

Information System Security

أمن نظم المعلومات

مدرسة المقرر
د. بشرى علي معلا

عناوين المحاضرة الخامسة

- مقدمة عن Feistel cipher
- مخطط مقياس تسمية المعطيات (DES(Data Encryption Standard)
- ✓ الشكل العام للخوارزمية
- ✓ المراحل العامة لعملية التسمية
- ✓ المراحل العامة لعملية معالجة النص الصريح

مقدمة عن Feistel Cipher

❖ تمتلك خوارزميات التشفير الكتلي التقليدية هيكلية وصفت لأول مرة من قبل Horst Feistel من IBM عام ١٩٧٣. ➤ تعتمد على بارامترات التصميم الآتية:

✓ طول البلوك / الكتلة (Block Size) ✓
كلما كان طول الكتلة و طول المفتاح أكبر كلما كان مستوى الأمن أعلى
✓ طول المفتاح (Key Size)

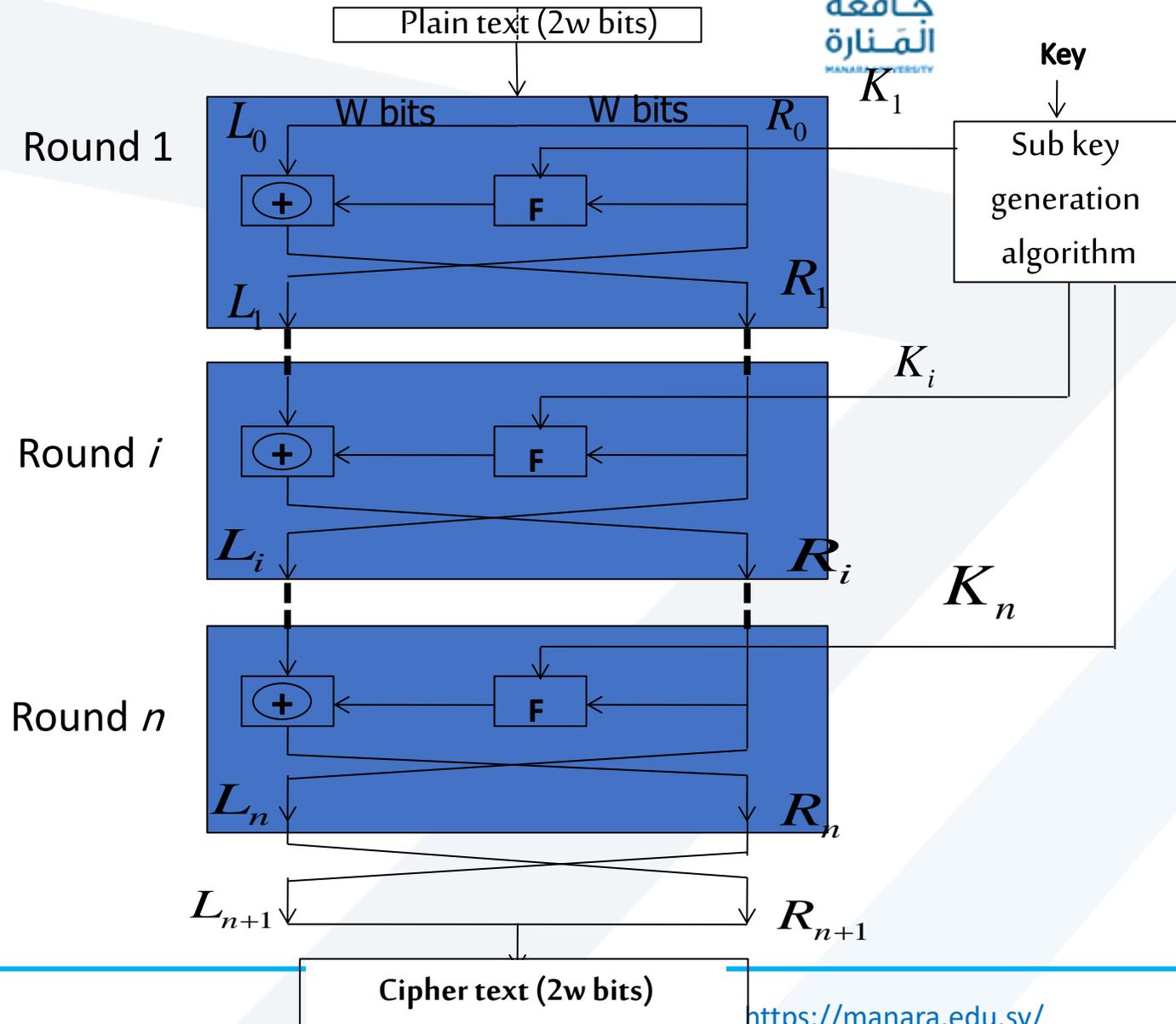
✓ عدد الحلقات (Number of rounds): يزيد استخدام الدورات المتعددة من مستوى الأمن

✓ 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 Software Encryption /Decryption): وهي تخص سرعة تنفيذ الخوارزمية التي تظهر أهميتها عند تضمين التعمية في التطبيقات العملية.



الشكل العام لشبكة Feistel



خطوات عمل Feistel Chiper

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

➤ خطوات العمل:

✓ يقسم كتلة النص الصريح إلى نصين L_0, R_0 .

✓ يمر هذان النصفان من خلال n حلقة معالجة.

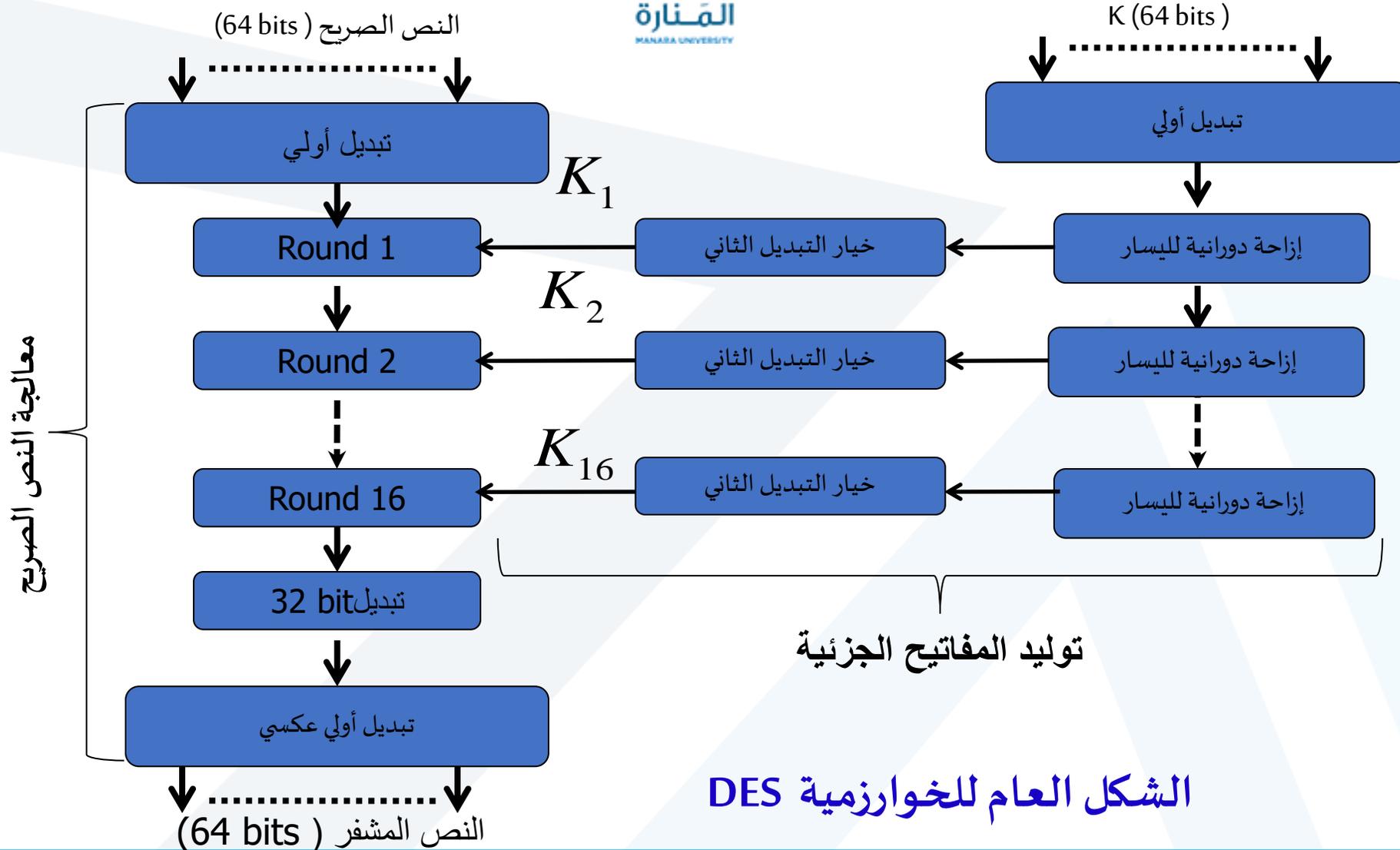
✓ في النهاية يضم هذان النصفان لإنتاج النص المشفر.

✓ تكون المفاتيح الجزئية مختلفة عن بعضها البعض و عن المفتاح الأساسي K .

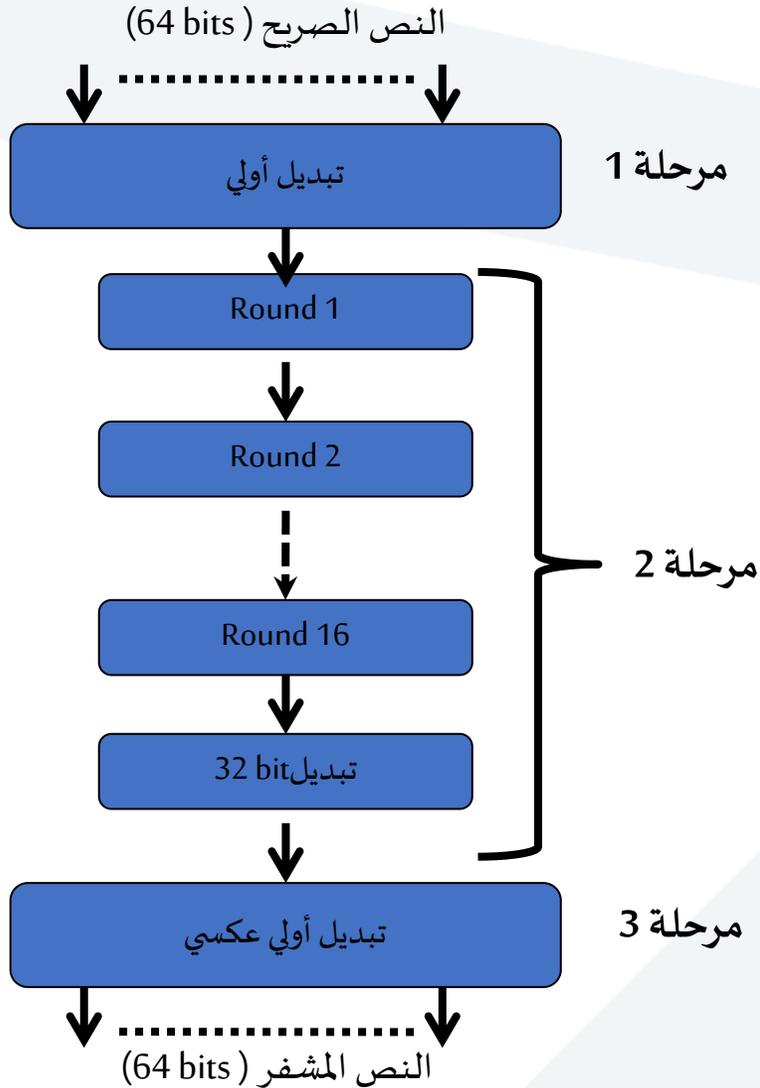
✓ تتم عملية فك التشفير اعتماداً على نفس عملية التشفير ولكن مع عكس ترتيب المفاتيح أي $K_n \rightarrow K_1$

خوارزمية معيار تشفير المعطيات DES(Data Encryption Standard)

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



عملية معالجة النص الصريح:



❖ تشمل عملية المعالجة ثلاث مراحل أساسية:

✓ **مرحلة 1:** تبدل مواقع أولي (IP (Initial Permutation)

✓ **مرحلة 2:** مكونة من 16 حلقة تشمل تابعين:

١. تابع تبدل حروف

٢. تابع تبدل مواقع

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

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

عملية معالجة النص الصريح وفق DES (1/3)

➤ مرحلة 1: عملية التبدل الأولي (IP):

✓ تنفذ عملية التبدل الأولي :

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

فتكون الغاية من عملية التبدل هي إعادة ترتيب
البتات وفق الجدول المجاور:

| | | | | | | | | |
|----|----|----|----|----|----|----|----|---|
| 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 |

$$X=IP(M)$$

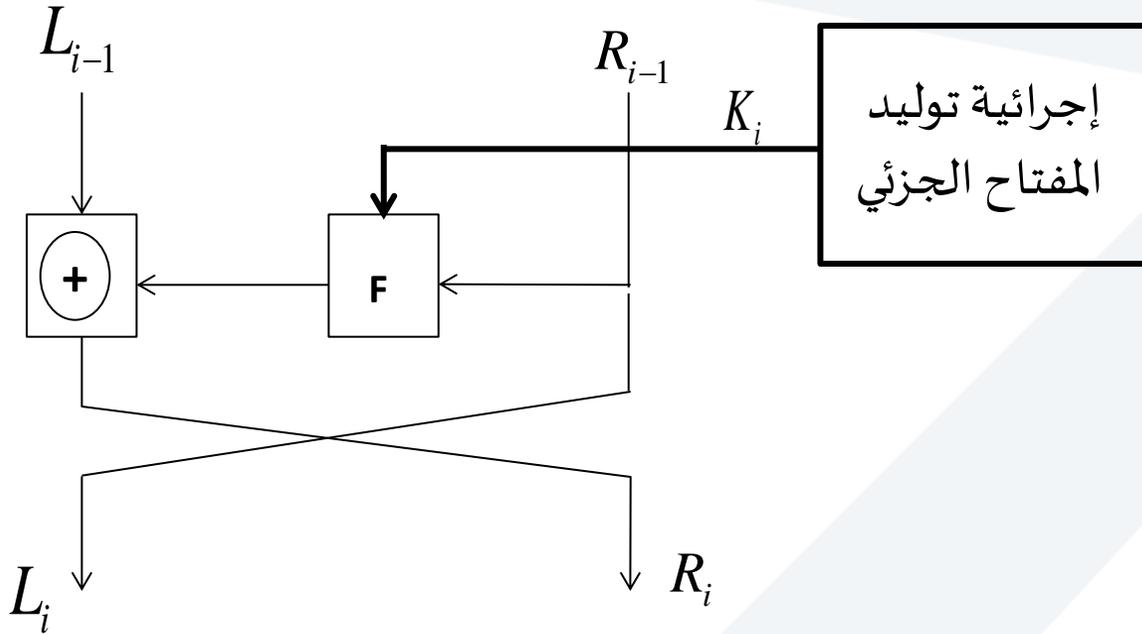
عملية معالجة النص الصريح وفق DES (2/3)

➤ مرحلة 2 : تقسم إلى جزأين

١. تنفيذ الـ 16 حلقة: سندرس البنية الداخلية للحلقة

٢. التبدل 32bits : هي تبدل نصفي الخرج مع بعضهما أي جعل الجزء اليساري يميني وبالعكس

البنية الداخلية للحلقة الواحدة في DES (1/4):

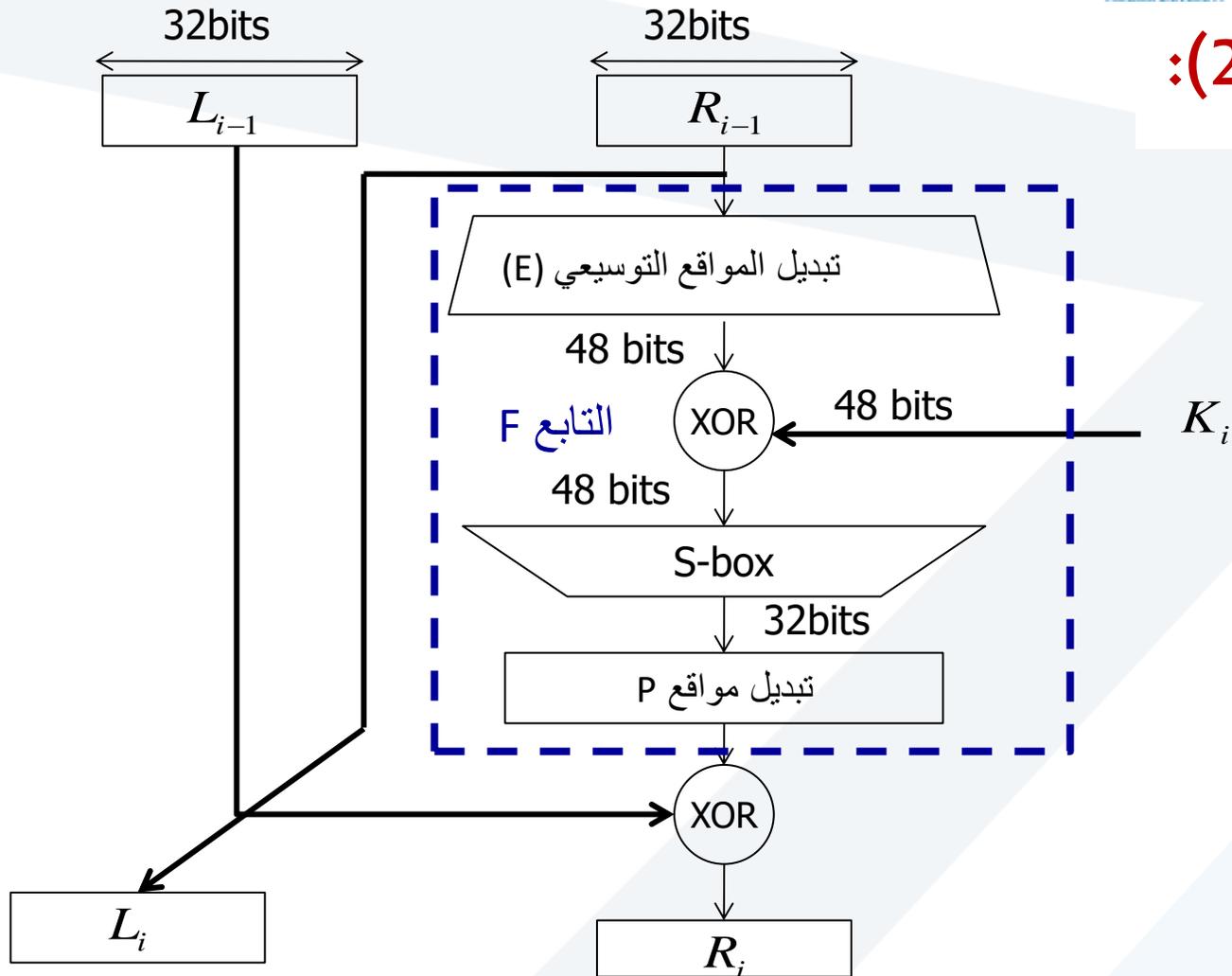


يعبر عن عملية المعالجة كما يلي:

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

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

البنية الداخلية للحلقة الواحدة في DES (2/4):



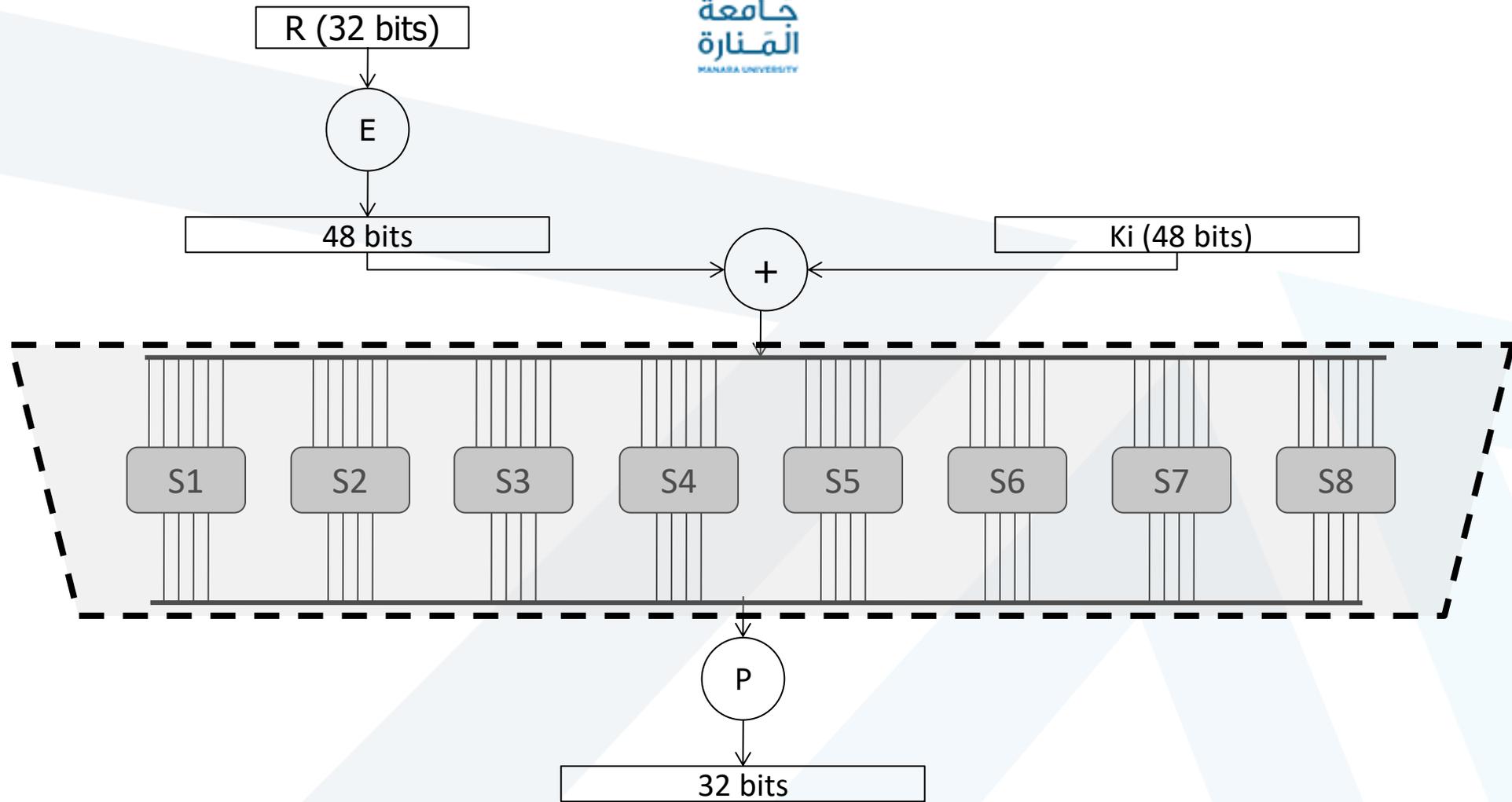
البنية الداخلية للحلقة الواحدة في DES (3/4):

✓ 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)

| | | | | | |
|----|----|----|----|----|----|
| 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 |

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

حيث تكرر 16 خانة من خانات الدخل R

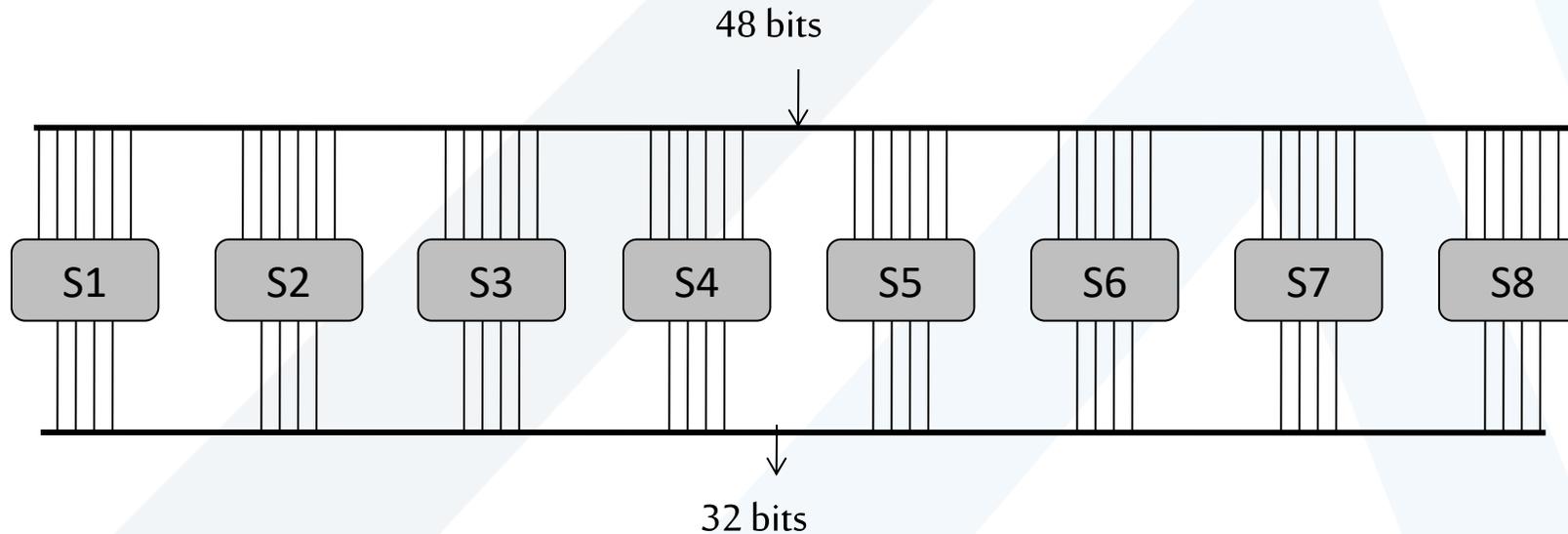
جدول تبديل المواقع التوسيعي (E)

مراحل تنفيذ التابع F (2/3)

٢. تجمع R الموسعة مع المفتاح الجزئي باستخدام بوابة XOR، فيكون الناتج مكون من 48 خانة .

٣. 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.



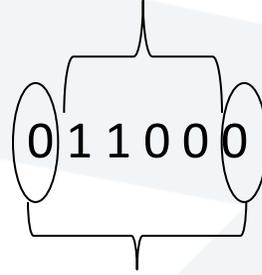
آلية عمل الصندوق Si :

- 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



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)

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

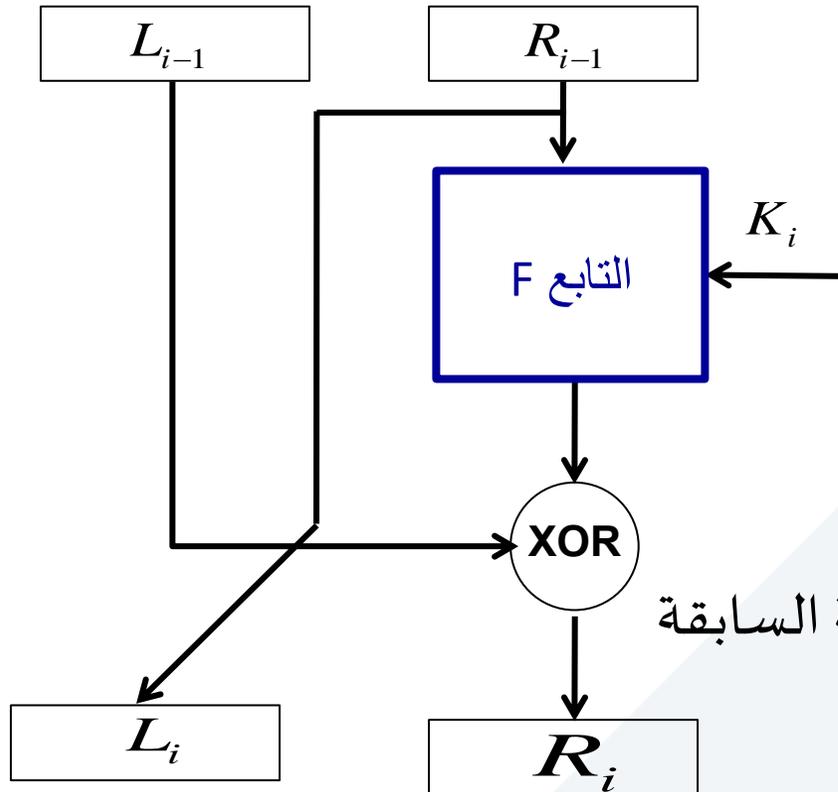
| | | | | | | | |
|----|----|----|----|----|----|----|----|
| 16 | 7 | 20 | 21 | 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 | 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 | 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 | 22 | 11 | 4 | 25 |

جدول تبديل المواقع (P)

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 أن 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 R_i من دخل الحلقة التالية

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

✓ 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 التبدل العكسي للتبدل الأولي (IP^{-1}) :
تنفذ 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 |

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

الجداول الملحقه

جدول التبدیل الأولی IP

| | | | | | | | | |
|----|----|----|----|----|----|----|----|---|
| 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 |

جدول التبدیل الأولی العکسی IP^{-1}

| | | | | | | | |
|----|---|----|----|----|----|----|----|
| 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 |

جدول التوسيع E

| | | | | | |
|----|----|----|----|----|----|
| 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 |

| 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 |

نهاية المحاضرة