

Branch Name:	MCA
Program Code:	CS201
Course Name:	Information and Network Security Practical
Course Code:	4CS2010205P
Pre-requisite Course:	- Computer Networks, Operating Systems, Programming in C/C++ or Java, Discrete Mathematics, and Database Management Systems. - Students are expected to have a fundamental understanding of network protocols, operating system concepts, and basic programming skills.

Course Objectives:

1. Understand the basic principles of information security, including confidentiality, integrity, availability, and classical encryption techniques..
2. Learn and apply symmetric and asymmetric encryption, hash functions, and digital signatures for secure data communication.
3. Analyze authentication methods and key management systems, including PKI, X.509 certificates, and Kerberos.
4. Explore common network security protocols and tools, such as SSL/TLS, IPSec, firewalls, IDS/IPS, and Wireshark.
5. Evaluate and implement security measures to defend against attacks like brute-force, replay, forgery, and malware.

Teaching and Examination Scheme:

Teaching Scheme (Hours per week)				Evaluation Scheme (Marks)				
Lecture (L)	Tutorial (T)	Practical (P)	Credit	Theory (Marks)		Practical (Marks)		Total (Marks)
				University Assessment	Continuous Assessment	University Assessment	Continuous Assessment	
-	-	4	2	-	-	25	25	50

LAB/ Practical:

Note: The practical list provided is a part for reference only. The course t teacher may Change/formulate it as per his/her methodology and requirement.

Tools and Libraries Used for Practical:

- OpenSSL - Wireshark - Kali Linux - Metasploit Framework - Hashcat - Tcpdump - Nmap - Snort - WiFi Pineapple

Sr.No	List of Practicals
1	Implement Caesar Cipher Encryption and Decryption
2	Design Monoalphabetic and Playfair Cipher in Python or C
3	Implement Vigenère Cipher for text messages
4	Develop Rail Fence and Columnar Transposition Cipher encryption programs
5	Demonstrate Brute Force Attack on a simple encrypted message
6	Implement Block Cipher Modes (ECB, CBC, CFB, OFB, CTR) using sample text

7	Implement RSA Algorithm for key generation, encryption, and decryption
8	Demonstrate Diffie-Hellman Key Exchange with manual steps or code
9	Compare MD5 and SHA-256 Hash outputs for integrity verification
10	Generate HMAC using SHA-512 for message authentication
11	Illustrate Meet-in-the-Middle Attack conceptually on Double Encryption
12	Create and verify a Digital Signature using DSA Algorithm
13	Demonstrate X.509 Certificate structure and validation process
14	Set up a simple PKI structure using OpenSSL (CA, CSR, Certificates)
15	Simulate Kerberos Authentication Process through diagrams or Packet captures
16	Configure SSL/TLS for securing web communication (HTTPS setup)
17	Demonstrate Email Security using PGP or S/MIME for email encryption
18	Setup IPsec in Transport or Tunnel Mode for secure communication
19	Capture and analyze network packets using Wireshark
20	Simulate Firewall Rules and IDS/IPS using pfSense or Snort

Text Books:

1. "Cryptography and Network Security: Principles and Practice" Author: William Stallings Publisher: Pearson Education Edition: 7th Edition (2017) ISBN: 978-9332585225 Pages: Approx. 752
2. "Cryptography and Network Security" Authors: Behrouz A. Forouzan & Debdeep Mukhopadhyay Publisher: McGraw-Hill Education Edition: 3rd Edition (2015) ISBN: 978-9339212131 Pages: Approx. 672
3. "Applied Cryptography: Protocols, Algorithms, and Source Code in C" Author: Bruce Schneier Publisher: Wiley India Edition: 2nd Edition ISBN: 978-8126508193 Pages: Approx. 784
4. "Network Security and Cryptography" Author: Bernard Menezes Publisher: Cengage Learning Edition: 1st Edition (2010) ISBN: 978-8131509862 Pages: Approx. 420

Reference Books:

1. "Network Security: Private Communication in a Public World" Authors: Charlie Kaufman, Radia Perlman, Mike Speciner Publisher: Pearson Education Edition: 2nd Edition (2002) ISBN: 978-0130460196
2. "Understanding Cryptography: A Textbook for Students and Practitioners" Authors: Christof Paar, Jan Pelzl Publisher: Springer Edition: 1st Edition (2010) ISBN: 978-3642041006
3. "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" Authors: Dafydd Stuttard, Marcus Pinto Publisher: Wiley Edition: 2nd Edition (2011) ISBN: 978-1118026472
4. "Network Security Bible" Editor: Eric Cole Publisher: Wiley Edition: 2nd Edition (2009) ISBN: 978-0470502495

List of Open Source Software/learning website:

<https://www.cybrary.it/>
<https://owasp.org/>
<https://cryptohack.org/>
<https://www.hackthebox.com/>

<https://tryhackme.com/>
<https://letsdefend.io/>
<https://ocw.mit.edu/>
<https://www.coursera.org/>

Course Learning Outcomes (CLO): On completion of this course, the students will be able to:

CLO	Description	Bloom's Taxonomy Level
CLO1	Explain the core principles of information security (confidentiality, integrity, availability) and classify common threats and attacks.	Understand
CLO2	Apply symmetric and asymmetric encryption algorithms (DES, AES, RSA, etc.) to secure data in transmission and storage.	Apply
CLO3	Analyze and compare hashing techniques and message authentication codes to ensure data integrity and authenticity.	Analyze
CLO4	Evaluate digital signature schemes and key management infrastructure (PKI, X.509, Kerberos) for secure communication.	Evaluate
CLO5	Use modern network security protocols (SSL, TLS, IPSec, S/MIME, PGP) to secure emails and web communication.	Apply
CLO6	Identify, use, and analyze network defense tools (Wireshark, firewalls, IDS/IPS) for traffic monitoring and threat detection.	Analyze

Mapping of CLOs with Pos & PSOs

Course Learning Outcomes	Program Outcomes(POs)												Program Specific Outcomes(PSOs)	
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CLO1	H	M	M	-	-	-	-	-	-	M	H	L	M	L
CLO2	H	H	M	M	H	-	-	-	-	M	-	L	H	M
CLO3	H	M	H	M	M	-	-	-	-	M	-	-	M	M
CLO4	H	M	M	H	M	M	-	-	-	-	M	L	H	H
CLO5	H	M	L	M	H	-	-	-	-	H	M	L	M	H
CLO6	H	H	M	M	M	M	L	-	-	M	M	M	H	H

H:High, M:Medium, L:Low