

نموذج (٥)

مختصر توصيف المقرر

رقم المقرر ورمزه: MTH 445	اسم المقرر: نظرية التشفير Coding and Cryptography Theory
لغة تدريس المقرر: الإنجليزية	المتطلب السابق للمقرر: MTH 444
الساعات المعتمدة: ٣ ساعات	مستوى المقرر: الثامن

Module Description

وصف المقرر :

<p>In this course we will study the arithmetic on \mathbb{Z} , the ring $\mathbb{Z} / n\mathbb{Z}$ and then the field $\mathbb{Z} / p\mathbb{Z}$. When $p=2$ we can introduce the binary code. We give an overview on the history of the cryptography and introduce the symmetric cryptography.</p> <p>We introduce The RSA coding and the notion of code correcting.</p> <p>A Large part of the course is devoted to linear codes, the Hamming codes, dual codes, generating Matrix and many notions related to linear codes are introduced</p>	<p>في هذا المقرر نقوم بدراسة الحساب على الحلقة \mathbb{Z} وحفلات $\mathbb{Z} / n\mathbb{Z}$. بالخصوص فالحقول التي هي بشكل $\mathbb{Z} / p\mathbb{Z}$. أين p عدد أولي مما يمكننا من ادخال الكود الثنائي. نعطي لمحة عن تاريخ التشفير ثم نعرض خصائص التشفير المتماثل. نقدم كذلك التشفير RSA فكرة عن الكود القابل التصحيح جزءا كبيرا من المقرر يخصص لدراسة الكود الخطي و كود هامينغ فالكود الإزدواجي ، للمصفوفة المولدة للكود و مفاهيم كثيرة تخص الكود الخطي</p> 
--	--

Module Aims

أهداف المقرر :

مخرجات التعليم: (الفهم والمعرفة والمهارات الذهنية والعملية)

<p>This course deals with the mathematical ideas underlying modern coding theory and cryptography, including algebra, number theory and probability theory.</p> <p>This course aims to address the efficient error free and secure delivery of information using binary data streams. For efficiency, the information source is coded to reduce redundancy. To minimize the effects of errors, channel coding is employed and finally cryptographic techniques are required to make the data secure. The aim is to present the basic theory and objectives of each of these steps, together with the basics of information theory.</p>	<p>من بين أهداف هذا المقرر هو دراسة المفاهيم الرياضية التي هي تدخل في بناء الكودات و عملية تشفير المعلومة و أهمها بعض جوانب الجبر (نظرية الأعداد) و الإحتمالات.</p> <p>هذا المقرر يهدف الى معالجة الاخطاء بكفاءة وتأمين اوصول المعلومات باستخدام بيانات ثنائية.</p> <p>لضمان تأمين وصول المعلومة صحيحة للمرسل اليه حتى ولو كان الإرسال عبر قنوات من المفترض انها تشوهها ندرس طرق بناء كودات يقل فيها التكرار الغير مفيد . لتقليل اثار الاخطاء, ويستخدم قنوات الترميز, واخيرا نكتشف من خلال هذا المقرر أن تقنيات التشفير لها أهمية كبيرة لتأمين البيانات.</p> <p>والهدف من هذا المقرر هو تقديم النظريات الأساسية والاهداف لكل خطوة و دراسة اساسيات نظرية المعلومات</p>
--	---

يفترض بالطالب بعد دراسته لهذا المقرر أن يكون قادرا على:

<ul style="list-style-type: none">- Know the importance of the coding theory- How he can make some elementary codes- Know all the tools used in linear codes- Extract the generator of a code- Construct the dual code of a given linear code- Correct some errors induced by the canal- Determine the Hamming distance between two words code	<ul style="list-style-type: none">- ذو معرفة متقدمة في أهمية التشفير- بناء بعض الكودات البسيطة- صرد كل مفاهيم التشفير الخطي- بناء مصفوفة المولدة لكود خطي- بناء الكود الأزواجي لكود خطي- تطبيق مبادئ أخطاء الناجمة عن عملية الإرسال- تحديد مسافة هامينغ بين كلمتان و تصليح الأخطاء 
--	--

محتوى المقرر

ساعات التدريس	عدد الأسابيع	قائمة الموضوعات
6	2	الحساب
3	1	دراسة الحلقة Z/nZ
3	1	تاريخ التشفير
3	1	التشفير المتماثل الحديث
3	1	مواضيع إضافية في نظرية الحساب
3	1	التشفير RSA
3	1	مدخل الى التشفير المصحح
6	2	الفضاءات الثنائية لهامينغ و التشفير الخطي
3	1	كود التناهي و الكود الخطي
6	2	تطبيقات الكود الخطي
3	1	الكود الخطي و حماية المعلومة و البيانات

الكتاب المقرر والمراجع المساندة

الرقم الدولي ISBN	سنة النشر	اسم الناشر	اسم المؤلف	اسم الكتاب
	2008	Springer Undergraduate Mathematics Series 2008	Norman L. Biggs	An Introduction to information communication and cryptography
	2011	Pearson-Lawrence C. Washington, Wade	Trappe	Introduction to Cryptography with Coding Theory
	1995	Originally published Editor: Doug Stinson	Doug Stinson	Cryptography: Theory and Practice

