Home

Savitribai Phule Pune University
Third Year of Artificial Intelligence and Data Science (2019 Course)
317530: Cyber Security

Teaching Scheme:	Credit	Examination Scheme:
TH: 04 Hours/Week##	03	Mid_Semester(TH): 30 Marks End_Semester(TH): 70 Marks

Prerequisite Courses, if any: **Computer Networks (317521)**

Companion Course, if any: **Mini Project (317536)**

Course Objectives:

- To offer an understanding of principle concepts, central topics and basic approaches in information and cyber security.
- To know the basics of cryptography.
- To acquire knowledge of standard algorithms and protocols employed to provide confidentiality, integrity and authenticity.
- To enhance awareness about Personally Identifiable Information (PII), Information Management, cyber forensics.

Course Outcomes:

On completion of the course, learner will be able to–

CO1: Gauge the security protections and limitations provided by today's technology.
CO2: Identify cyber security threats.
CO3: Analyze threats in order to protect or defend it in cyberspace from cyber-attacks.
CO4: Build appropriate security solutions against cyber-attacks

Course Contents

Unit I	Introduction	(06 Hours)
Introduction, Elements of Information Security, Security Policy, Techniques, Steps, Categories, Operational Model of Network Security, Basic Terminologies in Network Security. Threats and Vulnerability, Difference between Security and Privacy.		
#Exemplar/Case Studies	**Case study on cyber attacks**	
Mapping of Course Outcomes for Unit I	C01, C02	
Unit II	**Data Encryption Techniques And Standards**	**(08 Hours)**
Introduction, Encryption Methods: Symmetric, Asymmetric, Cryptography, Substitution Ciphers. Transposition Ciphers, Stenography applications and limitations, Block Ciphers and methods of operations, Feistal Cipher, Data Encryption Standard (DES), Triple DES, Weak Keys in DES Algorithms, Advance Encryption Standard (AES).		
#Exemplar/Case Studies	Symmetric encryption algorithm case study	
Mapping of Course Outcomes for Unit II	C03, C04	
Unit III	**Public Key And Management**	**(08 Hours)**
Public Key Cryptography, RSA Algorithm: Working, Key length, Security, Key Distribution, Deffie-Hellman Key Exchange, Elliptic Curve: Arithmetic, Cryptography, Security, Authentication methods, Message Digest, Kerberos, X.509 Authentication service. Digital Signatures: Implementation, Algorithms, Standards (DSS), Authentication Protocol.		
#Exemplar/Case	Public encryption algorithm case study	

Studies	
Mapping of Course Outcomes for Unit III	C03, C04

Unit IV	**Security Requirements**	**(08 Hours)**

IP Security: Introduction, Architecture, IPV6, IPv4, IPSec protocols, and Operations, AH Protocol, ESP Protocol, ISAKMP Protocol, VPN. WEB Security: Introduction, Secure Socket Layer (SSL), SSL Session and Connection, SSL Record Protocol, Change Cipher Spec Protocol, Alert Protocol, Handshake Protocol. Electronic Mail Security: Introduction, Pretty Good Privacy, MIME, S/MIME, Comparison. Secure Electronic Transaction (SET).

#Exemplar/Case Studies	Cisco Security case study
Mapping of Course Outcomes for Unit IV	C03, C04

Unit V	**Firewall And Intrusion**	**(08 Hours)**

Introduction, Computer Intrusions. Firewall Introduction, Characteristics and types, Benefits and limitations. Firewall architecture, Trusted Systems, Access Control. Intrusion detection, IDS: Need, Methods, Types of IDS, Password Management, Limitations and Challenges.

#Exemplar/Case Studies	Firewall And Intrusion case study
Mapping of Course Outcomes for Unit V	C03, C04

Unit VI	**Cyber Forensic, Hacking& its countermeasures**	**(08 Hours)**

Personally Identifiable Information (PII), Cyber Stalking, Cybercrime, PII Confidentiality Safeguards, Information Protection Law: Indian Perspective. Hacking: Remote connectivity and VoIP hacking, Wireless Hacking, Mobile Hacking, countermeasures

#Exemplar/Case Studies	Cyber Forensics, ethical hacking case study
Mapping of Course Outcomes for Unit VI	C03, C04

Learning Resources

Text Books:

6. Dr. V.K. Pachghare, Cryptography and Information Security, PHI, ISBN 978-81-303-5082-3
7. Nina Godbole,SunitBelapure, Cyber Security,Wiley India, ISBN:978-81-345-2179-1
8. PDF Digital Content : Stuart McCLURE, Joel Scambray, George Kurtz, Hacking Exposed Network Security Secrets and Solutions, McGrowHill, 2012 ISBN: 978-0-07-178028-5 Digital Ref: http://84.209.254.175/linux-pdf/Hacking-Exposed-7-Network-Security-Secrets.pdfCollege libraries are requested to purchase the copy

Reference Books:

10. William Stallings, “Cryptography and Network Security: Principles and Practice”, 7/e, Pearson, ISBN:9789332585225. https://pearsoned.co.in/web/books/9789332585225_Cryptography-and-Network-Security_William-Stallings.aspx
11. Atul Kahate, “Cryptography and Network Security”, Mc Graw Hill Publication, 2nd Edition, 2008, ISBN : 978-0-07-064823-4

e-Books: https://www.simplilearn.com/introduction-to-cyber-security-beginners-guide-pdf
MOOC Courses: https://onlinecourses.swayam2.ac.in/cec20_cs15/preview
@The CO-PO mapping table

PO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	2	2	-	-	-	1	-	-	-	-	-	1
CO2	2	2	-	1	-	1	-	-	-	-	-	1
CO3	2	2	-	-	-	1	-	-	-	-	-	1
CO4	2	2	2	2	2	1	-	-	-	-	-	1