MODULE DESCRIPTION FORM

Module Information					
Module Title	**Cybersecurity**			**Module Delivery**	
Module Type	**Core**			☑ Theory ☑ Lecture ☑ Lab ☑ Tutorial ☑ Practical ☐ Seminar	
Module Code	**AIE326**				
ECTS Credits	**4**				
SWL (hr/sem)	**100 H/Sem.**				
Module Level	3	**Semester of Delivery**	6		
Administering Department	Artificial Intelligence Eng.	**College**	College of Engineering		
Module Leader	Jamal Muhsen Alawi	**e-mail**			
Module Leader's Acad. Title	Lecturer	**Module Leader's Qualification**	MSC		
Module Tutor	Abbas Hameed	**e-mail**			
Peer Reviewer Name	Hasnaa Mohammad	**e-mail**			
Scientific Committee Approval Date		**Version Number**	1.0		

Relation with other Modules			
Prerequisite module	**NONE**	**Semester**	
Co-requisites module	**NONE**	**Semester**	

Module Aims, Learning Outcomes and Indicative Contents	
Module Objectives	**Introduction to security of computer ,Symmetric Ciphers Model , Conventional Encryption Model, Cryptography Concepts: Cryptography, Cryptanalysis, Block Cipher, Stream Cipher, Classical Encryption Techniques: Caesar, Affine, Monoalphabetic, Hill, Playfair, Vigenere, Transposition, One Time Pad, Symmetric-Key Algorithms: Euclid Algorithm, DES, Feistel System, Public-Key Algorithms: RSA • Other Public Key Algorithms • Authentication Protocols: Shared Secret Key, Diffie-Hellman, KDC, Kerberos, Public-Key Authentication, OSI Security Architecture: Network Security Model, Email Security: PGP, S/MIME, Protection Services: OS Protection, Database Protection, Network Protection.**

Module Learning Outcomes	Knowledge	A1	**A1.1** Define the fundamental concepts of computer security and the importance of protecting information systems and networks. **A1.2** Explain the principles of cryptography including Cryptography, Cryptanalysis, Block Ciphers, and Stream Ciphers. **A1.3** Describe classical encryption techniques such as Caesar, Affine, Monoalphabetic, Hill, Playfair, Vigenere, Transposition, and One-Time Pad. **A1.4** Explain symmetric encryption models including the Symmetric Cipher Model and the Conventional Encryption Model. **A1.5** Illustrate symmetric-key algorithms including the Euclid Algorithm, Data Encryption Standard (DES), and the Feistel System. **A1.6** Describe public-key cryptography and explain the RSA algorithm and other public-key algorithms used for secure communication. **A1.7** Explain authentication protocols including Shared Secret Key authentication, Diffie–Hellman key exchange, Key Distribution Center (KDC), Kerberos, and Public-Key Authentication. **A1.8** Describe the OSI Security Architecture and the Network Security Model used to protect communication systems. **A1.9** Explain email security mechanisms including Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME). **A1.10** Discuss protection services including Operating System Protection, Database Protection, and Network Protection.
		A4	**A4.1** Recognize the basic concepts of computer security and cryptographic systems. **A4.2** Identify different classical encryption techniques and analyze their strengths and weaknesses. **A4.3** Apply symmetric encryption algorithms such as DES and understand their role in secure data communication. **A4.4** Implement public-key cryptography techniques such as RSA for secure key exchange and encryption. **A4.5** Demonstrate authentication protocols including Diffie–Hellman, Kerberos, and shared secret authentication mechanisms. **A4.6** Apply the OSI security architecture and network security model to analyze secure communication systems.

			A4.7 Evaluate email security mechanisms such as PGP and S/MIME for protecting electronic communication. **A4.8** Analyze different protection services including operating system, database, and network protection techniques to enhance system security.
	Skills	B1	B.1.1 Function efficiently as an individual B.1.2 Function as a member of multidisciplinary and multicultural teams.
		B3	B.3.1 Acquire and apply new knowledge. B.3.2 Practice the strategies of searching for information in life – long self-learning
	Ethics	C3	C.3.1 Utilize contemporary technologies. C.3.2 Make use of codes of practice and standards, quality guidelines. C.3.3 Utilize health and safety requirements C.3.4 Show environmental issues and risk management principles.
Indicative Contents	Indicative content includes the following. **Unit 1:** Introduction to Computer Security, Security of Computer Systems, Cryptography Concepts including Cryptography, Cryptanalysis, Block Cipher, and Stream Cipher. [6 hours] **Unit 2:** Classical Encryption Techniques including Caesar, Affine, Monoalphabetic, Hill, Playfair, Vigenere, Transposition, and One Time Pad. [8 hours] **Unit 3:** Symmetric Encryption Models including Symmetric Ciphers Model, Conventional Encryption Model, Euclid Algorithm, DES, and Feistel System. [4 hours] **Unit 4:** Public-Key Algorithms including RSA and Other Public Key Algorithms, Authentication Protocols including Shared Secret Key, Diffie-Hellman, KDC, Kerberos, and Public-Key Authentication. [6 hours] **Unit 5:** OSI Security Architecture and Security Applications including Network Security Model, Email Security (PGP, S/MIME), and Protection Services such as OS Protection, Database Protection, and Network Protection. [6 hours]		
Learning and Teaching Strategies			
Strategies	• Presentation • Interactive learning • Discussions • Brainstorming • Group Solving Problems • Problem-Based Learning • Self-learning		

Student Workload (SWL) for 15 weeks			
Structured SWL (h/sem)	78	**Structured SWL (h/w)**	5.2
Unstructured SWL (h/sem)	22	**Unstructured SWL (h/w)**	4.8
Total SWL (h/sem)	100		

Module Evaluation

تقييم المادة الدراسية

		Time/Number	Weight (Marks)	Week Due	Relevant Learning Outcome
Formative assessment	**Quizzes**	2	10% (10)	5 and 10	A1
	Assignments	2	10% (10)	2, 4,6,8,10,12 and 14	A1
	Projects / Lab.	2	10% (10)	2, 4,6,8,10,12 and 14	A4, B1, B3, C3
	Report	1	10% (10)	13	A1,A4, B1, B3
Summative assessment	**Midterm Exam**	1hr	10% (10)	7	A1, A4
	Final Exam	3hr	50% (50)	15	A1, A4
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus)

المنهاج الاسبوعي النظري

Weeks	Material Covered	Los
Week 1	Introduction to Computer Security	A1.1, B1.1, B1.2, B3.1, C3.1
Week 2	Security of Computer Systems and Cryptography Concepts (Cryptography, Cryptanalysis, Block Cipher, Stream Cipher)	A1.2, A4.1, B1.1, B1.2, B3.1, C3.1

Week 3	Classical Encryption Techniques: Caesar, Affine, Monoalphabetic	A1.3, A4.2, B1.1, B1.2, B3.1, C3.1
Week 4	Classical Encryption Techniques: Hill, Playfair, Vigenere	A1.3, A4.2, B1.1, B1.2, B3.1, C3.1
Week 5	Transposition Cipher and One Time Pad	A1.3, A4.2, B1.1, B1.2, B3.1, C3.1
Week 6	Symmetric Cipher Model and Conventional Encryption Model	A1.4, A4.3, B1.1, B1.2, B3.1, C3.1
Week 7	Symmetric-Key Algorithms: Euclid Algorithm, DES, Feistel System	A1.5, A4.3, B1.1, B1.2, B3.1, C3.1
Week 8	Public-Key Algorithms: RSA and Other Public Key Algorithms	A1.6, A4.4, B1.1, B1.2, B3.1, C3.1
Week 9	Authentication Protocols: Shared Secret Key, Diffie-Hellman	A1.7, A4.5, B1.1, B1.2, B3.1, C3.1
Week 10	Mid-term EXAM	A1, A4
Week 11	Authentication Protocols: KDC, Kerberos, Public-Key Authentication	A1.7, A4.5, B1.1, B1.2, B3.1, C3.1
Week 12	OSI Security Architecture and Network Security Model	A1.8, A4.6, B1.1, B1.2, B3.1, C3.1
Week 13	Email Security: PGP and S/MIME	A1.9, A4.7, B1.1, B1.2, B3.1, C3.1
Week 14	Protection Services: OS Protection, Database Protection, Network Protection	A1.10, A4.8, B1.1, B1.2, B3.1, C3.1
Week 15	Rubric Exam Preparatory week before the final Exam	A1, A4, B1, C3

Delivery Plan (Weekly Lab. Syllabus) المنهاج الاسبوعي للمختبر		
Weeks	**Material Covered**	**Los**
Week 1	Introduction to Cyber Security Lab Environment: Introduction to MATLAB environment and basic commands used for cryptographic computations.	A4.1, B1.1, B1.2, B3.1, C3.1, C3.2
Week 2	Classical Encryption Practice: Implement Caesar Cipher, Affine Cipher, and Monoalphabetic Cipher using Python.	A4.1, B1.1, B1.2, B3.1, C3.1, C3.2
Week 3	Classical Encryption Practice: Implement Hill Cipher, Playfair Cipher, and Vigenere Cipher.	A4.1, B1.1, B1.2, B3.1, C3.1, C3.2
Week 4	Transposition Cipher and One Time Pad implementation and analysis.	A4.2, B1.1, B1.2, B3.1, C3.1, C3.2
Week 5	Symmetric Encryption: Implement simplified DES structure and Feistel Network concept.	A4.3, B1.1, B1.2, B3.1, C3.1, C3.2
Week 6	Euclid Algorithm implementation for computing GCD and modular arithmetic used in cryptography.	A4.3, B1.1, B1.2, B3.1, C3.1, C3.2

Week 7	Public Key Cryptography: Implement RSA algorithm and encryption/decryption process.	A4.4, B1.1, B1.2, B3.1, C3.1, C3.2
Week 8	Key Exchange: Implement Diffie-Hellman key exchange algorithm.	A4.4, B1.1, B1.2, B3.1, C3.1, C3.2
Week 9	Authentication Protocol Simulation: Shared Secret Key authentication.	A4.5, B1.1, B1.2, B3.1, C3.1, C3.2
Week 10	Mid -term EXAM	A1, A4
Week 11	Authentication Systems: Simulation of Kerberos authentication protocol.	A4.5, B1.1, B1.2, B3.1, C3.1, C3.2
Week 12	Email Security: Demonstration of PGP and S/MIME encryption and digital signatures.	A4.6, B1.1, B1.2, B3.1, C3.1, C3.2
Week 13	Mini Cyber Security Project: Implement and test a selected encryption or authentication system.	A1, A4, B1, B3, C3
Week 14	Rubric Exam Preparatory week before the final Exam	A1, A4

Learning and Teaching Resources
مصادر التعلم والتدريس

	Text	Available in the Library?
Required Texts	**Behrouz A. Forouzan**, *Cryptography and Network Security*, 4th Edition, McGraw-Hill, 2017.	YES
Recommended Texts	**William Stallings**, *Cryptography and Network Security: Principles and Practice*, 8th Edition, Pearson, 2019.	NO
Websites	https://eng.alayen.edu.iq//colleges/e/42	

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.