جامعة المنارة الخاصة
كلية الهندسة
هندسة الروبوت والأنظمة الذكية

مهارات الحاسوب

Computer Skills UNRC101

مدرس المقرر
أ.د. مثنى علي القبيلي

الفصل الدراسي الأول | الاثنين 19/12/2022 | العام الدراسي 2022-2023

عناوين المحاضرة السادسة

- مقدمة عن Feistel Cipher
- مخطط مقياس تعمية المعطيات (DES(Data Encryption Standard
  - ✓ الشكل العام للخوارزمية
  - ✓ المراحل العامة لعملية التعمية
  - ✓ المراحل العامة لعملية معالجة النص الصريح
  - ✓ البنية الداخلية للحلقة الواحدة
  - ✓ مخطط التعمية
  - ✓ مخطط فك التعمية
- 2DES
- 3DES

مقدمة عن Feistel Cipher

❖ تمتلك خوارزميات التشفير الكتلي التقليدية هيكلية وصفت لأول مرة من قبل Horst Feistel من IBM عام 1973.

➢ تعتمد على بارامترات التصميم الآتية:

✓ طول البلوك / الكتلة (Block Size)

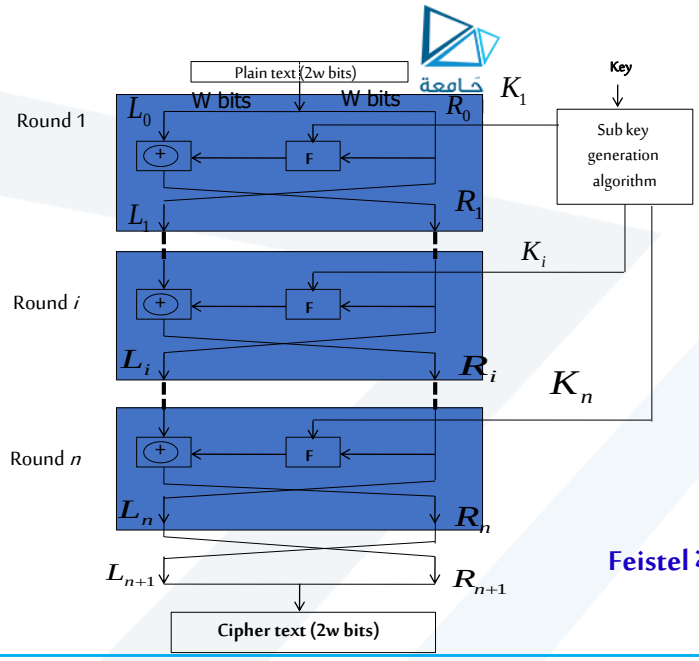
✓ طول المفتاح (Key Size)

كلما كان طول الكتلة و طول المفتاح أكبر كلما كان مستوى الأمن أعلى

✓ عدد الحلقات (Number of rounds) : يزيد استخدام الدورات المتعددة من مستوى الأمن

✓ خوارزمية توليد المفتاح الجزئي (Subkey generation algorithm) : كلما كانت الخوارزمية أكثر تعقيداً كلما ارتفع مستوى حصانتها ضد تحليل التعمية.

✓ برمجيات تشفير وفك تشفير سريعة :(Fast Soft ware Encryption /Decryption) و هي تخص سرعة تنفيذ الخوارزمية التي تظهر أهميتها عند تضمين التعمية في التطبيقات العملية.



الشكل العام لشبكة Feistel

مقدمة عن Feistel Chiper

- دخل الخوارزمية هو عبارة عن كتلة من النص الصريح بطول 2w خانة والمفتاح K .

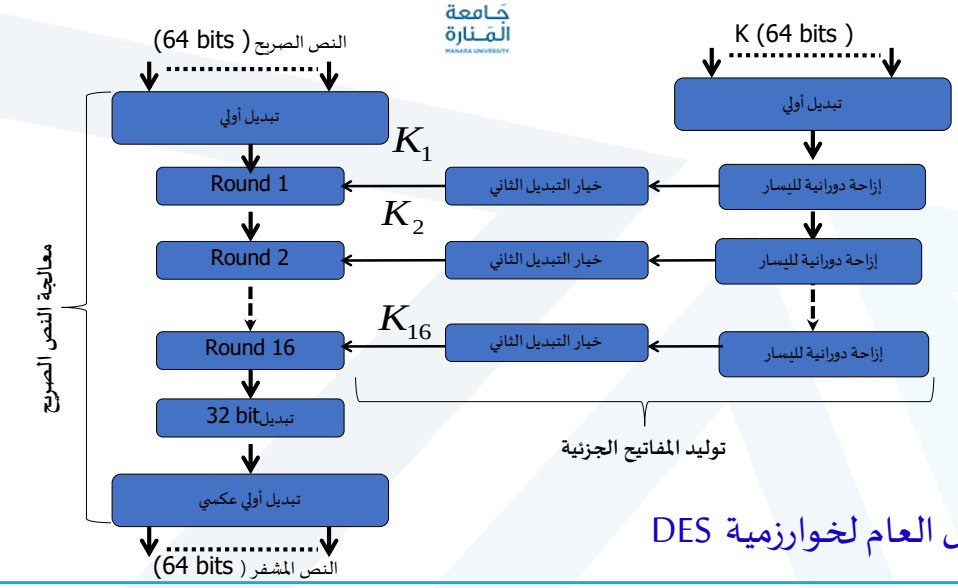
➢ خطوات العمل:

- ✓ يتم تقسيم كتلة النص الصريح إلى نصفين L0, R0 .
- ✓ يمر هذان النصفان من خلال n حلقة معالجة.
- ✓ يتم في النهاية ضم هذين الجزأين لإنتاج النص المشفر.
- ✓ تكون المفاتيح الجزئية مختلفة عن بعضها البعض و عن المفتاح الأساسي K .
- ✓ تتم عملية فك التشفير اعتماداً على نفس عملية التشفير و لكن مع عكس ترتيب المفاتيح أي

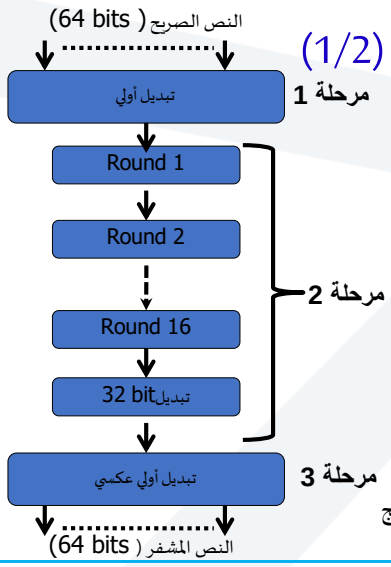
$$K_n \longrightarrow K_1$$

خوارزمية معيار تشفير المعطيات
DES(Data Encryption Standard)

- تسمى أيضاً خوارزمية تشفير المعطيات (DEA (Data Encryption Algorithm.
- تعد أكثر خوارزميات التشفير المتناظر الكتلي انتشاراً
- تستخدم دخلين:
  - النص الصريح المطلوب تعميته (كتلة مكونة من 64 خانة)
  - المفتاح مكون من 64 خانة (عملياً طوله 56 خانة و 8خانات إزدواجية)
- تعطي خرجاً يمثل النص المشفر المكون من 64 خانة



الشكل العام لخوارزمية DES



المراحل العامة لعملية التعمية وفق DES (1/2)

1. **عملية معالجة النص الصريح:**

❖ تشمل عملية المعالجة ثلاث مراحل أساسية :

✓ مرحلة 1 : تبديل مواقع أولي IP (Initial Permutation)

✓ مرحلة 2 : مكونة من 16 حلقة تشمل تابعين :

1. تابع تبديل حروف
2. تابع تبديل مواقع

خرج هذه المرحلة مكون من 64 خانة , يتم بعد ذلك تبديل نصفي الخرج مع بعضهما (تبديل 32 bits)

✓ مرحلة 3: تبديل مواقع أولي عكسي IP^{-1} و يكون الناتج هو النص المشفر

المراحل العامة لعملية التعمية وفق DES (2/2)

2. **عملية توليد المفاتيح الجزئية :**

- استخدام المفتاح ذي الطول 56 خانة (حيث يوجد 8 خانات ازدواجية).
- إنتاج مفتاح جزئي من أجل كل مرحلة من المراحل الـ 16 بـ:

1. تبديل مواقع
2. إزاحة دورانية لليسار
3. تبديل مواقع

ملاحظة:

عملية التبديل هي نفسها ولكنها تتم على الخانات بعد عملية الإزاحة وهذا ما يجعل المفاتيح الجزئية مختلفة عن بعضها البعض.

عملية معالجة النص الصريح وفق DES (1/3)

- **مرحلة 1: عملية التبديل الأولي (IP):**
  - ✓ تتم عملية التبديل الأولي وفق الجدول الآتي:

من أجل خانات الدخل (M) الـ 64 مرقمة من 1 إلى 64

فتكون الغاية من عملية التبديل هي إعادة ترتيب البتات وفق هذا الجدول

X=IP(M)

Li	58	50	42	34	26	18	10	2
	60	52	44	36	28	20	12	4
	62	54	46	38	30	22	14	6
	64	56	48	40	32	24	16	8
Ri	57	49	41	33	25	17	9	1
	59	51	43	35	27	19	11	3
	61	53	45	37	29	21	13	5
	63	55	47	39	31	23	15	7

عملية معالجة النص الصريح وفق DES (2/3)

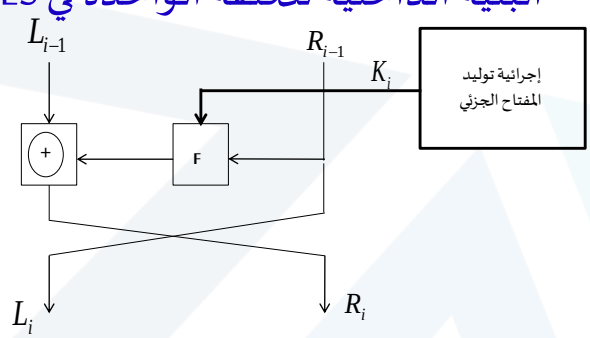
- مرحلة 2 : تقسم إلى جز أين

1. تنفيذ الـ 16 حلقة: سندرس البنية الداخلية للحلقة

2. التبديل 32bits :

هي تبديل نصفي الخرج مع بعضهما أي جعل الجزء اليساري يميني و بالعكس

البنية الداخلية للحلقة الواحدة في DES (1/4)

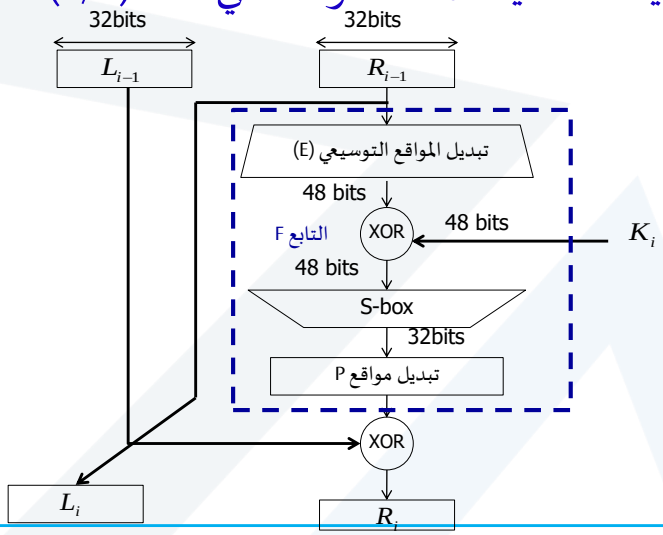


يعبر عن عملية المعالجة كما يلي:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

البنية الداخلية للحلقة الواحدة في DES (2/4)



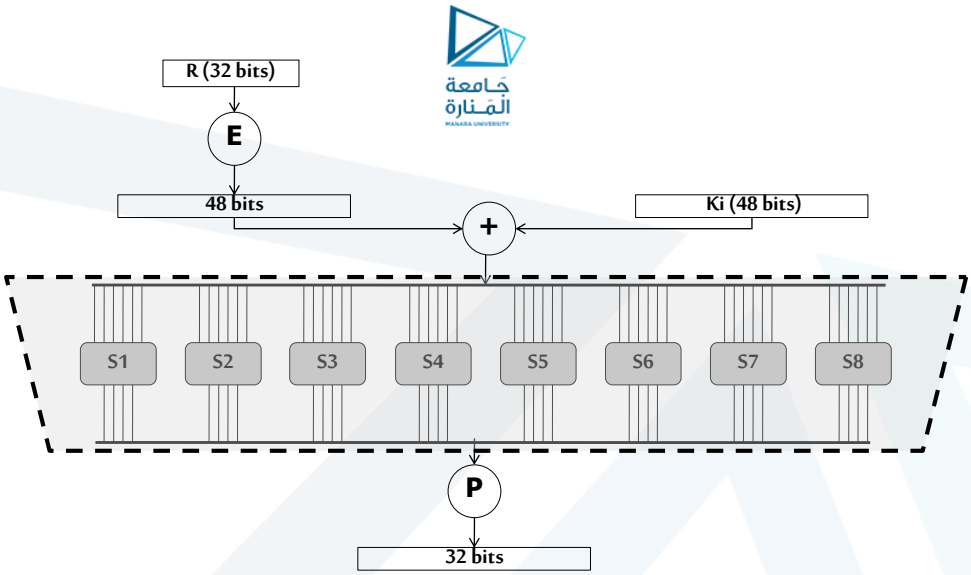
البنية الداخلية للحلقة الواحدة في DES (3/4)

✓ تنفيذ التابع F :

➢ له دخلان هما:

- مفتاح الحلقة (مفتاح جزئي) مكون من 48 خانة
- الدخل R (الجزء الأيمن من الكتلة) و مكون من 32 خانة

و يتضمن أربع مراحل كما يظهر في الشكل الآتي:



مخطط تنفيذ التابع F

مراحل تنفيذ التابع F (1/ 3)

1 .يتم توسيع الدخل R ليصل إلى 48 خانة , باستخدام الجدول الآتي (E):

حيث تكرر 16 خانة من خانات الدخل R

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

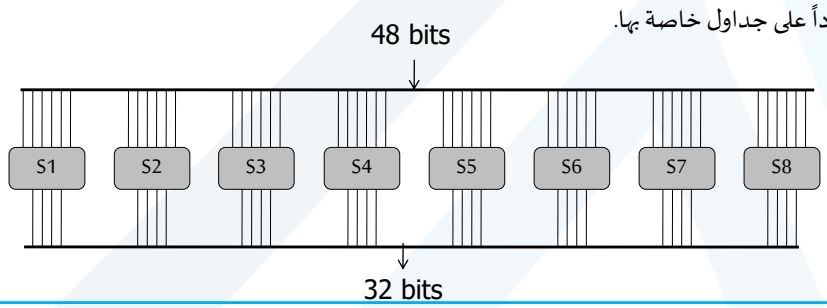
جدول تبديل المواقع التوسيعي (E)

مراحل تنفيذ التابع F (2/3)

2. يتم جمع R الموسعة مع المفتاح الجزئي باستخدام بوابة XOR, الناتج مكون من 48 خانة .

3. تجرى عليه عملية تبديل الحروف و ذلك بإدخاله على ما يسمى S-box أي الصناديق S . و نحصل على خرج مكون من 32 خانة.

صناديق S مكونة من 8 صناديق , كل منها له دخل مكون من 6 خانات و خرج مكون من 4 خانات و يتم ذلك اعتماداً على جداول خاصة بها.



آلية عمل الصندوق Si :

- تدل الخانتان الأولى والأخيرة من دخل Si على رقم السطر ضمن الجدول Si

- تدل الخانات الأربع المتبقية على رقم العمود ضمن نفس الجدول Si

- تعطي القيمة المقابلة لالتقاء هذا السطر و هذا العمود قيمة الخرج الخاصة بهذا الصندوق و هكذا ..

مثال:

إذا فرضنا أن دخل الصندوق S1 هو : 011000 ماهي خانات الخرج؟

العمود 12

011000

السطر 0

إذا كان دخل الصندوق S1 هو

الخرج هو 0101

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

جدول الصندوق S1

مراحل تنفيذ التابع F (3/ 3)

4. تطبيق تابع تبديل المواقع (P) المبين بالجدول الآتي:

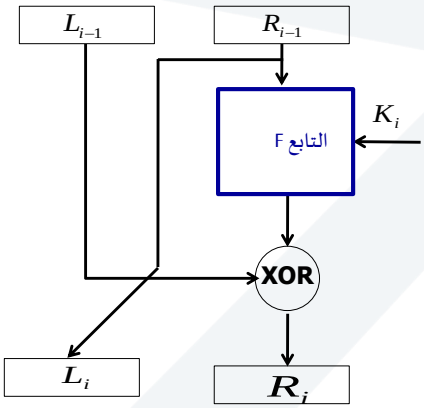
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

جدول تبديل المو اقع (P)

و هذه هي المرحلة الأخيرة من مراحل تنفيذ التابع F. ناتج تطبيق هذا التبديل مكون من 32 خانة و هو أحد مدخلي بوابة XOR

البنية الداخلية للحلقة الواحدة في DES (4/4)

❑ يمكن ان نعبر عن إجرائية الحلقة الواحدة كالآتي:



✓ يجمع الخرج الناتج عن تنفيذ التابع F مع القسم اليساري L_{i-1} من خانات الدخل لنحصل على خرج يمثل القسم الأيمن من دخل الحلقة التالية R_i

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

✓ و يكون القسم اليساري للحلقة التالية هو نفسه القسم الأيمن من دخل الحلقة السابقة

$$L_i = R_{i-1}$$

عملية معالجة النص الصريح وفق DES (3/3)

➢ مرحلة 3 : تطبيق عملية **التبديل العكسي** للتبديل الأولي (IP^{-1}) :

تتم وفق الجدول الآتي:

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

$$Y = IP^{-1}(X) = IP^{-1}(IP(M))$$

المراحل العامة لعملية التعمية وفق DES (2/2)

2. عملية توليد المفاتيح الجزئية :

- ❖ استخدام المفتاح ذي الطول 56 خانة (حيث يوجد 8 خانات ازدواجية).
- ❖ إنتاج مفتاح جزئي من أجل كل مرحلة من المراحل الـ 16 بـ:

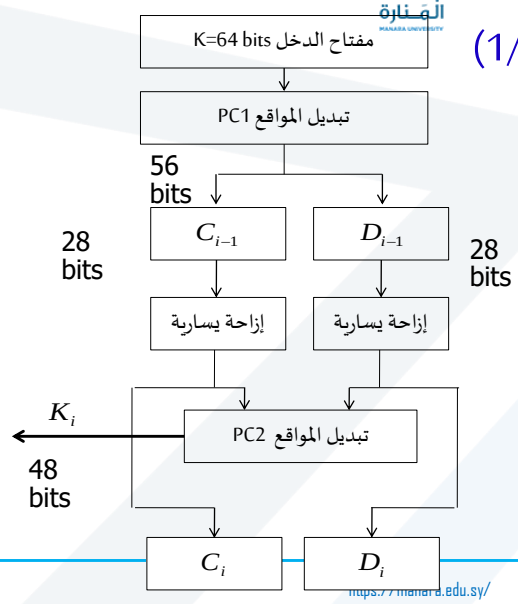
1. تبديل مواقع
2. إزاحة دوانية لليسار
3. تبديل مواقع

ملاحظة:

عملية التبديل هي نفسها ولكنها تتم على الخانات بعد عملية الإزاحة وهذا ما يجعل المفاتيح الجزئية مختلفة عن بعضها البعض.

عملية توليد المفاتيح الجزئية (1/4)

❑ مخطط توليد المفتاح الجزئي:



عملية توليد المفاتيح الجزئية (2/4)

❑ مفتاح الدخل:

هو المفتاح ذي الطول 64 خانة, يتم ترقيمها من 1 حتى 64

مع إهمال كل خانة ثامنة أي سيكون الدخل الفعلي هو 56 خانة كما هو مبين بالجدول الآتي:

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

مفتاح الدخل

عملية توليد المفاتيح الجزئية (3/ 4)

1. يتم معالجة المفتاح المكون من 56 خانة على شكل نصفين كل منهما 28 خانة ترمز بـ

D_{i-1}, C_{i-1} ; $16 \geq i \geq 1$ باستخدام جدول (PC1) :

Ci-1	57	49	41	33	25	17	9
	1	58	50	42	34	26	18
	10	2	59	51	43	35	27
	19	11	3	60	52	44	36
Di-1	63	55	47	39	31	23	15
	7	62	54	46	38	30	22
	14	6	61	53	45	37	29
	21	13	5	28	20	12	4

جدول (PC1)

عملية توليد المفاتيح الجزئية (4/4)

2. تنفذ إزاحة دورانية يسارية لكل جزء بشكل مستقل بمقدار خانة واحدة أو خانتين تبعاً للجدول الآتي:

رقم الحلقة	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
التدوير	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

3. يحسب الشكل النهائي للمفتاح الجزئي K_i المكون من 48 خانة من خلال استخدام خيار التبديل الثاني (PC2) الموضح بالجدول الآتي:

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

ملاحظة: دخل إجرائية توليد المفتاح الجزئي التالي هما جزئي المفتاح الجزئي السابق بعد التدوير .

مخطط التعمية وفق DES(1/2)

1) الدخل : النص الصريح $M = m_1 \ldots\ldots m_{64}$

مفتاح بطول 64 خانة $K = k_1 \ldots\ldots k_{64}$ (ثماني خانات إزدواجية)

2) الخرج : نص مشفر بطول 64 خانة $C = c_1 \ldots\ldots c_{64}$

3) الإجرائية:

1. يتم توليد 16 مفتاح جزئي للحلقات، طول كل منها 48 خانة .
2. تبديل مواقع الخانات و من ثم تقسم النتيجة إلى نصفين يساري و يميني كل منها بطول 32 خانة.

$$L_0 = m_{58} m_{50} \ldots\ldots m_8 \qquad R_0 = m_{57} m_{49} \ldots\ldots m_7$$

مخطط التعمية وفق DES(2/2)

3. يتم تنفيذ 16 حلقة بحيث يتم حساب R_i, L_i حيث $16 \geq i \geq 1$
4. يتم تبديل الكتل النهائية R_{16}, L_{16} فيما بينها
5. تطبيق ا لتبديل الأولي العكسي IP^{-1} وبالنتيجة الحصول على النص المشفر

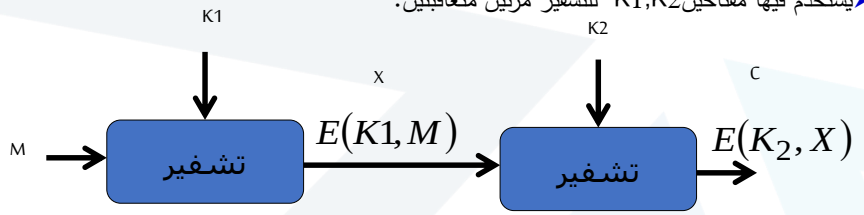
مخطط فك التعمية وفق DES

تستخدم عملية فك التعمية نفس خوارزمية التعمية و لكن مع استخدام المفاتيح الجزئية بترتيب معاكس

خوارزمية 2DES(1/4)

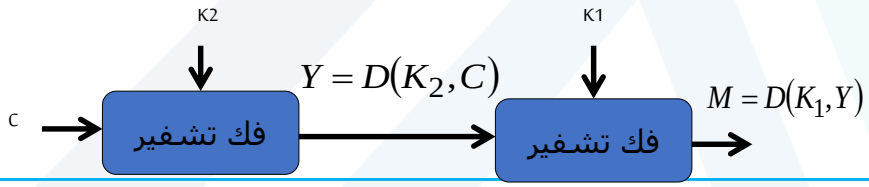
➢يستخدم فيها مفتاحين K1,K2 للتشفير مرتين متعاقبتين:

$$C = E(K_2, E(K1, M))$$



➢يتم فك التشفير بشكل متعاقب أيضاً:

$$M = D(K_1, D(K_2, C))$$



خوارزمية 2DES(2/4)

- كانت الفرضية تقوم على أساس أن استخدام مفتاحين في عملية التشفير سيحسن المستوى الأمني لكن تحليل التعمية أثبت أن هذا التشفير المضاعف يتطلب من المهاجم وقتاً مضاعفاً فقط لا أكثر لكسر التشفير.
- طول المفتاح الكلي المستخدم هو 112 bits
- في حال استطاع المهاجم (هجوم رجل في المنتصف) الحصول على زوج واحد فقط (نص مشفرC، نص صريحM) سيكون قادراً على كسر هذه الخوارزمية، وهذا ما يسمى هنا هجوم (brute force)

- يقوم المهاجم بتشفير النص الصريح باستخدام جميع الـ 2^{56} مفتاح ممكن ويخزن كل قيم X الناتجة

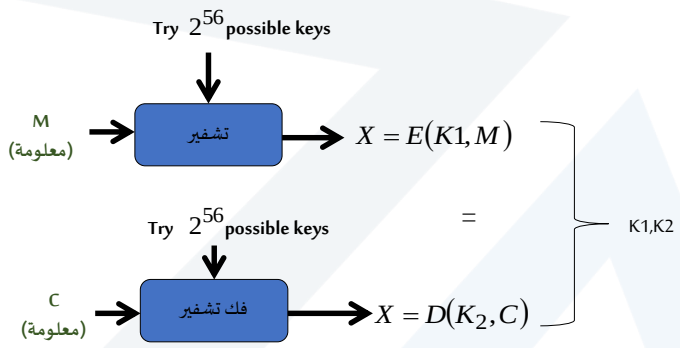
$$X = E(K1, M)$$

- يقوم المهاجم بفك تشفير النص المشفر باستخدام الـ 2^{56} مفتاح ممكن ويخزن كل قيم X الناتجة

$$X = D(K_2, C)$$

- من خلال المقارنة يمكن للمهاجم أن يستنتج المفتاحين المستخدمين.

خوارزمية 2DES(3/4)



خوارزمية 2DES(4/4)

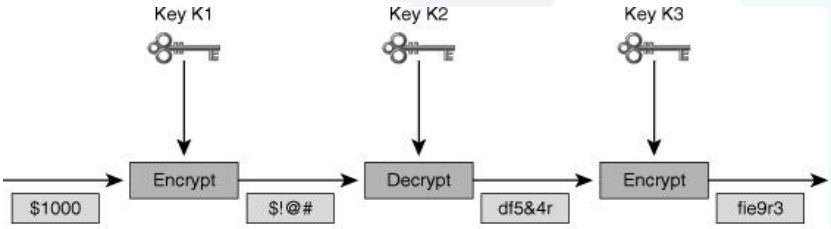
- من أجل خوارزمية 2DES يحتاج المهاجم من نوع Brute Force إلى زمن مضاعف للكسر مقارنة من DES .

  - ✓ من أجل DES المهاجم يحتاج إلى 2^{56} تكرار
  - ✓ من أجل 2DES المهاجم يحتاج إلى $2 \times 2^{56} = 2^{57}$ تكرار

خوارزمية 3DES(Triple -DES)

- يتم فيها استخدام ثلاثة مفتاح للتشفير K1,K2,K3 بحيث يتم التشفير كالآتي:

$$C = E(K_3, D(K_2, E(K1, M)))$$



- في حال كان K1=K3 يكون طول المفتاح الكلي =56X2=112 bits
- في حال كان K1≠K3 يكون طول المفتاح الكلي =56X3=168 bits

Thanks