SANJEEV AGRAWAL GLOBAL EDUCATIONAL (SAGE) UNIVERSITY, BHOPAL

Scheme & Syllabus

for

Master of Technology (Cyber Security & Forensic)

School of Advanced Computing

Program Educational Objectives (PEOs)

PEO-1: Demonstrate skills as a cyber security professional and perform the duties with ethical and moral values.

PEO-2: To produce post graduates who can contribute in research and development in the field of cyber security and digital forensics.

PEO-3: To engage in sustainable development and demonstrate data analysis skills for effective interpretation and decision making to solve real life problems.

PEO-4: To maintain an appropriate level of awareness, knowledge and skills to minimize the occurrence and severity of information security incidents.

PEO-5: Promote Design, Research, and implementation of products and services in the field of Cyber Security and Forensicthrough strong communication and entrepreneurial skills.

Program Outcomes (POs):

PO-1: Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

PO-2: Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO-3: Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

PO-4: Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

PO-5: Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

PO-6: The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO-7: Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

PO-8: Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

PO-9: Individual and team work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO-10: Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO-11: Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO-12: Life-long learning: Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Curriculum Components

Components	Credits
Program Core (08 Courses)	28
Program Electives (Discipline Specific Electives) (04 Courses)	16
Project Based Learning (PBL)/MOOCs (04 courses)	12
Project (02 Courses)	28
Total	**84**

First Semester																
Course Code	**Course Title**	**Contact Hours Per Week**			**Credits**	**ESE Duration (Hours)**	**Theory**						**Practical**			**GT**
		L	**T**	**P**			**MSE**	**ASG**	**TA**	**ATTD**	**ESE**	**Tot**	**CE**	**ESE**	**Tot**	
MA20M101	Advanced Mathematics	3	1	-	4	3	30	05	05	10	50	100	-	-	-	100
CY20M102	Cryptography and Network Security	2	1	2	4	3	30	05	05	10	50	100	20	30	50	150
CY20M103	Digital Forensic and Cyber Crime	3	-	2	4	3	30	05	05	10	50	100	20	30	50	150
Table-1	DSE-I	3	1	-	4	3	30	05	05	10	50	100	-	-	-	100
Table-1	DSE-II	3	1	-	4	3	30	05	05	10	50	100	-	-	-	100
AI20M104	Software Lab-I	-	-	4	2	2	-						20	30	50	50
PB20M101	Project Based Learning-I	-	-	4	2	2	-						50^	50	100	100
		Total			**24**											**750**

L-Lecture, T-Tutorial, P-Practical, MSE- Mid Semester Exam, ASG- Assignment, TA- Teacher's Assessment, ATTD-Attendance, CE-Continuous Evaluation ,ESE- End Semester Exam, Tot-Total, GT-Grand Total, ^ - Two assessment by panel of Expert

Second Semester																
Course Code	**Course Title**	**Contact Hours per Week**			**Credits**	**ESE Duration (Hours)**	**Theory**						**Practical**			**GT**
		L	**T**	**P**			**MSE**	**ASG**	**TA**	**ATTD**	**ESE**	**Tot**	**CE**	**ESE**	**Tot**	
CY20M201	Data Privacy	3	1	-	4	3	30	05	05	10	50	100	-	-	-	100
CY20M202	Cyber Forensic	3	1	-	4	3	30	05	05	10	50	100				100
CY20M203	Ethical Hacking	3	-	2	4	3	30	05	05	10	50	100	20	30	50	150
Table-1	DSE-III	3	1	-	4	3	30	05	05	10	50	100	-	-	-	100
Table-1	DSE-IV	3	1	-	4	3	30	05	05	10	50	100	-	-	-	100
AI20M204	Software Lab-II	-	-	4	2	2	-				-	-	20	30	50	50
PB20M201	Project Based Learning-II	-	-	4	2	2	-				-	-	50^	50	100	100
		Total			**24**											**700**

L-Lecture, T-Tutorial, P-Practical, MSE- Mid Semester Exam, ASG- Assignment, TA- Teacher's Assessment, ATTD-Attendance, CE-Continuous Evaluation ,ESE- End Semester Exam, Tot-Total, GT-Grand Total, ^ - Two assessment by panel of Expert

Third Semester																
Course Code	**Course Title**	**Contact Hours per Week**			**Credits**	**ESE Duration (Hours)**	**Theory**						**Practical**			**G T**
		L	**T**	**P**			**MSE**	**ASG**	**TA**	**ATTD**	**ESE**	**Tot**	**CE**	**ESE**	**Tot**	
	MOOC-1	-	-	8	4	-	-	-	-	-	-	-	50	50	100	100
	MOOC-2	-	-	8	4	-	-	-	-	-	-	-	50	50	100	100
CY20M303	Dissertation Phase-I	-	-	24	12	2	-						150	150	300	300
		Total			**20**											**500**

L-Lecture, T-Tutorial, P-Practical, MSE- Mid Semester Exam, ASG- Assignment, TA- Teacher's Assessment, ATTD-Attendance, CE-Continuous Evaluation ,ESE- End Semester Exam, Tot-Total, GT-Grand Total

Fourth Semester																
Course Code	**Course Title**	**Contact Hours per Week**			**Credits**	**ESE Duration (Hours)**	**Theory**						**Practical**			**GT**
		L	**T**	**P**			**MSE**	**ASG**	**TA**	**ATTD**	**ESE**	**Tot**	**CE**	**ESE**	**Tot**	
CY20M401	Dissertation Phase-II	-	-	32	16						-	-	200	200	400	400
		Total			**16**											**400**

L-Lecture, T-Tutorial, P-Practical, MSE- Mid Semester Exam, ASG- Assignment, TA- Teacher's Assessment, ATTD-Attendance, CE-Continuous Evaluation ,ESE- End Semester Exam, Tot-Total, GT-Grand Total

Distribution of credits across all components

SEM No.	Prog. Core	Discipline Specific Electives (DSE)	Project Based Learning (PBL)/ MOOCs	Project	Total Credit
I.	14	08	02	-	**24**
II.	14	08	02	-	**24**
III.	-	-	08	12	**20**
IV.	-	-	-	16	**16**
Total	**28**	**16**	**12**	**28**	**84**

Table-1
List of Discipline Specific Electives (DSE)

SN	Course Code	DSE-I
1.	**CY20M106**	Block chain Technology
	CY20M107	Mobile and Wireless Network Security
	CY20M108	Malware Analysis and Reverse Engineering
SN	**Course Code**	**DSE-II**
2.	**CY20M109**	Intrusion Detection Systems
	CY20M110	Security Threats and Modeling
	CY20M111	IT Security- Threats and Vulnerability
SN	**Course Code**	**DSE-III**
1.	**CY20M207**	Database Security and Access Control
	CY20M208	Cyber Crime and Information Warfare
	CY20M209	Securing Coding
SN	**Course Code**	**DSE-IV**
2.	**CY20M210**	Incidence Response Management
	CY20M211	Cyber Threat Intelligence
	CY20M212	Information Security and Risk Management

SANJEEV AGRAWAL GLOBAL EDUCATIONAL (SAGE) UNIVERSITY, BHOPAL

Syllabus

for

Master of Technology (Cyber Security & Forensic)

I Semester

School of Advanced Computing

COURSE CODE	ADVANCED MATHEMATICS	TOTAL LECTURE:45 TUTORIAL:15
MA20M101		3 – 1 – 0 = 4

Course Objectives :

- To introduce students to the theoretical distributions, sampling distributions and their applications
- To introduce the students to the solution of partial differential equation
- Demonstrate an understanding to the theory and applications of linear algebra
- To extend the concept of the computer algorithms related to dimensionality reduction and feature extraction.
- To introduce the concepts of Stochastic process and Markov process transition.

UNIT	CONTENTS	HOURS
1	Probability, compound probability and discrete random variable. Binomial, Normal and Poisson's distributions, Sampling distribution, elementary concept of estimation and theory of hypothesis, recurred relations.	12
2	Solution of Partial Differential Equation (PDE) by separation of variable method, numerical solution of PDE (Laplace, Poisson's, Parabola) using finite difference methods, Elementary properties of FT, DFT, WFT, Wavelet transform, Haas transform.	12
3	Finite differences: forward, backward and central difference operators, polynomial interpolation: equally spaced and unequally spaced data; Numerical Differentiation, Numerical integration- Trapezoidal and Simpson1/3rd and 3/8th rules; Initial value problems - Taylor series method, Euler and modified Euler methods, Runge- Kutta methods.	12
4	Solution of Linear systems– Gaussian elimination method, LU factorization method, Cholesky's factorization method. Linear least-squares problems - Normal equations, QR method (or Gram Schmidt Ortho- normalization), Singular value decomposition (SVD) for linear least-squares problems, numerical rank determination via SVD, Principal Component Analysis.	12

5	Stochastic process, Markov process transition probability transition probability matrix, just and higher order Markov process, Application of Eigen value problems in Markov Process, Markov chain. Queuing system, transient and steady state, traffic intensity, distribution queuing system, concepts of queuing models (M/M/1: Infinity/ Infinity/ FC FS), (M/M/1: N/ Infinity/ FC FS), (M/M/S: Infinity/ Infinity/ FC FS)	12

Course Outcomes

At the end of the course the students should be able to:

CO 1	**Understand**[2] probability, sampling distribution and discrete random variable.
CO 2	**Understand**[2] the terms and their applications of Solution of Partial Differential Equations
CO 3	**Understand**[2] the numerical methods and their use in obtaining approximate solutions to otherwise intractable linear/non-linear system of equations and differential equations.
CO 4	**Analyse**[4] the fundamental use of matrices in the computer algorithms related to dimensionality reduction and feature extraction.
CO 5	**Implement**[6] Stochastic process, Markov process transition probability transition probability matrix and Markov process.
Text Books	• *Gupta* S C & *Kapoor* V K , (2014):**Fundamentals of Mathematical Statistics**, Delhi:Sultan Chand & Sons. • Jimmie Gilbert, (2010):**Linear Algebra And Matrix Theory**, India Elsevier. • Grewal Dr B S, (2014): **Numerical Methods in Engineering & Science: With Programs in C, C++ & MATLAB**, 10th Edition, Khanna Publishers.
Reference Books	• Rohatgi V.K., (2009): **An introduction to probability and statistics**, Second Edition, Wiley India. • Trefethen L. N. and Bau David, (1997):**Numerical Linear Algebra**, SIAM, Philadelphia.

COURSE CODE	CRYPTOGRAPHY AND NETWORK SECURITY	TOTAL LECTURE:30 TUTORIAL:15 PRACTICAL: 15
CY20M102		2 – 1–2 = 4

Course Objectives :

- To understand basics of Cryptography and Network Security.
- To learn about how to maintain the Confidentiality, Integrity and Availability of a data.
- Have a strong understanding of different cryptographic protocols and techniques and be able to use them.
- Apply methods for authentication, access control, intrusion detection and prevention.
- Indentify and mitigate software security vulnerabilities in existing systems.

UNIT	CONTENTS	HOURS
1	Introduction: Introduction to Cryptography, Security Threats, Vulnerability, Active and Passive attacks, Security services and mechanism, Conventional Encryption Model, CIA model. Math Background : Modular Arithmatic, Euclidean and Extended Euclidean algorithm, Prime numbers, Fermat and Euler's Theorem.	10
2	Classical Cryptography: Dimensions of Cryptography, Classical Cryptographic Techniques. Block Ciphers (DES, AES) : Feistal Cipher Structure, Simplifies DES, DES, Double and Triple DES, Block Cipher design Principles, AES, Modes of Operations.	10
3	Public-Key Cryptography: Principles Of Public-Key Cryptography, RSA Algorithm, Key Management, Diffie-Hellman Key Exchange, Elgamal Algorithm, Elliptic Curve Cryptography.	10
4	Hash and MAC Algorithms: Authentication Requirement, Functions, Message Authentication Code, Hash Functions, Security Of Hash Functions And Macs, MD5 Message Digest Algorithm, Secure Hash Algorithm, Digital Signatures. Key Management : Key Distribution Techniques, Kerberos	8

5	Security in Networks : Threats in networks, Network Security Controls – Architecture, Encryption, Content Integrity, Strong Authentication, Access Controls, Wireless Security, Honeypots, Traffic flow security, Firewalls – Design and Types of Firewalls, Personal Firewalls, IDS, Email Security – PGP, S/MIME	7
List of Experiments for Practical		
1	Write a Program to implement Ceaser Cipher.	
2	Write a Program to implement Affine Cipher with equation c=3x+12.	
3	Write a Program to implement Playfair Cipher with key ldrp.	
4	Write a Program to implement polyalphabetic Cipher.	
5	Write a Program to implement AutoKey Cipher.	
6	Write a Program to implement Hill Cipher. (Use any matrix but find the inverse yourself).	
7	Write a Program to implement Rail fence technique.	
8	Write a Program to implement Simple Columner Transposition technique.	
9	Write a Program to implement Advanced Columner Transposition technique.	
10	Write a Program to implement Euclidean Algorithm.	
11	Write a Program to implement implement Advanced Euclidean Algorithm.	
12	Write a Program to implement Simple RSA Algorithm with small numbers.	
Course Outcomes		
At the end of the course the students should be able to:		
CO 1	**Understand**[2] cryptography and network security concepts and application.	
CO 2	**Apply**[3] security principles to system design.	

CO 3	**Identify**[4] and investigate network security threat.
CO 4	**Analyze**[4] and design network security protocols.
CO 5	**Conduct**[6] research in network security.
Text Books	• Stallings William, (2006):**Cryptography And Network Security Principles And Practice**, IVth Edition, Pearson Education. • Mao Wenbo, (2003):**Modern Cryptography: Theory and Practice**, Prentice Hall PTR • Stallings William, (1999):**Network Security Essentials: Applications and Standards**, Ist Edition, Pearson.
Reference Books	• R. Stinson Douglas,(2005):**Cryptography: Theory and Practice**, IIIrd Edition, Chapman and Hall/CRC.

COURSE CODE	DIGITAL FORENSIC AND CYBER CRIME	TOTAL LECTURE:45 PRACTICAL: 15
CY20M103		3–0–2 = 4

Course Objectives

- To learn the process of computer forensics.
- To understand the basic digital forensics and techniques for conducting the forensic examination on different digital devices.
- To understand how to examine digital evidences such as the data acquisition, identification analysis.
- To conduct digital investigations that conform to accepted professional standards and are based on the investigative process.
- Identify and document potential security breaches of computer data that suggest violations of legal, ethical, moral, policy and/or societal standards.

UNIT	CONTENTS	HOURS
1	Introduction to Cyber Crime & Threat: Types of Cyber Crimes, Threat, Cyber security, recent threats to cyber domain, Internet, Privacy. Cyber Laws and Ethics. Cyber Security Threats Unauthorized Access, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Software Piracy.	10
2	Introduction to Digital Forensics: Use of Digital Forensics in Law Enforcement, cyber law in India. Digital Forensics Services, Benefits of Professional Forensics Methodology, Steps Taken by Digital Forensics Specialists, Types of Digital Forensics. Locard's Principal as applicable to Digital Forensics, Computing Devices, Storage Media, Potential Digital Evidence, Artifacts, Search & seizure, Forensic acquisition of digital devices, Digital evidence handling, Chain of Custody, Legal Report Writing Computing Device Forensics Hardware & software, Data Storage system, Hard Disk Geometry & Fundamentals, Disk Forensics.	10
3	Mobile Phone Forensics: Recent developments in mobile technology, Cell Phone Theory, Smart devices, Smart Operating Systems, Android, iOS, RIM OS, Windows, Mobile Phone Forensics, Logical v/s Physical extraction, Mobile phone forensics tools, SIM Forensics, Call Data Records, Smartphones.	10
4	Data Acquisition: Understanding storage formats and digital evidence, determine the best acquisition method, acquisition tools. Data Recovery Data	8

	Recovery defined, Data Backup and Recovery, the Role of Backup in Data Recovery, the Data-Recovery Solution, Hiding and Recovering Hidden Data.	
5	Current Computer Forensics Tools: Software, hardware tools, validating and testing forensics software, email investigation- investigation email crime and violations, understanding email server, email forensics tools Internet Security Systems, Firewall Security Systems, Wireless Network Security Systems. Identity Management Security Systems, Identity Theft, Biometric Security Systems.	7

Experiments: Study of various Digital forensics tools:	
1	Hard drive imaging software (FTK Imager Lite).
2	Hash calculator (Hash Calc).
3	A virtual Linux machine for Windows that includes an incident response and forensic tool suite (SIFT work station 3).
4	A digital forensics platform and graphical interface to The Sleuth Kit (Autopsy).
5	Memory analysis tool (Volatility).
6	Disk Image file (Malware Analyst's Cookbook DVD).
7	Allows viewing of Windows registry file (Access Data's Registry Viewer).
8	Cryptographic tool (Invisible Secrets).
9	Data hiding and watermarking tool (OpenSteg)

Course Outcomes

At the end of the course the students should be able to:

CO 1	**Comprehend**[2] the basics of Cyber Crime & threat Terminologies. Understand the various types of Cyber threats in different cyber domains.
CO 2	**Comprehend**[2]the basics of Digital forensics, applicability of DF for Law enforcement agencies. Cyber law in India, Types of Digital forensics technology, Digital evidence collection and handing, Computing Device Forensics Hardware & software.
CO 3	**Comprehend**[2] the Mobile Phone Forensics & recent developments, Smart phone Operating Systems, Logical v/s Physical extraction, Mobile phone forensics tools.

CO 4	**Understand**[2] Data acquisition methods, acquisition tools, Data Backup and Recovery solutions, Hiding and Recovering Hidden Data. Illustrate the methods for data recovery, evidence collection and data seizure.
CO 5	**Understand**[2] various Digital Forensics tools, validating and testing of digital evidence collected.
Text Books	• Vacca, J. R. (2005): ***Computer forensics: computer crime scene investigation*** . Hingham, MA: Charles River Media.
Reference Books	• Gogolin, G. (Ed.), (2021): ***Digital forensics explained,*** CRC Press.

COURSE CODE	DSE-I	TOTAL LECTURE:45 TUTORIAL: 15
CY20M106	BLOCKCHAIN TECHNOLOGY	3-1-0= 4

Course Objectives:

- Familiarize the functional/operational aspects of crypto currency ECOSYSTEM.
- Understand emerging abstract models for Block chain Technology.
- Identify major research challenges and technical gaps existing between theory and practice in crypto currency domain.
- The student will be able to comfortably discuss and describe the history, technology, and applications of Block chain.
- The student will be able to assess Block chain applications in a structured manner.

UNIT	CONTENTS	HOURS
1	Blockchain Data structure, Hash chain, Distributed database, Index structure, Blockchain Architecture - Hashes, Transactions, Asymmetric-Key Cryptography, Addresses and Address Derivation, Private Key	12
2	Storage, Ledgers, Blocks, Chaining Blocks. Consensus and multiparty agreements - Protocols, Proof of Work, Proof of Stake, Delegated Proof of Stake, Proof of Elapsed Time, Deposit based consensus, Proof of importance.	12
3	Federated consensus or Federated Byzantine consensus, Reputation-based mechanisms, Practical Byzantine Fault Tolerance. Blockchain implementation,	13
4	Forking - Soft Fork, Hard Forks, Cryptographic Changes and Forks, Smart contract programing, Blockchain Platforms – Cryptocurrencies (Bitcoin, Litecoin, Ethereum, Ripple), Hyperledger	13
5	Ethereum. Blockchain - Outside of Currencies, IPFS protocol and Blockchain, Blockchain Concurrency and scalability, Network models and timing assumptions.	10

Course Outcomes

At the end of the course the students should be able to:

CO 1	**Understanding**[2] of basic principles of distributed ledger technology
CO 2	**Use**[3] cryptographic primitives in Blockchain technology
CO 3	To **assess**[3] Blockchain applications in a structured manner.
CO 4	**Understand**[2] the concept of cryptocurrency.
CO5	**Understand**[2] Blockchain and its use cases.
Text Books	• Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016): ***Bitcoin and cryptocurrency technologies: a comprehensive introduction***. Princeton University Press. • Shukla S., Dhawan M., Sharma S., Venkatesan S., (2019):**Blockchain Technology: Cryptocurrency and Applications**, Oxford University Press. • Thompson Josh, (2017):**Blockchain: The Blockchain for Beginnings, Guild to Blockchain Technology and Blockchain Programming**, Create Space Independent Publishing Platform.
Reference Books	• Joseph Bonneau et al, 2015, "SoK: Research perspectives and challenges for Bitcoin and cryptocurrency", IEEE Symposium on security and Privacy. • Garay, J., Kiayias, A., & Leonardos, N. (2015, April). **The bitcoin backbone protocol: Analysis and applications**,(pp. 281-310). Springer, Berlin, Heidelberg. • R.Pass et al, 2017, "**Analysis of Blockchain protocol in Asynchronous networks**" , EUROCRYPT(eprint.iacr.org/2016/454) .

COURSE CODE	DSE-I	TOTAL LECTURE:45 TUTORIAL: 15
CY20M107	MOBILE & WIRELESS NETWORK SECURITY	3-1-0= 4

Course Objectives

- To conceptualize the wireless environment in terms of security and privacy
- To impart state-of-the-art technologies of wireless network security
- To analyze the various categories of threats, vulnerabilities, countermeasures in the area of wireless and mobile networking
- To familiarize students with the issues and technologies involved in designing a wireless system that is robust against attacks.
- To understand the security and privacy problems in the realm of wireless networks and mobile computing.

UNIT	CONTENTS	HOURS
1	Introduction to wireless technologies, Design Factors, security threats and vulnerabilities present at the different protocol layers, family of security protocols and algorithms used in the existing wireless networks (Bluetooth, Wi-Fi, WiMAX and LTE standards).	10
2	Introduction To Mobile Network Techs, Vulnerabilities Threats And Attack Entry Points. Categorization Of Attacks In Mobile Networks, Signaling Attacks. Threats And Attacks In 4g Networks- Attacks Against Security And Confidentiality, Ip-Based Attacks, Gtp-Based Attacks, Volte Sip-Based Attacks, Diameter-Based Attacks.	13
3	Emerging physical layer security in wireless communications. Class of information- Theoretic security, artificial-noise-aided security, security-oriented beam forming, security-oriented diversity, and physical-layer secret key generation techniques. Review on various wireless jammers, open challenges in wireless security.	13
4	Security in Ad Hoc Wireless Networks, Network Security Requirements, Issues andChallenges in Security Provisioning, Network Security Attacks, Key Management inAdhoc Wireless Networks, Secure Routing in Adhoc Wireless Networks.	11
5	Introduction, RFID Security and privacy, RFID chips Techniques and Protocols, RFID anti-counterfeiting, Man-in-the-middle attacks on RFID systems, Digital Signature Transponder, Combining Physics and Cryptography	13

	to Enhance Privacy in RFID Systems, Scalability Issues in Large-Scale Applications, An Efficient and Secure RFID Security Method with Ownership Transfer, Policy-based Dynamic Privacy Protection Framework leveraging Globally Mobile RFIDs, User-Centric Security for RFID based Distributed Systems, Optimizing RFID protocols for Low Information Leakage, RFID: an anti-counterfeiting tool.	

Course Outcomes

At the end of the course the students should be able to:

CO 1	Gain in-depth **knowledge**[2] on wireless and mobile network security and its relation to the new security based protocols.
CO 2	**Apply**[3] proactive and defensive measures to counter potential threats, attacks and intrusions.
CO 3	**Design**[6] secured wireless and mobile networks that optimize accessibility whilst minimizing vulnerability to security risks.
CO 4	**Impart**[3] state-of-the-art technologies and protocols of wireless network security.
CO 5	**Identify**[4] and investigate in-depth both early and contemporary threats to mobile and wireless networks security.
Text Books	• Makki, S. K., Reiher, P., Makki, K., Pissinou, N., & Makki, S. (Eds.). (2007). ***Mobile and wireless network security and privacy***. Springer Science & Business Media. • Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). **A survey on wireless security: Technical challenges, recent advances, and future trends**. *Proceedings of the IEEE*, *104*(9), 1727-1765.
Reference Books	• Kitsos, P., & Zhang, Y. (2008). ***RFID security*** (Vol. 233). Springer Science+ Business Media, LLC. • Cache, J., & Liu, V. (2007). Hacking Wireless Exposed.

COURSE CODE	DSE-I	Total Lecture:45 Tutorial:15
CY20M108	MALWARE ANALYSIS & REVERSE ENGINEERING 3 –1-0= 4	

Course Objectives

- To learn fundamentals of malware analysis which includes analysis of JIT compilers for malware detection in legitimate code.
- To explore the techniques for detecting, analyzing, reverse engineering and eradicating malware
- Employ network and system-monitoring tools to examine how malware interacts with the file system, registry, network, and other processes in a Windows environment
- Assess the threat associated with malicious documents
- Build an isolated, controlled laboratory environment for analyzing the code and behavior of malicious program.

UNIT	CONTENTS	HOURS
1	Fundamentals of Malware Analysis (MA), Reverse Engineering Malware (REM) Methodology, Brief Overview of Malware analysis lab setup and configuration, Introduction to key MA tools and techniques, Behavioral Analysis vs. Code Analysis, Resources for Reverse-Engineering Malware (REM) Understanding Malware Threats, Malware indicators, Malware Classification, Examining Clam AV Signatures, Creating Custom Clam AV Databases.	12
2	Malware Forensics Using TSK for Network and Host Discoveries, Using Microsoft Offline API to Registry Discoveries, Identifying Packers using PEiD, Registry Forensics with Reg Ripper Plu-gins:, Bypassing Poison Ivy's Locked Files, Bypassing Conficker's File System ACL Restrictions, Detecting Rogue PKI Certificates.	12
3	Malware and Kernel Debugging Opening and Attaching to Processes, Configuration of JIT Debugger for Shellcode Analysis, Controlling Program Execution, Setting and Catching Breakpoints, Debugging with Python Scripts and Py Commands, DLL Export Enumeration, Execution, and Debugging, Debugging a VMware Workstation Guest (on Windows), Debugging a Parallels Guest (on Mac OS X). Introduction to WinDbg Commands and Controls, Detecting Rootkits with Win Dbg Scripts, Kernel Debugging with IDA Pro.	13

4	Memory Forensics and Volatility Memory Dumping with MoonSols Windows Memory Toolkit, Accessing VM Memory Files Overview of Volatility, Investigating Processes in Memory Dumps, Code Injection and Extraction, Detecting and Capturing Suspicious Loaded DLLs, Finding Artifacts in Process Memory, Identifying Injected Code with Malfind and YARA.	12
5	Researching and Mapping Source Domains/IPsUsing WHOIS to Research Domains, DNS Hostname Resolution, Querying Passive DNS, Checking DNS Records, Reverse IP Search New Course Form, Creating Static Maps, Creating Interactive Maps.	11

Course Outcomes

At the end of the course the students should be able to:

CO 1	**Understand**[2] the concept of malware and reverse engineering.
CO 2	I**mplement**[6] tools and techniques of malware analysis.
CO 3	**Learn**[1] various techniques for analysis & reverse engineering
CO 4	**Use**[3] python language for development & analysis of anti-malwares.
CO 5	**Setup**[4] an environment for malware analysis & recognize common malware characteristics.
Text Books	• Sikorski, M., & Honig, A. (2012). ***Practical malware analysis: the hands-on guide to dissecting malicious software***. no starch press. • Eilam, E. (2005). Reversing, Secrets of Reverse Engineering Wiley Publishing. • Malin, C. H. (2013). ***Linux Malware Incident Response: A Practitioner's Guide to Forensic Collection and Examination of Volatile Data: An Excerpt from Malware Forensic Field Guide for Linux Systems***. Elsevier.
Reference Books	• Sikorski, M., & Honig, A. (2012). ***Practical malware analysis: the hands-on guide to dissecting malicious software***. no starch press. • Shashidhar, N., & Cooper, P. (2016, April). Teaching malware analysis: The design philosophy of a model curriculum. In *2016 4th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 119-125). IEEE. • Singh, A. (Ed.). (2009). ***Identifying malicious code through reverse engineering*** (Vol. 44). Springer Science & Business Media.

COURSE CODE	DSE-II	Total Lecture:45 Tutorial: 15
CY20M109	INTRUSION DETECTION SYSTEM	3-1-0= 4

Course Objectives

- To provide an in depth introduction to the science and art of intrusion detection.
- To understand methodologies, techniques, and tools for monitoring events in computer system or network
- To understand when, where, how, and why to apply Intrusion Detection tools and techniques in order to improve the security posture of an enterprise.
- Apply knowledge of the fundamentals and history of Intrusion Detection in order to avoid common pitfalls in the creation and evaluation of new Intrusion Detection Systems
- Analyze intrusion detection alerts and logs to distinguish attack types from false alarms

Unit	Contents	Hours
1	Understanding Intrusion Detection – Intrusion detection and prevention basics , IDSand IPS analysis schemes.	12
2	Attacks, Detection approaches –Misuse detection – anamoly detection – specification based detection – hybrid detection	12
3	Theoretical Foundations Of Detection: Taxonomy of anomaly detection system – fuzzy logic Bayes theory – Artificial Neural networks – Support vector machine – Evolutionary computation –Association rules – Clustering	12
4	Architecture And Implementation: Centralized – Distributed Cooperative Intrusion Detection, Tiered architecture	11
5	Justifying Intrusion Detection: Intrusion detection in security – Threat, Applications And Tools:Tool Selection and Acquisition Process, Bro Intrusion Detection –Prelude Intrusion Detection - Cisco Security IDS.	13

Course Outcomes

At the end of the course the students should be able to:

CO 1	**Obtain**[2] comprehensive knowledge on the subject of intrusion detection
CO 2	**Understand**[2] the state of the art of intrusion detection research

CO 3	Get a hands-on **exposure**[4] to the principles and techniques used in intrusion detection, as well as the technical challenges and fundamental limitations of intrusion detection
CO 4	**Create**[6] independent research in intrusion detection
CO 5	**Explain**[4] the fundamental concepts of Network Protocol Analysis and demonstrate the skill to capture and analyze network packets.
Text Books	• Roberto, D. P., & Mancini, L. V. (2008). **Intrusion detection system.** • Endorf Carl, Eugene Schultz and Jim Mellander, 2004, " Intrusion Detection & Prevention", Ist Edition, Tata McGraw-Hill.
Reference Books	• Anderson, Ross, 2001, Security Engineering: "A Guide to Building Dependable Distributed Systems". New York: John Wiley & Sons. pp. 387–388. ISBN 978-0-471-38922-4. • Anderson, James P, 1980, "Computer Security Threat Monitoring and Surveillance," Washing, PA, James P. Anderson Co. • Christopher Kruegel,Fredrik Valeur, Giovanni Vigna, 2005, "Intrusion Detection and Correlation Challenges and Solutions", 1st Edition, Springer.

COURSE CODE	DSE-II	Total Lecture:45 Tutorial: 15
CY20M110	SECURITY THREATS & MODELING	3 – 1-0 = 4

Course Objectives

- To understand various security threats & attacks.
- To learn various attack management techniques.
- To study different security models.
- To implement of various security protocols.
- Learn threat management by assessing, analyzing or applying models.

UNIT	CONTENTS	HOURS
1	Introduction:Security threats, its sources, Target Assets and vulnerabilities, Consequences of threats, Active/ Passive Threats, Web-threats, Network Threats, E-mail threats, Sabotage-Internal treats- Environmental threats - Threats to Server security, Insider threats, Cybercrimes, hackers and Intruders.	12
2	Attack Tree, Attack Graphs: Types of Attack Scenarios and Detection Approaches, Threat exploitation and analysis: Session Hijacking – Phishing – DNS Pharming – Tab-nabbing – Clickjacking – XSS – SQL – Command Injection – IP Spoofing, Email-Spoofing, Information Hiding (Stenography), Buffer Overflow Virology- Worms, Virus, Spam's, Ad ware, Spy ware, Trojans, Backdoors, Bots, Malware.	12
3	Security Threat Management: Risk Assessment - Forensic Analysis – Security threat correlation – Threat awareness - Vulnerability sources and assessment Vulnerability assessment tools -Threat identification - Threat Analysis – Threat Modeling - Model for Information Security Planning. Footprinting- Scanning Enumeration - basic banner grabbing, Enumerating Common Network services.	13
4	Security models:Access Control Matrix Model, Take-Grant Protection Model Secure Web Engineering Privacy- Privacy Issues, Privacy in social networks, Privacy Models, Privacy preserving Data Mining techniques, Privacy enhancing technology, Web Privacy, Security Policies – Security Policies and Procedures, Writing Security Policies, Sample Security Policies, Types: Integrity policies, Confidentiality policies, WWW Policies, Same Origin Policy, E-mail Security Policies, etc. Security certification – Security monitoring and auditing, Forensics Investigator.	11
5	Security protocols: Transport layer protocols – SSL – Electronic mail security – PEM and S/MIME security protocol – Pretty Good Privacy – Web Security - Firewalls design principles – Trusted systems – Electronic payment protocols.	12

	Intrusion detection – password management – Viruses and related Threats – Virus Counter measures, Virtual Private Networks. Application Level Security: HTTP Vs HTTPS, SSL, IPV6 Security Requirements Specifications: Antivirus, Firewalls, IDS, IPS, Log Files, Honey Pots, Honey NetSecure Software Engineering: Need for secure systems, Software security issues, Secure Software Life Cycle, Secure Programming Vs Defensive Programming, Proactive security development process, Secure design principles and Patterns, Insecure Code Samples, Code Reviews and Static Analysis, Security Testing, Creating a Software Security Programs.	

Course Outcomes

At the end of the course the students should be able to:

CO 1	**Learn**[1] the sources of security threats and attack scenarios.
CO 2	**Learn**[1] threat management by assessing, analyzing or applying models.
CO 3	**Learn**[1] various security protocols.
CO 4	Practically **understand**[2] and implement security programs.
CO5	**Learn**[1] & implement various security protocols.
Text Books	• Kizza, J. M. (2010). **Computer Networks and Online Crimes. In *Ethical and Social Issues in the Information Age*** (pp. 247-261). Springer, London. • Swiderski, F., & Snyder, W. (2004). ***Threat modeling*.** Microsoft Press. • Calabrese, T. (2003). ***Information security intelligence: Cryptographic principles and applications*.** Delmar Publishers Inc..
Reference Books	• Kizza, J. M. (2010). **Computer Networks and Online Crimes. In *Ethical and Social Issues in the Information Age*** (pp. 247-261). Springer, London. • Calabrese, T. (2003). ***Information security intelligence: Cryptographic principles and applications*.** Delmar Publishers Inc...

COURSE CODE	DSE-II	TOTAL LECTURE:45 TUTORIAL: 15
CY20M111	IT SECURITY- THREATS & VULNERABILITY	3-1-0 = 4

Course Objectives

- To provide understanding of the main issues related to security in modern networked computer systems.
- To understand underlying concepts and foundations of computer security,
- To gain basic knowledge about security-relevant decisions in designing IT infrastructures.
- To learn different techniques to secure complex systems
- To develop practical skills in managing a range of systems, from personal laptop to large-scale infrastructures.

UNIT	CONTENTS	HOURS
1	Information Security: Introduction, How Much of Our Daily Lives Relies on Computers, Security Truisms, Basic Security, Terminology, Cyber Ethics, The Perception of Security, Threat Model, Security Is a Multidisciplinary Topic, Security Role-Playing Characters.	12
2	Passwords under Attack: Introduction, Authentication Process, Password Threats, Strong Passwords, Password Management. Email Security – Introduction, Email Systems, Email Security and Privacy.	12
3	Malware The Dark Side of Software, What Is Malware?, How Do I Get Malware?, What Does Malware Do?, Malware: Defense in Depth, Introduction, Data Backup, Firewalls, Software Patches, Antivirus Software, User Education Securely Surfing the World Wide Web: Introduction, Web Browser, "HTTP Secure", Web Browser History, Online Shopping, Consumer Decisions, Spyware and Key-Loggers, Wireless Sniffing, Scams and Phishing Websites, Misuse and Exposure of Information.	13

4	Wireless Internet Security: Introduction, How Wireless Networks Work, Wireless Security Threats, Public Wi-Fi Security, Wireless Network Administration Social Networking: Introduction, Choose Your Friends Wisely, Information Sharing, Malware and Phishing.	11
5	Social Engineering: Phishing for Suckers: Introduction, Social Engineering: Malware Distribution, Phishing, Detecting a Phishing URL, Application of Knowledge Staying Safe Online: The Human Threat: Introduction, The Differences between Cyberspace and the Physical World, Consider the Context: Watch What You Say and How It Is Communicated, What You Do on the Internet Lasts Forever, Nothing Is Private, Now or in the Future, Can You Really Tell Who You Are Talking with?, Cameras and Photo Sharing, I Am a Good Person, That Would Never Happen to Me, Is There Anything I Can Do to Make the Internet a Safer Place for My Child?	12

Course Outcomes

At the end of the course the students should be able to:

CO 1	Gained a good **understanding**[2] of the concepts and foundations of IT security.
CO 2	**Identify**[4] vulnerabilities of IT systems.
CO 3	The students can **use**[3] basic security tools to enhance system security and can develop basic security enhancements in stand-alone applications.
CO 4	**Learn**[1] various password management techniques.
CO 5	**Detect**[4] phishing in social engineering
Text Books	• Douglas Jacobson, Joseph Idziorek, 2016, "Computer Security Literacy: Staying Safe in a Digital World", Ist Edition, Chapman and Hall/CRC Press. • Mike Harwood, 2015, "Internet Security: How to Defend Against Attackers on the Web", IInd Edition, Jones & Bartlett Learning Publisher
Reference Books	• Richard E Smith, 2015, "Elementary Information Security", IInd Edition, Jones & Bartlett Learning Publisher. • Sean Philip Oriyano, 2010, "Hacker Techniques, Tools, and Incident Handling", Ist Edition, Jones & Bartlett Learning Publisher. • David Kim & Michael G. Solomon, 2016 "Fundamentals of Information Systems Security", IIIrd Edition, Jones & Bartlett Learning Publisher. .

Code	SOFTWARE LAB-I PYTHON PROGRAMMING	Practical: 30
AI20M104		0– 0–4 = 2

Course Objectives:

- This course introduces core programming basics—including data types, control structures, algorithm development, and program design with functions—via the Python programming language.
- The course discusses the fundamental principles of Object-Oriented Programming
- Learn about data and information processing techniques.
- Students will solve problems and explore real-world software development challenges
- Learn to create practical and contemporary applications.

Unit	Contents	Hours
I.	Introduction to Python Programming Language. : Introduction to Python Language, Strengths and Weaknesses, IDLE, Dynamic Types, Naming Conventions, String Values, String Operations, String Slices, String Operators, Numeric Data Types, Conversions, Built In Functions	5
II.	Data Collections and Language Component: Introduction, Control Flow and Syntax, Indenting, The if Statement, Relational Operators, Logical, Operators, True or False, Bit Wise Operators, The while Loop, break and continue, The for Loop, Lists, Tuples, Sets, Dictionaries, Sorting Dictionaries, Copying Collections.	10
III.	Object and Classes : Classes in Python, Principles of Object Orientation, Creating Classes, Instance Methods, File Organization, Special Methods, Class Variables, Inheritance, Polymorphism, Type Identification, Custom Exception Classes	10
IV.	Functions and Modules : Introduction, Defining Your Own Functions, Parameters , Function Documentation, Keyword and Optional Parameters, Passing Collections to a Function, Variable Number of Arguments, Scope, Functions - "First Class Citizens", Passing Functions to a Function, Mapping Functions in a Dictionary, Lambda, Modules, Standard Modules – sys, Standard Modules – math, Standard Modules – time, The dir Function	10
V.	I/O and Error Handling In Python : Introduction, Data Streams, Creating Your Own Data Streams, Access Modes, Writing Data to a File, Reading Data From a File, Additional File Methods, Using Pipes as Data Streams, Handling IO	10

	Exceptions, Working with Directories, Metadata, Errors, Run Time Errors, The Exception Model, Exception Hierarchy, Handling Multiple Exceptions	

Course Outcomes as per Bloom's Taxonomy	
At the end of the course the students should be able to:	
CO 1	**Apply** the principles python programming
CO 2	**Write** clear and effective python code
CO 3	**Create** applications using python programming
CO 4	**Access** database using python programming
CO 5	**Develop** web applications using python programming
Text Books	• Dive into Python, Mike • Learning Python, 4th Edition by Mark Lutz • Programming Python, 4th Edition by Mark Lutz • Kenneth A. Lambert, The Fundamentals of Python: First Programs, 2011, Cengage Learning, ISBN: 978-1111822705.
Reference Books	• Starting Out with Python (2009) Pearson , Tonny Gaddis • Beginning Pyhton Wrox Publication Peter Norton, Alex Samuel • Python Algorithms Apress, Magnus Liet Hetland • Python Object Oriented Programming PACKT Press, Dusty Phillips • Python for Unix and Linux System Administration O'Relly, Noad Gift

COURSE CODE	PROJECT BASED LEARNING-I	TOTAL PRACTICAL:30
PB20M101		**(LTP=0-0-4=2)**
Learning Objectives:	• Integrating the knowledge and skills of various courses on the basis of multidisciplinary projects • Develop the skill of critical thinking and evaluation. • To develop 21st century success skills such as critical thinking, problem solving, communication, collaboration and creativity/innovation among the students. • To enhance deep understanding of academic, personal and social development in students. • Employ the specialized vocabularies and methodologies.	
Course Outcomes		
At the end of the course the students will be able to:		
Course Outcomes:	• **Apply**[3]a sound knowledge/skills to select and develop their topicand project respectively. • **Develop**[6] plans and allocate roles with clear lines of responsibilityand accountability. • **Design**[6] solutions to complex problems following a systematic approach like problem identification, formulation and solution. • **Collaborate**[6] with professionals and the community at large in written and in oral forms. • **Correlate**[4]the knowledge, skills and attitudes of a professional.	
General Guidelines:	• PBL will be an integral part of UG/PG Programs at different levels. • Each semester offering PBL will provide a separate Course Code, twocredits will be allotted to it. • Faculty will be assigned as mentor to a group of 30 students minimum byHoS. • Faculty mentor will have 4 hours/week to conduct PBL for assigned students. • Student will select a topic of their choice from syllabus of any course offered in respective semester (in-lines with sustainable development goals). • Student may work as a team maximum 3 or minimum 2 members for single topic. • For MSE, student's performance will be assessed by panel of three experts either from other department/school, or from same department/school based on chosen topic. This will be comprised of apresentation by student followed by viva-voce. It will be evaluated for 30 marks. • 20 marks would be allotted for continuous performance assessment by concerned guide/mentor. For ESE, student will need to submit a project report in prescribed format,duly signed by concerned guide/mentor and head of the school. The report should be	

	comprised of following components: 1. Introduction 2. Review of literature 3. Methodology 4. Result and Discussion 5. Conclusion and Project Outcomes 6. References • Student will need to submit three copies for 1. Concerned School 2.Central Library 3. Self • The integrity of the report should be maintained by student. Any malpractice will not be entertained. • Writing Ethics to be followed by student, a limit of 10 % plagiarism is permissible. Plagiarism report is to be attached along with the report. • Project could be a case study/ analytical work /field work/ experimentalwork/ programming or as per the suitability of the program.

SANJEEV AGRAWAL GLOBAL EDUCATIONAL (SAGE) UNIVERSITY, BHOPAL

Syllabus

For

MTech (Cyber Security & Forensic)

Semester-II

School of Advanced Computing

COURSE CODE	DATA PRIVACY	TOTAL LECTURE:45 TUTORIAL: 15
CY20M201		3 – 1 – 0 = 4

Course Objectives :

- To learn fundamental concepts of data privacy.
- To learn different data explosion techniques.
- To understand protection models.
- To create architectural, algorithmic and technological foundations for the maintenance of the privacy of individuals.
- To understand the confidentiality of organizations, and the protection of sensitive information, despite the requirement that information be released publicly or semi-publicly.

UNIT	CONTENTS	HOURS
1	Introduction- Fundamental Concepts, Definitions, Statistics, Data Privacy Attacks, Data linking and profiling, access control models, role based access control, privacy policies, their specifications, languages and implementation, privacy policy languages, privacy in different domains- medical, financial, etc.	12
2	Data explosion- Statistics and Lack of barriers in Collection and Distribution of Person-specific information, Mathematical model for characterizing and comparing real-world data sharing practices and policies and for computing privacy and risk measurements, Demographics and Uniqueness.	12
3	Protection Models- Null-map, k-map, Wrong map Survey of techniques- Protection models (null-map, k-map, wrong map), Disclosure control, Inferring entity identities, Strength and weaknesses of techniques, entry specific databases.	12
4	Computation systems for protecting delimited data- MinGen, Datafly, Mu-Argus, k-Similar, Protecting textual documents: Scrub.	12
5	Technology, Policy, Privacy and Freedom- Medical privacy legislation, policies and best practices, Examination of privacy matters specific to the World Wide Web, Protections provided by the Freedom of Information Act or the requirement for search warrants.	12

Course Outcomes

At the end of the course the students should be able to:	
CO 1	**Understand**[2] the concepts of privacy in today's environment.
CO 2	Obtain the **understanding**[2] of how automation is changing the concepts and expectations concerning privacy and the increasingly interconnected issue of security.
CO 3	**Understand**[2] the knowledge of the role of private regulatory and self-help efforts.
CO 4	Have an **understanding**[2]of how emerging issues are affecting society and business, with a concentration on how information security must shape corporate practices.
CO 5	**Describe**[1] different protection models and data explosion techniques.
Text Books	• Raghunathan, B. (2013). ***The complete book of data anonymization: from planning to implementation*****.** CRC Press. • Sweeney, L. (2001). ***Computational disclosure control: A primer on data privacy protection*** (Doctoral dissertation, Massachusetts Institute of Technology).

COURSE CODE	CYBER FORENSICS	TOTAL LECTURE:45 TUTORIAL:15
CY20M202		3 – 1 – 0 = 4

Course Objectives :

- Describe how to prepare for digital evidence investigations and explain the differences
- Define digital forensics from electronic media.
- Be able to understand the recovery method
- Be able to work on different forensic tools
- Explain the importance of maintaining professional conduct between law enforcement agency and corporate investigations.

UNIT	CONTENTS	HOURS
1	Cyber forensics Introduction to Cyber forensics, Type of Computer Forensics Technology- Type of Vendor and Computer Forensics Services. Information Security Investigations, Corporate Cyber Forensics, Scientific method in forensic analysis, investigating large scale Data breach cases, Analyzing Malicious software.	12
2	Digital Evidence in Criminal Investigations. The Analog and Digital World, Training and Education in digital evidence, the digital crime scene, Investigating Cybercrime,. Computer Forensics Evidence and Capture- Data Recovery-Evidence collection and Data Seizure-Duplication and preservation of Digital Evidence-Computer image verification and Authentication	12
3	Investigating Network Intrusions and Duties Support Functions and Competencies Cyber Crime, Network Forensics and Investigating logs, Investigating network Traffic, Investigating Web attacks, Router Forensics.	12
4	Computer Forensics Analysis- Discovery of Electronic Evidence- Identification of data- Reconstructing Past events- networks	12
5	Countermeasure: Information warfare- Surveillance tool for Information warfare of the future-Advanced Computer Forensics. Cyber forensics tools and case studies.	12

Course Outcomes

At the end of the course the students should be able to:

CO 1	**understand**[2] the concepts of Network investigations
CO 2	**Perform**[3] web based investigations.
CO 3	**Perform**[3] digital forensics analysis upon networks and network devices.
CO 4	**Utilize**[3] various forensic tools to collect digital evidence.
CO 5	**Utilize**[3] a systematic approach to computer investigations.
Text Books	• Barbara, J. J. (Ed.). (2007). ***Handbook of digital and multimedia forensic evidence*****. Springer Science & Business Media**. • Bayuk, J. (Ed.). (2010**).** ***CyberForensics: understanding information security investigations*****. Springer Science & Business Media**.
Reference Books	• Ventre, D. (Ed.). (2012). ***Cyberwar and information warfare***. John Wiley & Sons. • Vacca, J. R. (2005). ***Computer forensics: computer crime scene investigation*** (pp. 217-301). Hingham, MA: Charles River Media.

COURSE CODE	ETHICAL HACKING	TOTAL LECTURE:45 PRACTICAL:15
CY20M203		3 – 0 – 2 = 4

Course Objectives :

- Introduce the methodologies and framework of ethical hacking for enhancing the security.
- Impacts of Hacking; Types of Hackers.
- Introduces the concepts of Ethical Hacking .
- Gives the students the opportunity to learn about different tools and techniques in Ethical hacking and security.
- Practically apply Ethical hacking tools to perform various activities.

UNIT	CONTENTS	HOURS
1	**Introduction:** Hacking Impacts, The Hacker Framework: Planning the test, Sound Operations, Reconnaissance, Enumeration, Vulnerability Analysis, Exploitation, Final Analysis, Deliverable, Integration Information Security Models: Computer Security, Network Security, Service Security, Application Security, Security Architecture Information Security Program: The Process of Information Security, Component Parts of Information Security Program, Risk Analysis and Ethical Hacking.	10
2	**The Business Perspective:** Business Objectives, Security Policy, Previous Test Results, Business Challenges Planning for a Controlled Attack: Inherent Limitations, Imposed Limitations, Timing is Everything, Attack Type, Source Point, Required Knowledge, Multi-Phased Attacks, Teaming and Attack Structure, Engagement Planner, The Right Security Consultant, The Tester, Logistics, Intermediates, Law Enforcement.	10
3	**Preparing for a Hack:** Technical Preparation, Managing the Engagement Reconnaissance: Social Engineering, Physical Security, Internet Reconnaissance.	10
4	**Enumeration:** Enumeration Techniques, Soft Objective, Looking Around or Attack, Elements of Enumeration, Preparing for the Next Phase Exploitation: Intutive Testing, Evasion, Threads and Groups, Operating Systems, Password	8

	Crackers, RootKits, applications, Wardialing, Network, Services and Areas of Concern.	
5	**Deliverable:** The Deliverable, The Document, Overal Structure, Aligning Findings, Presentation Integration: Integrating the Results, Integration Summary, Mitigation, Defense Planning, Incident Management, Security Policy, Conclusion	7

List of Experiment

1) Study the use of network reconnaissance tools like WHOIS, dig, traceroute, nslookup to gather information about networks and domain registrars.
2) Case Study of kaali tool
3) To learn about hacking tools and skills
4) To study about Footprinting and Reconnaissance.
5) To study about Fingerprinting.
6) To study about system Hacking.
7) To study about Wireless Hacking.
8) To learn & study about Sniffing & their tools.

Course Outcomes

At the end of the course the students should be able to:

CO 1	**Demonstrate**[2] the use and availability of tools to support an ethical hacking.
CO 2	**Analyze**[4] the results of a controlled attack.
CO 3	**Describe**[1] the role of politics, inherent and imposed limitations and metrics for planning of a test.
CO 4	**Analyze**[4] the dangers associated with penetration testing.
CO 5	To **understand**[2] ethical hacking in business perspective.
Text Books	• Tiller, J. S. (2004). ***The ethical hack: a framework for business value penetration testing*****.** Auerbach publications.
Reference Books	• EC-Council, 2016, "Ethical Hacking and Countermeasures Attack Phases", IInd Edition, Cengage Learning. • Simpson, M. T., Backman, K., & Corley, J. (2010). ***Hands-on ethical hacking and network defense*****.** Cengage Learning.

COURSE CODE	DSE-III	TOTAL LECTURE:45 TUTORIAL:15
CY20M207	DATABASE SECURITY & ACCESS CONTROL	3 – 1–0 = 4

Course Objectives

- To learn about the threats to database security.
- To understand what causes these threats by studying how vulnerabilities arise in the development and uses of database systems.
- To understand the architecture and levels of database security.
- To narrate and evaluate the design principles of conventional discretionary and mandatory security techniques.
- To describe the mandatory and discretionary security techniques related to database security.

UNIT	CONTENTS	HOURS
1	Overview of Information Security, Database design using the relational model :- Functional dependencies : Keys in a relational model, Concept of functional dependencies, Normal forms based on primary keys, BCNF Further Dependencies : Multi-values dependencies and fourth normal form, Join dependencies and fifth normal form, Inclusion dependencies, Other dependencies and normal forms.	12
2	Understand the need for a database security architecture, database security architecture, Database security lifecycle, data risk assessment, Analyze data threats, risks and vulnerabilities, Implement a feedback mechanisms, Understand how to adjust policies and practices based on feedback mechanisms using different security models.	12
3	Distinction between data and database security from network and perimeter security, external and internal database threats, flaws in perimeter security, risks of not securing an organization's data, typical database security hierarchy, analysis general security landscape, evaluation of security fundamentals, Understand the importance for staying current with database releases, fixes and security patches , Managing USB ports and USB enabled devices, Understand the implications of the physical placement of database	12

	files and their copies	
4	Access control models for XML databases. Managing and Querying Encrypted Data, Access control of relational databases, Temporal role-based access control in database management, Security in Data Warehouses and OLAP Systems.	12
5	Geospatial Database Security, Damage Quarantine and Recovery in Data Processing Systems, Secure Semantic Web Services, Privacy-enhanced Location-based Access Control, Efficiently Enforcing the Security and Privacy Policies in a Mobile Environment.	12

Course Outcomes

At the end of the course the students should be able to:

CO 1	**Analyze**[4] and determine for any organization the database security requirements and appropriate solutions.
CO 2	**Protect**[3] a database system from different types of threats, vulnerabilities and attacks.
CO 3	**Describe**[1] the mandatory and discretionary security techniques related to database security.
CO 4	**Describe**[1] the various information security policies related to database.
CO 5	**Implement**[6] multilevel security in databases.
Text Books	• Castano, 1995, "Database Security", IInd Edition, Pearson Education. • Basta, A., & Zgola, M. (2011). ***Database security***. Cengage Learning.
Reference Books	• Gertz, M., & Jajodia, S. (Eds.). (2007). ***Handbook of database security: applications and trends***. Springer Science & Business Media. • Afyouni, H. A. (2006). **Database security and Auditing.** ***Protecting Data Integrity and Accessibility*****.**

COURSE CODE	DSE-III	TOTAL LECTURE:45 TUTORIAL:15
CY20M208	CYBER CRIME & INFORMATION WARFARE	3-1-0 =4

Course Objectives

- To study different Cyber Crime & its challenges, cyber terrorism & Information Warfare.
- To use information as tool for defense.
- To study ways of handling cyber terrorism & Information warfare.
- Articulate the main elements of various cybercrime offences.
- Understand the unique challenges posed to law enforcement agents, policy makers and prosecutors.

UNIT	CONTENTS	HOURS
1	Introduction of cyber crime, challenges of cyber crime, categorizing cyber crime, cyber terrorism, virtual crimes, perception of cyber criminals: hackers, insurgents and extremist group.	12
2	Interception of data, surveillance and protection, criminal copy right infringement, cyber stalking, hiding crimes in cyber space and methods of concealment.	12
3	Anonymity and markets, privacy and security at risk in the global information society, privacy in cyber space, war fare concept, information as an intelligence weapon, attack and retaliation attack and defense.	12
4	An I-WAR risk analysis model, implication of I –WAR for information managers, perceptual intelligence.	12
5	I-WAR, handling cyber terrorism and information warfare, Jurisdiction.	12

Course Outcomes

At the end of the course the students should be able to:

CO 1	**Demonstrate**[2] different types of cyber-attacks.

CO 2	**Demonstrate**[2] different cyber criminals.
CO 3	**Demonstrate**[2] secure the computer/networks from these cyber-attacks.
CO 4	**Use**[3] information as tool for defense.
CO 5	**Understand**[2] information warfare.
Text Books	• Clough Jonathan, 2010, "**Principle of cyber-crime**", Ist Edition, Cambridge University Press.
Reference Books	• Hutchinson William, Warren Matthew, 2001, "**Information warfare: Corporate attack and defence in digital world**", 1st Edition, A Butterworth-Heineman

COURSE CODE	DSE-III	TOTAL LECTURE:45 TUTORIAL:15
CY20M209	SECURE CODING	3-1-0 = 4

Course Objectives

- To provide an understanding of the various security attacks and knowledge to recognize and remove common coding errors that lead to vulnerabilities.
- Gives an outline of the techniques for developing a secure application.
- Understand the basic principles and practices of secure computing and writing secure software.
- To learn and apply knowledge of information management and computer networking and communications while performing software-security assessments.
- Synthesize alternative designs and implementations that incorporate mitigations for observed vulnerabilities.

UNIT	CONTENTS	HOURS
1	Introduction: Security, CIA Triad, Viruses, Trojans, and Worms In a Nutshell, Security Concepts- exploit, threat, vulnerability, risk, attack. Malware Terminology: Rootkits, Trapdoors, Botnets, Key loggers, Honeypots. Active and Passive Security Attacks. IP Spoofing, Tear drop,DoS, DDoS,XSS, SQL injection, Smurf, Man in middle, Format String attack. Types of Security Vulnerabilities- buffer overflows, Invalidated input, race conditions, access-control problems, weaknesses in authentication, authorization, or cryptographic practices. Access Control Problems.	12
2	Need for secure systems: Proactive Security development process, Secure Software Development Cycle (S-SDLC) , Security issues while writing SRS, Design phase security, Development Phase, Test Phase, Maintenance Phase, Writing Secure Code – Best Practices SD3 (Secure by design, default and deployment), Security principles and Secure Product Development Timeline.	12
3	Threat modelling process and its benefits: Identifying the Threats by Using Attack Trees and rating threats using DREAD, Risk Mitigation Techniques and Security Best Practices. Security techniques, authentication, authorization. Defence in Depth and Principle of Least Privilege.	12
4	Secure Coding Techniques: Protection against DoS attacks, Application Failure Attacks, CPU Starvation Attacks, Insecure Coding Practices In Java Technology. ARP Spoofing and its countermeasures. Buffer Overrun- Stack	12

	overrun, Heap Overrun, Array Indexing Errors,FormatString Bugs. Security Issues in C Language: String Handling, Avoiding Integer Overflows and Underflows and Type Conversion Issues- Memory Management Issues, Code Injection Attacks,Canary based countermeasures using StackGuard and Propolice. Socket Security, Avoiding Server Hijacking, Securing RPC, ActiveX and DCOM.	
5	Database and Web-specific issues: SQL Injection Techniques and Remedies,Race conditions, Time of Check Versus Time of Use and its protection mechanisms. Validating Input and Page 21 of 46 Interprocess Communication, Securing Signal Handlers and File Operations. XSS scripting attack and its types – Persistent and Non persistent attack XSS Countermeasures and Bypassing the XSS Filters. Testing Secure Applications: Security code overview, secure software installation. The Role of the Security Tester, Building the Security Test Plan. Testing HTTP-Based Applications, Testing File-Based Applications, Testing Clients with Rogue Servers.	12

Course Outcomes

At the end of the course the students should be able to:

CO 1	To implement security as a culture and show mistakes that make applications vulnerable to attacks.
CO 2	To **understand**[2] various attacks like DoS, buffer overflow, web specific, database specific, web-spoofing attacks.
CO 3	To **Demonstrate**[2] skills needed to deal with common programming errors that lead to most security problems and to learn how to develop secure applications.
CO 4	To **identify**[2] the nature of the threats to software and incorporate secure coding practices throughout the planning and development of the product
CO5	Able to properly handle application faults, **implement**[3] secure authentication, authorization and data validation controls used to prevent common vulnerabilities.
Text Books	• Howard Michael and LeBlanc David, 2004, "**Writing Secure Code**", IInd Edition Microsoft Press. • Deckar Jason, 2005, "**Buffer Overflow Attacks: Detect, Exploit**", Prevent, Ist Edition , Syngress.

Reference Books	• Swiderski Frank and Snyder Window, 2004, "**Threat Modeling**", 1st Edition, Microsoft Professional.

COURSE CODE	DSE-IV	TOTAL LECTURE:45 TUTORIAL: 15
CY20M210	INCIDENCE RESPONSE AND MANAGEMENT	3-1-0 = 4

Course Objectives:

- To learn how to define an incident relating to cyber security.
- To learn protocols for first on crime scene investigations.
- Obtain basic knowledge on dealing with system security related incidents.
- Increase knowledge on potential defenses and counter measures against common threat vectors/vulnerabilities.
- Obtain current knowledge of events and tools/support kits in the subject area.

UNIT	CONTENTS	HOURS
1	Cyber Incident Statistics, Computer Security Incident, Information as Business Asset, Data Classification, Information Warfare, Key Concepts of Information Security, Vulnerability, Threat and Attacks, Types of Computer Security Incidents, Examples of Incidents, Incidents Categorization, Low Level Incident, Mid Level Incident, High Level Incident.	12
2	Incident Prioritization, Incident Response, Incident Handling, Disaster Recovery, Technologies and Impacts, Virtualization and Impacts, Estimated Cost of an Incident, Incident Reporting Organizations, Vulnerability Reports, Incident Identification, Need for Incidents Response, Goals for Incident Response.	12
3	Incident Response and Handling Process; Step 1: Identification; Step 2: Incident Recording; Step 3: Initial Response; Step 4: Communicating the Incident; Step 5: Containment; Step 6: Formulating a Response Strategy; Step 7: Incident Classification; Step 8: Incident Investigation; Step 9: Data Collection; Step 10: Forensic Analysis, Step 11: Evidence Protection; Step 12: Notify External Agencies; Step 13: Eradication; Step 14: System Recovery; Step 15: Incident Documentation; Step 16: Incident Damage and Cause assessment; Step 17: Review and Update the Response Policies.	12
4	Incident Response Team development, Security Awareness and Training Checklist, Incident Management, Purpose of Incident management, Incident management process.	12
5	Incident management team, Incident Response Team and Members, Member Goals and Responsibilities, Developing Skills in Incident Response Personnel, Incident Response Team Structure, Team Dependencies and Services.	12

Course Outcomes	
At the end of the course the students should be able to:	
CO 1	Obtain basic **knowledge**[1] on dealing with system security related .
CO 2	Increase **knowledge**[1] on potential defences and counter measures against common threat vectors/vulnerabilities.
CO 3	Gain experience using tools and common processes in performing **analysis**[4] of compromised systems and dynamic malware analysis.
CO 4	Obtain current **knowledge**[1] of events and tools/support kits in the subject area.
CO 5	**Explain**[4] security awareness.
Text Books	Luttgens Jason, Pepe Matthew, and Mandia Kevin, 2014, "**Incident Response & Computer Forensics**", Third Edition, McGraw-Hill Education, ISBN: 978-0071798686.
Reference Books	Murdoch Don, 2016, "**Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder**", CreateSpace Independent Publishing Platform, 2.2 Edition , ISBN: 978-1500734756

COURSE CODE	DSE-IV	TOTAL LECTURE:45 TUTORIAL: 15
CY20M211	CYBER THREAT INTELLIGENCE	3-1-0 = 4

Course Objectives

- To learn basic fundamentals of cyber threat intelligence.
- To demonstrate how cyber has changed the nature of intelligence collection.
- To analyze the cyber threats at different levels.
- To learn how to collect cyber threat data.
- To validate and prioritize risks involved.

UNIT	CONTENTS	HOURS
1	Defining Cyber Threat Intelligence: The Need for Cyber Threat Intelligence: The menace of targeted attacks, The monitor-and-respond strategy, Why the strategy is failing, Cyber Threat Intelligence Defined, Key Characteristics: Adversary based, Risk focused, Process oriented, Tailored for diverse consumers, The Benefits of Cyber Threat Intelligence.	12
2	Developing Cyber Threat Intelligence Requirements: Assets That Must Be Prioritized: Personal information, Intellectual property, Confidential business information, Credentials and IT systems information, Operational systems. Adversaries: Cybercriminals, Competitors and cyber espionage agents, Hacktivists. Intelligence Consumers: Tactical users, Operational users, Strategic users.	12
3	Collecting Cyber Threat Information: Level 1: Threat Indicators, File hashes and reputation data, Technical sources: honeypots and scanners, Industry sources: malware and reputation feeds. Level 2: Threat Data Feeds, Cyber threat statistics, reports, and surveys, Malware analysis. Level 3: Strategic Cyber Threat Intelligence, Monitoring the underground, Motivation and intentions, Tactics, techniques, and procedures.	12
4	Analyzing and Disseminating Cyber Threat Intelligence: Information versus Intelligence, Validation and Prioritization: Risk scores, Tags for context, Human assessment. Interpretation and Analysis: Reports, Analyst skills, Intelligence platform, Customization. Dissemination: Automated feeds and APIs, Searchable knowledge base, Tailored reports.	12
5	Selecting the Right Cyber Threat Intelligence Partner: Types of Partners: Providers of threat indicators, Providers of threat data feeds, Providers of comprehensive cyber threat intelligence	12

Course Outcomes	
At the end of the course the students should be able to:	
CO 1	**Examine**[3] the history and development of cyber intelligence operations and how those operations can integrate with other intelligence collection.
CO 2	Threat **Study**[1] the technique to Develop Cyber Threat Intelligence Requirements.
CO 3	**Evaluate**[3] the benefits and risks of the current cyber intelligence structure.
CO 4	**Use**[3] the attributes of computer network exploitation, defense and attack within the intelligence context.
CO 5	**Examine**[3]the intelligence challenge of attribution in cyber-attacks.
Text Books	• Friedman, J., & Bouchard, M. (2015). ***Definitive Guide to Cyber Threat Intelligence: Using Knowledge about Adversaries to Win the War against Targeted Attacks.*** CyberEdge Group. • Friedman, J., & Bouchard, M. (2015). ***Definitive Guide to Cyber Threat Intelligence: Using Knowledge about Adversaries to Win the War against Targeted Attacks***. CyberEdge Group. • Dalziel, H. (2014). ***How to define and build an effective cyber threat intelligence capability***. Syngress.
Reference Books	• Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., & Shakarian, P. (2017). ***Darkweb cyber threat intelligence mining***. Cambridge University Press. • Gourley Bob, 2014, "**The Cyber Threat**", Create space Independent Pub.

COURSE CODE	DSE-IV	TOTAL LECTURE:45 TUTORIAL: 15
CY20M212	INFORMATION SECURITY & RISK MANAGEMENT	3-1-0 = 4

Course Objectives

- To understand and development of concepts required for risk-based planning and risk management of computer and information systems.
- Extract and summarize the most appropriate risk management terms given a practical scenario.
- Apply the FAIR framework to a practical scenario such that the identified risks are appropriately addressed.
- Articulate the strengths and weaknesses of common risk management frameworks
- Evaluate the proper course of actions in order to adequately identify and assess risk.

Unit	Contents	Hours
1	An Introduction to Risk Management: Introduction to the Theories of Risk Management; The Changing Environment; The Art of Managing Risks.	12
2	The Threat Assessment Process: Threat Assessment and its Input to Risk Assessment; Threat Assessment Method; Example Threat Assessment	12
3	Vulnerability Issues: Operating System Vulnerabilities; Application Vulnerabilities; Public Domain or Commercial Off-the-Shelf Software; Connectivity and Dependence; Vulnerability assessment for natural disaster, technological hazards, and terrorist threats; implications for emergency response, vulnerability of critical infrastructures	13
4	The Risk Process: What is Risk Assessment? Risk Analysis; Who is Responsible?	11
5	Tools and Types of Risk Assessment: Qualitative and Quantitative risk Assessment; Policies, Procedures, Plans, and Processes of Risk Management; Tools and Techniques; Integrated Risk Management; Future Directions: The Future of the Risk Management.	12

Course Outcomes	
At the end of the course the students should be able to:	
CO 1	The cognitive skills and ability to identify, **analyze**[4] and articulate the importance of managing IS-related risk and security issues in organizations, and the relationship between these and the achievement of business value from IS/IT investments.
CO 2	**Understand**[2] the risk assessment
CO 3	The cognitive skills and practical ability to **develop**[2] and document IS/IT risk and security management plans that detail contingency planning strategies and practices.
CO 4	.**Understand**[2] the art of Managing Risks.
CO 5	**Design**[6] a set of key technology risk indicators that can be used to signal the existence of potentially undesirable conditions.
Text Books	• Freund, J., & Jones, J. (2014). ***Measuring and managing information risk: a FAIR approach***. Butterworth-Heinemann. • Hubbard, D. W., & Seiersen, R. (2016). ***How to measure anything in cybersecurity risk***. John Wiley & Sons. • Hubbard, D. W. (2020). ***The failure of risk management: Why it's broken and how to fix it***. John Wiley & Sons.

Code	SOFTWARE LAB-II R PROGRAMMING	Practical: 30
AI0M204		0– 0–4 = 2

Course Objective

- To learn how to program in R
- To learn how to use R for effective data analysis.
- You will learn how to install and configure software necessary for a statistical programming environment.
- The course covers practical issues in statistical computing which includes programming in R, reading data into R, accessing R packages, writing R functions, debugging, and organizing and commenting R code.

Unit	Contents	Hours
I.	Introduction: Introducing to R, R Data Structures, Help functions in R, Vectors, Scalars, Declarations, recycling, Common Vector operations, Using all and any, Vectorized operations, NA and NULL values, Filtering, Vectorized if-then else, Vector Equality, Vector Element names	5
II.	Matrices, Arrays And Lists: Creating matrices, Matrix operations, Applying Functions to Matrix Rows and Columns, Adding and deleting rows and columns, Vector/Matrix Distinction, Avoiding Dimension Reduction, Higher Dimensional arrays, lists, Creating lists, General list operations, Accessing list components and values, applying functions to lists, recursive lists	10
III.	Data Frames: Creating Data Frames, Matrix-like operations in frames, Merging Data Frames, Applying functions to Data frames, Factors and Tables, factors and levels, Common functions used with factors, Working with tables, Other factors and table related functions, Control statements, Arithmetic and Boolean operators and values, Default values for arguments, Returning Boolean values, functions are objects, Environment and Scope issues, Writing Upstairs, Recursion, Replacement functions, Tools for composing function code, Math and Simulations in R	10
IV.	OOP: S3 Classes, S4 Classes, Managing your objects, Input/Output, accessing keyboard and monitor, reading and writing files, accessing the internet, String Manipulation, Graphics, Creating Graphs, Customizing Graphs, Saving graphs to files, Creating three-dimensional plots	10
V.	Interfacing: Interfacing R to other languages, Parallel R, Basic Statistics, Linear Model, Generalized Linear models, Non-linear models, Time Series and Auto-correlation, Clustering	10

Course Outcomes as per Bloom's Taxonomy	
At the end of the course the students should be able to:	
CO 1	**Understand** the basics in R programming in terms of constructs, control statements, string functions
CO 2	**Understand** the use of R for Big Data analytics
CO 3	**Create** applications using R programming
CO 4	**Learn** to apply R programming for Text processing
CO 5	**Apply** the R programming from a statistical perspective
Text Books	• Norman Matloff , "The Art of R Programming: A Tour of Statistical Software Design", No Starch Press, 2011 • Jared P. Lander, "R for Everyone: Advanced Analytics and Graphics", Addison-Wesley Data & Analytics Series, 2013.
Reference Books	• Mark Gardener, " Beginning R – The Statistical Programming Language", Wiley, 2013 • Robert Knell, "Introductory R: A Beginner's Guide to Data Visualisation, Statistical Analysis and Programming in R", Amazon Digital South Asia Services Inc, 2013.

COURSE CODE	PROJECT BASED LEARNING-II	TOTAL PRACTICAL:30
PB20M201		**(LTP=0-0-4=2)**
Learning Objectives:	• Integrating the knowledge and skills of various courses on the basis of multidisciplinary projects • Develop the skill of critical thinking and evaluation. • To develop 21st century success skills such as critical thinking, problem solving, communication, collaboration and creativity/innovation among the students. • To enhance deep understanding of academic, personal and social development in students. • Employ the specialized vocabularies and methodologies.	
Course Outcome		
At the end of the course the students will be able to:		
Course Outcomes:	• **Apply**[3]a sound knowledge/skills to select and develop their topicand project respectively. • **Develop**[6] plans and allocate roles with clear lines of responsibilityand accountability. • **Design**[6] solutions to complex problems following a systematic approach like problem identification, formulation and solution. • **Collaborate**[6] with professionals and the community at large in written and in oral forms. • **Correlate**[4]the knowledge, skills and attitudes of a professional.	
General Guidelines:	• PBL will be an integral part of UG/PG Programs at different levels. • Each semester offering PBL will provide a separate Course Code, twocredits will be allotted to it. • Faculty will be assigned as mentor to a group of 30 students minimum byHoS. • Faculty mentor will have 4 hours/week to conduct PBL for assigned students. • Student will select a topic of their choice from syllabus of any course offered in respective semester (in-lines with sustainable development goals). • Student may work as a team maximum 3 or minimum 2 members for single topic. • For MSE, student's performance will be assessed by panel of three experts either from other department/school, or from same department/school based on chosen topic. This will be comprised of apresentation by student followed by viva-voce. It will be evaluated for 30 marks. • 20 marks would be allotted for continuous performance assessment by concerned guide/mentor. For ESE, student will need to submit a project report in prescribed format,duly signed by concerned guide/mentor and head of the school. The report should be	

	comprised of following components: 1. Introduction 2. Review of literature 3. Methodology 4. Result and Discussion 5. Conclusion and Project Outcomes 6. References • Student will need to submit three copies for 1. Concerned School 2.Central Library 3. Self • The integrity of the report should be maintained by student. Any malpractice will not be entertained. • Writing Ethics to be followed by student, a limit of 10 % plagiarism is permissible. Plagiarism report is to be attached along with the report. • Project could be a case study/ analytical work /field work/ experimentalwork/ programming or as per the suitability of the program.

SANJEEV AGRAWAL GLOBAL EDUCATIONAL (SAGE) UNIVERSITY, BHOPAL

Syllabus

for

MTech (Cyber Security & Forensic)

Semester-III & IV

School of Advanced Computing

COURSE CODE	MOOC-1/ MOOC-2	**Total Lecture:** **Practical:60**
		(LTP=0-0-8=4)
Learning Objective:	• Integrating the knowledge and skills of various courses available in online mode. • Develop the skills of critical thinking and evaluation. • To make students to learn themselves by choosing the course as per there area of interest.	
	CONTENTS	**HOURS**
General Guidelines:	• This course creates an excellent opportunity for students to acquire the necessary skill set for research, employability through massive open online courses (MOOCs) where the rare expertise of world famous experts from academics and industry are available. • The basket for MOOCs will be a dynamic one, as courses keep on updating with time. • In this semester 8 credits will have to be acquired with online courses (MOOCs). Students will have to complete 2 MOOC's of their choice in the third semester. • The MOOC-1 and MOOC-2 each carries internal marks of 50, which will be attained after he/she gets the MOOC certificate for which he/she got himself/herself enrolled. For end sem evaluation a Viva-Voce examination shall be conducted and it will carrie 50 marks.	60

GUIDELINES FOR M. TECH. DISSERTATION/ THESIS

Phase-1

- Every candidate shall be required to submit a thesis or dissertation on a topic approved by the Dissertation Review Committee (DRC).
- A Dissertation Review Committee shall be constituted with the Head of the Department as Chairperson, Dissertation Supervisor and one senior faculty member of the Department offering the M. Tech. programme.
- Candidate has to present in Dissertation Work Review I, in consultation with his Dissertation Supervisor, the title, objective and plan of action of his dissertation work to the Dissertation Work Review Committee (DRC) for approval within four weeks from the commencement of Second year First Semester. The Dissertation Work Review I carries internal marks of 100. Evaluation should be done by the DRC for 50 marks and the Supervisor will evaluate the review for the other 50 marks. Only after obtaining the approval of the DRC can the student initiate the Dissertation work.
- If a candidate wishes to change his/her supervisor or topic of the dissertation, he/she can do so with the approval of the DRC. However, the DRC shall examine whether or not the change of topic/supervisor leads to a major change of his initial plans of dissertation proposal. If yes, his/her date of registration for the dissertation work starts from the date of change of Supervisor or topic as the case may be.
- A candidate shall submit his dissertation progress report in two stages at least with a gap of three months between them.
- The work on the dissertation shall be initiated at the beginning of the II year and the duration of the dissertation is two semesters. A candidate is permitted to submit thesis only after successful completion of all theory and practical courses with the approval of DRC not earlier than 40 weeks from the date of approval of the dissertation work. For the approval of DRC the candidate shall submit the draft copy of thesis to the Head of the Department and make an oral presentation before the DRC.
- The Dissertation Work Review II in II Year III Sem. carries internal marks of 100. Evaluation should be done by the DRC for 50 marks and the Supervisor will evaluate the work for the other 50 marks. The Supervisor and DRC will examine the Problem

Definition, Objectives, Scope of Work, Literature Survey in the same domain and progress of the Dissertation Work. A candidate has to secure a minimum of 70% of marks to be declared successful in Dissertation Work Review II. If he fails to obtain the minimum required marks, he has to reappear for Dissertation Work Review-II as and when conducted.

- One paper in third semester has to be published in any one journal of UGC care, SCOPUS or SCI.
- After successful completion of Dissertation Work Review II, it will be further adjudicated by an external examiner selected by the University. For this, the Principal of the College/School/Institute shall submit name of examiners from among the list of experts in the relevant specialization as submitted by the supervisor concerned and Head of the Department. It will carries external marks of 200.

Phase-2

- The Dissertation Work Review III in II Year IV Sem. carries 250 internal marks. Evaluation should be done by the DRC for 125 marks and the Supervisor will evaluate it for the other 125 marks. The DRC will examine the overall progress of the Dissertation Work and decide whether or not the Dissertation is eligible for final submission. A candidate has to secure a minimum of 70% of marks to be declared successful in Dissertation Work Review III. If he fails to obtain the required minimum marks, he has to reappear for Dissertation Work Review III as and when conducted. For Dissertation Evaluation (Viva Voce) in II Year II Sem. there are external marks of 250 and it is evaluated by the external examiner. The candidate has to secure a minimum of 50% marks in Dissertation Evaluation (VivaVoce) examination.
- One paper in fourth semester has to be published in any one journal of UGC care, SCOPUS or SCI.
- Dissertation Work Reviews II and III shall be conducted in phase I (Regular) and Phase II (Supplementary). Phase II will be conducted only for unsuccessful students in Phase I. The unsuccessful students in Dissertation Work Review II (Phase II) shall reappear for it at the time of Dissertation Work Review III (Phase I). These students shall reappear for Dissertation Work Review III in the next academic year at the time of Dissertation Work

Review II only after completion of Dissertation Work Review II, and then Dissertation Work Review III follows. The unsuccessful students in Dissertation Work Review III (Phase II) shall reappear for Dissertation Work Review III in the next academic year only at the time of Dissertation Work Review II (Phase I).

- After approval from the DRC, a soft copy of the thesis should be submitted for ANTIPLAGIARISM check and the plagiarism report should be submitted to the University and be included in the final thesis. The Thesis will be accepted for submission, if the similarity index is less than 30%. If the similarity index has more than the required percentage, the student is advised to modify accordingly and re-submit the soft copy of the thesis after one month. The maximum number of re-submissions of thesis after plagiarism check is limited to TWO. The candidate has to register for the Dissertation work and work for two semesters. After three attempts, the admission is liable to be cancelled. The college authorities are advised to make plagiarism check of every soft copy of theses before submissions.
- Three copies of the Dissertation thesis certified by the supervisor shall be submitted to the College/School/Institute, after submission of a 2 research paper related to the dissertation work in a UGC care, SCOPUS or SCI journal. A copy of the submitted research paper shall be attached to thesis.
- The thesis shall be adjudicated by an external examiner selected by the University. For this, the Principal of the College/School/Institute shall submit a panel of three examiners from among the list of experts in the relevant specialization as submitted by the supervisor concerned and Head of the Department.
- If the report of the external examiner is unsatisfactory, the candidate shall revise and resubmit the Thesis. If the report of the examiner is unsatisfactory again, the thesis shall be summarily rejected. Subsequent actions for such dissertations may be considered, only on the specific recommendations of the external examiner and /or Dissertation work Review Committee. No further correspondence in this matter will be entertained, if there is no specific recommendation for resubmission.
- If the report of the examiner is satisfactory, the Head of the Department shall coordinate and make arrangements for the conduct of Dissertation Viva- Voce examination. The Dissertation VivaVoce examination shall be conducted by a board consisting of the

Supervisor, Head of the Department and the external examiner who adjudicated the Thesis, with an external marks of 250. The candidate has to secure a minimum of 50% of marks in Dissertation Evaluation (Viva-Voce) examination.

- If he fails to fulfill the requirements as specified in previous point he will reappear for the Viva-Voce examination only after three months. In the reappeared examination also, if he fails to fulfill the requirements, he will not be eligible for the award of the degree, unless he is asked to revise and resubmit his dissertation work by the board within a specified time period (within four years from the date of commencement of his first year first semester).
- The Dissertation Viva-Voce External examination marks must be submitted to the University on the day of the examination.