نموذج (5)

مختصر توصيف المقرر

اسم المقرر: نظرية التشفير Coding and Cryptography Theory	رقم المقرر ورمزه: MTH 445
المتطلب السابق للمقرر: MTH 444	لغة تدريس المقرر: الإنجليزية
مستوى المقرر: الثامن	الساعات المعتمدة: 3 ساعات

وصف المقرر : Module Description

فى هذا المقرر نقوم بدراسة الحساب على الحلقة $\mathbb{Z}$ وحفلات $\mathbb{Z}$. $n\mathbb{Z}$ / بالخصوص فالحقول التي هي بشكل $p\mathbb{Z}\mathbb{Z}$ / .أين p عدد أولي مما يمكننا من ادخال الكود الثنائى. نعطى لمحة عن تاريخ التشفيرثم نعرض خصائص التشفير المتماثل. نقدم كذلك التشفير RSA فكرة عن الكود القابل التصحيح جزءا كبيرا من المقرر يخصص لدراسة الكود الخطى و كود هامينغ فالكود الإزدواجي ، للمصفوفة المولدة للكود و مفاهيم كثيرة تخص الكود الخطي	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. We introduce the RSA coding and the notion of code correcting. 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

أهداف المقرر : Module Aims

مخرجات التعليم: (الفهم والمعرفة والمهارات الذهنية والعملية)

من بين أهداف هذا المقرر هو دراسة المفاهيم الرياضيات التي هي تدخل في بناء الكودات و عملية تشفير المعلومة و أهمها بعض جوانب الجبر (نظرية الأعداد) و الإحتمالات. هذا المقرر يهدف الى معالجة الاخطاء بكفاءة وتامين ايصال المعلومات باستخدام بيانات ثنائية. 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 . لتقليص اثار الاخطاء، ويستخدم قنوات الترميز، واخيرا نكتشف من خلال هذا المقرر أن تقنيات التشفير لها أهمية كبيرة لتأمين البيانات. والهدف من هذا المقرر هو تقديم النظريات الاساسية والاهداف لكل خطوة و دراسة اساسيات نظرية المعلومات	This course deals with the mathematical ideas underlying modern coding theory and cryptography, including algebra, number theory and probability theory. 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.

يفترض بالطالب بعد دراسته لهذا المقرر أن يكون قادرا على:

– معرفة متقدمة في أهمية التشفير – بناء بعض الكودات البسيطة – س – رد كل مفاهيم التشفير الخطي – بناء مصفوفة المولدة لكود خطي – بناء الكود الأزدواجي لكود خطي – تطبيق مبادىء أخطاء الناجمة عن عملية الإرسال – تحديد مسافة هامينغ بين كلمتان و تصليح الأخطاء	- 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

محـــتوى المقـــرر

قائمة الموضوعات	عدد الأسابيع	ساعات التدريس
لحساب	2	6
راسة الحلقة Z/nZ	1	3
اريخ التشفير	1	3
لتشفير المتماثل الحديث	1	3
واضيع إضافية في نظرية لحساب	1	3
لتشفير RSA	1	3
دخل الى التشفيرالمصحح	1	3
لفضاءات الثنائية لهامينغ و لتشفير الخطي	2	6
كود الثنائي و الكود الخطي	1	3
طبيقات الكود الخطي	2	6
لكود الخطي و حماية المعلومة ـ البينات	1	3

الكتاب المقرر والمراجع المساندة

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