# نموذج وصف المقرر

| |
|---|
| **1.** اسم المقرر |
| **التشفير الكتلي** |
| **2.** رمز المقرر |
| |
| **3.** الفصل / السنة |
| **الفصل الثاني /2024-2025** |
| **4.** تاريخ إعداد هذا الوصف |
| **2025/1/29** |
| 5. أشكال الحضور المتاحة |
| في الصف |
| 6. عدد الساعات الدراسية (الكلي)/ عدد الوحدات (الكلي) |
| 30 ساعة/2 وحدات |
| 7. اسم مسؤول المقرر الدراسي ( اذا اكثر من اسم يذكر) |
| الاسم: أ.د.هاله بهجت عبد الوهاب<br>الآيميل : Hala.B.AbdulWahab@uotechnology.edu. |
| **8. اهداف المقرر** |

| | |
|---|---|
| **اهداف المادة الدراسية** | • تهدف هذه المادة إلى تعليم الطالب على كيفية استخدام خوارزميات التشفير وبرمجتها بشكل ملائم لتشفير النصوص الهامه والسريه<br>• تعليم على اساس رياضي وتطبيقهابشكل عملي لخوارزميات التشفير<br>• الكتلي او خوارزميات المفتاح |

| |
|---|
| **9. استراتيجيات التعليم والتعلم** |

| | |
|---|---|
| **الاستراتيجية** | محاضرات نظري - مختبرات عملية -كتب منهجية – مصادر( انترنيت ) – استخدام الاجهزة الحديثة لوصول الماده الى الطلبة باستخدام ta show بالاضافه الى السبوره الذكية |

| |
|---|
| **10. بنية المقرر** |

| الأسبوع | الساعات | مخرجات التعلم المطلوبة | اسم الوحدة او الموضوع | طريقة التعلم | طريقة التقييم |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| 1 | نظري عملي | 1,3,5,7 | mmetric Cipher Model. | محاضرات نظرية | حضور- مناقشات – اختبارات |
| 2 | نظري عملي 2 س | 1,3,5,7 | Confusion and Diffusion | محاضرات نظرية+ تطبيق عملي | حضور- مناقشات – اختبارات |
| 3 | نظري عملي 2 س | 1,3,5,7 | Feistel Mode | محاضرات نظرية+ تطبيق عملي | حضور- مناقشات – اختبارات |
| 4 | نظري عملي 2 س | 1,3,5,7 | DataEncryption Standard DES | محاضرات نظرية+ تطبيق عملي | حضور- مناقشات – اختبارات |
| 5 | نظري عملي 2 س | 1,3,5,7 | Key of DES algorithm | محاضرات نظرية+ تطبيق عملي | حضور- مناقشات – اختبارات |
| 6 | نظري عملي 2 س | 1,3,5,7 | Example of DES | محاضرات نظرية+ تطبيق عملي | حضور- مناقشات – اختبارات |
| 7 | نظري عملي 2 س | 1,3,5,7 | Type of DES | محاضرات نظرية+ تطبيق عملي | حضور- مناقشات – اختبارات |
| 8 | نظري عملي 2 س | 1,3,5,7 | Cast algorithm | محاضرات نظرية+ تطبيق عملي | حضور- مناقشات – اختبارات |
| 9 | نظري عملي 2 س | 1,3,5,7 | Gost Algorithm | محاضرات نظرية+ تطبيق عملي | حضور- مناقشات – اختبارات |
| 1 | نظري عملي 2 س | 1,3,5,7 | Key generation of Gost | محاضرات نظرية+ تطبيق عملي | حضور- مناقشات – اختبارات |
| 1 | نظري عملي 2 س | 1,3,5,7 | Example of Gost | محاضرات نظرية+ تطبيق عملي | حضور- مناقشات – اختبارات |
| 1 | نظري عملي 2 س | 1,3,5,7 | Feal Algorithm | محاضرات نظرية+ تطبيق عملي | حضور- مناقشات – اختبارات |
| 1 | نظري عملي 2 س | 1,3,5,7 | Key Generation of Feal | محاضرات نظرية+ تطبيق عملي | حضور- مناقشات – اختبارات |
| 1 | نظري عملي 2 س | 1,3,5,7 | RC4 Algorithm | محاضرات نظرية+ تطبيق عملي | حضور- مناقشات – اختبارات |

| | | | | | |
|---|---|---|---|---|---|
| 1 | نظري<br>2 عملي | 1,3,<br>6,7 | أمتحان نهاية الكورس | محاضرات<br>نظرية+<br>تطبيق عمل | حضور<br>اختبارات |

## 11. تقييم المقرر

توزيع الدرجة من 100 على وفق المهام المكلف بها الطالب مثل التحضير اليومي والامتحانات اليومية والشفوية والشهرية والتحريرية والتقارير .... الخ
5 درجات حضور
5 درجات واجبات وتقارير
15 درجة امتحان منتصف الكورس (مد)
15 درجة امتحان المختبر تنفيذ البرامج الخاصة بالخوارزميات وادارة الفايلات
60 درجة الامتحان نهاية الكورس (الفصل الاول)

## 12. مصادر التعلم والتدريس

| | |
|---|---|
| **الكتب المقررة المطلوبة ( المنهجية أن وجدت )** | • H. Boker & F. Piper, " Cipher System, The Protection of Communications ", Northwood Books, Landon, 1982. |
| **المراجع الرئيسة ( المصادر)** | • B. Schneier, "**Applied Cryptography**", 2nd ed., John Wiley & Sons, Inc., 1996.<br>• ANSI X9.44, "**Public key cryptography using reversible algorithms for the financial services industry: Transport of symmetric algorithm keys using RSA**", 1994.. |
| **الكتب والمراجع الساندة التي يوصى بها (المجلات العلمية، التقارير.... )** | • Diffie: Whitfield Diffie and Martin Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Nov 1976 |
| **المراجع الإلكترونية ، مواقع الانترنيت** | • H. Boker & F. Piper, " Cipher System, The Protection of Communications ", Northwood Books, Landon, 1982. |