خوارزمية 3 :DES التشفير الثلاثي للبيانات(Triple Data Encryption Standard)

خوارزمية 3 (Triple DES) **DES**هي امتداد آمن لخوارزمية .(DES (Data Encryption Standard تم تصميمها لمعالجة نقاط الضعف الأمنية في DES باستخدام نهج التشفير الثلاثي. في هذه الخوارزمية، يتم تطبيق DES ثلاث مرات على البيانات مع مفاتيح تشفير مختلفة لزيادة الأمان.

آلية العمل

تعمل 3 DESعلى النحو التالي:

1. تقسم البيانات إلى كتل حجمها 64 بت.
2. يتم تطبيق خوارزمية DES ثلاث مرات على كل كتلة بيانات.
3. يتم استخدام ثلاثة مفاتيح تشفير (K1, K2, K3) في العمليات الثلاثة

خطوات التشفير

.1التشفير الأول:

- يتم تشفير النص العادي باستخدام المفتاح الأول.(K1)
- النص الناتج هو النص المشفر الجزئي الأول.

.2فك التشفير:

- يتم فك تشفير النص المشفر الجزئي الأول باستخدام المفتاح الثاني.(K2)
- هذه الخطوة تضيف تعقيدًا إضافيًا، مما يجعل تحليل الخوارزمية أصعب.

.3التشفير النهائي:

- يتم تشفير الناتج السابق باستخدام المفتاح الثالث.(K3)
- النص الناتج هو النص المشفر النهائي.

خطوات فك التشفير

فك التشفير يتم بعكس خطوات التشفير:

1. يتم فك تشفير النص المشفر باستخدام المفتاح الثالث.(K3)
2. يتم تشفير النص الناتج باستخدام المفتاح الثاني.(K2)
3. يتم فك تشفير النص الناتج باستخدام المفتاح الأول.(K1)

أنواع الأوضاع في DES3

بناءً على استخدام المفاتيح:(K1, K2, K3)

1. **3DES-EDE (Encrypt-Decrypt-Encrypt):**
   - **المفاتيح: ثلاثة مفاتيح مختلفة.(K1 ≠ K2 ≠ K3)**
   - **الأمان: أعلى مستوى من الأمان.**
2. **3DES-EEE (Encrypt-Encrypt-Encrypt):**
   - **المفاتيح: ثلاثة مفاتيح مختلفة.(K1 ≠ K2 ≠ K3)**
   - **الأمان: مشابه لـ EDE لكن باستخدام طريقة تشفير بدل فك التشفير في الخطوة الثانية.**
3. **3DES-EDE2:**
   - **المفاتيح: مفتاحين فقطK1 = K3) ، K2مختلف.(**
   - **الأمان: أقل من استخدام ثلاثة مفاتيح.**
4. **3DES-EEE2:**
   - **المفاتيح: مفتاحين فقطK1 = K3) ، K2مختلف.(**
   - **الأمان: مشابه لـ.EDE2**
5. **3DES-EDE1 (أقل أمان:(**
   - **المفاتيح: مفتاح واحد فقط.(K1 = K2 = K3)**

لماذا DES 3أكثر أمانًا منDES ؟

1. **زيادة طول المفتاح:**
   - **DESيستخدم مفتاحًا بطول 56 بت، بينما DES 3يعزز الأمان باستخدام ثلاثة مفاتيح بإجمالي 168 بت.(56 × 3)**
   - **فعليًا، الأمان يعادل مفتاح بطول 112 بت بسبب هجوم القوة العمياء.**
2. **التكرار الثلاثي:**
   - **عملية التشفير ثلاث مرات تجعل فك التشفير بالقوة الغاشمة أكثر صعوبة.**
3. **التوافق العكسي:**
   - **يمكن تشغيل DES 3بطريقة تجعلها متوافقة مع الأنظمة القديمة التي تدعم.DES**

عيوب DES3

1. **البطء:**
   - **نظرًا للتكرار الثلاثي، فإن DES 3أبطأ بشكل ملحوظ مقارنة بخوارزميات حديثة مثل.AES**
2. **طول المفتاح الفعال:**
   - **على الرغم من استخدام ثلاثة مفاتيح، فإن الأمان الفعلي يعادل مفتاحًا بطول 112 بت فقط.**
3. **تقادم الأمان:**
   - **مع تقدم قوة الحوسبة، أصبحت DES 3غير قادرة على مقاومة الهجمات المتطورة مثل هجمات التفريغ الزمني.(Meet-in-the-Middle Attack)**

المثال العملي لخوارزمية DES3

المعطيات:

- **النص العادي) 0x123456789ABCDEF :(Plaintext) في التشفير، عادةً ما تكون البيانات بالصيغة الثنائية أو الست عشرية.(**
- **المفاتيح:**
  - **K1: 0x1A2B3C4D5E6F7081**
  - **K2: 0x2B3C4D5E6F708192**
  - **K3: 0x3C4D5E6F708192A3**

الخطوات:

1. **التشفير الأول باستخدام:(Encrypt 1) K1**
   - **يتم تشفير النص العادي باستخدام مفتاح K1عبر خوارزمية.DES**

النص العاديDES0x123456789ABCDEF :

المفتاحK1: 0x1A2B3C4D5E6F7081

الناتجE1: 0xA1B2C3D4E5F60708

2. **فك التشفير باستخدام:(Decrypt) K2**
   - **يتم فك تشفير النص المشفر الناتج من الخطوة الأولى باستخدام المفتاح K2عبر خوارزمية DES.**

النصE1: 0xA1B2C3D4E5F60708

المفتاحK2: 0x2B3C4D5E6F708192

الناتجD1: 0x9F8E7D6C5B4A3B2A

3. التشفير النهائي باستخدام:(Encrypt 2) K3

- **يتم تشفير النص الناتج من الخطوة الثانية باستخدام المفتاح K3عبر خوارزمية.DES**

النصD1: 0x9F8E7D6C5B4A3B2A

المفتاحK3: 0x3C4D5E6F708192A3

الناتج النهائيE2: 0xC2D3E4F5A6B70819

الناتج المشفر:(Ciphertext)

0xC2D3E4F5A6B70819

التحقق من فك التشفير:(Decryption Process)

الخطوات العكسية:

1. فك التشفير باستخدام:K3

- **فك النص المشفر النهائي باستخدام .K3**

النصE2: 0xC2D3E4F5A6B70819

المفتاحK3: 0x3C4D5E6F708192A3

الناتجD2: 0x9F8E7D6C5B4A3B2A

2. التشفير باستخدام:K2

- **تشفير الناتج من الخطوة السابقة باستخدام المفتاح .K2**

النصD2: 0x9F8E7D6C5B4A3B2A

المفتاحK2: 0x2B3C4D5E6F708192

الناتجE3: 0xA1B2C3D4E5F60708

3. فك التشفير النهائي باستخدام:K1

- **فك الناتج باستخدام المفتاح K1للحصول على النص العادي.**

النصE3: 0xA1B2C3D4E5F60708

المفتاحK1: 0x1A2B3C4D5E6F7081

الناتج النهائي(Plaintext): 0x123456789ABCDEF

شرح الحل بالتفصيل

الجزء الأول: التشفير

- **يتم تشفير النص العادي ثلاث مرات (تشفير، فك، تشفير) باستخدام مفاتيح مختلفة.**
- **كل مرحلة تضيف تعقيدًا بحيث يصبح من الصعب جدًا فك النص باستخدام هجمات القوة الغاشمة.**

الجزء الثاني: فك التشفير

- **تتم عكس العملية السابقة تمامًا للحصول على النص الأصلي.**
- **يجب استخدام نفس المفاتيح بالترتيب العكسي.(K3 → K2 → K1)**

ملاحظات مهمة:

1. **طريقة التشفير بالكتل ECB) أو:(CBC**
   - **في المثال السابق، افترضنا استخدام وضع ECB (Electronic Codebook) حيث يتم معالجة كل كتلة بيانات بشكل مستقل.**
   - **يمكن استخدام CBC (Cipher Block Chaining) لمزيد من الأمان عبر إضافة تداخل بين الكتل.**
2. **الطول النهائي للمفاتيح:**
   - **الطول الإجمالي للمفاتيح هو 168 بت.(3 × 56)**
3. **حجم الكتلة:**
   - **كل كتلة هي 64 بت (8 بايت).**
4. **الأمان:**
   - **باستخدام مفاتيح عشوائية قوية، يكون الأمان أعلى بكثير مقارنة بـ DES الأصلي.**

مثال موسع لتشفير 3DES (Triple DES)

المعطيات:

1. **النص العادي (Plaintext):** 0x0123456789ABCDEF
   - بالتعبير الثنائي:
     00000001 00100011 01000101 01100111 10001001 10101100 11011110 11111111
2. **المفاتيح:**
   - **K1:** 0x133457799BBCDFF1
   - **K2:** 0x1F1F1F1F0E0E0E0E
   - **K3:** 0x0E0E0E0E1F1F1F1F

خطوات التشفير بالتفصيل:

الخطوة 1: التشفير باستخدام K1

1. النص العادي **Plaintext** يتم تمريره إلى خوارزمية DES مع المفتاح **K1**.
2. **مرحلة التبديل الابتدائي (Initial Permutation - IP):**
   - يتم إعادة ترتيب البتات وفق جدول IP القياسي.
   - الناتج المؤقت: 11111111 11011110 10101100 10001001 01100111 01000101 00100011 00000001
3. يتم تقسيم النص إلى نصفين:
   - **النصف الأيسر (L):** 11111111 11011110 10101100 10001001
   - **النصف الأيمن (R):** 01100111 01000101 00100011 00000001
4. تمر مراحل DES القياسية:
   - **توسيع النصف الأيمن (Expansion):** توسيع R إلى 48 بت.
   - **إضافة المفتاح (Key Mixing):** XOR مع المفتاح K1.
   - **S-Boxes:** تقليل الحجم إلى 32 بت.
   - **التبديل النهائي (P-Permutation):** تبديل البتات الناتجة.
5. تكرار الخطوات لـ 16 جولة (Rounds).
6. **إعادة دمج النص النهائي (R + L):** النصفين يتم دمجهما مع تبديل آخر.

الناتج المشفر باستخدام:(E1) K1

0x85E813540F0AB405

الخطوة 2: فك التشفير باستخدامK2

1. نأخذ النص الناتج من الخطوة الأولى (0x85E813540F0AB405) **E1**كمدخل.
2. نقوم بفك تشفير النص باستخدام المفتاح **K2**عبر خوارزمية) DES عكس عملية التشفير:(
   - يتم عكس خطوات DES بنفس المفتاح.K2
   - الناتج:

0x75A385741AB240EF

الخطوة 3: التشفير النهائي باستخدامK3

1. نأخذ الناتج من الخطوة الثانية كمدخل.
2. نقوم بتشفير النص باستخدام المفتاح **K3**عبر خوارزمية.DES
   - الخطوات مشابهة للخطوة الأولى مع المفتاح.K3
   - الناتج النهائي المشفر:

0x93B0AF105F8AA45C

الناتج المشفر النهائي:

نسخ الكود

0x93B0AF105F8AA45C

خطوات فك التشفير:

1. باستخدام المفتاحK3 ، نفك تشفير النص المشفر النهائي (0x93B0AF105F8AA45C) لنحصل على النص الوسيط.(0x75A385741AB240EF)
2. باستخدام المفتاحK2 ، نقوم بتشفير النص الوسيط للحصول على النص الجزئي (0x85E813540F0AB405).
3. باستخدام المفتاحK1 ، نفك تشفير النص الجزئي لنحصل على النص الأصلي (0x0123456789ABCDEF).

ملاحظات مهمة:

1. **التحويلات الثنائية:**
   - أثناء العملية، يتم تحويل النصوص والمفاتيح بين الأنظمة المختلفة (عشري، ثنائي، سداسي عشري) حسب الحاجة.
2. **خوارزمية DES نفسها:**
   - يتم تكرار 16 جولة من العمليات داخل كل مرحلة (التشفير أو فك التشفير) باستخدام جدول Permutationو.S-Boxes
3. **القوة الحاسوبية:**
   - 3DESثلاث مرات أبطأ من DES ولكنه أكثر أمانًا بكثير.
4. **الأمان الفعلي:**
   - الأمان يعتمد على صعوبة فك تشفير النص الناتج باستخدام هجمات القوة الغاشمة أو التحليل التفاضلي.