

توصيف مقرر دراسي

قسم: الميكاترونكس		كلية: الهندسة	
CEME501	رمز المقرر:	Information System Security	
-	المتطلب السابق:	2: عملي	2: نظري
		الساعات المعتمدة: 2	

التوصيف
<p>يهدف هذا المقرر إلى تعريف بأسباب ظهور مفهوم أمن المعلومات وأهميته والهجمات المختلفة التي تهدد أي نظام، والحاجة إلى تطبيق تقنيات الأمن، وكما يستعرض متطلبات الأمن الأساسية (الموثوقية، تكاملية المعطيات، المصادقة....) التي يجب توافرها ضمن أي نظام ويوضح العلاقة بين هذه المتطلبات و الهجمات وتدرج أهميتها حسب الغاية التطبيق المستخدمة فيه، والتعريف بمفهوم التشفير وتصنيفاته (متناظر-غير متناظر، كتلي-تسلسلي) بالإضافة إلى تمكين الطالب من استخدام التقنيات المختلفة (خوارزميات تشفير متناظر مثل خوارزمية DES-خوارزميات التشفير غير المتناظر مثل خوارزمية RSA وخوارزمية حقيبة الظهر-خوارزمية RC4 التسلسلية-توابع البعثة-التواقيع الرقمية-...)، وجعله قادراً على اختيار التقنية أو دمج التقنيات المختلفة بهدف الوصول إلى حل المشكلة الأمنية التي تواجهه. كما يتطرق المقرر إلى مفهوم الشهادة الرقمية (توليدها-توزيعها..) والأمن في الأنظمة الديناميكية، إضافة إلى بمفهوم إدارة مفاتيح التشفير وآليات توزيعها وتقنيات التعافي في حال تعرض النظام لهجوم.</p>
المحتوى
<ul style="list-style-type: none"> • مقدمة إلى أمن المعلومات ومتطلباته • تصنيف خوارزميات التشفير: <ul style="list-style-type: none"> ✓ حسب المفاتيح: <ul style="list-style-type: none"> ○ خوارزميات التشفير المتناظر ○ خوارزميات التشفير غير المتناظر ✓ حسب النص الصريح: <ul style="list-style-type: none"> ○ التشفير الكتلي ○ التشفير التسلسلي • خوارزمية DES • خوارزمية RSA • خوارزمية KNAPSACK • تابع البعثة (HASH) • تقنية التوقيع الرقمي (Digital Signature) • الشهادة الرقمية (Digital Certificate) وهيكلية المفتاح العام (PKI) • إدارة مفاتيح التشفير: توليد المفاتيح-توزيعها-تقنيات التعافي في حال الهجوم • البروتوكول WEP:

✓ خوارزمية RC4

• الأمن في المجموعات الديناميكية

المراجع

- 1- Hans Delfs and Helmut Knebl, "Introduction to Cryptography (Principles and Applications)", Third Edition .Springer .2015 . 508 pages.
- 2- Christof Paar and Jan Pelsl, "Understanding Cryptography", Springer -2010-372 pages.
- 3-Kim-Kwang Raymond Choo, "Secure key establishment", Springer, Advances in Information Security Series,2008,229 pages.

عميد كلية الهندسة
أ.د. علاء الدين حسام الدين