# المدخل الى

# خوارزميات التشفير

إعداد الدكتور

إبراهيم محمد جمال سرحان

الطبعة الأولى

2024م

دار الحامد

# المحتويات




| الموضوع | الصفحة |
|---|---|
| مقدمة الكتاب..... | 11 |
| **الفصل الأول** | |
| **الشفرات الكلاسيكية والتطور التاريخي** | |
| 1-1 مقدمة..... | 15 |
| 1-2 شفرات الانتقال..... | 15 |
| 1-3 شفرات الإحلال..... | 17 |
| 1-4 الإحلال أحادي الأحرف..... | 17 |
| 1-5 الإحلال متعدد الأحرف..... | 22 |
| 1-6 الرموز وما يقابلها من الشفرات..... | 23 |
| 1-7 الإحلالات متعددة الأحرف وشفرات فايجنر..... | 24 |
| 1-8 تحليل شفرة للشفرات الكلاسيكية (نظرة تاريخية)..... | 27 |
| 1-9 طريقة كاسيكي..... | 30 |
| 1-10 فهرس التطابق..... | 32 |
| **الفصل الثاني** | |
| **خوارزميات شفرات التدفق** | |
| 2-1 مقدمة..... | 37 |
| 2-2 التصنيف..... | 37 |
| 2-3 شفرة الوسادة..... | 39 |
| 2-4 شفرات التدفق المتزامنة..... | 42 |
| 2-5 طور ناتج التغذية الخلفية..... | 42 |

2-6 خصائص شفرات التدفق المتزامنة..... 43
2-7 شفرات التدفق المتزامنة ذاتياً..... 45
2-8 خصائص شفرات التدفق المتزامنة ذاتياً..... 46
2-9 مسجلات الإزاحة ذات التغذية الخلفية..... 47
2-10 مسجلات الإزاحة ذات التغذية الخلفية الخطية..... 47

**الفصل الثالث**

**شفرات الكتل**

3-1 مقدمة..... 51
3-2 شفرات الكتل..... 51
3-3 الأمنية العملية وتعقيد الهجومات..... 57
3-4 هجوم النص المشفر المختار وهجوم المفتاح المتصل..... 58
3-5 المعايير المطلوبة لتقييم شفرات الكتل وطور العملية..... 59

**الفصل الرابع**

**خوارزميات تشفير الكتل**

4-1 أساليب العمليات..... 63
4-2 خصائص طور كتاب الترميز الإلكتروني..... 64
4-3 ملاحظات عن كتاب الترميز الإلكتروني..... 65
4-4 خصائص طور عمليات CBC..... 69
4-5 ملاحظات عن CBC..... 70
4-6 ملاحظات عن CFB..... 72
4-7 طور تسلسل الكتلة..... 73
4-8 بحث المفتاح المكثف وعمليات التشفير المتعددة..... 75

4-9 دمج شفرات الكتل..... 77
4-10 تعاقب الشفرات وعمليات التشفير المتعددة..... 77
4-11 دمج عدة خوارزميات كتل..... 79
4-12 مضاعفة طول الكتلة..... 83
4-13 البياض..... 83
4-14 الهجومات على التشفير المتعدد..... 84

## الفصل الخامس

## خوارزمية تشفير البيانات القياسية

5-1 مقدمة..... 87
5-2 طريقة التشفير الدي أي اس DES..... 90
5-3 خصائص الـ دي أي اس ونقاط القوة فيها..... 99
5-4 توليد وإدارة مفتاح الشفرة..... 105
5-5 قوة الـ دي أي اس..... 106
5-6 أطوار عمليات الـ دي أي اس..... 108
5-7 أمنية الـ دي أي اس..... 110
5-8 الاستخدام المادي والبرمجي للـ دي أي اس..... 113

## الفصل السادس

## مقدمة عن المفتاح العام

6-1 مقدمة..... 117
6-2 مبادئ أساسية..... 121
6-3 تبادل المفتاح باستخدام التشفير التناظري..... 122
6-4 تبادل المتفاح بدون تبادل المفاتيح..... 124

6-5 توزيع المفاتيح العامة..... 124
6-6 تكتل العبارة..... 125

## الفصل السابع

## خوارزميات المفتاح العام: طريقة أر أس أي

7-1 تشفير المفتاح العام RSA..... 129
7-2 أمنية الـ أر أس إيه..... 132
7-3 تشفير الـ أر أس إيه في الواقع العملي..... 140
7-4 توليد الأعداد الأولية..... 144
7-5 الـ أر أس إيه في الكيان المادي..... 145
7-6 سرعة الـ أر أس إيه..... 145
7-7 الأمنية وما يقابلها من إثبات الشخصية..... 147

## الفصل الثامن

## خوارزميات المتفاح العام: الطرق المحددة الأخرى

8-1 طريقة Hellman–Pohlig ..... 151
8-2 طريقة تشفير رابين..... 151
8-3 استعمال الحشو..... 155
8-4 تشفير المفتاح العام..... 158
8-5 طريقة تشفير EIGamal الأساسية..... 158
8-6 ملخص لطريقة EIGamal..... 159
8-7 تواقيع EIGamal..... 160
8-8 سرعة EIGamal..... 165
8-9 طريقة تشفير EIGamal العامة..... 165

8-10 طريقة تشفير McEliece ..... 167
8-11 تشفير McEliece في الواقع العملي ..... 171
8-12 طريقة تشفير حقيبة الظهر ..... 171
8-13 طريقة تشفير حقيبة الظهر Merkle – Hellman ..... 173

## الفصل التاسع

## خوارزميات المفتاح العام: الطرق الاحتمالية

9-1 طرق تشفير المتفاح العام المحتملة ..... 179
9-2 أمنية خوارزميات المتفاح العام ..... 181
9-3 طريقة التشفير المحتملة ..... 182
9-4 طريقة تشفير Micali – Goldwasser ..... 183
9-5 طريقة تشفير Blum - Goldwasser المحتملة ..... 184
9-6 تشفير النص الواضح الواعي ..... 190
9-7 الانتقادات الموجهة لشفرة المفتاح العام ..... 191
المصادر ..... 193

## مقدمة الكتاب

في هذا الكتاب يتم وصف خوارزميات التشفير بشئ من التفصيل.

في الفصل الاول يتم وصف الشفرات الكلاسيكية بغرض تعريف القارئ بالتطورات التاريخية في هذا المجال ولربما يتم استخدامها لبعض الاغراض التامينية الخاصة. في الفصل الثاني تم وصف خوارزميات شفرات التدفق وهي من الشفرات الهامة في تامين البيانات الحساسة والمحوسبة. اما الفصل الثالث والرابع كانا عن شفرات الكتل كمقدمة عن شفرت البيانات القياسية (DES ) التي تم تقديمها بتفصيل في الفصل الخامس. اما الفصل السادس فكان عن المفاتيح العامة عموما ليتم وصف طريقة ار اس ايه ( RSA ) المشهورة في الفصل السابع ثم طرق التشفير الاخرى مثل طريقة الجمال في الفصل الثامن. ختاما في الفصل التاسع فقد تم تقديم طرق التشفير الاحتمالية وهي من الطرق التي بدات تتطور مع تطور تقانة الحاسوب.