

UNIVERSITY OF MUMBAI



Syllabus for Sem V & VI
Program: Bachelor of Science
Course: Computer Science

Credit Based Semester and Grading System with
effect from
Academic Year 2018-2019

Preamble

This is the third year curriculum in the subject of Computer Science. The revised structure is designed to transform students into technically competent, socially responsible and ethical Computer Science professionals. In these Semesters we have made the advancements in the subject based on the previous Semesters Knowledge.

In the first year basic foundation of important skills required for software development is laid. Second year of this course is about studying core computer science subjects. The third year is the further advancement which covers developing capabilities to design formulations of computing models and its applications in diverse areas.

The proposed curriculum contains two semesters, each Semester contains two Electives: Elective-I and II. Every Elective contains three papers based on specific areas of Computer Science. It also includes one Skill Enhancement paper per semester, helps the student to evaluate his/her computer science domain specific skills and also to meet industry expectations. This revised curriculum has not only taken the specific areas of computer science into consideration but will also give the opportunity to the student to prove his/her ability in the subject practically through the Project Implementation. In Semester V and Semester VI student has to undertake a Project. It can boost his/her confidence and also can encourage the student to perform innovations in the subject as the choice of the Project topic is kept open covering most of the areas of Computer Science subject as per the students interest and the subject they have learned during the Course.

Proposed Curriculum contains challenging and varied subjects aligned with the current trend with the introduction of Machine Intelligence specific subject such as Artificial Intelligence, Information Retrieval. Data Management related subjects such as Cloud Computing and Data Science. Image processing topics such as Game Programming, Digital Image Processing. Introduction of physical world through Architecting of IoT and Wireless Sensor Networks and Mobile Communication. Security domain is also evolved by the introduction of Ethical Hacking, Cyber Forensic and Information and Network Security. To get the hands on experience Linux Server Administration and Web Services topics are included.

In essence, the objective of this syllabus is to create a pool of technologically savvy, theoretically strong, innovatively skilled and ethically responsible generation of computer science professionals. Hope that the teacher and student community of University of Mumbai will accept and appreciate the efforts.

T.Y.B.Sc. (Semester V and VI)
Computer Science Syllabus
Credit Based Semester and Grading System
To be implemented from the Academic year 2018-2019

SEMESTER V			
Course	TOPICS	Credits	L / Week
	Elective-I (Select Any Two)		
USCS501	Artificial Intelligence	3	3
USCS502	Linux Server Administration	3	3
USCS503	Software Testing and Quality Assurance	3	3
	Elective-II (Select Any Two)		
USCS504	Information and Network Security	3	3
USCS505	Architecting of IoT	3	3
USCS506	Web Services	3	3
	Skill Enhancement		
USCS507	Game Programming	2	3
	Practical		
USCSP501	Practical of Elective-I	2	6
USCSP502	Practical of Elective-II	2	6
USCSP503	Project Implementation	1	3
USCSP504	Practical of Skill Enhancement : USCS507	1	3

SEMESTER VI			
Course	TOPICS	Credits	L / Week
	Elective-I (Select Any Two)		
USCS601	Wireless Sensor Networks and Mobile Communication	3	3
USCS602	Cloud Computing	3	3
USCS603	Cyber Forensics	3	3
	Elective-II (Select Any Two)		

USCS604	Information Retrieval	3	3
USCS605	Digital Image Processing	3	3
USCS606	Data Science	3	3
	Skill Enhancement		
USCS607	Ethical Hacking	2	3
	Practical		
USCSP601	Practical of Elective-I	2	6
USCSP602	Practical of Elective-II	2	6
USCSP603	Project Implementation	1	3
USCSP604	Practical of Skill Enhancement : USCS607	1	3

SEMESTER VI

THEORY

Course: USCS607	TOPICS (Credits : 02 Lectures/Week: 03) Ethical Hacking	
Objectives: To understand the ethics, legality, methodologies and techniques of hacking.		
Expected Learning Outcomes: Learner will know to identify security vulnerabilities and weaknesses in the target applications. They will also know to test and exploit systems using various tools and understand the impact of hacking in real time machines.		
Unit I	<p>Information Security : Attacks and Vulnerabilities</p> <p>Introduction to information security : Asset, Access Control, CIA, Authentication, Authorization, Risk, Threat, Vulnerability, Attack, Attack Surface, Malware, Security-Functionality-Ease of Use Triangle</p> <p>Types of malware : Worms, viruses, Trojans, Spyware, Rootkits</p> <p>Types of vulnerabilities : OWASP Top 10 : cross-site scripting (XSS), cross site request forgery (CSRF/XSRF), SQL injection, input parameter manipulation, broken authentication, sensitive information disclosure, XML External Entities, Broken access control, Security Misconfiguration, Using components with known vulnerabilities, Insufficient Logging and monitoring, OWASP Mobile Top 10, CVE Database</p> <p>Types of attacks and their common prevention mechanisms : Keystroke Logging, Denial of Service (DoS /DDoS), Waterhole attack, brute force, phishing and fake WAP, Eavesdropping, Man-in-the-middle, Session Hijacking, Clickjacking, Cookie Theft, URL Obfuscation, buffer overflow, DNS poisoning, ARP poisoning, Identity Theft, IoT Attacks, BOTs and BOTNETs</p> <p>Case-studies : Recent attacks – Yahoo, Adult Friend Finder, eBay, Equifax, WannaCry, Target Stores, Uber, JP Morgan Chase, Bad Rabbit</p>	15L
Unit II	<p>Ethical Hacking – I (Introduction and pre-attack)</p> <p>Introduction: Black Hat vs. Gray Hat vs. White Hat (Ethical) hacking, Why is Ethical hacking needed?, How is Ethical hacking different from security auditing and digital forensics?, Signing NDA, Compliance and Regulatory</p>	15L

	<p>concerns, Black box vs. White box vs. Black box, Vulnerability assessment and Penetration Testing.</p> <p>Approach : Planning - Threat Modeling, set up security verification standards, Set up security testing plan – When, which systems/apps, understanding functionality, black/gray/white, authenticated vs. unauthenticated, internal vs. external PT, Information gathering, Perform Manual and automated (Tools: WebInspect/Qualys, Nessus, Proxies, Metasploit) VA and PT, How WebInspect/Qualys tools work: Crawling/Spidering, requests forging, pattern matching to known vulnerability database and Analyzing results, Preparing report, Fixing security gaps following the report</p> <p>Enterprise strategy : Repeated PT, approval by security testing team, Continuous Application Security Testing,</p> <p>Phases: Reconnaissance/foot-printing/Enumeration, Phases: Scanning, Sniffing</p>	
<p>Unit III</p>	<p>Ethical Hacking :Enterprise Security</p> <p>Phases : Gaining and Maintaining Access : Systems hacking – Windows and Linux – Metasploit and Kali Linux, Keylogging, Buffer Overflows, Privilege Escalation, Network hacking - ARP Poisoning, Password Cracking, WEP Vulnerabilities, MAC Spoofing, MAC Flooding, IPspoofing, SYN Flooding, Smurf attack, Applications hacking : SMTP/Email-based attacks, VOIP vulnerabilities, Directory traversal, Input Manipulation, Brute force attack, Unsecured login mechanisms, SQL injection, XSS, Mobile apps security,</p> <p>Malware analysis : Netcat Trojan, wrapping definition, reverse engineering</p> <p>Phases : Covering your tracks : Steganography, Event Logs alteration</p> <p>Additional Security Mechanisms : IDS/IPS, Honeypots and evasion techniques, Secure Code Reviews (Fortify tool, OWASP Secure Coding Guidelines)</p>	<p>15L</p>
<p>Textbook(s):</p> <ol style="list-style-type: none"> 1) Certified Ethical Hacker Study Guide v9, Sean-Philip Oriyano, Sybex; Study Guide Edition,2016 2) CEH official Certified Ethical Hacking Review Guide, Wiley India Edition, 2007 		

Additional Reference(s):

- 1) Certified Ethical Hacker: Michael Gregg, Pearson Education, 1st Edition, 2013
- 2) Certified Ethical Hacker: Matt Walker, TMH, 2011
- 3) http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines
- 4) https://www.owasp.org/index.php/Category:OWASP_Top_Ten_2017_Project
- 5) https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10
- 6) https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents
- 7) https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide
- 8) <https://cve.mitre.org/>
- 9) <https://access.redhat.com/blogs/766093/posts/2914051>
- 10) <http://resources.infosecinstitute.com/applications-threat-modeling/#gref>
<http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html>

Suggested List of Practical – SEMESTER VI

Course:	(Credits : 02 Lectures/Week:06)	
USCSP604	Practical of Skill Enhancement	
USCS607 : Ethical Hacking		
<ol style="list-style-type: none"> 1. Use Google and Whois for Reconnaissance 2. a) Use CrypTool to encrypt and decrypt passwords using RC4 algorithm b) Use Cain and Abel for cracking Windows account password using Dictionary attack and to decode wireless network passwords 3. a) Run and analyze the output of following commands in Linux – ifconfig, ping, netstat, traceroute b) Perform ARP Poisoning in Windows 4. Use NMap scanner to perform port scanning of various forms – ACK, SYN, FIN, NULL, XMAS 5. a) Use Wireshark (Sniffer) to capture network traffic and analyze b) Use Nemesy to launch DoS attack 6. Simulate persistent cross-site scripting attack 7. Session impersonation using Firefox and Tamper Data add-on 8. Perform SQL injection attack 9. Create a simple keylogger using python 10. Using Metasploit to exploit (Kali Linux) 		

Scheme of Examination

1. Theory:

I. Internal 25 Marks :

a) Test – 20 Marks

20 marks Test – Duration 40 mins

It will be conducted either using any open source learning management system like Moodle (Modular object-oriented dynamic learning environment)

OR

A test based on an equivalent online course on the contents of the concerned course (subject) offered by or build using MOOC (Massive Open Online Course) platform.

b) 5 Marks – Active participation in routine class instructional deliveries

Overall conduct as a responsible student, manners, skill in articulation, leadership qualities demonstrated through organizing co-curricular activities, etc.

II. External 75 Marks as per University Guidelines

11. Practical and Project Examination:

There will be separate Practical examination for Elective-I, II, Skill enhancement and project of these Elective-I 100, Elective-II: 100 and Skill Enhancement: 50 and Project Implementation: 50.

In the Practical Examination of Elective-I and II, the student has to perform practical on each of the subjects chosen. The Marking Scheme for each of the Elective is given below:

	Subject Code	Experiment-I	Experiment-II	Total Marks
Elective-I	USCSP501/ USCSP601	Experiment-40+Journal-5 +viva-5 Total:50M	Experiment-40+Journal-5+viva-5 Total:50M	100 M
Elective-II	USCSP502/ USCSP602	Experiment-40+Journal-5 +viva-5 Total:50M	Experiment-40+Journal-5+viva-5 Total:50M	100 M

Project Implementation	USCSP503/ USCSP603	**Project Evaluation Scheme	50M
Skill Enhancement	USCSP504/ USCSP604	Experiment-40+Journal:5+viva-5 Total-50M	50M
Total Marks			300M

(Certified Journal is compulsory for appearing at the time of Practical Examination)

****Project Evaluation Scheme:**

Presentation	Working of the Project	Quality of the Project	Viva	Documentation
10Marks	10 Marks	10 Marks	10 Marks	10Marks

(Certified Project Document is compulsory for appearing at the time of Project Presentation)
