عملي أمن نظم المعلومات

جلسة العملي الرابعة

مدرسة المقرر

د. بشرى علي معلا

المسألة الأولى

من أجل خوارزمية التشفير المتناظر DES، خرج تبديل المو اقع التوسيعي E.

0 0 0 0 0 0 0 0 11 1 1 1 1 1 1 0 0 0 0 1 1 1 1 00 0 0 0000 1 1 1 1 1 1 1 1 0 0 0 00 000

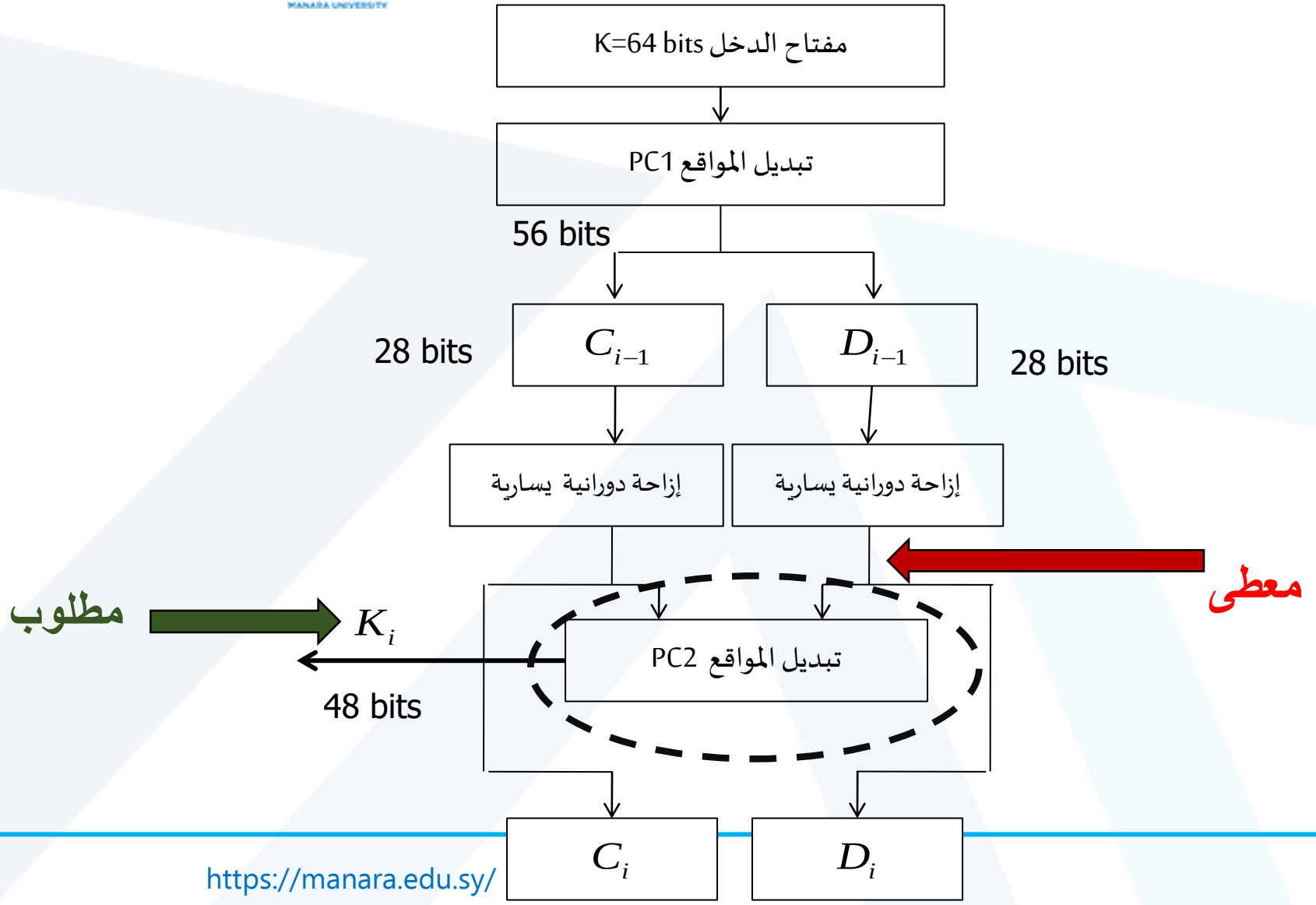
ومن أجل الحلقة الأولى إذا كان دخل التبديل الثاني PC2هو:

11111 1 1 1 1 1 1 1 1 1 1 1 1 1 1111111 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1110

المطلوب:

1. حساب المفتاح الجزئي للحلقة الأولى (K1) .
2. حساب خرج الصناديق S-BOX.

حل المسألة الأولى



حل المسألة الأولى

1. حساب المفتاح الجزئي للحلقة الأولى (K1) .

1. نرقم خانات دخل جدول PC2 من 1 حتى 56

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
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0

49	50	51	52	53	54	55	56
0	0	0	0	0	0	0	0

حل المسألة الأولى

1. حساب المفتاح الجزئي للحلقة الأولى (K1) .

2. نطبق جدول التبديل PC2 :

1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
0	0	0	0	1	0	0	0
0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0

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

3. نمسح قيم الجدول بشكل ZGZAG :

1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
0	0	0	0	1	0	0	0
0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0

فتكون قيمة المفتاح K1 :

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0

2. حساب خرج الصناديق S-BOX.

1. نجري نحسب دخل صناديق S-BOX بحساب : $E \oplus K1$

0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 1 0 0 0 0

1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 0 0 0 1 0 1 1 1 1 1 1 0 0 1 0 0 0 0

2. نقسم الدخل إلى كل 6 خانات على حدى لتكون كل منها دخل لأحد صناديق S-BOX

1 1 1 1 1 1 | 1 1 0 0 0 0 | 0 0 0 0 1 1 | 1 1 0 0 0 0 | 0 0 0 0 1 0 | 0 0 1 0 1 1 | 1 1 1 1 0 0 | 1 0 0 0 0 0

S1 S2 S3 S4 S5 S6 S7 S8

باستخدام جداول S-BOX نقاطع السطر و العمود لكل جدول ونحصل على القيم المبينة تالياً:

الصندوق	الدخل	رقم السطر	رقم العمود	القيمة العشرية	الخرج الثنائي
S1	111111	3	15	13	1101
S2	110000	2	8	5	0101
S3	000011	1	1	7	0111
S4	110000	2	8	15	1111
S5	000010	0	1	12	1100
S6	001011	1	7	5	0101
S7	111100	2	14	9	1001
S8	100000	2	0	7	0111

فيكون الخرج هو: 11010101011111111100010110010111

المسألة الثانية

1. لدينا رسالة M مكونة من 256 بت يراد تشفيرها باستخدام خوارزمية التشفير المتناظر DES، ما هي الخطوة الأولى التي يجب إجراؤها و لماذا؟

2. بفرض لدينا ما يلي: Ci-1=C0 =10111100110100011010010000101

Di-1=D0=11010010001011101000011111111

خرج الجدول التوسيعي E : 00000000111111110000111100001111000000011111111

المطلوب: 1. دخل صناديق S-BOX

2. خرج الصندوق S-BOX 4 فقط

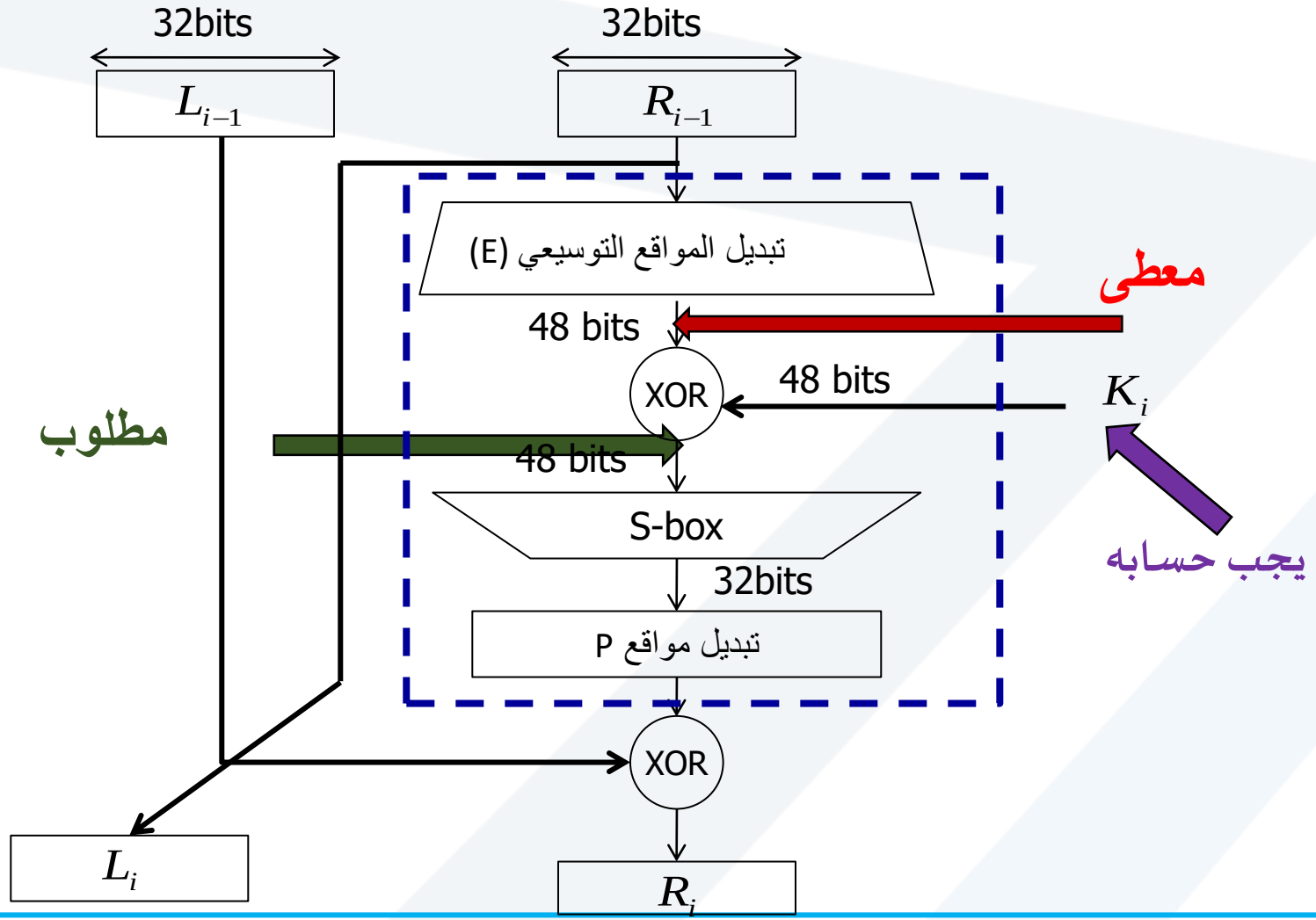
حل المسألة الثانية:

1. بما أن النص الصريح M>64 bits ، يجب أن تقسيم الرسالة إلى بلوكات طول كل منها 64 بت ، 4=64 ÷ 256 أي سنقسم الرسالة إلى 4 بلوكات.

2. دخل صناديق S-BOX

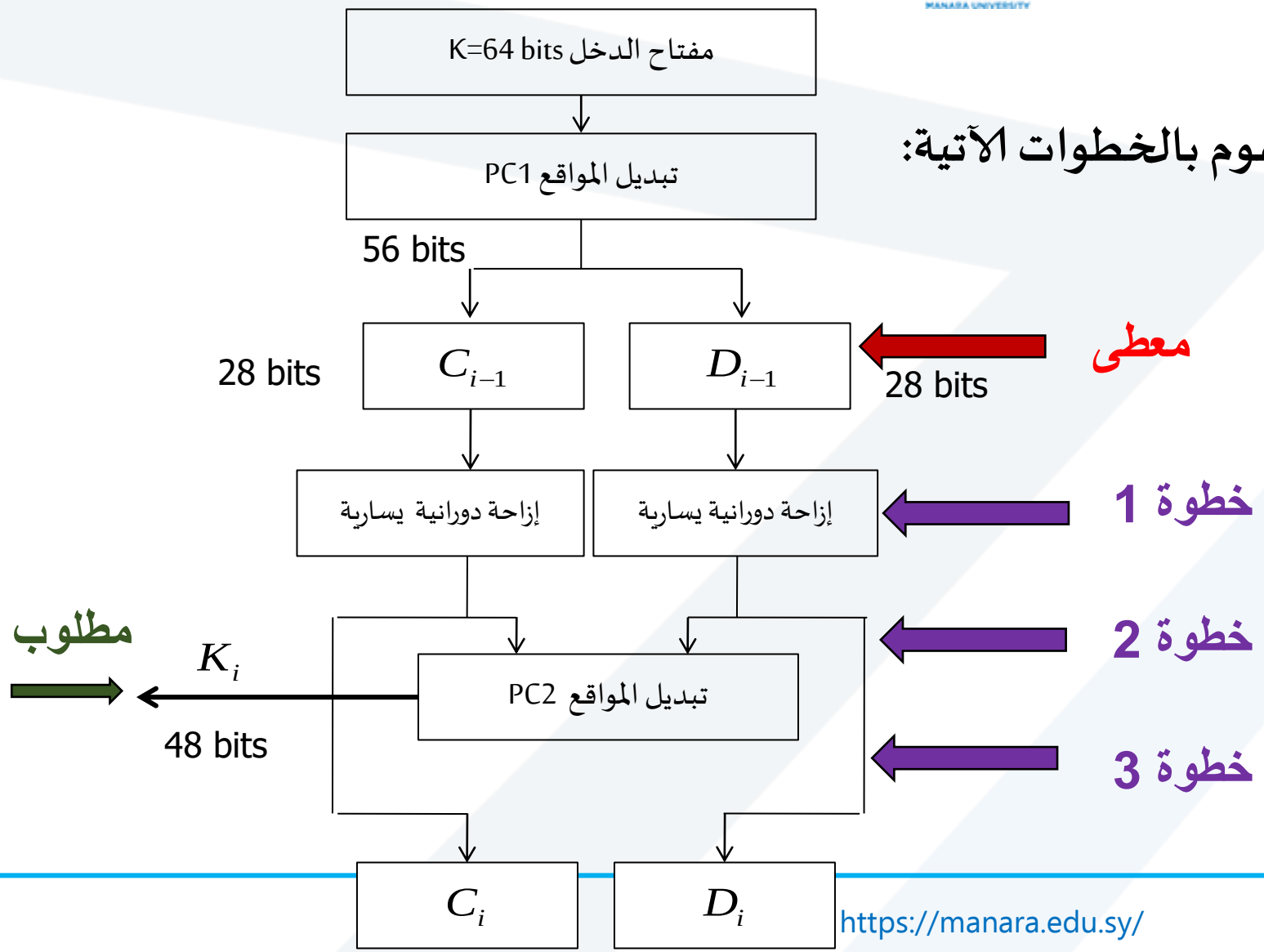
دخل صناديق S-BOX يساوي

يجب حسابه ← $E \oplus K1$ ← معطى



من أجل حساب المفتاح الجزئي للحلقة K1 نقوم بالخطوات الآتية:

1. تطبيق الإزاحة الدورانية
2. لصق الجزأين للحصول على دخل PC2
3. تطبيق جدول التبديل PC2



1. بما أننا في الحلقة I=1 نقوم **بالإزاحة دورانية نحو اليسار** بمقدار خانة واحدة:

الجدول:

رقم الحلقة	1	2	3	4	5 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

قبل الإزاحة C0 =10111100110100011010010001O1

بعد الإزاحة C0=11011110011010001101001000 10

قبل الإزاحة D0=1101001000101110100001111111

بعد الإزاحة D0=1110100100010111010000111111

2 . نلصق الجزأين فنحصل على **دخل جدول التبديل PC2**

C0D0=1101111001101000110100100010111010010001011101000011111 1

3 . نطبق **جدول التبديل PC2**

1. نرقم خانات دخل الجدول من 1 حتى56

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
1	**1**	**0**	**1**	**1**	**1**	**1**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**1**	**1**	**1**	**1**

2. نضع قيم الخانات في جدول PC2

0	1	1	0	1	1	0	0
0	0	0	1	1	0	0	1
0	0	0	1	1	1	1	1
0	1	1	0	0	1	1	1
1	0	1	0	1	0	0	1
0	1	1	1	0	1	1	0

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

3.نمسح أسطر الجدول PC2 فنحصل على المفتاح الجزئي

0	1	1	0	1	1	0	0
0	0	0	1	1	0	0	1
0	0	0	1	1	1	1	1
0	1	1	0	0	1	1	1
1	0	1	0	1	0	0	1
0	1	1	1	0	1	1	0

K1= 01101100000110010001111101100111101010010111010

فيكون دخل صناديق S-BOX : $E \oplus K1$

0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1

0 1 1 0 1 1 0 0 0 0 0 1 1 0 0 1 0 0 0 1 1 1 1 1 0 1 1 0 0 1 1 1 1 0 1 0 1 0 0 1 0 1 1 1 0 1 1 0

0 1 1 0 1 1 0 0 1 1 1 0 0 1 1 0 0 0 0 1 0 0 0 0 0 1 1 0 1 0 0 0 1 0 1 0 1 0 0 1 1 0 0 0 1 0 0 1

2. خرج الصندوق S-BOX 4 فقط

011011 | 001110 | 011000 | 010000 | 011010 | 001010 | 100110 | 001001

S1 S2 S3 S4 S5 S6 S7 S8

نلاحظ أن دخل الصندوق S-BOX 4 هو 010000

فيكون رقم السطر 0 و رقم العمود 8

باستخدام الجدول S-BOX4 يكون الخرج هو

فيكون دخل صناديق S-BOX :

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

S-BOX 4

نلاحظ أن دخل الصندوق S-BOX 4 هو 010000

فيكون رقم السطر 0 و رقم العمود 8

باستخدام الجدول S-BOX4 يكون الخرج هو 1 فيكون الخرج بالثنائي هو 0001

المسألة الثالثة

1.ما هي الغاية من استخدام صناديق S-BOX ؟

الغاية هي التحويل من الدخل من 48 بت إلى 32 بت بهدف الحصول على دخل لبوابة XOR التي مدخلها الثاني هو الجزء اليساري للحلقة السابقة

2. إذا كان R2 =00000000001111111111000001111100 ما هي قيمة L3 ؟

هي ذاتها قيمة R2 لأن : $L_i = R_{i-1}$

الجداول الملحقة

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

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

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

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

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

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

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

جدول تبديل المواقع (P)

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