SARVAJANIK UNIVERSITY
Sarvajanik College of Engineering and Technology
Master of Computer Applications

MCA Semester III

Subject Name: Cyber Security & Forensics **Subject Code:** MTCA14307

Type of course: Professional Elective Course

Prerequisite: Basic Knowledge of Algorithm, Internet, Cloud Computing, Social Networking, Web Application, Mobile Application, Relational Database Management System

Rationale: After studying this course, students will be able to understand the basic concepts of cyber security & Ethical hacking. The course knowledge will be helpful to develop technology that prevents hackers from accessing a network, website, or device.

Teaching and Examination Scheme:

TEACHING SCHEME				Theory Marks			Practical Marks		Total
L	T	P	C	TEE	CA1	CA2	TEP	CA3	
2	1	0	3	60	25	15	0	0	100

CA1: Continuous Assessment (assignments/projects/open book tests/closed book tests **CA2:** Sincerity in attending classes/class tests/ timely submissions of assignments/self-learning attitude/solving advanced problems **TEE:** Term End Examination **TEP:** Term End Practical Exam (Performance and viva on practical skills learned in course) **CA3:** Regular submission of Lab work/Quality of work submitted/Active participation in lab sessions/viva on practical skills learned in course

Content:

Sr. No.	Content	Teaching Hrs.	Module Weightage
1	**Introduction to Cybercrime:** Introduction, Classifications of Cybercrimes: E-Mail Spoofing, Spamming, Cyber defamation, Internet Time Theft, Newsgroup Spam/Crimes from Usenet Newsgroup, Industrial Spying/Industrial Espionage, Hacking, Online Frauds, Pornographic Offenses , Software	6	20%

	Piracy, Password Sniffing, Credit Card Frauds and Identity Theft. Cyber offenses: How Criminals Plan that attack, Categories of Cybercrime, How Criminals Plan the Attacks: Passive Attack, Active Attacks, Scanning/Scrutinizing gathered Information, Attack (Gaining and Maintaining the System Access), Social Engineering, Cyberstalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector and Cloud Computing.		
2	Cybercrime: Mobile and Wireless Devices Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era and Laptops.	**12**	**40%**
3	**For Tutorial** **Tools and Methods Used in Cybercrime** Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks. Phishing and Identity Theft: Introduction, Phishing, Identity Theft (ID Theft): Types of Identity Theft, Techniques of ID Theft, Identity Theft- Countermeasures, How to Protect your Online Identity.	**6**	
4	**Cybercrimes and Cybersecurity: The Legal Perspectives** Introduction, Why Do We Need Cyberlaws: The Indian Context, The Indian IT Act, Challenges to Indian Law and Cybercrime Scenario in India, Consequences of Not Addressing the Weakness in Information Technology Act , Amendments to the Indian IT Act, Cybercrime and Punishment, Cyberlaw, Technology and Students: Indian Scenario.	**12**	**40%**
5	**For Tutorial**	**9**	

	Understanding Computer Forensics Introduction, Historical Background of Cyberforensics, Digital Forensics Science, The Need for Computer Forensics, Cyberforensics and Digital Evidence, Forensics Analysis of E-Mail : RFC282, Digital Forensics Life Cycle, Chain of Custody Concept, Network Forensics, Approaching a Computer Forensics Investigation, Setting up a Computer Forensics Laboratory: Understanding the Requirements, Computer Forensics and Steganography, Relevance of the OSI 7 Layer Model to Computer Forensics, Forensics and Social Networking Sites: The Security/Privacy Threats, Challenges in Computer Forensics, Special Tools and Techniques, Forensics Auditing and Antiforensics.		

Suggested Specification table with Marks (Theory):

Distribution of Theory Marks					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
20	20	15	15	15	15

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create and above Levels (Revised Bloom's Taxonomy)

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Reference Books:

Sr no	**Title of book /article**	**Author(s)**	**Publisher and details like ISBN**	**Year of publication**	**Publication Edition**
1	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives	Nina Godbole, SunitBelpure,	Wiley ISBN: 9788126521791	2011	2nd Edition

2	The Web Application Hacker′s Handbook: Finding and Exploiting Security Flaws	DafyddStuttard	Wiley ISBN:978-1118026472	2011	2nd Edition
3	The Browser Hacker's Handbook Book	Wade Alcorn , Christian Frichot, Michele Orru,	Wiley ISBN:978-1118662090	2014	1st Edition

Course Outcomes:

Sr. No.	CO statement	Marks % Weightage
CO-1	Able to identify insights on how to apply Cyber Security, Ethical Hacking to solve interdisciplinary problems.	20%
CO-2	Able to learn various types of algorithms and its applications of Cyber Security and Ethical Hacking using forensic detection	40%
CO-3	Identify & Evaluate Information Security threats and vulnerabilities in Information Systems and apply security measures to real time scenarios	NA
CO-4	Identify common trade-offs and compromises that are made in the design and development process of Information Systems	40%
CO-5	Demonstrate the use of standards and cyber laws to enhance information security in the development process and infrastructure protection.	NA

Mapping with POs:

	PO 1	PO 2	PO 3	PO 4	PO 5	PO 6	PO 7	PO 8	PO 9	PO 10	PO 11	PO 12	PS O1	PS O2	PS O3
CO-1	3	3	2	3	3	2	1	2	3	2	0	3			
CO-2	3	3	2	2	3	2	1	2	3	2	0	3			

CO-3	3	3	2	0	3	2	1	2	3	2	0	3			
CO-4	3	3	0	1	2	0	0	0	2	0	0	3			
CO-5	3	3	0	3	2	0	0	1	1	1	0	3			
Rationale*															

Rationale*: Explaining why it is matching this particular program outcome

List of Open learning website:

- https://www.cyberdegrees.org/resources/free-online-courses/

List of Open Source Software:
NA

FOR LAB SESSIONS:
NA

List of Experiments:
NA

Major Equipment Needed:

NA