

Branch Name:	MCA
Program Code:	CS201
Course Name:	Information and Network Security
Course Code:	4CS2010205T
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. Analyse 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	
3	-	-	3	60	40	-	-	100

Course Contents:

Unit No	Topic	Total Hours	Weightage (%)
1	Introduction to Information Security ○ Overview of Security Goals: Confidentiality, Integrity, Availability (CIA triad) ○ Security Services & Mechanisms: Access control, authentication, non-repudiation ○ Security Attacks: Passive and active attacks, threat models	12	25
	Symmetric Key Encryption ○ Symmetric Cipher Model: Components and process of encryption and decryption ○ Substitution Techniques: Caesar Cipher, Monoalphabetic Cipher, Playfair Cipher, Vigenère Cipher ○ Transposition Techniques: Rail Fence Cipher, Columnar Transposition Cipher		
	Basics of Cryptography ○ Cryptography vs Cryptanalysis: Purpose and techniques		

	○ Cryptanalytic Attacks: Brute-force, known-plaintext, chosen-plaintext, ciphertext-only ○ Block Cipher Modes of Operation: ■ Electronic Code Book (ECB) ■ Cipher Block Chaining (CBC) ■ Cipher Feedback (CFB) ■ Output Feedback (OFB) ■ Counter (CTR) Block and Stream Ciphers ○ Stream Cipher vs Block Cipher: Definitions, applications, and differences ○ Data Encryption Standard (DES): Architecture, limitations ○ Double & Triple DES ○ Advanced Encryption Standard (AES): Architecture, key sizes, round structure		
2	Public Key Cryptography ○ Introduction and principles of asymmetric encryption ○ RSA Algorithm: Key generation, encryption, and decryption steps ○ Diffie-Hellman Key Exchange Algorithm ○ Meet-in-the-Middle Attack: Attack on double encryption systems Hash Functions and Message Digests ○ Properties of Hash Functions: Pre-image resistance, second pre-image resistance, collision resistance ○ Simple Hash Functions ○ MD5: Structure, steps, vulnerabilities ○ Secure Hash Algorithms (SHA): Differences between SHA-1 and SHA-512 Message Integrity and Authentication ○ Message Integrity: Definition, role in secure communication ○ Message Authentication: Techniques, security requirements ○ Message Authentication Codes (MACs): Use cases, types (HMAC, CMAC)	11	25
3	Digital Signatures and Key Management Infrastructure - Digital Signatures Fundamental Concepts and Security Requirements ○ Authentication, data integrity, and non-repudiation ○ Comparison with Message Authentication Codes (MAC) ○ Real-world use cases (e.g., secure emails, software distribution) Digital Signature Algorithms and Standards ○ DSA (Digital Signature Algorithm): Key generation, signature creation, and verification ○ DSS (Digital Signature Standard): FIPS 186 compliance, limitations of DSA Signature Schemes ○ ElGamal Signature: Based on discrete logarithm problem ○ Schnorr Signature: Simplicity, efficiency, and use in cryptocurrencies Attacks and Challenges ○ Forgery attacks, replay attacks ○ Issues due to poor random number generation -Key Exchange and Infrastructure	12	25

	Key Management and Distribution ○ Centralized (e.g., Key Distribution Center) and decentralized approaches ○ Manual key exchange vs automated key management tools ○ Key lifecycle: generation, storage, usage, rotation, revocation X.509 Certificates ○ Structure: Subject, Issuer, Public key, Validity, Digital signature ○ Certificate validation process ○ CRL (Certificate Revocation List) and OCSP (Online Certificate Status Protocol) Public Key Infrastructure (PKI) ○ Components: Certificate Authority (CA), Registration Authority (RA), certificate directories ○ Trust models: Hierarchical PKI, Web of Trust, Bridge model ○ Application in HTTPS, VPNs, secure emails (S/MIME) Kerberos Authentication Protocol ○ Architecture: Authentication Server (AS), Ticket Granting Server (TGS), Key Distribution Center (KDC) ○ Ticket-based authentication process (TGT and Service Tickets) ○ Symmetric encryption and session key exchange ○ Application in enterprise environments (e.g., Windows Active Directory) ○ Limitations and improvements in Kerberos v5		
4	Network Security Applications and Monitoring Tools Network Security Protocols ○ Email Security: ■ S/MIME (Secure/Multipurpose Internet Mail Extensions) ■ PGP (Pretty Good Privacy) ○ Web Security: ■ SSL (Secure Socket Layer) ■ TLS (Transport Layer Security) ○ IP Security (IPSec): ■ AH (Authentication Header), ESP (Encapsulating Security Payload) ■ Transport and Tunnel Modes Network Monitoring and Defense ○ Viruses, Worms, and Malware: Types and examples ○ Firewall Design Principles: Packet filtering, stateful inspection, proxy firewalls ○ Intrusion Detection and Prevention Systems (IDS/IPS): ■ Signature-based vs Anomaly-based detection ○ Wireshark: ■ Introduction to packet analysis ■ Capturing and analyzing network traffic	11	25

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 Schnei **Publisher:** Wiley India **Edition:** 2nd Edition (Reprint 2015) **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