مهارات الحاسوب

الدكتور المهندس
مثنى القبيلي

هندسة الروبوتيكس والأنظمة الذكية
كلية الهندسة
جامعة المنارة

الفصل الدراسي الأول ٢٠٢١-٢٠٢٢

المسألة الأولى

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

0000000 0111111110 0 0 01111 00 0 0 0000 1111111 10 0 0 00 000

و من أجل الحلقة الأولى إذا كان دخل التبديل الثاني PC2هو:

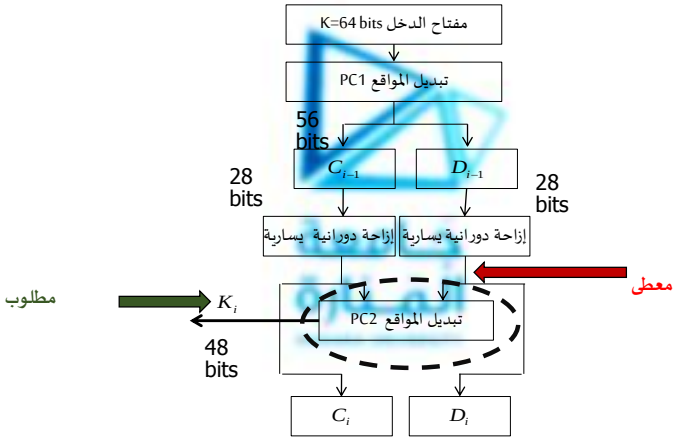
11111111111111111111111111111000000000000000000000000001110

المطلوب:

١. حساب المفتاح الجزئي للحلقة الأولى (K1) .
٢. حساب خرج الصناديق S-BOX.

2

حل المسألة الأولى



3

حل المسألة الأولى

11111111111111111111111111111000000000000000000000000001110

١. حساب المفتاح الجزئي للحلقة الأولى (K1).

١. نرقم خانات دخل جدول PC2 من ١ 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 49 50 51 52 53 54 55 56

11111111111111111111111111111000000000000000000000000001110

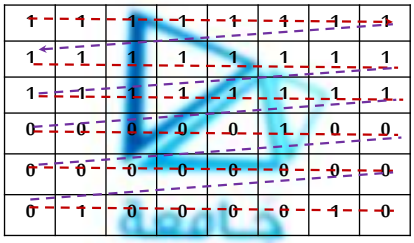
٢. نطبق جدول التبديل PC2:

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

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

4

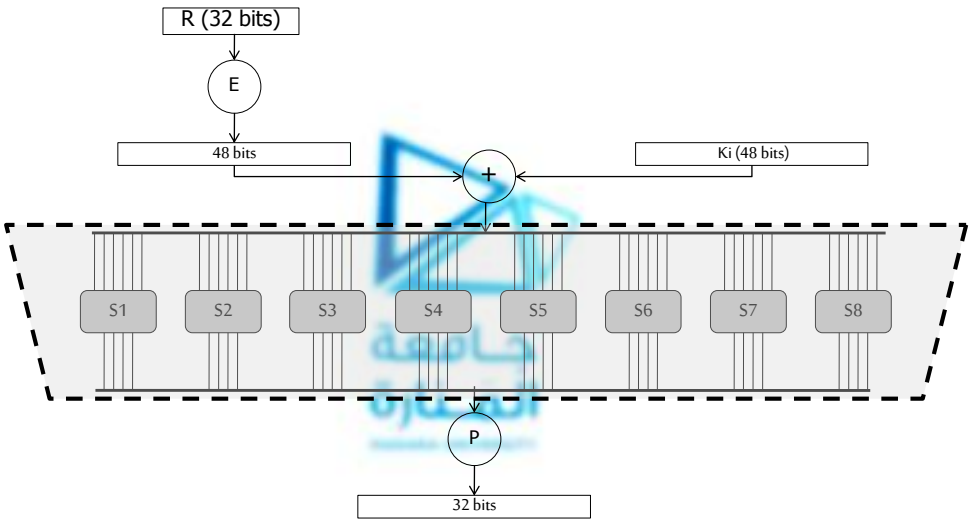
٣. نمسح قيم الجدول بشكل ZGZAG :



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

5



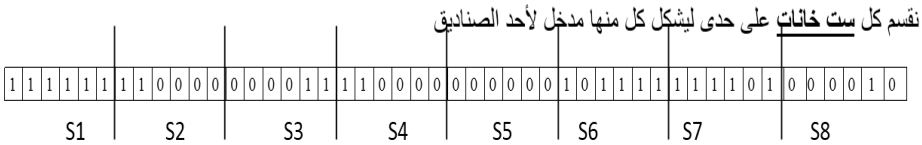
مخطط تنفيذ التابع F

6

يلزمنا أولا حساب دخل الصناديق S (S-box) و هي عبارة عن خرج تبديل المواقع التوسيعي $\oplus K_1$

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

نقسم كل **ست خانات** على حدى ليشكل كل منها مدخل لأحد الصناديق



7

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	000001	1	0	14	**1110**
S6	001111	1	7	5	**0101**
S7	111101	3	14	3	**0011**
S8	000010	0	1	2	**0010**

فيكون الخرج هو: 11010101011111111100101001100 10

8

المسألة الثانية

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

٢. بفرض لدينا ما يلي:

Ci-1=C0 =10111100110100011010010001O1

Di-1=D0=11010010001011101000011111111

خرج الجدول التوسيعي E :

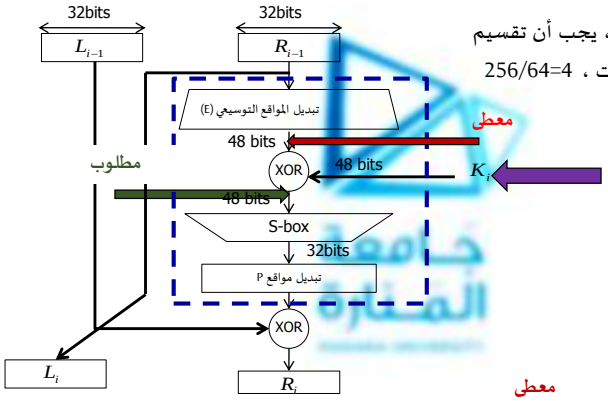
00000000111111110000111100001111000000000111111111

المطلوب: ١. دخل صناديق S-BOX

٢. خرج الصندوق S-BOX 4 فقط

9

حل المسألة الثانية



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

٢. دخل صناديق S-BOX

دخل صناديق S-BOX يساوي

$E \oplus K1$

معطى

يجب حسابه

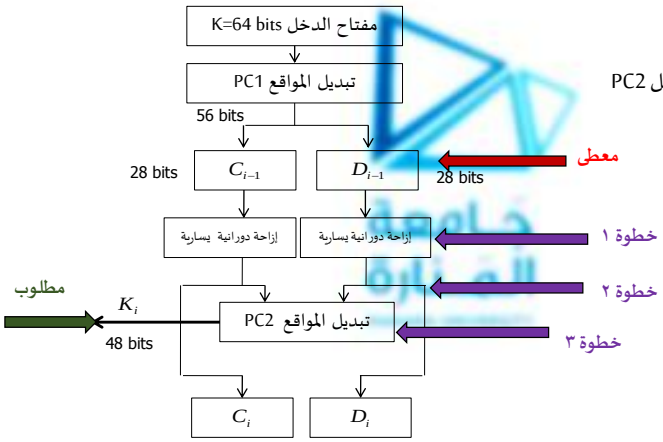
10

من أجل حساب المفتاح الجزئي للحلقة K1 نقوم بالخطوات الآتية:

١. تطبيق الإزاحة الدورانية

٢. لصق الجزأين للحصول على دخل PC2

3. تطبيق جدول التبديل PC2



11

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

الجدول:

رقم الحلقة	1	2	3	4	5 ٥	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 =10111100110100011010010000101**

بعد الإزاحة **C0=11011110011010001101001000010**

قبل الإزاحة **D0=11010010000101110100001111111**

بعد الإزاحة **D0=11101001000010111010000111111**

12

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

C0D0=1101111001101000110100100010111010010001011101000001111111

٣ . نطبق **جدول التبديل PC2**

١. نرقم خانات دخل الجدول من ١ حتى٥٦

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

2. نضع قيم الخانات في جدول PC2

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

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

13

٣.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= 011011000001100100011111011001111010100101110110

14

فيكون دخل صناديق S-BOX :

$$E \oplus K1$$

0 0 0 0 0 0 0 0 1 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 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

٢. خرج الصندوق S-BOX 4 فقط

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

S1 S2 S3 S4 S5 S6 S7 S8

نلاحظ أن دخل الصندوق S-BOX 4 هو 010000

فيكون رقم السطر 0 و رقم العمود8

باستخدام الجدول S-BOX4 يكون الخرج هو

15

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

16

المسألة الثالثة

بفرض لدينا الرسالة M المبينة تالياً تشفر باستخدام خوارزمية التشفير المتناظر DES و بفرض مفتاح الدخل هو K المعطى.

M=0010010101100001000010101010101110111100110010101011110000000001

K=0101100000011111101111001001010011010011101001000101001011101010

المطلوب:

1.احسب L_0,R_0

٢. احسب L_1و R_1 بفرض أن خرج الصناديق S-BOX هو :

10000000011111000001010101000011

٣. أوجد المفتاح الجزئي للحلقة الأولى K1 .

17

عملية معالجة النص الصريح وفق DES

➢ 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

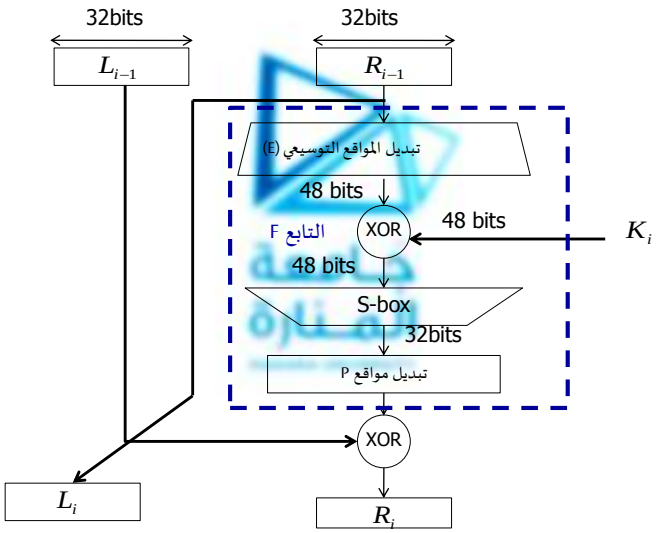
18

L0=00100010010100000101000110001011

R0=01111000010110110111110000101100

19

البنية الداخلية للحلقة الواحدة في DES



20

مراحل تنفيذ التابع F

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 المواقع (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

21

نطبق جدول التبديلP فيكون:

F(R0,K1)= 00100100100100110011100001001100

نطبق $R_1 = L_0 \oplus F(R_0, K_1)$

00100100100100110011100001001100

<u>00100010010100000101000110001011</u>

R1 =00000110110000110110100111000111

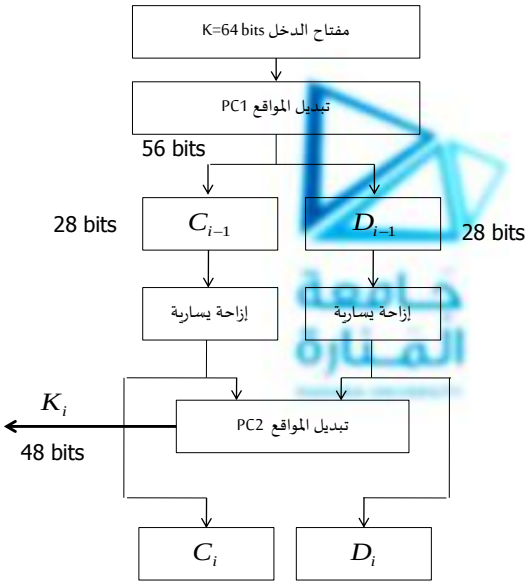
$L_i = R_{i-1} \Rightarrow L1 = R0$

L1= R0=01111000010110110111110000101100

22

عملية توليد المفاتيح الجزئية

❑ مخطط توليد المفتاح الجزئي:



23

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)

24

نطبق خيار التبديل الأول PC1 :

C1=10111100110100011010010000101

D1=11010010000101110100001111111

25

عملية توليد المفاتيح الجزئية

٢. 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

بعد الإزاحة الدورانية نحو اليسار بمقدار خانة واحدة:

C1=11011110011010001101001000010

D1=11101001000010111010000111111

26

عملية توليد المفاتيح الجزئية

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

دخل خيار التبديل الثاني PC2 هو:

C1D1= 11011110011010001101001000101110100100010111010000111111

نطبق خيار التبديل الثاني PC2 :

K1=011011000101100100011111011001111010100101110110

27

المسألة الرابعة

من أجل خوارزمية التشفير المتناظر DES . في حساب التابع f . إذا كان خرج تبديل المواقع التوسيعي E معطى بالشكل:

10 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 00 00

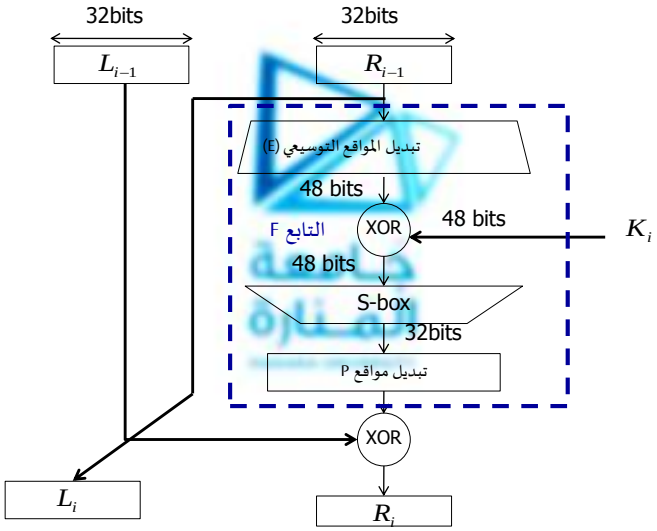
و المفتاح الجزئي للحلقة هو :

1 0 0 0 0 0 1 1 0 0 0 0 1 1 0 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0 1 1 1 0 0 1 1 1 1 0 0 1 1 1 1 0 0 1 1 1 100

المطلوب :احسب خرج الصناديق S (S-box).

28

البنية الداخلية للحلقة الواحدة في DES

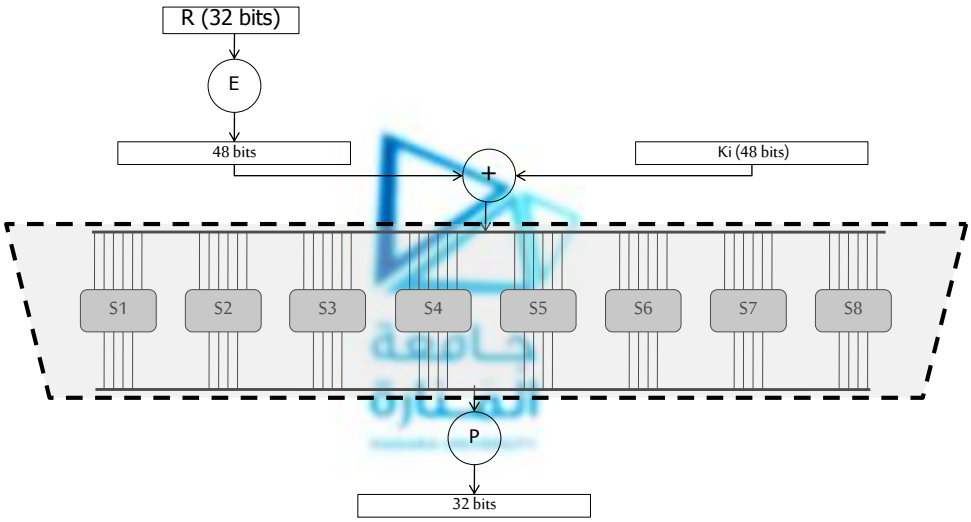


29

من أجل حساب خرج S-box يلزمنا حساب خرج تبديل المواقع التوسيعي E $\oplus K_i$

$$
\begin{array}{l}
100000100000100000100000100000100000100000100000 \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \oplus \\
\underline{100000110000110000111000111000111100111100111100} \\
000000010000010000011000011000011100011\ 1\ 00011100
\end{array}
$$

30



مخطط تنفيذ التابع F

31

نقسم ناتج الجمع كل 6 خانات على حدى لتمثل مدخل أحد الصناديق:

000000	010000	010000	011000	011000	011100	0 11100	0 11 10 0
S1	S2	S3	S4	S5	S6	S7	S8

باستخدام الجداول الخاصة بالصناديق يكون:

الصندوق	S1	S2	S3	S4	S5	S6	S7	S8
دخله	000000	010000	010000	011000	011000	011100	011100	011100
السطر	0	0	0	0	0	0	0	0
العمود	0	8	8	12	12	14	14	14
خرجه	**1110**	**1001**	**0001**	**1011**	**1101**	**0101**	**0110**	**1100**

فيكون خرج S-box :

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

32