الجمهوريّة العربيّة السوريّة		Syrian Arab Republic
وزارة التعليـم العالـــــي		Ministry of Higher Education
الجامعة الافتراضيّة السوريّة		Syrian Virtual University

وثيقة تعريف: التعمية

١- معلومات أساسيّة:

اسم المقرّر	التعمية
رمز المقرّر	ISE - CR
ساعات الجلسات المسجّلة	١٨
ساعات الجلسات المتزامنة	١٨
ساعات المذاكرة	---
ساعات الامتحان	٢
ساعات الجهد الدراسي المقابل للجلسات المسجّلة	٣٦
ساعات الجهد الدراسي المقابل للجلسات المتزامنة	٣٦
عدد الساعات المعتمدة	٣

٢- المقرّرات المطلوب دراستها قبل المقرّر مباشرةً:

المقرّر	الرمز
تحليل عددي	ISE – NA

٣- الهدف من المقرّر:

يعد التشفير (التعمية) Cryptography أحد أهم الوسائل المستخدمة لتوفير بيئة آمنة لتبادل المعلومات وحمايتها. نعرض في هذه المادة أسس ومبادئ تشفير المعلومات ونبين كيفية استخدام هذه التقنيات لتحقيق الأهداف الثلاث التالية: السرية Confidentiality، وسلامة المعطيات Integrity، والتحقق من الهوية Authentication. يجري ذلك من خلال استعراض أساليب التشفير المتناظر التقليدية التي ظهرت واستخدمت في الماضي وتلك المستخدمة حالياً، مثل المعيارين DES وAES. كما يتعرض المقرر لأساليب التشفير اللامتناظر مع التركيز على خوارزمية RSA. يضاف إلى ذلك دراسة موضوعات لها علاقة بالتحقق من سلامة الرسائل والتحقق من الهوية وإدارة المفاتيح.

الجمهوريّة العربيّة السوريّة		Syrian Arab Republic
وزارة التعليـم العـالـــــي		Ministry of Higher Education
الجامعة الافتراضيّة السوريّة		Syrian Virtual University

٤- المحصّلات التعليميّة المرجوّة (ILO – Intended Learning Objectives/Outcomes):

الرمز	المحصّلات التعليميّة المرجوّة
ILO	Intended Learning Objectives/Outcomes
ILO1	فهم المبادئ العامة لأمن المعلومات وما يرتبط منها بعلم التعمية
ILO2	التعرف على التشفير التقليدي والخوارزميات القديمة المستخدمة في إطاره
ILO3	فهم بنية وطريقة عمل أنظمة التشفير المتناظر، وتفاصيل المعيارين DES وAES
ILO4	فهم بنية وطريقة عمل خوارزميات التشفير اللامتناظر، وتفاصيل خوارزمية RSA
ILO5	فهم توابع التهشير وطرق التحقق من الرسائل
ILO6	التعرف على آليات إدارة المفاتيح وتبادلها
ILO7	اكتساب مهارة تنفيذ خوارزمية تشفير واختبارها

٥- محتوى المقرر:

المحصّلات التعليميّة	القسم النظري مع ملاحظات وتوضيحات إن وجدت	ساعات مسجّلة	ساعات متزامنة	أنماط المهام	القسم العملي مع ملاحظات وتوضيحات إن وجدت
ILO1	• أهداف أمن الحواسيب • متطلبات أمن الحواسيب • معمارية الأمن • خدمات الأمن • آليات الأمن	٣	٣	---	---

	• نموذج أمن الشبكات				
ILO2	• نموذج التشفير المتناظر • تقنيات التشفير بالتعويض • تقنيات التشفير بتغيير الموقع	١.٥	١.٥	وظائف	تمارين
ILO3	• التشفير الدفقي • التشفير الكتلي • خوارزمية تشفير فيستل • معيار تشفير البيانات DES • معيار التشفير المتقدم AES • عمليات التشفير الكتلي	٤.٥	٤.٥	وظائف	تمارين
ILO4	• مبادئ التشفير بالمفتاح العام • تطبيقات التشفير بالمفتاح العام • متطلبات التشفير بالمفتاح العام • خوارزمية RSA • تبادل المفاتيح Diffie-Hellman • خوارزمية ElGamal • خوارزمية ECC	١.٥	٤.٥	وظائف	تمارين
ILO5	• توابع التهشير • التحقق من الرسائل • رمز التحقق من الرسالة MAC • التوقيع الرقمي • خوارزمية HMAC	٦	٣	وظائف	تمارين
ILO6	• توزيع المفاتيح المتناظرة • شهادات المفتاح العام • البنية التحتية للمفاتيح العامة PKI	١.٥	١.٥	وظائف	تمارين
ILO7	• وظيفة المقرر	٠	٠	وظائف	---

الجمهوريّة العربيّة السوريّة		Syrian Arab Republic
وزارة التعليـم العـالـــــي		Ministry of Higher Education
الجامعة الافتراضيّة السوريّة		Syrian Virtual University

٦- معايير التقويم:

ILO Code	المحصّلات التعليميّة	النتائج التعليميّة	نمط التقويم				
			تفاعل في الجلسات المتزامنة	عملي	امتحانات	عروض ومقابلات	تقارير
ILO1	فهم المبادئ العامة لأمن المعلومات وما يرتبط منها بعلم التعمية	فهم الأسس اللازمة لتعلم التشفير	✓		✓		
ILO2	التعرف على التشفير التقليدي والخوارزميات القديمة المستخدمة في إطاره	الاطلاع على أساس علم التشفير تاريخياً	✓	✓	✓		
ILO3	فهم بنية وطريقة عمل أنظمة التشفير المتناظر، وتفاصيل المعيارين DES وAES	تعلم إمكانيات معايير التشفير المتناظر	✓	✓	✓		
ILO4	فهم بنية وطريقة عمل خوارزميات التشفير اللامتناظر، وتفاصيل خوارزمية RSA	تعلم إمكانيات التشفير اللامتناظر	✓	✓	✓		
ILO5	فهم توابع التهشير وطرق التحقق من الرسائل	تعلم كيفية التحقق من سلامة رسالة وهوية مصدرها	✓	✓	✓		
ILO6	التعرف على آليات إدارة المفاتيح وتبادلها	الاطلاع على حلول تشارك مفاتيح التشفير	✓		✓		

ILO7	اكتساب مهارة تنفيذ خوارزمية تشفير واختبارها	التطبيق العملي لتطوير خوارزمية تشفير		✓			✓

٧- أدوات ومختبرات القسم العملي:

إسم الأداة	توصيفها
.NET	بيئة تطوير لخوارزميات التشفير

٨- المراجع الأساسية:

Stallings, William. *Cryptography and network security: principles and practice*. Pearson, 2017.

٩- المراجع الإضافية:

- Katz, Jonathan, et al. *Handbook of applied cryptography*. CRC press, 1996.
- Schneier, Bruce. *Schneier's Cryptography Classics Library: Applied Cryptography, Secrets and Lies, and Practical Cryptography*. Wiley Publishing, 2007.