

Curriculum Planner (Department of Computer Science)

Course: GE 3
Semester: IV
Paper: Information Security and Cyber Laws
Teacher Name: - Dr. Sushil Malik

Topic	References	Schedule(Aproximate)
Unit 1: Definitions :Protection, Security, risk, threat, vulnerability, exploit, attack, confidentiality, integrity, availability,non-repudiation,authentication , authorization, codes, plain text,encryption, decryption, cipher text, key, ciphers, Symmetric and asymmetric cryptography, Public key , private key ,Crypt analysis,, Cyber forensics. Substitution cipher (Caesar), Transposition cipher (Rail-Fence),	[3] Ch1 (Pg 10-18) [3] Ch8 (Pg 450-451,454-456,459-460,467-468,470-471) [3] Pg 330 [For definition of authorization]	January 2023
Unit 2: Risk analysis, process, key principles of conventional computer security, security policies, data protection, access control, internal vs external threat, security assurance , passwords, access control, computer forensics and incident response.	[1] Ch 10 (Pg 233-243 (Till Single sign-on)) [1] Ch 4 (Pg 87-109) [A2] Pg 565-568 [A3] Pg 1.13	
Unit 3: CYBER ATTACKS (definitions and examples): Denial-of-service attacks, Man-in-the middleattack, Phishing, spoofing and spam attacks, Drive-by attack, Password attack, SQL injection attack, Cross-site scripting attack, Eavesdropping attack, Birthday attack, Malware attacks, Social Engineering attacks Assignment, Test	https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/	February 2023
Unit 4: <i>Brief Introduction of handling the attacks described in UNIT 3.</i> Firewalls, logging and intrusion detection systems, e-mail security, security issues in operating systems, ethics of hacking and cracking. Quizzes,PPT	[A2] 514-527 (except table 7-7), 527-533 (Types of IDS Introductiononly) , (535-539). (739) [A1] (pg. 1-7, 10-12(Excluding venderspecific Certificate)) https://www.tutorialspoint.com/operating_system/os_security.htm	March 2023
Unit 5: Definitions: <i>Digital Signature and ElectronicSignature, Digital Certificate</i> i.[Section 43] Penalty and compensation for damage to computeretc. ii.[Section 65] Tampering with computer source documents iii.[Section 66A] Punishment for sending offensive messages through communication service etc. iv.[Section 66B] Punishment for dishonestly receiving stolen computer resource or communication device	[A3] 4.11-21, 4.40-49, 4.54 [3] (pg. 477-480) https://www.indiacode.nic.in/handle/123456789/1999?sam_handle=123456789/1362	April 2023

<p>v.[Section 66C] Punishment for identity theft vi.[Section 66D] Punishment for cheating by impersonation by using computer resource vii.[Section 66E] Punishment for violation of privacy viii.[Section 66F] Punishment for cyber terrorism ix.[Section 67] Punishment for publishing or transmitting obscene material in electronic form x.[Section 67A] Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form xi.[Section 67B] Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form xii.[Section 72] Breach of confidentiality and privacy</p>		
<p>Unit 6: Brief introduction of IT infrastructure in India, National agencies handling IT</p> <p>Revision, Doubt solving, Mock Practical</p>	<p>https://digitalindia.gov.in/infrastructure</p> <ul style="list-style-type: none"> • Aadhaar • BHARAT BROADBAND NETWORK (BBNL), • CENTRE FOR EXCELLENCE FOR INTERNET OF THINGS (COE-IT) • COMMON SERVICE CENTRES (CSCS), • CYBER SWACHHTA KENDRA, • DIGILOCKER • DIGITAL SAKSHARTA ABHIYAAN (DISHA) • DIGITIZE INDIA PLATFORM • EBASTA,ESIGN • GOVERNMENT E-MARKETPLACE, INTEGRATED HEALTH INFORMATION SYSTEM (IHIP) • MEGHRAJ • MOBILE SEVA APP STORE • NATIONAL SUPER COMPUTING • MISSION (NSM),OPEN DATA 	

References:

- [1]. Merkow, M., & Breithaupt, J.(2005) Information Security Principles and Practices. 5th edition. Prentice Hall.
- [2]. Snyder, G.F. (2010). Network Security, Cengage Learning.
- [3]. Whitman, M. E. & Mattord, H. J. (2017) Principles of Information Security. 6th edition. Cengage Learning.

Additional Resources:

- [A1]. Basta, A., & Halton, W., (2010) Computer Security: Concepts, Issues and Implementation, Cengage Learning India.
- [A2] Charles P. Pfleeger, Shari Lawrence Pfleeger, Security in Computing, 4 th Edition,
- [A3] Sushila Madan, Cyber Crimes and Laws, Scholar Tech Press (MKM Publishers Pvt. Ltd) Second Revised Edition,

2017

Online Resources:

- [1]. <https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/>
- [2]. <https://www.ibef.org/industry/infrastructure-sector-india.aspx>
- [3]. <https://www.ibm.com/in-en/topics/infrastructure>
- [4]. <https://business.mapsofindia.com/india-budget/infrastructure/it.html>
- [5]. <https://nasscom.in/knowledge-center/publications/it-infrastructure-services-digital-era>
- [6]. <https://digitalindia.gov.in/infrastructure>
- [7]. <https://techdifferences.com/difference-between-digital-signature-and-digital-certificate.html>
- [8]. <https://techdifferences.com/difference-between-digital-signature-and-electronic-signature.html>