وزارة التعليم العالي والبحث العلمي

جهاز الاشراف والتقويم العلمي

دائرة ضمان الجودة والاعتماد الأكاديمي

استمارة وصف البرنامج الأكاديمي للعام الدراسي ٢٠٢٥-٢٠٢٦ للكليات والمعاهد

الجامعة : جامعة شط العرب الاهلية

الكلية \المعهد : الكلية التقنية الهندسية

القسم العلمي : قسم هندسة تقنيات الحاسوب

تاريخ ملء الملف : ٢٠٢٥\٩\١

التوقيع

اسم رئيس القسم : م. قاسم عبدالجبار رشيد ازرام

التاريخ : ١ / ٩ / ٢٠٢٥

التوقيع

اسم المعاون العلمي : م. عصام خليل ابراهيم

التاريخ : ٢٠٢٥/٩/

م.عصام خليل ابراهيم
معاون العميد للشؤون العلمية

دقق الملف من قبل

شعبة ضمان الجودة والأداء الجامعي

اسم مدير شعبة ضمان الجودة والأداء الجامعي

مصادقة السيد العميد

أ.م.د. مازن عبدالاله علوان
عميد الكلية التقنية الهندسية

Ministry of Higher Education and Scientific Research

Supervision and Scientific Evaluation Body

Quality Assurance and Academic Accreditation Office

Course Description Sample

Subject: Security of computers and networks

1. Educational Institution	Shatt Al Arab University College
2. Department / Center	Computer Technology Engineering
3. Course Title /Code	Security of computers and networks
4. Lecturer Name	Asst. Lecturer. Athraa Qays Obaid
5. Type of Teaching	Lectures – Hands-on Labs
6. Academic Year /Term	2025/2026
7. Total No. of Teaching Hours	120
8. Date of Preparing this Course Description	11/10/2025

9. **Course Objectives**

- Deep understanding of encryption principles, algorithms, and protocols (symmetric, asymmetric, hashing, digital signatures, key exchange).
- Application of encryption for data confidentiality, integrity verification, and authentication in standalone and networked environments.
- Techniques for analyzing encryption systems to evaluate strengths and weaknesses.
- Discussion of protocols and methods for licensing, email protection, virtual private networks, and e-commerce security.

10. **Course Output, Methodology and Evaluation**

(A) **Cognitive Objectives**

1. Comprehensive understanding of computer and network security and protection mechanisms.
2. Distinction between classical and modern encryption systems and their mathematical principles.
3. Description of various cryptanalysis methods.
4. Overview of protocols for authorization, email protection, VPNs, and e-commerce.
5. Recommendations for securing data during processing, storage, and transmission, along with a summary of security threats and mitigation strategies.

(B) **Skill Objectives Related to the Program**:

1. Using encryption algorithms to protect stored and transmitted data.
2. Mathematical analysis of encrypted texts.
3. Implementing specific settings to protect computers and networks, prevent exploitation of security vulnerabilities, and address them.
4. Programming and implementing some encryption algorithms.

Methods of Teaching and Learning

1. Theoretical explanations with mathematical examples and diagrams.
2. Presentation of selected explanatory questions and solutions.
3. Class group discussions and oral questions.
4. Self-directed learning through report preparation.
5. Laboratory applications of practical course topics.

Methods of Evaluation

Number	calendar element	degree
1	Quizzes	5
2	Semester Exam	10
3	Practical Exam	5

4	Final Exam	60

(C) **Sentimental and Value Objectives**

1. Instilling a spirit of creativity and innovation in students.
2. Fostering a sense of responsibility among students.
3. Cultivating values of diligence and perseverance to achieve satisfactory results.
4. Enhancing students' ability to work collaboratively.

Methods of Teaching and Learning

1. Presenting scientific problems and asking students to find multiple solutions using different scientific methods to stimulate their creativity.

2. Forming teams that are evaluated based on their work results, with periodic changes to their structure, to foster a spirit of collaboration and encourage students to put forth their best efforts while working under various conditions and with different people.

Methods of Evaluation

1. Direct Assessment: This assessment is conducted by the instructor directly through observing student interaction and their application of emotional and value-based objectives, along with recording observations regarding that.

2. Practical Projects: The evaluation measures the student's ability to achieve and innovate, work within teams, and obtain results and solutions for various scientific problems faced by students.

D) **General and Qualitative Skills (other skills related to the ability of employment and personal development)**

1. Designing encryption and decryption programs.
2. Designing various programs for cryptanalysis.
3. Using MATLAB programming language to enhance students' programming skills in the field of computer network security.

11. **Course Structure**

Week	No of Hours	Required Learning Output	Title of Subject	Teaching Method	Evaluation
1,2, and 3	2 hrs theoretical /Practical	Understanding the concept of symmetric encryption, encryption algorithms, the encryption key, and the concept of cryptanalysis.	Symmetric Ciphers model: plaintext, encryption algorithm, secret key, ciphertext decryption algorithm, A Model of conventional encryption. Cryptography, Cryptanalysis, block and stream cipher	Lectures and practical laboratories	• Interactive assessment. • Periodic written tests. • Direct assessment.
4	2 hrs theoretical /Practical	Applying encryption and decryption processes to the simplest form of encryption.	Caeser Cipher the AffineCipher	Lectures and practical laboratories	• Interactive assessment. • Periodic written tests. • Direct assessment.
5, and 6	2 hrs theoretical /Practical	Understanding another type of encryption: the monoalphabetic cipher.	Mono alphabetic substitution ciphers Shift ciphers	Lectures and practical laboratories	• Interactive assessment. • Periodic written tests. • Direct assessment.
7	2 hrs theoretical /Practical	Understanding and applying the Hill cipher.	Hill cipher	Lectures and practical laboratories	• Interactive assessment. • Periodic written tests. • Direct assessment.

8	2 hrs theoretical /Practical	Applying encryption and decryption using matrix-based encryption.	Playfair cipher	Lectures and practical laboratories	• Interactive assessment. • Periodic written tests. • Direct assessment.
9	2 hrs theoretical /Practical	Encrypting and decrypting using polyalphabetic cipher methods.	Polyalphabetic ciphers Vigenère cipher	Lectures and practical laboratories	• Interactive assessment. • Periodic written tests. • Direct assessment.
10, 11, 12, And 13	2 hrs theoretical /Practical	Applying encryption and decryption to another type of encryption.	The Transposition cipher Affine cipher	Lectures and practical laboratories	• Interactive assessment. • Periodic written tests. • Direct assessment.
14, 15, And 16	2 hrs theoretical /Practical	Breaking a cipher with a symmetric key.	OTP	Lectures and practical laboratories	• Interactive assessment. • Periodic written tests. • Direct assessment.
17	2 hrs theoretical /Practical	Learning how to find the modular exponentiation using Euclid's method.	Cryptanalysis of a Symmetric key	Lectures and practical laboratories	• Interactive assessment. • Periodic written tests. • Direct assessment.
18, And 19	2 hrs theoretical /Practical	Applying encryption methods using a symmetric key.	Euclid's Algorithm	Lectures and practical laboratories	• Interactive assessment. • Periodic written tests. • Direct assessment.

20, 21, and 22	2 hrs theoretical /Practical	Applying encryption methods using an asymmetric key.	SYMMETRIC-KEY ALGORITHMS -Other Public-Key Algorithms	Lectures and practical laboratories	• Interactive assessment. • Periodic written tests. • Direct assessment.
23, 24, 25, 26, And 27	2 hrs theoretical /Practical	Implementing sender authentication methods.	AUTHENTICATION PROTOCOLS, -Authentication Based on a Shared Secret Key, -Establishing a Shared Key: The Diffie - Hellman Key Exchange, -Authentication Using a Key Distribution Center, -Authentication Using Kerberos, - Authentication Using Public-Key Cryptography	Lectures and practical laboratories	• Interactive assessment. • Periodic written tests. • Direct assessment.
28	2 hrs theoretical /Practical	Implementing email protection methods.	OSI security Architecture, a model for network security EMAIL SECURITY	Lectures and practical laboratories	• Interactive assessment. • Periodic written tests. • Direct assessment.
29, and 30	2 hrs theoretical /Practical	Understanding operating system protection methods.	PROTECTION SERVICES: • OS protection service: protected objects and methods of OS protection, security of OS, memory and addressing protection, fence protection • Database protection service: Network protection service: IP and E-	Lectures and practical laboratories	• Interactive assessment. • Periodic written tests. • Direct assessment.

			Commerce protection, VPN and next generation networks protection		

12.**Infrastructure**

a. Textbooks	William Stalling," cryptography and network security principles and practice ", 6th ed., 2015, Pearson.
b. References	William Stalling," cryptography and network security principles and practice ", 6th ed. , 2015, Pearson.
c. Recommended books and periodicals (journals, reports, etc.)	
d. Electronic references, internet websites, etc	Google

13. **The Plan of Improving the Course**
