Centurion University

Course Structure and Syllabus

of

M.Sc. Cybersecurity & Digital Forensics

School of Forensic Sciences

2019

School of Forensic Sciences

Academic Regulations

M.Sc. Cybersecurity & Digital Forensics

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

CENTURION UNIVERSITY OF TECHNOLOGY & MANAGEMENT

At: Ramachandrapur, Jatni, Odisha 752050
www.cutm.ac.in

2019

Program Objectives

Objective of the programme is to strengthen the foundations of cyber forensics at national & International level. The following are the objectives of this programme:

- To prevent or mitigate harm to—or destruction of—computer networks, applications, devices, and data. For cybersecurity strategy to succeed, it must continually evolve to keep pace with the shifting strategies and technologies used by hackers.
- The goal of computer forensics is to examine digital data with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information. It is used in both computer crime and civil proceedings.
- To identify evidence in a short time frame, and estimate the overall menace and impact of the malicious cyber-attack.
- Activity on the victim user or organization and suggest for protection against the attack.
- To emphasize the importance of technical methods in cybercrime investigation.
- To publicize information on the developments in the field of digital forensic sciences.
- To highpoint the importance of digital forensic for resolution of the modern society.
- To review the steps necessary for achieving highest excellence in digital forensic.
- To generate talented human resource, commensuration with latest requirements of information security.
- To provide a platform for students and security professionals to exchange views, chalk-out collaborative programs and work in an all-inclusive manner for the advancement of digital science.
- To train knowledge and skill of cyber forensics so that it can be applied in digital forensic lab.

Course Structure

Semester I				
Code	Course	Course Type (Lecture-Tutorial-Practice)	Credit	Prerequisite
CUTM1676	Principles of Information Security	4-0-0	4	NIL
CUTM1677	Digital Forensics	4-0-2	6	NIL
CUTM1678	Computer Networks	4-0-2	6	NIL
CUTM1679	Cyber Crime & Investigations	4-0-0	4	NIL
CUTM1680	Intellectual Property Rights	4-0-0	4	NIL
	Total Credits		**24**	NIL

Semester II				
Code	Course	Course Type (Lecture-Tutorial-Practice)	Credit	Prerequisite
CUTM1681	Number theory &Cryptography	4-0-0	4	NIL
CUTM1682	Advanced Information Security	4-0-0	4	NIL
CUTM1683	Cyber Forensics	4-0-2	6	NIL
CUTM1684	System and Network Security	4-0-2	6	NIL
CUTM1685	Cyber Law	4-0-0	4	NIL
	Total Credits		**24**	NIL

Semester III				
Code	Course	Course Type (Lecture-Tutorial-Practice)	Credit	Prerequisite
CUTM1686	Mobile Security Analysis	4-0-2	6	NIL
CUTM1687	IT Governance, Risk and Compliance	4-0-0	4	NIL
CUTM1688	Business Continuity Planning (BCP) And Disaster Recovery (Dr)	4-0-0	4	NIL

CUTM1689	Penetration Testing & Vulnerability Assessment	4-0-2	6	NIL
CUTM1690	Digital Frauds	4-0-0	4	NIL
	Total Credits		**24**	NIL

Semester IV				
Code	Course	Course Type (Lecture-Tutorial-Practice)	Credit	Prerequisite
CUTM1691	Project/Dissertation	Project	**24**	NIL

Total credit: 96

Nomenclature

Subject Name	Code	Type of course	T-P-Pj (Credit)	Prerequisite
MSc. Cybersecurity & Digital Forensics.	(MCSDF)	Theory, Practice& Project	4-2-24	"after B.Sc. degree (10+2+3 system of education) from any science subjects Core / BCA / ITM / IT / CS / Electronics / IST (in case of biology and chemistry they need to submit additional computer certificate) or B.E. / B.Tech. in IT / CS / ECE / Mechanical/ Civil / EEE / ETC (except architect) with at least 50% marks or equivalent CGPA (45% for SC/ST candidates)"

Objective

This course focusses on two aspects of Cyber Security: analysis and assessment of risk plus how to minimize it, and, how to extract and use digital information from a wide range of systems and devices. The course is structured so that all students cover the same introductory material, but then choose to specialize in either Cyber Security or Digital Forensics. Any aforesaid science graduate who requires keen interest & knowledge of IT programming languages with basic knowledge of math beyond calculus.

Learning outcome

1. They will cover basic digital forensics and network security, and also cover computer system tools and the Linux/UNIX operating system which are highly essential in cyber world.
2. Able to deal with digital evidence in a professional manner (that includes adhering to appropriate legal guidelines).
3. It will then follow either the Cyber Security or Digital Forensics pathway within the course (though each lead to the same named degree: the pathways are simply opportunities to specialize within the field).
4. In addition, all students will take a Research Methods module and complete a project module to devote them into the world of research for their future edifice and expertise.
5. Candidates after the completion of their post-graduation have lucrative openings & scopes in the emerging areas surrounding research & development in academics, nuclear power plants, corporates, Govt. organization like railway, banking & also in national as well as International grounds with good designations as Chief Information Security Officer, Forensic Computer analyst, Information Security Analyst, Digital Forensics Investigator, Digital Forensics specialist, Homeland Security Professional and many more.

Evaluation Systems

Theory + Practice			
T+P	**Components**	**% of Marks**	**Method**
Internal Exam	Internal Lab	25	Report, Work Viva.
	Internal Theory	25	Written
External Exam	External Lab	25	Lab work, Report, Viva
	External theory	25	Written Exam

Theory			
T	**Components**	**% of Marks**	**Method**
Internal Exam	1st Internal	25%	Written, Attendance, Assignments
	2nd Internal	25%	Written, Attendance, Assignments
External Exam	External theory	50%	Written

Program Outcomes

Pos: Cybersecurity masters will be able to;

POs	Outcomes
PO1	Cyber forensic knowledge: Apply knowledge of mathematics, tools, techniques various disciplines of science and basic principles of digital forensic in investigation.
PO2	Perform live hands on as well as to carry out problem analysis and data interpretation of tools analysis.
PO3	The cybercrime and digital society: Apply cognitive informed by the circumstantial knowledge to assess corporate and digital criminal laws, society, health and educational issues and the consequent responsibilities relevant to the cyber forensics
PO4	Discrete and team work: Functions affectively as an individual, and as a member or leader in assorted teams, and in multidisciplinary settings in the field of digital forensics.
PO5	Conduct digital investigations: Tracing cyber victims and help the cyber police officials in proper collection, preservation and handling of digital evidences which will aid in maintaining the integrity of digital evidences.
PO6	Understanding of professional and ethical responsibility of cyber security professionals.
PO7	Communication: Communicate effectively on various activities of digital forensics with proper understanding of scientific tools and legal terminologies.
PO8	Understand thinking of felonious mind and finding digital signatures.
PO9	Life- long learning: Recognize the need for lifelong learning in the broadest contest of challenges and recent advances in the field of cyber forensic science.
PO10	Project Management: Demonstrate knowledge & understanding of the digital forensic science and apply these to one's own work, as a member and leader in a team, to manage projects in cyber forensic science.
PO11	Use of modern techniques, tools, skills, and digital devices necessary for forensic expert or any person working in such field.
PO12	Make a robust documentation on the basis of scientific tools analysis.

Program Specific Outcomes (PSOs): (MSc Cybersecurity & Digital Forensics, SFS)
PSO1: Masters will be able to develop skill which can be applied in the jobs of Cyber Forensic Science in private and public sector.
PSO2: Masters will be able to pursue higher studies and research.
PSO3: Masters will be able to use software and technologies that can be effectively used to solve various problems encountered during digital investigations.

Mapping PSOs with POs (Scale of High, Medium and Low):

	PO1	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**PO11**	**PO12**
PSO1	H	H	H	H	H	M	L	L	H	M	H	H
PSO2	H	H	H	M	H	H	H	M	H	H	H	M
PSO3	H	H	M	H	M	M	M	H	L	H	H	H

Course Syllabus

PRINCIPLES OF INFORMATION SECURITY

Code-CUTM1676

Course Objectives

- The objective of this course is to focus on the models, tools, and techniques for enforcement of security.
- Students will learn security from multiple perspectives.

Learning Outcomes

- Will gain familiarity with computer network, defences against them, and forensics to investigate the aftermath.
- Develop a basic understanding of Risk assessment
- Develop an understanding of security policies as well as protocols to implement such policies

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.

DIGITAL FORENSICS

Code-CUTM1677

Course Objectives
• This course focuses on two aspects of Cyber Security: analysis and assessment of risk plus how to minimize it, and, how to extract and use digital information from a wide range of systems and devices. • The course is structured so that all students cover the same introductory material, but then choose to specialize in either Cyber Security or Digital Forensics. • Any aforesaid science graduate who requires keen interest & knowledge of IT programming languages with basic knowledge of math beyond calculus.

Learning Outcomes

- explain the origins of forensic science
- explain the difference between scientific conclusions and legal decision-making
- explain the role of digital forensics and the relationship of digital forensics to traditional forensic science, traditional science and the appropriate use of scientific methods
- outline a range of situations where digital forensics may be applicable
- identify and explain at least three current issues in the practice of digital forensic investigations.

Course Syllabus

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:

- Computer Forensics: Cyber Criminals, Laws and Evidence by Marie-Helen Maras,1stedition, Jones and Bartlett Publishers, 1 February 2011
- Computer Forensics, Computer Crime Scene Investigation by John. R. Vacca, 2nd Edition, Charles River Media Publication, 15 June 2002
- 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:

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

SEMESTER-1 (LABORATORY/PRACTICES)

DIGITAL FORENSICS LAB-1

Code-CUTM1677

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

   Basic Searches, Deleted partition/ Volume Analysis, File hash analysis, Perfect Files Window XP system analysis.
9. Disk Management.
10. Window Forensic Techniques II and Internet / Email Analysis

    Regular expression searches, Registry analysis, Internet cache analysis, Email and email header analysis. USB store analysis, Windows 7 analysis.

COMPUTER NETWORKS

Code-CUTM1678

Course Objectives

The course objectives include learning about computer network organization and implementation, obtaining a theoretical understanding of data communication and computer networks, and gaining practical experience in installation, monitoring, and troubleshooting of current LAN systems.

Learning Outcomes

- explain the concepts of confidentiality, availability, and integrity (CIA) in context of Information Assurance; articulate the threats to CIA and be able to analyse a given architecture, discern vulnerabilities, and recommend physical, logical, or administrative controls to mitigate the threat; (Cybersecurity Fundamentals—Theory)
- demonstrate expertise in configuring host and network level technical security controls, to include host firewalls, user access controls, host logging, network filtering, intrusion detection, and prevention and encryption at all levels; (Managing Security—Applied)
- describe the hardware, software, and services that comprise an enterprise network, and be able to articulate how these components integrate to form a network solution; (Network Integration—Theory)
- Explain key networking protocols, and their hierarchical relationship in the context of a conceptual model, such as the OSI and TCP/IP framework; be able to articulate the low-level data communications and subsequent abstractions that allow networked hosts and applications to communicate across the internet; (Networking Protocols—Theory)
- Build multiple host and network architectures, given business requirements and constraints; student will configure operating systems, network specific services, routing, switching, and remote access solutions; (Networking—Applied)

Course Syllabus

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:

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

Reference Book:

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

COMPUTER NETWORK LAB

Code-CUTM1678

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)/ Subneting.
6. Routing (Static / Dynamic)- RIP,OSPF.
7. Transfer files beetween system 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.

CYBER CRIME & INVESTIGATIONS

Code-CUTM1679

Course Objectives

This course focusses on two aspects of Cyber Security: analysis and assessment of risk plus how to minimize it, and, how to extract and use digital information from a wide range of systems and devices. The course is structured so that all students cover the same introductory material, but then choose to specialize in either Cyber Security or Digital Forensics. Any aforesaid science graduate who requires keen interest & knowledge of IT programming languages with basic knowledge of math beyond calculus.

Learning Outcomes

- Discuss data and identify data sources
- Describe and discuss digital evidence
- Compare and contrast the differences between digital evidence and traditional evidence
- Discuss the ways in which digital evidence is authenticated
- Describe and critique digital forensics process models
- Critically evaluate standards and good practices for digital evidence and digital forensics

Course Syllabus

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:

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

REFERRENCE BOOK:

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

INTELECTUAL PROPERTY RIGHTS

Code-CUTM1680

Course Objectives

The main objective of the IPR is to make the students aware of their rights for the protection of their invention done in their project work. The students will get a basic idea about registration in India and abroad of their invention, designs, thesis written/developed by them during their project work and for this they must have knowledge of patents, copy right, trademarks, designs.

Learning Outcomes

- Once the students complete their syllabus and assessment, they will develop the basic knowledge and awareness of acquiring the patent and copyright for their innovative works.
- They will also get an idea about plagiarism while writing any article, blog, research or review paper and learn how to avoid it.

Course Syllabus

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:

- Law relating to patents, trademarks, copyright, design and geographical indications by Dr. B.L. Wadehra, 5th edition, Universal law Publication, 2012.

Law of Intellectual Property by Dr. S.R. Myneni, 6Edition, Asia Law House Publication, 01 Jan 2013.

REFERRENCE BOOK:

- International Property by David I. Bainbridge,9th Edition, Pearson Education Publication, 24 May 2012.

Intellectual Property, Patents, Copyright, trademarks and allied rights by W.R. Cornish, D Llewelyn,6th Edition, sweet and Maxwell Publication, 18 June 2007.

Semester II

NUMBER THEORY & CRYPTOGRAPHY

Code-CUTM1681

Course Objectives

Covers fundamental algorithms for integer arithmetic, greatest common divisor calculation, modular arithmetic, and other number theoretic computations. Algorithms are derived, implemented and analysed for primality testing and integer factorization. Applications to cryptography are explored including symmetric and public-key cryptosystems. A cryptosystem will be implemented and methods of attack investigated. To be able to implement and analyse algorithms for integer factorization and primality testing. To be able to use a system like Maple to explore concepts and theorems from number theory. To understand fundamental algorithms from symmetric key and public key cryptography.

Learning Outcomes

- To understand fundamental number theoretic algorithms such as the Euclidean algorithm, the Chinese Remainder algorithm, binary powering, and algorithms for integer arithmetic.
- To understand fundamental algorithms for symmetric key and public key cryptography.
- To understand the number theoretic foundations of modern cryptography and the principles behind their security.
- To implement and analyze cryptographic and number theoretic algorithms.
- To be able to use Maple to explore mathematical concepts and theorems.

Course Syllabus

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:

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

REFERENCE BOOK:

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

ADVANCED INFORMATION SECURITY

Code-CUTM1682

Course Objectives

- The objective of this course is to focus on the models, tools, and techniques for enforcement of security.
- Students will learn security from multiple perspectives.

Learning Outcomes

- Will gain familiarity with computer network, defences against them, and forensics to investigate the aftermath.
- Develop a basic understanding of Risk assessment
- Develop an understanding of security policies as well as protocols to implement such policies

Course Syllabus

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:

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

Cryptography and Network Security by Dr. William Stallings, 6th Edition, Pearson Education Publication, 01 Jan 2013.

REFERENCE BOOK:

- The CISSP Prep Guide: Gold Edition by Ronald L. Krutz, Russel Dean Vines, Gold Edition, Wiley Publication, 31 Oct 2002.

Certified Information Systems Security Professional, Study Guide by Ed Tittle, Mike Chapple, James Michael Stewart, 6th Edition, Sybex Publication, 06 July 2012.

CYBER FORENSICS

Code-CUTM1683

Course Objective

The aim of this course is to equip you with the knowledge and techniques to computer forensics practices and evidence analysis. It prepares you to use various forensic investigation approaches and tools necessary to start a computer forensics investigation. It also aims at increasing the knowledge and understanding in cyber security and ethical hacking.

Learning Outcomes

Having studied this course, you are expected to be able to:

- Define computer forensics.
- Identify the process in taking digital evidence.
- Describe how to conduct an investigation using methods of memory, operating system, network and email forensics.
- Assess the different forensics tools.
- Differentiate among different types of security attacks.
- Describe the concept of ethical hacking.

Course Syllabus

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 Sleuth Kit – Portioning 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:

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

REFERENCE BOOK:

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

DIGITAL FORENSICS LAB II

Code-CUTM1683

Image Analysis and Stegnography

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

SYSTEM & NETWORK SECURITY

Code-CUTM1684

Course Objectives

The course objectives include learning about computer network organization and implementation, obtaining a theoretical understanding of data communication and computer networks, and gaining practical experience in installation, monitoring, and troubleshooting of current LAN systems.

Learning Outcomes

- Able to understand the concepts of confidentiality, availability, and integrity (CIA) in context of Information Assurance.
- Articulate the threats to CIA and be able to analyze a given architecture.
- Discern vulnerabilities.

- Recommend physical, logical, or administrative controls to mitigate the threat; (Cybersecurity Fundamentals—Theory)

Course Syllabus

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:

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

REFERENCE BOOK:

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

NETWORK SECURITY LAB

Code-CUTM1684

1. Configuring Window 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 Window Host.
10. Connecting from the Windows client to the Linux Nessus server.
11. Installing and configuration of Linux firewall iptables.

CYBER LAW

Code-CUTM1685

Course Objectives

The Objectives of This Course Is to Enable Learner to Understand, Explore, And Acquire A Critical Understanding Cyber Law. Develop Competencies for Dealing with Frauds and Deceptions (Confidence Tricks, Scams) And Other Cyber Crimes for Example, Child Pornography Etc. That Are Taking Place Via the Internet.

Learning Outcomes

- Make Learner Conversant with The Social and Intellectual Property Issues Emerging From 'Cyberspace.
- Give Learners in Depth Knowledge of Information Technology Act and Legal Frame Work Of Right to Privacy, Data Security and Data Protection.
- Make Study on Various Case Studies on Real Time Crimes.

Course Syllabus

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 Cyber Jurisprudence – 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:

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

REFERENCE BOOK:

- Computers, Technology and the new internet laws by Karnika Seth, Updated Edition, Lexis nex is Publication, 01 Jan 2013.

Legal dimensions of cyber space by S.K.Verma, Volume 1, Ashgate Publication, 01 Jan 2001.

Semester III

MOBILE SECURITY ANALYSIS

Code-CUTM1686

Course Objectives

This course focuses on two aspects of Cyber Security: analysis and assessment of risk plus how to minimize it, and, how to extract and use digital information from a wide range of systems and devices. The course is structured so that all students cover the same introductory material, but then choose to specialize in either Cyber Security or Digital Forensics. Any aforesaid science graduate who requires keen interest & knowledge of IT programming languages with basic knowledge of math beyond calculus

Learning Outcomes

- Students learn cryptography basics (concepts, algorithms, techniques, implementation, and evaluation) for mobile apps.
- Students learn basic cryptography implementation for Android mobile security.
- Understand how to outsource application and data to a cloud in mobile computing which will leverage services provided by cloud providers.
- Deal with the various aspects arising in architecting secure complex systems, such as analysing and identifying system threats and vulnerabilities, and investigating operating systems security.

Course Syllabus

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:

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

REFERENCE BOOK:

- Mobile Security: How to Secure, Privatize, and Recover your devices by Timothy Speed, Darla Nykamp, Mary Heiser, Joseph Anderson, Jaya Nampalli, reprint edition, Packt Publication, 2013

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

Code-CUTM1686

1. Study various methods for taping into wire.
2. Sudy 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.

IT GOVERNANCE, RISK& COMPLIANCE

Code-CUTM1687

Course Objectives

This course focusses on two aspects of Cyber Security: analysis and assessment of risk plus how to minimize it, and, how to extract and use digital information from a wide range of systems and devices. The course is structured so that all students cover the same introductory material, but then choose to specialize in either Cyber Security or Digital Forensics. Any aforesaid science graduate who requires keen interest & knowledge of IT programming languages with basic knowledge of math beyond calculus.

Learning Outcomes

- Understand the concepts of governance, risk management and compliance (GRC)
- Understand the regulatory environment
- The reason for being governance is essential for effective regulatory compliance risk management
- Identify high-risk areas and compliance in your organization
- Apply Risk-based Approach
- The role of the compliance officer and his team
- Develop and implement a governance, risk management and compliance strategic plan
- Understand, define, and enhance organizational culture as it relates to performance, risk, and compliance
- Implement governance, risk management and compliance processes that are effective and efficient
- Using a risk-based audit approach

Course Syllabus

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:

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

BUSINESS CONTINUITY PLANNING & DISASTER RECOVERY

Code-CUTM1688

Course Objectives

This course focuses on two aspects of Cyber Security: analysis and assessment of risk plus how to minimize it, and, how to extract and use digital information from a wide range of systems and devices. The course is structured so that all students cover the same introductory material, but then choose to specialize in either Cyber Security or Digital Forensics. Any aforesaid science graduate who requires keen interest & knowledge of IT programming languages with basic knowledge of math beyond calculus.

Learning Outcomes

- Understand the concept of business continuity
- Learn the importance of a BCP (business continuity planning)
- See how load balancing maintains business continuity
- Discover how a DCP (Disaster recovery plan) is a second line of defence
- Learn how to choose the right failure over solution

Course Syllabus

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:

- 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.

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.

PENETRATION TESTING & VULNERABILITY ASSESSMENT

Code-CUTM1689

Course Objectives

In the end, the goal is to identify security weaknesses in a network, machine, or piece of software. Once they're caught, the people maintaining the systems or software can eliminate or reduce the weaknesses before hostile parties discover them. "Security" isn't limited to how well the machines and software stand up against penetration attempts.

Learning Outcomes

- Explain the basic principles and techniques of how attackers can enter computer systems.
- put acquired knowledge into practice by performing ethical penetration tests and hide the intrusion.
- perform analyses of data breaches and audits of information technology security.
- evaluate the strengths and weaknesses of various information technology solutions in terms of data security.
- independently present and perform demonstrations of pen-tests for educational purposes.
- evaluate the societal role of hacking from a social, ethical and economic standpoint

Course Syllabus

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-Fivestagesofhacking-VulnerabilityResearch-Legalimplication 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:

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

REFERENCE BOOK:

- Shakeel Ali &Tedi Heriyanto, "Backtrack -4: Assuring security by penetration testing", PACKT Publishing., 2011. ISBN: 978-1-849513-94-4.

ETHICAL HACKING LAB

Code-CUTM1689

1. To learn about hacking tools and skills.
2. To study about Foot printing 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.

DIGITAL FRAUDS

Code-CUTM1690

Course Objectives

To provide students with a comprehensive overview of collecting, investigating, preserving, and presenting evidence of cybercrime left in digital storage devices. To introduce topics of forensic data examination of computers and digital storage media. Investigation of computers used for wrong-doing. Understand file system basics and where hidden files may lie on the disk, as well as how to extract the data and preserve it for analysis. Understand some of the tools of e-discovery. Legal aspects must form a constant background for these types of investigations.

Learning Outcomes

- Understand the importance of a systematic procedure for investigation of data found on digital storage media that might provide evidence of wrong-doing.
- Understand the file system storage mechanisms of two common desktop operating systems (i.e., versions of Microsoft Windows and LINUX).
- Use tools for faithful preservation of data on disks for analysis. Find data that may be clear or hidden on a computer disk.

Course Syllabus

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:

- 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.
- Detecting Accounting Fraud: Analysis and Ethics by Cecil W Jackson, 1Edition, Pearson Education Publication, 26 Jan 2014.

REFERENCE BOOK:

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

Semester-IV

PROJECT/DISSERTATION

Credits - 24

very 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 cybersecurity & 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**