Information Security

Code	Credit Hours
CS-484	3+0

Course Description:

The successful completion of this course will enable the students to familiarize themselves with the core concepts of information security. Students will learn to analyze information security-related threats, which may allow an attacker to compromise the security of an information system.

This course is the combination of techniques and tools, which can be used to secure applications and resources of an organization. This course will help students to understand the tools and building-blocks of security such as cryptography and security protocols.

Textbook:

1. Michael E. Whitman and Herbert J. Mattord, *Principles of Information Security*, 6th Edition, Publisher: Cengage Learning, 2017.

Reference Books:

1. William Stallings and Lawrie Brown, *Computer Security: Principles and Practice*, 4th Edition, 2017.

2. William Stallings, *Cryptography and Network Security: Principles and Practice*, 8th Edition, published by Pearson Education, Inc., publishing as Prentice Hall, 2022.

Prerequisites:

N/A

Assessment System for Theory:

Quizzes	15%
Assignments	5%
Projects	10%
Mid Terms	30%
ESE	40%

Assessment System for Lab:

Quizzes	N/A
Assignments	N/A
Lab Work and Report	N/A
Lab ESE/Viva	N/A

Teaching Plan:

Week No	Topics	Learning Outcomes
1	Introduction to IS	Course outline, objectives, teaching plan, assessment, method, review of concepts.
2-6	Cryptography, Hash Functions, and Digital Signatures	This section covers primary encryption algorithms i.e. DES, AES, and RSA. Hash functions (e.g. SHA 256) and digital signatures are also covered.
7-8	User Authentication and Access control mechanisms	The approaches to user authentication are presented with an emphasis on Kerberos. Furthermore, the framework for designing an identity verification system is included.
9	**MID SEMESTER EXAM**	
10-14	Risk Management	All three phases of risk management (i.e. risk assessment, risk analysis, and risk mitigation) are discussed using practical examples.
15-17	Software Security and Introduction to Privacy	Best practices for designing secure software are elaborated along with a general outline of privacy and trusted computing.
18	**END OF SEMESTER EXAM**	

Practical Plan:

Experiment No	Description
1	N/A
2	N/A
3	N/A
4	N/A
5	N/A
6	N/A
7	N/A
8	N/A
9	N/A
10	N/A
11	N/A
12	N/A
13	N/A
14	N/A
15	N/A
16	N/A