA: Course Technology, Cengage Learning, 2011. (ISBN No. : 978-1-111-64012-5)
5. Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar

Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar

Mode of assessment:

Recommended by Board of Studies	**13.05.2016**		
Approved by Academic Council	**No. 41**	**Date**	**17.06.2016**

CIS6001	CYBER ATTACK DETECTION AND PREVENTION SYSTEMS	L	T	P	J	C
		2	0	2	4	4
Pre-requisite	**Nil**	**Syllabus version**				
		1.0				

Course Objectives:

1. To understand the intrusion detection and prevention technologies, various types of network behavior analysis.
2. To understand the honeypots, multiple IDS methods, tools to analyze various types of attacks like wireless attacks and their detection.
3. To understand the the attack source and also provides practical knowledge for dealing with intrusions in real world applications.

Expected Course Outcome:

1. To understand the intrusion detection and prevention technologies, various types of network behavior analysis.
2. To understand the honeypots, multiple IDS methods, tools to analyze various types of attacks like wireless attacks and their detection.
3. To understand the the attack source and also provides practical knowledge for dealing with intrusions in real world applications.

Module:1	**Introduction to IDPS**	**3 hours**

IDPS Technologies, Components and Architecture Implementation Uses of IDPS Technologies, Key Functions, Common Detection Methodologies Signature, Anomaly and Stateful Protocol Analysis, Types of IDPS Technologies

Module:2	**Host and Network IDPS**	**4 hours**

Application, Transport, Network and Hardware Layer attacks, Sniffing Network Traffic, Replay Attacks, Command Injection, Internet Control Message Protocol Redirect, DDoS, Dangers and defenses with Man-in-the Middle, Secure Socket Layer attacks, DNS Spoofing, Defense- in-Depth Approach, Port Security, Use Encrypted Protocols

Module:3	**Network Behaviour Analysis**	**3 hours**

Components and Architecture Typical, Network Architecture, Sensor Locations.

Module:4	**Honeypots**	**5 hours**

Honeynets- Gen I, II and III, Honeymole, Detecting the Attack - Intrusion Detection, Network Traffic Capture, Monitoring on the box, Setting up the Realistic Environment.

Module:5	**Working with SNORT IDS**	**4 hours**

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

Module:6	**Multiple IDPS Technologies**	**4 hours**

Need for multiple IDPS Technologies, Integrating Different IDPS Technologies -Direct and Indirect, Firewalls, Routers and Honeypots, IPS using IP Trace back - Probabilistic and De- terministic Packet Marking, Marking

Module:7	**Wireless IDPS**	**5 Hours**

WLAN Standards, WLAN Components, Threats against WLANs, 802.11 Wireless Infrastruc- ture Attacks, WEP Attacks, Wireless Client Attacks, Bluetooth Attacks, Cellphones, Personal Digital Assistance and Other Hybrid Devices Attack Detection, Jailbreaking.

Module:8	**Contemporary issues:**		**2 hours**
RecentTrends			
	Total Lecture hours:	**30hours**	

Text Book(s) and Journals

1.Shui Yu, Distributed Denial of Service Attack and Defense, Springer, 2014 2.Bradd Lhotsky, OOSEC Host based Intrusion detection, PACKT Publication, 2013

Reference Books

1. John Hoopes, Virtualization for Security: Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis, and Honeypotting, Syngress,2009.
2. Karen Scarfone and Peter Mell, Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication 800-94, 2007

Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar

List of Challenging Experiments (Indicative)		
1.	Extract the features based on various color models and apply on image and video retrieval	6 hours
2.	Network monitoring, packet sniffing with Wire shark and Deep Packet inspection	6 hours
3.	Protocol and traffic analysis with MRTG and Performance measurement using PRTG for different sensors	6 hours
4.	Real time environment setup with honeynet and capturing intrusions and Analyzing the benchmark dataset to categorize the various kind of intrusion types	6 hours
5.	Analysis of SNORT IDS with ACID and Design custom rules for intrusion detection based on attack signatures with SNORT IDS	6 hours
6.	Comparative study of various IP traceback schemes and Tools available for wireless attack detection and prevention	6 hours
	Total Laboratory Hours	**30 hours**

Mode of assessment:			
Recommended by Board of Studies	**13-05-2016**		
Approved by Academic Council	**No. 41**	**Date**	**17-06-2016**

CIS6002	MALWARE ANALYSIS	L	T	P	J	C
		2	0	2	0	3
Pre-requisite		**Syllabus version**				
		1.0				

Course Objectives:

1. To recognize the types of malware through analysis methods
2.To learn basic and advanced malware analysis techniques
3.To practice the android malware analysis techniques for real world applications

Expected Course Outcome:

1.Identify various malwares and understand the behavior of malwares in real world applications.
2.Implement different malware analysis techniques.
3.Analyze the malware behavior in windows and android.
4.Understand the purpose of malware analysis.
5.Identify the various tools for malware analysis.

Module:1	**Introduction**	**3 hours**

Malware Analysis Goals of Malware Analysis, Techniques Static and Dynamic Analysis, Types of Malware Backdoor, Botnet, Downloader, Information Stealing malware, Launcher, Rootkit, Scareware, Worm or Virus.

Module:2	**Data Collection Methods**	**4 hours**

Volatile Data Collection Methodology-Preservation of Volatile Data, Physical Memory Acquisition on a Live Windows System, Identifying Users Logged into the System, Non-Volatile Data Collection Inspect Prefetch Files, Examine the File System, Remote Registry Analysis, Examine Web Browsing Activities, Examine Cookie Files.

Module:3	**Windows Basics**	**3 hours**

Introduction to Windows Malware - Windows Basics Relevant to Malware Behavior-File System and Directory structure, Registry, Boot Sequence, Malware payloads.

Module:4	**Dynamic Malware Analysis**	**5 hours**

Malware activities, Self-Start techniques, Essential setup for executing malware, Executing DLL files, Classifying Malware Based on their Behavior

Module:5	**Basic Static Analysis**	**4 hours**

Number System Static Analysis with File Attributes and PE Header Packet Identification

Module:6	**Advanced Static Analysis Reverse Engineering**	**4 hours**

Advanced Static Analysis Reverse Engineering Assembly level computing Standard x86 instructions, Introduction to IDA, OllyDbg, Advanced Malware Analysis Virus, Trojan. Parsing Basic Analysis of an APK.

Module:7	**Android Malware Analysis**	**5 hours**
APK File Structure Security Model Android Root Brief Description of Spreading and Dis- tribution Introduction to Android Debugging Tools and Their Usage Dex Structure Parsing Basic Analysis of an APK. Exploits MasterKey VulnerabilityFileNameLength Vulnerability Introduction to Obfuscation DEX code obfuscation		
Module:8	**RECENT TRENDS**	**2 hours**
	Total Lecture hours:	**30 hours**

Text Book(s)	
1.	
Reference Books	
1.	Cameron H. Malin, Eoghan Casey, James M. Aquilina and Curtis W. Rose, Malware Forensics Field Guide for Windows Systems, Syngress, Elsevier, 2012
2	Christopher C. Elisan , Advanced Malware Analysis, Tata McGraw Hill, 2015 3.Cameron H. Malin, Eoghan Casey, James M. Aquilina and Curtis W. Rose, Malware
3	Cameron H. Malin, Eoghan Casey, James M. Aquilina and Curtis W. Rose, Malware Forensics Field Guide for Linux Systems, Syngress, Elsevier, 2014.
4	Ken Dunham, Saeed Abu-Nimeh, Michael Becher and Seth Fogie, Mobile Malware Attacks and Defense, Syngress, Elsevier, 2009
5	John Aycock, Computer Viruses and Malware, Springer, 2006.
6	ErciFiliol, Computer Viruses: from theory to applications, Springer, 2005.

Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar

List of Challenging Experiments (Indicative)		
1.	Packet sniffing with Wire shark	3 hours
2.	Capturing intruders through packet inspection	3 hours
3.	Analysis of various Malware types and behavior	3 hours
4.	Basic Static Analysis	3 hours
5.	Basic Dynamic Analysis	3 hours
6.	Analyzing windows programs	3 hours
7.	Android malware analysis	3 hours
8.	Data encoding and malware countermeasures	3 hours
9.	Comparative study of various malware analysis tools	3 hours
10.	Tools available in Antivirus Application	3 hours
	Total Laboratory Hours	**30 hours**

Mode of assessment:			
Recommended by Board of Studies	**13.05.2016**		
Approved by Academic Council	**No. 41**	**Date**	**17.06.2016**

CIS6003	PENETRATION TESTING AND VULNERABILITY ASSESSMENT	L	T	P	J	C
		2	0	2	4	4
Pre-requisite		**Syllabus version**				
		1.0				

Course Objectives:

1. To learn the tools that can be used to perform information gathering.
2. To identify operating systems, server applications to widen the attack surface and perform vulnerability assessment activity and exploitation phase.
3. To learn how vulnerability assessment can be carried out by means of automatic tools or manual investigation.
4. To learn the web application attacks starting from information gathering to exploitation phases.
5. To learn how to metasploit and meterpreter are used to automate the attacks and penetration testing techniques.

Expected Course Outcome:

1. To understand the basic principles for Information Gathering and Detecting Vulnerabilities in the system.
2. Gain knowledge about the various attacks caused using the network and communication system in an application
3. Usage of exploits at various platforms
4. Helps to understand the various protocols defined for various network and server application.
5. Ability to determine the security threats and vulnerabilities in computer networks using penetration testing techniques
6. Using the acquired knowledge into practice for testing the vulnerabilities and identifying threats.
7. Acquiring knowledge about the tools used for penetration testing.

Module:1	**Information Gathering**	**4 hours**

Introduction - Terminologies - Categories of Penetration Testing - Phases of Penetration Test - Penetration Testing Reports - Information Gathering Techniques - Active, Passive and Sources of Information Gathering - Approaches and Tools - Traceroutes, Neotrace, Whatweb, Netcraft, Xcode Exploit Scanner and NSlookup. Host discovery - Scanning for open ports and services - Types of Port

Module:2	**Host discovery and Evading techniques**	**4 hours**

Vulnerability Scanner Function, pros and cons - Vulnerability Assessment with NMAP - Test- ing SCADA environment with NMAP - Nessus Vulnerability Scanner - Safe check - Silent dependencies - Port Range Vulnerability Data Resources

Module:3	**Vulnerability Scanner**	**5 hours**

SDN Data plane, Control Plane, Application Plane. SDN security attack vectors and SDN Harderning, Overlay model and network model for cloud computing.

Module:4	**Moile Application Security**	**4 hours**

Types of Mobile Application Key challenges in Mobile Application and its impact Need for mobile application penetration testing Mobile application penetration testing methodology Android and ios Vulnerabilities - OWASP mobile security risk - Exploiting WM - BlackBerry Vulnerabilities - Vulnerability Landscape for Symbian - Exploit Prevention - Handheld Exploita- tion

Module:5	**Common Vulnerability Analysis of Application Protocols**	**4 hours**

Testing for vulnerability web application and resources - Authentication Bypass with Insecure Cookie Handling - XSS Vulnerability - File inclusion vulnerability - Remote file Inclusion - Patching file Inclusions - Testing a website for SSI Injection.

Module:6	**Wireless Network Vulnerability Analysis**	**5 hours**

WLAN and its inherent insecurities Bypassing WLAN Authentication uncovering hidden SSIDs MAC Filters Bypassing open and shard authentication - Attacking the client caffe latte attack Deauthenticating the client cracking WEP with the hirte attack AP-less WPA cracking - Advanced WLAN Attacks Wireless eavesdropping using MITM session hijacking over wireless - WLAN Penetration Test Methodology.

Module:7	**Exploits**	**4 hours**

Architecture and Environment- Leveraging Metasploit on Penetration Tests, Understanding - Metasploit Channels, Metasploit Framework and Advanced Environment configurations - Un- derstanding the Soft Architecture, Configuration and Locking, Advanced payloads and addon modules Global datastore, module datastore, saved environment Meterpreter.

Module:8	**RECENT TRENDS**	**2 hours**

	Total Lecture hours:	**30 hours**	

Text Book(s)

1. Rafay Baloch, Ethical Hacking and Penetration Testing Guide, CRC Press, 2015. ISBN : 78-1-4822-3161-8.
2. Dr. Patrick Engebretson, The Basics of Hacking and Penetration Testing Ethical Hacking and Penetration Testing made easy , Syngress publications, Elsevier, 2013. ISBN :978-0-12-411644-3.
3. Andrew Whitaker and Daniel P. Newman, Penetration Testing and Network Defence The practical guide to simulating, detecting an responding to network attacks, Cisco Press, 2010. ISBN: 1-58705-208-3.
4. Vivek Ramachandran, BackTrack 5 Wireless Penetration Testing, Beginners guide Master bleeding edge wireless testing techniques with BackTrack 5, PACKT Publishing, 2011. ISBN 978-1-849515-58-0.
5. Mayor, K.K.Mookey, Jacopo Cervini, Fairuzan Roslan, Kevin Beaver, Metasploit Toolkit for Penetration Testing, Exploit Development and Vulnerability Research, Syngress publications, Elsevier, 2007. ISBN : 978-1-59749-074-0

Reference Books

Abhinav Singh, Metasploit Penetration Testing Cookbook, PACKT Publishing, 2012. ISBN 978-1-84951-742-3

Ken Dunham, Mobile Malware Attacks and Defence, Syngress Publisher 2009. ISBN: 978-1-59749-298-0

Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar		
List of Challenging Experiments (Indicative)		
1.	Set up of Kali Linux in a Virtual machine and setup with DNS info and collection of local network	2 hours
2.	Scan the network for Windows XP and Windows 7 Target machines in local network and virtual network	2 hours
3.	Identify the open ports and firewall rules setup	2 hours
4.	Use password guessing tools to guess a password. Use password strengthening tools to strengthen the password. Try guessing the password and tabulate the enhanced difficulty due to length of password and addition of special characters.	2 hours
5.	Extract password hashes from Windows XP/NT machine. Use a password extraction tool, using word list, single crack or external mode to recover the password. Increase the complexity of the password and determine the point at which the cracking tool fails.	2 hours
6.	Cracking Linux passwords	2 hours
7.	Experiments on SQL injections	2 hours
8.	Analysis of WEP flaws	2 hours
9.	Experiments on Wireless DoS Attacks	2 hours
10.	Prevention against Cross Site Scripting Attacks	2 hours
11.	Experiments on Metasploit Framework	2 hours
12.	Cross Site Scripting	2 hours
13.	Cross Site Request Forgery	2 hours
14.	File upload vulnerability on Social engineering	2 hours
	Total Laboratory Hours	**30 hours**
Mode of assessment:		
Recommended by Board of Studies	**13.05.2016**	
Approved by Academic Council	**No. 41**	**Date** **17.06.2016**

CIS6004	WIRELESS AND MOBILE NETWORK SECURITY	L	T	P	J	C
		2	0	0	4	3
Pre-requisite		**Syllabus version**				
		1.0				

Course Objectives:

1. To learn about securing wireless networks
2. Identify and analyze various the security issues in wireless mobile communication
3. To learn various issues of application level security in wireless environment and its related solution

Expected Course Outcome:

1. Identify the requirement of security and various issues at wireless and mobile network.
2. Analyze the threats in wireless environment including device, networks and servers.
3. Distinguish the attacks at various protocols in wireless network and differentiate the solution required for them.
4. Assess the security requirement for mobile adhoc environment, ubiquitous environment
5. Recognize the attacks in various environment and Report consequences of them.
6. Select an appropriate solution for security and Justify and demonstrate the usage of preventive measures and countermeasures.
7. Implement the security solution for various environment in wireless network

Module:1	**Security Issues in Mobile Communication**	**3 hours**

Mobile Communication History, Security Wired Vs Wireless, Security Issues in Wireless and Mobile Communications

Module:2	**Security of Device, Network, and Server Levels**	**6 hours**

Mobile Devices Security Requirements, Mobile Wireless network level Security, Server Level Security. Application Level Security in Wireless Networks - Application of WLANs, Wireless Threats, Security for 2G Wi-Fi Applications,Recent Security Schemes for Wi-Fi Applications

Module:3	**Application Level Security in Cellular Networks**	**5 hours**

Generations of Cellular Networks, Security Issues and attacks in cellular networks, GSM,GPRS and UMTS security for applications, 3G security for applications

Module:4	**Application Level Security in MANETs**	**3 hours**

MANETs, applications of MANETs, MANET Features, Security Challenges in MANETs, Security Attacks on MANETs.

Module:5	**Application Level Security in Ubiquitous Networks**	**3 hours**

Ubiquitous Computing, Need for Novel Security Schemes for UC, Security Challenges for UC

Module:6	**Application Level Security in Heterogeneous Wireless Networks**	**3 hours**

Heterogeneous Wireless network architecture, Heterogeneous network application in disaster management, Security problems and solutions in heterogeneous wireless networks.

Module:7	**Wireless Sensor Network Security**	**5 hours**
Attacks on wireless sensor networks and counter measures Prevention mechanisms: authenti- cation and traffic protection centralized and passive intruder detection decentralized intrusion detection		
Module:8	**RECENT TRENDS**	**2 hours**

	Total Lecture hours:	**30 ours**	

Project

1. Generally a team project [2 to 3members]
2. Concepts studied in Wireless and Mobile security should have been used.
3. Innovative idea should have been attempted
4. Sample : (a)Design and Implementation of Security algorithm for Wireless networks (b)Implementation of security protocol for mobile network

Text Book(s)

1.	

Reference Books

1.	Pallapa Venkataram, Satish Babu, Wireless and Mobile Network Security, First Edition, Tata McGraw Hill, 2010.
2	Hakima Chaouchi, Maryline Laurent-Maknavicius, Wireless and Mobile Network Security Security Basics, Security in On-the-shelf and Emerging Technologies, Wiley, 2009
3	Tara M. Swaminathan and Charles R. Eldon, Wireless Security and Privacy- Best Practices and Design Techniques, Addison Wesley, 2002.

Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar

Mode of assessment:

Recommended by Board of Studies	**13.05.2016**		
Approved by Academic Council	**No. 41**	**Date**	**17.06.2016**

CIS6005	MULTIMEDIA SECURITY	L	T	P	J	C
		2	0	0	4	3
Pre-requisite		**Syllabus version**				
		1.0				

Course Objectives:

1. Provide a framework to conduct research and development using multimedia security techniques.
2. Impart the knowledge of implementation on digital watermarking and multimedia security techniques.
3. Design a customary multimedia security system to suit real world applications.

Expected Course Outcome:

1. Learn the basic watermarking techniques to design a good digital mark.
2. Study the digital authentication and authorization schemes to evaluate security issues related to electronic documents, image and video.
3. Analyze the basic characteristics of digital watermarking to perform the theoretical analysis and performance measures.
4. Acquire the concepts of steganography to access the sensitive information concealing of file, message, image, or video within another file.
5. Obtain a suitable least significant bits construction and dynamic embedding with one-dimensional cellular automata to resist differential attack and support parallel computing.
6. Examine the multimedia encryption techniques to address the open issues related to confidentiality of the media content.
7. Develop a multimedia system including include multimedia compression techniques and standards, multimedia interfaces, video indexing and retrieval techniques.

Module:1	**Introduction to Digital Watermarking**	**5 hours**

Digital Watermarking Basics: Models of Watermarking, Basic Message Coding, Error Coding, Digital Watermarking Theoretic Aspects: Mutual information and Channel Capacity, Designing a good digital mark, Theoretical analysis of Digital watermarking

Module:2	**Watermarking Schemes**	**3 hours**

Spread Spectrum Watermarking, Transform Domain Watermarking, Quantization Watermark- ing

Module:3	**Media-Specific Digital Watermarking**	**4 hours**

Video Watermarking, Audio Watermarking, Binary Image Watermarking, Robustness to Tem- poral and Geometric Distortions, Affine resistant transformations

Module:4	**Steganography**	**5 hours**

Introduction- Digital Image formats- Modern Steganography, Steganography Channels Steganog- raphy Goals

Module:5	**Steganography Schemes**	**6 hours**

Image : Substitution, Bit Plane Coding, Transform Domain, Audio: Data Echo Hiding, Phase Coding, Video: Temporal technique, Spatial technique			
Module:6	**Multimedia Encryption**		**2 hours**
Introduction, Goals, Desired Characteristics, Performance metrics.			
Module:7	**Multimedia Techniques**		**3 hours**
Chaos based, Block based, Transform based techniques			
Module:8	**Contemporary Issues**: **RECENT TRENDS**		**2 hours**
	Total Lecture hours:	**30 hours**	

Text Book(s)	
	1. Shih, F. Y. (2017). Digital watermarking and steganography: fundamentals and techniques. 2. CRC press. 3. Nematollahi, Mohammad Ali, Vorakulpipat, Chalee, Rosales, Hamurabi Gamboa (2017). Digital Watermarking: Techniques and Trends, Springer, Signals and Communication 4. Pande, Amit, Zambreno, Joseph (2013). Embedded Multimedia Security Systems, Springer, Image Processing 5. Singh, Amit Kumar, Mohan, Anand (2019). Handbook of Multimedia Information Security: Techniques and Applications, Springer, Security and Cryptology.
Reference Books	
1.	Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T. (2007). Digital watermarking and steganography. Morgan kaufmann.
2	Yi, Xun, Paulet, Russell, Bertino, Elisa (2014). Homomorphic Encryption and Applications, Springer, Security and Cryptology.
Mode of assessment:	

Recommended by Board of Studies	**13.05.2016**		
Approved by Academic Council	**No. 41**	**Date**	**17.06.2016**

CIS6006	CLOUD SECURITY AND ANALYTICS	L	T	P	J	C
		2	0	0	4	3
Pre-requisite		**Syllabus version**				
		1.0				

Course Objectives:

1. To appraise the students with basic knowledge on security issues from the cloud providers and users perspective.
2. To teach a student how to secure private and public cloud.
3. 3. To explain students how to develop a prototype for cloud security

Expected Course Outcome:

1. Comprehend the basics of cloud platforms and risk issues in cloud computing.
2. Describe cloud security architecture, challenges and requirements.
3. Understand the functionalities of security protocols.
4. Identifying best practices and strategies for a secure cloud environment.
5. Illustrate how to perform security analytics in cloud platform.

Module:1	**Introduction**	**3 hours**

Review of cloud platforms and architectures Security issues from the cloud providers perspec- tive, users perspective Understanding security and privacy - Cloud Computing risk issues.

Module:2	**Securing the cloud**	**3 hours**

Security challenges Security requirements for the architecture - Securing private and public clouds Security patterns Cloud security architecture Infrastructure security.

Module:3	**Security Protocols and Standards**	**6 hours**

Host security, Compromise response, Security standards Message Level Security (MLS), Transport Level Security, OAuth, OpenID, eXtensible Access Control Markup Language (XACML), and Security Assertion Markup Language (SAML).

Module:4	**Strategies and Practices**	**4 hours**

Strategies and best practices Security controls: limits, best practices, monitoring Security criteria - assessing risk factors in Clouds.

Module:5	**Security management in the cloud**	**4 hours**

Security management in the cloud: SaaS, PaaS, IaaS availability management Security as a service-Trust Management for Security.

Module:6	**Security Analytics I**	**5 hours**

Techniques in Analytics - Challenges in Intrusion Detection System and Incident Identification DDoS attacks Analytics - Analysis of Log file - Simulation and Security Process.

Module:7	**Security Analytics II**	**3 hours**

Access Analytics - Security Analysis with Text Mining Security Intelligence and Breaches

Module:8	**Contemporary issues**		**2 hours**
	Total Lecture hours:	**30 hours**	

Text Book(s)	
	Ronald L. Krutz , Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud computing, Wiley 2010 Securing the Cloud: Cloud Computer Security Techniques and Tactics, by Vic (J.R) Winkler, Elseiver 2011
Reference Books	
	Ben Halpert , Auditing Cloud Computing: A Security and Privacy Guide: , John Wiley Sons, 2011. Ianlim, E.Coleen Coolidge, Paul Hourani, Securing Cloud and Mobility: A Practitioners Guide, Auerbach Publications, Feb 2013. Pethuru Raj, Cloud Enterprise Architecture, CRC Press, 2013. Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar
Mode of assessment:	

Recommended by Board of Studies	**13.05.2016**		
Approved by Academic Council	**No. 41**	**Date**	**17.06.2016**

CIS6007	SECURE SOFTWARE SYSTEMS	L	T	P	J	C
		2	0	2	0	3
Pre-requisite		**Syllabus version**				
		1.0				

Course Objectives:

1. To learn the development principles and process models of secure software engineering.
2. To study the requirements, modelling, design testing and validation procedures that ensure security.
3. To apply secure software engineering principles across cross-disciplines.

Expected Course Outcome:

1. Evaluate a secure software development process including designing secure applications, writing secure code against attacks.
2. Assess the reports through security testing procedures
3. Solve the security issues of vulnerabilities, flaws, and threats.
4. Identify and use the standard Secure Coding Principles for design secure software systems
5. Develop secured web programming to enhance the software code more resistant to attacks.
6. Identify the need of Security and safety metrics

Module:1	**Introduction**	**4 hours**

What is System engineering-Systems engineering and the systems-System engineering processes-Understanding Software systems engineering-The software system engineering processes-Steps in the software development processes-Functional and non-functional requirements Verification and validation

Module:2	**Engineering secure and safe systems**	**5 hours**

Introduction-The approach-security versus safety-Four approaches to develop critical systems- The dependability approach-The safety engineering approach-The secure systems approach- The real-time systems approach Security-critical and safety-critical systems

Module:3	**Architecting Secure Software Systems**	**5 hours**

Security Requirements Analysis, Threat Modelling, Security Design Patterns Anti-Patterns, Attack Patterns, Security Design Patterns, Authentication, Authorization -Security Coding Security Algorithm, Security Protocol, Key Generation

Module:4	**Validating Security**	**3 hours**

Generating the Executable, Security Testing vulnerability assessment, code coverage tools - Secured Deployment, Security Remediation, Security Documentation, Security Response Planning, Safety-Critical Systems

Module:5	**Secure Coding Principles**	**4 hours**

Coding in C String manipulation, vulnerabilities and exploits, Pointers based vulnerabilities. Coding

C++ and JAVA - Memory management, common errors, Integer Security, Double free Vulnerabilities		
Module:6	**Security in web-facing applications**	**4 hours**
Overview of web security, Identity Management, publickey infrastructure, Code injection, Parameter tampering, secured web programming, application vulnerability description language		
Module:7	**Security and safety metrics**	**3 hours**
Defining metrics-differentiating measures and metrics Software Metrics-Measuring and re- porting metrics Metrics for meeting requirements-Risk metrics-Security metrics for software systems-safety metrics for software systems		
Module:8	**RECENT TRENDS**	**2 hours**

	Total Lecture hours:	**30 hours**	

Text Book(s)	
1.	Defining metrics-differentiating measures and metrics Software Metrics-Measuring and re- porting metrics Metrics for meeting requirements-Risk metrics-Security metrics for software systems-safety metrics for software systems
Reference Books	
1.	Asoke K. Talukder, Manish Chaitanya, Architecting Secure Software Systems, ISBN 9781420087840, 2008
2	John Musa D, Software Reliability Engineering, 2nd Edition, Tata McGraw-Hill, 2005. Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar
Mode of assessment:	

Recommended by Board of Studies	**13.05.2016**		
Approved by Academic Council	**No. 41**	**Date**	**17.06.2016**

CIS6008	DIGITAL FORENSICS	L	T	P	J	C
		2	0	2	4	4
Pre-requisite	**Nil**				**Syllabus version**	
					1.0	

Course Objectives:

1. To learn the basics of digital forensics
2. To learn about the different digital forensic systems and services
3. To learn about file recovery using various tools
4. To learn about processing the crime scene and preserving digital evidence

Expected Course Outcome:

1. Describe what a digital investigation is, the sources of digital evidence, and the limitations of forensics
2. Describe the legal requirements for use of seized data
3. Conduct data collection on backup drives
4. Recover data based on a given search term from an imaged system
5. Capture and interpret network traffic
6. Handle the challenges associated with mobile device forensics 7.Handling forensics challenges in social and cloud computing

Module:1	Overview of Computer Forensics Technology	**4 hours**

Computer Forensics Fundamental- Types of Computer Forensics Technology

Module:2	**Computer Forensics system and Services**	**4 hours**

Types of Computer Forensics system Computer Forensics Services

Module:3	**Computer Forensics: Evidence Capture - Data Recovery and Data Seizure**	**4 hours**

Data Backup and Recovery Test Disk Suite, Data-Recovery Solution, Hiding and Recovering Hidden Data, Evidence Collection and Data Seizure

Module:4	**Duplication and Preservation of Digital Evidence**	**4 hours**

Preserving the Digital Crime scene, Computer Evidence Processing steps, Legal aspects of Collecting and Preserving Computer Forensic Evidence

Module:5	**Digital Forensics Tools and Platform**	**4 hours**

Tools (Encase)- Building software, Installing Interpreters, Working with images and File Sys- tems Forensics

Module:6	**Network Forensics and Operating System Artifacts**	**4 hours**

Network Forensic Scenario: Destruction of email, damaging computer evidence and System Testing.

Operating System Artifacts: Windows System Artifacts, Linux System Artifacts			
Module:7	**Mobile Forensics**		**4 hours**
Introduction to mobile forensics, understanding Android, Android forensic setup and predata extraction techniques, data recovery techniques			
Module:8	**Contemporary issues**		**2 hours**
	Total Lecture hours:	**30 hours**	

Text Book(s)		
1.	John R. Vacca, Computer Forensics: Computer Crime Scene Investigation, Second Edition, Charles River Media,2005	
2.	Cory Altheide, Harlan Carvey, Digital Forensics with Open Source Tools, British Library Cataloguing-in-Publication Data,2011.	
3.	Sathish Bommisetty, Rohit Tamma, Heather Mahalik, Practical Mobile Forensics, Kindle Edition, 2014	
4.	Greg Gogolin,Digital Forensics Explained,CRC Press,2013.	
Reference Books		
1.	David Lilburn Watson, Andrew Jones, Digital Forensics Processing and Procedures, Syngress,2013.	
2	Bill Nelson, Amelia Philips, Christopher Steuart, Guide to Computer Forensics and Investigations, Fifth Edition, Cengage Learning,2016	
Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar		
List of Challenging Experiments (Indicative)		
1.	File Recovery (Deleted, fragmented, hidden)	8 hours
2.	Network Forensics (Determining the type attacks, extracting files from network logs, encrypted files)	8 hours
3.	OS Forensics (Windows and Linux artifacts, memory, registry)	6 hours
4.	OS Forensics (Windows and Linux artifacts, memory, registry)	6 hours
5.	Mobile Forensics(Tools for Android and iOS)	4 hours
6.	Data backup and preservation and password recovery	4 hours
	Total Laboratory Hours	**36 hours**

Mode of assessment:			
Recommended by Board of Studies	**13.05.2016**		
Approved by Academic Council	**No. 41**	**Date**	**17.06.2016**

CIS6009	TRUSTED NETWORK SYSTEMS	L	T	P	J	C
		2	0	0	4	3
Pre-requisite	**Nil**				**Syllabus version**	
						1.0

Course Objectives:

1. To learn the need for End to end security in wireless communication networks
2. To learn about the security issues in communication networks. .
3. To understand the methods of securing Telephonic Network
4. To familiarise with the technologies that enable the operation of trusted network systems

Expected Course Outcome:

1.Review the basics of Certification and trust mechanisms that enable authenticated communication
2.Familiarize with the issues and technologies involved in designing a wireless and mobile system that is robust against various attacks
3.Gain knowledge and understanding of the various ways in which wireless networks can be attacked and trade offs in protecting networks
4.Attain a broad knowledge of the state-of-the-art and open problems in wireless end to end security
5.Become aware with the latest encryption techniques that enable secured communications
6.Analyse the techniques and standards used to implement Secured and trusted network systems
7.Categorise the attacks on the networks and anlyse the methods of ensuring security

Module:1	**Certificates and Public Key Infrastructure**	**3 hours**

X.509 Basic Certificate fields, RSA Certification- PKI Management Model- Certificate Life Cycle- CA Trust models Encryption algorithms supported in PKI- Two models for PKI De- ployment

Module:2	**Proactive Security Framework**	**6 hours**

Identity and Trust -Visibility - Correlation - Instrumentation and Management-Isolation and Virtualization -Anomaly Detection Zones -Network Device Virtualization -Policy Enforcement Visualization Techniques

Module:3	**Wireless Security**	**8 hours**

Overview of Cisco Unified Wireless Network Architecture -Authentication and Authorization of Wireless Users - Lightweight Access Point Protocol (LWAPP) - Wireless Intrusion Prevention System Integration - Precise Location Tracking -Network Admission Control (NAC) in Wireless Networks.

Module:4	**IP Telephony Security**	**3 hours**

Protecting the IP- Securing the IP Telephony Applications-Protecting Cisco Unified Call Manager- Protecting Against Eavesdropping Attacks

Module:5	**IPv6 Security**	**3 hours**
IPv6 Security -Filtering in IPv6 -ICMP Filtering - Extension Headers in IPv6 Spoofing - Broadcast Amplification or Smurf Attacks -IPv6 Routing Security IPsec and IPv6		
Module:6	**Data Center Security**	**3 hours**
-Protecting the Data Center Against Denial of Service (DoS) Attacks and Worms-Data Center Segmentation- Deploying Network Intrusion Detection and Prevention Systems		
Module:7	**Whats app Encryption**	**5 hours**
Introduction -Terms -Client Registration - Initiating Session Setup -Receiving Session Setup Exchanging Messages -Transmitting Media and Other Attachments -Group Messages -Call Setup - Verifying Keys -Transport Security-Conclusion		
Module:8	**Contemporary issues**	**2 hours**
	Total Lecture hours:	**30 hours**

Text Book(s)	
1.	O. Santos and Omar Lupi Da Rosa Santos, End-to-end network security: Defense-in- depth. Indianapolis, IN: Cisco Press, 2007. 2. G. Schudel and D. J. Smith, Router security strategies: Securing IP network traffic planes. United States: Cisco Press, 2007. 3. .
Reference Books	
1.	E. A. Fisch, G. B. White, and U. W. Pooch, Secure computers and networks: Analysis, design, and implementation. Boca Raton, FL: Taylor Francis, 1999.
Mode of assessment:	

Recommended by Board of Studies	**13.05.2016**		
Approved by Academic Council	**No. 41**	**Date**	**17.06.2016**

CIS6010	CRITICAL INFRASTRUCTURE PROTECTION	L	T	P	J	C
		2	0	0	4	3
Pre-requisite	**Nil**			**Syllabus version**		
						1.0

Course Objectives:

1. To introduce the concepts and components of CIP
2. To understand the complexity, and criticality interdependencies within the CIP specialty and among the National Critical Infrastructures (NCIs).

Expected Course Outcome:

1. Helps to understand the evolving threats affecting the critical infrastructure
2. Assess and manage risks that could lead to disruption in service.
3. Evaluate the ability of an organization against critical conditions.
4. Respond rapidly to any incident.
5. Quickly recover operations and service delivery.

Module:1	**Evolving threats to critical infrastructure**	**5 hours**

Critical Infrastructure Protection and Cyber Crime: What is Critical Infrastructure, Scien- tific and Technological Nature of Critical Infrastructure Vulnerabilities (The Electronic Power Grid, Other Critical Infrastructure), Internet Infrastructure Attacks (Internet Router Attacks, Domain Name Services (DNS) Attacks)

Module:2	**Critical infrastructure risk management framework**	**3 hours**

General policy frameworks for the protection of critical infrastructure, Security goals, identify assets, networks, and functions, asset risk, prioritize, effective measures.

Module:3	**Critical Infrastructure Risk in the Context of National Preparedness**	**6 hours**

Law enforcement and crime prevention, counter terrorism , national security and defense , emergency management, including the dissemination of information ,business continuity planning, protective security (physical, personnel and procedural),e-security ,natural disaster planning and preparedness, professional networking, and infrastructure development

Module:4	**Physical security essentials**	**5 hours**

Physical security threats, physical security prevention and mitigation measures, recovery from physical security breaches, threat assessment, planning and implementation. Border secu- rity, customs and immigration, an intelligent led risk informed approach, threat assessments, National Terrorism Threat Advisory System, Prevention and preparedness, Response and re- covery.

Module:5	**Public information and media management**	**3 hours**

Identification of Critical Infrastructure, Disaster recovery -Measuring risk and avoiding disaster, the business impact assessment

Module:6	**Biometric Security**	**7 hours**
Biometrics- Introduction- benefits of biometrics over traditional authentication systems bene- fits of biometrics in identification systems- Standards, biometric architecture, using biometric systems, security considerations, selecting a biometric for a system Applications Key bio- metric terms and processes - biometric matching methods -Accuracy in biometric systems. Physiological biometrics, behavioral biometrics, multi biometrics, Biometric document fraud and immigration law enforcement		
Module:8	**Recent Trends and applications**	**2 hours**
	Total Lecture hours:	**30 hours**

PROJECT

1. Generally a team project [2 to 3members]
2. Concepts studied in Wireless and Mobile security should have been used
3. Innovative idea should have been attempted
4. Sample :
   (a) Unimodal Biometric based authentication
   (b) Multimodal Biometric Based authentication
   (c) Project using Router attacks
   (d) Project using DNS attacks
   (e) A CIP-related topic upon which to write a critical analysis report.

	Total Laboratory Hours	**60 hours**	

Text Book(s)

1.	Collins, Pamela A., and Ryan K. Baggett. Homeland security and critical infrastructure protection. Praeger Security International, 2009.
2.	Anil K Jain, Patrick Flynn, Arun A Ross, Handbook of Biometrics, Springer, 2008 3.Vacca, John R. Cyber security and IT infrastructure protection. Syngress, 2013.

Reference Books

Mode of assessment:

Recommended by Board of Studies	**13.05.2016**		
Approved by Academic Council	**No. 41**	**Date**	**17.06.2016**

CIS6011	RISK DETECTION, MANAGEMENT AND MITIGATION	L	T	P	J	C
		2	0	0	4	3
Pre-requisite	**Nil**				**Syllabus version**	
						1.0

Course Objectives:

1. To discuss the main categories of risks which can affect a software project.
2. To introduce the knowledge of project risks and how to assess them.
3. To acquaint learners with the role and purpose of risk categories, management and containment..

Expected Course Outcome:

1. Identify and analyze various types of project risks.
2. Articulate risk consequences of uncertainty and within a continuum of decision making roles.
3. Perform quantitative risk analysis using risk measurement and management techniques.
4. Assess the severity and consequences of a risk as well as its overall threat.
5. Analyze a risk formally using established processes.
6. Illustrate security audit process.

Module:1	**Risk Identifications and Categorization**	**4 hours**

Identifying and categorizing the risks: Project Risks, Technical Risks, Business Risks.

Module:2	**Risk Analysis**	**4 hours**

Risk Analysis, Modes of risk analysis Effective Risk analysis, Risk Mitigation, Qualitative Risk Analysis, Value Analysis

Module:3	**Risk Management**	**4 hours**

Approaches to managing risks - reduction, mitigation transfer, and acceptance. Assets at risk, threats.

Module:4	**Risk Analysis Process**	**3 hours**

Formal risk analysis and management processes FRAPP, Information Security risk assessment process such at NIST, and OCTAVE

Module:5	**Risk Analysis Process**	**3 hours**

Risk assessment methodology flowchart, ranking of risks, avoiding risks, transferring risk, risk reduction and risk leverage

Module:6	**Risk Measurement, Metrics and Risk Mitigation**	**4 hours**

Value at Risk(VaR), Why VaR, Historical VaR.Risk Mitigation Options, Risk Mitigation Strat- egy, Residual Risk

Module:7	**Security Audit Process**	**4 hours**
Risk Management Life cycle activities, Information Security life cycle, Risk Assessment Process and Methodology, case study of IT organization		
Module:8	**Contemporary issues:RECENT TRENDS**	**2 hours**
	Total Lecture hours:	**30 hours**

Text Book(s)	
1.	Mark Talabis, Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis, Syngress; 1 edition, ISBN: 978-1-59749-735-0, 2012.
2.	Thomas R Peltier, Information Security Risk Analysis.CRC Press,2001.
Reference Books	
1.	Marian Myerson, Risk Management Processes for Software Engineering Models by, Library of Congress Cataloging Publication, Norwood, USA, 2013.
Mode of assessment:	

Recommended by Board of Studies	**13.05.2016**		
Approved by Academic Council	**No. 41**	**Date**	**17.06.2016**

CIS6012	COMPUTER SECURITY AUDIT AND ASSURANCE	L	T	P	J	C
		2	0	0	4	3
Pre-requisite					**Syllabus version**	
					1.0	

Course Objectives:

1. To understand the fundamental concepts in computer security and auditing process
2. To understand the auditing process and role of auditing in computer security
3. To understand the fundamental concepts for information system auditing
4. To provide an overall view about the computer assisted audit tools and techniques
5. To design an audit plan for model information system using various kinds of auditing tool

Expected Course Outcome:

1. Understand the fundamental methods used in information system auditing process
2. Understand the role of auditor and how to prepare the auditing plan for information system auditing
3. Extract the information and plan for conducting the testing process for information system auditing
4. Apply computer assisted audit tools for auditing process and prepare an audit document
5. Evaluating the IT audit and Quality of the audit report
6. Design a security architecture for an information system with all the information policy and responsibilities 7.Design an audit plan for E-commerce application and mobile applications

Module:1	**Foundation for IT Audit and Assurance**	**3 hours**

Assurance Services - Need for Assurance - Characteristics of Assurance Services-Types of Assurance Services E-Commerce and Electronic Funds Transfer - Future of electronic payment system.

Module:2	**Audit Process**	**4 hours**

Audit Standards - Types of Auditors and their functions - Internal Audit Function and External Auditor. Audit Plan - Developing an Audit Schedule - Audit Budget - Preliminary Review - Audit Findings - Analysis Re-examination - Verification - Recommendations - Communication Strategy

Module:3	**Conducting Information System Audit**	**3 hours**

Standards - Practices and Guidelines - Information Gathering Techniques - Vulnerability - System Security Testing - Development of Security Requirements Checklist.

Module:4	**Computer Assisted Audit Tools and Techniques**	**5 hours**

Auditor Productivity Tools - Data and Resource Management - Flowcharting Techniques - Flowcharting as an analysis tool - Developing Audit Data Flow Diagrams - Appropriateness of flowcharting techniques - Computer assisted tools for operational reviews - Web Analysis tools

Module:5	**Managing IT Audit**	**4 hours**

Evaluating IT Audit Quality - Criteria for assessing the audit - Criteria for assessing the auditor - Best Practices in IT Audit Planning - IT Governance: Performance Measurement - Metrics and Management - Metric Reporting and Independent Assurance.

Module:6	**Security and Service continuity**	**4 hours**
Security Standards - ISO 27002 and National Institute of Standards and Technology - Information Security Controls - Security Architecture - Information Security Policy -Information Owner Responsibilities - Third- Party Responsibilities		
Module:7	**Virtual Application Security and ERP security**	**5 hours**
Intranet/Extranet Security - Identity Theft - E-Commerce Application Security as a strategic and structural problem - Planning and Control Approach to E-Commerce Security Management - Internet Security and Mobile Computing Security - ERP Data Warehouse-Data Warehouse integrity checklist - ERP-Security features of the basic component.		
Module:8	**RECENT TRENDS**	**2 hours**

	Total Lecture hours:	**30 hours**	

Text Book(s)	
1.	Information Technology Control and Audit, Fourth Edition, Sandra Senft, Frederick Gallegos, Aleksandra Davis, CRC Press, 2012.
Reference Books	
1.	Information System Audit and Assurance, D P Dube, V P Gulati, Tata Mc-Graw Hill, 2008
2	Micheal E.Whitman, Herbert J.Mattor, "Principles of Information Security", Course Technology, Delmar Cengage Learning, Fourth Edition, 2012.
3	Jennifer L.Bayuk, Jason Healey, Paul Rohmeyer and Marcus Sachs, "Cyber Security Policy Guidebook", John Wiley Sons, Kindle Edition, 2012
Mode of assessment:	

Recommended by Board of Studies	**13.05.2016**		
Approved by Academic Council	**No. 41**	**Date**	**17.06.2016**

CIS6013	WEB APPLICATION SECURITY	L	T	P	J	C
		2	0	0	4	3
Pre-requisite	**Nil**				**Syllabus version**	
					1.0	

Course Objectives:

1. To reveal the underlying in web application.
2. To identify and aid in fixing any security vulnerabilities during the web development process.
3. To understand the security principles in developing a reliable web application.

Expected Course Outcome:

1. Identify the vulnerabilities in the web applications.
2. Identify the various types of threats and mitigation measures of web applications.
3. Apply the security principles in developing a reliable web application.
4. Use industry standard tools for web application security.
5. Apply penetration testing to improve the security of web applications.

Module:1	**Overview of Web Applications**	**2 hours**

Introduction history of web applications interface ad structure benefits and drawbacks of web applications Web application Vs Cloud application.

Module:2	**Web Application Security Fundamentals**	**3 hours**

Security Fundamentals: Input Validation - Attack Surface Reduction Rules of Thumb- Classi- fying and Prioritizing Threads

Module:3	**Browser Security Principles**	**4 hours**

Origin Policy - Exceptions to the Same-Origin Policy - Cross-Site Scripting and Cross-Site Request Forgery - Reflected XSS - HTML Injection

Module:4	**Web Application Vulnerabilities**	**6 hours**

Understanding vulnerabilities in traditional client server application and web applications, client state manipulation, cookie based attacks, SQL injection, cross domain attack (XSS/XSRF/XSSI) http header injection. SSL vulnerabilities and testing - Proper encryption use in web application
- Session vulnerabilities and testing - Cross-site request forgery

Module:5	**Web Application Mitigations**	**5 hours**

Http request , http response, rendering and events , html image tags, image tag security, issue, java script on error , Javascript timing , port scanning , remote scripting , running remotecode, frame and iframe , browser sandbox, policy goals, same origin policy, library import, domain relaxation

Module:6	**Secure Website Design**	**5 hours**
Secure website design : Architecture and Design Issues for Web Applications, Deployment Considerations Input Validation, Authentication, Authorization, Configuration Management ,Sen- sitive Data, Session Management, Cryptography, Parameter Manipulation, Exception Manage- ment, Auditing and Logging, Design Guidelines, Forms and validity, Technical implementation		
Module:7	**Cutting Edge Web Application Security**	**3 hours**
Clickjacking - DNS rebinding - Flash security - Java applet security - Single-sign-on solution and security - IPv6 impact on web security		
Module:8	**RECENT TRENDS**	**2 hours**

	Total Lecture hours:	**30 hours**	

Text Book(s)	
1.	Sullivan, Bryan, and Vincent Liu. Web Application Security, A Beginner's Guide. McGraw Hill Profe ssional, 2011.
2.	Stuttard, Dafydd, and Marcus Pinto. The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. John Wiley Sons, 2011
Mode of assessment:	

Recommended by Board of Studies	**13.05.2016**		
Approved by Academic Council	**No. 41**	**Date**	**17.06.2016**

MAT5002	Mathematics for Computer Engineering	L	T	P	J	C
		3	0	0	0	3

Pre-requisite	Nil	Syllabus version
		1.0

Course Objectives:

Expected Course Outcome:

Module:1	Proof Techniques	6hours

Implications, equivalences, converse, inverse, contrapositive, negation, contradiction, structure, direct proofs, disproofs, natural number induction, structural induction,
weak/string induction, recursion, well orderings

Module:2	Linear algebra:	6 hours

Eigenvalues and eigenvectors-Gerschgorin Circles– Rutishauser method, Rotation and Reflection matrices- Face Recognition application.

Module:3	Number Theory	6hours

Divisibility -division algorithm -Euclidean algorithm- Definitions and basic properties of congruences - Solving linear congruences and quadratic congruences, Applications of congruences: The Chinese remainder theorem, Euler's theorem and Fermat's little theorem- Primarily checking

Module:4	Probability	6hours

Introduction to random variable -Binomial and Poisson distributions – Normal distribution, Weibull, exponential and Gamma distributions Performance modeling
application

Module:5	Statistical Measures	6hours

Correlation and regression- Covariance– partial and multiple correlation- multiple regression – Time Series data Analysis application.

Module:6	Sampling Theory	8hours

small sample tests- student's t –test ,F-test, chi-square test, goodness of fit , independence of attributes, Basic principles of experimentation, Analysis of variance –

application using Monte-Carlo methods and decision trees

Module:7	**Queuing Theory**		**5hours**
Introduction-Markov Process-Poisson Process-Pure Berth Process-Death Process-Birth-death processes- Queue notation-Little's theorem-Queuing models M/M/1; M/M/c; M/M/∞			
Module:8	**Expert Lecture**		**2hours**
Modular arithmetic-Applications to cryptosystem			
	Total Lecture hours:	**45 hours**	
Text Book(s)			
Reference Books			

1. Neal Koblitz, A course in number theory and cryptography, Springer reprint (2002).
2. J. P. Tremblay and R Manohar Discrete Mathematical Structures with applications to Computer Science, Tata McGraw Hill (2001).
3. Ronald E. Walpole , Raymond H. Myers Sharon L. Myers Keying E. Ye, Probability and Statistics for Engineers and Scientists (9^{th} Edition),
4. H. A .Taha Operations Research, 9^{th} Edition, PHI (2010).
5. Narasingh Deo, Graph Theory, PHI, 23^{rd} Indian reprint (2002).

Mode of assessment:			
Recommended by Board of Studies	**09-03-2016**		
Approved by Academic Council	**No. 40**	**Date**	

SET5001	SCIENCE, ENGINEERING AND TECHNOLOGY PROJECT– I	L	T	P	J	C
						2
Pre-requisite		**Syllabus Version**				
Anti-requisite		1.0				

Course Objectives:

- To provide opportunity to involve in research related to science / engineering
- To inculcate research culture
- To enhance the rational and innovative thinking capabilities

Expected Course Outcome:

On completion of this course, the student should be able to:

1. Identify problems that have relevance to societal / industrial needs
2. Exhibit independent thinking and analysis skills
3. Demonstrate the application of relevant science / engineering principles

Modalities / Requirements

1. Individual or group projects can be taken up
2. Involve in literature survey in the chosen field
3. Use Science/Engineering principles to solve identified issues
4. Adopt relevant and well-defined / innovative methodologies to fulfill the specified objective
5. Submission of scientific report in a specified format (after plagiarism check)

Student Assessment : Periodical reviews, oral/poster presentation

Recommended by Board of Studies	17-08-2017		
Approved by Academic Council	No. 47	Date	05-10-2017

SET5002	SCIENCE, ENGINEERING AND TECHNOLOGY PROJECT– II	L	T	P	J	C
						2
Pre-requisite		**Syllabus Version**				
Anti-requisite		1.0				

Course Objectives:

1. To provide opportunity to involve in research related to science / engineering
2. To inculcate research culture
3. To enhance the rational and innovative thinking capabilities

Expected Course Outcome:

1. Identify problems that have relevance to societal / industrial needs
2. Exhibit independent thinking and analysis skills
3. Demonstrate the application of relevant science / engineering principles

Modalities / Requirements

6. Individual or group projects can be taken up
7. Involve in literature survey in the chosen field
8. Use Science/Engineering principles to solve identified issues
9. Adopt relevant and well-defined / innovative methodologies to fulfill the specified objective
10. Submission of scientific report in a specified format (after plagiarism check)

Student Assessment : Periodical reviews, oral/poster presentation

Recommended by Board of Studies	17-08-2017		
Approved by Academic Council	No. 47	Date	05-10-2017

ENG5001	Fundamentals of Communication Skills	L	T	P	J	C
		0	0	2	0	1
Pre-requisite	Not cleared EPT (English Proficiency Test)	**Syllabus version**				
		1.0				

Course Objectives:

1. To enable learners learn basic communication skills - Listening, Speaking, Reading and Writing
2. To help learners apply effective communication in social and academic context
3. To make students comprehend complex English language through listening and reading

Expected Course Outcome:

1. Enhance the listening and comprehension skills of the learners
2. Acquire speaking skills to express their thoughts freely and fluently
3. Learn strategies for effective reading
4. Write grammatically correct sentences in general and academic writing
5. Develop technical writing skills like writing instructions, transcoding etc.,

Module:1	Listening	**8 hours**

Understanding Conversation
Listening to Speeches
Listening for Specific Information

Module:2	Speaking	**4 hours**

Exchanging Information
Describing Activities, Events and Quantity

Module:3	Reading	**6 hours**

Identifying Information
Inferring Meaning
Interpreting text

Module:4	Writing: Sentence	**8hours**

Basic Sentence Structure
Connectives
Transformation of Sentences
Synthesis of Sentences

Module:5	Writing: Discourse	**4hours**

Instructions
Paragraph
Transcoding

	Total Lecture hours:	**30 hours**

Text Book(s)

1. Redston, Chris, Theresa Clementson, and Gillie Cunningham. *Face2face Upper Intermediate Student's Book.* 2013, Cambridge University Press.

Reference Books

1. Chris Juzwiak .*Stepping Stones: A guided approach to writing sentences and Paragraphs (Second Edition)*, 2012, Library of Congress.
2. Clifford A Whitcomb & Leslie E Whitcomb, *Effective Interpersonal and Team Communication Skills for Engineers*, 2013, John Wiley & Sons, Inc., Hoboken: New Jersey.

3.	ArunPatil, Henk Eijkman &Ena Bhattacharya, *New Media Communication Skills for Engineers and IT Professionals,*2012, IGI Global, Hershey PA.	
4.	Judi Brownell, *Listening: Attitudes, Principles and Skills*, 2016, 5th Edition, Routledge:USA	
5.	John Langan, Ten Steps to Improving College Reading Skills, 2014, 6th Edition, Townsend Press:USA	
6.	Redston, Chris, Theresa Clementson, and Gillie Cunningham. *Face2face Upper Intermediate Teacher's Book.* 2013, Cambridge University Press.	
	Authors, book title, year of publication, edition number, press, place	
Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar		
List of Challenging Experiments (Indicative)		
1.	amiliarizing students to adjectives through brainstorming adjectives with all letters of the English alphabet and asking them to add an adjective that starts with the first letter of their name as a prefix.	2 hours
2.	aking students identify their peer who lack Pace, Clarity and Volume during presentation and respond using Symbols.	4 hours
3.	sing Picture as a tool to enhance learners speaking and writing skills	2 hours
4.	sing Music and Songs as tools to enhance pronunciation in the target language / Activities through VIT Community Radio	2 hours
5.	Making students upload their Self- introduction videos in Vimeo.com	4 hours
6.	Brainstorming idiomatic expressions and making them use those in to their writings and day to day conversation	4 hours
7.	Making students Narrate events by adding more descriptive adjectives and add flavor to their language / Activities through VIT Community Radio	4 hours
8	Identifying the root cause of stage fear in learners and providing remedies to make their presentation better	4 hours
9	Identifying common Spelling & Sentence errors in Letter Writing and other day to day conversations	2 hours
10.	iscussing FAQ's in interviews with answers so that the learner gets a better insight in to interviews / Activities through VIT Community Radio	2 hours
	Total Laboratory Hours	**32 hours**
Mode of evaluation: Online Quizzes, Presentation, Role play, Group Discussions, Assignments, Mini Project		
Recommended by Board of Studies	22-07-2017	
Approved by Academic Council	No. 46	Date 24-8-2017

ENG5002	Professional and Communication Skills	L	T	P	J	C
		0	0	2	0	1
Pre-requisite	ENG5001	**Syllabus version**				
		v. 1.1				

Course Objectives:

1. To enable students to develop effective Language and Communication Skills
2. To enhance students' Personal and Professional skills
3. To equip the students to create an active digital footprint

Expected Course Outcome:

1. Improve inter-personal communication skills
2. Develop problem solving and negotiation skills
3. Learn the styles and mechanics of writing research reports
4. Cultivate better public speaking and presentation skills
5. Apply the acquired skills and excel in a professional environment

Module:1	**Personal Interaction**	**2hours**
Introducing Oneself- one's career goals Activity: SWOT Analysis		
Module:2	**Interpersonal Interaction**	**2 hours**
Interpersonal Communication with the team leader and colleagues at the workplace Activity: Role Plays/Mime/Skit		
Module:3	**Social Interaction**	**2 hours**
Use of Social Media, Social Networking, gender challenges Activity: Creating LinkedIn profile, blogs		
Module:4	**Résumé Writing**	**4 hours**
Identifying job requirement and key skills Activity: Prepare an Electronic Résumé		
Module:5	**Interview Skills**	**4 hours**
Placement/Job Interview, Group Discussions Activity: Mock Interview and mock group discussion		
Module:6	**Report Writing**	**4 hours**
Language and Mechanics of Writing Activity: Writing a Report		
Module:7	**Study Skills: Note making**	**2hours**
Summarizing the report Activity: Abstract, Executive Summary, Synopsis		
Module:8	**Interpreting skills**	**2 hours**
Interpret data in tables and graphs Activity: Transcoding		
Module:9	**Presentation Skills**	**4 hours**
Oral Presentation using Digital Tools Activity: Oral presentation on the given topic using appropriate non-verbal cues		
Module:10	**Problem Solving Skills**	**4 hours**
Problem Solving & Conflict Resolution Activity: Case Analysis of a Challenging Scenario		
	Total Lecture hours:	**30hours**

Text Book(s)				
1	Bhatnagar Nitin and Mamta Bhatnagar, *Communicative English For Engineers And Professionals*, 2010, Dorling Kindersley (India) Pvt. Ltd.			
Reference Books				
1	Jon Kirkman and Christopher Turk, *Effective Writing: Improving Scientific, Technical and Business Communication*, 2015, Routledge			
2	Diana Bairaktarova and Michele Eodice, *Creative Ways of Knowing in Engineering*, 2017, Springer International Publishing			
3	Clifford A Whitcomb & Leslie E Whitcomb, *Effective Interpersonal and Team Communication Skills for Engineers*, 2013, John Wiley & Sons, Inc., Hoboken: New Jersey.			
4	ArunPatil, Henk Eijkman &Ena Bhattacharya, *New Media Communication Skills for Engineers and IT Professionals,*2012, IGI Global, Hershey PA.			
Mode of Evaluation: CAT / Assignment / Quiz / FAT / Project / Seminar				
List of Challenging Experiments (Indicative)				
1.	WOT Analysis – Focus specially on describing two strengths and two weaknesses			2 hours
2.	ole Plays/Mime/Skit -- Workplace Situations			4 hours
3.	se of Social Media – Create a LinkedIn Profile and also write a page or two on areas of interest			2 hours
4.	pare an Electronic Résumé and upload the same in vimeo			2 hours
5.	Group discussion on latest topics			4 hours
6	Report Writing – Real-time reports			2 hours
7	Writing an Abstract, Executive Summary on short scientific or research articles			4 hours
8	Transcoding – Interpret the given graph, chart or diagram			2 hours
9	Oral presentation on the given topic using appropriate non-verbal cues			4 hours
10	blem Solving -- Case Analysis of a Challenging Scenario			4 hours
			Total Laboratory Hours	**32 hours**
Mode of evaluation: : Online Quizzes, Presentation, Role play, Group Discussions, Assignments, Mini Project				
Recommended by Board of Studies	22-07-2017			
Approved by Academic Council	No. 47	Date	05-10-2017	

FRE5001	FRANCAIS FONCTIONNEL	L	T	P	J	C
		2	0	0	0	2

Pre-requisite	Syllabus version
Nil	1.0

Course Objectives:

1. demonstrate competence in reading, writing, and speaking basic French, including knowledge of vocabulary (related to profession, emotions, food, workplace, sports/hobbies, classroom and family).
2. achieve proficiency in French culture oriented view point.

Expected Course Outcome:

1. remember the daily life communicative situations via personal pronouns, emphatic pronouns, salutations, negations, interrogations etc.
2. create communicative skill effectively in French language via regular / irregular verbs.
3. demonstrate comprehension of the spoken / written language in translating simple sentences.
4. understand and demonstrate the comprehension of some particular new range of unseen written materials.
5. demonstrate a clear understanding of the French culture through the language studied.

Module:1	Saluer, Se présenter, Etablir des contacts	**3 hours**

Les Salutations, Les nombres (1-100), Les jours de la semaine, Les mois de l'année, Les Pronoms Sujets, Les Pronoms Toniques, La conjugaison des verbes réguliers, La conjugaison des verbes irréguliers- avoir / être / aller / venir / faire etc.

Module:2	**Présenter quelqu'un, Chercher un(e) correspondant(e), Demander des nouvelles d'une personne.**	**3 hours**

La conjugaison des verbes Pronominaux, La Négation, L'interrogation avec *'Est-ce que ou sans Est-ce que'*.

Module:3	**Situer un objet ou un lieu, Poser des questions**	**4 hours**

L'article (défini/ indéfini), Les prépositions (à/en/au/aux/sur/dans/avec etc.), L'article contracté, Les heures en français, La Nationalité du Pays, L'adjectif (La Couleur, l'adjectif possessif, l'adjectif démonstratif/ l'adjectif interrogatif (quel/quelles/quelle/quelles), L'accord des adjectifs avec le nom, L'interrogation avec Comment/ Combien / Où etc.,

Module:4	**Faire des achats, Comprendre un texte court, Demander et indiquer le chemin.**	**6 hours**

La traduction simple :(français-anglais / anglais –français)

Module:5	**Trouver les questions, Répondre aux questions générales en français.**	**5 hours**

L'article Partitif, Mettez les phrases aux pluriels, Faites une phrase avec les mots donnés, Exprimez les phrases données au Masculin ou Féminin, Associez les phrases.

Module:6	**Comment ecrire un passage**	**3 hours**

Décrivez :
La Famille /La Maison, /L'université /Les Loisirs/ La Vie quotidienne etc.

Module:7	**Comment ecrire un dialogue**	**4 hours**
Dialogue: a) Réserver un billet de train b) Entre deux amis qui se rencontrent au café c) Parmi les membres de la famille d) Entre le client et le médecin		
Module:8	**Invited Talk: Native speakers**	**2 hours**
	Total Lecture hours:	**30 hours**

Text Book(s)	
1.	Echo-1, Méthode de français, J. Girardet, J. Pécheur, Publisher CLE International, Paris 2010.
2	Echo-1, Cahier d'exercices, J. Girardet, J. Pécheur, Publisher CLE International, Paris 2010.
Reference Books	
1.	CONNEXIONS 1, Méthode de français, Régine Mérieux, Yves Loiseau,Les Éditions Didier, 2004.
2	CONNEXIONS 1, Le cahier d'exercices, Régine Mérieux, Yves Loiseau, Les Éditions Didier, 2004.
3	ALTER EGO 1, Méthode de français, Annie Berthet, Catherine Hugo, Véronique M. Kizirian, Béatrix Sampsonis, Monique Waendendries , Hachette livre 2006.

Mode of Evaluation: CAT / Assignment / Quiz / FAT			
Recommended by Board of Studies			
Approved by Academic Council	No 41	Date	

GER5001	Deutsch für Anfänger	L	T	P	J	C
		2	0	0	0	2
Pre-requisite	NIL	Syllabus version				
		1.0				

Course Objectives:

The course gives students the necessary background to:

1. enable students to read and communicate in German in their day to day life
2. become industry-ready
3. make them understand the usage of grammar in the German Language.

Expected Course Outcome:

he students will be able to

6. create the basics of German language in their day to day life.
7. understand the conjugation of different forms of regular/irregular verbs.
8. understand the rule to identify the gender of the Nouns and apply articles appropriately.
9. apply the German language skill in writing corresponding letters, E-Mails etc.
10. create the talent of translating passages from English-German and vice versa and To frame simple dialogues based on given situations.

Module:1	3 hours

Einleitung, Begrüssungsformen, Landeskunde, Alphabet, Personalpronomen, Verb Konjugation, Zahlen (1-100), W-fragen, Aussagesätze, Nomen – Singular und Plural

Lernziel:

Elementares Verständnis von Deutsch, Genus- Artikelwörter

Module:2	3 hours

Konjugation der Verben (regelmässig /unregelmässig) die Monate, die Wochentage, Hobbys, Berufe, Jahreszeiten, Artikel, Zahlen (Hundert bis eine Million), Ja-/Nein- Frage, Imperativ mit Sie

Lernziel :

Sätze schreiben, über Hobbys erzählen, über Berufe sprechen usw.

Module:3	4 hours

Possessivpronomen, Negation, Kasus- AkkusatitvundDativ (bestimmter, unbestimmterArtikel), trennnbare verben, Modalverben, Adjektive, Uhrzeit, Präpositionen, Mahlzeiten, Lebensmittel, Getränke

Lernziel :

Sätze mit Modalverben, Verwendung von Artikel, über Länder und Sprachen sprechen, über eine Wohnung beschreiben.

Module:4	6 hours

Übersetzungen : (Deutsch – Englisch / Englisch – Deutsch)

Lernziel :

Grammatik – Wortschatz - Übung

Module:5	5 hours

Leseverständnis,Mindmap machen,Korrespondenz- Briefe, Postkarten, E-Mail

Lernziel : Wortschatzbildung und aktiver Sprach gebrauch		
Module:6	.	**3 hours**
Aufsätze : Meine Universität, Das Essen, mein Freund oder meine Freundin, meine Familie, ein Fest in Deutschland usw		
Module:7		**4 hours**
Dialoge: e) Gespräche mit Familienmitgliedern, Am Bahnhof, f) Gespräche beim Einkaufen ; in einem Supermarkt ; in einer Buchhandlung ; g) in einem Hotel - an der Rezeption ;ein Termin beim Arzt. Treffen im Cafe		
Module:8		**2 hours**
Guest Lectures/Native Speakers / Feinheiten der deutschen Sprache, Basisinformation über die deutschsprachigen Länder		
	Total Lecture hours:	**30 hours**

Text Book(s)	
1.	**Studio d A1 Deutsch als Fremdsprache, Hermann Funk, Christina Kuhn, Silke Demme : 2012**
Reference Books	
1	etzwerk Deutsch als Fremdsprache A1, Stefanie Dengler, Paul Rusch, Helen Schmtiz, Tanja Sieber, 2013
2	Lagune ,Hartmut Aufderstrasse, Jutta Müller, Thomas Storz, 2012.
3	eutsche SprachlehrefürAUsländer, Heinz Griesbach, Dora Schulz, 2011
4	hemenAktuell 1, HartmurtAufderstrasse, Heiko Bock, MechthildGerdes, Jutta Müller und Helmut Müller, 2010
	ww.goethe.de irtschaftsdeutsch.de ber.de, klett-sprachen.de ww.deutschtraning.org
Mode of Evaluation: CAT / Assignment / Quiz / FAT	
Recommended by Board of Studies	
Approved by Academic Council	No. 41 Date 17-06-2016

STS5001	Essentials of Business Etiquettes	L	T	P	J	C
		3	0	0	0	1
Pre-requisite		**Syllabus version**				
		2.0				

Course Objectives:

1. To develop the students' logical thinking skills
2. To learn the strategies of solving quantitative ability problems
3. To enrich the verbal ability of the students
4. To enhance critical thinking and innovative skills

Expected Course Outcome:

- Enabling students to use relevant aptitude and appropriate language to express themselves
- To communicate the message to the target audience clearly

Module:1	**Business Etiquette: Social and Cultural Etiquette and Writing Company Blogs and Internal Communications and Planning and Writing press release and meeting notes**	**9 hours**

Value, Manners, Customs, Language, Tradition, Building a blog, Developing brand message, FAQs', Assessing Competition, Open and objective Communication, Two way dialogue, Understanding the audience, Identifying, Gathering Information,. Analysis, Determining, Selecting plan, Progress check, Types of planning, Write a short, catchy headline, Get to the Point –summarize your subject in the first paragraph., Body – Make it relevant to your audience,

Module:2	**Study skills – Time management skills**	**3 hours**

Prioritization, Procrastination, Scheduling, Multitasking, Monitoring, Working under pressure and adhering to deadlines

Module:3	**Presentation skills – Preparing presentation and Organizing materials and Maintaining and preparing visual aids and Dealing with questions**	**7 hours**

10 Tips to prepare PowerPoint presentation, Outlining the content, Passing the Elevator Test, Blue sky thinking, Introduction , body and conclusion, Use of Font, Use of Color, Strategic presentation, Importance and types of visual aids, Animation to captivate your audience, Design of posters, Setting out the ground rules, Dealing with interruptions, Staying in control of the questions, Handling difficult questions

Module:4	**Quantitative Ability -L1 – Number properties and Averages and Progressions and Percentages and Ratios**	**11 hours**

Number of factors, Factorials, Remainder Theorem, Unit digit position, Tens digit position, Averages,

Weighted Average, Arithmetic Progression, Geometric Progression, Harmonic Progression, Increase & Decrease or successive increase, Types of ratios and proportions		
Module:5	**Reasoning Ability-L1 – Analytical Reasoning**	**8 hours**
Data Arrangement(Linear and circular & Cross Variable Relationship), Blood Relations, Ordering/ranking/grouping, Puzzle test, Selection Decision table		
Module:6	**Verbal Ability-L1 – Vocabulary Building**	**7 hours**
Synonyms & Antonyms, One word substitutes, Word Pairs, Spellings, Idioms, Sentence completion, Analogies		
	Total Lecture hours:	**45 hours**

Reference Books

1.	Kerry Patterson, Joseph Grenny, Ron McMillan, Al Switzler(2001) Crucial Conversations: Tools for Talking When Stakes are High. Bangalore. McGraw□Hill Contemporary
2.	Dale Carnegie,(1936) How to Win Friends and Influence People. New York. Gallery Books
3.	Scott Peck. M(1978) Road Less Travelled. New York City. M. Scott Peck.
4.	FACE(2016) Aptipedia Aptitude Encyclopedia. Delhi. Wiley publications
5.	ETHNUS(2013) Aptimithra. Bangalore. McGraw-Hill Education Pvt. Ltd.

Websites:

1.	**www.chalkstreet.com**
2.	**www.skillsyouneed.com**
3.	**www.mindtools.com**
4.	**www.thebalance.com**
5.	**www.eguru.ooo**

Mode of Evaluation: FAT, Assignments, Projects, Case studies, Role plays,
3 Assessments with Term End FAT (Computer Based Test)

Recommended by Board of Studies	09/06/2017		
Approved by Academic Council	No. 45th AC	Date	15/06/2017

STS5002	Preparing for Industry	L	T	P	J	C
		3	0	0	0	1
Pre-requisite		**Syllabus version**				
		2.0				

Course Objectives:

5. To develop the students' logical thinking skills
6. To learn the strategies of solving quantitative ability problems
7. To enrich the verbal ability of the students
8. To enhance critical thinking and innovative skills

Expected Course Outcome:

- Enabling students to simplify, evaluate, analyze and use functions and expressions to simulate real situations to be industry ready.

Module:1	**Interview skills – Types of interview and Techniques to face remote interviews and Mock Interview**	**3 hours**

Structured and unstructured interview orientation, Closed questions and hypothetical questions, Interviewers' perspective, Questions to ask/not ask during an interview, Video interview¸ Recorded feedback, Phone interview preparation, Tips to customize preparation for personal interview, Practice rounds

Module:2	**Resume skills – Resume Template and Use of power verbs and Types of resume and Customizing resume**	**2 hours**

Structure of a standard resume, Content, color, font, Introduction to Power verbs and Write up, Quiz on types of resume, Frequent mistakes in customizing resume, Layout - Understanding different company's requirement, Digitizing career portfolio

Module:3	**Emotional Intelligence - L1 – Transactional Analysis and Brain storming and Psychometric Analysis and Rebus Puzzles/Problem Solving**	**12 hours**

Introduction, Contracting, ego states, Life positions, Individual Brainstorming, Group Brainstorming, Stepladder Technique, Brain writing, Crawford's Slip writing approach, Reverse brainstorming, Star bursting, Charlette procedure, Round robin brainstorming, Skill Test, Personality Test, More than one answer, Unique ways

Module:4	**Quantitative Ability-L3 – Permutation-Combinations and Probability and Geometry and mensuration and Trigonometry and Logarithms and Functions and Quadratic Equations and Set Theory**	**14 hours**

Counting, Grouping, Linear Arrangement, Circular Arrangements, Conditional Probability, Independent and Dependent Events, Properties of Polygon, 2D & 3D Figures, Area & Volumes, Heights and distances, Simple trigonometric functions, Introduction to logarithms, Basic rules of logarithms, Introduction to functions, Basic rules of functions, Understanding Quadratic

Equations, Rules & probabilities of Quadratic Equations, Basic concepts of Venn Diagram		
Module:5	**Reasoning ability-L3 – Logical reasoning and Data Analysis and Interpretation**	**7 hours**
Syllogisms, Binary logic, Sequential output tracing, Crypto arithmetic, Data Sufficiency, Data interpretation-Advanced, Interpretation tables, pie charts & bar chats		
Module:6	**Verbal Ability-L3 – Comprehension and Logic**	**7 hours**
Reading comprehension, Para Jumbles, Critical Reasoning (a) Premise and Conclusion, (b) Assumption & Inference, (c) Strengthening & Weakening an Argument		
	Total Lecture hours:	**45 hours**

Reference Books

1.	Michael Farra and JIST Editors(2011) Quick Resume & Cover Letter Book: Write and Use an Effective Resume in Just One Day. Saint Paul, Minnesota. Jist Works
2.	Daniel Flage Ph.D(2003) The Art of Questioning: An Introduction to Critical Thinking. London. Pearson
3.	David Allen(2002) Getting Things done : The Art of Stress -Free productivity. New York City. Penguin Books.
4.	FACE(2016) Aptipedia Aptitude Encyclopedia.Delhi. Wiley publications
5.	ETHNUS(2013) Aptimithra. Bangalore. McGraw-Hill Education Pvt. Ltd.

Websites:

1.	**www.chalkstreet.com**
2.	**www.skillsyouneed.com**
3.	**www.mindtools.com**
4.	**www.thebalance.com**
5.	**www.eguru.ooo**

Mode of Evaluation: FAT, Assignments, Projects, Case studies, Role plays,
3 Assessments with Term End FAT (Computer Based Test)

Recommended by Board of Studies	09/06/2017		
Approved by Academic Council	No. 45th AC	Date	15/06/2017