Program	Master of Computer Applications (Autonomous) (M.C.A (Autonomous))	**Semester - 3**
Type of Course	-	
Prerequisite		
Course Objective	-	

Teaching Scheme (Contact Hours)				Examination Scheme				
			Credit	Theory Marks		Practical Marks		Total Marks
3	-	-	3	50	50	-	-	100

***SEE** - Semester End Examination, **CIA** - Continuous Internal Assessment (It consists of Assignments/Seminars/Presentations/MCQ Tests, etc.)*

Course Content

T - Teaching Hours | **W** - Weightage

Sr.	Topics	T	W
1	**Introduction & Introduction to Cybercrime** **Introduction:** Implication and Scope of Cyber Security concepts and its Importance in Economic growth of Nation, Impact of the course on Societal Problems / Sustainable Solutions / National Economy, Career Perspective, Overview of the course in current Innovations and Research Trends. **Introduction to Cybercrime:** Introduction, Cybercrime: Definition and Origins of the word, Cybercrime and Information Security, who are Cybercriminals? Classifications of Cybercrimes. Categories of Cybercrime. How Criminals Plan Attacks? Social Engineering, Cyber stalking, Cybercafé and Cybercrimes, Botnets, Attack Vector.	9	20
2	**Tools and Methods used in Cybercrime** **Tools and Methods used in Cybercrime:** Introduction, Proxy Server and Anonymizers, Phishing, Password Cracking, Key loggers and Spyware, Virus and Worms, DOS and DDOS attack.	8	20
3	**Cyber Security Vulnerabilities and Cyber Security Safeguards** **Cyber Security Vulnerabilities and Cyber Security Safeguards:** Cyber Security Vulnerabilities Overview software, System administration, poor cyber security awareness. Cyber Security Safeguards-Overview, Access control, Audit, Authentication, Biometrics. Security policy and threat management.	8	20
4	**Intrusion Detection and Prevention** **Intrusion Detection and Prevention:** Intrusion, Physical Theft, Abuse of Privileges, Unauthorized Access by Outsiders, Malware Infection, Intrusion detection and prevention techniques Network-based Intrusion Detection Systems, Host-based Intrusion Prevention Systems.	8	20
5	**Network Defense tools** **Network Defense tools:** Firewalls and Packet Filters, Network Address Translation (NAT) and Port Forwarding, VPN. Digital Forensics Science: Need for Computer Cyber forensics and Digital Evidence, Digital Forensics Life cycle, Forensics of social networking sites. **Recap:** Summary of Cyber Security concepts	9	20
	Total	42	100

Course Outcomes

At the end of this course, students will be able to:	
CO1	Explore the Cyber Security principles.
CO2	Apply the cyber security concepts to secure from cyber-attacks.
CO3	Formulate the possibilities of cyber-attacks in a given use case, as a penetration tester.
CO4	Analyze cyber security tools to protect individual data.
CO5	Apply Digital Forensic tools to address cyber security issues.