توصيف المقرر

وصف المقرر: يوفر وصف المقرر هذا إيجازاً مقتضيا لأهم خصائص المقرر ومخرجات التعلم المتوقعة من الطالب تحقيقها مبرهناً عما إذا كان قد حقق الاستفادة القصوى من فرص التعلم المتاحة. ولابد من الربط بينها وبين وصف البرنامج.؛

١. المؤسسة التعليمية:	كلية المصطفى الجامعة
٢. القسم العلمي / المركز	هندسة تقنيات الحاسوب
٣. اسم المقرر	امنية الحاسوب وشبكاتها
٤. اشكال الحضور المتاحة	اسبوعي / نظري و عملي
٥. الفصل / السنة	٢٠١٧ / ٢٠١٨
٦. عدد الساعات الدراسية الكلي	١٢٠ ساعة بواقع ٤ ساعات اسبوعيا
٧. تاريخ اعداد هذا المقرر	ايلول ٢٠١٧
٨. اهداف المقرر:	
أ- **تهدف المادة الى بيان الوسائل والطرق التي يجب اتباعها لحماية الحاسوب من الدخول اليها من غير المخولين والعبث بها.** ب- **حماية البيانات وقواعد البيانات من المتطفلين.** ت- **حماية شبكة الحاسوب وخصوصا الشبكات الخاصة من هجمات المتطفلين من خلال تفعيل واستثمار بروتوكلات حماية الشبكات.** ث- معرفة اساسيات امنية المعلومات في الاتصالات ج- دراسة وتحليل خوارزمات التشفير المتناظر,Caser, substitution, vigener affine,OTP,Hill cipher, playfair,transposition ح- دراسة مفهوم تحليل الشفرة واعطاء مثال عن الشفرة substitution خ- دراسة وتحليل خوارزميات التشفير الغير متناظرRSA	

٩. مخرجات المقرر وطرائق التعليم والتعلم والتقييم:

أ- الأهداف المعرفية.

أ- القدرة على تطبيق المعرفة في مجال امنية الحاسبات.

ب- القدرة على فهم التشفير وتفاصيل خوازميات التشفير.

ت- القدرة على استخدام وتطبيق خوازميات التشفير.

توصيف المقرر

ث- معرفة اساسيات امنية المعلومات في الات ا صلات.

ج- دراسة وتحليل خوارزمات التشفير المتناظر والغير متناظرة.

ح- دراسة مفهوم تحليل الشفرة واعطاء مثال عن الشفرة.

ب-الأهداف المهاراتية الخاصة بالمقرر.

- ✓ تنفيذ الايعازات والدوال لخوارزميات التشفير.
- ✓ كتابة وتنفيذ خوارزميات التشفير لتنفيذها بلغة البرمجة MATLAB
- ✓ تصميم برامج التشفير وفك التشفير.

- **طرائق التعليم والتعلم:**

المحاضرات الاكاديمية : حيث توفر الاساس المتين الذي يعتمد عليه بتطوير الرصيد المعرفي للطلبة

المختبرات العملية والورش : التي توفر كل ما يحتاج اليه الطالب من خبرات تساعد على تطوير الجانب المهاري العملي وترسيخ المبادئ الضرورية للقيام بتنفيذ المشاريع العملية بصورة صحيحة واتباع خطوات السلامة المهنية للحد من الاضرار الناتجة على الاشخاص والممتلكات.

- **طرائق التقييم:**

التقيم التفاعلي : حيث تتم عملية التقييم هذه بصورة مباشرة بين الطالب والتدريسي وتكون واحدة من اساسيات التغذية الراجعة التي يعنمد عليها اعضاء الهيئة التدرى ى سة بتقييم عملية التعليم والتعلم.

الاختبارات التحريرية الدورية : وتوفر هذه الاختبارات لعضو الهيئة التدريسية عن مدى متابعة الطلبة للمحتوى الاكاديمي وكيفية التفاعل مع المعلومات والملاحظات المعطاة من قبل التدريسي للطلبة.

الاختبارات الفصلية : وتكون الحلقة الوسطية لتقييم مدى اهتمام الطالب وتفاعله مع المادة العلمية التي تلقاها خلال الفصل الدراسي بجانبيها الاكاديمي والمهاري.

الاختبارات النهائية : وتكون الحلقة النهائية لتقييم مدى اهتمام الطالب وتفاعله مع المادة العلمية التي تلقاها خلال السنة الدراسية بجانبيها الاكاديمي والمهاري.

ت-الأهداف الوجدانية والقيمية.

- ✓ زرع روح الابداع والابتكار لدى الطلبة.
- ✓ -تنمية الشعور بالمسؤولية للطلبة.
- ✓ -تنمية قيم الحرص والمثابرة على انجاز العمل للوصول الى النتائج المرضية.
- ✓ تنمية قابلية الطلبة على العمل الجماعي.

توصيف المقرر

- **طرائق التعليم والتعلم:**
طرح مشكلات علمية والطلب من الطلبة ايجاد اكثر من حل لها بطرق علمية مختلفة لتحفيز الجانب الابداعي لدى الطلبة
تشكيل فرق عمل يتم تقييم نتائج عملها وتغير بنيتها بصورة دورية لتنمية روح التعاون وتحفيز الطلبة على بذل جميع الجهود اللازمة للعمل تحت ظروف مختلفة ومع اشخاص عدة.
- **طرائق التقييم:**
التقييم المباشر : حيث يتم هذا التقييم من قبل التدريسي بصورة مباشرة ومن خلال ملاحضة تفاعل الطلبة وتطبيقهم الاهداف الوجدانية القيمية وتثبيت الملاحظات بخصوص ذلك
المشاريع العملية : يتم تقييم مدى قدرة الطالب على الانجاز والابداع وعلى العمل ضمن فرق والحصول على النتائج والحلول لمختلف المشكلات العلمية التي تواجه الطلبة

ث- المهارات العامية و التأهيل المنقولة (المهارات الاخرى المتعلقة بقابلة التوضيف و التطوير الشخصي)

- ✓ تصميم برامج التشفير وفك التشفى
- ✓ تصميم برامج مختلفة لتح ى لل الشفرة
- ✓ استخدام لغة البرمجة الماتلاب لزيادة مهارة الطالب في البرمجة في مجال امنية شبكات الحاسبات

١٠. بنية المقرر

الاسبوع	الساعات	مخرجات التعلم المطلوبة	اسم الوحدة او الموضوع	طريقة التعليم	طريقة التقييم
1,2,3		على التعرف مفهوم التشفير المتناظر وخوارزميات التشفير والمفتاح التشفير ومفهوم تحليل الشفرة	**Symmetric Ciphers model: plaintext, encryption algorithm, secret key, cihpertext, decryption algorithm, A Model of conventional encryption. Cryptography, Cryptanalysis, block and stream cipher**	محاضرة مختبرات و عملية	تقييم التفاعلي من خلال اختبرات تحريرية وتقيم مباشر

توصيف المقرر

4			**Caeser Cipher The affine Cipher**	محاضرة مختبرات و عملية	تقييم التفاعلي من خلال اختبرات تحريرية وتقيم مباشر
5,6			**Mono alphabetic substitution ciphers Shift ciphers**	محاضرة مختبرات و عملية	تقييم التفاعلي من خلال اختبرات تحريرية وتقيم مباشر
7			**Hill cipher**	محاضرة مختبرات و عملية	تقييم التفاعلي من خلال اختبرات تحريرية وتقيم مباشر
8			**Playfair cipher**	محاضرة مختبرات و عملية	تقييم التفاعلي من خلال اختبرات تحريرية وتقيم مباشر
9			**Polyalphabetic ciphers Vigenere cipher**	محاضرة مختبرات و عملية	تقييم التفاعلي من خلال اختبرات تحريرية وتقيم مباشر

توصيف المقرر

تقييم التفاعلي من خلال اختبارات تحريرية وتقيم مباشر	محاضرة مختبرات و عملية	**The Transposition cipher** **Affine cipher** otp			10,11, 12,13
تقييم التفاعلي من خلال اختبارات تحريرية وتقيم مباشر	محاضرة مختبرات و عملية	**Cryptanalysis of a Symmetric key**			14,15,16
تقييم التفاعلي من خلال اختبارات تحريرية وتقيم مباشر	محاضرة مختبرات و عملية	**Euclid's Algorithm**			17
تقييم التفاعلي من خلال اختبارات تحريرية وتقيم مباشر	محاضرة مختبرات و عملية	**SYMMETRIC-KEY ALGORITHMS** **-DES—The Data Encryption Standard, hers** **-16 round Feistel system**			18,19
تقييم التفاعلي من خلال اختبارات تحريرية وتقيم مباشر	محاضرة مختبرات و عملية	**PUBLIC-KEY ALGORITHMS,** **-RSA,** **- Other Public-Key Algorithms**			20,21,22

توصيف المقرر

تقييم التفاعلي من خلال اختبارات تحريرية وتقيم مباشر	محاضرة مختبرات و عملية	**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 Cryptograph**			23,24, 25,26,27
تقييم التفاعلي من خلال اختبارات تحريرية وتقيم مباشر	محاضرة مختبرات و عملية	**OSI security Architecture , a model for network security EMAIL SECURITY**			28
تقييم التفاعلي من خلال اختبارات تحريرية وتقيم مباشر	محاضرة مختبرات و عملية	**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**			29,30

١١. البنية التحتية :

توصيف المقرر

الكتب المقررة	Cryptography and network security: principles and practice(3rd edition), Author: Stallings, William. Year: 2003
المراجع الرئيسية	1- Computer security: Art and science . Author: Matthew Bishop, year: 2003 2- Handbook of cryptography
الكتب والمراجع التي يوصى بها المجلات العلمية ، التقارير ،	1- Computer security: Art and science . Author: Matthew Bishop, year: 2003 2- Handbook of cryptography
المراجع الالكترونية	

١٢. خطة تطوير المقرر اللدراسي

الجانب العملي : تصميم وتنفيذ البرامج بلغة C++بالاضافة الى لغة ال MATLAB

توفير لاب توب لكل طالب بدلا من حاسبات الدسك توب ومشاكل الكهرباء

الجانب النظري : استخدام مراجع علمية حديثة