CENTRAL UNIVERSITY OF KERALA
DEPARTMENT OF COMPUTER SCIENCE
M.Sc. COMPUTER SCIENCE – PROGRAMME STRUCTURE

ELECTIVES					
COURSE CODE	COURSE TITLE	CONTACT HRS/WEEK			CREDITS
		LEC	LAB	TUT	
CSC5017	Cyber Security	2	2	1	4

Lec = Lecture, Tut = Tutorial, Lab = Practical

This is a participatory, problem solving, experimental and **employability based skill development course**.

Course Objective:
The objective of the course is to provide theoretical and practical aspects of cyber security.

By completing this course, students will obtain the following course/learning outcomes:
1. Knowledge gained:
   (i) cyber security issues, tools and techniques that are critical in solving problems in cyber security domains
   (ii) perspective to information security based on national security policy, IT policy and cyber law
2. Skill gained:
   (iii) analysing and monitoring potential threats and attacks, devising security architecture and implementing security solutions
3. Competency gained:
   (iv) Identify and evaluate information security threats by applying security measures in model based scenarios.

Prerequisites: Basic knowledge in computer networks

Grading:

Lab implementation	– 20%
Participatory based group Project	– 10%
Assignment/Quiz/presentation	– 5%
Lab Test	– 5%
Final Exam	– 60%

CSC5017 – Cyber Security

Module-1
Cyber Security Concepts: CIA, Risks, Breaches, Threats, Attacks, Exploits. Information Gathering (Social Engineering, Foot Printing & Scanning). Open Source/ Free/ Trial Tools: nmap, zenmap, Port Scanners, Network scanners.

Infrastructure and Network Security: Introduction to System Security, Server Security, OS Security, Physical Security, Cyber-Physical System, Network packet Sniffing, DOS/ DDOS attacks. Intrusion detection and Prevention Techniques, Host based Intrusion prevention Systems, Network Session Analysis. Open Source/ Free/ Trial Tools: DOS Attacks, DDOS attacks, Wireshark, Cain & abel, iptables/ Windows Firewall, Snort, Suricata, fail2ban

Module-2
Cyber Security Vulnerabilities: Internet Security, Cloud Computing & Security, Social Network sites security, Cyber Security Vulnerabilities.

Cyber Security Safeguards: Overview, Access control, IT Audit, Authentication. Open Web Application Security Project (OWASP), Web Site Audit and Vulnerabilities assessment. Open Source/ Free/ Trial Tools: WinAudit, Zap proxy (OWASP), burp suite, DVWA kit.

Module-3
Malware: Explanation of Malware, Types of Malware: Virus, Worms, Trojans, Rootkits, Robots, Adware‘s, Spywares, Ransom wares, Zombies etc., OS Hardening (Process Management, Memory Management, Task Management, Windows Registry/ services another configuration), Malware Analysis. Open Source/ Free/ Trial Tools: Antivirus Protection, Anti Spywares, System tuning tools, Anti Phishing.

Module-4
Cyber Laws: Introduction, Cyber Security Regulations, Roles of International Law, the state and Private Sector in Cyberspace, Cyber Security Standards. The INDIAN Cyberspace, National Cyber Security Policy 2013.

Cyber Forensics: Introduction to Cyber Forensics, Need of Cyber Forensics, Cyber Evidence, Documentation and Management of Crime Sense, Image Capturing and its importance, Partial Volume Image, Web Attack Investigations, Denial of Service Investigations, Internet Crime Investigations, Internet Forensics, Steps for Investigating Internet Crime, Email Crime Investigations.

Open Source/ Free/ Trial Tools: Case Studies related to Cyber Law, Common Forensic Tools like dd, md5sum, sha1sum, Ram dump analysis, USB device

Text Book/References

1. William Stallings, ―Cryptography and Network Security, Pearson Education, 7th Edition, 2017.
2. V.K. Jain, ―Cryptography and Network Security, Khanna Publishing House, 1st Edition, 2020.
3. Sarika Gupta, Gaurav Gupta ―Information Security and Cyber Laws, Khanna Publishing House, 2019
4. Atul Kahate, ―Cryptography and Network Security, McGraw Hill, 4th Edition, 2019.
5. V.K. Pachghare, ―Cryptography and Information Security, PHI Learning, 3rd Edition, 2019.
6. Nina Godbole, Sunit Belapure ―Cyber Security, Wiley India Pvt Ltd, 2011.
7. Bothra Harsh, ―Mastering Hacking, Khanna Publishing House, Delhi, 2019.
8. Rajeev Alur, ―Principles of Cyber-Physical Systems, MIT Press, 2015.