جامعة الكفيل
University of Alkafeel

الخطة الدراسية

قسم هندسة تقنيات الحاسوب / كلية الهندسة التقنية / جامعة الكفيل / العام الدراسي 2020 – 2021

المرحلة الدراسية:	الرابعة
التخصص:	شبكات إتصالات الحاسوب
اسم المادة الدراسية باللغة العربية:	امنية الحاسوب وشبكاتها
اسم المادة الدراسية باللغة الإنجليزية:	Security of computer & Networks
اهداف المادة:	تهدف المادة الى بيان الوسائل والطرق التي يجب اتباعها لحماية الحاسوب من الدخول اليها من غير المخولين والعبث فيها كذلك حماية البيانات وقواعد البيانات من المتطفلين كذلك حماية شبكة الحاسوب وخصوصا الشبكات الخاصة من هجمات المتطفلين من خلال تفعيل واستثمار بروتوكولات حماية الشبكات.
وصف المادة:	دراسة المفاهيم والمبادئ الأساسية للحوسبة وأمن الشبكات .يغطي المنهج موضوعات الأمان الأساسية ، بما في ذلك التشفير المتماثل والمفتاح العام والتوقيعات الرقمية ووظائف تجزئة التشفير ومخاطر المصادقة وبروتوكولات أمان الشبكة
عدد الساعات النظرية:	2
عدد الساعات العملية:	2
عدد الوحدات:	6
اسم التدريسي باللغة العربية:	د. فاتنه طالب محمد
اسم التدريسي باللغة الإنجليزية:	Fatina Talib Mohammed
اللقب العلمي:	مدرس
عنوان البريد الالكتروني الجامعي:	fatinat.shukur@uokufa.edu.iq
رقم الهاتف الجوال (WhatsApp):	07805781440

المنهج المقرر / الجزء النظري:

Week	Syllabus
1st, 2nd, 3rd	Introduction, Symmetric Ciphers model: plaintext, encryption algorithm, secret key, cipher text, decryption algorithm, A Model of conventional encryption. Cryptography, Cryptanalysis, block and stream cipher
4th	Caesar Cipher The affine Cipher
5th, 6th	Mono alphabetic substitution ciphers Shift ciphers
7th	Hill cipher
8th	Playfair cipher
9th	Polyalphabetic ciphers Vigenere cipher
10th	The Transposition cipher
11th	Affine cipher
12th	One-time pad
13th, 14th, 15th	Cryptanalysis of a Symmetric key
16th	Euclid's Algorithm
17th, 18th, 19th	SYMMETRIC-KEY ALGORITHMS -DES—The Data Encryption Standard, hers -16 round Feistel system
20th, 21st	PUBLIC-KEY ALGORITHMS, -RSA, - Other Public-Key Algorithms,
22nd ,23rd, 24th ,25th	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,
26th, 27th	OSI security Architecture, a model for network security, EMAIL SECURITY -PGP—Pretty Good Privacy, S/MIME
28th, 29th, 30th	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

المنهج المقرر / الجزء العملي:

Week	Syllabus
1	**Introduction to MATLAB Instruction**
2	**Implement Encryption by Caesar Cipher**
3	**Implement Decryption by Caesar Cipher**
4	**Compute the greatest common divisor (GCD)**
5	**Multiplicative Inverses Modulo n**
6	**First Exam**
7	**Hill cipher / Encryption**
8	**Hill cipher / Decryption**
9	**Encrypt by using Vigenère cipher**
10	**Second Exam**
11	**Decrypt by using Vigenère cipher**
12	**Encrypt by using Affine cipher**
13	**Decrypt by using Affine cipher**

المصادر:

المراجع الرئيسية:

[1] Cryptography and Network Security, 7th Edition

[2] Handbook of Applied Cryptography

المراجع المساعدة:

[1] Defensive Security Handbook: Best Practices for Securing Infrastructure

[2] Network Monitoring and Analysis: A Protocol Approach to Troubleshooting

[3] Network Security Essentials :Application And Standards, 6Th Edition