# نموذج وصف المقرر

## Course Description

In this course, the student learns about all the traditional and modern security systems that have been used and that are currently in use. The student also learns how to break each system and understand why some security systems are weak and why other security systems are strong. We will even go over DES, AES, and Digital Signature which are among the main modern encryption systems in use today.

| | |
|---|---|
| ١. المؤسسة التعليمية ( Educational institution) | University of Basrah |
| ٢. القسم العلمي / المركز ( Scientific department/center) | Computer Science |
| ٣. اسم / رمز المقرر(Course name) | **Data Security** |
| ٤. أشكال الحضور المتاحة ( Available attendance forms) | Teaching Presence |
| ٥. الفصل / السنة (Semester/year) | ANNUAL TEACHING |
| ٦. عدد الساعات الدراسية (الكلي) ( Credit Hours) | **Practical 40-36…Theoretical 60 -54** |
| ٧. تاريخ إعداد هذا الوصف ( Date this description was prepared) | **1-9-2023** |
| ٨. أهداف المقرر (Course objectives) | |
| In this course you will learn the inner workings of cryptographic systems and how to use them properly in real-world applications.<br>• Describe some basic concepts of encryption<br>• Describe cryptography and its uses in cybersecurity<br>• Description of hash and digital signature<br>• Describe the concept and use of digital certificates | |

٩. مخرجات المقرر وطرائق التعليم والتعلم والتقييم ( Course outcomes and teaching, learning and evaluation methods)

أ- الاهداف المعرفية (Cognitive goals )

**Teaching students the basic concepts of cybersecurity, best practices, and .core competencies used by crypto experts**

ب - الاهداف المهاراتية الخاصة بالمقرر (Skills objectives for the course )

ب١ -

**Analytical Skills Cryptography learners need a strong understanding of mathematical principles, such as linear algebra, number theory, and combinatorics. Learners apply these principles when designing and decrypting strong cryptographic systems .**

طرائق التعليم والتعلم (Teaching and learning methods )

Providing the student with primary and secondary topics related to data security

Programming theoretical topics related to data security into computer programs

Requiring the student to use JavaScript programs related to theoretical vocabulary

طرائق التقييم (Evaluation methods )

**conducting the midterm exam**

**class participation**

**grading a number of in-class assignments**

**conducting a practical exam**

ج- الاهداف الوجدانية والقيمية (Emotional goals )

C1- The student listens to the Teacher's explanation

C2- Submit homework on time and participate in the class

C3- The student encourages his classmates to remain calm in class

C4- The student should develop his relationships with his colleagues in order to achieve the best so that he always acts “honestly and ethically in all his dealings”.

طرائق التعليم والتعلم (Teaching and learning methods )

Giving the student an opportunity to explain a small part of the class to his classmates to enhance his self-confidence

## ۱۰.بنية المقرر ( Course structure)

| الأسبوع( (Week | الساعات (H) | مخرجات التعلم المطلوبة | اسم الوحدة / أو الموضوع | طريقة التعليم | طريقة التقييم |
|---|---|---|---|---|---|
| 1 - 2 | 6 | Practical exercise | • Introduction to cryptography<br>• Private-key encryption<br>• Principle of Kerchhoff<br>• Scenarios of attacks<br>• Introduction to public key | Lectures( Theoretical + Practical ) | conducting the Midterm exam + class participation + grading a number of in-class assignments + conducting a practical exam |
| 3 - 4 | 6 | Practical exercise | • Application of cryptography<br>• Classical ciphers: Caeser, Shift cipher, monoalphabetic cipher, Vigenere cipher, auto key cipher<br>• Hill cipher<br>Playfair cipher | ( Lectures Theoretical Practical + ) | conducting the Midterm exam + class participation + grading a number of in-class assignments + conducting a practical exam |
| 5 - 7 | 6 | Practical exercise | • Private-key cryptosystems<br>• Permutation-substitution networks<br>• Feistel networks<br>• Data encryption standard (DES)<br>DES structur | ( Lectures Theoretical Practical + ) | conducting the Midterm exam + class participation + grading a number of in-class assignments + conducting a practical exam |
| 8 - 9 | 6 | Practical exercise | • Advanced Encryption Standard (AES)<br>• Work of AES<br>Security of AES | ( Lectures Theoretical Practical + ) | conducting the Midterm exam + class participation + grading a number of in-class |

| | | | | | |
|---|---|---|---|---|---|
| assignments + conducting a practical exam | | | | | |
| conducting the Midterm exam + class participation + grading a number of in-class assignments + conducting a practical exam | ( Lectures Theoretical Practical + ) | • Message authentication codes<br>CBC-MAC | Practical exercise | 6 | 10 - 12 |
| conducting the Midterm exam + class participation + grading a number of in-class assignments + conducting a practical exam | ( Lectures Theoretical Practical + ) | Applied hash functions like SHA-3 | Practical exercise | 6 | 13 - 15 |
| conducting the Midterm exam + class participation + grading a number of in-class assignments + conducting a practical exam | ( Lectures Theoretical Practical + ) | • Public key cryptosystems<br>Hybrid encryption<br>• RSA cipher | Practical exercise | 6 | 16 - 18 |
| conducting the Midterm exam + class participation + grading a number of in-class assignment | ( Lectures Theoretical Practical + ) | • Digital signature schemes<br>• Security of digital signature schemes<br>• RSA digital signature | Practical exercise | 6 | 19 - 21 |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| s + conducting a practical exam |  |  |  |  |  |
| conducting the Midterm exam + class participation + grading a number of in-class assignments + conducting a practical exam | ( Lectures Theoretical Practical + ) | • Schnorr digital signature<br>• Identification protocols<br>• Certificates for public key | Practical exercise | 6 | 22 - 24 |
| conducting the Midterm exam + class participation + grading a number of in-class assignments + conducting a practical exam | ( Lectures Theoretical Practical + ) | • Secure authentication protocols<br>• Mutual authentication<br>• Pseudo-random number generators (PRNG) and their security | Practical exercise | 6 | 24 - 26 |
|  |  | • RC4 algorithm<br>• Elliptic curve over real numbers<br>• |  |  | 27-30 |

| ١١. البنية التحتية |  |
|---|---|
| We recommend relying in the future on the book of the late Professor Dr. Iyad Ibrahim Abdel Sada (may God have mercy on him) as a primary reference, especially since he has modern scientific material in the Arabic language in the field of .information security | ١- الكتب المقررة المطلوبة<br>Required course )<br>(books |
| cryptography : theory and practice, 4th edition, Douglas r. Stinson, Maura B. Paterson, CRC press, 2019 | ٢- المراجع الرئيسية<br>(References)ٌ |
| 1. A Handbook of Applied Cryptography by Alfred J. Menezes,Paul C. Van Oorschot and Scott A. Vanstone, CRC Press Series on Discrete Mathematics and Its Applications<br>2. Oded Goldreich ,Springer-Verlag 1998 M,odern Cryptography, Probabilistic Proofs and Pseudorandomness | Books and references (أ |
| https://www.ccs.neu.edu/home/wichs/class/crypto-fall15/index.html<br>https://faculty.uobasrah.edu.iq/faculty/360/teaching | Electronic references, (ب<br>.....، Internet sites |

| **١٢. خطة تطوير المقرر الدراسي (Course development plan)** |
|---|
| Access to the curriculum for dealing with information security in the rest of the Iraqi and foreign government universities based on the developments in the security fields. |