

# Introduction to Cryptography

Prepared by Dr. Mohammad Alkhatib

Associate Professor

Major: Information Security



Introductory Lecture



جامعة القادسية  
EVERYONE'S SMART UNIVERSITY

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

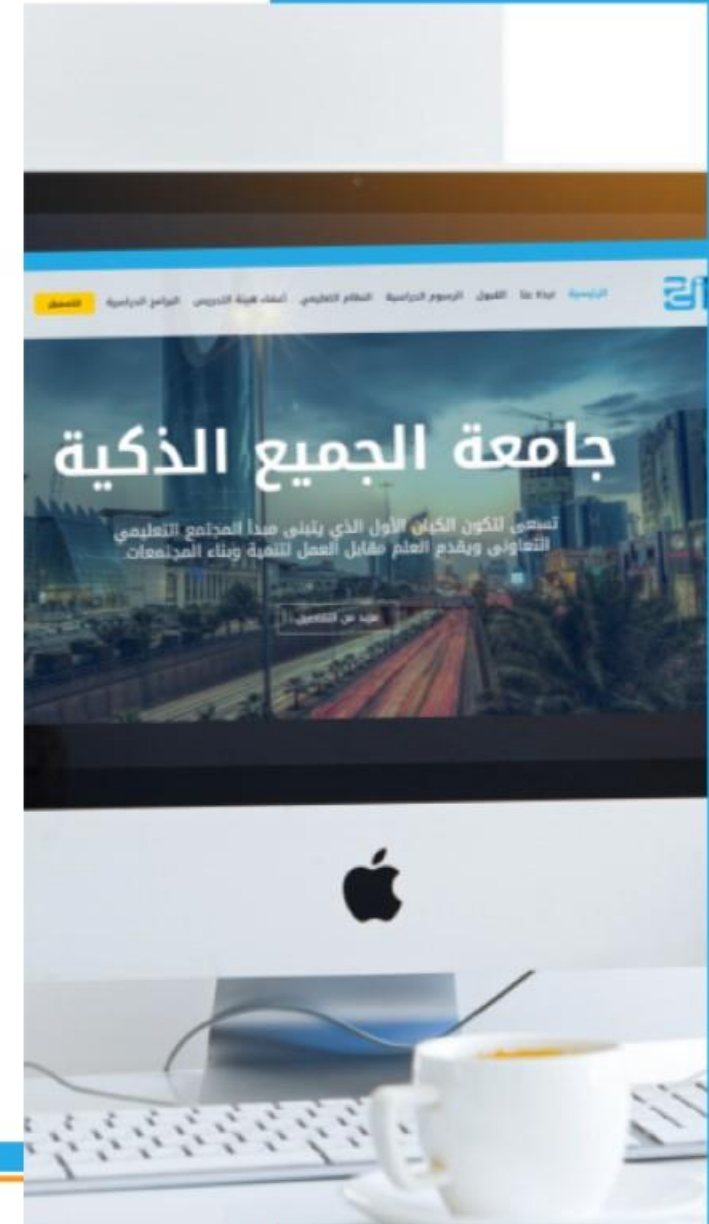
# Chapter 01

## Course Learning Outcomes

### 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

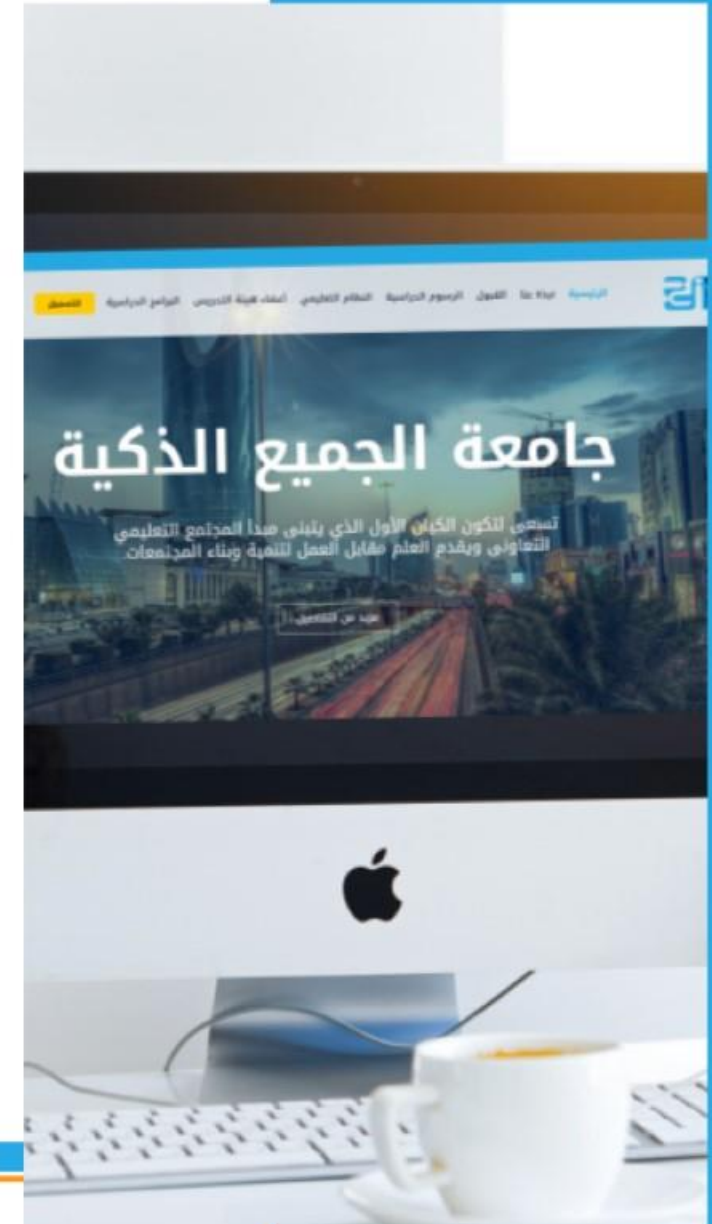


# Chapter 01

## Teaching Strategies

### Teaching Strategies:

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

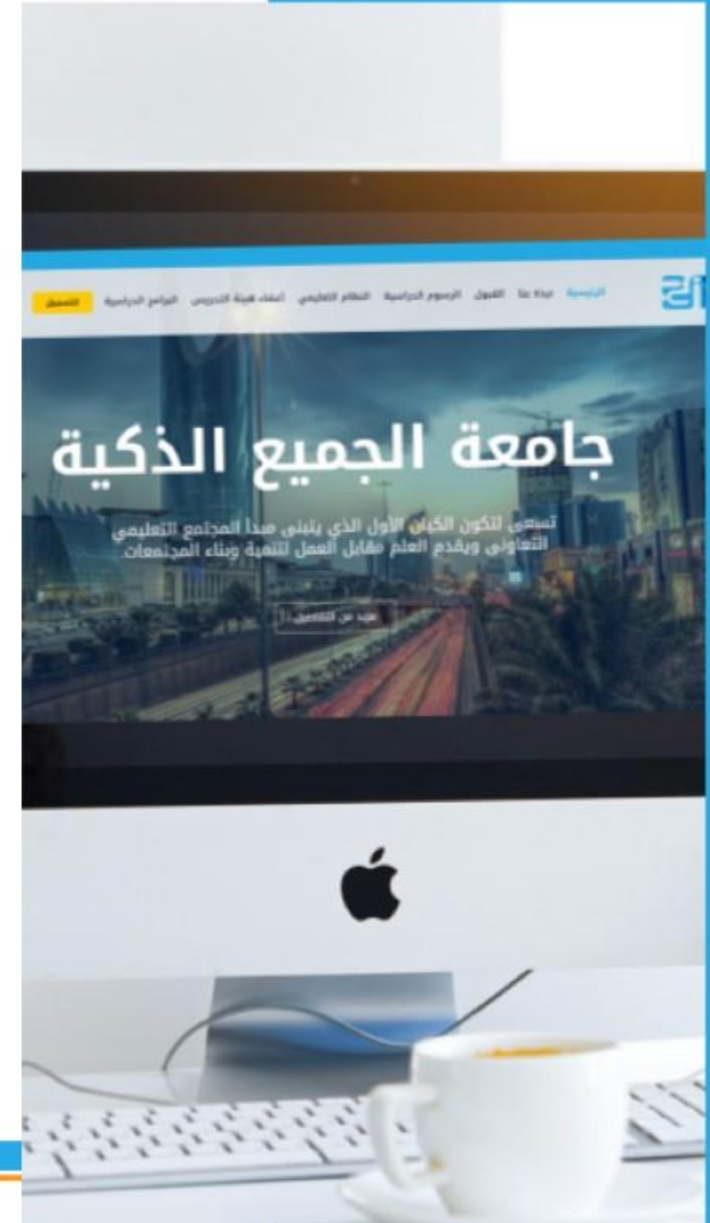


# Chapter 01

## Assessment Methods

### Assessment Methods:

- ☐ Quizzes
- ☐ Final exam

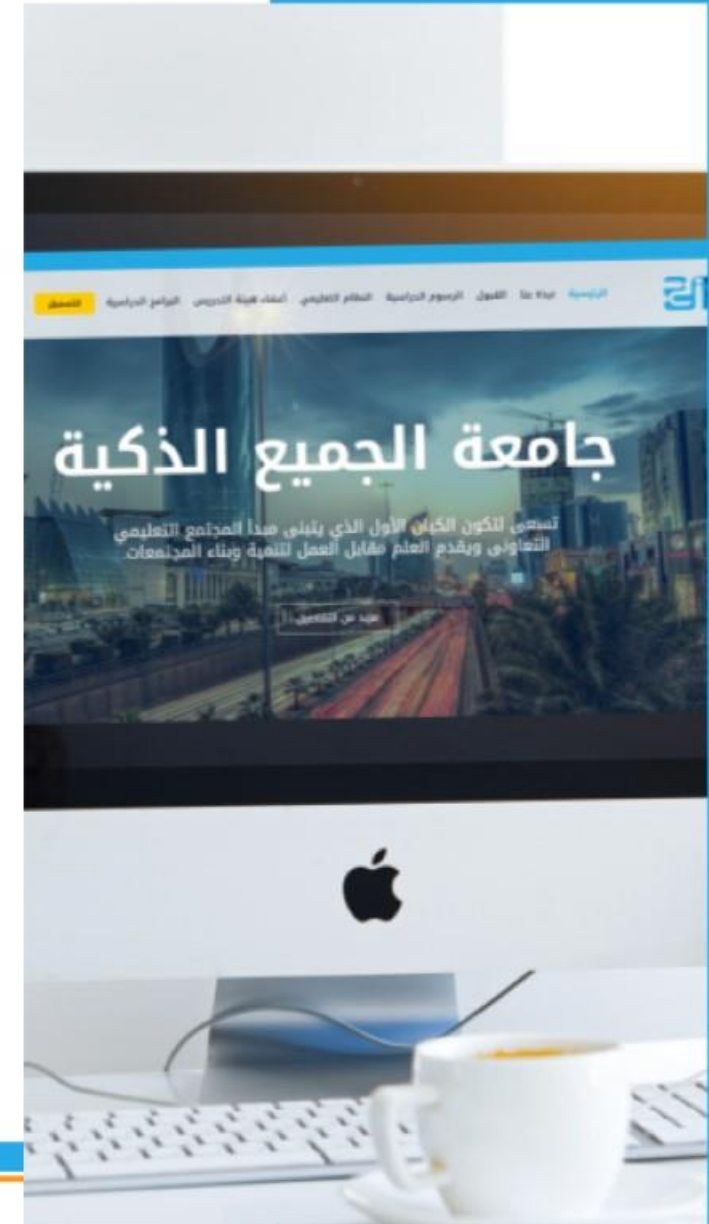


# Chapter 01

## Topics

### Topics:

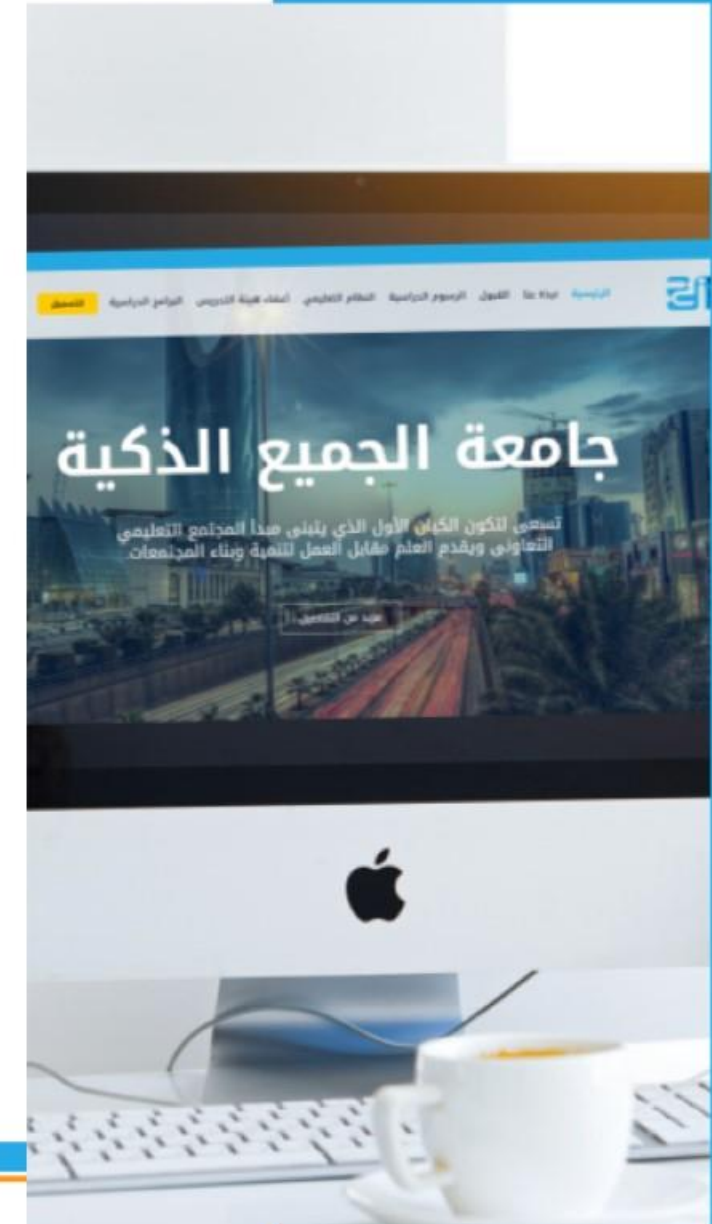
- ☐ Module 1: Foundations and principles of Cryptography.
- ☐ Module 2: Cryptography protocols.
- ☐ Module 3: Cryptography techniques.
- ☐ Module 4: Cryptography Algorithms.
- ☐ Module 5: Public key Algorithms



### 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



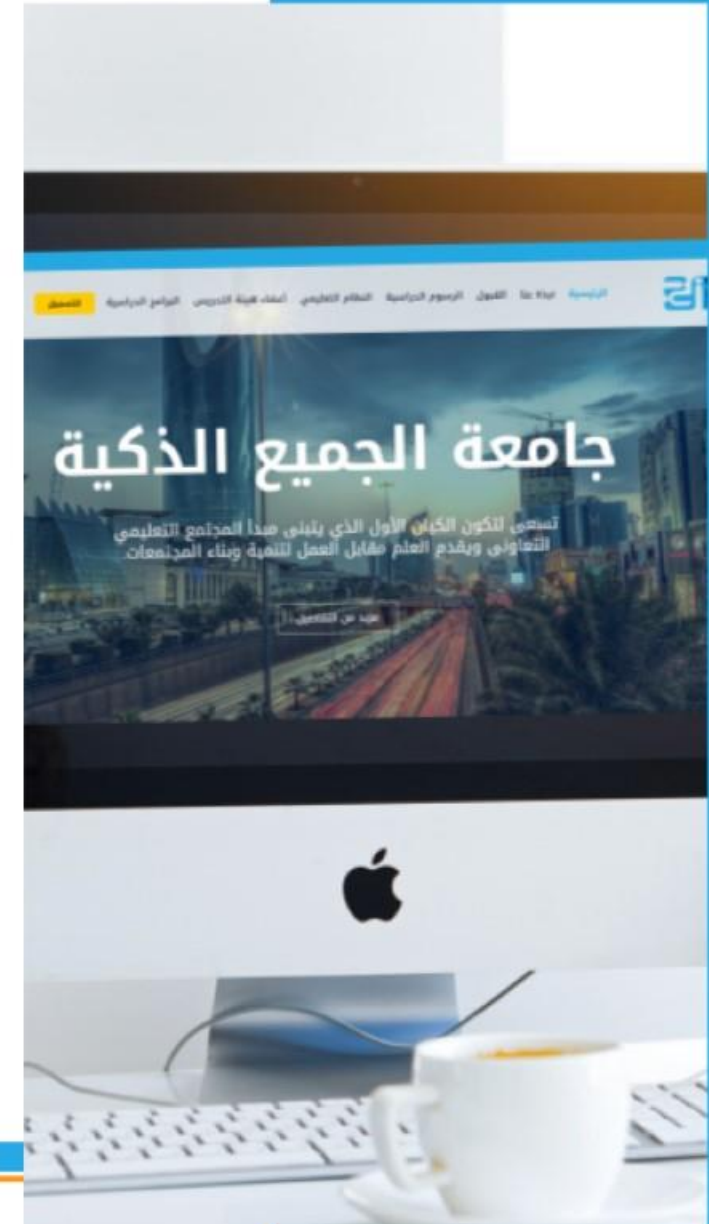
# Chapter 01

## Course Content

### Course Content:

#### ❑ Chapter 1: Introduction to Information Security

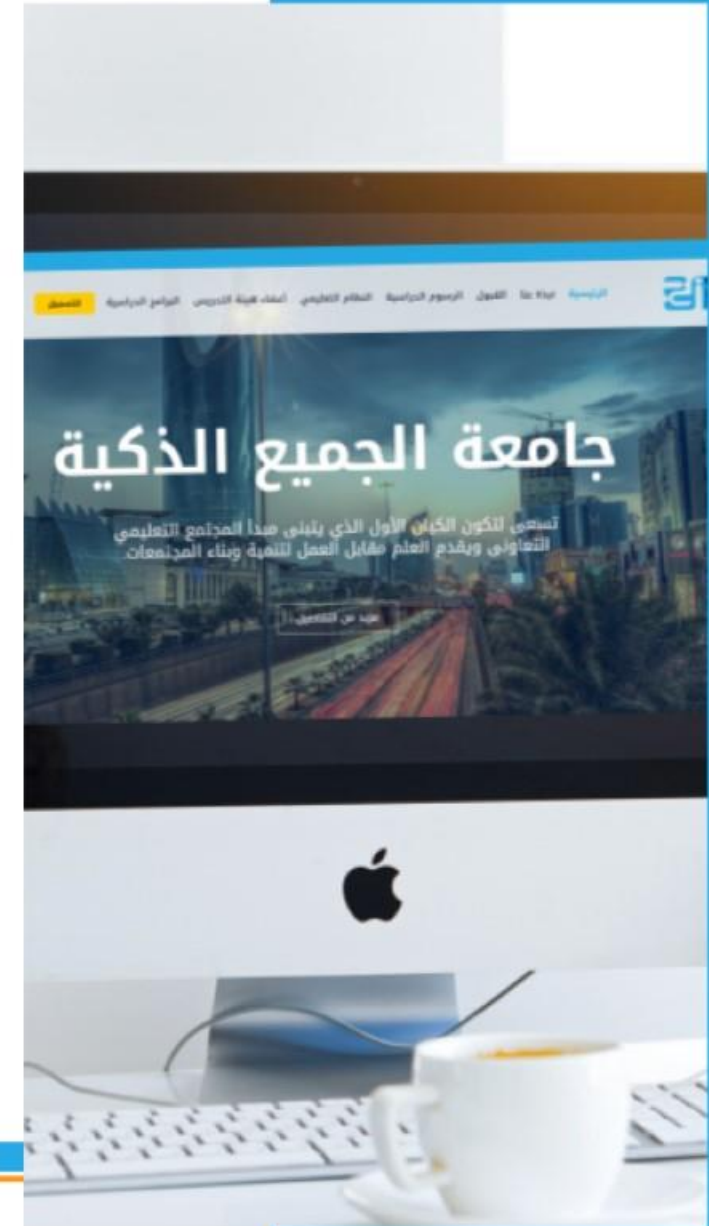
- ✓ Terminology
- ✓ Security Services
- ✓ Confidentiality
- ✓ Data integrity
- ✓ Authentication



### Course Content:

#### ❑ Chapter 2: Introduction to Cryptography

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



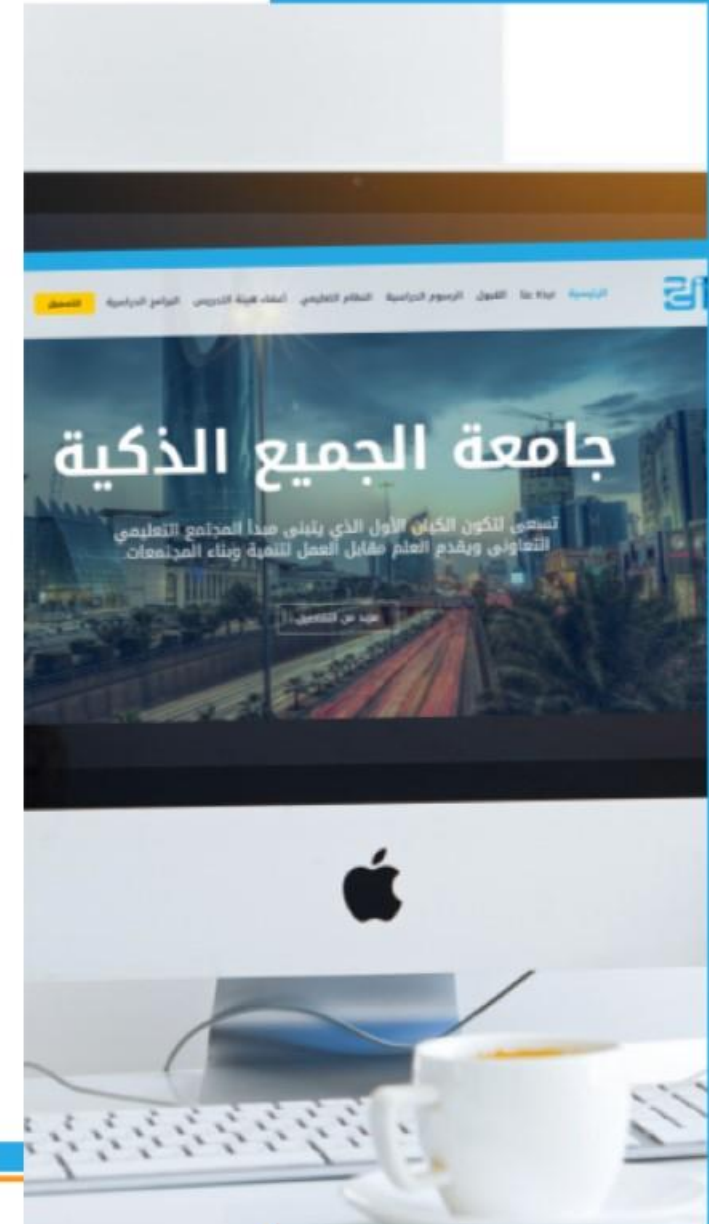
# Chapter 01

## Course Content

### Course Content:

#### ❑ Chapter 3: Symmetric cryptography

- ✓ Stream ciphers
- ✓ RC4
- ✓ A5

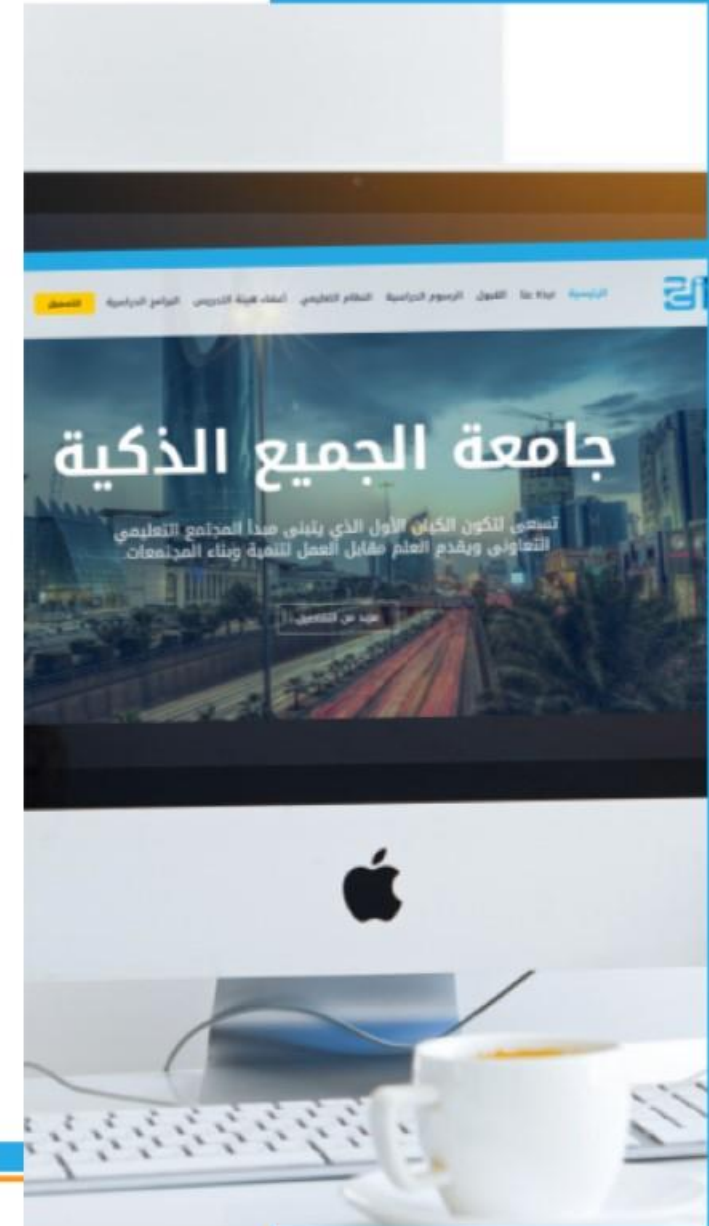


# Chapter 01

## Course Content

### Course Content:

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



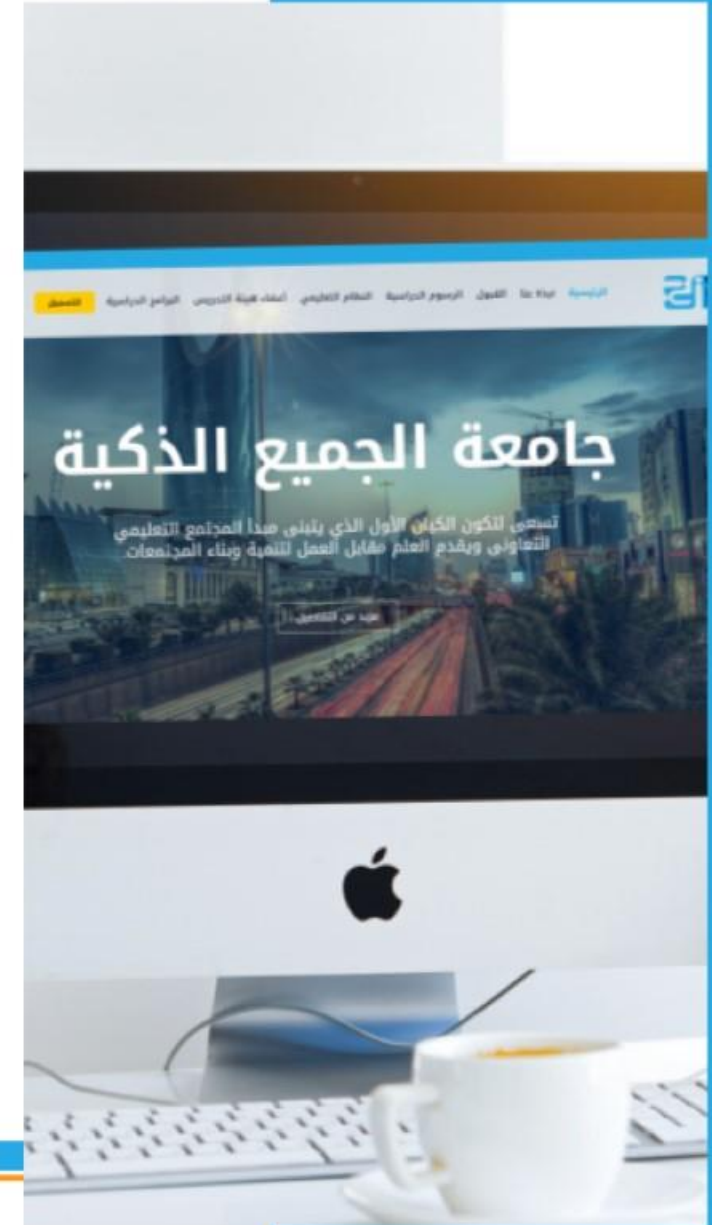
# Chapter 01

## Course Content

### Course Content:

#### ❑ Chapter 5: Introduction to Public Key Cryptography

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



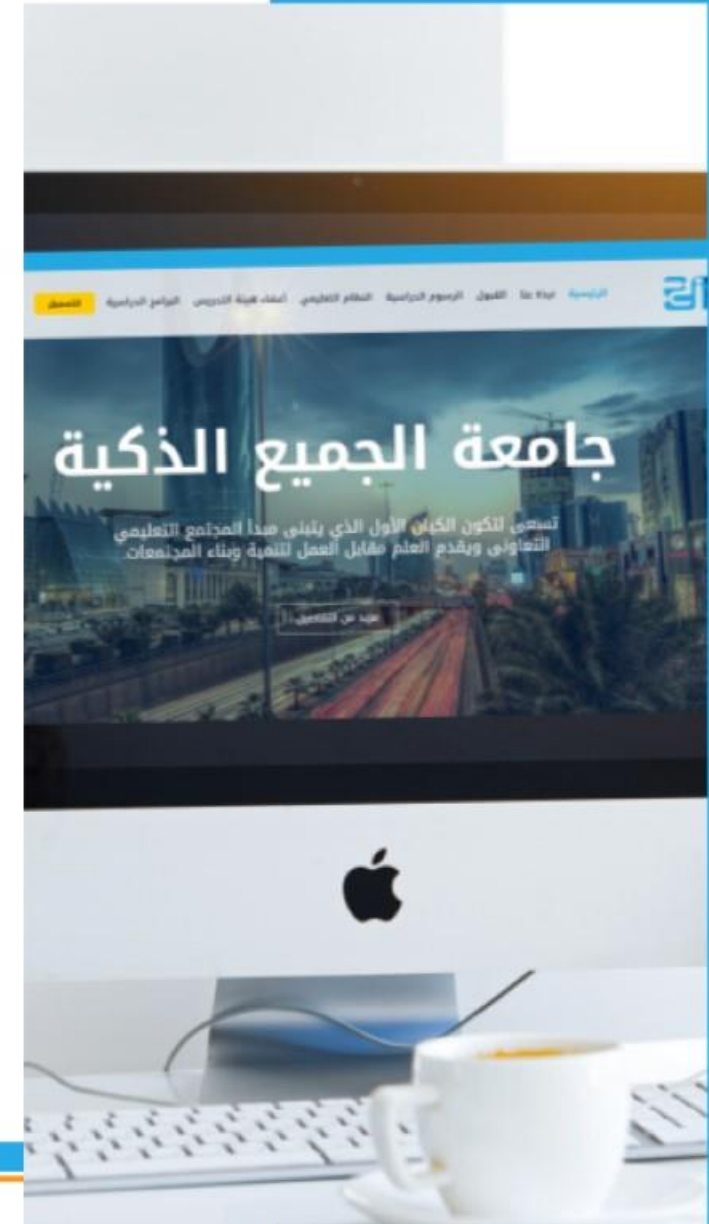
# Chapter 01

## Course Content

### Course Content:

#### ❑ Chapter 6: Public Key Cryptography

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

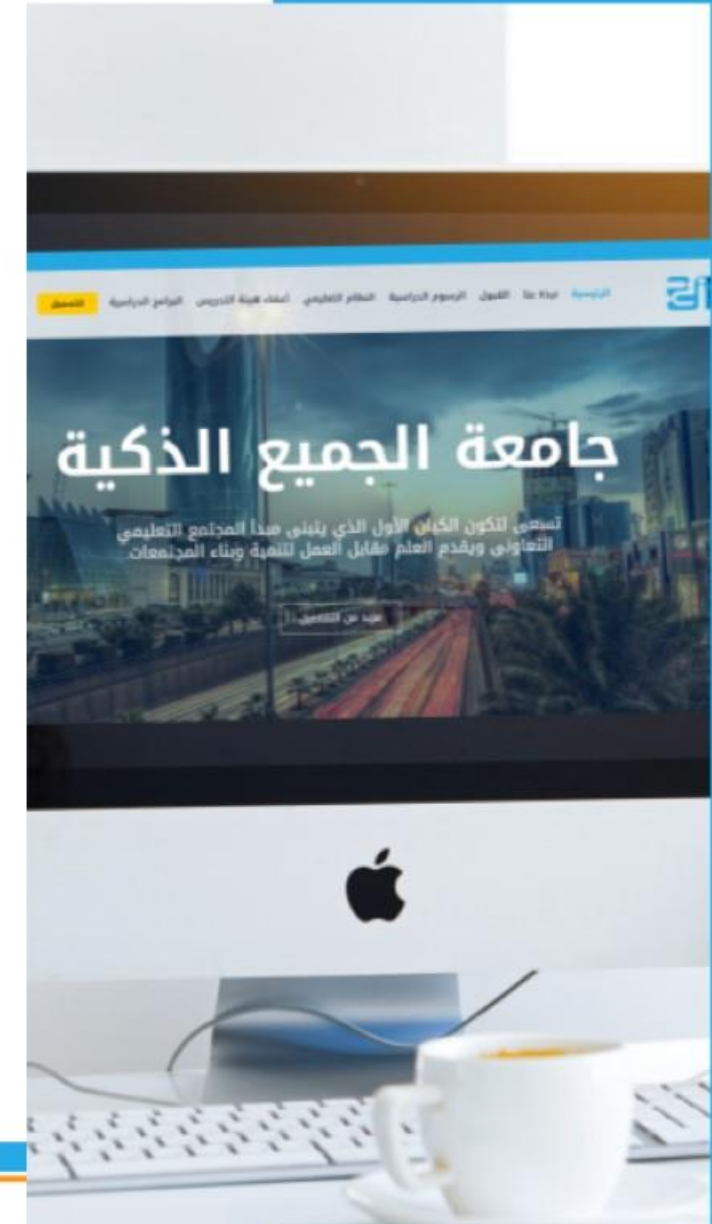


# Chapter 01

## Course Content

### Course Content:

- ❑ Chapter 7: Public Key Cryptography
  - ✓ Cryptographic Hash Functions

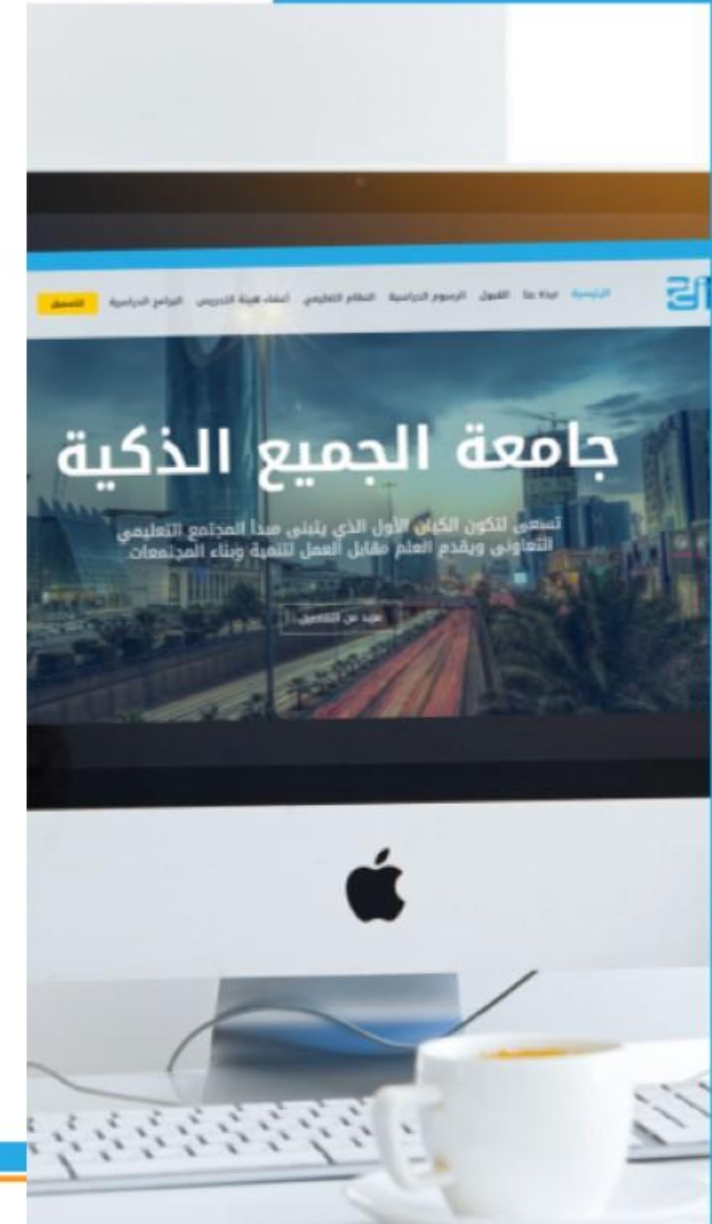


# Chapter 01

## Course Content

### Course Content:

- ❑ Chapter 8: Public Key Cryptography
  - ✓ Digital Signature

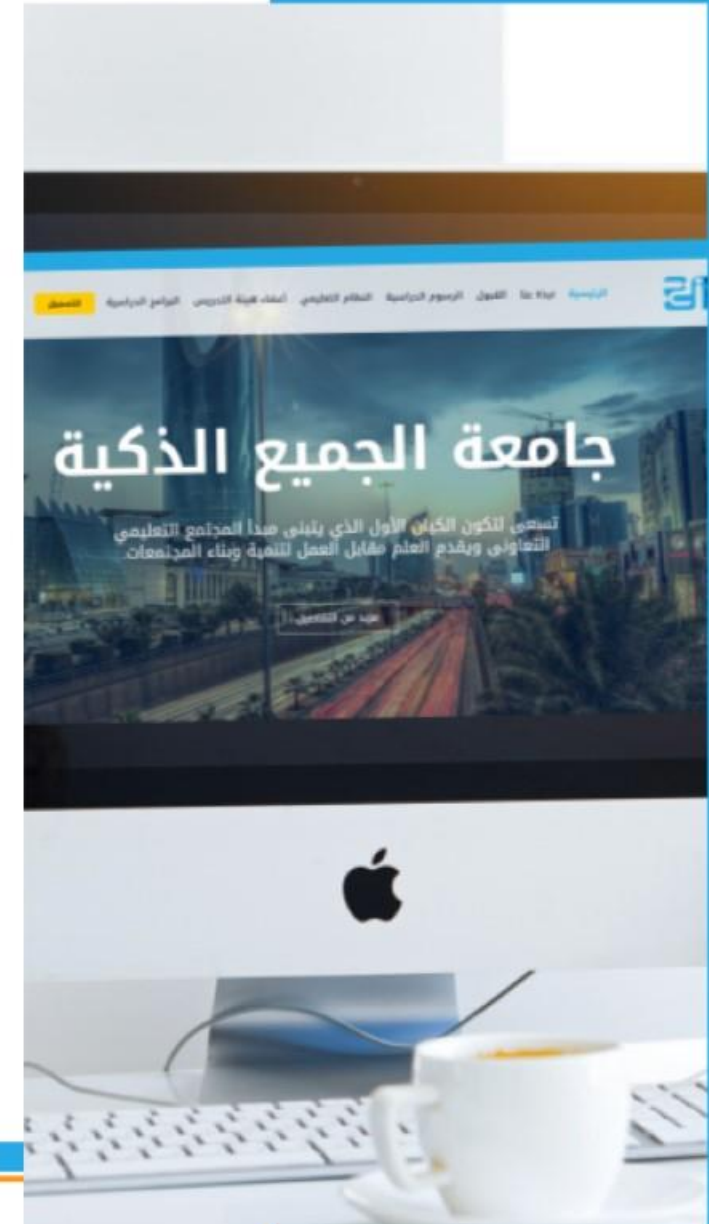


# Chapter 01

## Course Content

### Course Content:

- ❑ Chapter 9: Public Key Cryptography
  - ✓ Message Authentication Code



# Chapter 01

## Course Content

### Course Content:

- ❑ Chapter 10: User Authentication
  - ✓ User Authentication Methods

