Course Title: Information Security (3 Cr.)
Course Code: CACS459
Year/Semester: IV/VIII
Class Load: 6 Hrs./Week (Theory: 3 Hrs., Practical: 3 Hrs.)

Course Description

The course "Information Security" introduces both theoretical and practical concepts related to computer and information security. It covers cryptographic algorithms, authentication systems, access controls, malicious software, network security, and security auditing.

Course Objectives

The primary objectives of this course are:

- To familiarize students with fundamental computer security concepts, security policies, and mechanisms.
- To enable students to design, implement, and manage secure computer systems effectively.

Course Contents

Unit I: Overview of Computer Security (4 Hrs)

- Computer Security Concepts
- Computer Security, Information Security, Network Security
- Threats, Attacks, and Assets
- Security Requirements
- Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy

Unit II: Cryptographic Algorithms (12 Hrs)

- **Classical Cryptosystems:** Caesar, Vigenère, Playfair, Rail Fence Ciphers
- **Modern Ciphers:** Block vs. Stream Ciphers, Symmetric vs. Asymmetric Ciphers
- **Symmetric Encryption:** Feistel Cipher Structure, Data Encryption Standard (DES), Advanced Encryption Standard (AES)
- **Mathematical Concepts:** Groups, Rings, Fields, Modular Arithmetic, Galois Fields, Polynomial Arithmetic
- **Number Theory:** Prime Numbers, Fermat's Theorem, Primality Testing (Miller-Rabin Algorithm), Euclidean Algorithm, Extended Euclidean Algorithm, Euler's Totient Function
- **Asymmetric Encryption:** Diffie-Hellman Key Exchange, RSA Algorithm

Unit III: Message Authentication and Hash Functions (6 Hrs)

- Message Authentication
- Hash Functions
- Message Digests: MD4 and MD5
- Secure Hash Algorithm: SHA-1
- HMAC
- Digital Signatures

Unit IV: User Authentication (5 Hrs)

- User Authentication Principles
- Password-Based Authentication
- Token-Based Authentication
- Biometric Authentication
- Remote User Authentication
- Two-Factor Authentication

Unit V: Access Control (5 Hrs)

- Access Control Principles
- Subjects, Objects, and Access Rights
- Access Control Matrix and Capability Lists
- Discretionary Access Control (DAC)
- Role-Based Access Control (RBAC)
- Attribute-Based Access Control (ABAC)
- Identity, Credential, and Access Management
- Trust Frameworks

Unit VI: Malicious Software and Intrusion (4 Hrs)

- Malicious Software
- Virus and Its Phases, Virus Classification
- Worms and Their Propagation Model
- Trojan Horse
- Intrusion and Intruders

- Intrusion Detection System (IDS)
- Analysis Approaches: Anomaly-Based, Signature-Based
- Honeypots

Unit VII: Network Security (5 Hrs)

- Overview of Network Security
- Email Security: S/MIME, Pretty Good Privacy (PGP)
- Secure Socket Layer (SSL) and Transport Layer Security (TLS)
- IP Security (IPSec)
- Firewalls and Their Types

Unit VIII: Security Auditing (7 Hrs)

- Security Audit
- Security Auditing Architecture
- Security Audit Trail
- Implementing Logging Functions
- Audit Trail Analysis

Laboratory Work

The practical component includes the implementation and simulation of:

- Classical ciphers such as Caesar, Playfair, and Rail Fence
- DES and AES encryption algorithms
- Primality Testing, Euclidean Algorithm, and RSA
- Hash Functions: MD5, SHA
- Authentication Systems: Password-based, CAPTCHA, Two-Factor Authentication
- Role-Based Access Control
- Malicious Software Analysis

Teaching Methods

The course will employ various teaching methodologies, including:

- Classroom lectures
- Laboratory activities
- Group discussions

- Student presentations
- Case studies
  The instructor may choose any programming language for laboratory work based on students' proficiency and comfort level.

Evaluation Criteria

Assessment will be based on:

- Theory examinations
- Practical assignments
- Case study analysis
- Group projects
- Class participation

Textbooks

1. William Stallings & Lawrie Brown, *Computer Security: Principles and Practice*, Pearson.
2. William Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson.

Reference Books

1. Mark Stamp, *Information Security: Principles and Practices*, Wiley.
2. Matt Bishop, *Introduction to Computer Security*, Addison-Wesley.
3. Matt Bishop, *Computer Security: Art and Science*, Addison-Wesley.
4. Charles P. Pfleeger & Shari Lawrence Pfleeger, *Security in Computing*, Pearson.

This syllabus provides a comprehensive guide to understanding fundamental and advanced concepts in information security, preparing students for both academic and practical applications in the field.