

Guidelines for

GE 4: INFORMATION SECURITY & CYBER LAWS

TOPIC	Reference
Course Introduction: Computer network as a threat, hardware vulnerability, software vulnerability, importance of data security.	[1] 1.1-1.3 (pgs 1-18) [1] 7.2 (only Categories of Attack, pgs 424-425)
Introduction to Cryptography and Applications : Important terms, Threat, Flaw, Vulnerability, Exploit, Attack, Ciphers, Codes, Caesar Cipher, Rail-Fence Cipher, Asymmetric and symmetric key cryptography	[1] 2.1(Only introduction, Terminology, definitions, exclude algorithm: pgs 36-40) [1] 2.2(including Advantages and Disadvantages of the Caesar Cipher: pgs42-43) [1] 2.3 (pgs 53-54) [1] 2.7 (only definitions on pg 92, pg 93- Table only) [1](pg 121-Sidebar 3.1 only, pg 122)
Risk Analysis and Threat: Risk analysis, process, key principles of conventional computer security, security policies, authentication, data protection, access control, internal vs external threat, passwords, authentication, and access control, computer forensics and incident response	[1] 8.2 (pg568-570) [1] 8.3 (pg591-597) [1] 4.5 (pg242, 244-245 till two-factor authentication, 252-254till definition of OTP) [1] Incident Response Plan (pg 565-566introduction only)
Information Gathering Techniques: Tools of the attacker, scanning and spoofing, password cracking, malicious software, session hijacking	[1] Sec 3.3 (pg 133-138,includingKinds of malicious code) [2] Ch3 (pg46Introduction) [2] Ch 6 (pg 127 introduction of password crackers) [2] Ch7 (pg 138) [2] Ch8 (pg 158session hijacking introduction)
Safety Tools and Issues : Firewalls, logging and intrusion detection systems, Windows and windows XP / NT security, Unix/Linux security, ethics of hacking and cracking	[1] What is Firewall (pgs 514, 518), What Firewalls Can-and-Cannot-Block, IDS definition (pgs 526-527) [1] Difference between the Law and Ethics (pg 739) [1] Crackers or Malicious Hackers (pg 20), Classification of Hackers (pg 24) [2] Ch 16 (Vulnerabilities in Windows Pgs313-315till File Sharing) [2] Ch 17 (VulnerabilitiesPgs323-324till Login Passwords)
Digital Crime: Overview of digital crime, criminology of computer crime. Cyber Forensics	[3] Chapter 1 (Sec 1.1, 1.2, 1.4, 1.5, 1.7)
Cyber laws to be covered as per IT 2008: Definitions, Digital Signature And Electronic Signature [Section 43] [Section 65] [Section 66 A] [Section 66 B] [Section 66C] [Section 66D] [Section 66E] [Section 66F] [Section 67] [Section 67A] [Section 67B] [Section 72A]	[3] Digital Signature (pg 2.21), Electronic Signature (pg 2.22) [3] (pgs 4.19-4.21), (pgs 4.39-4.49), (pgs 4.54) [3] Corresponding case laws given in Ch 5 (<i>Case Laws for discussion only, not mandatory for examination</i>)

**** In reference [1], exclude all Sidebars except Sidebar 3.1**

Reference Books:

[1]Charles P. Pfleeger, Shari Lawrence Pfleeger, Security in Computing,4th Edition, Pearson

[2] A. Basta, N. Basta, and M. Brown, Computer Security and Penetration Testing, 2nd Edition, Cengage Learning India

[3] Sushila Madan, Cyber Crimes and Laws, Scholar Tech Press (MKM Publishers Pvt. Ltd) Second Revised Edition, 2017

Suggested Reading:

Sushma Arora, Raman Arora, Cyber Crimes and Laws, Taxmann, January 2017 Edition

Information Security and Cyber Laws Lab

Practical: 60 lectures

1. Demonstrate the use of Network tools: ping, ipconfig, ifconfig, tracert, arp, netstat, whois

Suggested Reading: whois, ping, tracert, netstat, ifconfig: [2] (pgs 31-33, 36-39, 86)

2. Use of Password cracking tools: John the Ripper, Ophcrack. Verify the strength of passwords using these tools.

Suggested Reading: [2] Chap 6 (John the Ripper)

3. Perform encryption and decryption of Caesar cipher. Write a script for performing these operations.

4. Perform encryption and decryption of a Rail fence cipher. Write a script for performing these operations.

5. Use nmap/zenmap to analyse a remote machine.

Suggested Reading: [2] Chap 3 (Nmap)

6. Use Burp proxy to capture and modify the message.
7. Demonstrate sending of a protected word document.
8. Demonstrate sending of a digitally signed document.
9. Demonstrate sending of a protected worksheet.