UNIVERSITY OF MADRAS

MASTER OF COMPUTER APPLICATIONS (MCA) DEGREE PROGRAMME

SYLLABUS WITH EFFECT FROM 2023-2024

Title of the Paper	**Cyber Security**		
Elective - III Theory	I Year & II Semester	Credit:3	435E2B

Course Objectives:

To understand the basics of Cybercrime and Computer forensics with protecting mechanism

To explore the working principles of WLAN, Email and Smartphone along with security mechanism and guidelines

To gain the ability to understand the importance of cyber investigations with its functioning role and learn the basics of Wi Fi and its security measures

To understand and learn the method of seize the digital evidence

To learn and analyze the concepts of digital forensics with cybercrime prevention techniques

Unit I: Introduction to cybercrime: Classification of cybercrimes – reasons for commission of cybercrime – malware and its type – kinds of cybercrime – authentication – encryption – digital signatures – antivirus – firewall – steganography – computer forensics – why should we report cybercrime – introduction counter cyber security initiatives in India – generating secure password – using password manager-enabling two-step verification – security computer using free antivirus.

Unit II: Tips for buying online: Clearing cache for browsers – wireless LAN-major issues with WLAN-safe browsing guidelines for social networking sites – email security tips – introduction-smartphone security guidelines – purses, wallets, smart phones – platforms, setup and installation-communicating securely with a smartphone.

Unit III: Cyber investigation roles**:** Introduction – role as a cybercrime investigator – the role of law enforcement officers – the role of the prosecuting attorney – incident response: introduction-post mortem versus live forensics – computer analysis for the hacker defender program-network analysis – legal issues of intercepting Wi-Fi transmission – Wi-Fi technology – Wi-Fi RF-scanning RF – eavesdropping on Wi-Fi – fourth amendment expectation of privacy in WLAN.

Unit IV: Seizure of digital information: introduction – defining digital evidence – digital evidence seizure methodology – factors limiting the wholesale seizure of hardware – other options for seizing digital evidence – common threads within digital evidence seizure – determining the most appropriate seizure method– conducting cyber investigations–demystifying computer/cyber crime – IP addresses – the explosion of networking – interpersonal communication.

Unit V: Digital forensics and analyzing data: introduction – the evolution of computer forensics– phases of digital forensics-collection – examination-analysis – reporting – Cyber crime prevention: Introduction – crime targeted at a government agency.

Text books:

1. Dr.JeetendraPande, **"**Introduction to Cyber Security" Published by Uttarakhand Open University, 2017.(Chapter: 1.2-6.4,9.3-12.2)
2. Anthony reyes, Kevin o'shea, Jim steele, Jon R. Hansen, Captain Benjamin R. Jean Thomas Ralph, "Cyber-crime investigations" - bridging the gaps between security professionals, law enforcement, and prosecutors, 2007.(Chapter: 4, 5, 6, 7, 8, 9,10)

Reference Books:

1. Sebastian Klipper," Cyber Security: Ein Einblick fur Wirtschaftswissenschaftler Fachmedien Wiesbaden,2015.
2. John G.Voller Black and Veatch, "Cyber Security" Published by John Wiley & Sons, Inc., Hoboken, New Jersey Published simultaneously in Canada ©2014.

Course Outcomes

On the successful completion of the course, students will be able to

CO1	Understand, describe, analyze and examine the basics of Cyber security concepts and its implementation in India.	K1-K6
CO2	Comprehend and demonstrate the security tips in browsers, WLAN, social networks, Email security and Smart phone. Apply the investigations in post mortem and Forensics.	K1-K6
CO3	Understand, apply and evaluate the various investigation roles and Wi Fi protecting mechanisms.	K1-K6
CO4	Understand, illustrate and evaluate the method of seize the digital information and evidences forensics data and evaluate the forensics reports.	K1-K6
CO5	Comprehend, apply and appraise the methods digital forensics with cybercrime prevention techniques.	K1-K6

K1- Remember, K2- Understand, K3- Apply , K4- Analyze, K5- Evaluate, K6- Create

Mapping with Programme Outcomes:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10
CO1	CO1	S	L	-	L	M	L	M	M	-
CO2	CO2	M	S	-	L	M	L	M	M	-
CO3	CO3	M	S	L	L	M	L	M	M	-
CO4	CO4	S	M	L	S	M	L	S	M	-
CO5	CO5	M	S	M	L	S	L	M	S	-

S- Strong; M-Medium; L-Low