University of Fallujah
College of Information Technology
Department of Cybersecurity

MODULE DESCRIPTION FORM

نموذج وصف المادة الدراسية

Module Information معلومات المادة الدراسية					
Module Title	**Cryptography**			**Module Delivery**	
Module Type	**Core**			☒ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	**CYS229**				
ECTS Credits	**6**				
SWL (hr/sem)	**150**				
Module Level	2		**Semester of Delivery**	1	
Administering Department	Dept. of Cybersecurity		**College**	College of Information Technology	
Module Leader	Dr. Ahmad AlSabhany		**e-mail**	Ahmad.alsabhany@uofallujah.edu.iq	
Module Leader's Acad. Title	Asst. Prof.		**Module Leader's Qualification**	Ph.D.	
Module Tutor	Prof. Ali Makki Sagheer Saleh		**e-mail**	ali_makki@uoanbar.edu.iq	
Peer Reviewer Name	Prof. Ali Makki Sagheer		**e-mail**	ali_makki@uoanbar.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**	The module builds upon the programming knowledge and skills acquired in Data Security Principles (CYS109). 1. Develop a solid understanding of the principles and security goals of modern cryptography. 2. Review classical cryptographic techniques and their historical significance. 3. Understand the design and operation of symmetric-key cryptographic systems. 4. Analyze and apply stream ciphers, block ciphers, and modern encryption algorithms, including DES, AES, and ChaCha20. 5. Develop practical cryptographic skills using CrypTool2 for encryption, decryption, and algorithm analysis. 6. Acquire foundational knowledge of public-key cryptography and key establishment mechanisms, including Diffie–Hellman. 7. Prepare for advanced study in cryptography, cryptanalysis, and secure communication protocols.
Module Learning Outcomes **مخرجات التعلم للمادة الدراسية**	1. Explain the fundamental principles, terminology, and security goals of modern cryptography. 2. Describe and apply classical cryptographic techniques and evaluate their strengths and limitations. 3. Analyze the operation of symmetric-key cryptographic systems, including stream ciphers and block ciphers. 4. Apply modern encryption algorithms, including DES, AES, and ChaCha20, to protect digital information. 5. Utilize CrypTool2 to perform encryption, decryption, and cryptographic experiments involving various cryptographic algorithms. 6. Explain the principles of public-key cryptography and the operation of key establishment mechanisms such as Diffie–Hellman. 7. Demonstrate readiness for advanced study in cryptography, cryptanalysis, and secure communication protocols.
Indicative Contents **المحتويات الإرشادية**	• Introduction to Modern Cryptography • Security Goals and Cryptographic Terminology • Review of Classical Cryptographic Techniques • Substitution and Transposition Ciphers • Caesar, Vigenère, and Playfair Ciphers • Cryptanalysis of Classical Ciphers • Symmetric-Key Cryptography Fundamentals • Stream Cipher Principles and Applications

	• Block Cipher Principles and Applications • Feistel Networks and Product Ciphers • Data Encryption Standard (DES) • Triple DES (3DES) • Advanced Encryption Standard (AES) • ChaCha20 and Modern Stream Ciphers • Modes of Operation for Block Ciphers • Key Management in Symmetric Cryptography • Introduction to Public-Key Cryptography • Diffie–Hellman Key Exchange • Key Establishment and Secure Communication Concepts • Practical Cryptography Using CrypTool

Learning and Teaching Strategies استراتيجيات التعلم والتعليم	
Strategies	**The module is delivered through lectures, laboratory sessions, guided practical exercises, and problem-solving activities. Students develop theoretical and practical cryptographic skills through the analysis and application of classical and modern cryptographic algorithms. Hands-on laboratory work using CrypTool2 enables students to perform encryption, decryption, and cryptographic experiments, while strengthening their understanding of symmetric-key cryptography and key establishment mechanisms.**

Student Workload (SWL) الحمل الدراسي للطالب محسوب لـ ١٥ اسبوعا			
Structured SWL (h/sem) الحمل الدراسي المنتظم للطالب خلال الفصل	78	**Structured SWL (h/w)** الحمل الدراسي المنتظم للطالب أسبوعيا	5
Unstructured SWL (h/sem) الحمل الدراسي غير المنتظم للطالب خلال الفصل	72	**Unstructured SWL (h/w)** الحمل الدراسي غير المنتظم للطالب أسبوعيا	5
Total SWL (h/sem) الحمل الدراسي الكلي للطالب 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 - #2
	Quiz	1	10% (10)	9	LO #4 - #7
	Lab	1	10% (10)	13	All
Summative assessment	**Midterm Exam**	2hr	10% (10)	7	LO #1 - #3
	Final Exam	3hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

المنهاج الاسبوعي النظري

	Material Covered
Week 1	**Review of Classical Cryptography: Caesar, Substitution, and Transposition Ciphers**
Week 2	**Vigenère, Playfair, and Classical Cryptanalysis**
Week 3	**Symmetric-Key Cryptography Fundamentals and Security Analysis**
Week 4	**Stream Ciphers and Pseudorandom Number Generation (LCG, LFSR)**
Week 5	**Block Cipher Fundamentals and Feistel Networks**
Week 6	**Data Encryption Standard (DES) and Triple DES**
Week 7	**Block Cipher Modes, Padding, Modes of Operation (ECB, CBC, CFB, OFB, CTR), and Pitfalls**
Week 8	**Midterm Examination**
Week 9	**Advanced Encryption Standard (AES): Structure and Design**
Week 10	**Advanced Encryption Standard (AES): Modes of Operation and Applications**
Week 11	**ChaCha20 and Modern Stream Cipher Design**
Week 12	**ChaCha20 Applications, Performance, and Security Analysis**
Week 13	**Practical Cryptographic Systems: PGP, GPG, and File Encryption**
Week 14	**Introduction to Public-Key Cryptography and Diffie–Hellman Key Exchange**
Week 15	**Cryptographic Applications, Algorithm Comparison, Course Review, and Final Preparation**
Week 16	**Review of Classical Cryptography: Caesar, Substitution, and Transposition Ciphers**

Delivery Plan (Weekly Lab. Syllabus)

المنهاج الاسبوعي للمختبر

	Material Covered
Week 1	**Classical Ciphers using CrypTool 2: Caesar, Substitution, and Transposition**
Week 2	**Vigenère and Playfair Ciphers with Classical Cryptanalysis**
Week 3	**Implementing Classical Ciphers in C++**
Week 4	**Stream Cipher Fundamentals and XOR Encryption using Python**

Week 5	**Pseudorandom Number Generation and Stream Cipher Analysis**
Week 6	**Exploring Block Ciphers and Feistel Networks using CrypTool 2**
Week 7	**DES and Triple DES Experiments using CrypTool 2 and CyberChef**
Week 8	**Midterm Practical Assessment**
Week 9	**AES Encryption and Key Management using CrypTool 2**
Week 10	**AES File Encryption and Modes of Operation using OpenSSL in Kali Linux**
Week 11	**ChaCha20 Encryption and Secure Random Generation using Python**
Week 12	**Comparative Analysis of DES, AES, and ChaCha20 using CrypTool 2, Python, and OpenSSL**
Week 13	**Hashing, Message Integrity, and Password Verification using OpenSSL and CyberChef**
Week 14	**Diffie–Hellman Key Exchange Simulation using CrypTool 2 and Python**
Week 15	**Integrated Cryptography Project and Practical Review**

Learning and Teaching Resources **مصادر التعلم والتدريس**		
	Text	**Available in the Library?**
Required Texts	1. Cryptography And Network Security Principles and Practice, William Stallings, Fifth Edition	Yes
Recommended Texts	2. Stallings, W. (2023). *Cryptography and Network Security: Principles and Practice* (8th ed.). Pearson. 3. Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley. 4. Easttom, C. (2022). *Modern Cryptography: Applied Mathematics for Encryption and Information Security* (2nd ed.). Springer.	Yes
Websites	• https://www.cryptool.org/en/ • https://gchq.github.io/CyberChef/	

Grading Scheme: مخطط الدرجات				
Group	**Grade**	**التقدير**	**Marks %**	**Definition**
Success Group (50 - 100)	**A** - Excellent	**امتياز**	90 - 100	Outstanding Performance
	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.