MCA (Master of Computer Applications)
MCA (Master of Computer Applications) Semester II

Course Code	PS02EMCA57	Title of the Course	CYBER SECURITY
Total Credits of the Course	4	Hours per Week	4

Course Objectives:	1. Understanding of the concepts of Cyber crimes, cyber security. 2. Learning how to avoid becoming victims of cyber crimes. 3. Preparing for a platform to the students who wish to seek career or research in cyber security. 4. Acquiring knowledge of security risk related to data and information. 5. Understanding of the tools and methods to protect systems from cyber attacks.

Course Content		
Unit	Description	Weightage* (%)
1.	**Introduction to Cybercrime** - Cybercrime : Definition And Origins Of The World - Cybercrime And Information Security - Who Are Cybercriminals? - Classifications Of Cybercrimes - Cybercrime: The Legal Perspectives - Cybercrimes: An Indian Perspectives - Cybercrime And The Indian ITA-2000 - Cyber Offenses: How Criminals Plan The Attacks - Social Engineering - Cyberstalking - Botnets	25
2.	**Tools and Methods Used in Cybercrime** - Password Cracking - Key Loggers And Spywares - Virus And Worms - Trojan Horses And Backdoors - DoS And DDoS Attacks - SQL Injection - Buffer Overflow - Phishing - Identity Theft	25

	- Networking Commands	
3.	**Cryptography** - Security Services: Confidentiality, Authentication, Integrity, - Non-repudiation, Access Control, Availability - Symmetric Key Algorithms (DES & AES) - Asymmetric Key Algorithms (RSA) - Digital Signature & Message Digest - Digital Certificate	25
4.	**Computer Forensics & Forensics of Hand-Held Devices** - The Need For Computer Forensics - Digital Forensics Life Cycle - Forensics And Social Networking Sites: The Security/Privacy - Threats - Technical Challenges In Computer Forensics - Hand-Held Devices And Digital Forensics - Forensic Tools	25

Teaching-Learning Methodology	Blended learning approach incorporating traditional classroom teaching as well as online / ICT-based teaching practices

Evaluation Pattern		
Sr. No.	Details of the Evaluation	Weightage
1.	Internal Written / Practical Examination (As per CBCS R.6.8.3)	15%
2.	Internal Continuous Assessment in the form of Practical, Viva-voce, Quizzes, Seminars, Assignments, Attendance (As per CBCS R.6.8.3)	15%
3.	University Examination	70%

Course Outcomes: Having completed this course, the learner will be able to	
1.	understand cyber security concepts.
2.	show knowledge of latest security issues and solutions.
3.	have expertise in cyber security.

Suggested References:	
Sr. No.	References
1.	Nina Godbole, SunitBelpure, "Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley, 1st Edition, 2011.
2.	Andrew S Tanenbaum, David. J. Wetherall, "Computer Networks", Pearson Education, 5th Edition, 2011.
3.	Bruce Schneier Applied Cryptography: Protocols, Algorithms, and Source Code in C, 20th Anniversary Edition, John Wiley & Sons, 2015.
4.	Behrouz A. Forouzan, "Cryptography and Network Security", TMH, 2nd Edition, 2007.
5.	WilliamStallings,Network Security Essentials Applications and Standards,Pearson, 5th Edition, 2014.
6.	Charles P. Pfleeger; Shari LawrencePfleeger, Security in Computing, Prentice Hall,, Fifth Edition, 2015.
7.	Mike Shema, Anti-Hacker Tool Kit (Indian Edition), Mc Graw Hill, 2014.

*****