

ربيع 2026 - (CS400) توصيف مقرر أمن المعلومات

1. معلومات عامة عن المقرر

المؤسسة التعليمية	جامعة الزنتان
اسم الكلية	كلية التربية تيجي
القسم العلمي	قسم الحاسوب
اسم المقرر الدراسي	(Information Security) أمن المعلومات
رمز المقرر	CS400
طبيعة المقرر	تخصصي
عدد الوحدات الدراسية المعتمدة	وحدات دراسية 3
عدد الساعات التعليمية الأسبوعية	ساعات (نظري/عملي) - 42 ساعة إجمالي 3
المتطلبات السابقة للمقرر	CS302
البرنامج التعليمي	قسم الحاسوب - كلية التربية تيجي
لغة تدريس المقرر	اللغة العربية واللغة الإنجليزية
الفصل الدراسي/العام الدراسي	الفصل الدراسي ربيع 2026
منسق المقرر	أ. أمل الصويغي
تاريخ اعتماد التوصيف	2026

2. وصف المقرر

يزود المقرر الطالب بالمعلومات والمفاهيم الأساسية عن أمن المعلومات. ويتضمن ذلك تعريف الطالب بالأخطار المحتملة والأساليب المختلفة لمهاجمة أنظمة المعلومات وطرق الحماية المختلفة. يدرس الطالب السياسات الأمنية وطرق التشفير واستخدام الجدار الناري لتأمين أنظمة المعلومات.

3. أهداف المقرر

1. شرح مفاهيم أمن المعلومات الأساسية.
2. تفسير السياسات الأمنية المتبعة.
3. تلخيص طرق حماية أنظمة المعلومات.
4. تشفير المعلومات وفكها باستخدام الطرق المعروفة.
5. شرح دراية تامة بمفهوم الجدار الناري.
6. تحديد طرق مهاجمة أنظمة المعلومات وكيفية منعها.
7. فهم أهمية تأكيد هوية المستخدم وحماية البيانات.
8. تطبيق تقنيات التوقيع الرقمي والشهادات الأمنية.
9. التعرف على التهديدات والبرمجيات الخبيثة وطرق الوقاية منها.

4. مخرجات التعلم المستهدفة

أ- المعرفة والفهم

- 1. أ: يعرف مفاهيم أمن المعلومات وأهدافها.
- 2. أ: يوضح التهديدات الأمنية الشائعة.
- 3. أ: يشرح خوارزميات التشفير (المتماثلة وغير المتماثلة).

- أ4: يوضح تقنيات التحقق من صحة الرسائل والبيانات.
- أ5: يشرح مفهوم الشهادات الرقمية والتوقيع الإلكتروني.
- أ6: يوضح طرق الهجمات (مثل Man-in-the-Middle).
- أ7: يشرح آليات التأكد من هوية المستخدم.
- أ8: يوضح وظائف الجدار الناري والسياسات الأمنية.
- أ9: يعرف مخاطر البرمجيات الخبيثة.

ب- المهارات الذهنية

- في الأنظمة (Vulnerabilities) ب1: يحلل نقاط الضعف.
- ب2: يقارن بين خوارزميات التشفير المختلفة.
- ب3: يستنتج طرق الوقاية من الهجمات الأمنية.
- ب4: يقيم فعالية السياسات الأمنية.
- ب5: يصمم خططاً لتأمين الشبكات.
- ب6: يربط بين المفاهيم الأمنية والواقع العملي.
- ب7: ينقد الحلول الأمنية المطبقة.
- ب8: يوظف التفكير التحليلي في كشف الهجمات.
- ب9: يطور استراتيجيات للتعليم المستمر في أمن المعلومات.

ج- المهارات العلمية والعملية

- ج1: يطبق خوارزميات التشفير لعمليات التشفير وفك التشفير.
- ج2: يستخدم دالة الهاش (Hash) للتأكد من سلامة البيانات.
- ج3: ينفذ عمليات التوقيع الإلكتروني.
- ج4: يطبق بروتوكولات التحقق من الهوية.
- ج5: يستخدم إعدادات الجدار الناري.
- ج6: يستخدم أدوات كشف البرمجيات الخبيثة.
- ج7: يطبق آليات التأكد من صحة هوية المستخدم.
- ج8: يستخدم طرقاً لاختبار قوة كلمات المرور.
- ج9: يصمم نظاماً بسيطاً لحماية البيانات.

د- المهارات العامة

- د1: يتواصل بفعالية ضمن فريق أمني.
- د2: يدير الوقت لإنجاز المهام الأمنية.
- د3: يستخدم تقنية المعلومات للبحث عن التهديدات الجديدة.
- د4: يعرض التقارير الأمنية بوضوح.
- د5: يفكر نقدياً في الثغرات الأمنية.
- د6: يتحمل مسؤولية حماية البيانات.
- د7: يطور مهاراته لمواكبة التهديدات الرقمية.
- د8: يلتزم بأخلاقيات أمن المعلومات.
- د9: يستخدم المصادر والمكتبات الرقمية بفاعلية.
- د10: يحل المشكلات الأمنية بأسلوب منهجي.
- د11: يبدي مرونة في التعامل مع الهجمات المفاجئة.
- د12: يوثق العمليات الأمنية بطريقة علمية.

5. محتوى المقرر الدراسي

الموضوعات	الأسبوع
مقدمة في أمن المعلومات، التهديدات، نقاط الضعف، الأهداف	الأول
تقنيات التشفير	الثاني
خوارزميات التشفير المتماثلة	الثالث
خوارزميات التشفير غير المتماثلة	الرابع
(Message Authentication) التحقق من صحة الرسائل	الخامس
(Man-in-the-Middle) الشهادات الأمنية، الهجمات	السادس
التأكد من هوية المستخدم، كلمات المرور، البيانات الحيوية	السابع
التقييم النصفى	الثامن
البروتوكولات الخاصة بتأكيد الهوية	التاسع
الجدار الناري	العاشر
السياسات الأمنية	الحادي عشر
(السياسات الأمنية) (تكملة)	الثاني عشر
البرامج الخبيثة والفيروسات	الثالث عشر
(البرامج الخبيثة والفيروسات) (تكملة)	الرابع عشر
الامتحان النهائي + (Software Security) أمن البرمجيات	الخامس عشر

6. طرق التعليم والتعلم

- المحاضرات النظرية والعروض التقديمية.
- التفاعل والنقاش الجماعي في القضايا الأمنية.
- الأنشطة الموجهة ذاتياً في البحث عن الثغرات.
- التجارب المخبرية لتطبيق خوارزميات التشفير.

7. طرق التقييم

النسبة	توقيت التقييم	أسلوب التقييم
40%	على مدار الفصل	أعمال الفصل الدراسي
60%	نهاية الفصل	الامتحان النهائي
100%	-	المجموع

8. الإمكانيات المطلوبة لتنفيذ المقرر

- معمل حاسوب مجهز بأدوات وبرمجيات أمن الشبكات.
- وسبورة ذكية (Data Show) جهاز عرض.
- اتصال بشبكة الإنترنت للوصول إلى أدوات اختبار الاختراق والمصادر الأمنية.
- لمتابعة الواجبات والاختبارات (LMS) نظام إدارة تعلم إلكتروني.

9. المراجع

1. Security in Computing, 4th Ed, by Charles P. Pfleeger, Pearson Education.
2. Cryptography And Network Security Principles And Practice, 5th Ed, William Stallings, Pearson.
3. Modern Cryptography: Theory and Practice, by Wenbo Mao, Prentice Hall.

- ## 10. (مصفوفة المقرر) توزيع المخرجات

[illegible]