



نموذج وصف المادة الدراسية

معلومات المقرر الدراسية

اسم المقرر	مبدئ امن البيانات	أسلوب التدريس
نوع المقرر	اساسي	النظري
رمز المقرر	Cys1101	•
عدد الوحدات	5	العملي
عدد ساعات المقرر	125	
مستوى المقرر الدراسي	الفصل الدراسي	1
القسم الأكاديمي	قسم الامن السيبراني	كلية علوم الحاسوب وتكنولوجيا المعلومات
مسؤول المادة	ا.م.د احسان احمد محمد	ahssan.ahsan@gmail.com
اللقب العلمي	مدرس	الشهادة الأكademie
مدرس المادة	ا.م.د احسان احمد محمد	ahssan.ahsan@gmail.com
اسم مراجع النظير	د. علي كريم عبدالرحيم	alialmujab@uowa.edu.iq
تاريخ موافقة اللجنة العلمية	2025-12-24	اصدار
...		1.0

العلاقة مع المواد الدراسية الأخرى

وحدة المتطلبات الأساسية	لا شيء	الفصل الدراسي	...
وحدة المتطلبات المشتركة	لا شيء	الفصل الدراسي	...

ام.د. حسنه على لفافته
العميد
٢٠٢٦ - ٢٠٢٥
عميد الكلية



م.د. علي كريم عبد الرحيم
ر.ق. (امن السيبرانية)
٢٠٢٦ - ٢٠٢٥
رئيس القسم

أهداف المادة الدراسية ونتائج التعلم والمحتويات الإرشادية

<p>هدف هذه الوحدة هو تزويد الطلاب بفهم قوي للمفاهيم والممارسات الأساسية في أمن البيانات. سيتعلم الطلاب كيفية تحديد التهديدات والثغرات الأمنية، وتطبيق تقنيات التشفير والمصادقة، وتنفيذ ضوابط الوصول، وضمان سلامة البيانات وخصوصيتها. تقدم الوحدة أيضاً الأدلة الجنائية الرقمية، وأمن قواعد البيانات، والأطر القانونية ذات الصلة، مما يمكن الطلاب من تطوير رؤية شاملة لحماية المعلومات في بيئات الحوسبة الحديثة.</p>	<p>أهداف المادة الدراسية</p>
<p>١. سيتعلم الطالب مفاهيم التشفير الأساسية. ٢. سيتعرف على ماهية التحقيق الرقمي، ومصادر الأدلة الرقمية، وحدود علم الأدلة الجنائية الرقمية. ٣. نظرة عامة على مفاهيم المصادقة، والتقويض، والتحكم في الوصول، وسلامة البيانات. ٤. وأخيراً، سيتعرض بعضاً من تقنيات حماية البيانات المختلفة.</p>	<p>مخرجات التعلم للمادة الدراسية</p>
<p>١. مقدمة في مبادئ أمن البيانات • الأهداف الأمنية الأساسية: السرية، النزاهة، التوفير (CIA) • التهديدات، الثغرات، ومفاهيم المخاطر • الضوابط الأمنية والدافع العميق • المنظورات التنظيمية والتقنية لحماية البيانات</p> <p>٢. مفاهيم التشفير الأساسية • البدائل التشفيرية: التشفير، التجزئة، التواقيع الرقمية • التشفير المتماثل مقابل غير المتماثل • أساسيات توليد وتوزيع وإدارة المفاتيح • حالات الاستخدام: حماية البيانات، فحوصات السلامة</p> <p>٣. الرموز التاريخية • شفرات الاستبدال والتبدل الكلاسيكية • فيصر، فيجينير، ووحدة الوسام ذات المرة الواحدة (مفهوم) • أساسيات تحليل الشفرات والتطور نحو علم التشفير الحديث • دروس مستفادة من نقاطضعف التاريـخـية</p> <p>٤. الطب الشرعي الرقمي • الغرض ونطاق الأدلة الجنائية الرقمية • جمع الأدلة وسلسلة الحجز • تحليل السجلات وأساسيات التحقيق في الحوادث</p> <p>٥. سلامة البيانات والمصادقة • ضمان دقة البيانات واتساقها وموثوقيتها • رموز التحقق من صحة الرسائل (MAC)، التجزئة، المجاميع • الشهادات الرقمية وبروتوكولات المصادقة</p> <p>٦. تقنيات تخزين كلمات المرور ونزاهة البيانات • تجزئة كلمات المرور الآمنة: salts، تمديد المفاتيح (PBKDF2، bcrypt، scrypt) • سياسات كلمات المرور ومخاطر المصادقة • الهجمات الشائعة: القوة الغاشمة، القاموس، جداول قوس قزح • الحفاظ على السلامة في أنظمة المصادقة</p>	<p>المحتويات الإرشادية</p>

<p>7. التحكم في الوصول</p> <p>نماذج التحكم في الدخول: DAC، MAC، RBAC، ABAC</p> <ul style="list-style-type: none"> • مخاطر تصعيد الامتياز والخفيف منها • إدارة الجلسات وعمليات التفريض • أساسيات إدارة الهوية والوصول (IAM) <p>8. خصوصية البيانات</p> <p>مبادئ تقليل البيانات، تحديد الغرض، موافقة المستخدم</p> <p>المعلومات الشخصية القابلة للتعرف (PII) وتصنيف البيانات الحساسة</p> <p>تقنيات تعزيز الخصوصية (التعرف على الأسماء المستعارة، إخفاء الهوية)</p> <p>مخاطر خصوصية البيانات وأساليب الشائعة للخفيف</p> <p>9. أمن تخزين المعلومات</p> <p>طرق التخزين الآمنة: التشفير في حالة السكون، تشفير القرص/الحجم</p> <ul style="list-style-type: none"> • استراتي�يات النسخ الاحتياطي، التكرار، والاسترداد • الحفظ الآمن، والاحتفاظ بالأمر، وإدارة دورة الحياة • اعتبارات أمان التخزين الفيزيائي <p>10. أمان قاعدة البيانات</p> <p>التهديدات لقواعد البيانات: حقن SQL، إساءة استخدام الامتيازات، هجمات من الداخل</p> <ul style="list-style-type: none"> • التحكم في الوصول والأذونات القائمة على الأدوار في أنظمة قواعد البيانات • تشفير البيانات أثناء الراحة والنقل • تسجيل ومراجعة ومراقبة نشاط قواعد البيانات <p>11. ندوة التقرير</p> <p>عرض بحثية يقودها الطالب حول مواضيع أمنية مختارة</p> <ul style="list-style-type: none"> • تطوير مهارات كتابة التقارير (التنسيق، المرجع) • التقييم النقدي للمصادر ودراسات الحالة • مراجعة الأقران والنقاش داخل الصف <p>12. قانون أمن البيانات</p> <p>نظرة عامة على الوائح الوطنية والدولية لحماية البيانات</p> <p>مبادئ والتزامات الامتثال ISO27001 ISO27001 اللائحة العامة لحماية البيانات (GDPR) (/)</p> <ul style="list-style-type: none"> • الجوانب القانونية لاختراقات البيانات والإبلاغ عن الحوادث • الاعتبارات الأخلاقية عند التعامل مع البيانات الشخصية والحساسة 	<ul style="list-style-type: none"> • • • •
--	--

استراتيجيات التعليم والتعلم	الاستراتيجيات
<ul style="list-style-type: none"> - المحاضرات -2- التعلم القائم على حل المشكلات -3- دراسات حالة -4- التغذية الراجعة والتقييم التكويني 	

الحمل الدراسي للطالب محسوب لـ ١٥ أسبوعاً

3	Structured SWL (h/w) الحمل الدراسي المنظم للطالب أسبوعياً	48	Structured SWL (h/sem) الحمل الدراسي المنظم للطالب خلال الفصل
2	Unstructured SWL (h/w) الحمل الدراسي غير المنظم للطالب أسبوعياً	77	Unstructured SWL (h/sem) الحمل الدراسي غير المنظم للطالب خلال الفصل
125		Total SWL (h/sem) الحمل الدراسي الكلي للطالب خلال الفصل	

تقييم المادة الدراسية

نتائج التعلم ذات الصلة	الأسبوع المستحق	الوزن (الدرجات)	الوقت/العدد		
1,3	الكل	10% (10)	5	الاختبارات	التقييم التكويني
3,4	4,8,12	10% (10)	5	الواجبات	
3	3,5,7,9,14	10% (10)	2	المشاريع	
الكل	6,13	10% (10)	2	التقارير	
		(10) %10	2	امتحان منتصف الفصل	التقييم التخلصي
		(50) %50	3	امتحان النهائي	
		التقييم الكلي			

المنهج الأسبوعي النظري

المواد المغطاة	
نظرة عامة حول مبادئ أمن البيانات	الأسبوع 1
مقدمة في مبادئ أمن البيانات	الأسبوع 2
مفاهيم أساسية في علم التشفر	الأسبوع 3
الشفرات التاريخية	الأسبوع 4
الطب الشرعي الرقمي	الأسبوع 5
سلامة البيانات والمصادقة	الأسبوع 6
امتحان منتصف الفصل	الأسبوع 7
تقنيات تخزين كلمات المرور وسلامة البيانات	الأسبوع 8
التحكم في الوصول	الأسبوع 9
خصوصية البيانات	الأسبوع 10
أمن تخزين المعلومات	الأسبوع 11

الأسبوع 12	أمان قاعدة البيانات
الأسبوع 13	ندوة التقرير
الأسبوع 14	قانون أمن البيانات
الأسبوع 15	التحضير لامتحان النهائي

مصادر التعلم والتدريس		
هل هو متوفّر في المكتبة؟	نص	
كلا	Cryptography and Network Security, principles and practice, Global Edition – Eighth Edition, William Stallings, 2023	النصوص المطلوبة
كلا	https://cybersecurityguide.org/resources/reading-list/#book	النصوص الموصى بها
	https://www.coursera.org/professional-certificates/google-cybersecurity	الموقع الإلكترونية

مخطط الدرجات				
التعريف	الدرجات (%)	التقدير	الدرجة	المجموعة
أداء متميز	100 - 90	امتياز	أ - ممتاز	مجموعة النجاح (100 - 50)
فوق متميز مع بعض الأخطاء	89 - 80	جيد جدا	ب - جيد جدا	
أداء جيد مع أخطاء ملحوظة	79 - 70	جيد	ج - جيد	
عادل لكنه مع عيوب كبيرة	69 - 60	متوسط	د - متوسط	
الجهد يفي بالحد الأدنى من المعايير	59 - 50	مقبول	ه - مقبول	
يتطلب الأمر المزيد من الجهد لكن تم منح الساعات المعتمدة	(49-45)	رابس (قيد المعالجة)	و - راسب	
يتطلب النجاح جهداً كبيراً	(44-0)	رابس	ف - راسب	مجموعة الرسوب (49 - 0)

ملاحظة: النقاط العشرية فوق أو تحت 0.5 ستقتربها إلى العلامة الكاملة الأعلى أو الأدنى (على سبيل المثال، علامة 54.5 ستقتربها إلى 55، بينما العلامة 54.4 ستقتربها إلى 54). لدى الجامعة سياسة لا تبرر "الرسوب القريب من النجاح"، لذا فإن التعديل الوحيد على الدرجات الممنوحة من قبل العلامة الأصلية سيكون التقارب التلقائي المذكور أعلاه.