

Information Security

Prepared by Dr. Ayman Khallel

IT373

Information Security

Introduction



Outline

1. About me
2. Course content
3. Course Objectives
4. Discussion Session
5. References

About me

- **Name:** Ayman Khallel Ibrahim Al-ani
- **Professional Background:**
 - Head of the Cybersecurity Engineering Department
 - Conducting research in IPv6 network security, focusing on Neighbor Discovery Protocol and Duplicate Address Detection
- **Education:**
 - PhD from USM, Malaysia
 - MS from UUM, Malaysia
- **Interests:**
 - Cybersecurity methodologies and AI applications
 - Continuous learning and lecturing

Course content

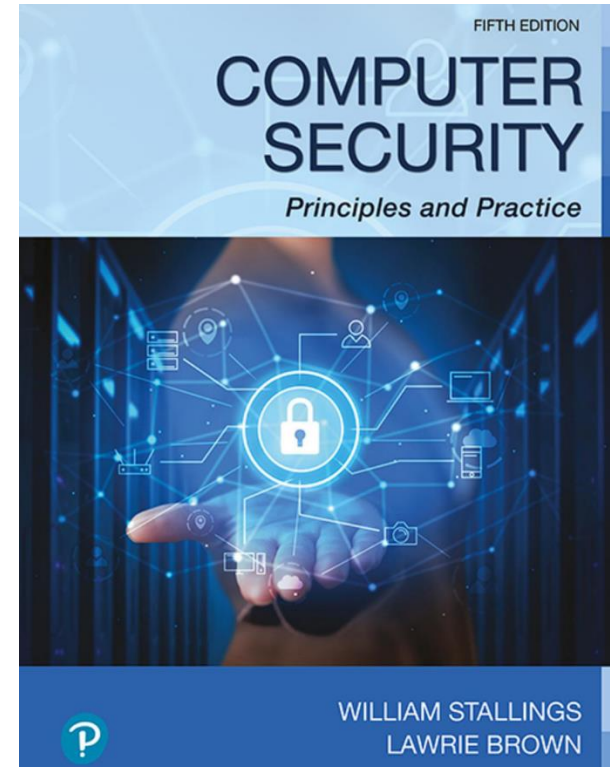
1. Overview of security concepts and definitions,
2. symmetric cryptography; modern encryption algorithms (DES, AES),
3. modern data encryption standards,
4. block cipher cryptanalysis and usage,
5. modern stream ciphers,
6. Asymmetric cryptography; public key cryptography,
7. key certificates and management,
8. message authentication and hash functions, hash algorithms,
9. digital signature and authentication protocols,
10. electronic mail security,
11. IP security,
12. web security.

Course Objectives

1. Understand Core Security Concepts and Cryptographic Techniques
2. Develop Practical Skills in Implementing and Analyzing Security Protocols

References

- Stallings W. Computer Security. Principles and Practice 5ed 2023





Thank You