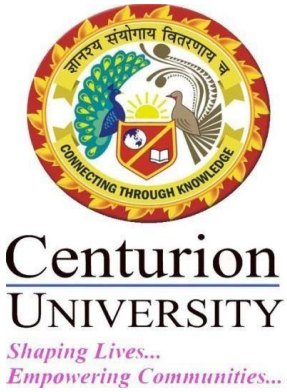

Centurion
UNIVERSITY
Shaping Lives...
Empowering Communities...

Centurion University of Technology & Management, Odisha

M. Sc. Cyber Security & Digital Forensics

(Two Years Programme)

School of Forensic Sciences

2019

Programme Objectives

To provide fundamental and advanced knowledge and expertise to integrate the monitoring and analysis of IP network traffic, as well as serial communications and physical constraints within a single intrusion detection system (IDS) frame work and provide capabilities for determining the physical safety of system operations by simultaneously examining behavior at multiple hierarchical layers. The course will enable to evaluate the technical, social and management dimensions of computing systems and technologies from security perspective.

To introduce the recent advancements in the field of Cyber Security and Digital Forensic and to empower the experts with newer techniques and tools for white collars crime using software's.

Eligibility Criteria

BSc. (+3 Sc) with 50% Mark or aggregate or equivalent in the qualifying degree.

Selection Process

The selection processes is through central counseling on the basis of merit in qualifying CUEE.

Award of degree

After successful completion of degree, student will be awarded with Master of Science in Cyber Security and Digital Forensics by Centurion University of Technology and Management.

.

Course Structure

Semester I				
Code	**Course**	**Course Type (Lecture-Tutorial-Practice)**	**Credit**	**Prerequisite**
MSCS1101	Principles of Information Security	4-0-0	4	
MSCS1102	Digital Forensics	4-0-2	6	
MSCS1103	Computer Networks	4-0-2	6	
MSCS1104	Cyber Crime & Investigations	4-0-0	4	
MSCS1105	Intellectual Property Rights	4-0-0	4	
	Total Credits		**24**	

Semester II				
Code	**Course**	**Course Type (Lecture-Tutorial-Practice)**	**Credit**	**Prerequisite**
MSCS1201	Number theory & Cryptography	4-0-0	4	
MSCS1202	Advanced Information Security	4-0-0	4	
MSCS1203	Cyber Forensics	4-0-2	6	
MSCS1204	System and Network Security	4-0-2	6	
MSCS1205	Cyber Law	4-0-0	4	
	Total Credits		**24**	

Semester III				
Code	**Course**	**Course Type (Lecture-Tutorial-Practice)**	**Credit**	**Prerequisite**
MSCS2101	Mobile Security Analysis	4-0-2	6	
MSCS2102	IT Governance, Risk and Compliance	4-0-0	4	
MSCS2103	Business Continuity Planning (BCP) And Disaster Recovery	4-0-0	4	
MSCS2104	Penetration Testing & Vulnerability Assessment	4-0-2	6	
MSCS2105	Digital Frauds	4-0-0	4	

	Total Credits		**24**	

Semester IV				
Code	**Course**	**Course Type (Lecture-Tutorial-Practice)**	**Credit**	**Prerequisite**
MSCS0301	Project/Dissertation		**24**	

Total credit: 96

Course Outline

Semester - I

MSCS 1101 - Principles of Information Security

MODULE I: (8Hrs)

Overview of Information Security- Threats - Frauds, Thefts, Malicious Hackers, Malicious Code, Denial-of-Services Attacks and Social Engineering, Vulnerability–Types, Risk–an introduction -Business Requirements - Information Security Definitions - Security Policies–Tier-1 (Origination-Level), Tier-2 (Function Level), Tier-3 (Application/Device Level)–Procedures - Standards–Guidelines–Baselines.

MODULE II : (7Hrs)

Information Asset Classification–Information system Asset inventory, Asset Classification criteria, roles and responsibilities–Methodology-Declassification or Reclassification-Retention and Disposal of Information, Assets-Provide Authorization for Access.

MODULE III : (7Hrs)

Risk Management–Need for the Risk Assessment, Risk Assessment Methodology, Risk Assessment Components, Risk Mitigation Techniques.

MODULE IV: (7Hrs)

Information Security& Domains–Fundamental Principles of Security–Security Definitions – Control types–Security Frameworks - Personnel Security. Application Security, Legal & Compliance, Business Continuity Management, Cryptography, Physical & Environmental Security and Security Operations.

Text Book:

- CISSP All-in-One Exam Guide by Shon Harris and Fernando Maymi, 7 Edition, McGraw-Hill Education, 1 June 2016.
- Information Security Management handbook, 6thEdition, Harold F Tipton, Micki Krause, Auerbach Publications, 5 April 2012.
- The CISSP Prep Guide: Gold Edition by Ronald L. Krutz, Russel Dean Vines, Gold Edition, Wiley Publication, 31 Oct 2002.

Reference Book:

- Certified Information Systems Security Professional, Study Guide by Ed Tittle, Mike Chapple, James Michael Stewart, 6th Edition, Sybex Publication, 06 July 2012.
- ISO/ IEC 27002: 2005, First Edition.

Session Plan

Topic coverage and Internal Test	***No. of Sessions*** *(in hrs.)*	***Activity*** *(lecture, tutorial, lab practice, field studies/field-trip, Workshop etc.)*	***Assignment*** *(project, assignment, field study, seminar, etc.)*	***Suggested Reading*** *(Book, Video, Online source, etc.)*
PRINCIPLES OF INFORMATION SECURITY				
Overview of Information Security- Threats - Frauds, Thefts, Malicious Hackers, Malicious Code, Denial-of-Services Attacks and Social Engineering, Vulnerability–Types, Risk–an introduction - Business Requirements - Information Security Definitions - Security Policies–Tier-1 (Origination-Level),Tier-2(Function Level), Tier-3 (Application/Device Level)–Procedures - Standards–Guidelines–Baselines.	8Hrs.	Lecture	Assignment	Information Security Management handbook, 6thEdition, Harold F Tipton, Micki Krause
Information Asset Classification– Information system Asset inventory, Asset Classification criteria,	7 Hrs.	Lecture	Assignment	Information Security Management handbook, 6thEdition,

roles and responsibilities– Methodology- Declassification or Reclassification- Retention and Disposal of Information, Assets- Provide Authorization for Access.				Harold F Tipton, Micki Krause.
Risk Management–Need for the Risk Assessment, Risk Assessment Methodology, Risk Assessment Components, Risk Mitigation Techniques.	7Hrs.	Lecture	Assignment	Information Security Management handbook, 6thEdition, Harold F Tipton, Micki Krause.
Information Security& Domains–Fundamental Principles of Security– Security Definitions – Control types–Security Frameworks - Personnel Security. Application Security, Legal & Compliance, Business Continuity Management, Cryptography, Physical & Environmental Security and Security Operations.	7 Hrs.	Lecture	Assignment	Information Security Management handbook, 6thEdition, Harold F Tipton, Micki Krause.

MSCS1102 Digital Forensics

MODULE I : (7Hrs)

Digital Forensics overview–Difference between computer Forensics and Digital Forensics, Digital Forensics in today's world, Computer Forensics investigation process, Forensics readiness planning and its benefits.

MODULE II : (7Hrs)

Understanding Digital Forensic Investigation–Digital Forensics Life Cycle- Understanding key steps in Forensics investigation, Role of forensic investigator – Ethics of a forensic investigator– challenges faced by forensic investigators.

MODULE III : (8Hrs)

Role of Digital Evidence& its collection-Digital Evidence–Authentication of Evidence-Importance of digital evidences in investigation and in court of law–Capabilities of a digital forensic investigator. Evidence Collection -Collections Options – Obstacles - Types of Evidence - Standards of Evidence - The rules of Evidence - Volatile Evidence– Electronic Evidence General Procedure - Collection and Archiving of evidence -Methods of Collection – Artifacts - Controlling Contamination - Chain of custody.

MODULE IV: (7Hrs)

Computer Forensics Investigation Process -Cyber Forensics investigation methodology, steps to prepare for a computer forensics investigation, procedure to collect evidence in crime scene, search warrants, evaluate and secure the crime scene.

Text Book:

1. Computer Forensics: Cyber Criminals, Laws and Evidence by Marie-Helen Maras,1stedition, Jones and Bartlett Publishers, 1 February 2011
2. Computer Forensics, Computer Crime Scene Investigation by John. R. Vacca, 2nd Edition, Charles River Media Publication, 15 June 2002
3. Cyber Forensics: A field manual for collecting, Examining, preserving evidence of computer crimes by Albert Marcella, Jr., Doug Menendez, Second Edition, CRC Press 2007.

Reference Book:

1. Guide to Computer Forensics and Investigations, Processing Digital Evidence by Bill Nelson, Amelia
2. Phillips, Christopher Stuart, 4th edition, Delmar Cengage Learning, 28 Oct 2009
3. Digital Forensics for Legal Professionals - Understanding Digital Evidence from the Warrant to the Courtroom by Larry Daniel, Lars Daniel, 1edition, Syngress, 14October 2011.

Session Plan

Topic coverage and Internal Test	***No. of Sessions*** *(in hrs.)*	***Activity*** *(lecture, tutorial, lab practice, field studies/field-trip, Workshop etc.)*	***Assignment*** *(project, assignment, field study, seminar, etc.)*	***Suggested Reading*** *(Book, Video, Online source, etc.)*
DIGITAL FORENSICS				
Digital Forensics overview–Difference between computer Forensics and Digital Forensics, Digital Forensics in today's world, Computer Forensics investigation process, Forensics readiness planning and its benefits.	7 Hrs.	Lecture	Assignment	Computer Forensics: Cyber Criminals, Laws and Evidence by Marie-Helen Maras
Understanding Digital Forensic Investigation–Digital Forensics Life Cycle- Understanding key steps in Forensics investigation, Role of forensic investigator –Ethics of a forensic investigator–challenges faced by forensic investigators.	7 Hrs.	Lecture	Assignment	Computer Forensics: Cyber Criminals, Laws and Evidence by Marie-Helen Maras
Role of Digital Evidence& its collection-Digital Evidence–Authentication of Evidence-Importance of digital evidences in	8 Hrs.	Lecture	Assignment	Computer Forensics: Cyber Criminals, Laws and Evidence by Marie-Helen Maras

investigation and in court of law–Capabilities of a digital forensic investigator. Evidence Collection -Collections Options – Obstacles - Types of Evidence - Standards of Evidence - The rules of Evidence - Volatile Evidence– Electronic Evidence General Procedure - Collection and Archiving of evidence -Methods of Collection – Artifacts - Controlling Contamination - Chain of custody.				
Computer Forensics Investigation Process - Cyber Forensics investigation methodology, steps to prepare for a computer forensics investigation, procedure to collect evidence in crime scene, search warrants, evaluate and secure the crime scene.	7 Hrs.	Lecture	Assignment	Computer Forensics: Cyber Criminals, Laws and Evidence by Marie-Helen Maras

SEMESTER-I LABORATORY

DIGITAL FORENSICS LAB-1

1. Digital Forensic Process and Methodologies.
2. Digital Concepts and Magnetic Media.
3. Evidence Preservation.
4. Forensic Software Packages.
5. Windows Filesystems: FAT, NTFS
6. Linux Filesystems: Ext, JFS, XFS & Swap.
7. Timeline and File Metadata Behaviors
8. Windows Forensic Techniques-I

   Basic searches, Deleted partition/volume analysis, File signature analysis, File hash analysis, Recycle bin analysis, Prefetch Files, Windows XP system analysis
9. Disk Management.
10. Windows Forensic Techniques II and Internet/Email Analysis.

    Regular-expression searches, Registry analysis, Internet cache analysis, Email and email header analysis, USBStor Analysis, Windows 7 analysis

MSCS 1103 - Computer Networks

MODULE I: **(9Hrs)**

Introduction-Networking – Devices, Need for computer networks - Network Topologies - Types of networks -Hardware needed for setting up simple LAN, Wireless networks and for inter-connecting LANs and WAN -Communication media - IEEE 802 series standards – Wireless technology - Spread spectrum - WAP and WML - Access points - Service Set ID (SSID) - Authentication methods (OSA, SKA) - Types of Cables–Ethernet - Token Ring - Optical Fiber - Introduction to MAC address - Introduction to IP address - Classes of IP address - Need for subnetting -Basics of IPV6 - Introduction to Unicast, Multicast and Broadcast.

MODULE II : **(7Hrs)**

Routing-Types of connections – Circuit switched, Packet switched – Importance of Packet Switches -Types of protocols and need for protocols - Packet switched Protocols - TCP/ IP. Fundamentals of routing – Link State Routing - Distance Vector Routing–RIP–EIGRP–OSPF - Configuring Routers - Understanding the router architecture - Assigning IP address to the routers - Configuring routing protocols.

MODULE III : **(7Hrs)**

OSI Layers- Interconnecting disparate systems/ networks–issues- Open Systems Interconnect 7layers and their functionality - Introduction to TCP/ IP - Origins of TCP/ IP and evolution of Internet - IP Layers Vs OSI - IP number concepts - Network address - Classes of Networks - Subnet masking - Static and dynamic IP numbers - UDP - Establishing a TCP session (Three way handshake) - Name to address translation - DomainName System

MODULE IV: **(7Hrs)**

Networking to the end user- Configuring Server for enterprise networking - Introduction to Domains and Work groups - Understanding DNS and configuring DNS - Introduction to ADS (Active Directory Service) -File sharing within network - Understanding DHCP - Introduction to Mail Exchange server and ISA server -Network operating system - Client Server applications - Peer to Peer Applications - Measuring performance - Monitoring tools.

Text Book:

1. Data Communications and Networking (Forouzan Behrouz A. 5th Edition) McGraw-Hill Education.
2. Information Security Management handbook, 6th Edition, Harold F Tipton, Micki Krause, Auerbach Publications, 5 April 2012.
3. Network Security: The Complete Reference by Roberta Bragg, Mark Rhodes-Ousley, Keith Strasberg, Paperback Edition, McGraw Hill Education, 27 January 2004.

Reference Book:

1. Cryptography and Network Security by Dr. William Stallings, 6th Edition, Pearson Education Publication, 01 Jan2013.
2. Network Security: Private Communications in a Public World by Mike Speciner, Radia Perlman, Charlie Kaufman 2nd, Edition, Prentice Hall, 22 April 2002.

Session Plan

Topic coverage and Internal Test	***No. of Sessions*** *(in hrs.)*	***Activity*** *(lecture, tutorial, lab practice, field studies/field-trip, Workshop etc.)*	***Assignment*** *(project, assignment, field study, seminar, etc.)*	***Suggested Reading*** *(Book, Video, Online source, etc.)*
COMPUTER NETWORKS				
Introduction- Networking – Devices, Need for computer networks - Network Topologies - Types of networks -Hardware needed for setting up simple LAN, Wireless networks and for inter-connecting LANs and WAN -Communication media - IEEE 802 series standards – Wireless technology - Spread spectrum - WAP and WML - Access points - Service Set ID (SSID) - Authentication methods (OSA, SKA) - Types of Cables–Ethernet -	9 Hrs.	Lecture	Assignment	1. Data Communications and Networking (Forouzan Behrouz A. 5th Edition) McGraw-Hill Education. **2.** Cryptography and Network Security by Dr. William Stallings

Token Ring - Optical Fiber - Introduction to MAC address - Introduction to IP address - Classes of IP address -Need for subnetting -Basics of IPV6 - Introduction to Unicast, Multicast and Broadcast.				
Routing-Types of connections – Circuit switched, Packet switched – Importance of Packet Switches - Types of protocols and need for protocols - Packet switched Protocols - TCP/ IP. Fundamentals of routing – Link State Routing - Distance Vector Routing–RIP–EIGRP–OSPF - Configuring Routers - Understanding the router architecture - Assigning IP address to the routers - Configuring routing protocols.	7 Hrs.	Lecture	Assignment	Data Communications and Networking (Forouzan Behrouz A. 5th Edition) McGraw-Hill Education.
OSI Layers- Interconnecting disparate systems/ networks–issues- Open Systems Interconnect 7layers and their functionality - Introduction to TCP/ IP	7 Hrs.	Lecture	Assignment	Data Communications and Networking (Forouzan Behrouz A. 5th Edition) McGraw-Hill Education.

- Origins of TCP/ IP and evolution of Internet - IP Layers Vs OSI - IP number concepts - Network address - Classes of Networks - Subnet masking - Static and dynamic IP numbers - UDP - Establishing a TCP session (Three way handshake) - Name to address translation - DomainName System				
Networking to the end user- Configuring Server for enterprise networking - Introduction to Domains and Work groups - Understanding DNS and configuring DNS - Introduction to ADS (Active Directory Service) -File sharing within network - Understanding DHCP - Introduction to Mail Exchange server and ISA server -Network operating system - Client Server applications - Peer to Peer Applications - Measuring performance - Monitoring tools.	7 Hrs.	Lecture	Assignment	1. Data Communications and Networking (Forouzan Behrouz A. 5th Edition) McGraw-Hill Education. 2. Cryptography and Network Security by Dr. William Stallings

COMPUTER NETWORKS LAB

1. Network Cabling (Straight/Cross).
2. Establish a LAN connection using three systems using bus topology.
3. Establish peer to peer network connection using two systems in a LAN.
4. Installing Network Components.
5. Configure IP Address in a system in LAN / (TCP/IP Configuration)/Subnetting.
6. Routing (Static/Dynamic) - RIP, OSPF.
7. Transfer files between systems in LAN using FTP Configuration.
8. Login a system remotely using telnet protocol.
9. Install and configure network interface card in LAN system.
10. Share a file and printer (remotely) between two systems in a LAN.

MSCS1104 - Cyber Crime & Investigations

MODULE I : (7Hrs)

Cyber Crime–Definition, Nature and Extent of Cyber Crimes in India and other countries – Classification of Cyber Crimes–Differences between conventional crimes and cybercrimes - Trends in Cyber Crimes across the world.

MODULE II : (7Hrs)

Forms of Cyber Crimes, Frauds–Cyber bullying, hacking, cracking, DoS–viruses, works, bombs, logical bombs, time bombs, email bombing, data diddling, salami attacks, phishing, steganography, cyberstalking, spoofing, cyberpornography, defamation, computer vandalism, crimes through social networking sites, malwares, social engineering, credit card frauds & financial frauds, telecom frauds. Cloud based, E-commerce Frauds and other forms.

MODULE III: (7Hrs)

Profile of Cyber criminals–Cyber Crime Psychology–Psychological theories dealing with cybercrimes-Learning, Motivation, personality and intelligence theories of cyber criminals – Criminal profiling. Impact of cybercrimes – Economic, Psychological and Sociological impact on individual, corporate and companies, government and the nation.

MODULE IV: (7Hrs)

Modus Operandi of various cybercrimes and frauds–Modus Operandi-Fraud triangle–fraud detection techniques-countermeasures. Intrusion Analysis, Intrusion Analysis as a Core Skillset, Methods to Performing Intrusion Analysis, Intrusion Kill Chain, Passively Discovering Activity in Historical Data and Logs, Detecting Future Threat Actions and Capabilities, Denying Access to Threats, Delaying and Degrading Adversary Tactics and Malware, Identifying Intrusion Patterns and Key Indicators.

Text Book:

1. Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats by Will Gragido, John Pirc, 1st edition, Syngress, 7 January 2011.
2. Cyber Crime & Warfare: All That Matters by Peter Warren, Michael Streeter, Kindle Edition, Hodder & Stoughton, 26 July 2013.
3. Digital Evidence and computer crime by Eoghan Casey, 3rd Edition, Academic Press Publication, 17 June 2011.

Reference Book:

1. The Psychology of Cyber Crime: Concepts and Principles by Grainne Kirwan, Andrew Power, 1st edition, Business Science Reference, 15 March 2012
2. Cyber Law of Information Technology and Internet (Lexix Nexis) Anirudh Rastogi Understanding Laws–Cyber Laws and Cyber Crimes (Lexix Nexis).
3. Cyber Crime Manual by Bibhas Chatterjee, Lawman Publication.

Session Plan

Topic coverage and Internal Test	***No. of Sessions*** *(in hrs.)*	***Activity*** *(lecture, tutorial, lab practice, field studies/field-trip, Workshop etc.)*	***Assignment*** *(project, assignment, field study, seminar, etc.)*	***Suggested Reading*** *(Book, Video, Online source, etc.)*
CYBER CRIME & INVESTIGATIONS				
Cyber Crime–Definition, Nature and Extent of Cyber Crimes in India and other countries – Classification of Cyber Crimes–Differences between conventional crimes and cybercrimes - Trends in Cyber Crimes across the world.	7 Hrs.	Lecture	Assignment	Will Gragido, John Pirc. Peter Warren, Michael Streeter
Forms of Cyber Crimes, Frauds–Cyber bullying, hacking, cracking, DoS–	7 Hrs.	Lecture	Assignment	Will Gragido, John Pirc. Peter Warren
Profile of Cyber criminals–Cyber Crime Psychology–Psychological theories dealing with cybercrimes-Learning, Motivation, personality and intelligence theories of cyber criminals – Criminal profiling. Impact of cybercrimes – Economic, Psychological and Sociological impact on individual, corporate and companies, government and the	7 Hrs.	Lecture	Assignment	Will Gragido, John Pirc. Peter Warren, Michael Streeter

nation.				
Modus Operandi of various cybercrimes and frauds–Modus Operandi-Fraud triangle–fraud detection techniques-countermeasures. Intrusion Analysis, Intrusion Analysis as a Core Skillset, Methods to Performing Intrusion Analysis, Intrusion Kill Chain, Passively Discovering Activity in Historical Data and Logs, Detecting Future Threat Actions and Capabilities, Denying Access to Threats, Delaying and Degrading Adversary Tactics and Malware, Identifying Intrusion Patterns and Key Indicators.	7 Hrs.	Lecture	Assignment	Will Gragido, John Pirc. Peter Warren, Michael Streeter

MSCS1105- Intellectual Property Rights

MODULE I: (7Hrs)

Intellectual Property -Meaning and concept of intellectual Property and the need for protection – The world Intellectual property Organization (WIPO) Convention - Origin and functions of World Trade Organization (WTO) - Trade Related Intellectual Property Rights (TRIPS) Agreement of WTO and its effects on Intellectual Property law in India; Dispute Settlement Mechanism.

MODULE II: (10Hrs)

Patents -The Patents Act O(1970), object definitions, salient features, patentable and non-patentable inventions, product and process patents–Patent applicants, provisional and complete specifications, priority dates, of claims, opposition to grant of patent, anticipation, provisions for secrecy of certain inventions - Patent office and power of Controller - Grant and sealing of patents, rights of patentees, rights of co-owners of patents, term of patent, patents of addition, assignment and transmission, register of patents - Amendment of applications and specifications, restoration of lapsed patents, rights of patentees of lapsed patents, surrender and revocation of patents - Compulsory licenses, exclusive marketing rights, licenses of right, use of invocation of patents purposes of government, acquisition of inventions by Central Government - Remedies for infringement of patents - Patent agents, scientific advisers, international arrangements - Right of plant breeders and farmers - National Law on Biological Diversity.

MODULE III: (7Hrs)

Trade Marks -The Trade Mark Act (1999), object, definitions, salient features, marks registrable and non–registrable, conditions for registration, absolute and relative grounds for refusal of registration, procedure for and duration of registration, effects of registration - Powers and functions of Registrar - Distinctiveness, deceptive similarity, concurrent registration, rectification and correction of register - Assignment and transmission - Use of trademarks and registered users, collective marks, registration of certification mars, trade mark agents - Appellate board - Infringement action, passing off action - International treaties.

MODULE IV: (7Hrs)

Copyright- The Copyright Act (1957) and recent amendments: works in which copyright subsists -meaning of copyright; ownership and rights of the owner; assignment; term of copyright - Registration of copyright; compulsory licenses - copyright societies - Rights of broadcasting organizations and of performers -International copyright - Acts constituting & not constituting infringement; remedies for infringement.

TEXT BOOK:

1. Law relating to patents, trademarks, copyright, design and geographical indications by Dr. B.L. Wadehra, 5th edition, Universal law Publication, 2012.
2. Law of Intellectual Property by Dr. S.R. Myneni, 6Edition, Asia Law House Publication, 01 Jan 2013.

REFERRENCE BOOK:

1. International Property by David I. Bainbridge,9th Edition, Pearson Education Publication, 24 May 2012.
2. Intellectual Property, Patents, Copyright, trademarks and allied rights by W.R. Cornish, D Llewelyn,6th Edition, sweet and Maxwell Publication, 18 June 2007.

Session Plan

Topic coverage and Internal Test	***No. of Sessions*** *(in hrs.)*	***Activity*** *(lecture, tutorial, lab practice, field studies/field-trip, Workshop etc.)*	***Assignment*** *(project, assignment, field study, seminar, etc.)*	***Suggested Reading*** *(Book, Video, Online source, etc.)*
INTELLECTUAL PROPERTY RIGHTS				
Intellectual Property - Meaning and concept of intellectual Property and the need for protection – The world Intellectual property Organization (WIPO) Convention - Origin and functions of World Trade Organization (WTO) - Trade Related Intellectual Property Rights (TRIPS) Agreement of WTO and its effects on Intellectual Property law in India; Dispute Settlement	7 Hrs.	Lecture	Assignment	Dr. B.L. Wadehra. W.R. Cornish, D Llewelyn

Mechanism.				
Patents -The Patents Act O(1970), object definitions, salient features, patentable and non- patentable inventions, product and process patents–Patent applicants, provisional and complete specifications, priority dates, of claims, opposition to grant of patent, anticipation, provisions for secrecy of certain inventions - Patent office and power of Controller - Grant and sealing of patents, rights of patentees, rights of co-owners of patents, term of patent, patents of addition, assignment and transmission, register of patents - Amendment of applications and specifications, restoration of lapsed patents, rights of patentees of lapsed patents, surrender and revocation of patents - Compulsory licenses, exclusive marketing rights, licenses of right, use of invocation of patents purposes of government, acquisition of inventions by Central Government - Remedies for infringement of patents	10 Hrs.	Lecture	Assignment	Dr. B.L. Wadehra. W.R. Cornish, D Llewelyn

- Patent agents, scientific advisers, international arrangements - Right of plant breeders and farmers - National Law on Biological Diversity.				
Trade Marks -The Trade Mark Act (1999), object, definitions, salient features, marks registrable and non–registrable, conditions for registration, absolute and relative grounds for refusal of registration, procedure for and duration of registration, effects of registration - Powers and functions of Registrar - Distinctiveness, deceptive similarity, concurrent registration, rectification and correction of register - Assignment and transmission - Use of trademarks and registered users, collective marks, registration of certification mars, trade mark agents - Appellate board - Infringement action, passing off action - International treaties.	7 Hrs.	Lecture	Assignment	Dr. B.L. Wadehra. W.R. Cornish, D Llewelyn.
Copyright- The Copyright Act (1957) and recent amendments: works in which copyright subsists -meaning of copyright; ownership and	7 Hrs.	Lecture	Assignment	Dr. B.L. Wadehra. W.R. Cornish, D Llewelyn.

rights of the owner; assignment; term of copyright - Registration of copyright; compulsory licenses - copyright societies - Rights of broadcasting organizations and of performers - International copyright - Acts constituting & not constituting infringement; remedies for infringement.				

MSCS1201 - Number Theory & Cryptography

MODULE I: (9Hrs)

NUMBER THEORY: Introduction - Divisibility - Greatest common divisor - Prime numbers - Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers - Euclidean algorithm - Fermat's theorem - Euler totient function - Euler's theorem. Congruences: Definition - Basic properties of congruences - Residue classes - Chinese remainder theorem.

MODULE II : (7Hrs)

ALGEBRAIC STRUCTURES: Groups - Cyclic groups, Cosets, Modulo groups - Primitive roots - Discrete logarithms. Rings – Sub rings, ideals and quotient rings, Integral domains. Fields - Finite fields – GF (P^n), GF (2^n) - Classification - Structure of finite fields. Lattice, Lattice as Algebraic system, sub lattices, some special lattices.

MODULE III : (7Hrs)

PROBABILITY THEORY: Introduction – Concepts of Probability – Conditional Probability - Baye's Theorem - Random Variables – discrete and continuous central Limit Theorem- Stochastic Process Markov Chain.

MODULE IV: (10Hrs)

CODING THEORY: Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Linear codes - Generator matrices and parity check matrices - Syndrome decoding – Hamming codes - Hadamard Code – Goppa codes.

PSEUDORANDOM NUMBER GENERATION: Introduction and examples - Indistinguishability of Probability Distributions - Next Bit Predictors - The Blum Blum-Shub Generator – Security of the BBS Generator.

TEXT BOOK:

1. D. S. Malik, J. Mordeson, M. K. Sen, Fundamentals of abstract algebra, Tata McGraw Hill.
2. P. K. Saikia, Linear algebra, Pearson Education, 2009.
3. I. Niven, H.S. Zuckerman and H. L. Montgomery, An introduction to the theory of numbers, John Wiley and Sons, 2004.
4. D P Bersekas and J N Tsitsiklis, Introduction to probability, Athena Scientific, 2008.
5. Douglas Stinson, 'Cryptography – Theory and Practice', CRC Press, 2006.
6. Sheldon M Ross, "Introduction to Probability Models", Academic Press, 2003.
7. C.L. Liu, 'Elements of Discrete mathematics', McGraw Hill, 2008.
8. Fraleigh J. B., 'A first course in abstract algebra', Narosa, 1990.
9. Joseph A. Gallian, ''Contemporary Abstract Algebra', Narosa, 1998.

REFERENCE BOOK:

1. Elementary Number Theory (7th ed.) by David M. Burton.
2. Rosen - Elementary number theory and its applications.
3. Elementary Number Theory and Its Applications, 5th edition, Instructor's Solutions Manual.

Session Plan

Topic coverage and Internal Test	***No. of Sessions*** *(in hrs.)*	***Activity*** *(lecture, tutorial, lab practice, field studies/field-trip, Workshop etc.)*	***Assignment*** *(project, assignment, field study, seminar, etc.)*	***Suggested Reading*** *(Book, Video, Online source, etc.)*
NUMBER THEORY & CRYPTOGRAPHY				
NUMBER THEORY: Introduction - Divisibility - Greatest common divisor - Prime numbers - Fundamental theorem of arithmetic - Mersenne primes - Fermat numbers - Euclidean algorithm - Fermat's theorem - Euler totient function - Euler's theorem. Congruences: Definition - Basic properties of congruences - Residue classes - Chinese remainder theorem.	9 Hrs.	Lecture	Assignment	D. S. Malik, J. Mordeson, M. K. Sen. I. Niven, H.S. Zuckerman and H. L. Montgomery.
ALGEBRAIC STRUCTURES: Groups - Cyclic groups, Cosets, Modulo groups - Primitive roots - Discrete logarithms. Rings – Sub rings, ideals and quotient rings, Integral domains. Fields - Finite fields – GF (P^n), GF (2^n) - Classification - Structure of finite fields. Lattice,	7 Hrs.	Lecture	Assignment	D. S. Malik, J. Mordeson, M. K. Sen. I. Niven, H.S. Zuckerman and H. L. Montgomery.

Lattice as Algebraic system, sub lattices, some special lattices.				
PROBABILITY THEORY: Introduction – Concepts of Probability – Conditional Probability - Baye's Theorem - Random Variables – discrete and continuous central Limit Theorem- Stochastic Process Markov Chain.	7 Hrs.	Lecture	Assignment	D P Bersekas and J N Tsitsiklis.
CODING THEORY: Introduction - Basic concepts: codes, minimum distance, equivalence of codes, Linear codes - Linear codes - Generator matrices and parity check matrices - Syndrome decoding – Hamming codes - Hadamard Code – Goppa codes. **PSEUDORANDOM NUMBER GENERATION**: Introduction and examples - Indistinguishability of Probability Distributions - Next Bit Predictors - The Blum Blum-Shub Generator – Security of the BBS Generator.	10 Hrs.	Lecture	Assignment	Neal Koblitz. Sheldon M Ross. I. Niven, H.S. Zuckerman and H. L. Montgomery.

MSCS1202 - Advanced Information Security

MODULE I: (7Hrs)

Digital Rights Management- Meaning of Digital Rights Management (DRM) - Need for DRM and preventing illegal file sharing on the Internet - DRM schemes - Microsoft DRM 2.0, and the Content Scrambling System.

MODULE II: (7Hrs)

DRM Schemes–Advantages and disadvantages of DRM schemes - Requirements for a good DRM scheme- secure hardware, secure software, and an efficient legal system.

MODULE III: (10Hrs)

Operating System Security-Cryptology-Classical Encryption Techniques - Substitution Techniques - Transposition Techniques–-Permutation Methods - Confidentiality using conventional encryption - Placement of Encryption -Symmetric and Asymmetric crypto systems–common crypto standards and applications - Traffic Confidentiality – Key Distribution - Random Number Generation - Key Management - Generating Keys - Nonlinear Key spaces - Transferring Keys - Verifying Keys - Using Keys - Updating Keys - Storing Keys - Backup Keys – Compromised Keys - Lifetime of Keys - Destroying Keys - Public-Key Key infrastructure - Criminal Code Systems Analysis -Sports Bookmaking Codes - Horse Race Bookmaking Codes - Number Bookmaking Codes - Drug Codes – Pager Codes- Steganography.

MODULE IV: (7Hrs)

Database Security-Overview of Database - Database application security models-Data base auditing models-Application data auditing-Practices of database auditing. Data Loss prevention – Content Filtering - Device Control - Network DLP - Host DLP.

TEXT BOOK:

1. CISSP All-in-One Exam Guide by Shon Harris and Fernando Maymi, 7th Edition, McGraw-Hill Education, 1 June 2016.
2. Information Security Management handbook, 6th Edition, Harold F Tipton, Micki Krause, Auerbach Publications, 5 April 2012.
3. The World Beyond Digital Rights Management by Jude Umeh, 1st edition, BCS - The Chartered Institute for IT, 2009.
4. Cryptography and Network Security by Dr. William Stallings, 6th Edition, Pearson Education Publication, 01 Jan 2013.

REFERENCE BOOK:

1. The CISSP Prep Guide: Gold Edition by Ronald L. Krutz, Russel Dean Vines, Gold Edition, Wiley Publication, 31 Oct 2002.
2. Certified Information Systems Security Professional, Study Guide by Ed Tittle, Mike Chapple, James Michael Stewart, 6th Edition, Sybex Publication, 06 July 2012.

Session Plan

Topic coverage and Internal Test	***No. of Sessions*** *(in hrs.)*	***Activity*** *(lecture, tutorial, lab practice, field studies/field-trip, Workshop etc.)*	***Assignment*** *(project, assignment, field study, seminar, etc.)*	***Suggested Reading*** *(Book, Video, Online source, etc.)*
ADVANCED INFORMATION SECURITY				
Digital Rights Management- Meaning of Digital Rights Management (DRM) - Need for DRM and preventing illegal file sharing on the Internet - DRM schemes - Microsoft DRM 2.0, and the Content Scrambling System.	7 Hrs.	Lecture	Assignment	Shon Harris and Fernando Maymi. Harold F Tipton, Micki Krause, Auerbach
DRM Schemes– Advantages and disadvantages of DRM schemes - Requirements for a good DRM scheme - secure hardware, secure software, and an efficient legal system.	7 Hrs.	Lecture	Assignment	Shon Harris and Fernando Maymi. Harold F Tipton, Micki Krause, Auerbach
Cryptology-Classical Encryption Techniques - Substitution Techniques -	10 Hrs.	Lecture	Assignment	Shon Harris and Fernando Maymi.

Transposition Techniques–-Permutation Methods - Confidentiality using conventional encryption - Placement of Encryption -Symmetric and Asymmetric crypto systems–common crypto standards and applications - Traffic Confidentiality – Key Distribution - Random Number Generation - Key Management - Generating Keys - Nonlinear Key spaces -Transferring Keys - Verifying Keys - Using Keys - Updating Keys - Storing Keys - Backup Keys – Compromised Keys - Lifetime of Keys - Destroying Keys - Public-Key Key infrastructure - Criminal Code Systems Analysis -Sports Bookmaking Codes - Horse Race Bookmaking Codes - Number Bookmaking Codes - Drug Codes – Pager Codes- Steganography.				Harold F Tipton, Micki Krause, Auerbach
Database Security- Overview of Database - Database application security models-Database auditing models- Application data auditing- Practices of database auditing. Data Loss	7 Hrs.	Lecture	Assignment	Shon Harris and Fernando Maymi. Harold F Tipton, Micki Krause, Auerbach

prevention – Content Filtering - Device Control - Network DLP - Host DLP.				

MSCS1203 - Cyber Forensics

MODULE I: (7Hrs)

Digital Forensics–Understanding OS file system-Boot Process-Hard Drive architecture. Introduction to Incident response, digital forensics four-step procedure, Concepts: computer/network/Internet forensic and anti-forensics. Memory forensics.

MODULE II : (7Hrs)

OS Forensics–Basic Windows / Linux Forensics including log analyzer-Register Viewer-Process Viewer-Browser logs review - Packet capturing - Password identification. UNIX/Linux incident response tools, UNIX/Linux file systems (Ext2/Ext3), Unix/Linux forensics investigation steps and technologies, Unix/Linux forensics case studies., Windows incident response tools, Windows file systems, Windows forensics tools, Windows acquisition, Windows forensics analysis – registry and other artifacts.

MODULE III: (7Hrs)

Forensic Imaging Process–Acquiring the Digital Evidence–Understanding Data Acquisition, Data Acquisition methods and Process. Disk and File System Analysis – Media Analysis Concepts – The SleuthKit – Partioning Disk Layouts–Special Containers – Hashing – Carving – Forensic Imaging.

MODULE (IV): (7Hrs)

Digital Forensics with Open Source Tools–Digital Forensics–Open Source tools–Benefits of Open Source Tools–Open Source Examination Platform–Preparing the Examination System–Using Linux as the host - Using Windows as the host, Loadable kernel module rootkits, Steganography hiding, detection and analysis.

TEXT BOOK:

1. Digital Forensics with Open Source Tools by Cory Altheide, Harlan Carvey, Paperback–Import Edition, Syngress, 24 May 2011.
2. Understanding Forensic Digital Imaging by Herbert L. Blitzer, Karen Stein-Ferguson, Jeffrey Huang, 1st Edition, Academic Press, 26 July 2010.
3. The basics of Digital Forensics by John Sammons, 2nd Edition, Elsevier Publication, 2012.
4. Windows Forensics Analysis Tool kit by Harlan Carvey, 3rd Edition, Syngress Publication, 2007.

REFERENCE BOOK:

1. Cyber Forensics: A field manual for collecting, Examining, preserving evidence of computer crimes by Albert Marcella, Jr., Doug Menendez, Second Edition, CRC Press 2007.
2. Encase Computer Forensics–The Official EnCE: Encase Certified Examiner Study Guide by Steve Bunting, 3rd Edition, John Wiley & Sons Publication, 2012.
3. ManYoungRhee, "Internet Security: Cryptographic Principles", "Algorithms and Protocols", Wiley Publications, 2003.
4. Nelson, Phillips, Enfinger, Steuart, "Computer Forensics and Investigations", Cengage Learning, India Edition, 2008.

Session Plan

Topic coverage and Internal Test	***No. of Sessions*** *(in hrs.)*	***Activity*** *(lecture, tutorial, lab practice, field studies/field-trip, Workshop etc.)*	***Assignment*** *(project, assignment, field study, seminar, etc.)*	***Suggested Reading*** *(Book, Video, Online source, etc.)*
CYBER FORENSICS				
Digital Forensics–Understanding OS file system-Boot Process-Hard Drive architecture. Introduction to Incident response, digital forensics four-step procedure, Concepts: computer/network/Internet forensic and anti-forensics. Memory forensics.	7 Hrs.	Lecture	Assignment	Cory Altheide, Harlan Carvey. John Sammons. Harlan Carvey
OS Forensics–Basic Windows / Linux Forensics including log analyzer-Register Viewer-	7 Hrs.	Lecture	Assignment	Cory Altheide, Harlan Carvey. John Sammons.

Process Viewer-Browser logs review - Packet capturing - Password identification. UNIX/Linux incident response tools, UNIX/Linux file systems (Ext2/Ext3), Unix/Linux forensics investigation steps and technologies, Unix/Linux forensics case studies., Windows incident response tools, Windows file systems, Windows forensics tools, Windows acquisition, Windows forensics analysis – registry and other artifacts.				Harlan Carvey
Forensic Imaging Process–Acquiring the Digital Evidence–Understanding Data Acquisition, Data Acquisition methods and Process. Disk and File System Analysis – Media Analysis Concepts – The Sleuth Kit – Partioning Disk Layouts–Special Containers – Hashing – Carving – Forensic Imaging.	7 Hrs.	Lecture	Assignment	Cory Altheide, Harlan Carvey. John Sammons. Harlan Carvey
Digital Forensics with Open Source Tools– Digital Forensics–Open Source tools–Benefits of Open Source Tools–Open Source Examination	7 Hrs.	Lecture	Assignment	Cory Altheide, Harlan Carvey. John Sammons. Harlan Carvey

Platform–Preparing the Examination System– Using Linux as the host - Using Windows as the host, Loadable kernel module rootkits, Steganography hiding, detection and analysis.				

SEMESTER-II LABORATORY

DIGITAL FORENSICS - LAB II

- Image Analysis and Steganography.
    1. Image types.
    2. Evidence hiding.
    3. Steganography.
- Live System Acquisition and Partial Acquisitions.
    4. Live system concerns.
    5. Large server concerns.
    6. Imaging speed and bandwidth.
    7. RAM acquisitions and concerns.
- Network Forensics Introductions.
    8. Network forensic concerns.
    9. Preservation of network traffic.
    10. Network traffic packet analysis tools and techniques.
    11. Forensic Suites: Encase, FTK, PRTK, Registry Viewer, Ilook, Black Bag – Apple

MSCS1204 - System & Network Security

MODULE I: **(7Hrs)**

Web Application: Protocols and standards, Hypertext Transfer Protocol (HTTP), Markup languages Hypertext Markup Language (HTML), Cascading Style Sheets (CSS), Extensible Hypertext Markup Language (XHTML), CGI scripts and clickable maps, JAVA applets, JAVA servlets, Perl. DHTML, XML, Client-side technologies, JavaScript, Server-side technologies, SQL, PHP.

MODULE II: **(7Hrs)**

Software and System Security: Control hijacking attacks – buffer overflow, integer overflow, bypassing browser memory protection, Sandboxing and Isolation, Tools and techniques for writing robust application software, Security vulnerability detection tools, and techniques – program analysis, Privilege, access control, and Operating System Security, Exploitation techniques, and Fuzzing.

MODULE III : **(7Hrs)**

Network Security & Web Security: Security Issues in TCP/IP – TCP, DNS, Routing (Topics such as basic problems of security in TCP/IP, IPsec, BGP Security, DNS Cache poisoning etc.), Network Defense tools – Firewalls, Intrusion Detection, Filtering, DNSSec, NSec3, Distributed Firewalls, Security architecture of World Wide Web, Security Architecture of Web Servers, and Web Clients, Web Application Security –Cross Site Scripting Attacks, Cross Site Request Forgery, Https, Threat Modeling, Attack Surfaces.

MODULE IV : **(10Hrs)**

Security in Mobile Platforms: Android security model, threat models, information tracking, rootkits, Threats in mobile applications, analyzer for mobile apps to discover security vulnerabilities, Viruses, spywares, and keyloggers and malware detection. Threats of Hardware Trojans and Supply Chain Security, Side Channel Analysis based Threats, and attacks. Cloud Platform and Infrastructure Security–Security Requirements of Cloud Infrastructure: Network – Virtualization – Storage – Physical and Environmental. Cloud Application: Security with respect to Access Control–Identity and Access Management, Federation, Multifactor Authentication. OWASP and SANS recommendation of Cloud Security requirements.

TEXT BOOK:

1. Principles of Computer Security: W.A. Coklin, G. White, Fourth Edition, McGraw-Hill
2. Cryptography and Network Security Principles and Practices, William Stallings, Seventh Edition, Pearson.

REFERENCE BOOK:

1. Web Technologies: TCP/IP, Web/Java Programming, and Cloud Computing Achyut S. Godbole, Tata McGraw-Hill Education, 2013

Session Plan

Topic coverage and Internal Test	***No. of Sessions*** *(in hrs.)*	***Activity*** *(lecture, tutorial, lab practice, field studies/field-trip, Workshop etc.)*	***Assignment*** *(project, assignment, field study, seminar, etc.)*	***Suggested Reading*** *(Book, Video, Online source, etc.)*
SYSTEM & NETWORK SECURITY				
Web Application: Protocols and standards, Hypertext Transfer Protocol (HTTP), Markup languages Hypertext Markup Language (HTML), Cascading Style Sheets (CSS), Extensible Hypertext Markup Language (XHTML), CGI scripts and clickable maps, JAVA applets, JAVA servlets, Perl. DHTML, XML, Client-side technologies, JavaScript, Server-side technologies, SQL, PHP.	7 Hrs.	Lecture	Assignment	W.A. Coklin, G. White William Stallings
Software and System Security: Control hijacking attacks – buffer overflow, integer overflow, bypassing browser memory	7 Hrs.	Lecture	Assignment	W.A. Coklin, G. White William Stallings

protection, Sandboxing and Isolation, Tools and techniques for writing robust application software, Security vulnerability detection tools, and techniques – program analysis, Privilege, access control, and Operating System Security, Exploitation techniques, and Fuzzing.				
Network Security & Web Security: Security Issues in TCP/IP – TCP, DNS, Routing (Topics such as basic problems of security in TCP/IP, IPsec, BGP Security, DNS Cache poisoning etc.), Network Defense tools – Firewalls, Intrusion Detection, Filtering, DNSSec, NSec3, Distributed Firewalls, Security architecture of World Wide Web, Security Architecture of Web Servers, and Web Clients, Web Application Security –Cross Site Scripting Attacks, Cross Site Request Forgery, Https, Threat Modeling, Attack Surfaces.	7 Hrs.	Lecture	Assignment	W.A. Coklin, G. White William Stallings
Security in Mobile Platforms: Android security model, threat models, information	10 Hrs.	Lecture	Assignment	W.A. Coklin, G. White William Stallings

tracking, rootkits, Threats in mobile applications, analyzer for mobile apps to discover security vulnerabilities, Viruses, spywares, and keyloggers and malware detection. Threats of Hardware Trojans and Supply Chain Security, Side Channel Analysis based Threats, and attacks.				

NETWORK SECURITY LAB

1. Configuring Windows Firewall.
2. Configuring Linux Firewall.
3. Adding users, setting permissions in windows.
   Security level, Share Level Permissions.
4. Port Security.
5. VLAN.
6. WLAN.
7. Access control List in Linux.
8. Nmap scanning tool using both Linux and Windows.
9. Installing Nessus Client on the Windows Host.
   - Connecting from the Windows client to the Linux Nessus server.
10. Installation and configuration of Linux firewall iptables.

MSCS1205- Cyber Law

MODULE I : (7Hrs)

Fundamentals of Cyber Law -Introduction on cyber space - Jurisprudence of Cyber Law - Scope of Cyber Law - Cyber law in India with special reference to Information Technology Act, 2000 (as amended) and Information Technology Act, 2008–Jurisdiction issues in Cyberspace-Theories in cyber law jurisdiction–Cybercrimes -Meaning and Types.

MODULE II : (7Hrs)

E- Governance and E–Commerce -Electronic Governance–Procedures in India - Essentials &System of Digital Signatures - The Role and Function of Certifying Authorities - Digital contracts–Validity of Electronic Contract-Types of Electronic Contract - UNCITRAL Model law on Electronic Commerce - Cryptography–Encryption and decryption–Legal Issues in E banking transactions.

MODULE III: (9Hrs)

Cyber Crimes Investigation -Investigation related issues - Issues relating to Jurisdiction in investigation and enforcement–Powers and function of Investigating Officials-Search and Confiscation-Issues in Cross Border Investigation-Coordination among nations for cybercrime investigation -Relevant provisions under Information Technology Act, Indian Evidence Act, Indian Penal Code - Cyber forensics - Case studies. Practices in CyberJurisprudence – Regional and Global - Important Case Laws in India and other countries – Need for International cooperation for cybercrime investigation and enforcement-Need for separate cyber court - cyber laws in other countries.

MODULE IV: (9Hrs)

Legal Issues and Courtroom Skills -Key legal aspects of computer crime -IT Act of 2000 and amendments–Evidentiary issues in trial of cybercrime cases - Overseas Co-operation in Cyber Terrorism prevention-Seizure of backups and data Disclosure - Selected comparative law overseas -Civil Issues and General Enforcement - Potential defamation - Intellectual Property infringements - Confidentiality Obligations -Data Preservation and Retention - Seizure of Records - Proceeds of Crime - Damages - The domain of the Instrument of Fraud - Evidential aspects of computer material - Planning operations - Admissibility - Discovery–civil and criminal - Particular Devices - Best Practice - Preparation of Material for Court - Challenges and suggested solutions -Evidential presentation and explanation - Key players in the courtroom - Role, obligation and expectations of an ‘expert witness’ –Online Arbitration–Cyber Regulation Appellate Tribunal.

TEXT BOOK:

1. Cyber law by Nandan Kamath, Fifth Edition, Universal law Publication, 01 Jan 2012
2. Intellectual property by Robert P Merges, 3Edition, Aspen Publication, 2003

REFERENCE BOOK:

1. Computers, Technology and the new internet laws by Karnika Seth, Updated Edition, Lexis nex is Publication, 01 Jan 2013.
2. Legal dimensions of cyber space by S.K.Verma, Volume 1, Ashgate Publication, 01 Jan 2001.

Session Plan

Topic coverage and Internal Test	***No. of Sessions*** *(in hrs.)*	***Activity*** *(lecture, tutorial, lab practice, field studies/field-trip, Workshop etc.)*	***Assignment*** *(project, assignment, field study, seminar, etc.)*	***Suggested Reading*** *(Book, Video, Online source, etc.)*
CYBER LAW				
Fundamentals of Cyber Law -Introduction on cyber space - Jurisprudence of Cyber Law - Scope of Cyber Law - Cyber law in India with special reference to Information Technology Act, 2000 (as amended) and Information Technology Act, 2008– Jurisdiction issues in Cyberspace-Theories in cyber law jurisdiction– Cybercrimes -Meaning and Types.	7 Hrs.	Lecture	Assignment	Nandan Kamath. Robert P Merges.

E- Governance and E–Commerce -Electronic Governance–Procedures in India - Essentials &System of Digital Signatures - The Role and Function of Certifying Authorities - Digital contracts–Validity of Electronic Contract-Types of Electronic Contract - UNCITRAL Model law on Electronic Commerce - Cryptography–Encryption and decryption–Legal Issues in E banking transactions.	7 Hrs.	Lecture	Assignment	Nandan Kamath. Robert P Merges.
Cyber Crimes Investigation - Investigation related issues - Issues relating to Jurisdiction in investigation and enforcement–Powers and function of Investigating Officials-Search and Confiscation-Issues in Cross Border Investigation-Coordination among nations for cybercrime investigation -Relevant provisions under Information Technology Act, Indian Evidence Act, Indian Penal Code - Cyber forensics - Case studies. Practices in CyberJurisprudence –	9 Hrs.	Lecture	Assignment	Nandan Kamath. Robert P Merges.

Regional and Global - Important Case Laws in India and other countries – Need for International cooperation for cybercrime investigation and enforcement-Need for separate cyber court - cyber laws in other countries.				
Legal Issues and Courtroom Skills -Key legal aspects of computer crime -IT Act of 2000 and amendments–Evidentiary issues in trial of cybercrime cases - Overseas Co-operation in Cyber Terrorism prevention-Seizure of backups and data Disclosure - Selected comparative law overseas -Civil Issues and General Enforcement - Potential defamation - Intellectual Property infringements - Confidentiality Obligations -Data Preservation and Retention - Seizure of Records - Proceeds of Crime - Damages - The domain of the Instrument of Fraud - Evidential aspects of computer material - Planning operations - Admissibility - Discovery–civil and	9 Hrs.	Lecture	Assignment	Nandan Kamath. Robert P Merges.

criminal - Particular Devices - Best Practice - Preparation of Material for Court - Challenges and suggested solutions - Evidential presentation and explanation - Key players in the courtroom - Role, obligation and expectations of an 'expert witness' –Online Arbitration– Cyber Regulation Appellate Tribunal.				

MSCS2101- Mobile Security Analysis

MODULE I: (7Hrs)

Mobile Issues and Development Strategies–Physical Security–Strong authentication with poor keyboards–Safe browsing environment–Secure Operating Systems–Application Isolation–Virus, Worms, Trojans, Spyware and malware - Insecure Device drivers.

MODULE II : (7Hrs)

Android Security -Developing and debugging on android–Androids Securable IPC mechanisms–Androids Security Model–Android Permissions Review–Content Providers–Mass storage - Android Security tools. **ioS Security**- ioS security overview-pairing, back up, configuration, introducing app security, blocking access, keybags & keychains, Sandboxing, Encrypting Devices, Organizational controls. Mobile device Management.

MODULE III : (7Hrs)

Vulnerabilities, Threats of Mobile Devices and Countermeasures- Understanding Attack vectors, Overview of various Mobile Malwares, Network Attacks, Mobile malware defenses: Advantages and disadvantages, protect against Mobile Malware, protect against identity theft, protect against Mobile DoS (Denial of Service Attacks), Protect against Bluetooth attacks.

MODULE IV : (7Hrs)

Legal Issues and Courtroom Skills -Mobile Security Penetration Testing tools – Mobile platform attack tools and utilities – browser extensions– networking tools – Web application tools. Mobile malware – Important post malware –Threat Scenarios – mitigating mobile malware – For developers and platform vendors.

TEXT BOOK:

1. Mobile Application Security by Himanshu Dwivedi,1st Edition, McGraw-Hill Education, February 5,2010.
2. Wireless and Mobile Device Security by Jim Doherty, 1st Edition, Jones and Barlett Publication, 2014
3. Learning iOS security, Allister Banks, Charles S Edge, packt Open sorce.

REFERENCE BOOK:

1. Mobile Security: How to Secure, Privatize, and Recover your devices by Timothy Speed, Darla Nykamp, MaryHeiser, Joseph Anderson, Jaya Nampalli, reprint edition, Packt Publication, 2013
2. Mobile Device Security: A comprehensive guide to securing your Information in a Moving World by Stephen Fried, illustrated edition, Taylor & Francis Publication, 2010

SEMESTER-III LABORATORY

SECURITY ANALYSIS AND REPORTING LAB

1. Study various methods for Taping into the wire.
2. Study the steps for installing Wireshark, the packet-sniffing tool for performing Network analysis.
3. Study of working with captured packets.
4. Study of advanced Wireshark features.
5. Study of security packet analysis.
6. Study of Operating System Fingerprinting.

Session Plan

Topic coverage and Internal Test	***No. of Sessions*** *(in hrs.)*	***Activity*** *(lecture, tutorial, lab practice, field studies/field-trip, Workshop etc.)*	***Assignment*** *(project, assignment, field study, seminar, etc.)*	***Suggested Reading*** *(Book, Video, Online source, etc.)*
MOBILE SECURITY ANALYSIS				
Mobile Issues and Development Strategies– Physical Security–Strong authentication with poor keyboards–Safe browsing environment–Secure Operating Systems–Application Isolation–Virus, Worms, Trojans, Spyware and malware - Insecure Device drivers.	7 Hrs.	Lecture	Assignment	Himanshu Dwivedi. Jim Doherty.
Android Security - Developing and debugging on android–Androids Securable IPC	7 Hrs.	Lecture	Assignment	Himanshu Dwivedi. Jim Doherty.

mechanisms–Androids Security Model–Android Permissions Review–Content Providers–Mass storage - Android Security tools. **ioS Security**- ioS security overview-pairing, back up, configuration, introducing app security, blocking access, keybags & keychains, Sandboxing, Encrypting Devices, Organizational controls. Mobile device Management.				Allister, Charles.
Vulnerabilities, Threats of Mobile Devices and Countermeasures- Understanding Attack vectors, Overview of various Mobile Malwares, Network Attacks, Mobile malware defenses: Advantages and disadvantages, protect against Mobile Malware, protect against identity theft, protect against Mobile DoS (Denial of Service Attacks), Protect against Bluetooth attacks.	7 Hrs.	Lecture	Assignment	Himanshu Dwivedi. Jim Doherty.
Legal Issues and Courtroom Skills - Mobile Security Penetration Testing tools – Mobile platform attack tools and utilities – browser extensions– networking tools – Web	7 Hrs.	Lecture	Assignment	Himanshu Dwivedi. Jim Doherty.

application tools. Mobile malware – Important post malware –Threat Scenarios – mitigating mobile malware – For developers and platform vendors.				

MSCS2102- IT Governance, Risk And Compliance

MODULE I: (7Hrs)

Governance, Risk & Compliance GRC–Definitions–Governance, Risk, Compliance, Risk Threshold, Risk Modeling, Risk Appetite, Governance Standards. Best Practices for IT Governance–ITIL - ISO/IEC 27001 - Control Objectives of Information and Related Technology (COBIT) – The Information Security Management Maturity Model - Capability Maturity Model – latest standards and compliance technologies.

MODULE II: (7Hrs)

Information Security Governance -Effective Information Security Governance - Importance of Information Security Governance - Outcomes of Information Security Governance - Strategic alignment – Risk Management - Performance Measurement - Information System Strategy - Strategic Planning - Steering Committee- Policies and Procedures.

MODULE III : (9Hrs)

Information Security Management Practices-Personnel Management - Financial Management–Quality Management - Information Security Management - Performance Optimization - Roles and Responsibilities - Auditing IT Governance Structure - Evaluation Criteria & Benchmark - Assessment Tools -Case Study Analysis - Risk Management framework–COSO - The Internal environment - Objective Setting -Event Identification - Risk assessment - Risk Response - Control activities - Information & communication–Monitoring–NIST - Risk Assessment - Risk Mitigation - Evaluation & Assessment - Case Study Analysis.

MODULE IV: (9Hrs)

Compliance–Introduction-Information Technology and security - Evolution of Information systems -Roles and responsibilities - Audit, Assessment and review - The Role of the Compliance Officer - The duties and responsibilities of the compliance officer and the function of compliance - Compliance officer activities - The requirements of a Compliance Officer - Drafting compliance reports – Designing an Internal Compliance System -Regulatory principles–Issues - Developing high-level compliance policies - Defining responsibility for compliance- The compliance function - Specific internal compliance control issues–Information System Audit - Scope of System Audit - Audit Planning - Audit Manual - Audit check lists - Audit Reports - Best Practices for IT compliance and Regulatory Requirements.

TEXT BOOK:

1. Information Security Governance: Guidance for Information Security Managers by W. KragBrotby,1st Edition, Wiley Publication, 13 April 2009
2. Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition by W. Krag Brot by, 2nd Edition, ISACA Publication, 01 Mar 2006

REFERENCE BOOK:

1. Security Governance Checklists: Business Operations, Security Governance, Risk Management, and
2. Enterprise Security Architecture by Fred Cohen, Large Print Edition, Fred Cohen & Associates Publication, 2005

Session Plan

Topic coverage and Internal Test	***No. of Sessions*** *(in hrs.)*	***Activity*** *(lecture, tutorial, lab practice, field studies/field-trip, Workshop etc.)*	***Assignment*** *(project, assignment, field study, seminar, etc.)*	***Suggested Reading*** *(Book, Video, Online source, etc.)*
IT GOVERNANCE, RISK AND COMPLIANCE (MCSDFT-312)				
Governance, Risk & Compliance GRC–Definitions–Governance, Risk, Compliance, Risk Threshold, Risk Modeling, Risk Appetite, Governance Standards. Best Practices for IT Governance–ITIL - ISO/IEC 27001 - Control Objectives of Information and Related Technology (COBIT) – The Information Security Management Maturity Model - Capability Maturity Model – latest standards and compliance technologies.	7 Hrs.	Lecture	Assignment	W. KragBrotby. W. Krag Brot.
Information Security Governance -Effective	7 Hrs.	Lecture	Assignment	W. KragBrotby.

Information Security Governance - Importance of Information Security Governance - Outcomes of Information Security Governance - Strategic alignment – Risk Management - Performance Measurement - Information System Strategy - Strategic Planning - Steering Committee- Policies and Procedures.				W. Krag Brot.
Information Security Management Practices- Personnel Management - Financial Management– Quality Management -	9 Hrs.	Lecture	Assignment	W. KragBrotby. W. Krag Brot.
Compliance– Introduction- Information Technology and security - Evolution of Information systems - Roles and responsibilities - Audit, Assessment and review - The Role of the Compliance Officer - The duties and responsibilities of the compliance officer and the function of compliance - Compliance officer activities - The requirements of a Compliance Officer - Drafting compliance reports – Designing an Internal Compliance	9 Hrs.	Lecture	Assignment	W. KragBrotby. W. Krag Brot.

System -Regulatory principles–Issues - Developing high-level compliance policies - Defining responsibility for compliance- The compliance function - Specific internal compliance control issues–Information System Audit - Scope of System Audit - Audit Planning - Audit Manual - Audit check lists - Audit Reports - Best Practices for IT compliance and Regulatory Requirements.				

MSCS2103- Business Continuity Planning and Disaster Recovery

MODULE I : (7Hrs)

Introduction -Introduction to Business Continuity Management (BCM) and Disaster Recovery (DR) -Terms and definitions - BCM principles - BCM lifecycle - (BCM program management, Understanding the organization - Determining business continuity strategy, Developing and implementing a BCM response, BCM exercising, Maintaining and reviewing BCM arrangements, Embedding BCM in the organization's culture)- BCM in business: Benefits and consequence - Contemporary landscape: Trends and directions.

MODULE II: (9Hrs)

Business Impact Analysis -BCM and DR–The relationship with Risk Management - Risk Management concepts and framework - Concepts of threat, vulnerabilities and hazard - Risk Management process - Risk assessment, risk control options analysis, risk control implementation, risk control decision, and risk reporting -Business Impact Analysis (BIA) concept, benefits and responsibilities - BIA methodology - Assessment of financial and operational impacts, identification of critical IT systems and applications, identifications of recovery requirements and BIA reporting - Relationship between BIA and Risk Management.

MODULE III: (8Hrs)

Business Continuity Strategy and Business Continuity Plan (BCP) Development -Business continuity strategy development framework - Cost-benefit assessment - Site assessment and selection - Selection of recovery options - Strategy considerations and selection - Linking strategy to plan - Coordinating with External Agencies -Business continuity plan contents - Information Systems aspects of BCP - Crisis Management - Emergency response plan and crisis communication plan - Awareness, training and communication - Plan activation - Business Continuity Planning Tools.

MODULE IV: (7Hrs)

Business Continuity Plan Testing and Maintenance -Test plan framework - Types of testing – Business Continuity Plan Testing - Plan maintenance requirements and parameters - Change management and control -Business Continuity Plan Audits. Disaster Recovery – Definitions - Backup and recovery - Threat and risk assessment - Site assessment and selection - Disaster Recovery Roadmap - Disaster Recovery Plan (DRP)preparation - Vendor selection and implementation - Difference between BCP and DRP - Systems and communication security during recovery and repair.

TEXT BOOK:

1. Business Continuity Planning: A Step-by-Step Guide with Planning Forms on CD-ROM by Kenneth L.Flumer, 3rd edition, Rothstein Associates Publication, 04 Oct 2004.
2. A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance by Julia Graham, David Kaye and Philip Jan Rothstein, Illustrated edition, Rothstein Associates Publication, 31 Jan2006

REFERENCE BOOK:

1. 4.Business Continuity Planning–Protecting Your Organization's Life by Ken Doughty, Illustrated edition, Taylor & Francis Publication, 2000
2. CISSP All-in-One Exam Guide by Shon Harris and Fernando Maymi, 7Edition, McGraw-Hill Education, 1 June 2016.

Session Plan

Topic coverage and Internal Test	***No. of Sessions*** *(in hrs.)*	***Activity*** *(lecture, tutorial, lab practice, field studies/field-trip, Workshop etc.)*	***Assignment*** *(project, assignment, field study, seminar, etc.)*	***Suggested Reading*** *(Book, Video, Online source, etc.)*
BUSINESS CONTINUITY PLANNING (BCP) AND DISASTER RECOVERY (DR)				
Introduction - Introduction to Business Continuity Management (BCM) and Disaster Recovery (DR) -Terms and definitions - BCM principles - BCM lifecycle - (BCM program management, Understanding the organization - Determining business continuity strategy, Developing and implementing a BCM response, BCM	7 Hrs.	Lecture	Assignment	Kenneth L.Flumer. Julia Graham, David Kaye.

exercising, Maintaining and reviewing BCM arrangements, Embedding BCM in the organization's culture)- BCM in business: Benefits and consequence - Contemporary landscape: Trends and directions.				
Business Impact Analysis -BCM and DR– The relationship with Risk Management - Risk Management concepts and framework - Concepts of threat, vulnerabilities and hazard - Risk Management process - Risk assessment, risk control options analysis, risk control implementation, risk control decision, and risk reporting -Business Impact Analysis (BIA) concept, benefits and responsibilities - BIA methodology - Assessment of financial and operational impacts, identification of critical IT systems and applications, identifications of recovery requirements and BIA reporting - Relationship between BIA and Risk Management.	9 Hrs.	Lecture	Assignment	Kenneth L.Flumer. Julia Graham, David Kaye.
Business Continuity Strategy and Business	8 Hrs.	Lecture	Assignment	Kenneth L.Flumer.

Continuity Plan (BCP) Development -Business continuity strategy development framework - Cost-benefit assessment - Site assessment and selection - Selection of recovery options - Strategy considerations and selection - Linking strategy to plan - Coordinating with External Agencies - Business continuity plan contents - Information Systems aspects of BCP - Crisis Management - Emergency response plan and crisis communication plan - Awareness, training and communication - Plan activation - Business Continuity Planning Tools.				Julia Graham, David Kaye.
Business Continuity Plan Testing and Maintenance -Test plan framework - Types of testing – Business Continuity Plan Testing - Plan maintenance requirements and parameters - Change management and control - Business Continuity Plan Audits. Disaster Recovery	7 Hrs.	Lecture	Assignment	Kenneth L.Flumer. Julia Graham, David Kaye.

MSCS2105 - Penetration Testing & Vulnerability Assessment

MODULE I: (7Hrs)

OWASP: Introduction to web applications security, threats and OWASP principles, introduction to secure design, web server: introduction a secure setup of apache, firewalling a server Browser: general concepts, functionalities, browsers war, configuration (HTTP-cookies, contents, scripting etc. attack to browsers, and users tracking/profiling (third party cookies, super cookies, XSS, CSFR, Command Injection), browser security (add-ons, plugins, same-origin policy etc.) & secure browsing.

MODULE II : (7Hrs)

OWASP Privacy preserving: attacks to privacy, (spyware & backdoors, browser, email etc.) Tracking techniques: (HTTP cookies, third party cookies, browser fingerprinting, CSP) Advanced browser configuration, anonymity and onion routing (Tor). Internet E-mail: Architecture and infrastructure, functions, agents and standards, MIME & PGP, phishing, spamming & spoofing, DKIM, SPF, introduction to email forensics.

MODULE III : (7Hrs)

Introduction to Ethical Hacking Terminology-Five stages of hacking-Vulnerability Research-Legal implication of hacking Impact of hacking. Foot printing & Social engineering.

Information gathering methodologies- Competitive Intelligence- DNS Enumerations- Social Engineering attacks. Scanning & Enumeration Port Scanning-Network Scanning- Vulnerability Scanning- NMAP scanning tool- OS Fingerprinting Enumeration. System Hacking Password.

MODULE IV: (7Hrs)

Sniffers & SQL Injection Active and passive sniffing- ARP Poisoning- Session Hijacking-DNS Spoofing- Conduct SQL Injection attack - Countermeasures. cracking techniques- Key loggers- Escalating privileges- Hiding Files-Steganography technologies- Countermeasures.

TEXT BOOK:

1. Kimberly Graves, “CEH: Official Certified Ethical Hacker Review Guide”, Wiley Publishing Inc., 2007.ISBN: 978-0-7821-4437-6.

REFERENCE BOOK:

1. Shakeel Ali & TediHeriyanto, “Backtrack -4: Assuring security by penetration testing”, PACKT Publishing., 2011. ISBN: 978-1-849513-94-4.

Session Plan

Topic coverage and Internal Test	***No. of Sessions*** *(in hrs.)*	***Activity*** *(lecture, tutorial, lab practice, field studies/field-trip, Workshop etc.)*	***Assignment*** *(project, assignment, field study, seminar, etc.)*	***Suggested Reading*** *(Book, Video, Online source, etc.)*
Penetration Testing & Vulnerability assessment				
OWASP: Introduction to web applications security, threats and OWASP principles, introduction to secure design, web server: introduction a secure setup of apache, firewalling a server Browser: general concepts, functionalities, browsers war, configuration (HTTP-cookies, contents, scripting etc. attack to browsers, and users tracking/profiling (third party cookies, super cookies, XSS, CSFR, Command Injection), browser security (add-ons, plugins, same-origin policy etc.) & secure browsing.	7 Hrs.	Lecture	Assignment	
OWASP Privacy preserving: attacks to privacy, (spyware & backdoors, browser, email etc.) Tracking techniques: (HTTP cookies, third	7 Hrs.	Lecture	Assignment	Kimberly Graves. Shakeel Ali & TediHeriyanto.

party cookies, browser fingerprinting, CSP) Advanced browser configuration, anonymity and onion routing (Tor). Internet E-mail: Architecture and infrastructure, functions, agents and standards, MIME & PGP, phishing, spamming & spoofing, DKIM, SPF, introduction to email forensics.				
Introduction to Ethical Hacking Terminology- Five stages of hacking- Vulnerability Research- Legal implication of hacking Impact of hacking. Foot printing & Social engineering. **Information gathering methodologies-** Competitive Intelligence- DNS Enumerations- Social Engineering attacks. Scanning & Enumeration Port Scanning-Network Scanning- Vulnerability Scanning- NMAP scanning tool- OS Fingerprinting Enumeration. System Hacking Password.	7 Hrs.	Lecture	Assignment	Kimberly Graves Shakeel Ali & TediHeriyanto
Sniffers & SQL Injection Active and passive sniffing- ARP Poisoning- Session Hijacking- DNS	7 Hrs.	Lecture	Assignment	Kimberly Graves Shakeel Ali & TediHeriyanto

Spoofing- Conduct SQL Injection attack - Countermeasures. cracking techniques- Key loggers- Escalating privileges- Hiding Files- Steganography technologies- Countermeasures.				

ETHICAL HACKING LAB

1. To learn about hacking tools and skills.
2. To study about Footprinting and Reconnaissance.
3. To study about Fingerprinting.
4. To study about system Hacking.
5. To study about Wireless Hacking.
6. To learn & study about Sniffing & their tools.

MSCS2106-Digital Frauds

MODULE I: (7Hrs)

Fundamentals of Frauds- Definition of fraud, fraud risk management, fraud taxonomy, fraudulent behavior, red flags.

MODULE II: (7Hrs)

Banking Frauds–Authentication Management, Payment Fraud, Fraud Consulting and Services, Card &Emerging Payments Fraud, Contact Center Fraud Prevention, Cheque Fraud, Internal Threats. Corporate Frauds –What is Corporate Frauds – Services – Solutions.

MODULE III : (7Hrs)

Financial Frauds - Financial Inclusions and mobile financial Services, regulating for financial inclusions, Agent network issues, Telecommunication access network issues, Account to account interoperability issues, Customer data and risk based financial issues, Consumer Protection, Collaboration among financial, telecommunications and competition authorities.

MODULE IV: (10Hrs)

Frauds in IT and Telecom-IT Frauds: Theft of Proprietary Information, Insider abuse of internet access, system penetration, unauthorized access to information, laptop/mobile theft, financial fraud, misuse of public web application, virus, abuse of wireless network– Countermeasures–Telecom Frauds - Organizational or Non-Technical Fraud: involving Administration services, processes - Human Fraud - Insider Fraud - Call-sell Fraud - Facilitation Fraud - Creeping Fraud - Chaining Fraud - Calling-Card Fraud - Phantom Account -Partnership Fraud - Process Fraud–Ghosting - Abuse of test or emergency lines or accounts – Unauthorized Feature/Service Activation-Accounting - Dealer or Reseller Fraud - Subscription Fraud - Roaming Subscription Fraud - Premium-Rate Services Fraud- Illustrative Cases - Technical Fraud: Network Systems, Billing Systems –Cloning – Tumbling - Voice-mail Hacking - PBX Hacking - SIM Stuffing- Clip-on Fraud - Line Tapping - War Dialing - Handset Fraud – Fixed Network Fraud – Mobile Network Fraud – Frauds in 2G, 3G and 4G Frauds.

TEXT BOOK:

1. Managing the risk of fraud and misconduct by Richard H Girgenti, and Timothy P Hedley, first edition, Mc-Graw Hill Education Publication, 09 Mar 2011.
2. Detecting Accounting Fraud: Analysis and Ethics by Cecil W Jackson, 1 Edition, Pearson Education Publication, 26 Jan 2014.

REFERENCE BOOK:

1. Anatomy of a fraud investigation by Stephen Pedeault, 1Edition, John Wiley & Sons Publication, 2010.
2. Telecom and Network Security: Toll Fraud and Telabuse update by Jan Wilson, 2nd Edition, Telecommunications reports International Publication, 22 April 2010.

Session Plan

Topic coverage and Internal Test	***No. of Sessions*** *(in hrs.)*	***Activity*** *(lecture, tutorial, lab practice, field studies/field-trip, Workshop etc.)*	***Assignment*** *(project, assignment, field study, seminar, etc.)*	***Suggested Reading*** *(Book, Video, Online source, etc.)*
DIGITAL FRAUDS (MCSDFT-315)				
Fundamentals of Frauds- Definition of fraud, fraud risk management, fraud taxonomy, fraudulent behavior, red flags.	7 Hrs.	Lecture	Assignment	Richard H Girgenti, and Timothy P Hedley. Cecil W Jackson.
Banking Frauds– Authentication Management, Payment Fraud, Fraud Consulting and Services, Card &Emerging Payments Fraud, Contact Center Fraud Prevention, Cheque Fraud, Internal Threats. Corporate Frauds –What is Corporate Frauds – Services – Solutions.	7 Hrs.	Lecture	Assignment	Richard H Girgenti, and Timothy P Hedley. Cecil W Jackson.
Financial Frauds - Financial Inclusions and mobile financial Services, regulating for financial inclusions, Agent network issues, Telecommunication access network issues, Account to account	7 Hrs.	Lecture	Assignment	Richard H Girgenti, and Timothy P Hedley. Cecil W Jackson.

interoperability issues, Customer data and risk based financial issues, Consumer Protection, Collaboration among financial, telecommunications and competition authorities.				
Frauds in IT and Telecom-IT Frauds: Theft of Proprietary Information, Insider abuse of internet access, system penetration, unauthorized access to information, laptop/mobile theft, financial fraud, misuse of public web application, virus, abuse of wireless network– Countermeasures– Telecom Frauds - Organizational or Non-Technical Fraud: involving Administration services, processes - Human Fraud - Insider Fraud - Call-sell Fraud - Facilitation Fraud - Creeping Fraud - Chaining Fraud - Calling-Card Fraud - Phantom Account -Partnership Fraud - Process Fraud–Ghosting - Abuse of test or emergency lines or accounts – Unauthorized Feature/Service Activation-Accounting -	10 Hrs.	Lecture	Assignment	Richard H Girgenti, and Timothy P Hedley. Cecil W Jackson.

Dealer or Reseller Fraud - Subscription Fraud - Roaming Subscription Fraud - Premium-Rate Services Fraud- Illustrative Cases - Technical Fraud: Network Systems, Billing Systems –Cloning – Tumbling - Voice-mail Hacking - PBX Hacking - SIM Stuffing- Clip-on Fraud - Line Tapping - War Dialing - Handset Fraud – Fixed Network Fraud – Mobile Network Fraud – Frauds in 2G, 3G and 4G Frauds.				

MSCS0301 PROJECT/DISSERTATION

Credits - 24

Every student will have to do project report in any area of this program detailed in the curriculum under the guidance of regular / guest faculty / industry experts. It should be research based to create new knowledge in any area of cyber security & Digital Forensics. The student shall submit the project report before the term end examination. Marks will be awarded (out of 24 credits) for the project/dissertation report after viva internally.

Mark Distribution:

1. Project Demo:	06
2. Project Report:	06
3. Presentation/Seminar:	06
4. Viva:	06
Total	**24**