نموذج وصف المقرر

1. اسم المقرر
Security of Computer and Networks
2. رمز المقرر
MU0244005
3. الفصل / السنة
سنوي
4. تاريخ إعداد هذا الوصف
2025/09/27
5. أشكال الحضور المتاحة
حضوري فقط
6. عدد الساعات الدراسية (الكلي)/ عدد الوحدات (الكلي)
نظري/ 2 عملي / 2 كلي / 4 الوحدات / 3
7. اسم مسؤول المقرر الدراسي (اذا اكثر من اسم يذكر)
الاسم: محمد حسن علوان الآيميل: mohammed.hassan@uomus.edu.iq
8. اهداف المقرر

اهداف المادة الدراسية	**1. إكتساب الطالب المفاهيم الأساسية عن أنظمة الزمن الحقيقي.** **2. إكتساب الطالب المعرفة والمهاره على استيعاب الانظمه واتمتتها وربطها بالحاسوب.** **3. إكتساب الطالب المهارة والقدرة اللازمتين لفهم الانظمه الرقميه ومتعلقات الحاسوب الاخرى مثل تحويل نوع الاشاره من رقمي الى دوري مستمر وبالعكس وفهم اساسيات التعامل مع ذاكرة الحاسوب ومبدئ عمل ال interrupt .** **4. البحث في المواضيع الحديثة وتعريف المشكلات التي تحتاج الى المزيد من البحث العلمي المعمق.**

9. استراتيجيات التعليم والتعلم

الاستراتيجية	○ **المحاضرات الاسبوعية للمحاضرات النظرية وتطبيق بعض التجارب المفيدة في المختبر.** ○ **التدريبات والأنشطة في قاعة الدرس.** ○ **إرشاد الطلاب إلى بعض المواقع الالكترونية للإفادة منها لتطوير القابليات.** ○ **عقد حلقات بحثية يتم من خلالها شرح وتحليل بعض المشاكل والية ايجاد الحلول لها.**

10. بنية المقرر

الأسبوع	الساعات	مخرجات التعلم المطلوبة	اسم الوحدة او الموضوع	طريقة التعلم	طريقة التقييم
1, 2, 3	**6 نظري + 6 عملي**	**1, 2**	**Introduction, Symmetric Ciphers model: plaintext, encryption algorithm, secret key, cipher text, decryption algorithm, A Model of conventional encryption. Cryptography, Cryptanalysis, block and stream cipher**	**نظري + عملي**	**Discussion in class**
4	**2 نظري + 2 عملي**	**2**	Caeser Cipher The affine Cipher	**نظري + عملي**	**Discussion in class**
5, 6	**4 نظري + 4 عملي**	**6**	**Mono alphabetic substitution ciphers Shift ciphers**	**نظري + عملي**	**Discussion in class**
7	**2 نظري + 2 عملي**	**6**	**Hill cipher**	**نظري + عملي**	**Exam#1**
8	**2 نظري + 2 عملي**	**6,7**	**Playfair cipher**	**نظري + عملي**	**quiz**
9	**2 نظري + 2 عملي**	**8**	**Polyalphabetic ciphers Vigenere cipher**	**نظري + عملي**	**Exam**
10	**2 نظري + 2 عملي**	**8,9**	**The Transposition cipher**	**نظري + عملي**	**Discussion in class**
11	**2 نظري + 2 عملي**	**10**	**Affine cipher**	**نظري + عملي**	**Discussion in class**
12	**2 نظري + 2 عملي**	**11**	**One time pad**	**نظري + عملي**	**quiz**
13 14 15	**6 نظري + 6 عملي**	**8,9,10,11**	Cryptanalysis of a Symmetric key	**نظري + عملي**	**quiz**
16	**2 نظري + 2 عملي**	**13,14,15**	Euclid's Algorithm	**نظري + عملي**	**exam**
17 18 19	**6 نظري +6 عملي**	**16**	SYMMETRIC-KEY ALGORITHMS *-DES—The Data Encryption Standard, hers*	**نظري + عملي**	**Discussion in class**

		-16 round Feistel system			
Discussion in class	**نظري + عملي**	PUBLIC-KEY - ALGORITHMS, RSA, - Other Public-Key Algorithms,	**16**	**4 نظري + 4 عملي**	20 21
quiz	**نظري + عملي**	AUTHENTICATION PROTOCOLS, -Authentication Based on a Shared Secret Key, -Establishing a Shared Key: The Diffie - Hellman Key Exchange, -Authentication Using a Key Distribution Center, -Authentication Using Kerberos, Authentication Using - Public-Key Cryptography,	**17,18**	**8 نظري + 8 عملي**	22 23 24 25
quiz	**نظري + عملي**	OSI security Architecture , a model for network security, EMAIL SECURITY PGP—Pretty Good - Privacy, S/MIME	**22**	**4 نظري + 4 عملي**	26 27
quiz	**نظري + عملي**	Protocols of computer networks PROTECTION SERVICES: • OS protection service: protected objects and methods of OS protection, security of OS, memory and addressing protection, fence protection • Database protection service: Network protection service: IP and E-Commerce protection, VPN and next generation networks protection	**26** **27**	**6 نظري + 6 عملي**	28 29 30

11. تقييم المقرر									
توزيع الدرجة من 100 على وفق المهام المكلف بها الطالب مثل التحضير اليومي والامتحانات اليومية والشفوية والشهرية والتحريرية والتقارير .... الخ									
الفصل الاول			الفصل الثاني			سعي	امتحان تهائي	درجة نهائية
عملي	نشاطات	فصلي	عملي	نشاطات	فصلي			
10	5	10	10	5	10	50	50	100

12. مصادر التعلم والتدريس	
الكتب المقررة المطلوبة (المنهجية أن وجدت)	
المراجع الرئيسة (المصادر)	William Stallings, Cryptography and Network Security; Principals and Practice, 7rd Ed. 2017. • Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill Int. Ed. 2008. -
الكتب والمراجع الساندة التي يوصى بها (المجلات العلمية، التقارير....)	1. William Stallings, Cryptography and Network Security; Principals and Practice, 7rd Ed. 2017. 2. Matt Bishop, Computer Security: Art and Science, Addison Wesley Professional Copyright: 2003, ISBN: 0-201-44099-7 3. Schneier, Bruce , Secrets and Lies : Digital Security in a Network World, John Wiley & Sons, 2000. ISBN 0-471-25311-1 4. Charlie Kaufman, Radia Perlman, Mike Speciner: Network Security - private communication in a public world, 2nd Ed., Prentice Hall, 2002. Newman, Robert C: Enterprise Security, 1st ed., Prentice Hall, 2003.
المراجع الإلكترونية ، مواقع الانترنيت	

Course Description Form

13. Course Name:
Security of Computer and Networks
14. Course Code:
CTE 414

15. Semester / Year:
Yearly
16. Description Preparation Date:
1.05.2024
17.Available Attendance Forms:
Only Attendance
18.Number of Credit Hours (Total) / Number of Units (Total)
Theoretical / 2 practical / 2 comprehensive / 4 units / 3
19. Course administrator's name (mention all, if more than one name)
Name: Asaad Nayyef **Email: Asaad.Abdulrahman.Nayyef@uomus.edu.iq**
20. Course Objectives

Course Objectives	1. Understand computer and network security principles. 2. Identify and assess security threats and vulnerabilities. 3. Implement effective security measures. 4. Apply cryptographic techniques for data protection. 5. Stay updated with emerging security trends.

21. Teaching and Learning Strategies	
Strategy	This course will give an introduction to the field of cryptography. It will cover the following topics: class cipher systems, symmetric cipher systems, block ciphers, public key systems and other related topics.

22. Course Structure

Week	Hours	Required Learning Outcomes	Unit or subject name	Learning method	Evaluation method
1 2 3	**6 theory + 6 practical**	1, 2	**Introduction, Symmetric Ciphers model: plaintext, encryption algorithm, secret key, cipher text, decryption algorithm, A Model of conventional encryption. Cryptography, Cryptanalysis, block and stream cipher**	**Theoretical + practical**	**Discussion in class**
4	**2 theory + 2 practical**	2	Caeser Cipher The affine Cipher	**Theoretical + practical**	**Discussion in class**

5 6	**4 theory + 4 practical**	6	Mono alphabetic substitution ciphers Shift ciphers	**Theoretical + practical**	**Discussion in class**
7	**2 theory + 2 practical**	6	Hill cipher	**Theoretical + practical**	**quiz**
8	**4 theory + 4 practical**	6,7	Playfair cipher	**Theoretical + practical**	**quiz**
9	**2 theory + 2 practical**	8	Polyalphabetic ciphers Vigenere cipher	**Theoretical + practical**	**Exam**
10	**4 theory + 4 practical**	8,9	The Transposition cipher	**Theoretical + practical**	**Discussion in class**
11	**2 theory + 2 practical**	10	Affine cipher	**Theoretical + practical**	**Discussion in class**
12	**2 theory + 2 practical**	11	One time pad	**Theoretical + practical**	**quiz**
13 14 15	**6 theory + 6 practical**	8,9,10,11	Cryptanalysis of a Symmetric key	**Theoretical + practical**	**quiz**
16	**2 theory + 2 practical**	13,14,15	Euclid's Algorithm	**Theoretical + practical**	**exam**
17 18 19	**6 theory +6 practical**	16	SYMMETRIC-KEY ALGORITHMS -DES—The Data Encryption Standard, hers -16 round Feistel system	**Theoretical + practical**	**Discussion in class**
20 21	**4 theory + 4 practical**	16	-RSA, PUBLIC-KEY ALGORITHMS, - Other Public-Key Algorithms,	**Theoretical + practical**	**Discussion in class**
22 23 24 25	**8 theory + 8 practical**	17,18	AUTHENTICATION PROTOCOLS, -Authentication Based on a Shared Secret Key, -Establishing a Shared Key: The Diffie - Hellman Key Exchange, -Authentication Using a Key Distribution Center, -Authentication Using Kerberos, Authentication Using Public-Key - Cryptography	**Theoretical + practical**	**exam**
26 27	**4 theory + 4 practical**	22	OSI security Architecture , a model for network security, EMAIL SECURITY PGP—Pretty Good Privacy, S/MIME-	**Theoretical + practical**	**quiz**
28 29 30	**6 theory + 6 practical**	26	Protocols of computer networks PROTECTION SERVICES: • OS protection service: protected objects and methods of OS protection, security of OS, memory and addressing protection, fence protection • Database protection service:	**Theoretical + practical**	**exam**

			Network protection service: IP and E-Commerce protection, VPN and next generation networks protection		

23. Course Evaluation

Distributing the score out of 100 according to the tasks assigned to the student such as daily preparation, daily oral, monthly, or written exams, reports .... etc

24. Learning and Teaching Resources

quired textbooks (curricular books, if any)	
Main references (sources)	• William Stallings, Cryptography and Network Security; Principals and Practice, 7rd Ed. 2017. • Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill Int. Ed. 2008.
Recommended books and references (scientific journals, reports…)	1. William Stallings, Cryptography and Network Security; Principals and Practice, 7rd Ed. 2017. 2. Matt Bishop, Computer Security: Art and Science, Addison Wesley Professional Copyright: 2003, ISBN: 0-201-44099-7 3. Schneier, Bruce , Secrets and Lies : Digital Security in a Network World, John Wiley & Sons, 2000. ISBN 0-471-25311-1 4. Charlie Kaufman, Radia Perlman, Mike Speciner: Network Security - private communication in a public world, 2nd Ed., Prentice Hall, 2002. Newman, Robert C: Enterprise Security, 1st ed., Prentice Hall, 2003.
Electronic References, Websites	http://williamstallings.com/Crypto/Crypto4e.html