



MODULE DESCRIPTION FORM

نموذج وصف المادة الدراسية

Module Information			
معلومات المادة الدراسية			
Module Title	Data Security Principles		Module Delivery
Module Type	Core		☒ Theory ☒ Lecture ☐ Lab ☐ Tutorial ☐ Practical ☐ Seminar
Module Code	CYS109		
ECTS Credits	5		
SWL (hr/sem)	125		
Module Level	1	Semester of Delivery	
Administering Department	Dept. of Cybersecurity	College	College of Information Technology
Module Leader	Dr. Ahmad A. AlSabhany	e-mail	Ahmad.alsabhany@uofallujah.edu.iq
Module Leader's Acad. Title	Lect.	Module Leader's Qualification	Ph.D.
Module Tutor	Dr. Ahmad A. AlSabhany	e-mail	Ahmad.alsabhany@uofallujah.edu.iq
Peer Reviewer Name	Dr. Omar Salah Farhan	e-mail	omar.alshareef@uofallujah.edu.iq
Scientific Committee Approval Date	25-5-2026	Version Number	1.0

Relation with other Modules			
العلاقة مع المواد الدراسية الأخرى			
Prerequisite module	None	Semester	
Co-requisites module	None	Semester	

Module Aims, Learning Outcomes and Indicative Contents

أهداف المادة الدراسية ونتائج التعلم والمحتويات الإرشادية

Module Objectives أهداف المادة الدراسية	1. Explain the fundamental concepts of data security, including the importance of protecting digital information and the core security objectives such as confidentiality, integrity, and availability. 2. Differentiate between cryptography, cryptanalysis, and cryptology, and describe the role of cryptographic techniques in securing communication systems. 3. Describe the components of an encryption system, including plaintext, ciphertext, encryption algorithms, secret keys, and decryption processes. 4. Apply modular arithmetic concepts in cryptographic operations, and perform calculations used in classical encryption algorithms. 5. Implement and analyze classical cryptographic algorithms, such as the Caesar cipher and affine cipher, and evaluate their security limitations. 6. Explain the principles of stream ciphers and the One-Time Pad, including the use of XOR operations and keystream generation for encryption and decryption. 7. Discuss the concept of pseudorandom number generation and its role in generating secure keystreams for cryptographic systems. 8. Describe the design principles of modern block ciphers, including confusion and diffusion, and explain the basic structure and operation of the Data Encryption Standard (DES). 9. Evaluate the strengths and limitations of different cryptographic techniques, including classical ciphers, stream ciphers, and block ciphers.
Module Learning Outcomes مخرجات التعلم للمادة الدراسية	1. MLO1. Explain the fundamental concepts of data security and identify the key objectives of information protection, including confidentiality, integrity, and availability. 2. MLO2. Describe the principles of cryptography and distinguish between cryptography, cryptanalysis, and cryptology. 3. MLO3. Analyze the structure of encryption systems and identify the roles of plaintext, ciphertext, encryption algorithms, secret keys, and decryption processes. 4. MLO4. Apply modular arithmetic operations used in classical cryptographic algorithms. 5. MLO5. Implement and evaluate classical encryption techniques such as the Caesar cipher and affine cipher. 6. MLO6. Demonstrate how stream ciphers operate using XOR operations and keystream generation, including the One-Time Pad. 7. MLO7. Explain the role of pseudorandom number generators in cryptographic systems. 8. MLO8. Describe the structure and operation of modern block ciphers, with emphasis on the design and operation of the Data Encryption Standard (DES). 9. MLO9. Compare different cryptographic approaches and evaluate their strengths and limitations in practical security applications.
Indicative Contents المحتويات الإرشادية	Total hrs = 48 = SSWL - (Exam hrs) = 48 - 3 = 45 hr (Time table hrs x 15 weeks)

Learning and Teaching Strategies

استراتيجيات التعلم والتعليم

Strategies	1. Conceptual Lectures – Focused lectures explaining the principles of cryptographic systems, including cipher structures, security goals, and algorithm design. 2. Analytical Problem Solving – Guided exercises that develop understanding of the mathematical foundations of cryptography, including modular arithmetic and complexity considerations. 3. Cipher System Analysis – Activities that examine classical and modern encryption techniques, emphasizing key space size, entropy, and resistance to attacks.
-------------------	---

Student Workload (SWL)

الحمل الدراسي للطلاب محسوب لـ ١٥ اسبوعا

Structured SWL (h/sem) الحمل الدراسي المنتظم للطلاب خلال الفصل	48	Structured SWL (h/w) الحمل الدراسي المنتظم للطلاب أسبوعيا	3
Unstructured SWL (h/sem) الحمل الدراسي غير المنتظم للطلاب خلال الفصل	77	Unstructured SWL (h/w) الحمل الدراسي غير المنتظم للطلاب أسبوعيا	5
Total SWL (h/sem) الحمل الدراسي الكلي للطلاب خلال الفصل	150		

Module Evaluation

تقييم المادة الدراسية

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	Assignments	2	10% (10)	5 and 10	All
	Quiz	1	10% (10)	4	LO #1 - #3
	Quiz	1	10% (10)	9	LO #4 - #7
	Report	1	10% (10)	13	LO #7 - #9
Summative assessment	Midterm Exam	2hr	10% (10)	7	LO #1 - #6
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus) المنهاج الاسبوعي النظري	
	Material Covered
Week 1	Introduction to Data Security: Data, Information, Knowledge, and Information Systems
Week 2	Computer Security Concepts and the CIA Triad (Confidentiality, Integrity, Availability)
Week 3	Security Terminology: Threats, Vulnerabilities, Attacks, Risk, Security Policies
Week 4	Security Services, Security Technologies, and Security Requirements
Week 5	Classical Cryptography: Caesar Cipher and its limitations
Week 6	Mathematical Foundations of Cryptography: Modular Arithmetic
Week 7	Modular Arithmetic Applications in Cryptography
Week 8	Affine Cipher: Encryption, Decryption, and Key Space Analysis
Week 9	Affine Cipher Exercises
Week 10	Cryptanalysis of Classical Ciphers
Week 11	Stream Ciphers vs Block Ciphers
Week 12	Random Number Generators (TRNG, PRNG, CSPRNG)
Week 13	Block Cipher Design Principles and Overview of DES
Week 14	DES Components Overview and Security Analysis
Week 15	Course Revision and Final Review
Week 16	Preparatory week before the final Exam

Learning and Teaching Resources مصادر التعلم والتدريس		
	Text	Available in the Library?
Required Texts	Cryptography And Network Security Principles and Practice, William Stallings, Fifth Edition	Yes
Recommended Texts	Understanding Cryptography, Christof Paar and Jan Pelzl	Yes
Websites		

Grading Scheme مخطط الدرجات				
Group	Grade	التقدير	Marks %	Definition
Success Group	A - Excellent	امتياز	90 - 100	Outstanding Performance

(50 - 100)	B - Very Good	جيد جدا	80 - 89	Above average with some errors
	C - Good	جيد	70 - 79	Sound work with notable errors
	D - Satisfactory	متوسط	60 - 69	Fair but with major shortcomings
	E - Sufficient	مقبول	50 - 59	Work meets minimum criteria
Fail Group (0 – 49)	FX – Fail	راسب (قيد المعالجة)	(45-49)	More work required but credit awarded
	F – Fail	راسب	(0-44)	Considerable amount of work required
Note: Marks Decimal places above or below 0.5 will be rounded to the higher or lower full mark (for example a mark of 54.5 will be rounded to 55, whereas a mark of 54.4 will be rounded to 54. The University has a policy NOT to condone "near-pass fails" so the only adjustment to marks awarded by the original marker(s) will be the automatic rounding outlined above.				