AC 4-3-2014
Item No. – 4.55

UNIVERSITY OF MUMBAI

Syllabus for the

Program -M.E.

Course - Computer Network & Information Security

(As per Credit Based Semester and Grading System with effect from the academic year 2014–2015)

Program Structure for
ME (Computer Network & Information Security)

Mumbai University

(With Effect from 2014-2015)

Semester I

Subject Code	Subject Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
CISC101	Mobile & Adaptive System	04	--	--	04	--	--	04
CISC102	Network Programming	04	--	--	04	--	--	04
CISC103	Information Security System	04	--	--	04	--	--	04
CISE101X	Elective I	04	--	--	04	--	--	04
CISE102X	Elective II	04	--	--	04	--	--	04
CISL101	Laboratory-I Network Programming	--	02	--	--	02	--	01
CISL102	Laboratory -II Information Security System	--	02	--	--	02	-	01
Total		**20**	**04**	**--**	**20**	**04**	**--**	**22**

Subject Code	Subject Name	Examination Scheme							
		Theory							
		Internal Assessment			End Sem. Exam.	Exam. Duration (in Hrs)	Term Work	Pract. /oral	Total
		Test1	Test 2	Avg.					
CISC101	Mobile & Adaptive System	20	20	20	80	03	--	--	100
CISC102	Network Programming	20	20	20	80	03	--	--	100
CISC103	Information Security System	20	20	20	80	03	--	--	100
CISE101X	Elective I	20	20	20	80	03	--	--	100
CISE102X	Elective II	20	20	20	80	03	--	--	100
CISL101	Laboratory -I Network Programming	--	--	--	--	--	25	25	50
CISL102	Laboratory -II Information Security System	--	--	--	--	--	25	25	50
Total		**100**	**100**	**100**	**400**	**--**	**50**	**50**	**600**

Semester II

Subject Code	Subject Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
CISC201	Network Security	04	--	--	04	--	--	04
CISC202	Web Application Security	04	--	--	04	--	--	04
CISC203	Internet Routing Design	04	--	--	04	--	--	04
CISE201X	Elective III	04	--	--	04	--	--	04
CISE202X	Elective IV	04	--	--	04	--	--	04
CISL201	Laboratory -I Network Security	--	02	--	--	02	--	01
CISL202	Laboratory –II Web Application Security	--	02	--	--	02	--	01
Total		**20**	**04**	**--**	**20**	**04**	**--**	**22**

Subject Code	Subject Name	Examination Scheme							
		Theory					Term Work	Pract. /Oral	Total
		Internal Assessment			End Sem. Exam.	Exam. Duration (in Hrs)			
		Test1	Test 2	Avg.					
CISC201	Network Security	20	20	20	80	03	--	--	100
CISC202	Web Application Security	20	20	20	80	03	--	--	100
CISC203	Internet Routing Design	20	20	20	80	03	--	--	100
CISE201X	Elective III	20	20	20	80	03	--	--	100
CISE202X	Elective IV	20	20	20	80	03	--	--	100
CISL201	Lab-I –Network Security	--	--	--	--	--	25	25	50
CISL202	Lab-II - Web Application Security	--	--	--	--	--	25	25	50
Total		**100**	**100**	**100**	**400**	--	**50**	**50**	**600**

Semester III

Subject Code	Subject Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
CISS301	Seminar	--	06	--	--	03	--	03
CISD301	Dissertation I	--	24	--	--	12	--	12
Total		--	30	--	--	15	--	15

Subject Code	Subject Name	Examination Scheme						
		Theory				Term Work	Pract. / Oral	Total
		Internal Assessment			End Sem. Exam.			
		Test1	Test 2	Avg.				
CISS301	Seminar	--	--	--	--	50	--	50
CISD301	Dissertation I	--	--	--	--	100	--	100
Total		--	--	--	--	**150**	--	**150**

Semester IV

Subject Code	Subject Name	Teaching Scheme (Contact Hours)			Credits Assigned			
		Theory	Pract.	Tut.	Theory	Pract.	Tut.	Total
CISD 401	Dissertation II	--	30	--	--	15	--	15
Total		--	30	--	--	15	--	15

Subject Code	Subject Name	Examination Scheme						
		Theory				Term Work	Pract. / Oral	Total
		Internal Assessment			End Sem. Exam			
		Test1	Test 2	Avg.				
CISD 401	Dissertation II	--	--	--	--	100	100	200
Total		--	--	--	--	**100**	**100**	**200**

Note:

- In case of Seminar, 01 Hour / week / student should be considered for the calculation of load of a teacher
- In case of Dissertation I, 02 Hour / week / student should be considered for the calculation of load of a teacher
- In case of Dissertation II, 02 Hour / week / student should be considered for the calculation of load of a teacher

Subject Code	Elective I	Subject Code	Elective II
CISE1011	Distributed System	CISE1021	Grid And Cloud Computing
CISE1012	High Speed And Broadband Network	CISE1022	Computer Communication Network
CISE1013	Operating System Security	CISE1023	Cyber Law & Ethics
CISE1014	Advanced Computer Forensic Analysis	CISE1024	Bio-Metric Security

Subject Code	Elective III	Subject Code	Elective IV
CISE2011	Mobile & Wireless Security	CISE2021	Information Retrieval System
CISE2012	Network Management and Performance Evaluation	CISE2022	Public Key Infrastructures & Trust Management
CISE2013	Network Vulnerabilities and Risk Management	CISE2023	Database Security
CISE2014	Information Hacking Techniques	CISE2024	TCP/IP Technology

Subject Code	Subject Name	Credits
CISC101	**Mobile & Adaptive System**	**04**
Module	**Detailed content**	**Hours**
1	Introduction and overview: General issues that will be addressed on this module. Properties of wireless PANs, LANs, WANs, Basic structure and operation, Ad-hoc and Infrastructure networks. Physical constraints and limitations (transmission & reception)	8
2	Network structures and architectures: Hand-off and mobility support at the physical/link level. Technologies at physical link layer. PANs Blue tooth, LANs IEEE802.11, Hiper LAN.	6
3	Global system for mobile communication (GSM): Mobile Services, System Architecture, Protocols, Localization & Calling, Handover, Security.GPRS**:** GPRS System Architecture.UMTS: UMTS System Architecture.LTE: Long Term Evolution.	8
4	Mobile IP: Mobile IPv4 and Mobile IPv6. Problems with routing, QoS and security. Overview of use of intelligence in mobile systems. Power management, replication, adaptation etc. Power management issues. From the lowest (physical device) levels, through communication protocols, broadcast methodologies, trans coding, etc.	8
5	File systems: CODA, Mobile infrastructure support, Mobile middleware. Adaptive and reconfigurable system.Next generation wireless overview (3G/4G): UMTS, IMT-2000 and W-CDMA.	6
6	Mobile multimedia and their relationship to proxying: Programmable networking and Applications for mobile systems. Code mobility and control/signaling.	4

Text Books :

1. Jochen Schiller, “Mobile Communications”, Pearson Education, Second Edition, 2008.
2. Dr. Sunilkumar, et al “Wireless and Mobile Networks: Concepts and Protocols”, Wiley India.
3. Raj Kamal, “Mobile Computing”, OXFORD UNIVERSITY PRESS.
4. “Mobility: Processes, computers and agents." Ed. Dejan Milojicic, Frederick Douglis and Richard Wheeler. ACM Press. ISBN 0-201-37928-7.

References:

1. Asoke K Talukder, et al, “Mobile Computing”, Tata McGraw Hill, 2008.
2. Matthew S.Gast, “802.11 Wireless Networks”, SPD O’REILLY.
3. Ivan Stojmenovic, “Handbook of Wireless Networks and Mobile Computing”, Wiley, 2007.
4. Kumkum Garg, “Mobile Computing”, Pearson.
5. Handbook of Security of Networks, Yang Xiao, Frank H Li, Hui Chen, World Scientific,2011.

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISC102	**Network Programming**	**04**
Module	**Detailed content**	**Hours**
1	The Transport Layer: TCP and UDP with policy control, TCP Connection Establishment and Termination, TIME_WAIT State, Port Numbers, Concurrent Servers, Buffer Sizes and Limitations.	5
2.	Sockets and Socket Programming: Introduction, Socket Address Structures, Value-Result Arguments, Byte Ordering Functions, Byte Manipulation Functions, socket Function. TCP Client-Server: TCP Echo Server, TCP Echo Client, Normal Termination, Connection abort before accept return, Termination of server process, Crashing of Server Host, Crashing and Rebooting of Server Host, Shutdown of Server Host. UDP Sockets: UDP Echo server, UDP Echo Client, Lost Datagram's, Lack of flow control with UDP.	8
3	IPv4 and IPv6 Interoperability: IPv4 Client, IPv6 Server, IPv6 Client, IPv4 Server, IPv6 Address Testing Macros, IPV6_ADDRFORM Socket Option ICMPv4 and ICMPv6	5
4.	Name and Address Conversions: Domain Name System, Functions. Advanced Name and Address Conversions: Functions and Implementation	4
5.	Multicasting and Broadcasting: Broadcast Addresses, Unicast versus Broadcast, Multicasting: Multicast Addresses, Multicasting versus Broadcasting on A LAN, Multicasting on a WAN, Multicast Socket Options, Simple Network Time Protocol, SNTP.	6
6.	Routing Sockets: Data link Socket, Address Structure, Reading and Writing, Interface Name and Index Functions, data link access, raw socket (creation input, output)	4
7.	Threads: Thread Functions: Creation and Termination, TCP Echo Server, Thread-Specific Data, Web Client and Simultaneous Connections	4
8	Client-Server Design Alternatives: TCP Client Alternatives, TCP Test Client, Iterative Server, Concurrent Server, Thread Locking around accept, Descriptor Passing, TCP Concurrent Server, One Thread per Client, TCP Pre-threaded Server.	4

References:

1. Richard Stevens, Bill Fenner, "UNIX network programming Volume-1 - The Sockets Networking API", 3rd edition.
2. W. Richard Stevens, "Advanced Programming in the Unix Environment", Addison Wesley.
3. UNIX Internals – "A new Frontier" , PHI

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISC103	**Information Security system**	**04**

Module	Detailed content	Hours
1	Computer Security Overview: The Basic Components, Threats, Policy and Mechanism, Protection State, AC Matrix, Assumption and Trust Assurance, Operational issues, Classical Crypto System - substitution transformation.	8
2	Symmetric Key Cryptography: DES Structure, DES Analysis, Security of DES. AES Intro, Transformation, Key Expansions, AES Ciphers and Examples, Analysis of AES. IDEA Modern Symmetric Key cryptography ECB, CBC, CFD, OFB and CTR, Key Length and Key Management	8
3	Asymmetric Key Cryptography: Number Theory: - Primes, Primarily Testing, Factorization, Chinese Remainder Theorem, Exponentiation and logarithm. Public key Cryptography DHKE, RSA, RABIN Cryptosystem	8
4	Authentication and Digital Signature: Zero Knowledge authentication: Blind Signature, Fiat Shamin Protocol, Feige Fiat Shamin Protocol, Guillou Quisquater Protocol, authentication Protocol : Password, Challenge Response and Biomatric Authentication Application : kierboroes, etc.Digital Sign : DSA and DSC	8
5	Hash Function: MD5 MAC , SHA Internet Security Protocol: SSL, SHTPD SET, 3D Protocol, Electronics Money, Email Security PEM.	8

References:

1. B.A. Forouzan and Debdeep Mukhopadhyay. Tata Mc Graw Hill " Cryptography and Network Security.
2. Bruce Schneier 'Wiley' "Applied Cryptography"
3. Matt Bishop and S.S. Venkatramanayya 'Pearson Ed' "Introduction to Computer Security "
4. Atul Kahte " Tata McGraw Hill" Cryptography and Network Security.

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISE1011	**Distributed System**	**04**
Module	**Detailed content**	**Hours**
1	Characterization of Distributed Systems: Introduction, Examples of distributed Systems, Resource sharing and the Web Challenges, System Models- Architectural models, Fundamental Models, Theoretical Foundation for Distributed System: Limitation of Distributed system, absence of global clock, shared memory, Logical clocks, Lamport's & vectors logical clocks, Causal ordering of messages, global state, termination detection. Distributed Mutual Exclusion: Classification of distributed mutual exclusion, requirement of mutual exclusion theorem, Token based and non token based algorithms, performance metric for distributed mutual exclusion algorithms.	10
2	Distributed Deadlock Detection: system model, resource Vs communication deadlocks, deadlock prevention, avoidance, detection & resolution, centralized dead lock detection, distributed dead lock detection, path pushing algorithms, edge chasing algorithms. Agreement Protocols: Introduction, System models, classification of Agreement Problem, Byzantine agreement problem, Consensus problem, Interactive consistency Problem, Solution to Byzantine Agreement problem, Application of Agreement problem, Atomic Commit in Distributed Database system.	8
3	Distributed Objects and Remote Invocation: Communication between distributed objects, Remote procedure call, Events and notifications, Java RMI case study. Security: Overview of security techniques, Cryptographic algorithms, Digital signatures Cryptography pragmatics, Distributed file systems : File services architecture, SUN Network File System, The Andrew file System.	8
4	Transactions and Concurrency Control: Transactions, Nested transactions, Locks, Optimistic Concurrency control, Timestamp ordering, Comparison of methods for concurrency control. Distributed Transactions: Flat and nested distributed transactions, Atomic Commit protocols, Concurrency control in distributed transactions, Distributed deadlocks, Transaction recovery. Replication: System model and group communication, Fault Tolerant services, highly available services, transactions with replicated data.	8
5	Distributed Algorithms: Introduction to communication protocols, Deadlock free Packet switching, Introduction to Wave & traversal algorithms, Election algorithm. CORBA Case Study: CORBA RMI, CORBA services.	6

Text Books:

1. Distributed Systems Concepts and design, G. Coulouris, J. Dollimore and T. Kindberg, Fourth Edition, Pearson Education.
2. Distributed Operating Systems Concepts and Design, Pradeep K. Sinha, PHI.
3. Advanced Concepts in Operating Systems, M. Singhal, N. G. Shivaratri, Tata McGraw-Hill Edition.

Reference Books:

1. Distributed Systems- Principles and Paradigms, PHI.
2. Distributed Operating System, Andrew S. Tanenbaum, Pearson.
3. Distributed Operating Systems and Algorithm Analysis, R.Chow, T. Johnson, Pearson.

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISE1012	High Speed And Broadband Network	04
Module	**Detailed content**	**Hours**
1	Introduction: Introduction to modern networking trends Optical networking: principles and challenges; evolution of optical networks, wavelength routed network, wavelength division multiplexing (WDM) network technology, sub-carrier multiplexing optical networks. Enabling technologies: optical transmitter, optical fiber, optical receivers, optical amplifiers, optical switching elements, optical cross-connects (OXC), multiplexers/de-multiplexers, wavelength routers, optical wavelength converters, WDM network test beds. Network architecture, IP over WDM.	10
2	Optical Communication Systems: Block diagrams of optical communication systems, direct intensity modulation, digital communication systems, Laser semiconductor transmitter, Generations of optical fiber link, description of 8 Mb/s optical fiber communication link, description of 2.5 Gb/s optical fiber communication link.	8
3	Components of fiber optic Networks: Overview of fiber optic networks, Transreceiver, semiconductors optical amplifiers, couplers/splicers, wavelength division multiplexers and demultiplexers, filters, isolators and optical switches.	6
4	Fiber Optic Networks: Basic networks, SONET/SDH, Broad cast and select WDM Networks, wavelength routed networks, optical CDMA.	6
5	ATM: The WAN Protocol : Faces of ATM, ATM Protocol operations (ATM cell and Transmission) ATM Networking basics, Theory of Operations, B-ISDN reference model, PHY layer , ATM Layer (Protocol model), ATM layer and cell, Traffic Descriptor and parameters, Traffic Congestion control defined, AAL Protocol model, Traffic contract and QoS, User Plane overview, Control Plane AAL, Management Plane, Sub-DS3 ATM, ATM public services.	10

Text Books:

1. Optical fiber communications – Gerd Keiser, 3 rd Ed. MGH.
2. Fiber Optic Communication Technology – Djafar K. Mynbaev and Lowell L. Scheiner, (Pearson Education Asia)
3. Optoelectronic devices and systems – S.C. Gupta, PHI, 2005.

References:

1. Fiber Optics Communications – Harold Kolimbiris (Pearson Education Asia)
2. Optical Fiber Communications and its applications – S.C. Gupta (PHI) 2004.
3. WDM Optical Networks – C. Siva Ram Murthy and Mohan Guru Swamy, PHI.
4. Fiber Optic communications – D.C. Agarwal, S.Chand Publications, 2004. Multiwavelength Optical

Networks: A Layered Approach by Thomas E. Stern, Krishna Bala.

5. Optical Networking by Debra Cameron, Wiley, December 2001
6. Optical Network Design and Implementation by Vivek Alwayn, Cisco Press
7. DWDM Network Designs and Engineering Solutions by Ashwin Gumaste, Tony Antony, Tony Anthony, Pearson Education.
8. Mohan Gurusamy, C. Siva Murthy, WDM Technology and Issues in WDM Optical Networks, Prentice Hall Publications,

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISE1013	**Operating System Security**	**04**
Module	**Detailed content**	**Hours**
1	Introduction: Secure OS, Trust Model, Thread Model Access Control Fundamentals: Protection System, Reference Monitor, Secure OS, Definition Assessment criteria.	8
2	Multics : Multics System, Multics Security, Multics Vulnerability Analysis Security in ordinary OS: Unix Security and Windows Security.	8
3	Verifiable Security Goal: Information Flow, Information Flow Secrecy Models, Information Flow Integrity models, Covert Channel.	8
4	Security Kernels: The Security Kernel, Secure Communication Processor, Gemini Secure OS, Securing Commercial OS, Retrofitting Security into a commercial OS, Commercial Era, Microkernel Era, Uinx Era.	8
5	Case Study: Building a secure OS for Linux: Linux Aecurity Modules, security Enhanced Linux. Secure Capability System: Capability System Fundamentals, capability Security, Challenges in Secure Capability System, Building Secure Capability System.	8

References:

1. Operating system security, Trent Jaeger, Morgan & Claypool Publishers, 2008
2. Guide to Operating system security , Thomson
3. Modern Operating systems, Andrew S Tanenbaum
4. Secure Operating Systems. John Mitchell. Multics-Orange Book-Claremont

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISE1014	**Advanced Computer Forensics Analysis**	**04**
Module	**Detailed content**	**Hours**
1	Introduction to Cyber Forensics Technology: Introduction to computer forensics, use of forensics in law enforcement, Types of computer Forensics Technology- Military, law, Specialized forensics technique spyware and Adware, pitfall with firewall Biometrics security systems.	10
2	Types of Computer Forensics systems: Internet security system, IDS, Firewall, Public key, Network disaster Recovery system, SAN security system, Satellite Encryption security system, Identity management security system, Identity Theft.	10
3	Ethical Hacking: Windows Hacking, Malware, Scanning, Cracking. Digital Evidence in Criminal Investigations: The Analog and Digital World, Training and Education in digital evidence, Evidence Collection and Data Seizure: Why Collect Evidence, Collection Options Obstacles, Types of Evidence, The Rules of Evidence, Volatile Evidence, General Procedure, Collection and Archiving, Methods of Collection, Artifacts, Collection Steps, Controlling Contamination: The Chain of Custody, Reconstructing the Attack, The digital crime scene, Investigating Cybercrime, Duties Support Functions and Competencies.	10
4	Computer Forensics Analysis: Discovery of electronic evidence- electronic document discovery, identification of data- Time keeping, forensic identification and analysis of technical surveillance devices. Reconstructing fast events: Useable File Formats, Unusable File Formats, Converting Files, Investigating Network Intrusions and Cyber Crime, Network Forensics and Investigating logs, Investigating network Traffic, Investigating Web attacks, Router Forensics.	10

References:

1. Cyber Security : Belapure: wiley
2. By John R. Vacca Computer forensics: computer crime scene investigation, Volume 1
3. Ali Jahangiri, Live Hacking: The Ultimate Guide to Hacking Techniques & Countermeasures for Ethical Hackers & IT Security Experts, Ali Jahangiri, 2009
4. Computer Forensics: Incident Response Essentials, Warren G. Kruse II & Jay G. Heiser
5. Computer Forensics & Privacy, Michael Caloyannides
6. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, edited by Albert J. Marcella Jr. & Robert S. Greenfield

7. Handbook of Computer Crime Investigation, edited by Eoghan Casey

8. Christof Paar, Jan Pelzl, Understanding Cryptography: A Textbook for Students and Practitioners, 2nd Edition, Springer's, 2010

9. Computer Forensics: Investigating Network Intrusions and Cyber Crime (Ec-Council Press Series: Computer Forensics), 2010

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISE1021	Grid and Cloud Computing	04

Module	Detailed content	Hours
1	System models for advanced computing : clusters of cooperative computing, grid computing and cloud computing; software systems for advanced computing-service oriented software and parallel and distributed programming models with introductory details, Features of grid and cloud platform.	10
2	Cloud Computing services models and features: Saas, Paas and Iaas, Service oriented architecture and web services; Features of cloud computing architectures and simple case studies.	8
3	Virtualization: Characteristic features, Taxonomy Hypervisor, Virtualization and Cloud Computing,Pros and Cons of Cloud Computing, Technology Examples/Case Studies.	8
4	Cloud programming Environmental: Map Reduce Hadoop Library from Apache, Open Source Cloud Software Systems –Eucalyptus.	8
5	Grid Computing: Grid Architecture and Service modeling, Grid resource management, Grid Application trends.	6

Text Books :

1. Distributed and Cloud Computing, Kaittwang Geoffrey C.Fox and Jack J Dongrra, Elsevier India 2012.

2. Mastering Cloud Computing- Raj Kumar Buyya, Christian Vecchiola and S.Tanurai Selvi, TMH, 2012.

Reference Books :

1. Cloud Computing, John W. Ritting House and James F Ramsome, CRC Press, 2012.

2. Enterprise Cloud Computing, Gautam Shroff, Cambridge University Press, 2012.

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISE1022	Computer Communication Network	04
Module	**Detailed content**	**Hours**
1	Introduction: Overview of computer networks, seven-layer architecture, TCP/IP protocol Suite, Addressing, IP versions. Connectors, Transceivers and Media	6
2	MAC protocols for high-speed LANS, MANs, and wireless LANs. (For example, FDDI, DQDB, HIPPI, Gigabit Ethernet, Wireless ethernet, etc.)	6
3	Fast access technologies (ADSL, Cable Modem, etc.)	4
4	Why IPv6, basic protocols, extensions and options, support for QoS, security, etc., neighbour discovery, auto-configuration, routing. Changes to other protocols. Application Programming Interface for IPv6. 6	6
5	Mobility in networks. Mobile IP. Security related issues. IP Multicasting. Multicast routing protocols, address assignments, session discovery, etc.	6
6	TCP extensions for high-speed networks, transaction-oriented applications. Other new options in TCP.	4
7	Network security at various layers. Secure-HTTP, SSL, ESP, Authentication header, Key distribution protocols. Digital signatures, digital certificates.	4

References:

1. W. R. Stevens._TCP/IP Illustrated, Volume 1: The protocols,_Addison Wesley, 1994.
2. G. R. Wright._TCP/IP Illustrated, Volume 2: The Implementation,_Addison Wesley, 1995.
3. W. R. Stevens._TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the Unix Domain Protocols,_Addison Wesley, 1996.
4. R. Handel, M. N. Huber, and S. Schroeder._ATM Networks: Concepts, Protocols, Applications,_Addison Wesley, 1998.
5. W. Stallings.*Cryptography and Network Security: Principles and Practice,* 2nd Edition, Prentice Hall, 1998.
6. C. E. Perkins, B. Woolf, and S. R. Alpert._Mobile IP: Design Principles and Practices,_Addison Wesley, 1997.
7. Peter Loshin._IPv6 Clearly Explained,_Morgan Kauffman, 1999.
8. M. Gonsalves and K. Niles._IPv6 Networks,_McGraw Hill, 1998.

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISE1023	**Cyber Law & Ethics**	**04**

Module	Detailed content	Hours
1	Introduction: Cyber Security and its problem-Intervention Strategies: Redundancy, Diversity and Autarchy.	08
2	Private ordering solutions, Regulation and Jurisdiction for global Cyber security, Copy Right source of risks, Pirates, Internet Infringement, Fair Use, postings, criminal liability, First Amendments, Data Losing.	08
3	Copy Right-Source of risks ,Pirates ,Internet Infringement ,FairUse, postings, Criminal Liability,First Amendments, Losing Data, Trademarks, Defamation, Privacy-Common Law Privacy, Constitutional law, Federal Statutes, Anonymity, Technology expanding privacy rights.	08
4	Duty of Care, Criminal Liability, Procedural issues, Electronic Contracts & Digital Signatures, Misappropriation of information, Civil Rights, Tax, Evidence.	08
5	Ethics, Legal Developments, Late 1990 to 2000,Cyber security in Society, Security in cyber laws case studies, General law and Cyber Law-a Swift Analysis.	08

References:

1. Jonathan Rosenoer,"Cyber Law: The law of the Internet", Springer-Verlag, 1997
2. Mark F Grady, FransescoParisi, "The Law and Economics of Cyber Security", Cambridge University Press, 2006

Assessment:

Internal: Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination: Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students.Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISE1024	**Bio-Metric Security**	**04**
Module	**Detailed content**	**Hours**
1	Introduction : Biometric Fundamentals, Biometric Technologies, Biometrics Vs Traditional Techniques characteristics Of A Good Biometric System,Benefits Of Biometrics,Key Biometric Processes:Verification, Identification And Biometric Matching Performance Measures In Biometric Systems: Far, Frr, Fte Rate, Eer And Atv Rate.	8
2	Physiological Biometrics: Leading Technologies : Finger,Scan,Facial Scan ,Iris Scan,Voice Scan,Hand Scan, Retina Scan,Components, Working Principles, Competing Technologies, Strengths And Weaknesses.	8
3	Automated Biometric System And Behavioural Biometrics: Automated Fingerprint Identification Systems,Leading Technologies: Signature Scan, Keystroke Scan Components, Working Principles, Strengths And Weaknesses.	8
4	Biometric Applications: Categorizing Biometric Applications –Application Areas: Criminal And Citizen Identification, Surveillance, Pc/Network Access, E-Commerce And Retail/Atm–Costs To Deploy–Other Issues In Deployment.	8
5	Privacy And Standards In Biometrics: Assessing The Privacy Risks Of Biometrics–Designing Privacy-Sympathetic Biometric Systems–Need For Standards–Different Biometric Standards.	8

References:

1. Samir Nanavati, Michael Thieme, Raj Nanavati, “Biometrics–Identity Verification in a Networked World”, Wiley-dreamtech India Pvt Ltd, New Delhi, 2003
2. Paul Reid, “Biometrics for Network Security”, Pearson Education, New Delhi, 2004
3. John R Vacca,“Biometric Technologies and Verification Systems”, Elsevier Inc, 2007
4. Anil K Jain, Patrick Flynn, Arun A Ross, “Handbook of Biometrics”, Springer, 200

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

SEMESTER II

Subject Code	Subject Name	Credits
CISC201	Network Security	04

Module	Detailed content	Hours
1	Introduction: Security Problem in TCP/IP Protocol Suite, security issues in physical and data link layer	4
2	Security at Network Layer Routing algorithm vulnerabilities: route and sequence number spoofing, instability and resonance effects. Information hiding: DMZ networks, route aggregation and segregation ICMP redirect hazard: denial of service. ARP hazard: phantom sources, ARP explosions and slow links. Defending against Chernobyl packets and meltdown. Fragmentation vulnerabilities and remedies: (ICMP Echo overrun) IPSec	8
3	Security at Transport Layer: SSL and TLS Secure network infrastructure services: DNS, NTP, SNMP, SSL Architecture, SSL/TLS Basic Protocol, SSL Message Formats, Session Resumption, Computing the keys, Client Authentication, PKI as deployed by SSL, Version Numbers, Negotiating Cipher Suites, Negotiating Compression Methods, Exportability, Encoding, Mobile systems: Address Export and re-use. Session key management: Blind- key cryptosystems (NTP).	8
4	Security at Session Layer Introduction SYN Attack Session Hijacking DNS Poisoning SSH Downgrade Attack Authentication Techniques and Attacks and different presentation layer attack	6
5	Security at Application Layer: PGP, S/MIMIE E-mail security, PGP, PEM, S/MIME, Secure binding of multimedia streams, Secure RTP. Secure RSVP.	6
6	Firewalls and IDS Firewalls: Network partitioning, firewall platforms, partitioning models and methods, Secure SNMP, Secure routing interoperability: virtual networks (DARTnet/CAIRN). Transparent and opaque network services. Source masking and hidden channels. IDS, Honeypots, Honey nets.	8

References:

1. Stallings, W., “Cryptography and Network Security: Theory and Practice”, Second Edition, John Wiley
2. “Charles P. Pfleeger “Security in computing”, Pearson Education
3. Stalling W., “ Network Security Essentials”, Pearson
4. Garfinkel S., Spafford G., “Practical Unix and Internet Security”, O'Reilly
5. Blacharski D., “Network Security in a Mixed Environment”
6. Practical Packet Analysis: Using Wireshark to Solve Real-Word Network problems by Chris Sanders

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISC202	**Web Application Security**	**04**
Module	**Detailed content**	**Hours**
1	Introduction: N/W security vs application security, open web application security projects, Security fundamentals: Input validation, Attack surface reduction, classifying and prioritizing threats.	6
2	Web application security principles: Authentication: Access Control overview, authentication fundamentals, two factor and three factor authentication, web application authentication, securing password based authentication, secure authentication best practices. Authorization: Access control , Authorization, session management, authorization fundamentals, authorization goals, types of permissions, Authorization layers, controls by layer, client site attack	10
3	Browser Security Principles: Defining the same origin policy, Exceptions to the same origin policy: HTML<script> element, JSON and JSONP, iframe and java script document domain, Adobe flash player cross domain policy file, XML Http Request (ajax) and cross-origin resource sharing Cross-site Scripting: Reflected XSS, POST based Reflected XSS, stored XSS, Local XSS, XSS defense in depth CSP and Cross-site Request Forgery: HTTP Get, relying on POST, URL rewriting, Shared Secretes, Double-submitted cookies,	8
4	Application Security basics: Reverse Engineering, Attack vectors, input Validation, Secure SDLC- Data classification, Secure requirement-Secure Architecture. Factors in Developing An Application Security Program-Policies, procedures, baselines and guidelines, ROI on application security.	8
5	Software Engineering and Security: Security Challenge in software engineering, Secure Software development methodologies, Waterfall model with security, Comprehensive Lightweight Application Security Process, Extreme Programming and Security, Aspect-Oriented Programming and Security.	8

Text Books:

1. Web application Security by Bryan Sullivan and Vincent Liu TMH
2. John Davies, Rudi Studer, and Paul Warren John , “Semantic Web Technologies: Trends and Research in Ontology-based Systems”, Wiley & Son's
3. Carlos Serrao, Vicente Aguilera, Fabio Cerullo, “Web Application Security” Springer; 1st Edition

References:

1. Jeffrey C. Jackson , “Web Technologies: A Computer Science Perspective”, Prentice Hall ,2006
2. Joel Scambray, Vincent Liu , Caleb Sima ,“Hacking exposed”, McGraw-Hill; 3rd Edition (October, 2010)
3. Software Security Theory Programming and Practice, Richard sinn, cengage Learning
4. Database Security and Auditing, Hassan, Cengage Learning
5. The Web Application Hacker’s handbook, Defydd Stuttard, Wiley Publishing

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISC203	**Internet Routing Design**	**04**
Module	**Detailed content**	**Hours**
1	Networking and Network Routing: An Introduction: Addressing and Internet Service: An Overview, Network Routing, IP Addressing, Service Architecture, Protocol Stack Architecture, Router Architecture, Network Topology, Architecture, Network Management Architecture, Public Switched Telephone.	4
2	Routing Algorithms: Shortest Path and Widest Path: Bellman–Ford Algorithm and the Distance Vector Approach, Dijkstra's Algorithm, Widest Path Algorithm, Dijkstra-Based Approach, Bellman–Ford-Based Approach, *k*-Shortest Paths Algorithm. OSPF and Integrated IS-IS : OSPF: Protocol Features, OSPF Packet Format, Integrated IS-IS, Key Features, comparison BGP : Features ,Operations, Configuration Initialization, phases, Message Format. IP Routing and Distance Vector Protocol Family :RIPv1 and RIPv2.	8
3	Routing Protocols: Framework and Principles: Routing Protocol, Routing Algorithm, and Routing Table, Routing Information Representation and Protocol Messages, Distance Vector Routing Protocol, Link State Routing Protocol, Path Vector Routing, Protocol, Link Cost.	6
4	Internet Routing and Router Architectures: Architectural View of the Internet, Allocation of IP Prefixes and AS Number, Policy-Based Routing, Point of Presence, Traffic Engineering Implications, Internet Routing Instability. Router Architectures: Functions, Types, Elements of a Router, Packet Flow, Packet Processing: Fast Path versus Slow Path, Router Architectures.	6
5	Analysis of Network Algorithms: Network Bottleneck, Network Algorithmics, Thinking Algorithmically, Refining the Algorithm, Cleaning up, Characteristics of Network Algorithms. IP Address Lookup Algorithms : Impact, Address Aggregation, Longest Prefix Matching, Naïve Algorithms, Binary , Multibit and Compressing Multibit Tries, Search by Length Algorithms, Search by Value Approaches, Hardware Algorithms, Comparing Different Approaches. IP Packet Filtering and Classification : Classification, Classification Algorithms, Naïve Solutions, Two-Dimensional Solutions, Approaches for *d* Dimensions.	6
6	Quality of Service Routing: QoS Attributes, Adapting Routing: A Basic Framework. Update Frequency, Information Inaccuracy, and Impact on Routing, Dynamic Call Routing in the PSTN, Heterogeneous Service, Single-Link Case, A General Framework for Source-Based QoS Routing with Path Caching , Routing Protocols for QoS Routing, QOSPF: Extension to OSPF for QoS Routing, ATM PNNI.	6
7	Routing and Traffic Engineering: Traffic Engineering of IP/MPLS Networks, VPN Traffic Engineering, Problem Illustration: Layer 3 VPN, LSP Path Determination: Constrained Shortest Path Approach, LSP Path Determination: Network Flow Modeling Approach, Layer 2 VPN Traffic Engineering, Observations and General Modeling Framework, Routing/Traffic Engineering for Voice Over MPLS.	4

References:

1. Network Routing: Algorithms, Protocols, and Architectures Deepankar Medhi and Karthikeyan Ramasamy (Morgan Kaufmann Series in Networking)
2. Network Algorithmics: An Interdisciplinary Approach to Designing Fast Networked Devices George Varghese (Morgan Kaufmann Series in Networking)

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISE2011	Mobile and Wireless Security	04
Module	**Detailed content**	**Hours**
1	Introduction : Security And Privacy For Mobile And Wireless Networks: Introduction- State Of The Art- Areas For Future Research- General Recommendation For Research. Pervasive Systems: Enhancing Trust Negotiation With Privacy Support: Trust Negotiation- Weakness Of Trust Negotiation- Extending Trust Negotiation To Support Privacy	8
2	Mobile Security: Mobile System Architectures, Overview Of Mobile Cellular Systems, Gsm And Umts Security & Attacks, Vulnerabilities In Cellular Services, Cellular Jamming Attacks & Mitigation, Security In Cellular Voip Services, Mobile Application Security.	8
3	Securing Wireless Networks: Overview Of Wireless Security, Scanning And Enumerating 802.11 Networks, Attacking 802.11 Networks, Attacking Wpa Protected 802.11 Networks, Bluetooth Scanning And Reconnaissance, Bluetooth Eavesdropping, Attacking And Exploiting Bluetooth, Zigbee Security And Zigbee Attacks	8
4	Adhoc Network Security: Security In Ad Hoc Wireless Networks, Network Security Requirements, Issues And Challenges In Security Provisioning, Network Security Attacks, Key Management In Adhoc Wireless Networks, Secure Routing In Adhoc Wireless Networks .Introduction To Wireless Adhoc Networks, Including Mobile Ad Hoc Networks (Manets),Wireless Sensor Networks(Wsn) And Wireless Mesh Networks	8
5	Rfid Security : Introduction,Rfid Security And Privacy,Rfid Chips, Techniques And Protocols,Rfid Anticounterfeiting,Man In The Middle Attacks On Rfid Sysrems,Digital Signature Transponder, User Centric Security For Rfid Based Distributed System, Optimizing Rfid Protocols For Low Information Leakage.	8

Text Books:

1. Kia Makki, Peter Reiher, "Mobile and Wireless Network Security and Privacy ", Springer, 2007, ISBN 978-0-387-71057-0
2. C. Siva Ram Murthy, B.S. Manoj, "Adhoc Wireless Networks Architectures and Protocols", Prentice Hall, 2004, ISBN 9788131706885
3. Noureddine Boudriga, Security of Mobile Communications, 2010, ISBN 9780849379413.
4. Kitsos, Paris; Zhang, Yan , "RFID Security Techniques, Protocols and System-On-Chip Design ",2008, ISBN 978-0-387-76481-8
5. Johny Cache, Joshua Wright and Vincent Liu," Hacking Wireless Exposed: Wireless Security Secrets & Solutions ",second edition, McGraw Hill, 2010, ISBN: 978-0-07-166662-6

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISE2012	Network Management And Performance Evaluation	04

Module	Detailed content	Hours
1	Introduction to Network Management: Analogy of Telephone Network Management, Communication,* protocols and Standards, Case Histories of Networking and Management, Challenges of Information Technology Managers, Network Management: Goals, Organization, and Functions, Network and System Management. Network Management System Platform, Current Status and future of Network Management	8
2	SNMP v1 Network Management: Organization and Information Models: The History of SNMF Management Tue SNMP Mode, The Organization Model, System Overview, The Information Model. The SNMP Communication Model. Functional model -SNMP Management: SNMP v2: Major Changes in SNMPv2, SN[Mpv2 System Architecture, SNMPv2 Structure of Management Information, The SNMPv2 Management Information Base. SNMPv2 Protocol, Compatibility with SNMP v1	8
3	Network Management Tools and Systems: Network Management Tools, Network Statistics Measurement Systems, History of Enterprise Management, Network Management systems, Commercial network management Systems, System Management, and Enterprise Management Solutions - Web-Based Management: NMS with Web Interface and Web-Based Management, Web Interface to SNMP Management, Embedded Web-Based Management, Desktop management Interface, Web-Based Enterprise Management, WBEM: Windows Management Instrumentation. Java management Extensions, Management of a Storage Area Network: Future Directions	8
4	Performance Modeling and Estimation: Overview of Probability and Stochastic Processes - Probability, Random Variables Stochastic Processes, Queuing Analysis - How Queues Behave - A Simple Example Why Queuing Analysis, Queuing Models, Single-Server Queues. Multi server Queues, Examples, Queues with Priorities, Networks of Queues. Other Queuing Models. Estimating Model Parameters - Modeling and Estimation of Self-Similar Traffic: Self-Similar Traffic.-Self-Similarity, Self-Similar Data Traffic, Examples of Self-Similar Data Traffic, and Performance Implications of Self-Similarity. Modeling and Estimation of Self-Similar Data Traffic	8
5	Quality of Service in IP Networks: Exterior Routing Protocols and Multicast - Path-Vector Protocols: BGP and [DKH Multicasting. Integrated and Differentiated Services - Integrated Services Architecture (ISA), Queuing Discipline, Random Early Detection, Differentiated Services, Protocol for QOS Support -Resource Reservation: RSVP. Multiprotocol Label Switching, Real-Time Transport Protocol (RTP)	8

Text Books :

1.Mani Subramanian. "Neiwork Management, Principles and Practice", Pearson Education, 2000, rp2007.

2.William Sellings. "'High-Speed Networks and Internets: Performance and Quality of Service - 2cd", Prentice Hall/Pearson Education, 2002.

References:

1.Benou Claise and Ralf Wolier, "Network Management: Accounting and Performance Strategies", Pearson Education. 2007, rp2008,

2.J. Richard Burke, " Network Management - Concepts and Practice: A Hands-on Approach". PI U, 2004, rp2008.

3.Stephen B. Morris, "Network Management, MBs and MPLS", Pearson Education, 2003. rp200S.

4.Anurag Kumar, D.Manjunath and Joy Kuri, "Communicalion Networking: An Analytical Approach'1, Elsevier,20O4.

5.Engineering Internet Qos, Sanjay Jha and Mahbub Hassan, Artech House. 2002

6.Thomas G. Robertazzi, "ConpulerNetworks and Systems -Queuing Theory and Performance Evaluation – 3rd", Springer, 2000, rp2002.

7.Gary N. Higginbottom, "Performance Evaluation of Communication Networks". Artech House:. 1998.

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISE2013	Network Vulnerabilities and Risk Management	04

Module	Detailed content	Hours
1	Introduction to assessing Network Vulnerabilities: type and procedure of network vulnerability assessment	8
2	Principles of Security: Information Classification, Policy framework, role based security in a organization	8
3	Risk Assessment: Laws, Mandates and Regulations, Risk assessment best practices, Risk assessment best practice. Risk Assessment Methodologies: Defense –in depth approach, risk analysis, Asset valuation approach, Quantitative and Qualitative risk- assessment approaches. Scoping the project, Understanding the attacker.	8
4	Performing the Assessment: Vulnerability scan and Exploitation: Internet Host and network enumeration, IP network Scanning, Assessing Remote Information Services, Assessing Web servers, Assessing Web Applications, Assessing Remote Maintenance Services, Assessing Database services, Assessing Windows Networking Services, Assessing Email services.	8
5	Open source tools used for Assessment and Evaluation, and exploitatio framework	8

Text Books :

1 Network Security assessment, Chris McNab, O'reilly

2. Inside Network Security Assessment, Michael Gregg, Pearson

3. Security in Computing, fourth Edition, Charles Pfleeger, Pearson

4. The Security Risk Assessment Handbook: Douglas LanDoll, Auerbach Publication.

5. Nina Godbole, "Information Systems Security", Wiley

6. Cyber Security: Sunit Belapur, Wiley

7. Whitman & Mattord. Management of Information Security. Thomson Course.

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISE2014	Information Hacking Techniques	04

Module	Detailed content	Hours
1	Incident Handling Overview and preparation : Incident Handling Phase identification, Incident Handling phase containment Incident Handling: Recovering and improving capabilities, Type of incidents	8
2	Hacking Methodology : Enumeration, Scanning, Gaining Access , Maintaining access, Clearing Tracks	6
3	Reconnaissance , Scanning Host discovery, Network devices discovery, service discovery	4
4	Backdoors and Trojan horses , Buffer Overflows	4
5	Covering Tracks : Networks and Systems	4
6	Denial of Service Attacks, Exploiting System using Netcat Format String Attacks	6
7	IP address Spoofing, Network sniffing Password Attacks, root kits Session Hijacking and Defenses, Virtual Machine Attacks, Web application attacks, Worms, Bots & Bot- nets	6

References:

1 . Jon Erickson, Hacking: The Art of Exploitation, Second Edition.

2. Hacker Techniques, Exploits & Incident Handling (Security 504)

http://www.sans.org/training/description.php?mid=40

3. Brain Hatch, Hacking Linux Exposed, 3rd edition Hacking Linux Exposed, 3rd edition.

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISE2021	INFORMATION RETRIEVAL SYSTEM	04
Module	**Detailed content**	**Hours**
1	Introduction: Definition, Objectives, Functional Overview, Relationship to DBMS, Digital libraries and Data Warehouses, Information Retrieval System Capabilities- Search, Browse, Miscellaneous.	6
2	Cataloging and Indexing: Objectives, Indexing Process, Automatic Indexing, Information Extraction, Data Structures: Introduction, Stemming Algorithms, Inverted file. Structures, N-gram data structure, PAT data structure. Signature file structure, Hypertext data structure - Automatic Indexing: Classes of automatic indexing. Statistical indexing. Natural language. Concept indexing. Hypertext linkages	8
3	Document and Term Clustering: Introduction, Thesaurus generation, Item clustering. Hierarchy of clusters - User Search Techniques: Search statements and binding, Similarity measures and ranking. Relevance feedback, Selective dissemination of information search, Weighted searches of Boolean systems, Searching the Internet and hypertext - Information Visualization: Introduction, Cognition and perception. Information visualization technologies.	10
4	Text Search Algorithms: Introduction, Software text search algorithms, Hardware text search systems. Information System Evaluation-Introduction, Measures used in system evaluation, Measurement example TREC results	8
5	Multimedia Information Retrieval : Models and Languages - Data Modeling, Query Languages, Indexing and Searching - Libraries and Bibliographical Systems -Online IR Systems, OPACs, Digital Libraries	8

Text Books :

1. Information Storage and Retrieval Systems: Theory and Implementation By Kowalski, Gerald, Mark T Maybury Kluwer Academic Press, 2000.
2. Modern Information Retrieval By Ricardo Baeza-Yates, Pearson Education, 2007.
3. Information Retrieval: Algorithms and Heuristics By David A Grossman and Ophir Frieder, 2nd Edition. Springer International Edition, 2004.

References :

1. Information Retrieval Data Structures and Algorithms By William B Flake*, Ricardo Baeza-Yates. Pearson Education, 1992.
2. Information Storage & Retrieval By Robert Korfhagc - John Wiley & Sons.
3. Introduction to Information Retrieval By Christopher D. Manning and Prabhakar Raghavan. Cambridge University Press. 2008.

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISE2022	**Public Key Infrastructures & Trust Management**	**04**

Module	Detailed content	Hours
1	Introduction: PKI Symmetric vs Asymmetric cipher, Services of Public key Cryptography, Algorithms. Concept of an infrastructure: Pervasive Substrate, application Enabler, PKI Defined	6
2	Core PKI services: Authentication, Integrity and confidentiality Definition, Mechanism, operational considerations. PKI enable services: Secure communication, secure Time Stamping, Notarization, Non-repudiation, privileges management, Privacy, mechanism Required to Create PKI-enable services.	8
3	Certificate and certification: Certificate, Certificate Policies, Certification Authority, Registration Authority Key and Certificate Management: Key/certificate Life Cycle Management, Certificate Revocation.	6
4	Trust Models: Policy Based Hierarchies, Distributed Trust Architecture, Four-Corner Trust Model, Web model, user-centric trust, cross certification. Multiple Certificates per Entity: Multiple Key pairs, Key pair uses, Real World Difficulties. Independent Certificate management.	6
5	PKI Information Dissemination: Repositories and other techniques: Private Dissemination, Publication and repositories, Inter domain repositories issues and options.	6
6	Electronic Signature Legislation and considerations: Electronic Signature Legislation: E-sign, Digital Signature in context, EU Electronic signature Directive. Legal Consideration for PKI: CA requirement, roles and responsibility, private enterprise PKIs.Deployment Considerations: benefits and cost of PKI, deployment issues and decisions, barriers to deployment.	8

Text Books :

Understanding PKI: Concepts, standards, and Development consideration By Adams, and Steve Lloyd

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISE2023	**Database Security**	**04**
Module	**Detailed content**	**Hours**
1	Introduction: Introduction to database security, problems in database security, Information security &architecture, database security models, multilevel database and security, security policies. Security requirements, Reliability and Integrity, Protecting sensitive data, access control, Access Control Mechanisms.	6
2	Operating system security Fundamentals: Operating system overview, Operating system security environment, components of an operating system security environment, authentication methods, administration of users.	6
3	Software Security Design: Introduction, Secure DBMS Design, Security and integrity mechanisms, secure DBMS architecture, A Methodological Approach to Security Software Design. Database application security Types of users, application types, application security models, data encryption.	6
4	Security Models: Introduction Access Matrix Model, Take-Grant Model, Acten Model, PN Model, Hartson and Hsiao's Model, Fernandez's Model, Bussolati and Martella's Model for Distributed databases, Bell and LaPadula's Model, Biba's Model, Dion's Model, Sea View Model, Jajodia and Sandhu's Model, The Lattice Model for the Flow Control.	6
5	Security Mechanisms: Introduction User Identification/Authentication, Memory Protection, Resource Protection, Control Flow Mechanisms, Isolation Security Functionalities in Some Operating Systems, Trusted Computer, System Evaluation Criteria.	6
6	Statistical Database Protection & Intrusion Detection Systems: Introduction Statistics Concepts and Definitions, Types of Attacks, Inference Controls evaluation Criteria for Control Comparison, Introduction IDES System, RETISS System, ASES System, Discovery. SQL injection: Introduction, SQL injection attack, web application and sql injection, prevention.	6
7	Database auditing: Introduction, auditing Types, auditing models, auditing database activities, auditing environment, application data auditing.	4

Text Books :

1. Database Security by Castano, Pearson Edition .
2. Database Security and Auditing: Protecting Data Integrity and Accessibility Ist Edition, Hassan Afyouni THOMOS Edition
3. Databse administration: Complete guide to DBA practices and procedures, Craig S. Mullins, Second edition.

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination.

Subject Code	Subject Name	Credits
CISE2024	**TCP/IP Technology**	**04**

Module	Detailed content	Hours
1	Introduction To Computer Networks : Introduction To Layered Architecture (Tcp/Ip, Osi), Networking Devices, Ip Class (A-E) Addressing, Subnetting, Vlsm, CIDR .	8
2	Netwrok Layer Protocols : Router Ios- Static And Default Routing-Interior Gateway Routing Protocols: Rip V1&V2, Ospf, Eigrp- Exterior Gateway Routing Protocol: BGP.	8
3	Transport Layer Protocols: Tcp & Udp Datagram And Its Characteristics, Rtp, Flow Control And Error Control Mechanisms, Silly Window Syndrome - Clark's And Nagle Algorithm - Congestion Control Mechanisms - Token Bucket And Leaky Bucket.	8
4	Socket Programming : Introduction To Socket Programming- Concurrent Processing In Client-Server Software-Byte Ordering And Address Conversion Functions – Socket Interface - System Calls Used With Sockets - Iterative Server And Concurrent Server- Multi Protocol And Multi Service Server- Tcp/Udp Client Server Programs – Thread	10
5	IPV6 : Introduction To Ipv6 – Ipv6 Advanced Features –V4 And V6 Header Comparison – V6 Address Types –Stateless Auto Configuration – Ipv6 Routing Protocols – Ipv4-	6

Reference Books

1. Douglas E. Comer ,"Internetworking with TCP/IP, Principles, Protocols, and Architecture", Addison-Wesley, 5th edition, Vol 1, 2005,ISBN-10: 0131876716 | ISBN-13: 978-0131876712 .

2. Douglas E. Comer, David L. Stevens ,"Internetworking with TCP/IP Vol. III, Client-Server Programming and Applications", Addison-Wesley, 2 nd edition, 2000 , ISBN-10: 013260969X,ISBN-13: 978-0132609692.

3. Wendell Odom," CCNP Route 642-902, CCIE", Official Certification Guide, Pearson .

4. Behrouz A. Forouzan, "Data Communications and Networking", McGraw-Hill, 5th edition, 2012, ISBN-10: 0073376221, ISBN-13: 978-0073376226.

Assessment:

Internal:
Assessment consists of two tests out of which; one should be compulsory class test (on minimum 02 Modules) and the other is either a class test or assignment on live problems or course project.

End Semester Examination:
Some guidelines for setting the question papers are as, six questions to be set each of 20 marks, out of these any four questions to be attempted by students. Minimum 80% syllabus should be covered in question papers of end semester examination