

وزارة التعليم العالي والبحث العلمي
جامعة البصرة/كلية علوم الحاسوب وتكنولوجيا المعلومات
قسم علوم الحاسوب

الأمنية

Security (CS405)

د. حميد عبد الكريم يونس
كلية علوم الحاسوب وتكنولوجيا المعلومات/جامعة البصرة
قسم علوم الحاسوب

شباط ٢٠١٩

Security (C405)

Syllabus:

1. Introduction.
 - Basic Concepts and Terminology.
2. Classical Encryption Techniques.
 - Symmetric Cipher Model.
 - Substitution Techniques.
 - Transposition Techniques.
3. Block Ciphers and the Data Encryption Standard.
 - Block Cipher Principles.
 - Differential and Linear Cryptanalysis.
 - Block Cipher Modes of Operation.
4. Advanced Encryption Standard.
5. Stream Cipher.
6. Introduction to Number Theory.

Reference:

William Stallings, "*Cryptography and Network Security. Principle and Practice*", Third Edition, Principle Hall, USA, 2003.