نموذج وصف المقرر

وصف المقرر

يوفر وصف المقرر هذا إيجازاً مقتضياً 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	جامعة البصرة
٢. القسم العلمي / المركز	كلية علوم الحاسوب وتكنولوجيا المعلومات/قسم علوم الحاسوب
٣. اسم / رمز المقرر	الامنية (CS405)
٤. أشكال الحضور المتاحة	حضور رسمي اسبوعي
٥. الفصل / السنة	نظام المقررات (المستوى الرابع)
٦. عدد الساعات الدراسية (الكلي)	٤٥ ساعة
٧. تاريخ إعداد هذا الوصف	٢٠١٨/١٠/٢٢
٨. أهداف المقرر	
• دراسة مقدمة عن امنية البيانات.	
• دراسة تقنيات التشفير الكلاسيكية.	
• دراسة نموذج التشفير المتناظر (الطرق التعويضية والطرق الابدالية).	
• دراسة انظمة التشفير الكتلية ومعيار تشفير البيانات.	
▪ مبادئ التشفير الكتلي.	
▪ تحليل الشفرة الخطي والتفاضلي.	
▪ اطوار عملية التشفير الكتلي.	
• دراسة معيار التشفير المتقدم.	
• دراسة التشفير الانسيابي.	
• دراسة مقدمة الى نظرية الاعداد.	

١٠.مخرجات المقرر وطرائق التعليم والتعلم والتقييم
أ- الأهداف المعرفية أ١- فهم لمبادئ الخدمات الامنية وميكانيكياتها. أ٢- فهم لنموذج أمنية الشبكات. أ٣- فهم لخوارزميات أنظمة التشفير الكلاسيكية والحديثة ومبادئها الرياضية طرق تصميمها وبنائها. أ٤- فهم اساليب وطرق كسر الشفرات . أ٥- فهم اساليب وطرق تنفيذ الهجمات وكيفيه استغلال الثغرات الامنية في الانظمة الحاسوبية والشبكات وطرق الحماية منها (اكتشاف – صد – تخفيف – منع). أ٦- معرفة برمجة وتنفيذ بعض خوارزميات التشفير.
ب - الأهداف المهاراتية الخاصة بالمقرر. ب ١ – الفهم الرياضي لمبادئ نظرية الارقام المستخدمة في بناء خوارزميات التشفير. ب ٢ – الفهم الرياضي لمبادئ طرق كسر الشفرة. ب ٣ – فهم طرق تنفيذ الهجمات على انظمة الحواسيب والشبكات واستغلال الثغرات الامنية وكيفية الحماية منها. ب ٤ - برمجة وتنفيذ بعض خوارزميات التشفير.
طرائق التعليم والتعلم
١- المحاضرات. ٢- طريقة التعلم الذاتي (تكليف الطلبة بإكمال تعلم بعض المهارات بعد إعطائهم أساسياتها).
طرائق التقييم
١- Quiz. ٢- الامتحانات الشهرية والنهائية. ٣- التقارير والواجبات (غير الإلزامية) .
ج- الأهداف الوجدانية والقيمية ج١-الملاحظة والإدراك . ج٢- التحليل والتفسير . ج٣- الاستنتاج والتقييم . ج٤- الأعداد والتقويم .
طرائق التعليم والتعلم
١- المحاضرات النظريه والعلمية. ٢- تدريب الطلبه في الورش والمختبرات التعليمية.
طرائق التقييم
١- الامتحانات الشهرية والنهائية. ٢- الامتحانات اليومية (quiz).

د - المهارات العامة والتأهيلية المنقولة (المهارات الأخرى المتعلقة بقابلية التوظيف والتطور الشخصي). د١- تطوير المهارة القيادية لدى الطالب . د٢- تطوير اللياقة الذهنية للطالب خلال المحاضرة عن طريق التوجيه المستمر للأسئلة . د٣- تطوير المهارات الرياضية والتحليل المنطقي . د٤- تطوير المهارات اللغوية للطالب لزيادة قدرة التعبير عن أفكاره .

١١.بنية المقرر					
الأسبوع	الساعات	مخرجات التعلم المطلوبة	اسم الوحدة / أو الموضوع	طريقة التعليم	طريقة التقييم
الاول	٣	الطالب يفهم الموضوع	Introduction	نظري	quiz
الثاني	٣	الطالب يفهم الموضوع	Substitution Cipher Techniques	نظري	quiz
الثالث	٣	الطالب يفهم الموضوع	Vigener Cipher	نظري	quiz
الرابع	٣	الطالب يفهم الموضوع	Transposition Techniques	نظري	quiz
الخامس	٣	الطالب يفهم الموضوع	Block Ciphers and the Data Encryption Standard	نظري	quiz
السادس	٣	الطالب يفهم الموضوع	DES Encryption	نظري	quiz
السابع	٣	الطالب يفهم الموضوع	Feistel Structure	نظري	quiz
الثامن	٣	الطالب يفهم الموضوع	Key Generation of DES	نظري	quiz
التاسع	٣	الطالب يفهم الموضوع	Block Cipher Modes of Operation	نظري	quiz
العاشر	٣	الطالب يفهم الموضوع	Differential and Linear Cryptanalysis	نظري	quiz
الحادي عشر	٣	الطالب يفهم الموضوع	Advanced Encryption Standard	نظري	quiz
الثاني عشر	٣	الطالب يفهم الموضوع	Stream Cipher	نظري	quiz
الثالث عشر	٣	الطالب يفهم الموضوع	RC4	نظري	quiz
الرابع العشر	٣	الطالب يفهم الموضوع	Introduction to Number Theory	نظري	quiz
الخامس عشر	٣	الطالب يفهم الموضوع	Extended Euclid	نظري	quiz

١٢.البنية التحتية	
١ـ الكتب المقررة المطلوبة	William Stallings, "Cryptography and

Network Security. Principle and Practice", Third Edition, Principle Hall, USA, 2003.	
	٢ـ المراجع الرئيسية (المصادر)
	ا ـ الكتب والمراجع التي يوصى بها (المجلات العلمية ، التقارير ،....)
	ب ـ المراجع الالكترونية، مواقع الانترنيت ....

١٣.خطة تطوير المقرر الدراسي