



نموذج وصف المقرر الدراسي



معلومات المقرر الدراسية					
اسم المقرر		تقنيات أمن المعلومات		أسلوب التدريس	
نوع المقرر		رئيسية		☒ محاضرة	
رمز المقرر		IT4101		☒ عملي	
عدد الوحدات		6		☒ نظري	
عدد ساعات المقرر		150			
مستوى المقرر الدراسي		4		الفصل الدراسي	
القسم الأكاديمي		تكنولوجيا المعلومات		علوم الحاسوب وتكنولوجيا المعلومات	
مسؤول المادة		ا.م.د احسان احمد محمد لهمود		ahssan.ahsan@gmail.com	
اللقب العلمي		أستاذ مساعد		الشهادة الأكاديمية	
مدرس المادة		ا.م.د احسان احمد محمد لهمود		دكتوراه	
اسم مراجع المقرر الدراسي		م.م نبيل صادق عبد العباس عطية		الايمل	
تاريخ موافقة اللجنة العلمية		01/09/2026		الايمل	
				V1	
				اصدار	

العلاقة مع المقررات الدراسية الاخرى			
المتطلب السابق للمادة	IT3202	الفصل الدراسي	لا يوجد
المتطلبات المصاحبة للمادة	لا يوجد	الفصل الدراسي	لا يوجد

مصادقة السيد العميد



مصادقة السيد رئيس القسم

أهداف المادة، ومخرجات التعلم، والمحتوى الإرشادي

1. التعريف بمفهوم أمن المعلومات: تهدف المادة إلى تزويد الطلاب بفهم أساسي لمفهوم أمن المعلومات وأهميته في عصرنا الرقمي الحالي. 2. تحديد المخاطر الأمنية المحتملة: يتعلم الطلاب التعرف على المخاطر الأمنية الشائعة مثل البرمجيات الخبيثة، وهجمات التصيد الاحتيالي، وانتهاكات البيانات، وفهم تبعات هذه المخاطر وأهمية حماية البيانات الحساسة. 3. استكشاف أمان كلمات المرور: تهدف المادة إلى تعليم الطلاب أهمية كلمات المرور القوية والمميزة، وكيفية إنشائها وحفظها بأمان، وأسباب منع مشاركتها مع الآخرين. 4. التعريف بالخصوصية عبر الإنترنت: يكتسب الطلاب فهماً لأهمية الخصوصية عند استخدام المنصات الرقمية والإنترنت، والمخاطر المحتملة لمشاركة المعلومات الشخصية، وكيفية حمايتها. 5. التثقيف حول عادات التصفح الآمن: تهدف المادة إلى تعليم الطلاب ممارسات التصفح الآمن، بما في ذلك تجنب المواقع المشبوهة، وفهم مؤشرات أمان المواقع (مثل شهادات SSL/TLS)، والتعرف على الاحتيال الإلكتروني وتجنبه. 6. التعريف ببرامج مضادات الفيروسات وجدران الحماية: يتعرف الطلاب على دور برامج مضادات الفيروسات وجدران الحماية في حماية أنظمة الحاسوب من البرمجيات الخبيثة والوصول غير المصرح به، وكيفية اختيار هذه الأدوات واستخدامها بفعالية. 7. تعليم الاستخدام المسؤول لمواقع التواصل الاجتماعي: تهدف المادة إلى تثقيف الطلاب حول السلوك المسؤول على منصات التواصل الاجتماعي، ومخاطر مشاركة المحتوى غير اللائق، وأهمية احترام خصوصية الآخرين عبر الإنترنت. 8. معالجة التنمر الإلكتروني والمضايقات عبر الإنترنت: توعية الطلاب بالآثار الضارة للتنمر والمضايقات الإلكترونية، وتعليمهم استراتيجيات الاستجابة لها والإبلاغ عنها، ونشر قيمة اللطف والاحترام المتبادل عبر الإنترنت. 9. التعريف بالنسخ الاحتياطي للبيانات واستعادتها: تهدف المادة إلى تعليم الطلاب أهمية إنشاء نسخ احتياطية للبيانات بانتظام، والأساليب المختلفة المتاحة للنسخ الاحتياطي، بالإضافة إلى خيارات استعادة البيانات عند فقدانها. 10. تعزيز الاستخدام الأخلاقي والمسؤول للتكنولوجيا: تهدف المادة إلى ترسيخ مفهوم المواطنة الرقمية والمسؤولية، من خلال تعليم الطلاب كيفية الاستخدام الأخلاقي للتكنولوجيا، بما في ذلك احترام قوانين حقوق النشر، وتجنب الانتحال العلمي (السرقة الأدبية)، وفهم تأثير أفعالهم عبر الإنترنت.	هدف المادة الدراسية
1. تحديد المخاطر الأمنية الشائعة وشرحها: يجب أن يكون الطلاب قادرين على التعرف على المخاطر	مخرجات تعلم المادة الدراسية

الأمنية الشائعة ووصفها مثل الفيروسات، والبرمجيات الخبيثة، والتصيد الاحتيالي، وسرقة الهوية. 2. إظهار المعرفة بأمان كلمات المرور: يجب أن يفهم الطلاب أهمية استخدام كلمات مرور قوية ومميزة، وأن يكونوا قادرين على إنشاء كلمات مرور آمنة لحساباتهم الرقمية وتذكرها. 3. تطبيق ممارسات التصفح الآمن: يجب أن يكون الطلاب قادرين على تطبيق عادات التصفح الآمن، بما في ذلك تجنب المواقع المشبوهة، والتعرف على المواقع الآمنة، وفهم أهمية عدم النقر على الروابط المجهولة. 4. فهم مفهوم الخصوصية عبر الإنترنت: يجب أن يستوعب الطلاب مفهوم الخصوصية عبر الإنترنت، وأن يكونوا قادرين على تحديد وشرح المعلومات الشخصية التي لا ينبغي مشاركتها عبر الإنترنت. 5. التعرف على التنمر الإلكتروني والاستجابة له: يجب أن يكون الطلاب قادرين على تحديد حالات التنمر الإلكتروني وفهم كيفية الاستجابة لمثل هذه الحوادث والإبلاغ عنها. 6. شرح دور برامج مضادات الفيروسات وجدران الحماية: يجب أن يفهم الطلاب الغرض من برامج مضادات الفيروسات وجدران الحماية في حماية أنظمة الحاسوب من التهديدات، وأن يكونوا قادرين على شرح أهميتها. 7. ممارسة الاستخدام المسؤول لمواقع التواصل الاجتماعي: يجب أن يفهم الطلاب أهمية السلوك المحترم على منصات التواصل الاجتماعي، بما في ذلك تجنب مشاركة المحتوى غير اللائق واحترام خصوصية الآخرين. 8. إظهار المعرفة بالنسخ الاحتياطي للبيانات واستعادتها: يجب أن يفهم الطلاب أهمية إجراء نسخ احتياطي للبيانات بانتظام، وأن يكونوا قادرين على شرح الطرق المختلفة للنسخ الاحتياطي والاستعادة. 9. إظهار الاستخدام الأخلاقي للتكنولوجيا: يجب أن يظهر الطلاب فهماً للاستخدام الأخلاقي للتكنولوجيا، بما في ذلك احترام قوانين حقوق النشر، وإسناد الفضل لأصحاب المحتوى الرقمي، وتجنب الانتحال العلمي (السرقية الأدبية).	
1. مقدمة في أمن المعلومات ● فهم مفهوم أمن المعلومات ● استكشاف أهمية أمن المعلومات 2. المخاطر الأمنية الشائعة ● الفيروسات، والبرمجيات الخبيثة، وتأثيرها ● هجمات التصيد الاحتيالي وكيفية التعرف عليها ● الحماية من سرقة الهوية 3. أمان كلمات المرور ● إنشاء كلمات مرور قوية ومميزة	المحتوى الإرشادي

- أدوات واستراتيجيات إدارة كلمات المرور
- أهمية عدم مشاركة كلمات المرور مع الآخرين

4. عادات التصفح الآمن

- التعرف على المواقع الإلكترونية الآمنة (شهادات SSL/TLS)
- تجنب المواقع المشبوهة والنوافذ المنبثقة
- فهم مخاطر النقر على الروابط المجهولة

5. الخصوصية عبر الإنترنت

- تحديد المعلومات الشخصية التي لا ينبغي مشاركتها عبر الإنترنت
- فهم أهمية إعدادات الخصوصية
- حماية المعلومات الشخصية على منصات التواصل الاجتماعي

6. التنمر الإلكتروني والمضايقات عبر الإنترنت

- التعرف على التنمر الإلكتروني وفهمه
- استراتيجيات الاستجابة لحوادث التنمر الإلكتروني والإبلاغ عنها
- تعزيز بيئة آمنة ومحترمة عبر الإنترنت

7. برامج مضادات الفيروسات وجدران الحماية

- مقدمة في برامج مضادات الفيروسات وجدران الحماية
- فهم دورها في الحماية من التهديدات
- اختيار برامج الأمان الموثوقة وتثبيتها

8. الاستخدام المسؤول لمواقع التواصل الاجتماعي

- نشر المحتوى المناسب ومشاركته
- احترام خصوصية الآخرين والمواطنة الرقمية
- فهم تبعات التصرفات عبر الإنترنت

9. النسخ الاحتياطي للبيانات واستعادتها

- أهمية إجراء نسخ احتياطي للبيانات بانتظام
- طرق النسخ الاحتياطي للبيانات (مثل: الأقراص الصلبة الخارجية، والتخزين السحابي)
- خيارات استعادة البيانات في حالة فقدانها

10. الاستخدام الأخلاقي للتكنولوجيا

- احترام قوانين حقوق النشر والملكية الفكرية
- فهم الانتحال العلمي (السرقية الأدبية) وإسناد الفضل للمحتوى الرقمي
- تعزيز السلوك الأخلاقي في التفاعلات عبر الإنترنت

11. التفكير النقدي والمعلومات عبر الإنترنت

- تقييم مصداقية وموثوقية المعلومات عبر الإنترنت

● تطوير مهارات التفكير النقدي اتخاذ قرارات مبنية على معرفة

● التحقق من صحة مصادر المعلومات عبر الإنترنت

استراتيجيات التعليم والتعلم

1. **المناقشات التفاعلية:** إشراك الطلاب في مناقشات حول مفاهيم أمن المعلومات، والمخاطر، وأفضل الممارسات. وتشجيعهم على مشاركة أفكارهم، وتجاربهم، وأسئلتهم المتعلقة بالسلامة والخصوصية عبر الإنترنت.
2. **العروض التقديمية متعددة الوسائط:** استخدام الموارد متعددة الوسائط مثل الفيديوهات، والرسوم المتحركة، والعروض التفاعلية لشرح المفاهيم المعقدة بطريقة جذابة بصرياً وسهلة الفهم. حيث تساعد هذه الموارد في جذب انتباه الطلاب وتعزيز فهمهم.
3. **الأنشطة العملية التطبيقية:** دمج الأنشطة العملية لتثبيت التعلم؛ مثل تكليف الطلاب بإنشاء واستخدام كلمات مرور قوية، أو التعرف على إيميالات التصيد الاحتيالي، أو التمييز بين المواقع الإلكترونية الآمنة وغير الآمنة من خلال تمارين تفاعلية.
4. **دراسات الحالة والسيناريوهات الواقعية:** تقديم دراسات حالة أو سيناريوهات من الحياة الواقعية توضح أهمية أمن المعلومات، وتشجيع الطلاب على تحليل ومناقشة المخاطر المحتملة والإجراءات المناسبة للحد منها.
5. **لعب الأدوار والتمثيل:** إشراك الطلاب في أنشطة لعب الأدوار حيث يمكنهم تمثيل مواقف مختلفة تتعلق بالأمان عبر الإنترنت؛ مثل محاكاة الرد على بريد تصيد احتيالي أو إنشاء كلمة مرور آمنة ضمن سيناريو تمثيلي.
6. **المشاريع الجماعية والتعلم التعاوني:** تعيين مشاريع جماعية يتعاون فيها الطلاب للبحث والتقديم حول جوانب مختلفة من أمن المعلومات، مما يعزز العمل الجماعي، والتفكير النقدي، والفهم العميق للمادة.
7. **الاستضافة والخبراء:** دعوة متحدثين أو خبراء في مجال أمن المعلومات لمشاركة معرفتهم وتجاربهم مع الطلاب، مما يوفر رؤى من العالم الحقيقي ويساعد الطلاب على ربط المفاهيم بالتطبيقات العملية.
8. **التلعيب (التعلم باللعب):** دمج الألعاب التعليمية أو الاختبارات القصيرة التفاعلية المتعلقة بأمن المعلومات لجعل التعلم ممتعاً ومحفزاً. يساعد هذا النهج في ترسيخ المعرفة، وتشجيع المنافسة الإيجابية، تقديم تغذية راجعة فورية.
9. **ورش عمل أمان الإنترنت:** تنظيم ورش عمل أو دعوة الجهات المختصة أو المحترفين في الأمن السيبراني لتقديم جلسات حول أمان الإنترنت والسلوك المسؤول عبر الإنترنت، مما يمنح الطلاب نصائح عملية ورؤى قيمة.
10. **التأمل والتقييم الذاتي:** تشجيع الطلاب على التأمل في سلوكياتهم عبر الإنترنت وتقييم تدابير الأمان التي يطبقونها حالياً، وحثهم على تحديد مجالات التحسين وتطوير خطط عمل شخصية لتعزيز ممارسات أمن المعلومات الخاصة بهم.

استراتيجيات

حمل عمل الطالب

5	الساعات المجدولة (ساعات/أسبوع)	65	الساعات المجدولة (ساعات/فصل دراسي)
6	الساعات غير مجدولة (ساعات/أسبوع)	85	الساعات غير المجدولة (ساعات/فصل دراسي)
150		الإجمالي (ساعات/فصل دراسي)	

تقييم المقرر الدراسي

						الوقت/العدد	الوزن (الدرجات)	الأسابيع	مخرجات التعلم
التقويم التكويني	اختبارات	2	5 (5%)	3,7					
	اختبار منتصف الفصل الدراسي	2	10%(10)	5,10					
	اختبار منتصف الفصل الدراسي عملي	5	10%(10)	12					
	واجب بيتي مختبر	3	5 (5%)	3,7,10					
	واجبات البيتية	1	5 (5%)	2,3,4,7,8					
	اختبار عملي	3	5 (5%)	3,7	جميع المخرجات				
	التنفيذ الأسبوعي	3	10%(10)	كل اسبوع					
التقييم النهائي			40%(40)						
	امتحان المد	ساعتان	10%(10)	7					
	امتحان النهائي	3 ساعات	50%(50)	16					
إجمالي التقييم		100%(100 درجة)							

خطة التدريس (المنهج الأسبوعي)

المنهج الدراسي	
مقدمة في أمن المعلومات	الأسبوع 1
المخاطر الأمنية الشائعة	الأسبوع 2
أمان كلمات المرور	الأسبوع 3
شرح أهمية وتطبيقات كل من السرية، والنزاهة (سلامة البيانات)، والمصادقة، والتوفر	الأسبوع 4
الهجمات على أجهزة الحاسوب وأمن الحاسوب	الأسبوع 5
آليات الأمان، ونموذج لأمن الشبكات. التشفير: المفاهيم والتقنيات	الأسبوع 6
مبادئ التشفير التقليدي	الأسبوع 7
معيار تشفير البيانات (DES)	الأسبوع 8
تشفير المفتاح العام	الأسبوع 9
خوارزمية RSA	الأسبوع 10
تبادل المفاتيح بأسلوب ديفي-هيلمان (Diffie-Hellman)	الأسبوع 11
تشفير المنحنيات البيضاوية (ECC)	الأسبوع 12
خوارزميات مصادقة الرسائل ودوال التجزئة (Hash Functions)	الأسبوع 13
الخصوصية عبر الإنترنت	الأسبوع 14
الاستخدام الأخلاقي للتكنولوجيا	الأسبوع 15

خطة التدريس (المنهج الأسبوعي في المختبر)	
المنهج الدراسي	
المختبر 1: تطبيق تشفير قيصر (Caesar Cipher)	الأسبوع 1
المختبر 2: تطبيق التشفير المتأكل (Affine Cipher) بالمعادلة $c=3x+12$	الأسبوع 2
المختبر 3: تطبيق تشفير بليفيير (Playfair Cipher) بمفتاح يدخله المستخدم	الأسبوع 3
المختبر 4: تطبيق التشفير متعدد الأبجديات (Polyalphabetic Cipher)	الأسبوع 4
المختبر 5: تطبيق تشفير المفتاح التلقائي (AutoKey Cipher)	الأسبوع 5
المختبر 6: تطبيق تشفير هيل (Hill Cipher)	الأسبوع 6
المختبر 7: تطبيق تقنية التشفير بالسياج (Rail Fence Technique)	الأسبوع 7
المختبر 8: تطبيق تقنية التبدل العمودي البسيط (Simple Columnar Transposition)	الأسبوع 8
المختبر 9: تطبيق تقنية التبدل العمودي المتقدم (Advanced Columnar Transposition)	الأسبوع 9
المختبر 10: تطبيق خوارزمية RSA المبسطة بأعداد صغيرة	الأسبوع 10
المختبر 11: تطبيق معيار التشفير المتقدم المبسط (Simplified DES)	الأسبوع 11
المختبر 12: تشفير الكتل ومعيار تشفير البيانات (DES)	الأسبوع 12
المختبر 13: معيار التشفير المتقدم (AES)	الأسبوع 13
المختبر 14: إجراء دراسة على أحد أنظمة كشف التسلل (مثل Snort)	الأسبوع 14
المختبر 15: مراجعة للاختبار	الأسبوع 15

المصادر التعليمية والتدريسية		
متوفر في المكتبة؟	النص	
لا	1. Security in Computing, Fourth Edition, by Charles P. Pfleeger, Pearson Education 2. Cryptography And Network Security Principles And Practice, Fourth or Fifth Edition, William Stallings, Pearso	الكتب الأساسية / المطلوبة
لا	Modern Cryptography: Theory and Practice, by Wenbo Mao, Prentice Hall.	الكتب الموصي بها
	https://www.w3schools.com/cpp/cpp_intro.asp	المواقع الإلكترونية

مخطط الدرجات				
المجموعة	الدرجة	التقدير	التقدير %	التقدير
مجموعة النجاح (100 - 50)	A - ممتاز	امتياز	90 - 100	أداء ممتاز
	B- جيد جداً	جيد جدا	80 - 89	فوق المتوسط مع بعض الأخطاء
	C- جيد	جيد	70 - 79	عمل جيد مع أخطاء ملحوظة
	D- مقبول	متوسط	60 - 69	مقبول لكن مع نقائص كبيرة
	E - كافٍ / مرضٍ	مقبول	50 - 59	العمل يلبي الحد الأدنى من المعايير
مجموعة الرسوب (49 - 0)	FX-راسب (قيد المعالجة)	راسب (قيد المعالجة)	(45-49)	يتطلب مزيداً من العمل ولكن يُمنح الطالب الدرجة
	F-راسب	راسب	(0-44)	يتطلب قدرًا كبيرًا من العمل
ملاحظة:				
سيتم تقريب العلامات العشرية التي تزيد أو تقل عن 0.5 إلى العلامة الكاملة الأعلى أو الأدنى (على سبيل المثال، العلامة 54.5 سيتم تقريبها إلى 55، بينما العلامة 54.4 سيتم تقريبها إلى 54). تطبق الجامعة سياسة عدم قبول حالات الرسوب القريبة من النجاح، لذا فإن التعديل الوحيد للدرجات الممنوحة من قبل المصحح/المصححين الأصليين سيكون التقريب التلقائي الموضح أعلاه فقط.				