جامعة المنارة

كلية الهندسة

قسم ميكاترونيكس

Information System Security

أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا

عناوين المحاضرة السادسة

- مخطط مقياس تعمية المعطيات DES(Data Encryption Standard)
  - ✓ المراحل العامة لتوليد المفاتيح الجزئية
  - ✓ مخطط التعمية
  - ✓ مخطط فك التعمية
  - ✓ 2DES
  - ✓ 3DES

عملية توليد المفاتيح الجزئية (1/5)

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

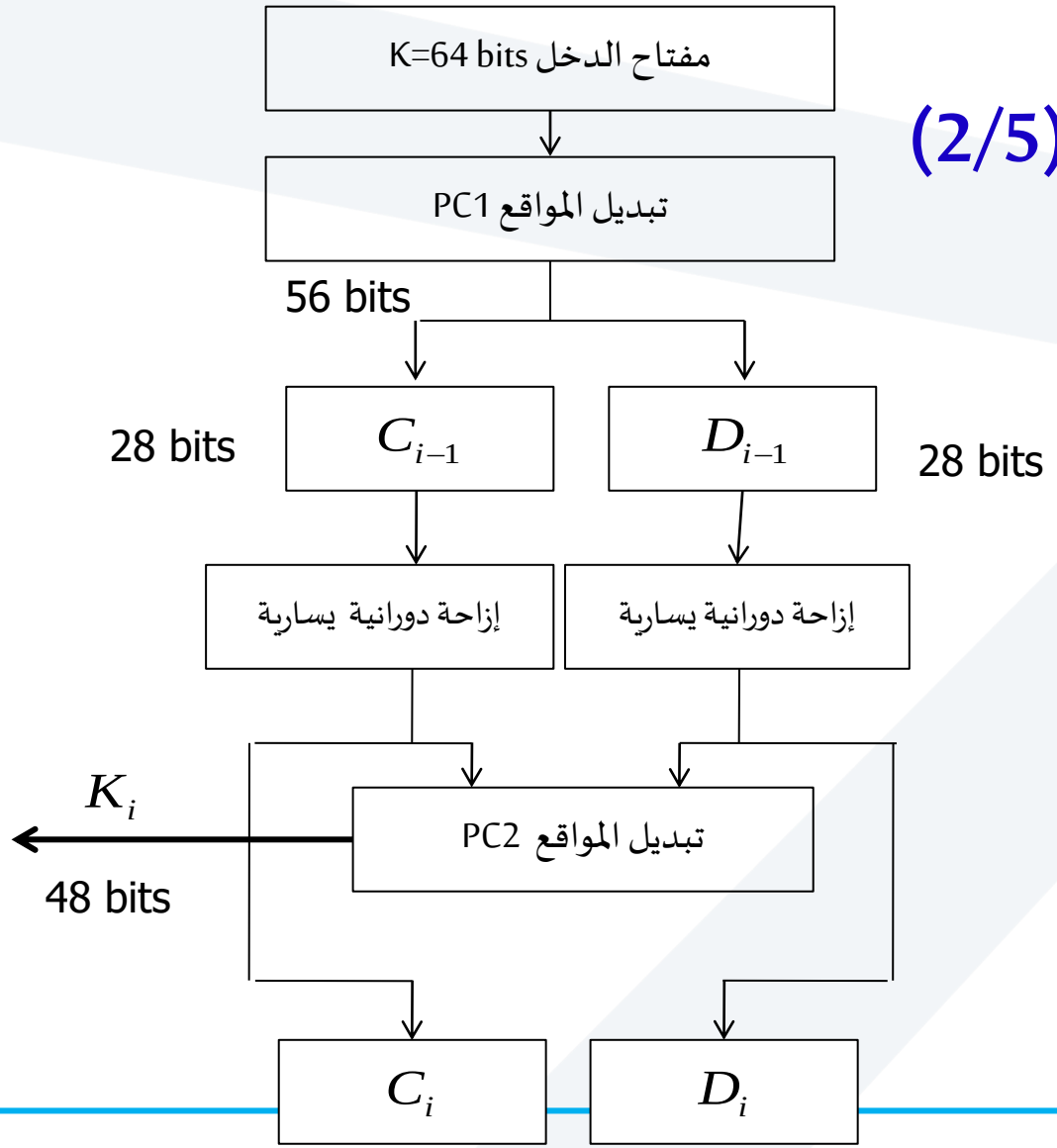
1. تبديل مواقع
2. إزاحة دورانية لليسار
3. تبديل مواقع

ملاحظة:

عملية التبديل هي ذاتها ولكنها تنفذ على الخانات بعد عملية الإزاحة، وهذا ما يجعل المفاتيح الجزئية مختلفة عن بعضها البعض.

عملية توليد المفاتيح الجزئية (2/5)

❑ مخطط توليد المفتاح الجزئي:



عملية توليد المفاتيح الجزئية (3/5)

❑ **مفتاح الدخل:**

هو مفتاح طوله 64 خانة, ترقم خاناته 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 (4/5)

1. يعالج المفتاح المكون من 56 خانة على شكل نصفين كل منهما 28 خانة ترمز C_{i-1}, D_{i-1} ; $1 \geq i \geq 16$

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)

باستخدام جدول (PC1) :

عملية توليد المفاتيح الجزئية (5/5)

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

جدول(PC2)

ملاحظة: دخل إجرائية توليد المفتاح الجزئي التالي هما جزأي 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. 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. تنفيذ 16 حلقة بحيث يتم حساب L_i , R_i حيث $16 \geq i \geq 1$

4. تبديل الكتل النهائية L_{16} , R_{16} فيما بينها

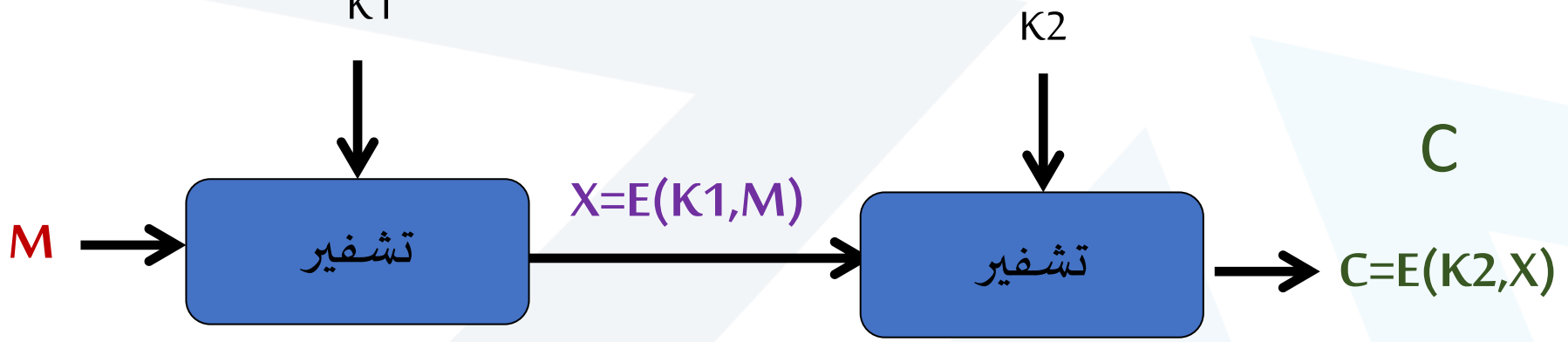
5. تطبيق ا لتبديل الأولي العكسي IP^{-1} وبالنتيجة الحصول على النص المشفر

مخطط فك التعمية وفق DES

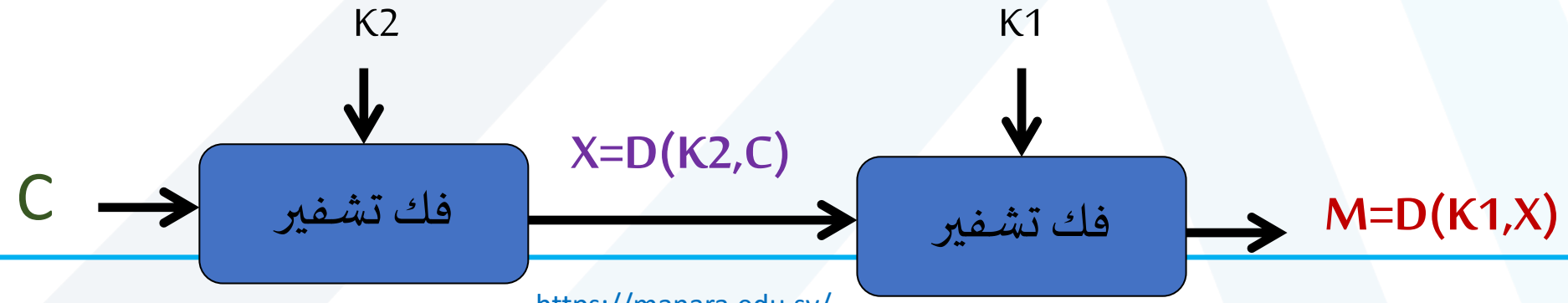
تستخدم عملية فك التعمية نفس خوارزمية التعمية و لكن مع استخدام المفاتيح الجزئية بترتيب معاكس

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



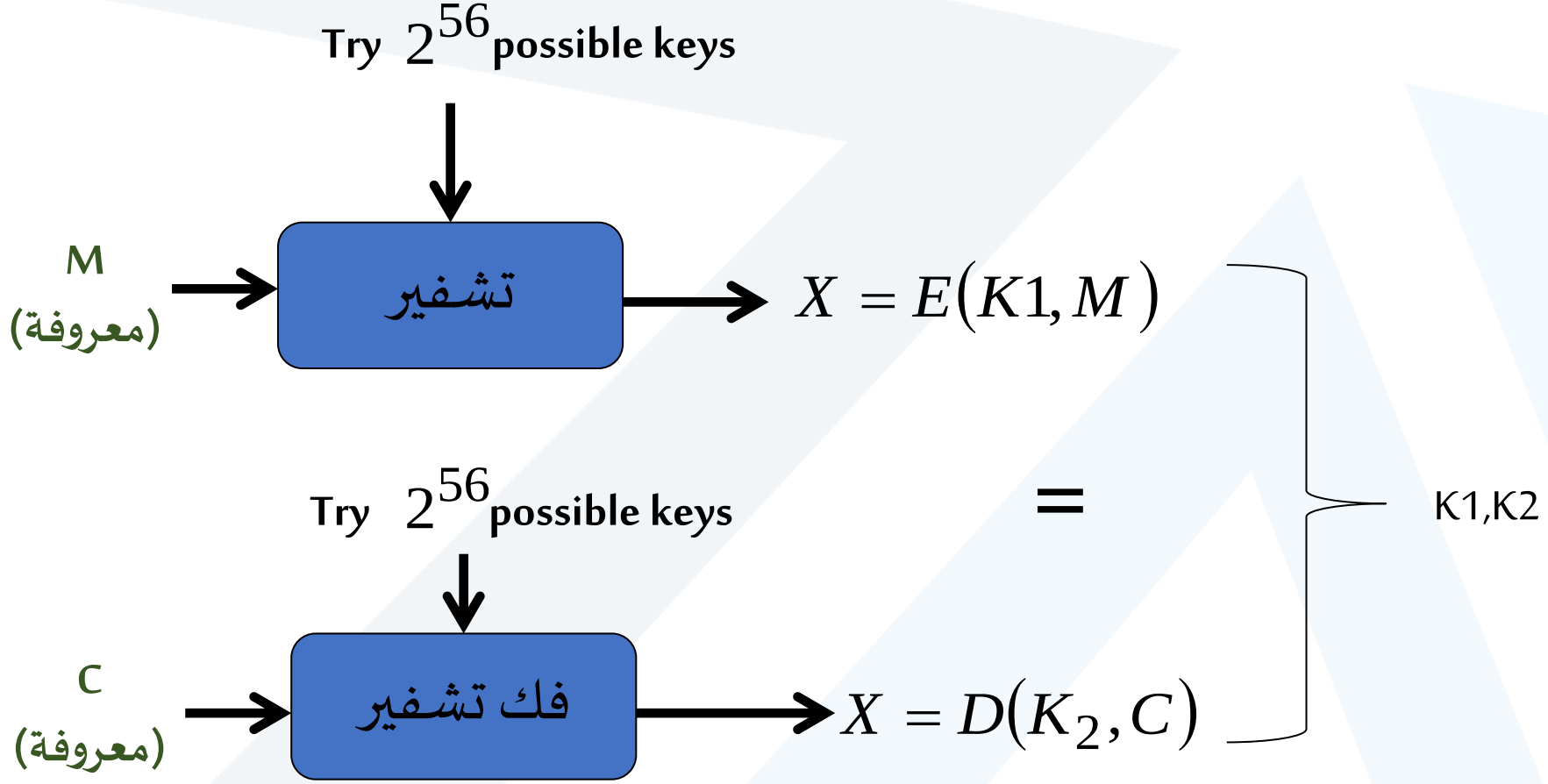
خوارزمية 2DES (2/4)

- قامت الفرضية 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 القوة الغاشمة / الهجوم الأعمى (brute force)
  - يقوم المهاجم بتشفير النص الصريح باستخدام جميع الـ 2^{56} مفتاح ممكن و يخزن كل قيم X الناتجة $X = E(K1, M)$
  - يقوم المهاجم بفك تشفير النص المشفر باستخدام الـ 2^{56} مفتاح ممكن و يخزن كل قيم X الناتجة $X = D(K_2, C)$
  - من خلال المقارنة يمكن للمهاجم أن يستنتج المفتاحين المستخدمين.

خوارزمية 2DES (3/4)

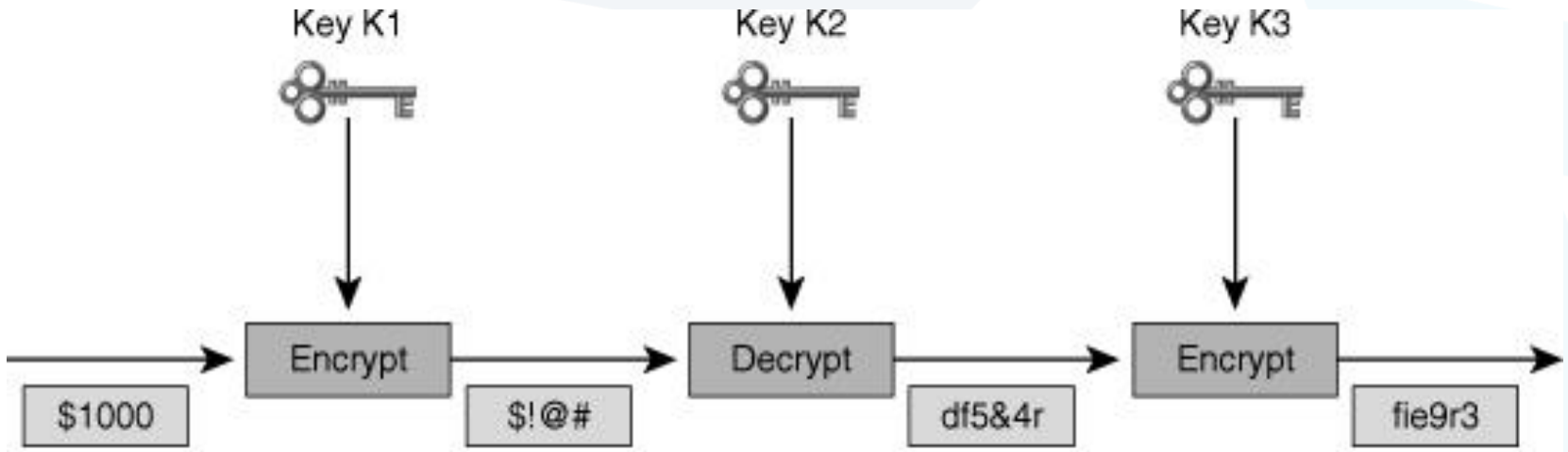


خوارزمية 2DES (4/4)

- 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 3(Triple-DES)

- تستخدم ثلاثة مفتاح للتشفير K1,K2,K3 بالتشفير 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

نهاية المحاضرة السادسة