

Introduction to Cryptography

Prepared by Dr. Mohammad Alkhatib

Associate Professor

Major: Information Security

جامعة الجميع الذكية

تسعى لتكون الكيان الأول الذي يتبنى مبدأ المجتمع التعليمي
التعاوني ويقدم العلم مقابل العمل لتنمية وبناء المجتمعات.

Introductory Lecture



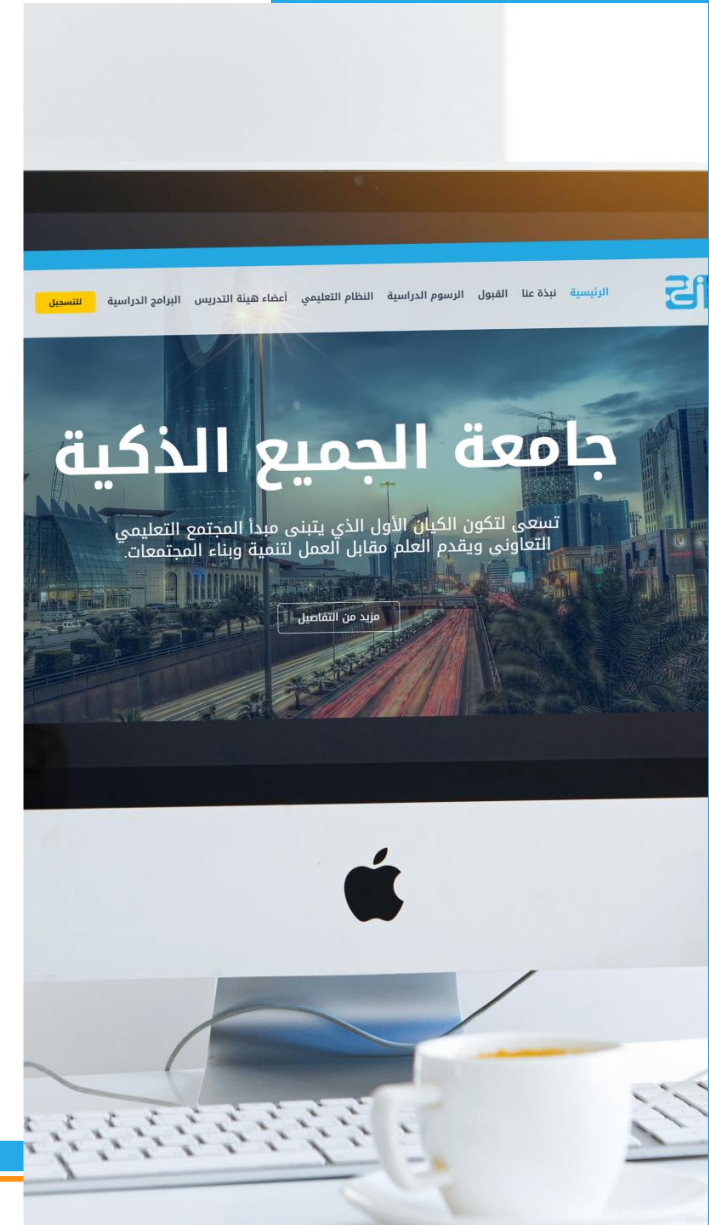
جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

This course covers the fundamental concepts of encoding and encrypting information, cryptographic protocols and techniques. Various cryptographic algorithms, and security of information will be covered in depth.

Learning Outcomes:

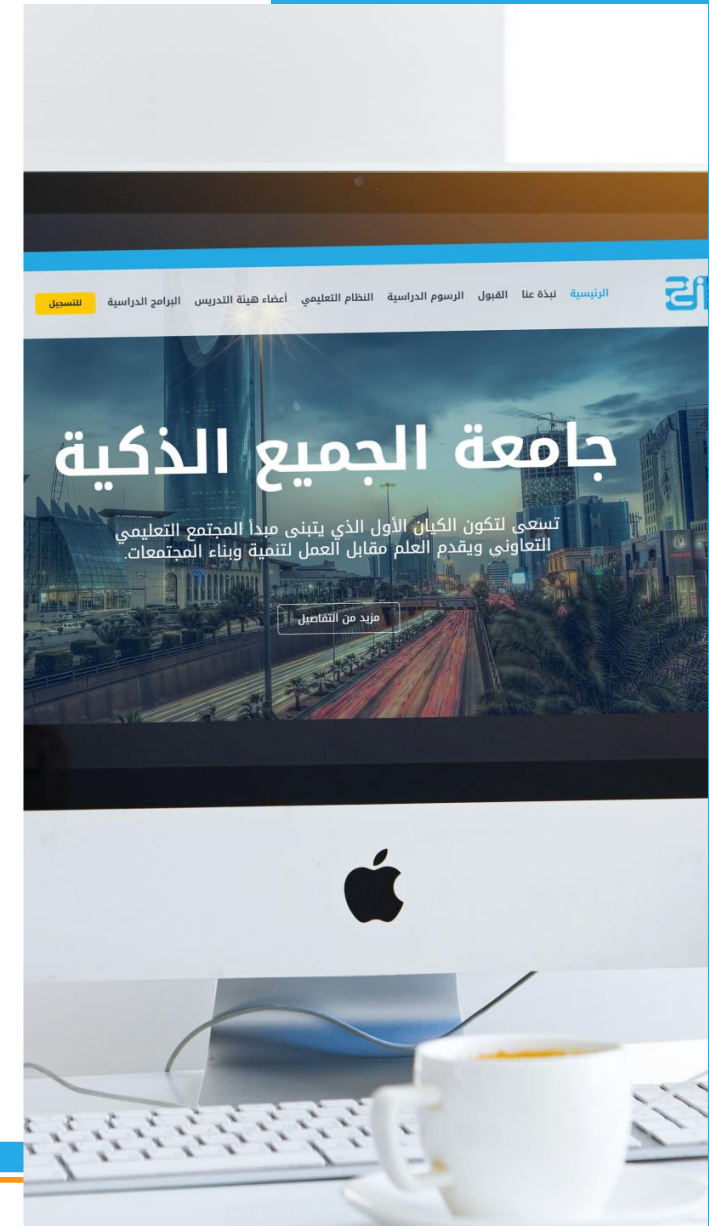
Upon successful completion of this course, students should be able to:

- ☐ Demonstrate the fundamentals of cryptography and encryption.
- ☐ Apply various cryptography protocols and techniques to encrypt and decrypt data.
- ☐ Discuss cryptography algorithms.
- ☐ Evaluate the role of cryptography in security information systems



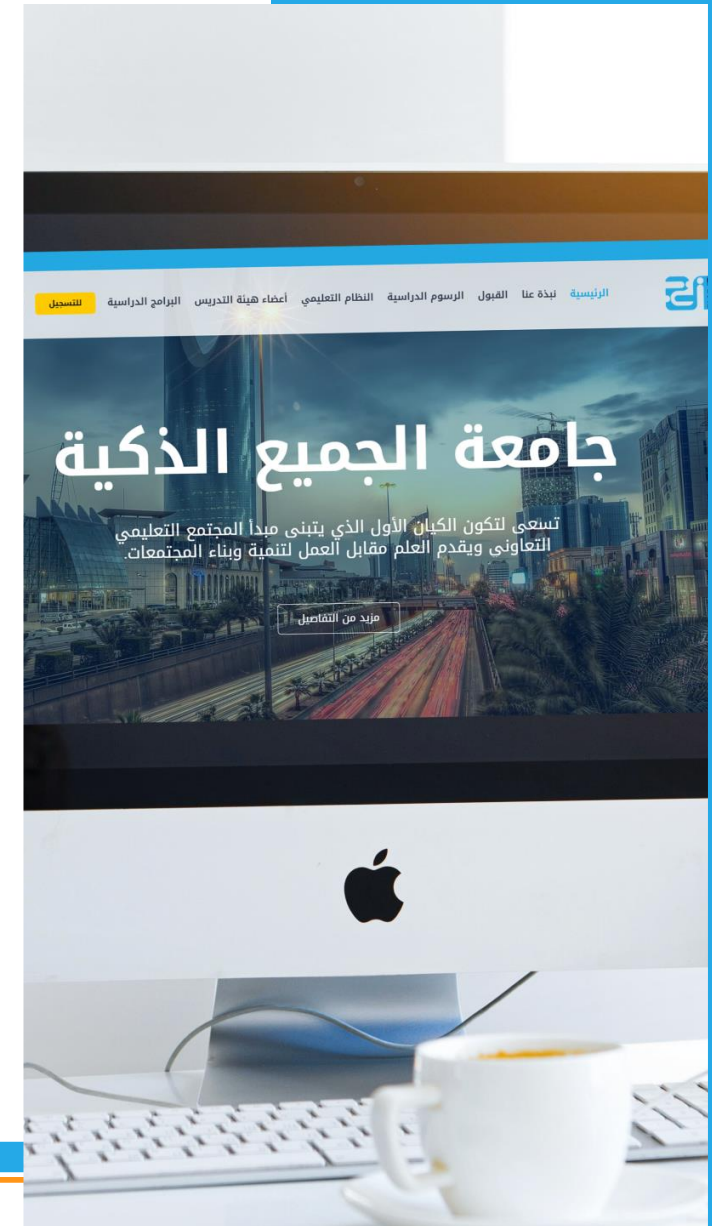
Teaching Strategies:

- ☐ Class lectures
- ☐ Class exercises and discussions.
- ☐ Tutorial
- ☐ Student Presentation



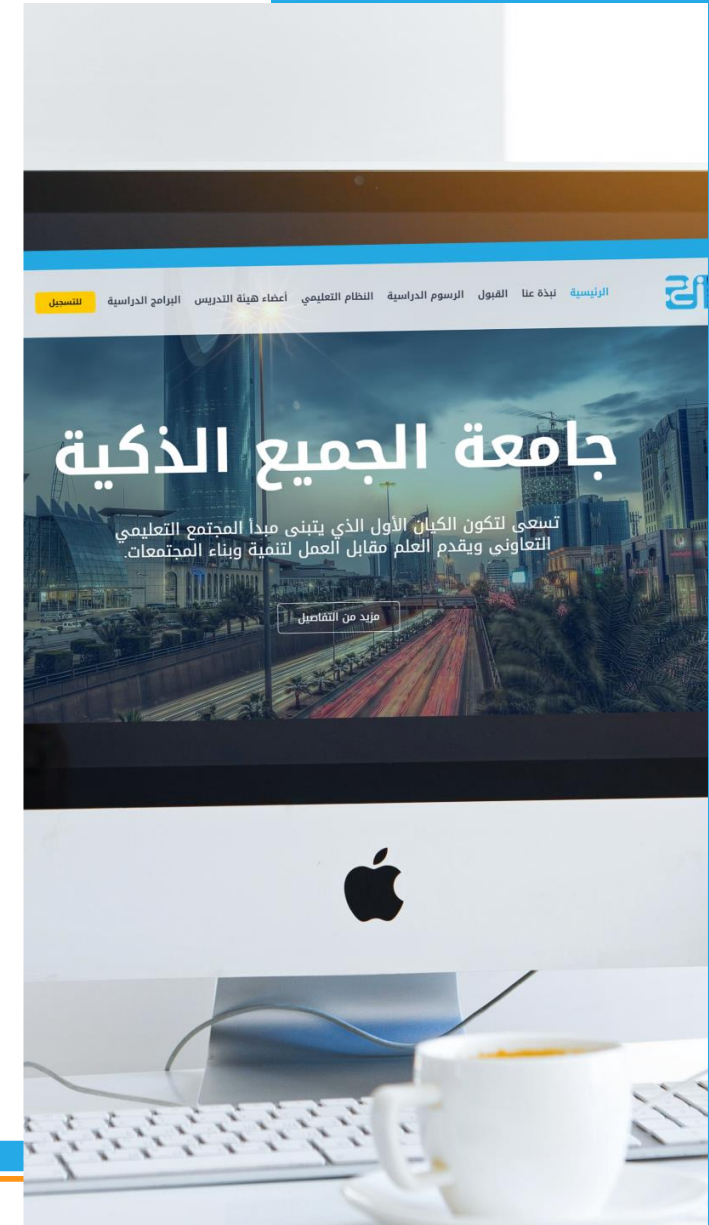
Assessment Methods:

- ☐ Quizzes
- ☐ Final exam



Topics:

- ☐ Module 1: Foundations and principles of Cryptography.
- ☐ Module 2: Cryptography protocols.
- ☐ Module 3: Cryptography techniques.
- ☐ Module 4: Cryptography Algorithms.
- ☐ Module 5: Public key Algorithms

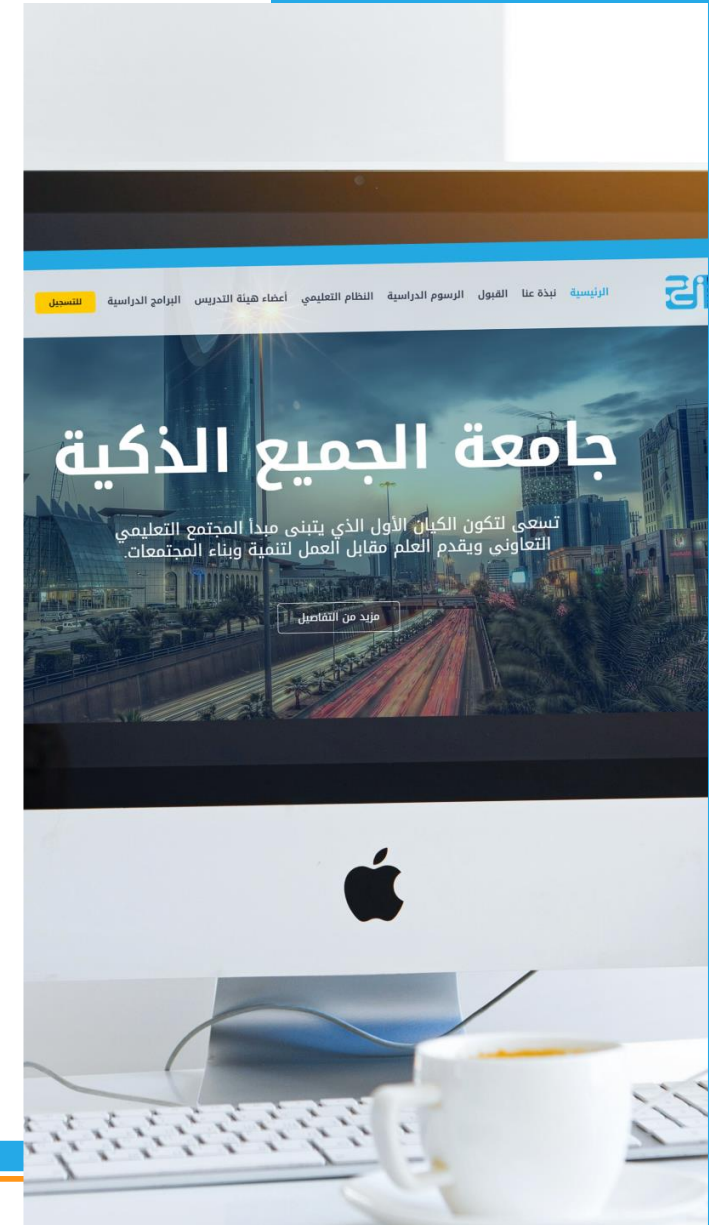


Textbook:

- ❑ **Required Textbook:** Stallings W., Cryptography and Network Security:

Principles and Practice, 2016, Pearson, ISBN: 0134444280.

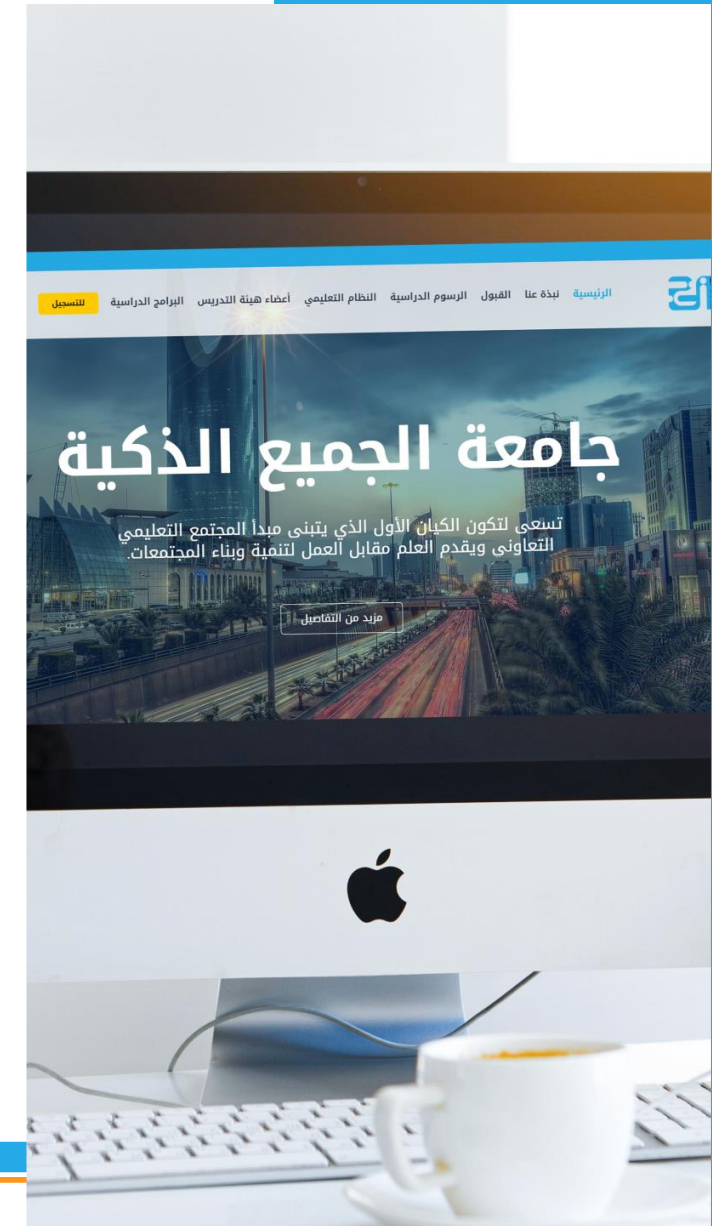
Note: The main material and reference for each course will be the textbook mentioned in the course specifications. Lecture notes and slides are additional resources that are prepared by the professor



Course Content:

❑ Chapter 1: Introduction to Information Security

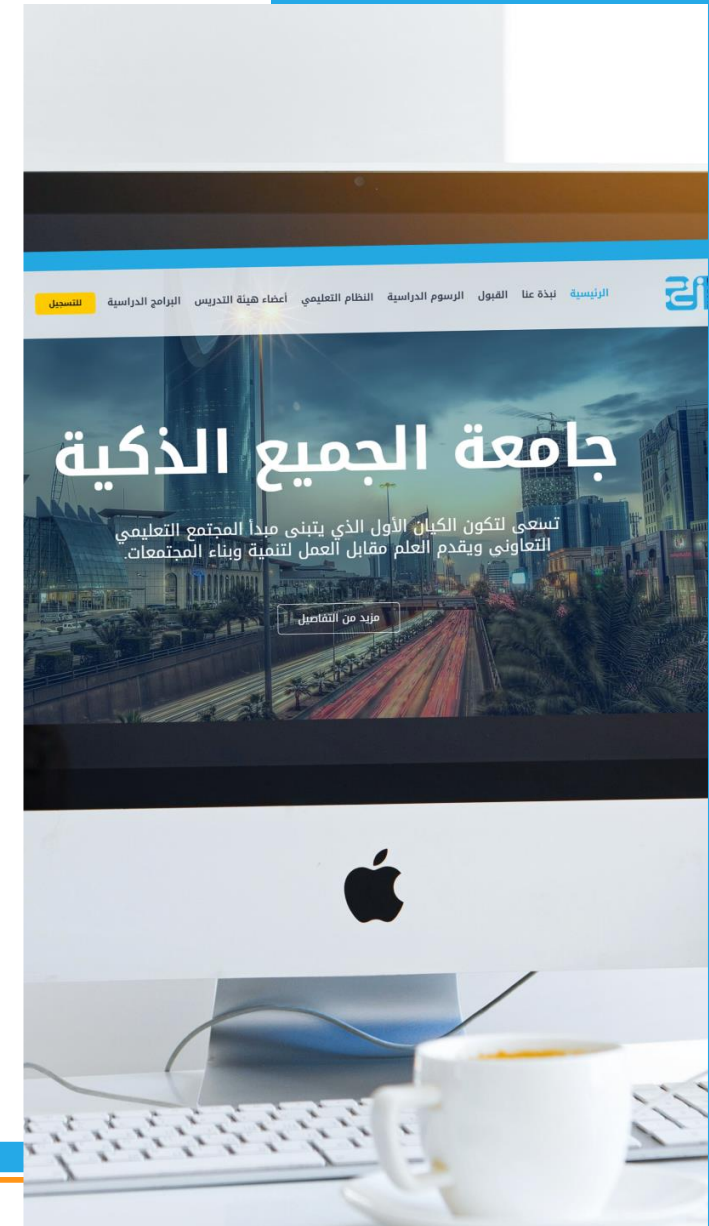
- ✓ Terminology
- ✓ Security Services
- ✓ Confidentiality
- ✓ Data integrity
- ✓ Authentication



Course Content:

❑ Chapter 2: Introduction to Cryptography

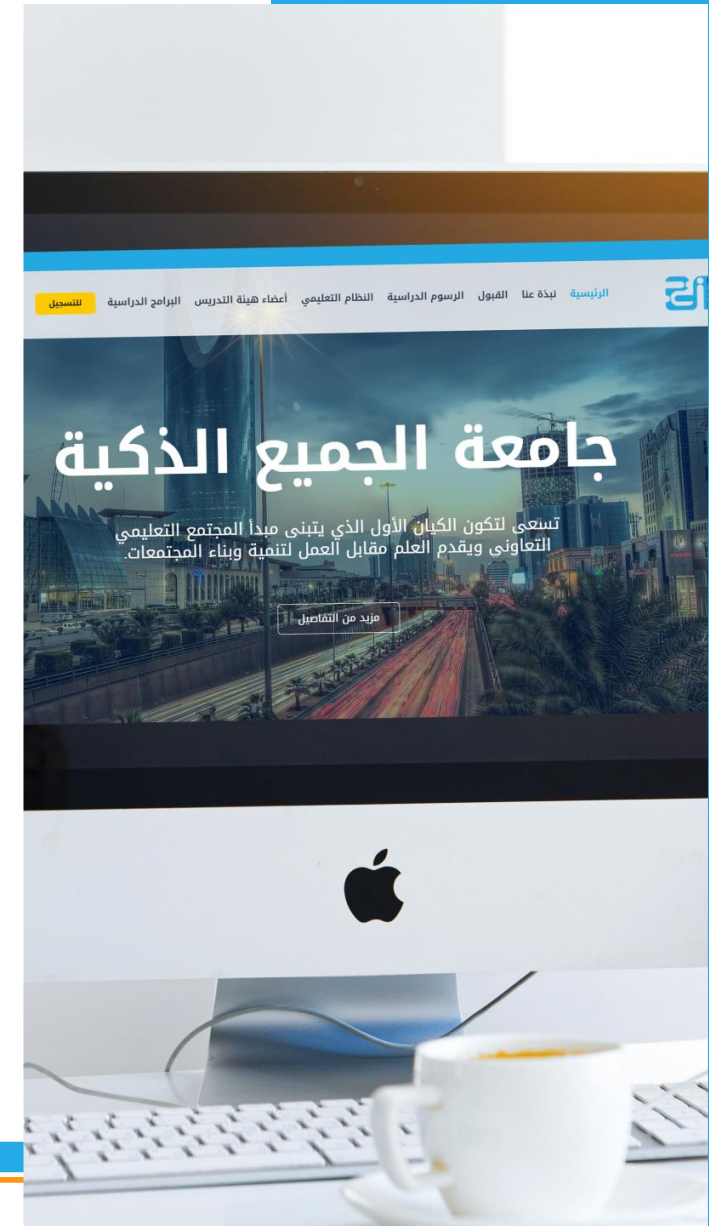
- ✓ Classical Cryptography
- ✓ *Shift Cipher*
- ✓ *Affine Cipher*
- ✓ *Substitution Cipher*
- ✓ Basic Cryptanalysis/Attacks
- ✓ Mathematical Background (Modular Arithmetic, Finite Fields)



Course Content:

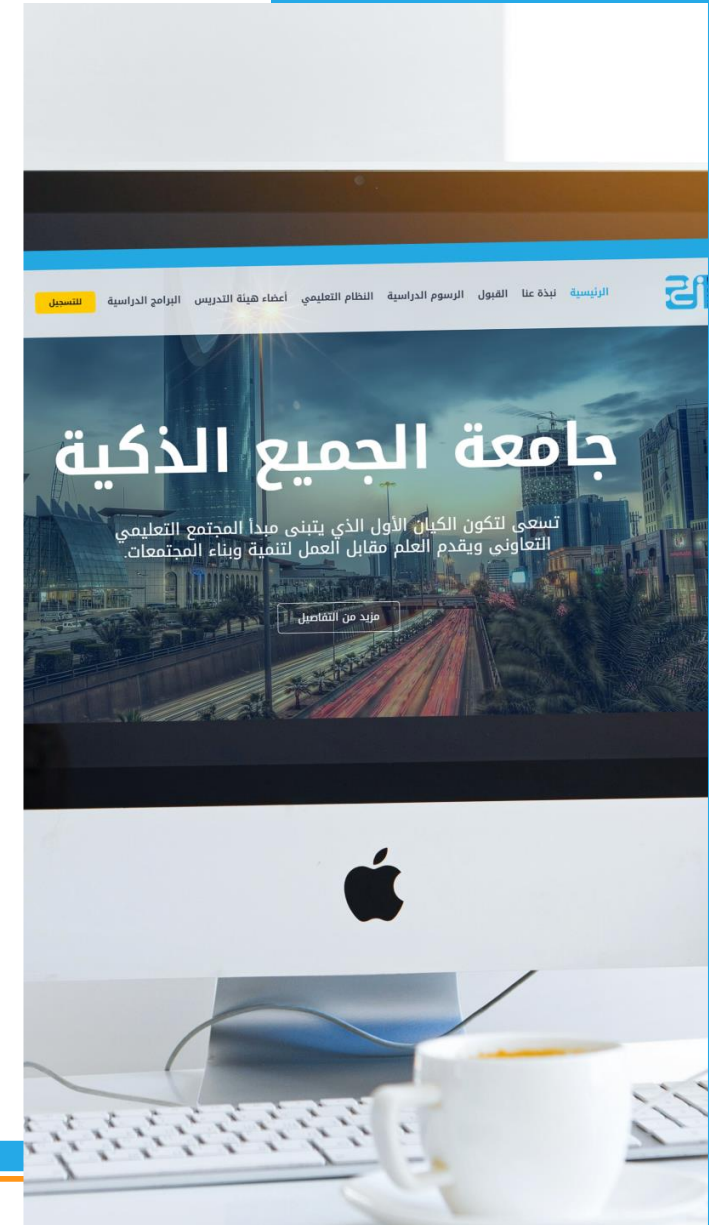
❑ Chapter 3: Symmetric cryptography

- ✓ Stream ciphers
- ✓ RC4
- ✓ A5



Course Content:

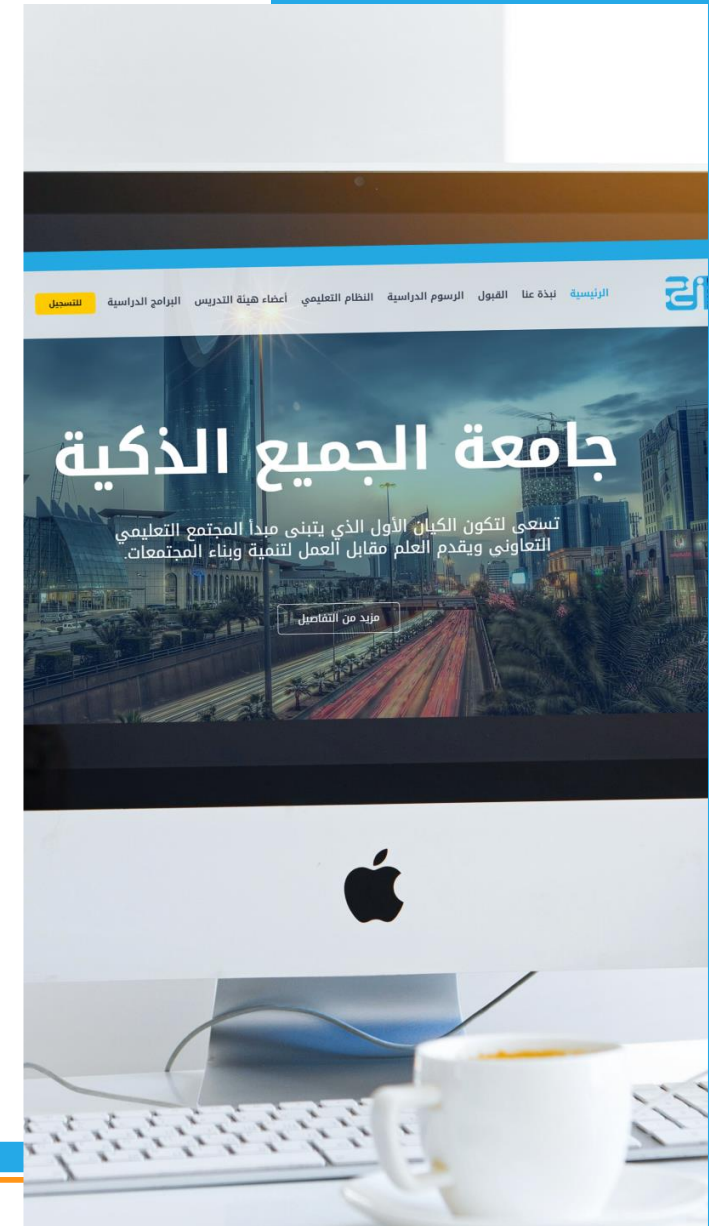
- ❑ **Chapter 4: Symmetric cryptography**
 - ✓ Block ciphers
 - ✓ Data Encryption Standard (DES)
 - ✓ Advanced Encryption Standard (AES)
 - ✓ Modes of Operations



Course Content:

❑ Chapter 5: Public Key Cryptography

- ✓ Number Theory Concepts
- ✓ Integer Factorization Problem
- ✓ Discrete Logarithm Problem



Course Content:

❑ Chapter 6: Public Key Cryptography

- ✓ Diffie-Hellman Key Exchange
- ✓ RSA Cryptosystem
- ✓ El Gamal Cryptosystem

