إدارة شبكات الاتصال وأمنها

الوحدة الخامسة

أنظمة التشفير التقليدية

الاختراقات المحتملة Expected Attacks

1. الاطلاع على محتوى الرسالة
2. تعديل المحتوى
3. تأخير الرسالة
4. العبث بترتيب الرسائل
5. التنكر
6. إنكار المرسل
7. إنكار المستقبل
8. تحليل حركة المرور

وسائل حماية البيانات

- تشفير الرسائل Encryptionلإخفاء المحتوى
- التوقيع الرقمي Digital Signatureللتأكد من المصدر
- التأكد من سلامة البيانات Hashing
- إشغال شبكة الحاسوب بشكل منتظم

تشفير الرسائل

- تتطلب عملية التشفير وفك التشفير معلومات سرية متفق عليها مسبقاً تسمى المفتاح key

1. طرق التشفير التماثلية Symmetric Encryption تستخدم مفتاحاً واحداً للتشفير وفك التشفير يتبادله المرسل والمستقبل فتسمى أيضاً Secret Key Encryption
2. طرق التشفير غير التماثلية Asymmetric Encryption يستخدم المستقبل مفتاحاً خاصاً غير مفتاح المرسل العام .وتسمى الطريقة تشفير المفتاح العام Public Key

المشاكل المحلولة بالتشفير

- لا أحد غير مخول يستطيع الاطلاع على الرسالة المشفرة
- قد يستطيع المعتدي تغيير محتوى الرسالة عشوائيا ولكن من السهل اكتشاف التغيير
- يتضمن التشفير التاريخ والوقت فنستطيع كشف التأخير ما إذا تم ذلك
- عن طريق التاريخ والوقت)أو رقم تسلسلي (نستطيع معرفة ما إذا تم تغيير ترتيب الرسالة
- بطريقة التشفير المتماثل غالباً لا يستطيع المرسل أو المستقبل التنكر أو الإنكار، فالاثنين فقط لديهما نفس المفتاح السري.
- تظهر مشكلة المفتاح السري في كثرة المستخدمين في المراسلات

التوقيع الرقمي

- **يضع المرسل توقيعاً رقميا على الرسالة**
  - لا يستطيع المرسل انكار ارساله للرسالة
  - لا يستطيع أي مستخدم ارسال رسالة باسم آخر
- **يستخدم التوقيع الرقمي في التشفير غير التماثلي)المفتاح العام(**
  - يقوم المرسل بتشفير الرسالة باستخدام مفتاحه الخاص Private Key + المفتاح العام للمستقبل
  - يقوم المستقبل بفك التشفير باستخدام مفتاح المرسل العام +مفتاحه الخاص
- **يجب توزيع المفتاح العام بطريقة آمنة لكي لا يحصل عليه طرف معادي**
  - اذا استطاع الخصم تزوير المفتاح الخاص بالمرسل فسيقنع المستقبل أن التوقيع بالمفتاح العام صحيح

إشغال الشبكة بشكل دائم

- يتم إشغال الشبكة بشكل متعمد بإرسال رسائل وهمية
- يتم تحديد حجم معين للرسائل الحقيقية والوهمية
- قد يضاف إلى الرسائل الحقيقية نص عشوائي لتصل إلى الحجم المطلوب

مفاهيم أساسية Basic Concepts

- فك الشيفرة :استرجاع نص الرسالة الأصلي Plaintext باستخدام مفتاح التشفير الأصلي Encryption Keyفي فك الشيفرة Ciphertextمن قبل الشخص المخول
- كسر الشيفرة :استرجاع النص الأصلي بغير المفتاح الأصلي من قبل شخص غير مخول)خصم(
- أسلوبان لكسر الشيفرة:
  - أسلوب القوة الجبارة Brute Force Attack
  - أسلوب تحليل الشيفرة Cryptanalysis

أسلوب القوة الجبارة Brute Force Attack

- تجريب جميع القيم الممكنة للمفتاح حتى الحصول على نص الرسالة الأصلي)ذو معنى سليم(
- كلما زاد حجم)عدد خانات (المفتاح ازدادت القيم المحتملة للمفتاح فيزداد الجهد والوقت المطلوب)جدول 1ص (157
- شرطان يجب توفرهما للتمكن من تطبيق استخدام القوة الجبارة
  - أن تكون لغة النص الأصلي مفهومة من قبل الخصم
  - سهولة التأكد من أن النص الأصلي ذو معنى سليم وذلك باستخدام أدوات مناسبة)مثل القاموس للغات الطبيعية(
- **عملية تجربة قيمة واحدة للمفتاح =فك تشفير الرسالة باستخدام تلك القيمة +التأكد من أن لها معنى سليم**

أسلوب تحليل الشيفرة Cryptanalysis

- **هو استغلال نقاط الضعف في خوارزمية التشفير في محاولة**
  - تحديد مفتاح التشفير أو
  - معرفة نص الرسالة الأصلية
- **خوارزميات التشفير الحديثة على شكل**
  - رقاقات إلكترونية Integrated Circuitsأو
  - برامج حاسوبية
- يجب الأخذ بعين الاعتبار أن معرفة تفاصيل أو طريقة عملية التشفير من قبل الخصم ليست صعبة، أو أنه يعرفها مسبقاً
- تصنف طرق تحليل الشيفرة بناء على المعلومات المتوفرة للمحلل

طرق تحليل الشيفرة

- **الحصول على النص المشفر فقط**
  - حصول الخصم على النص المشفر إضافة لمعرفته لخوارزمية التشفير
- **طريقة النص الأصلي المعروف**
  - معرفة الخصم لكلمات مشفرة ومقابلها بالنص الأصلي)حتى لو كانت قليلة(
- **طريقة النص الأصلي المختار**
  - أن يرسل الخصم كلمات معروفة لشخص ويجعله يعيد إرسالها إليه مشفرة
- ينصح بتغيير مفتاح التشفير والخوارزمية كل فترة

السرية التامة

- تعتبر السرية تامة إذا كان كل ما يستطيع المحلل عمله هو تخمين محتوى النص المشفر
- الخطورة تكمن هنا إذا كان عدد الرسائل قليل وحجمها صغير فيستطيع الخصم تخمين محتوى الرسالة بدلاً من كسر الشيفرة
- بعض الأحيان)حسب نقاط الضعف في آلية التشفير (يستطيع محلل الشيفرة أن يكسرة الشيفرة دون التخمين

السرية التامة

- **تصنف طرق التشفير من حيث قدرتها على توفير الأمن**
  - خوارزميات آمنة دون شروط Unconditionally Secure
    - لا يحتوي النص المشفر على أية معلومات مساعدة في فك التشفير
  - الخوارزميات الآمنة حسابياً Computationally Secure
    - يمكن كسر الشيفرة ولكن بإحدى حالتين أو كلاهما
      - تكلفة كسر الشيفرة كبيرة جداً تفوق قيمة البيانات نفسها
      - الوقت اللازم لكسر الشيفرة كبير جداً حيث لا تكون مفيدة بعد انقضاء ذلك الوقت

تصنيفات أنظمة التشفير

- **الخصائص التي تبنى عليها تصنيفات أنظمة التشفير**
  - **عدد المفاتيح المستخدمة**
    - تماثلية Synchronousتستخدم مفتاح واحد
    - غير تماثلية Asynchronousتستخدم مفتاحين
  - **العملية المستخدمة في التشفير**
    - تشفير بالتعويض Substitutionتغيير الأحرف
    - أنظمة ترتيبية Transpositionتغيير ترتيب الأحرف
    - أنظمة خليطة
  - **حجم النص المشفر**
    - كتلية :تشفر مجموعة من النص دفعة واحدة
    - جدولية :تشفير مستمر لنص مستمر)التشفير حرف حرف أو بت بت(

طرق تشفير تقليدية

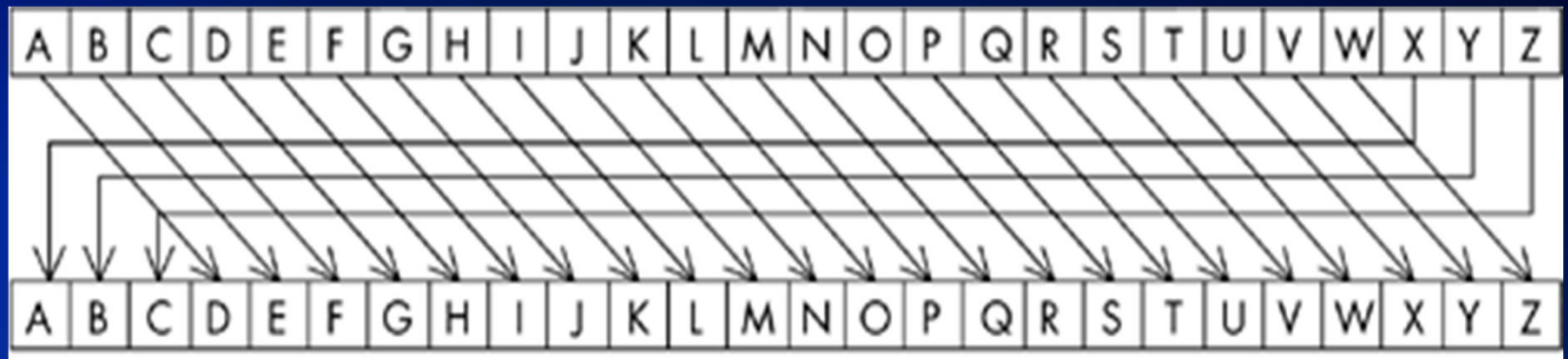
شيفرة قيصر Caesar Ciphers

- أبسط طرق التشفير التعويضية Substitution Cipher
- تعمل على استبدال الحرف المرتب بحرف آخر يليه أو يسبقه بمقدار قيمة المفتاح . k
- يتم تشفير Encrypt كامل النص الأصلي Plaintext إلى نص مشفر Ciphertext وفقاً للمعادلة

$$C_i = E(P_i) = (P_i + k) \bmod 26$$

- حيث أن Ci و Pi هي أرقام تمثل ترتيب الأحرف أبجدياً
- (mod 26) لاستخراج باقي القسمة الذي يضمن النتيجة من 0- 25 بحسب عدد حروف اللغة الإنجليزية

Caesar Ciphers شيفرة قيصر




```
Key:
  3

Plaintext:
  P = HELLO CAESAR CIPHER

Ciphertext:
  C = KHOOR FDHVDU FLSKHU
```

التشفير أحادي الأبجدية
Monoalphabetic Cipher

- أحد طرق التشفير التعويضية Substitution Cipher
- المفتاح عبارة عن مصفوفة الحروف الأبجدية غير المرتبة .أي
- يتم تشكيل !26مفتاحاً مختلفاً .ليقوم الخصم بتجريبها
- نقطة ضعفها في عملية التحليل للتكرار النسبي للأحرف
  - الجدول ص 169

التشفير متعدد الأحرف والتشفير متعدد الأبجدية

- **التشفير متعدد الأحرف:**
  - تشفير مجموعة 2) أو أكثر (من الأحرف معاً وتكون معتمدة على بعضها .ويختلف تشفير الحرف الواحد حسب ظهوره بين أحرف مختلفة
  - تقضي على نقطة الضعف في التمثيل النسبي للأحرف
- **التشفير متعدد الأبجدية:**
  - يستخدم أكثر من مفتاح واحد للتشفير
  - يختلف تشفير الحرف في كل ظهور عن التشفير السابق

شيفرة هل Hill Cipher

- أحد طرق التشفير متعدد الأحرف
- تسمح بتشفير أي عدد من الأحرف معاً)مقطع(
  - كلما زاد عدد الأحرف في المقطع كان النص المشفر أكثر أماناً
  - تشفير أربعة حروف كفيل بإخفاء التكرار النسبي للأحرف والتراكيب
- طريقة التشفير
  - يقسم النص الأصلي إلى مقاطع بطول معين (n)
  - توضع قيم ترتيب حروف المقطع في مصفوفة Pبعد واحد n X 1
  - يتم تشكيل مصفوفة المفتاح kببعدين n X n

شيفرة هل Hill Cipher

- طريقة التشفير ...تابع
  - تضرب مصفوفة المفتاح Kفي مصفوفة النص الأصلي Pلتنتج مصفوفة Cمكونة من قيم ترتيب أحرف النص المشفر

$$C = (K * P) \bmod 26$$

$$Ci = (K_{i,1} * P_1 + K_{i,2} * P_2 + ... + K_{i,n} * P_n) \bmod 26$$

- طريقة فك التشفير
  - يضرب معكوس المصفوفة Kفي المصفوفة المشفرة C

$$P = (K^{-1} * C) \bmod 26$$

شيفرة فيجينير Vigenere Cipher

- أحد طرق التشفير متعدد الأبجدية
- تستخدم بعض أو جميع مفاتيح شيفرة قيصر)حسب أحرف كلمة المفتاح(
- نقطة ضعفها أنها لا تخفي جميع تراكيب النص الأصلي
  - اذا عرف حجم المفتاح nفإن الأحرف 0, n, 2n...قد تم تشفيرها بنفس المفتاح
  - مثال ص 178

Vigenere Cipher شيفرة فيجينير

KEY \ PLAINTEXT	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

شيفرة فيجينير Vigenere Cipher

- **طريقة التشفير**
  - يتم تعيين مصفوفة المفتاح Kبطول (n)مكونة من قيم ترتيب حروف كلمة المفتاح
  - يقسم النص الأصلي إلى مقاطع بنفس طول كلمة المفتاح
  - في المقطع الواحد :يتم تبديل الحرف بحرف آخر +إزاحته بقيمة الحرف المقابل في كلمة المفتاح
  - تتكرر العملية بمقدار nحتى نهاية النص
- **طريقة فك التشفير**
  - يتم تبديل الحرف بحرف آخر -إزاحته بقيمة الحرف المقابل في كلمة المفتاح

شيفرة ون تايم باد One-Time Pad

- شيفرة آمنة بدون شروط Unconditionally Secure، لا يحتوي معلومات كافية لكشف النص الأصلي فيحقق السرية التامة.
- تعديل على شيفرة فيجينير بحيث أن كلمة المفتاح هي نص عشوائي بطول النص الأصلي.
- هناك صعوبة في توزيع المفتاح نظراً لطول المفتاح والحاجة إلى تغييره كل مرة

طرق التشفير الترتيبية Transposition Cipher

- تعتمد على إعادة ترتيب أحرف النص الأصلي
- بعكس طرق التشفير التعويضية التي يتم فيها تغيير الأحرف
- يتم تشكيل مصفوفة ذات بعدين يتم تحديد المفتاح بعدد الأعمدة n، أما الصفوف فيتم ملئها تتابعاً حتى انتهاء النص
- ثم يتم تفريغ أحرف الأعمدة واحداً تلو الآخر لنحصل على النص المشفر
- نقطة ضعف بأن مفتاح التشفير هو عدد أعمدة المصفوفة، وهو أحد قواسم طول النص

طرق التشفير الخليطة

- عمليتي تشفير معاً :تعويض +ترتيب

إدارة شبكات الاتصال وأمنها

الوحدة السادسة

التشفير المتماثل وخوارزمية دِس

Symmetric Encryption & DES Algorithm

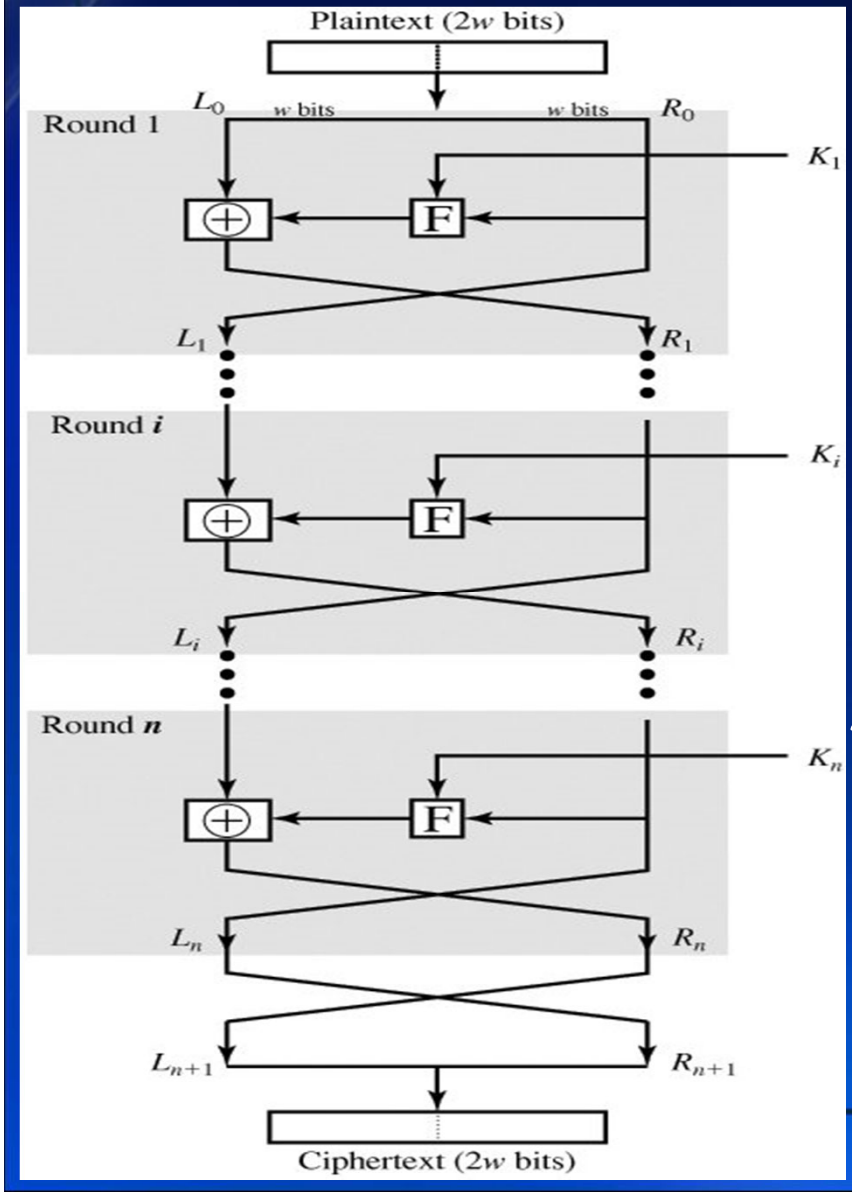
مقدمة Introduction

- شيفرة هِل تشفر nمن الأحرف معاً
  - نقطة القوة :كلما كبرت قيمة nيتم إخفاء التكرارات النسبية
  - نقطة الضعف :العلاقة الخطية البسيطة بين المفتاح والنص المشفر
    - إذا عرف الخصم مجموعة من النصوص الأصلية وتشفيرها يسهل حساب قيمة المفتاح)هجوم النص المعروف(
    - المفتاحين المتشابهين سينتجان نصين مشفرين متشابهين)هجوم القوة الجبارة ستأخذ وقتاً أقل
- صممت العديد من خوارزميات التماثل الحديثة تطويراً لشيفرة هِل
  - عززت نقاط القوة وتجنبت نقاط الضعف

Shannon's Proposal اقتراح شانون

- اقترح العالم شانون صفتين للشيفرة الجديدة :التشتت والتشويش
  - هجوم النص المعروف Known Plaintext Attackيصبح في غاية الصعوبة
- التشتت :Diffusion
  - تبعثر التكرارات والأنماط الإحصائية -عدد كبير من أحرف النص الأصلي معاً تحدد حرف واحد من النص المشفر
  - أي اختلاف بسيط في النص الأصلي ينتج إختلاف كبير في النص المشفر
- التشويش :Confusion
  - جعل العلاقة بين النص المشفر والمفتاح علاقة معقدة غير خطية

شبكات فيستل Feistel Networks



شيفرة كتلية)تشفر كتلة بعد كتلة(

- طريقة تحقق التشتت والتشويش
- تكرر عدد من جولات التشفير
- كل جولة تستخدم عمليتي التعويض وإعادة الترتيب
- كل جولة تعمل بالدالة التالية إضافة إلى تبديل النصف الأيسر الجديد بالنصف الأيمن
- $f_k [L_i, R_i] = (F(R_i) \oplus L_i , R_i)$

العوامل المؤثرة على مستوى الأمان في شبكات فيستل

- **الدالة F وما تقوم به من عمليات**
- **حجم المفتاح :كلما كان أكبر كلما استطعنا تعقيد العلاقة لضمان التشويش**
- **حجم الكتلة من النص الأصلي :زيادة عدد خانات النص الأصلي التي تحدد خانة واحدة مشفرة لضمان التشتت**
- **عدد الجولات :**
  - عدد جولات أكثر = المزيد من التشتت والتشويش
  - عدد جولات أكثر = وقت أطول في التشفير وفك التشفير
- **المفاتيح الفرعية وكيفية الحصول عليها :كل جولة تحتاج إلى مفتاح فرعي مختلف مشتق عن المفتاح الريسي وأصغر منه حجماً**
  - يتم توليد المفاتيح الفرعية عن طريق خوارزمية خاصة تعمل بمفتاح سري متفق عليه بين المرسل والمستقبل
  - كلما اختلفت المفاتيح الفرعية عن بعضها أكثر كلما زاد الأمان

خوارزمية فيستل لفك التشفير

- خوارزمية فيستل في فك التشفير هي نفسها في التشفير ولكن مع قلب ترتيب المفاتيح الفرعية

خوارزمية التشفير القياسية DES

- طورت خوارزمية DES من قبل فريق عمل بشركة IBM
- مطورة من خوارزمية Locifer منفذة لشيفرة فيستل
- من عيوبها : صغر حجم المفتاح نسبيا 56 bits مقارنة بمفتاح لوسيفير 128 btis
- تم تصغيرها لوضعها على IC ولم تكن التكنولوجيا في وقتها تسمح بأكثر من ذلك الحجم
- عرضة لهجوم القوة الجبارة

خوارزمية دِس المبسطة SDES

- طورت خوارزمية SDES من خوارزمية DES للأهداف التعليمية ولإيصال المفاهيم الرئيسية
- مكونة فقط من جولتي تشفير
- تستخدم مفتاح رئيسي بطول 10 bits يتم الاتفاق عليه مسبقاً بين المرسل والمستقبل
- تشفر كتلة بحجم 1 بايت = 8 bits
- لا تعتبر خوارزمية تشفير آمنة نظراً لصغر حجم المفتاح فيمكن كسره بالقوة الجبارة
- الرسمة ص207

Subkeys Generation تشكيل المفاتيح الفرعية

- تستخدم خوارزمية SDES مفتاح فرعي لكل مرحلة k1 و K2
- يتم اشتقاق كل من k1 و k2 بطول 8 Bits من المفتاح الرئيسي حسب الخطوات التالية: function $[k_1,k_2]$ = function_key(K)

1. اعادة ترتيب خانات المفتاح K حسب الدالة P10 أو Permuted Choice-1
   P10 = 3,5,2,7,4,10,1,9,8,6
2. تجزئة المفتاح إلى نصفين
3. عمل إزاحة دائرية لليسار بمقدار خانة واحدة على كل جزء
4. إعادة ترتيب الخانات حسب الدالة P8 أو Permuted Coice-2
   P8 = 6,3,7,4,8,5,10,9
5. بذلك نكون قد حصلنا على k_1
6. بالعودة إلى الخطوة 2 يتم عمل إزاحة دائرية لليسار بمقدار خانتين ثم تطبيق P8 لنحصل على k_2

Subkeys Generation تشكيل المفاتيح الفرعية

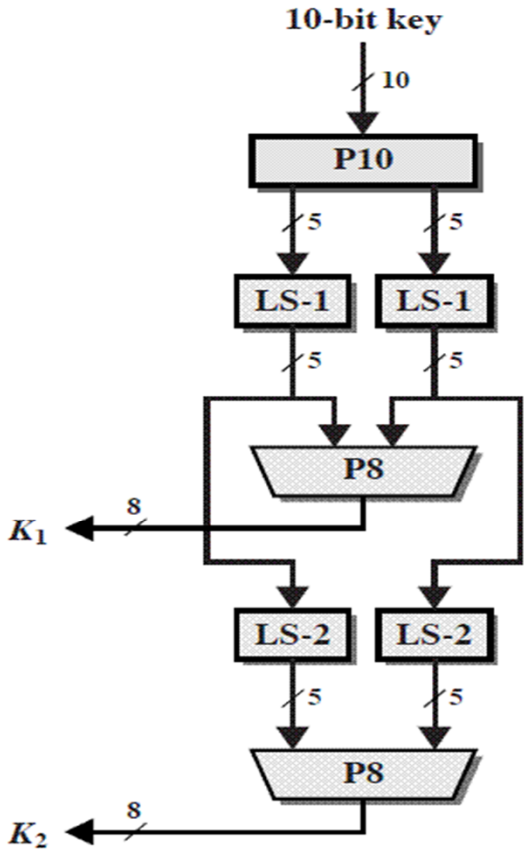


Figure C.2 Key Generation for Simplified DES

خطوات تشفير خوارزمية دِس المبسطة SDES

1. إعادة ترتيب الخانات في الكتلة النصية وتسمى Initial Permutation IP
IP(b1,b2,b3,b4,b5,b6,b7,b8) = (b2,b6,b3,b1,b4,b8,b5,b7)
2. تجزئة الكتلة النصية إلى نصفين (يمين ويسار)
3. تطبيق الدالة f_k والتي تشفر الجزء الأيسر باستخدام المفتاح K_1
3. التبديل بين النصفين الأيمن والأيسر SW
4. تطبيق الدالة fk مرة أخر لتشفير الجزء الأيمن (الذي أصبح على اليسار)
5. إعادة ترتيب خانات الكتلة النصية إلى الوضع الأصلي (عكس IP) : IP^{-1}
بحيث $X = IP^{-1}(IP(X))$

الدالة f_k

- مدخلاتها : مفتاح فرعي SK ب 8 خانات و النص الأصلي 8 خانات
- تستخدم المفتاح الفرعي في تبديل خانات النص الأصلي
- تستخدم S-Boxes لتبديل قيم النص الأصلي بقيم أخرى

$$fk(L,R) = (L \oplus F(R,SK), R)$$

الدالة F

- تستدعى من قبل الدالة fk
- مدخلاتها : قيم النصف الأيمن من النص الأصلي 4 خانات والمفتاح الفرعي 8 خانات
- تقوم بعمليات تبديل وعملية تعويض واحدة
- تكون العلاقة بين النص المشفر والمفتاح علاقة معقدة تضمن خاصية التشويش المطلوبة

الشكل 4 ص 210

خطوات الدالة F

- خطوة التمديد Expansion
  – يتم تمديد الخانات الأربعة للنصف الأيمن R إلى 8 خانات بمضاعفتها مع تغيير الترتيب

    p1,p2,p3,p4 → p4,p1,p2,p3,p2,p3,p4,p1
- خطوة أو الاستثنائية XOR
  – يتم تطبيق XOR على مخرجات خطوة التمديد مع المفتاح

    →B1,B2,B3,B4,B5,B6,B7,B8
- خطوة التعويض Substitution
  – تجزئة مخرجات XOR إلى نصفين (يمين ويسار)
  – من المصفوفتين S-Boxes (S0,S1) بالنظام العشري يتم استخدام النصفين يتم استخراج قيمة عشرية من كل مصفوفة

    S_0(B1B4, B2B3) & S_1(B5B8, B6B7)

خطوات الدالة F

- خطوة التعويض Substitution...
  - تحول الأعداد العشرية إلى ثنائيات ويتم ضم مخرجات S_0,S_1 بالترتيب (s_0على اليسار و S_1 على اليمين) فتشكل 4 خانات ثنائية
- خطوة إعادة الترتيب Transposition
  - يتم إعادة ترتيب مخرجات الخطوة السابقة حسب الدالة P4 : 2,4,3,1

أوجه اختلاف خوارزمية Des عن خوارزمية SDES

- حجم المفتاح :
  - تستخدم DES مفتاح بـ 56 خانة ثنائية ليشكل 16 مفتاحاَ فرعياً
  - تستخدم SDES مفتاح بـ 10 خانات ليشكل مفتاحين فرعيين فقط
- حجم الكتلة المشفرة (مقدار التشتت)
  - تعمل DES على تشفير كتلة مكونة من 64 خانة ثنائية
  - تعمل SDES على تشفير كتلة مكونة من 8 ثنائيات
- صناديق أس S-Boxes (مقدار التشويش)
  - تستخدم DES ثمانية صناديق 4 X 16 (64 قيمة مابين 0- 15)(4 ثنائيات)
  - تستخدم SDES صندوقين 4 X 4 (16 قيمة مابين 0-3)(ثنائيتان)

أوجه اختلاف خوارزمية Des عن خوارزمية SDES

- عدد الجولات (التشتت والتشويش)
  - تتكون DES من 16 جولة
  - تتكون SDES من جولتين فقط
- خوارزمية تشكيل المفاتح الفرعية (درجة اختلاف المفاتيح عن بعضها)
  - تشكل DES 16 مفتاحا مكون من 48 ثنائية
  - تشكل SDES مفتاحين يتكون كل منهما من 8 ثنائيات
- الدالة F تتشابه الخوارزميتان في طريقة الأداء ولكن
  - تتعامل DES (في النصف الأيمن للكتلة) مع 32 ثنائية تتمدد إلى 48
  - تتعامل SDES مع 4 ثنائيات تتمدد إلى 8

مدى الأمان الذي تحققه خوارزمية DES

- يعتبر مفتاح DES والمكون من 56 خانة ثنائية صغيراً نوعاً ما
  - استطاع الباحثون تطوير حاسوب يكسر الشيفرة في ثلاثة أيام بأسلوب القوة الجبارة
  - لا تعتبر آمنة لدرجة كبيرة
  - تم تطوير خوارزمية Triple DES لهذا السبب
- يصعب كسر شيفرة DES عن طريق التحليل
  - طريقة التحليل الخطي – اعتداء النص المعلوم يتطلب معرفة 243 زوجا من النص الأصلي والنص المشفر له، وهذا من الصعب توفيره عملياً
  - طريقة التحليل التفاضلي الاشتقاقي – اعتداء النص الأصلي المختار يتطلب 247 زوجاً من النصوص المختارة وتشفيرها، وهذا يصعب تحصيله أيضا

تطوير خوارزمية DES

- استخدام أكثر من مرحلة تشفير واحدة
  - كل مرحلة (تشفير كامل) بمفتاح مختلف : الشكل 9، 10 ص 222، 223
  - Double DES

$$C = Enc_{K_2}(Enc_{K_1}(P))$$
$$P = Dec_{K_1}(Dec_{K_2}(C))$$

- اعتداء الالتقاء في المنتصف
  - نوع من اعتداءات النص الأصلي المعروف
  - يبنى على أن نتيجة تشفير المرحلة الأولى هي نفس نتيجة فك تشفير المرحلة الثانية

$$C_1 = Enc_{K_1}(P) = Dec_{K_2}(C)$$

خوارزمية Triple DES (TDES)

- تحل مشكلة الالتقاء في المنتصف

$$C = EK_3(EK_2(EK_1(P)))$$

– بما أن خوارزمية التشفير هي نفس خوارزمية فك التشفير فيمكن تبديل المرحل الوسطى

$$C = EK_3(DK_2(EK_1(P)))$$

– لهذا يمكن تكرار أحد المفاتيح بين K_1 و K_2 أو K_2 و K_3

– أي يمكن أن تستخدم مفتاحين 2TDES أو ثلاثة مفاتيح 3TDES

– ولفك التشفير

$$P = DK_3(DK_2(DK_1(C)))$$

- بما أن طول المفتاح في DES = 56 فإن طول المفتاح في TDES = 168 وبهذا تكون آمنة جداً في وجه القوة الجبارة

طرق استخدام أنظمة التشفير الكتلية

- طريقة الكتاب الإلكتروني
  - يتم تشفير أو فك تشفير كل كتلة بشكل مستقل عن الأخريات
  - الشكل 11 ص 227

$$C_i = EK(P_i) / P_i = DK(P_i)$$

  - من عيوبها: قد أحد الكتل أكثر من مرة في النص الأصلي فلا ينصح بها في النصوص الطويلة أو الصور. مثال ص 228
- طريقة الكتل المتسلسلة
  - تعتمد الكتلة المراد تشفيرها على مشفر الكتلة السابقة لها (XOR)
  - الكتلة الأولى تعتمد على متجه ابتدائي، يتم الاتفاق عليه مسبقاً
    الشكل 13 ص 29

طرق استخدام أنظمة التشفير الكتلية

- طريقة العداد
  - تستخدم عداد بحجم مساوي لحجم الكتل
  - يشفر العداد باستخدام أحد خوارزميات التشفير
  - تطبق XOR على العداد المشفر مع النص الأصلي
  - لفك التشفير نطبق XOR على العداد النص المشفر والعداد المشفر

  شكل 14 ص 232
- فوائد طريقة العداد
  - لا نحتاج إلى فك تشفير جميع الكتل لفك تشفير كتلة واحدة
  - نستطيع تشفير أو فك تشفير جميع الكتل على التوازي
  - خوارزمية التشفير وفك التشفير واحدة
  - آمنة بنفس درجة الكتل المتسلسلة