MODULE DESCRIPTION FORM

نموذج وصف المادة الدراسية

Module Information معلومات المادة الدراسية					
Module Title	**Network Security & Cybersecurity**			**Module Delivery**	
Module Type	**Core**			☒ **Theory** ☒ **Lecture** ☒ **Lab** ☐ **Tutorial** ☐ **Practical** ☐ **Seminar**	
Module Code	**CET4203**				
ECTS Credits	**5**				
SWL (hr/sem)	**150**				
Module Level	4		**Semester of Delivery**	8	
Administering Department	CET		**College**	EETC	
Module Leader	Dr. Mohammed Joudah		**e-mail**	mjzaiter@mtu.edu.iq	
Module Leader's Acad. Title	Professor		**Module Leader's Qualification**	Ph.D.	
Module Tutor	Asst. Prof. Omar Nameer Mohammed Salim		**e-mail**	Omar Nameer Mohammed Salim	
Peer Reviewer Name	Dr. Mahmoud Shuker Mahmoud		**e-mail**	mahmoud.shukur@mtu.edu.iq	
Scientific Committee Approval Date	13/06/2023		**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 Aims أهداف المادة الدراسية	Upon completion of this course you will have acquired the following knowledge: 1. Understand hacking techniques. 2. Understand the fundamentals of secure network design. 3. Understand the issues involved with providing secure networks. 4. Understand underlying cryptography required for secure communications, authorization and 5. authorization. 6. Obtain hands on experience in cryptography and network security through laboratory work
Module Learning Outcomes مخرجات التعلم للمادة الدراسية	1. Students will be able to explain security principles. 2. Develop Concept of Security needed in Communication of data through computers and networks along with Various Possible Attacks. 3. Understand Various Encryption mechanisms for secure transmission of data and management of key required for required for encryption. 4. Students will be able to evaluate risks faced by computer systems and how various attacks work. 5. Students will be able to explain how various security mechanisms work, and correlate these security mechanisms with security principles. 6. Students will be able to compare various security mechanisms and articulate their advantages and limitations. 7. Understand authentication requirements and study various authentication mechanisms. 8. Understand network security concepts and study different Web security mechanisms. 9. Students will be able to create cybersecurity policies and procedures to help 10. secure a medium-sized organization's information technology infrastructure. 11. Students will understand the latest techniques hackers employ to test out cyber defenses. 12. Students will analyze the mission and strategy of the Iraq government agencies who protect our portion of the Internet. 13. Students will discuss hypothetical issues of cyber security with other students in the group Discussions format.
Indicative Contents المحتويات الإرشادية	Indicative content includes the following. <u>Security Concepts Overview</u>

	Difference types of attacks; the reasons for protecting the personal information and commercially sensitive information; the types of encryptions; the advantages and limitations of encryption such as symmetric key and asymmetric key. [15 hrs] Security for Malware and Wearable Devices Definition and function of malware; types of malware; mobile malware; app security; Android/iOS security model; how anti-virus software works and its limitations. [15hrs] Network Security Difference types of network; the function and limitations of a firewall; Different types of wireless security (i.e. WEP and WPA2); access control. [15 hrs] Web Security Digital certificate; one-time password; appropriate settings of cookies; protect private data in browsers; types of content-control software. [15 hrs] Communications Encrypting and decrypting an e-mail; digital signature; unsolicited e-mail; phishing; backdoor access in instant messaging. [15 hrs] Secure Data Management Physical security; backup procedures; data destruction utilities. [14 hrs]

Learning and Teaching Strategies استراتيجيات التعلم والتعليم	
Strategies	The main strategy that will be adopted in delivering this module is to encourage students' participation in the exercises, while at the same time refining and expanding their critical thinking skills. This will be achieved through classes, interactive tutorials and by considering type of simple experiments involving some sampling activities that are interesting to the students.

Student Workload (SWL) الحمل الدراسي للطالب			
Structured SWL (h/sem) الحمل الدراسي المنتظم للطالب خلال الفصل	74	**Structured SWL (h/w)** الحمل الدراسي المنتظم للطالب أسبوعيا	5.2
Unstructured SWL (h/sem) الحمل الدراسي غير المنتظم للطالب خلال الفصل	76	**Unstructured SWL (h/w)** الحمل الدراسي غير المنتظم للطالب أسبوعيا	5.4

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	**Quizzes**	2	10% (10)	5, 10	LO #1-10
	Assignments	2	10% (10)	2, 12	LO # 1-11
	Projects / Lab.	1	10% (10)	Continuous	
	Report	1	10% (10)	13	LO # 1-11
Summative assessment	**Midterm Exam**	2 hr	10% (10)	7	LO # 1-4
	Final Exam	4hr	50% (50)	16	All
Total assessment			100% (100 Marks)		

Delivery Plan (Weekly Syllabus) المنهاج الاسبوعي النظري	
	Material Covered
Week 1	Introduction, Symmetric Ciphers model: plaintext, encryption algorithm, secret key, cipher text, decryption algorithm.
Week 2	Model of Conventional Encryption and Cryptography Classification.
Week 3	Affine Cipher and Polyalphabetic algorithm (Vigenere cipher).
Week 4	Cryptanalysis of a Symmetric key.
Week 5	Hill cipher and Playfair cipher.
Week 6	Stream Cipher
Week 7	Mid-term Exam + Unit-Step Forcing, Forced Response, the RLC Circuit
Week 8	DES—The Data Encryption Standard, hers -16 round.
Week 9	Public-Key Algorithms, - RSA.
Week 10	Diffie Hellman Algorithm.
Week 11	Elgamal Algorithm.
Week 12	Cyber Security Tools
Week 13	Web Security.
Week 14	Email Security.
Week 15	PGP—Pretty Good Privacy and S/MIME.
Week 16	**Preparatory week before the final Exam**

Delivery Plan (Weekly Lab. Syllabus) المنهاج الاسبوعي للمختبر	
	Material Covered
Week 1	Lab 1: Implement the following SUBSTITUTION & TRANSPOSITION TECHNIQUES concepts: a) Caesar Cipher b) Playfair Cipher
Week 2	Lab 2: Implement the following algorithm : a) Hill Cipher b) Vigenere Cipher
Week 3	Lab 3: Implement the RSA Algorithm.
Week 4	Lab 4: Implement the DES Algorithm.
Week 5	Lab 5: Implement the Hash function SHA-1 Algorithm.
Week 6	Lab 6: Implement the SIGNATURE SCHEME - Digital Signature Standard.
Week 7	Lab 7: Demonstrate intrusion detection system (ids) using any tool (snort or any other s/w).

Learning and Teaching Resources مصادر التعلم والتدريس		
	Text	**Available in the Library?**
Required Texts	Stallings, W. (2016). Cryptography and network security: principles and practice (Eighth edition.). Pearson	No
Recommended Texts	Speciner, M. et al. (2002). Network security: Private communication in a public world. (Second edition.).	No
Websites	https://www.youtube.com/watch?v=0UMeUB1PIRo&list=RDCMUCu1lQtQ7SJU27bRlL6hzr9A&start_radio=1&rv=0UMeUB1PIRo&t=8	

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	**FX** – Fail	راسب (قيد المعالجة)	(45-49)	More work required but credit awarded

(0 – 49)	**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.