

Information Security

IT373
Information Security

Introduction



Course content

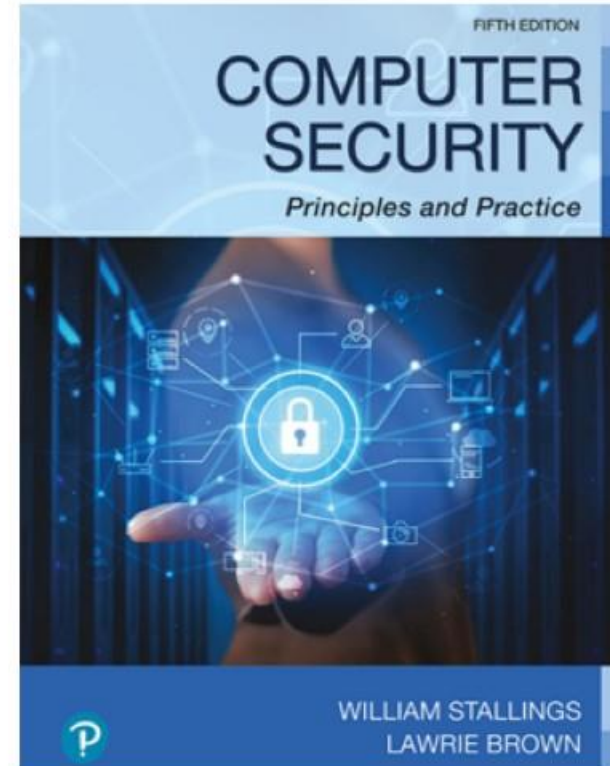
1. Overview of security concepts and definitions,
2. symmetric cryptography; modern encryption algorithms (DES, AES),
3. modern data encryption standards,
4. block cipher cryptanalysis and usage,
5. modern stream ciphers,
6. Asymmetric cryptography; public key cryptography,
7. key certificates and management,
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