Course: MCA (A.Y.-II) 2020 **Semester:** 2

Prerequisite: Fundamental knowledge of computer network.

Rationale: The key objectives of this course are to develop an understanding of information assurance as practiced in computer operating systems, networks and representative applications and to gain familiarity with prevalent attacks, defenses against them.

Teaching and Examination Scheme

Teaching Scheme					Examination Scheme					Total
Lecture Hrs/Week	Tutorial Hrs/Week	Lab Hrs/Week	Hrs/	Credit	Internal Marks			External Marks		
					T	CE	P	T	P	
3	1	2	-	5	20	20	20	60	30	150

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

Course Content

W - Weightage (%) , **T** - Teaching hours

Sr.	Topics	W	T
1	**Security Principles and Practices** Information security, Network security Model, Cryptography, Attacks on Cryptosystem, Traditional Cryptography, Modern cryptography methods (block cipher & stream cipher), Symmetric & Asymmetric Key Encryption, Feistel Cipher, DES- Data Encryption Standards, 3DES, AES- Advanced Encryption Standards,Block Cipher modes , Introduction to Public key encryption, Public key infrastructure, RSA algorithm, Model and Introduction to Hash, MAC and Digital Signature	15	9
2	**Security Threats** Types of security threats- worms, viruses, Trojan horse, malware, malicious spyware, adware, botnet, spam, phishing, stack and buffer overflow	8	3
3	**Operating System Security** Role of operating systems in information systems applications, Operating systems security, Patched operating systems, Protected objects and methods of protection, Memory address protection, File protection mechanism.	10	4
4	**Wireless Networks Security** Overview of wireless technology, Wireless security protocols -Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, Attacks on wireless networks.	10	4
5	**Understanding Cyber Forensics** Computer forensics, Cyber forensics and Digital evidence, Rules of evidence, Forensics analysis of e-mail- RFC282, Digital forensics life cycle, Chain of custody concept, Network forensics, Setting up a computer forensics laboratory, Computer forensics and steganography, Rootkits, Information hiding, Relevance of the OSI layer model to computer forensics, Forensics and social networking sites - security, privacy, threats.	15	9
6	**Challenges in Cyber Forensics** Technical challenges - understanding the raw data and its structure, Legal challenges in computer forensics and data privacy issues, Special tools and techniques - digital forensics tools, Special technique - data mining used in cyber forensics, Forensics auditing, Anti forensics.	10	5
7	**Forensics of Hand-Held Devices** Introduction, Hand-held devices and digital forensics -mobile phone, Personal Digital Assistant (PDA), printer, scanner, smart phone, iPhone, Challenges in forensics of the Digital images/still camera, Forensics of the BlackBerry wireless device, Toolkits for hand-held device forensics - EnCase, device seizure and PDA seizure, Palm DD, Cell seizure, MOBILedit, Forensic SIM, Organizational guidelines on cell phone forensics – hand-held forensics as the specialty domain in crime context.	12	6
8	**Concept of Virtualization** Software Virtualization, Hardware Virtualization, OS Partitioning, VM Ware Windows, Linux	10	4
9	**Introduction to kali linux / Santoku** Digital Forensics Tools : Autopsy,Mobile forensics: (ADB) DIVA.apk	10	4

Reference Books

1.	**Information systems security (TextBook)** By Nina Godbole | Wiley Publications,2008
2.	**Cyber Security understanding Cyber Crimes, Computer forensics and Legal Perspectives (TextBook)** By Nina Godbole and Sunit Belapure
3.	**Cryptography and Network Security Principles and Practices** By W. Stallings | Prentice-Hall of India, 2006 | 4th Edition
4.	**Information Security: Principles and Practices** By M. Merkow and J. Breithaupt | Pearson Education, 2006

Course Outcome

After Learning the Course the students shall be able to:

1. Recognize significance of information system security in terms of threats and attacks.
2. Infer the impact of operating system security.
3. Identify various approaches for improvement of security aspects in operating system and wireless networks protocol.
4. Explain significance of cyber forensics and digital evidence.
5. Describe current techniques and tools for cyber forensic examination.

List of Practical

1.	**Configuration of Virtual Laboratory for Mobile Forensic and Pen Testing, Configuration of Genymotion in virtual machine, Configuration of Santoku OS in virtual machine, Configuration of Appie.**
2.	**Use various functionality of ADB, Starts two instances of Emulator in Gynemotion, Connect adb through Santoku and Appie and perform, and its commands.**
3.	**Configuration of target vulnerable mobile application, DIVA (Damn insecure and vulnerable App), OWASP GoatDroid**
4.	**Understanding of Android Application architecture using santoku / Unzipping Archive android application file**
5.	**Reversing Engineering of Android Application using APKtools and JaDX Decompiler which a part of Santoku APKTool**
6.	**Practical related to the analysis of Dex file using Dexdump**
7.	**Practical related to insecure logging**

Miscellaneous

Useful Links

https://sites.google.com/a/paruluniversity.ac.in/information-security-and-cyber-forensics/home/academic- docs