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

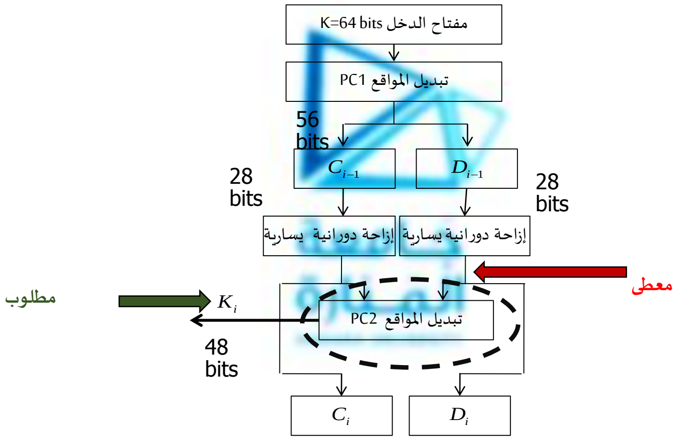
و من أجل الحلقة الأولى إذا كان دخل التبديل الثاني PC2هو:

11111 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 111111 1 1 1 1 00000000000000000000000000 1110

المطلوب:

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

حل المسألة الأولى



حل المسألة الأولى

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

١. حساب المفتاح الجزئي للحلقة الأولى (K1).

١. نرقم خانات دخل جدول PC2 من ١ حتى 56

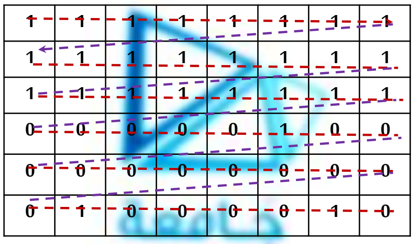
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0

٢. 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	0	1	0	0
0	0	0	0	0	0	0	0
0	1	0	0	0	0	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

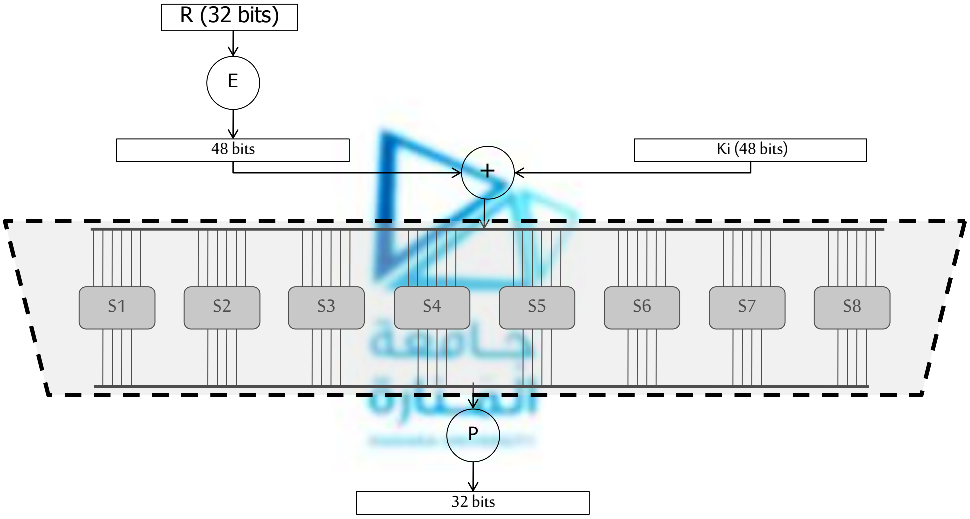
٣. نمسح قيم الجدول بشكل ZGZAG :



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



مخطط تنفيذ التابع F

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

نقسم كل **<u>ست خانات</u>** على حدى ليشكل كل منها مدخل لأحد الصناديق

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 1	0 0 1 1 1 1	1 1 1 1 0 1	0 0 0 0 1 0
S1	S2	S3	S4	S5	S6	S7	S8

7

الخرج الثنائي	القيمة العشرية	رقم العمود	رقم السطر	الدخل	الصندوق
1101	13	15	3	111111	S1
0101	5	8	2	110000	S2
0111	7	1	1	000011	s3
1111	15	8	2	110000	S4
1110	14	0	1	000001	S5
0101	5	7	1	001111	S6
0011	3	14	3	111101	S7
0010	2	1	0	000010	S8

فيكون الخرج هو: 11010101011111111110010100110010

8

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؟

٢. بفرض لدينا ما يلي:

Ci-1=C0 =1011110011010001101001000101

Di-1=D0=1101001000101110100001111111

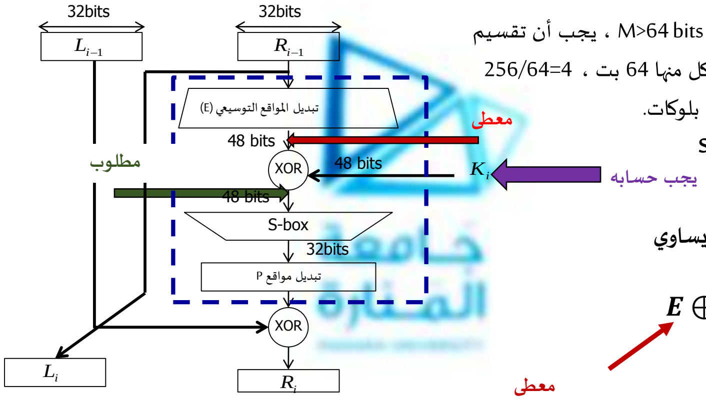
خرج الجدول التوسيعي E :

000000001111111100001111000011110000000011111111

المطلوب: ١. دخل صناديق S-BOX

٢. خرج الصندوق S-BOX 4 فقط

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

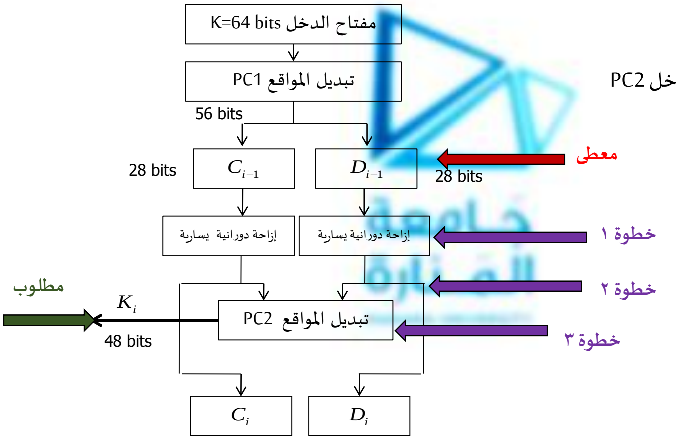
$$\underset{\text{معطى}}{E} \oplus \underset{\text{يجب حسابه}}{K1}$$

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



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

الجدول:

16	15	14	13	12	11	10	9	8	7	6	5 ٥	4	3	2	1	رقم الحلقة
1	2	2	2	2	2	2	1	2	2	2	2	2	2	1	1	التدوير

قبل الإزاحة **C0 =1011110011010001101001000101**

بعد الإزاحة **C0=1101111001101000110100100010**

قبل الإزاحة **D0=1101001000101110100001111111**

بعد الإزاحة **D0=1110100100010111010000111111**

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

C0D0=11011110011010001101001000101110100100010111010000111111

٣. نطبق **جدول التبديل PC2**

١. نرقم خانات دخل الجدول من ١ حتى٥٦

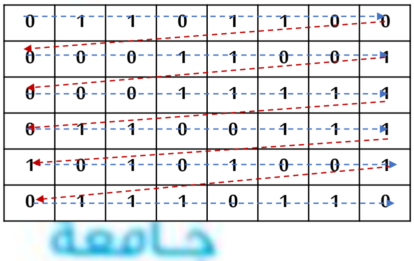
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56
1	1	0	1	1	1	1	0	0	1	1	0	1	0	0	0	1	1	0	1	0	0	1	0	0	0	1	0	1	1	1	0	1	0	0	1	0	0	0	1	0	1	1	1	0	1	0	0	0	0	1	1	1	1	1	1

2. نضع قيم الخانات في جدول PC2

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

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

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

٢. خرج الصندوق S-BOX 4 فقط

S1	S2	S3	S4	S5	S6	S7	S8
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

نلاحظ أن دخل الصندوق S-BOX 4 هو 010000 فيكون رقم السطر 0 و رقم العمود8

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

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 .

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

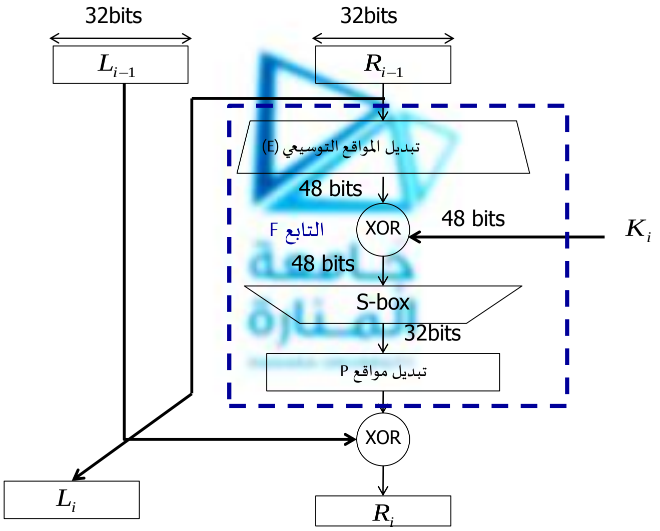
X=IP(M)

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

L0=00100010010100000101000110001011

R0=01111000010110110111110000101100

البنية الداخلية للحلقة الواحدة في DES



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

نطبق جدول التبديلP فيكون:

F(R0,K1)= 00100100100100110011100001001100

نطبق $R_1 = L_0 \oplus F(R_0, K_1)$

00100100100100110011100001001100

<u>00100010010100000101000110001011</u>

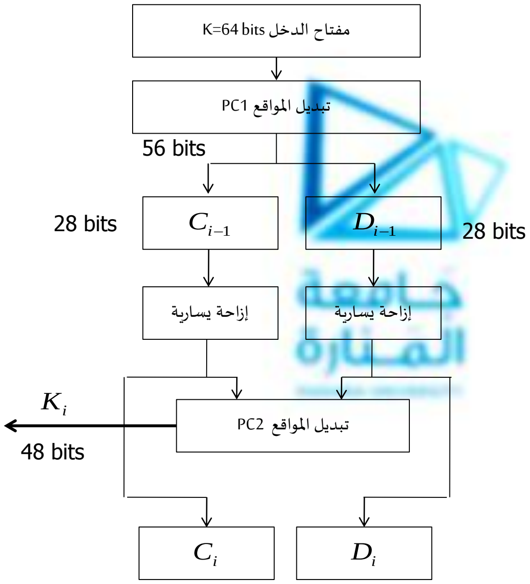
R1 =00000110110000110110100111000111

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

L1= R0=01111000010110110111110000101100

عملية توليد المفاتيح الجزئية

❑مخطط توليد المفتاح الجزئي:



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

$;16 \geq i \geq 1$ D_{i-1}, C_{i-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)

نطبق خيار التبديل الأول PC1 :

C1=1011110011010001101001000101

D1=1101001000101110100001111111

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=1101111001101000110100100010

D1=1110100100010111010000111111

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

المسألة الرابعة

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

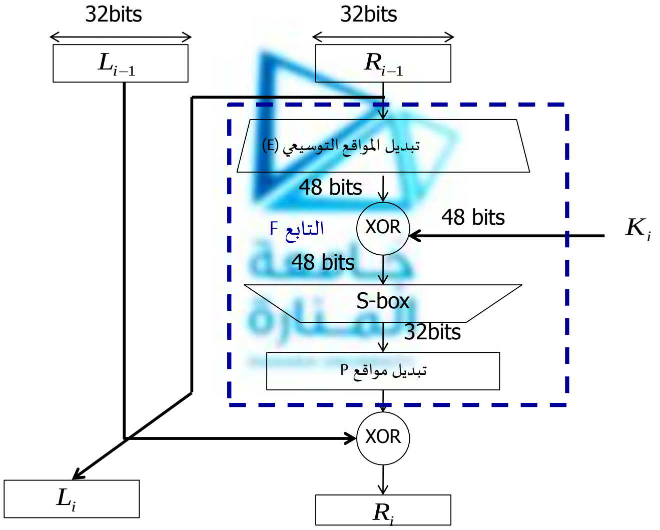
10 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 10 00 00

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 01 1 1 1 0 0 1 1 1 1 0 0 1 1 1 100

المطلوب :احسب خرج الصناديق S (S-box).

البنية الداخلية للحلقة الواحدة في DES



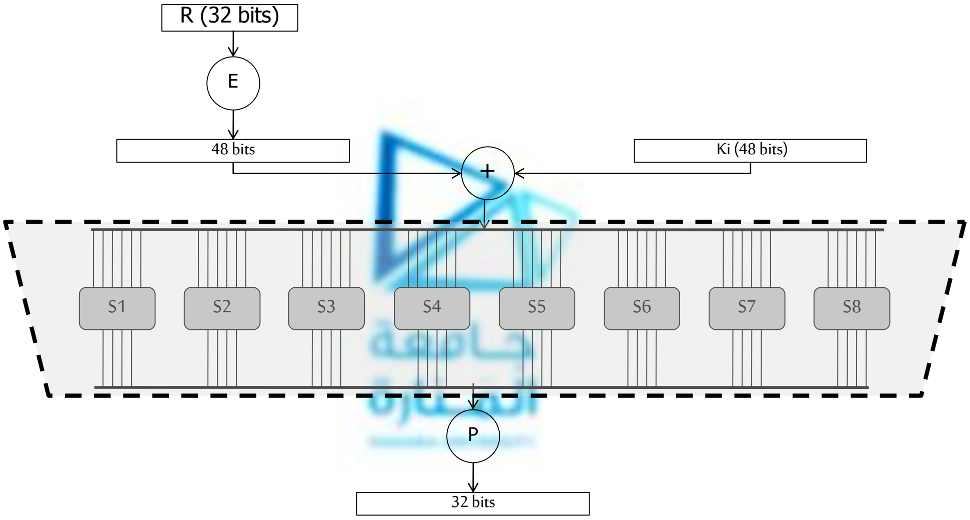
من أجل حساب خرج S-box يلزمنا حساب خرج تبديل المواقع التوسيعي E $K_i \oplus$

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 0 0 0 0 00

$\oplus$

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

0 0 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 11 0 0 0 0 1 1 0 0 0 0 1 1 1 0 0 0 1 1 1 0 0 0 11 100



مخطط تنفيذ التابع F

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