Course Description Form

1. Course Name:

Data Security II

2. Course Code:

3. Semester / Year:

Second Semester 2024-2025

4. Description Preparation Date:

26/1/2025

5. Available Attendance Forms: In classroom

weekly Attendance

6. Number of Credit Hours (Total) / Number of Units (Total)

4 hours weakly (2 theoretical and 2 practical) totally 60 hours

7. Course administrator's name (mention all, if more than one name)

Name: Asst.Prof. Enas Tariq Khudair
Email: Enas.T.Khudiruotechnology.edu.iq

8. Course Objectives

Course Objectives	• Data security focuses protecting data fr unauthorized acc maintaining its integrity availability, and preventing from leaving the organizati This extends to many aspect a user's daily routine, and force point this largely cov activities in the cloud, w email, network, and endpoir

9. Teaching and Learning Strategies

Strategy	**A- Knowledge and Understanding** A1: - Demonstrate knowledge of the concepts, terminology, principles and methods of information security and data security. A2: Consider information hiding as an important tool for data security. A3: Present the mathematics important to cryptography in data security. A4: Discuss a wide range of traditional cryptographic techniques, available tools and practical methods in information security and cyberspace. A5. Express professional responsibilities and make judgments based on legal and ethical principles in the practice of computing.

B- Course specific skill objectives

B1: Identifies a set of solutions for modern and advanced methods of hacking or attacking data and computer networks.
B2: Evaluates gaps and weaknesses in information systems and computer networks.
B3: Identifies the time and cost of addressing damages resulting from any attack on an information system or institution.
B4: Evaluates appropriate tools and techniques to address damages resulting from security breaches.
B5: Identifies the policies, procedures and plans necessary to manage and ensure the security of institutions.
B6: Suggests e-learning courses to prepare for professional certificates.

C- Emotional and value objectives

C1: Apply different protocols for information and network confidentiality.
C2: Apply the principles of design, development and management in establishing computer networks.
C3: Uses different network protocols.
C4: Builds information systems and secures computer networks.
C5: Prepares and presents technical reports in a coherent and organized manner, orally and in writing.
C6: Uses best practices and standards in the field of information and network protection for various organizations.
A7: Deals with different types of breaches and incidents on computer networks and information systems.
A8: Discovers vulnerabilities and sources of attacks and hacking by monitoring the performance of computer networks and information systems.
A9: Uses and develops encryption and information security programs.

D- General and transferable skills (other skills related to employability and personal development)

D1: Actively participates in team-based activities as a member or leader of an information security team.
D2: Organizes and communicates ideas effectively, both verbally and in writing.
D3: Uses and employs IT skills to protect information and networks.
D4: Works independently and with others.
D5: Manages learning and self-development, including time management and organizational skills.
D6: Conducts practical training in relevant institutions and companies.
D7: Participates in continuing professional development and recognizes the need for lifelong learning.

10. Course Structure

Week	Hours	Required Learning Outcomes	Unit or subject name	Learning method	Evaluation method
1	2 theoretical 2 laboratories	1,2,3,4	Data encryption standard (DES), Block Cipher, ECB Operation Mode ,CBC Operation Mode, Output Feedback Mode (OFM), Product Cipher , Iterated Bock Cipher, Festal Cipher.	lectures + Video lectures +	Attendance + answer

				Application in the laboratory	discussion questions
2	2 theoretical 2 laboratories	1,2,3,4	DES Cipher, Data Encryption Standard (DES), (DES) Data Encryption Standard history, Description of DES , Outline of the Algorithm .	lectures + Video lectures + Application in the laboratory	Attendance + answer discussion questions
3	2 theoretical 2 laboratories	1,2,3,4	The initial Permutation , The key Transformation , The Expansion Permutation, The S-Box Substitution, The P-Box Permutation, The Final Permutation, Decryption DES.	lectures + Video lectures + Application in the laboratory	Attendance + answer discussion questions
4	2 theoretical 2 laboratories	1,2,3,4	Full Example of DES	lectures + Video lectures + Application in the laboratory	Attendance + answer discussion questions
5	2 theoretical 2 laboratories	1,2,3,4	Exponential Cipher , Introduction, Public Key Cryptography , Public Key Applications, Security of Public Key Schemes .	lectures +	Attendance + answer

				Video lectures + Application in the laboratory	discussion questions
6	2 theoretical 2 laboratories	1,2,3,4	Exponential Cipher, pohling- Hellman Scheme, RSA description and algorithm , key generation algorithm , Encryption , Decryption	lectures + Video lectures + Application in the laboratory	Attendance + answer discussion questions
7	2 theoretical 2 laboratories	1,2,3,4	A Simple example of RSA encryption , Security Concern, Secrecy and Authenticity	lectures + Video lectures + Application in the laboratory	Attendance + answer discussion questions
8	2 theoretical 2 laboratories	1,2,3,4	Merkle-Hellman Knapsacks, MH Knapsack, Diffie-Hellman Knapsack	lectures + Video lectures + Application in the laboratory	Attendance + answer discussion questions

9	2 theoretical 2 laboratories	1,2,3,4	Stream Cipher , One time pad vernam cipher, drawback , solution , randomness, pseudo randomness, synchronous stream cipher ,self-synchronous stream cipher ,	lectures + Video lectures + Application in the laboratory	Attendance + answer discussion questions
10	2 theoretical 2 laboratories	1,2,3,4	Linear feedback shift registers, non-linear combination , generators nonlinear filter generator	lectures + Video lectures + Application in the laboratory	Attendance + answer discussion questions
11	2 theoretical 2 laboratories	1,2,3,4	Example (gaffe generator) randomness key tests	lectures + Video lectures + Application in the laboratory	Attendance + answer discussion questions

11. Course Evaluation

Attendance - oral exams and tests - mid-course exam - end-of-course exam

12. Learning and Teaching Resources

Required textbooks (curricular books, if any)	Not required
Main references (sources)	William Stallings, Cryptography and Network Security,(Principal and Practice) 2003

Recommended books and references (scientific journals, reports…)	William Stallings, Cryptography and Network Security,(Principal and Practice) 2011
Electronic References, Websites	