

CDD 005.82

368

ثع



069215

(3)



أمن المعلومات والتشفير

إعداد

ابراهيم محمد جمال سرحان

الطبعة الأولى

2024





المحتويات

الصفحة	الموضوع
13	المقدمة.....
الفصل الأول	
التعريف بتقنيات التشفير وأمنية المعلومات	
17	1. 1: المقدمة.....
21	1. 2: نبذة تاريخية مختصرة عن الاتصالات السرية.....
22	1. 3: أمنية نظم المعلومات.....
23	1. 4: تحليل العوامل المهددة لامن الانظمة الالية للمعلومات....
26	1. 5: المتطلبات الفنية لامن النظم الالية للمعلومات.....
29	1. 6: المتطلبات الادارية لامن النظم الالية للمعلومات.....
32	1. 7: الخلاصة.....
33	1. 8: أمنية المعلومات والتشفير.....
39	1. 9: تعريف: التشفير.....
41	1. 10: أهداف التشفير.....
45	1. 11: مصطلحات فنية وأفكار أساسية.....
46	1. 12: التحويلات التشفيرية.....
48	1. 13: المبادئ العملية الاساسية في نظام التشفير المستخدم في الجيوش.....
49	1. 14: تحليل الشفرة.....
53	1. 15: أمنية الخوارزميات.....

- 55 16.1: شفرة الوسادة الكاملة
- 56 17.1: أفكار رياضية

الفصل الثاني

أمنية وحماية المعلومات

- 63 2.1: عوامل تعريف قيمة الانظمة
- 74 2.2: ملخص عن الامنية الكاملة
- 75 2.3: انظمة التشفير العشوائية
- 76 2.4: الوصول الى الوثوقية
- 77 2.5: المشتركين في الاتصال
- 78 2.6: القنوات
- 79 2.7: الأمنية
- 83 2.8: شرط الحالة الأسوأ
- 84 2.9: أمنية المعلومات بشكل عام
- 85 2.10: مستقبل التشفير
- 87 2.10.1: الانسياق باتجاه التشفير المفوض حكومياً
- 88 2.10.2: ظهور عهد تنفيذ المفتاح
- 89 2.10.3: البدائل لمفتاح التعهد

الفصل الثالث

مقدمة في التشفير

- 93 3.1: التشفير
- 93 3.2: تشفير المفتاح التناظري
- 95 3.3: نظرة سريعة عن شفرات التدفق والكتل

- 97 4.3: تعريف شفرة الكتل
- 98 5.3: شفرات الاحلال وشفرات الانتقال
- 99 1.5.3: الاحلال
- 100 2.5.3: شفرات الاحلال البسيط
- 102 3.5.3: أنواع شفرات الإحلال
- 104 4.5.3: الشفرات الجمعية
- 105 5.5.3: احلال
- 109 6.5.3: شفرات الإحلال متعدد الأحرف
- 111 7.5.3: شفرة المفتاح الذاتي
- 112 8.5.3: طريقة سريعة لتحليل شفرات الإحلال
- 113 9.5.3: تحويرات لشفرات الإحلال
- 114 6.3: شفرات الانتقال
- 115 1.6.3: عمليات XOR البسيطة
- 116 7.3: تركيب التشفير
- 117 1.7.3: المجموع الموزون
- 118 2.7.3: تركيب الدوال
- 118 3.7.3: التركيب والالتفاف
- 120 8.3: شفرة الضرب
- 126 9.3: شفرات التدفق
- 132 1.9.3: شفرات التدفق ذاتية التزامن
- 132 2.9.3: شفرات التدفق التزامنية
- 133 3.9.3: هجوم الادخال

- 134 3. 9. 4: شفرة فيرنام.
- 136 3. 10: مساحة المفتاح.

الفصل الرابع

تقنيات التشفير

- 139 4. 1: التوقيعات الرقمية.
- 140 4. 1. 1: اجراء التوقيع.
- 140 4. 1. 2: اجراء التحقق.
- 142 4. 1. 3: الخصائص المطلوبة لدوال التوقيع والتحقق.
- 142 4. 2: اثبات الشخصية والتعرف.
- 144 4. 2. 1: التعريف.
- 145 4. 2. 2: وثوقية مصدر البيانات.
- 146 4. 3: تشفير المفتاح العام.
- 149 4. 3. 1: ضرورة تامين الوثوقية في انظمة المفتاح العام.
- 149 4. 3. 2: التوقيعات الرقمية من تشفير المفتاح العام العكسي.
- 151 4. 3. 3: بناء طريقة التوقيع الرقمي.
- 152 4. 3. 4: التوقيعات الرقمية في الواقع العملي.
- 152 4. 3. 5: حل النزاعات.
- 153 4. 3. 6: المتطلبات الضرورية لحل التوقيعات المتنازع عليها.
- 153 4. 4: انظمة التشفير التناظرية ومايقابلها من المفتاح العام.
- 157 4. 4. 1: ملخص للمقارنة بين انظمة المفتاح العام وانظمة التشفير التناظرية.
- 159 4. 5: ضغط البيانات، الترميز، والتشفير.

- 159 4 .6: الدوال الهاشية
- 163 4 .7: مقدمة الى البروتوكولات
- 164 4 .7 .1: البروتوكولات والميكانيكيات
- 165 4 .7 .2: مولدات الارقام العشوائية
- 168 4 .7 .3: قصور البروتوكول او الميكانيكية
- 169 4 .7.4: الهجمات ضد البروتوكولات
- 172 4 .8: انشاء المفتاح، الادارة، التصديق
- 174 4 .9: ادارة المفتاح بواسطة تقنيات المفتاح التناظري
- 176 4 .9 .1: فوائد هذا الاسلوب (الاقتراح)
- 176 4 .9 .2: مساوئ هذا الاقتراح
- 177 4 .9 .3: فوائد هذه الطريقة (الاقتراح)
- 178 4 .9 .4: الطرف الثالث الموثوق وشهادات المفتاح العام
- 179 4 .9 .5: الشهادات المتحققة بواسطة المفتاح العام

الفصل الخامس

استخدامات السلاسل العشوائية في التشفير

- 183 5 .1: توليد السلاسل العشوائية والعشوائية الوهمية
- 183 5 .1 .1: الارقام العشوائية الوهمية والسلاسل المتعاقبة
- 186 5 .2: اصناف الهجمات
- 187 5 .2 .1: الهجمات على طرق التشفير
- 191 5 .2 .2: الهجمات على البروتوكولات
- 192 5 .3: نماذج تخمين الامنية
- 193 5 .3 .1: وجهة نظر عن الامنية الحاسوبية

- 193 5. 3. 2: تعريف عامل الاداء.
- 194 5. 3. 3: تعريف عامل الاداء التاريخي.
- 194 5. 3. 4: ماهو حجم المفتاح المطلوب.
- 195 5. 3. 5: طول المفتاح التناظري.
- 197 5. 3. 6: تخمينات الوقت والكلفة لهجوم القوة الوحشية
- 201 5. 3. 7: طول المفتاح العام
- 202 5. 3. 8: مقارنة بين طول المفتاح التناظري والعام
- 203 5. 4: هجوم القوة الوحشية ضد الدوال الهاشية
- 204 5. 5: البتات العشوائية الوهمية والتسلسلات
- 208 5. 5. 1: عمومية اختيار البت القادم
- 209 5. 5. 2: المولدات المعتمدة على البرمجيات
- 209 5. 5. 3: توليد البت العشوائي الوهمي
- 210 5. 5. 4: الاختبارات الاحصائية

الفصل السادس

ثغرات التشفير وآليات معالجتها

- 213 6. 1: ثغرات التشفير وأمنية المعلومات.
- 213 6. 1. 1: مقدمة.
- 214 6. 1. 2: اهداف أمنية المعلومات.
- 215 6. 1. 3: أهداف أنظمة التشفير.
- 216 6. 1. 4: أمنية أنظمة التشفير.
- 217 6. 1. 5: المفاتيح الضعيفة.
- 218 6. 1. 6: معايير قوة الشفرة.

219 6. 1. 7: النظام التشفيري ذو الأمانة التامة.....
220 6. 1. 8: الحشو والإنتظار والتشويش.....
220 6. 1. 9: التشفير وتحليل الشفرة.....
221 6. 1. 10: ثغرات أنظمة التشفير.....
225 6. 2: آلية تقوية البيانات الحسائية.....
225 6. 2. 1: مقدمة.....
226 6. 2. 2: محاذير هامة في حماية البيانات الحسائية.....
227 6. 2. 3: استخدام آلية تبديل الطرق التشفيرية لتقوية أمانة البيانات
230 6. 2. 4: آلية آلية تعدد مستويات التحويل.....
232 6. 2. 5: آلية دمج التشفير مع الترميز.....
234 6. 2. 6: آلية إخفاء المفتاح العام في آر. أس. أية.....
236 6. 2. 7: إيجاد طريقة لتغيير الجداول الثابتة في دي. أي. أس الى جداول متغيرة.....
238 6. 2. 8: مقترحات أخرى لتأمين حماية البيانات.....
241 ملحق (1): أمثلة متنوعة عن طرق التشفير.....
274 ملحق (2): الاشكال الانسيابية للبرامج.....
284 ملحق (3): البرامج.....
359 المصادر.....