信息安全导论

现代密码学原理与实践

第5讲：数据加密标准(1)

- 重庆大学大数据与软件学院

- 开课时间：2025年秋季

课程回顾

Horst Feistel

Whitfield Diffie

.....

1958~1978

2001

密歇根大学 → 麻省理工 → 普林斯顿高等研究院 → 贝尔实验室 → **麻省理工**

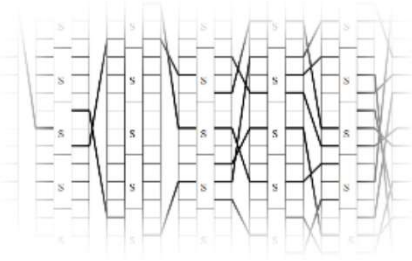
课程回顾

- **IBM与密码相关的发展历程**

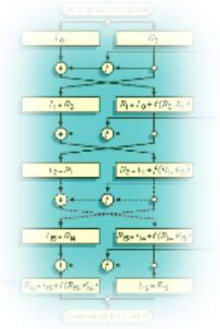
IBM701

IBM7950：收割者

IBM S-370



IBM Lucifer密码模块



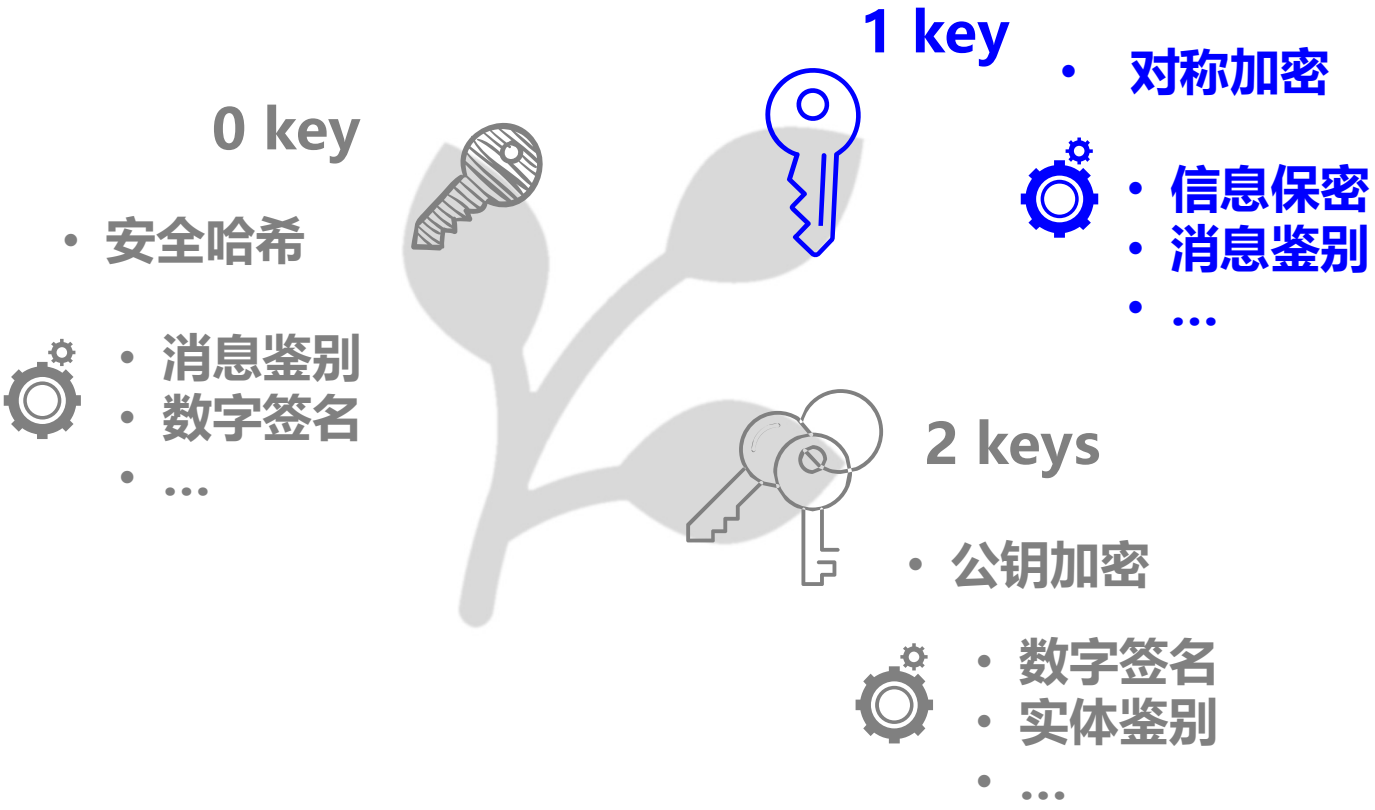
美国国家标准DES

1950年 朝鲜战争爆发 → 1958年 NSA专用机 → 1970年 大型商用机 → 1973年 IBM密码模块 → 1975年 第一代商密

目录 | CONTENTS

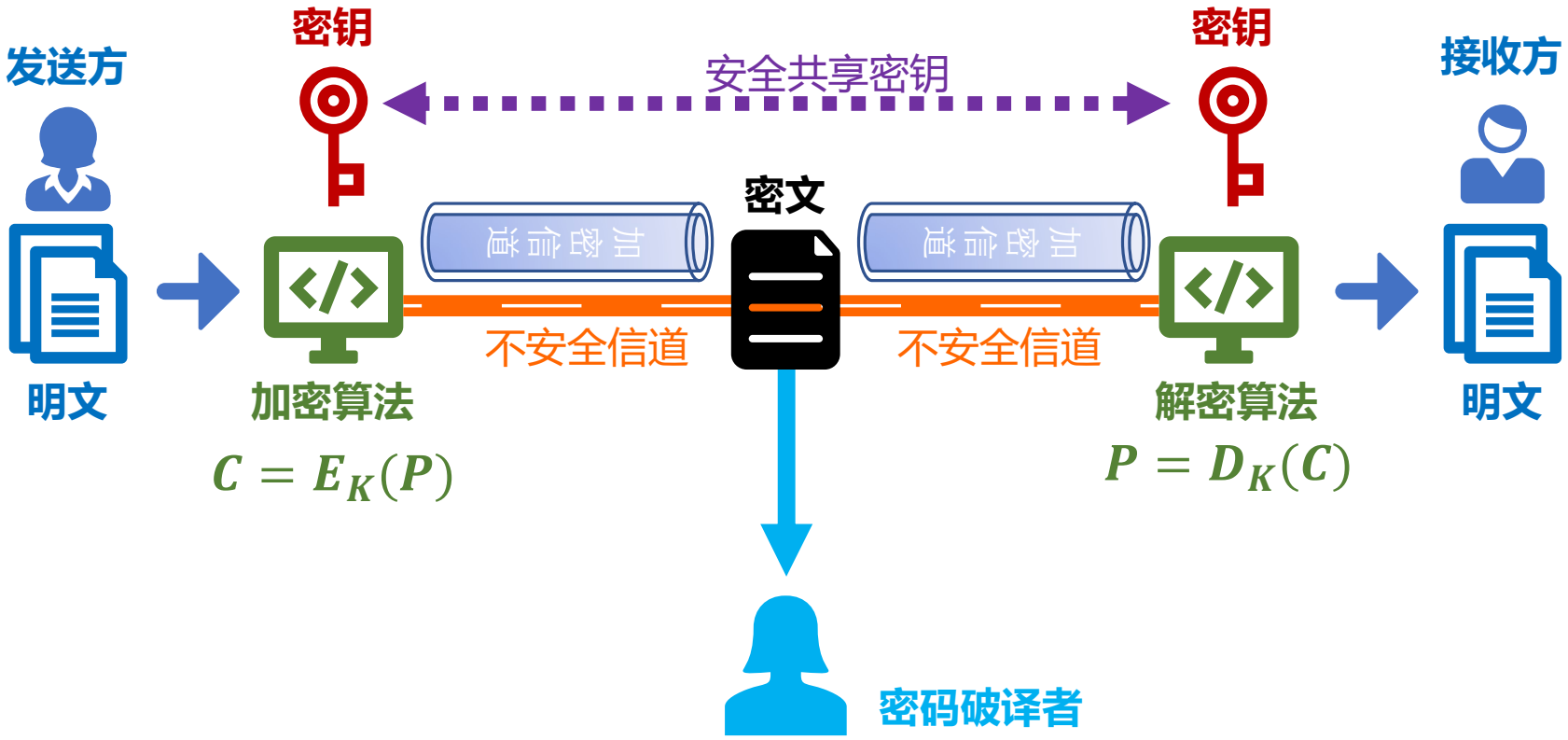
1 对称分组加密：基本概念

- **现代密码学：三足鼎立**



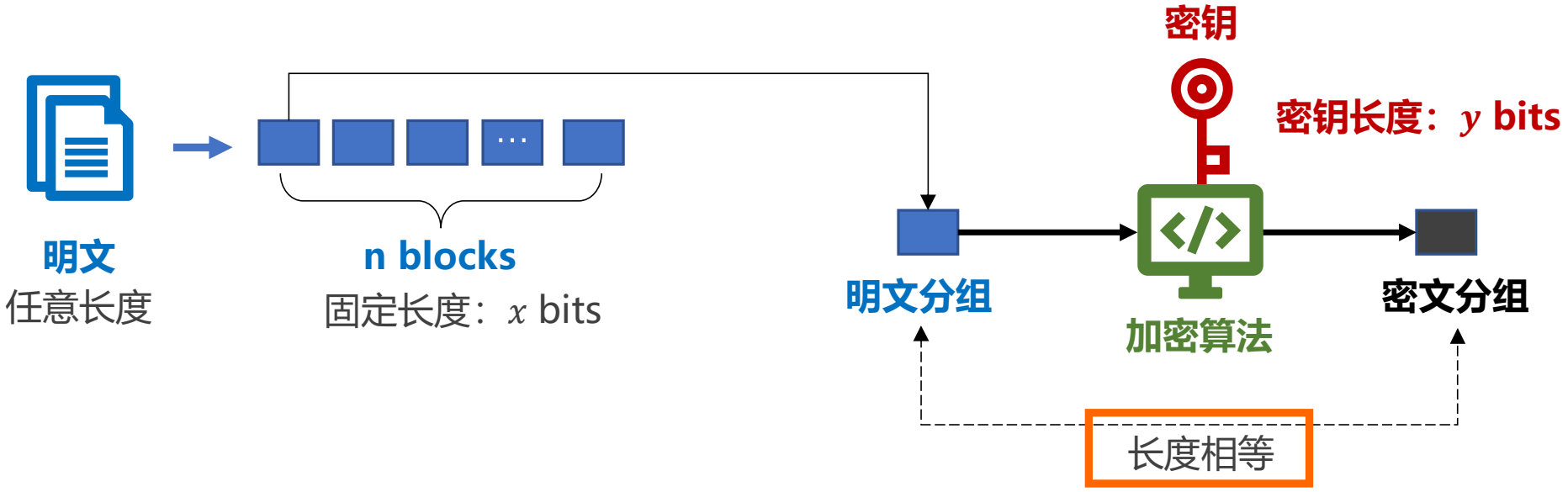
1 对称分组加密：基本概念

- **对称加密：基本模型**



1 对称分组加密：基本概念

- **对称加密：分组加密（Block Cipher）**



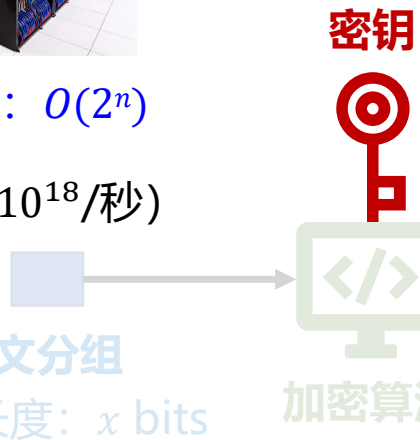
1 对称分组加密：基本概念

- **对称加密：分组加密**
  - **密钥长度：**
    - 密钥空间$|\mathcal{K}|$越大，能更好地抵御蛮力破解(攻击)：$O(2^n)$
    - 以2023年排名第一的超级计算机Frontier为例（10^{18}/秒）

y 的取值：

16 bits:	纳秒级
32 bits:	微秒级
64 bits:	秒级
128bits:	~10^{12} 年

2023年世界排名第1的超级计算机Frontier，美国橡树林国家实验室

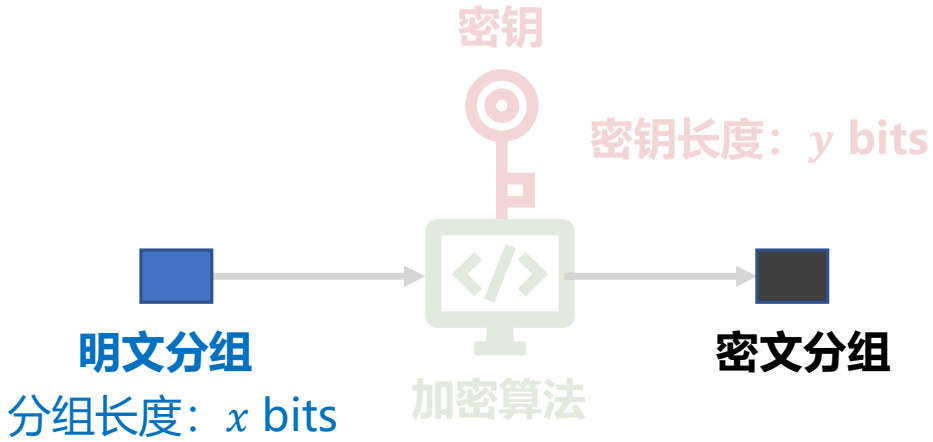


印度裔美籍数学家 Lov Grover

如果未来十年大规模量子计算机研发成功
密钥空间为2^{128}又被秒破，需升级到2^{256}

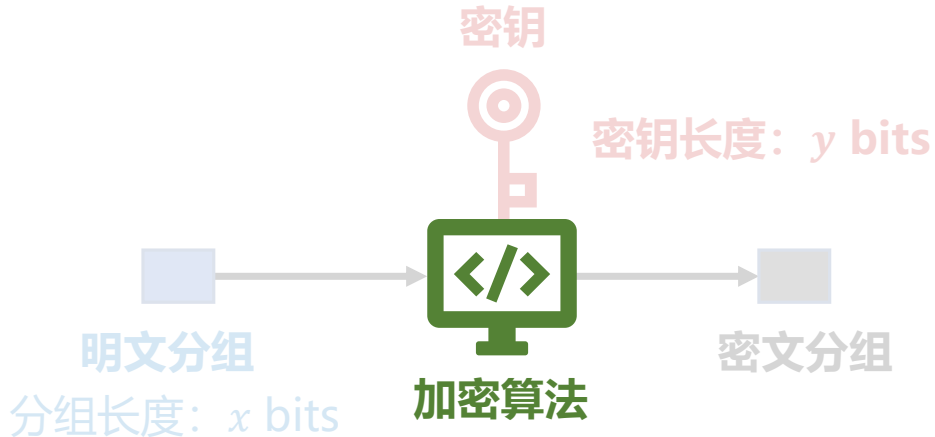
1 对称分组加密：基本概念

- **对称加密：分组加密**
  - 密钥长度：
  - **分组长度：**
    - 例如：64/128+ bits



1 对称分组加密：基本概念

- **对称加密：分组加密**
  - 密钥长度：128+ bits
  - 分组长度：64/128+ bits
  - **加密算法：**
    - 根据香农理论
      - **混合变换 (mix transformation)**
      - **乘积密码 (product cipher)**
      - **置换替换网络 (SPN)**
      - **多轮迭代 (multiple rounds)**



1 对称分组加密：基本概念

- **对称加密：分组加密**

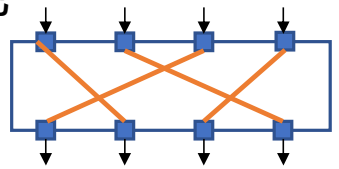
- **加密算法：选用和组合多种转换机制**

  - **置换**
  - **替换**
  - **异或**
  - **移位**
  - **分割**
  - **轮换**

1 对称分组加密：基本概念

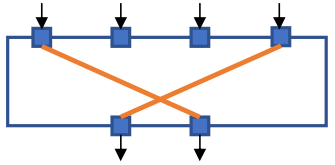
- **对称加密：分组加密**
  - **常用的转换机制**
    - **置换**
    - 替换
    - 异或
    - 移位
    - 分割
    - 轮换

- 交换分组中单位数据的位置来实现转换
- 通常使用置换盒(P-Box)来实现
  - 直接置换（可逆）



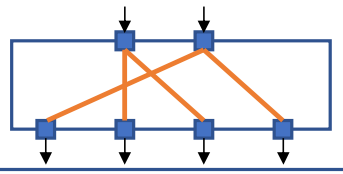
(3, 1, 4, 2)

  - 压缩置换（不可逆）



(1, 4)

  - 扩展置换（不可逆）



(2, 1, 1, 2)

1 对称分组加密：基本概念

- **对称加密：分组加密**
  - **常用的转换机制**
    - 置换
    - **替换**
    - 异或
    - 移位
    - 分割
    - 轮换

- 分组中单位数据的被替换成其他数据
- 通常使用替换盒(S-Box)来实现
  - e.g. 1

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \qquad \begin{cases} y_1 = x_1 \oplus x_2 \oplus x_3 \\ y_2 = x_1 \end{cases}$$

  - e.g. 2

左侧2比特

左侧1比特	00	01	10	11
0	00	10	01	11
1	10	00	11	01

110 → 11
001 → 10

1 对称分组加密：基本概念

- **对称加密：分组加密**
  - **常用的转换机制**
    - 置换
    - 替换
    - **异或**
    - 移位
    - 分割
    - 轮换

- 异或运算是加密算法中常用的算子
- 异或运算真值表

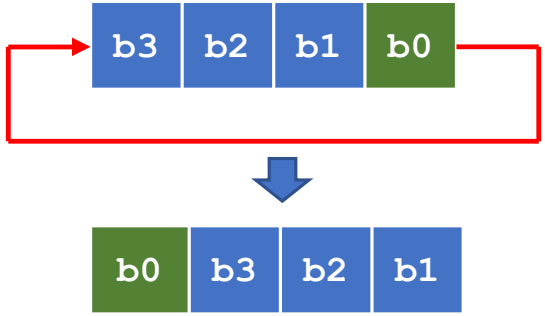
XOR	0	1
0	0	1
1	1	0

  - 提问：$A \oplus B \oplus B = ?$

1 对称分组加密：基本概念

- **对称加密：分组加密**
  - **常用的转换机制**
    - 置换
    - 替换
    - 异或
    - **移位**
    - 分割
    - 轮换

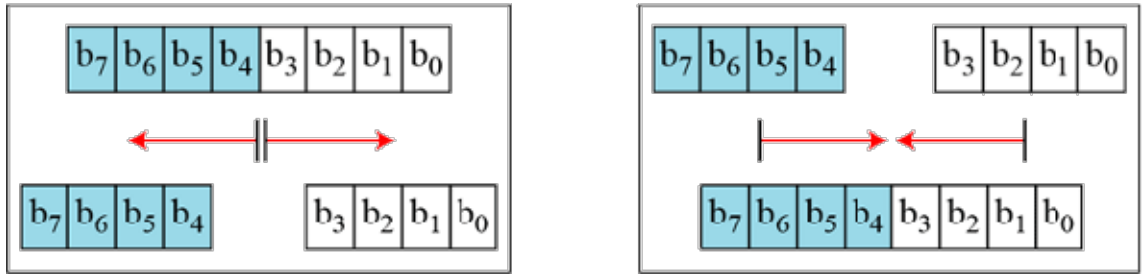
- 通常称之为循环移位
  - 水平方向：circular shift
  - 垂直方向：rotate
  - e.g.,



1 对称分组加密：基本概念

- **对称加密：分组加密**
  - **常用的转换机制**
    - 置换
    - 替换
    - 异或
    - 移位
    - **分割**
    - 轮换

- 将数据分组分割成相等的2份(或4份)
- 分别进行不同类型的转换，然后再合并
  - e.g.,

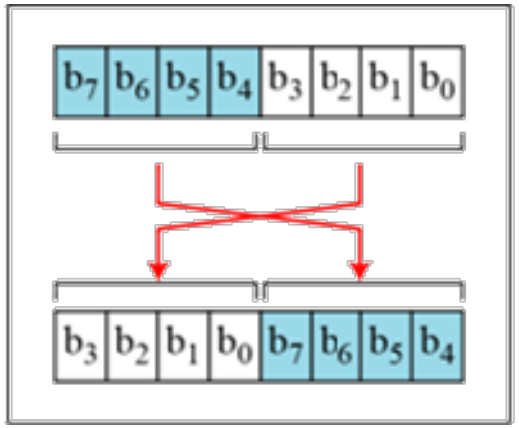


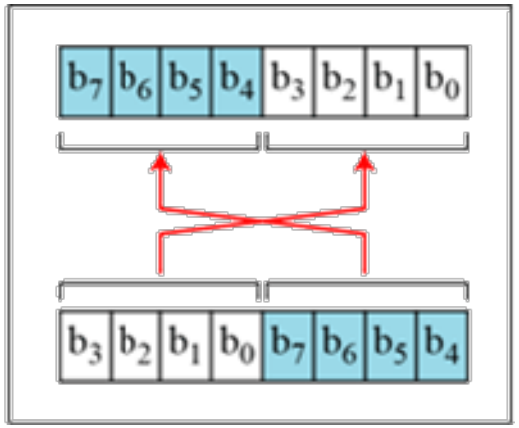
Split **Combine**

1 对称分组加密：基本概念

- **对称加密：分组加密**
  - **常用的转换机制**
    - 置换
    - 替换
    - 异或
    - 移位
    - 分割
    - **轮换**

- 数据分组分割之后，可能进行交换(swap)

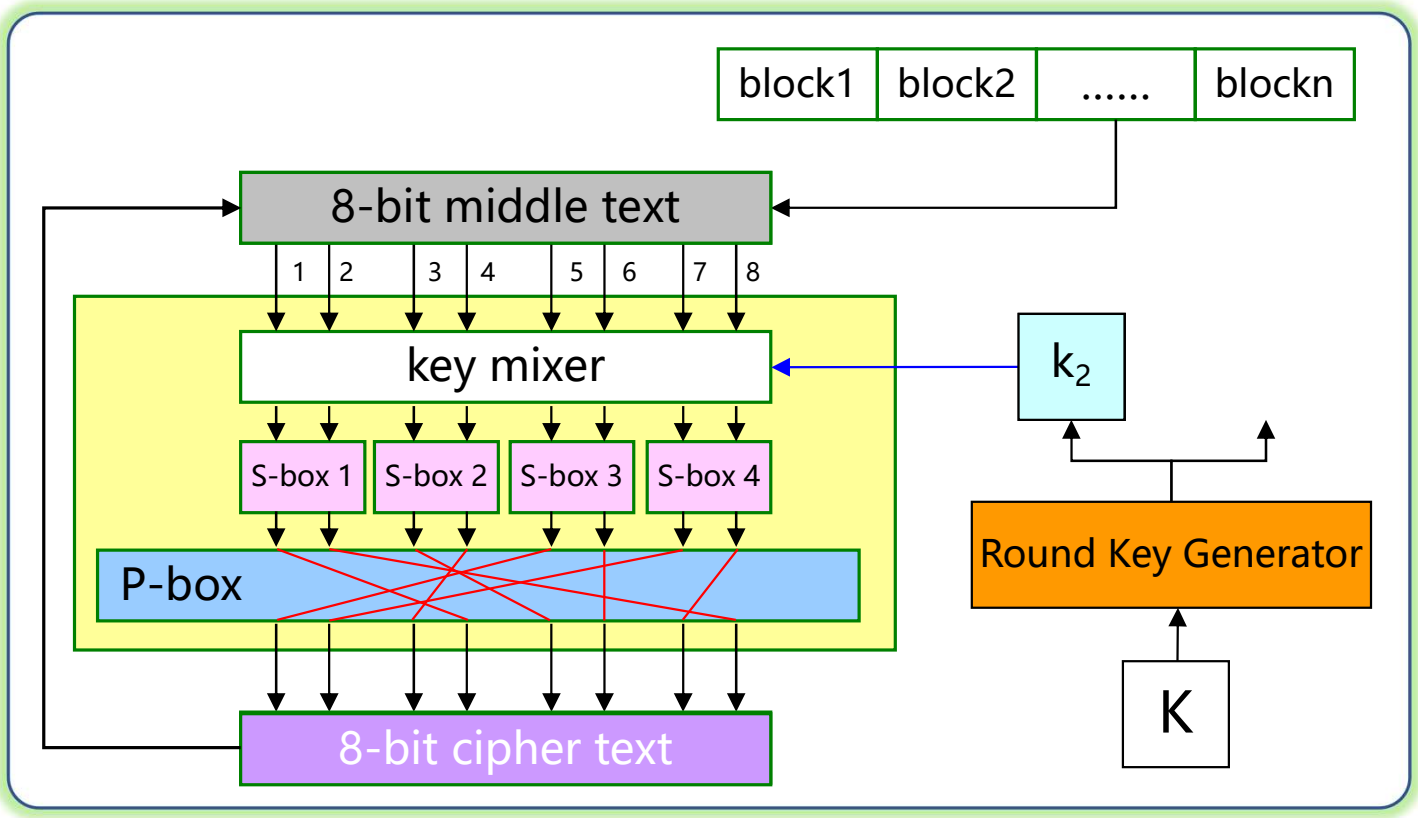




1 对称分组加密：基本概念

- **对称加密：分组加密**
  - 常用的转换机制
  - **乘积密码的示例**
    - **S-P组合变换**

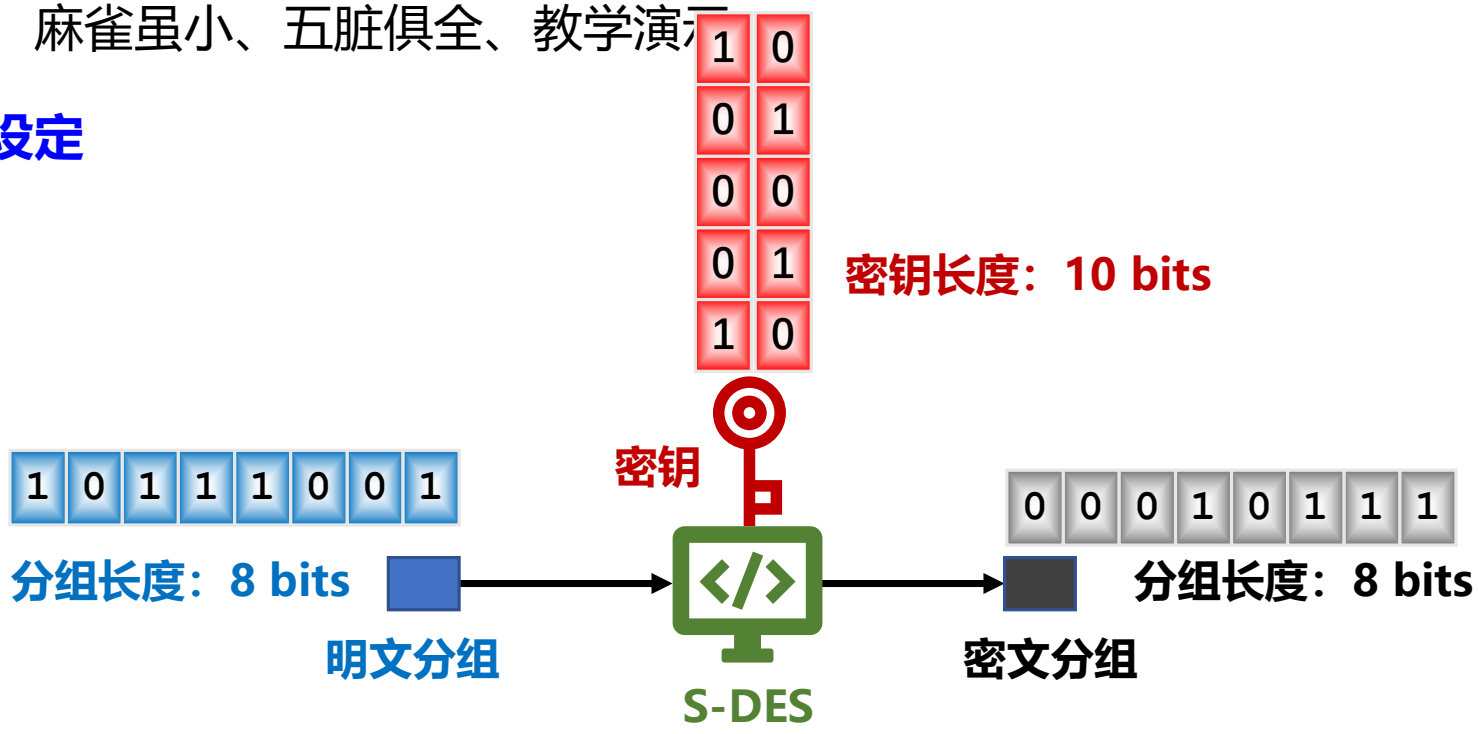
Round 2



目录 | CONTENTS

3 数据加密标准：S-DES

- **简化的数据加密标准： S-DES**
  - 动机：麻雀虽小、五脏俱全、教学演示
  - **基本设定**



3 数据加密标准：S-DES

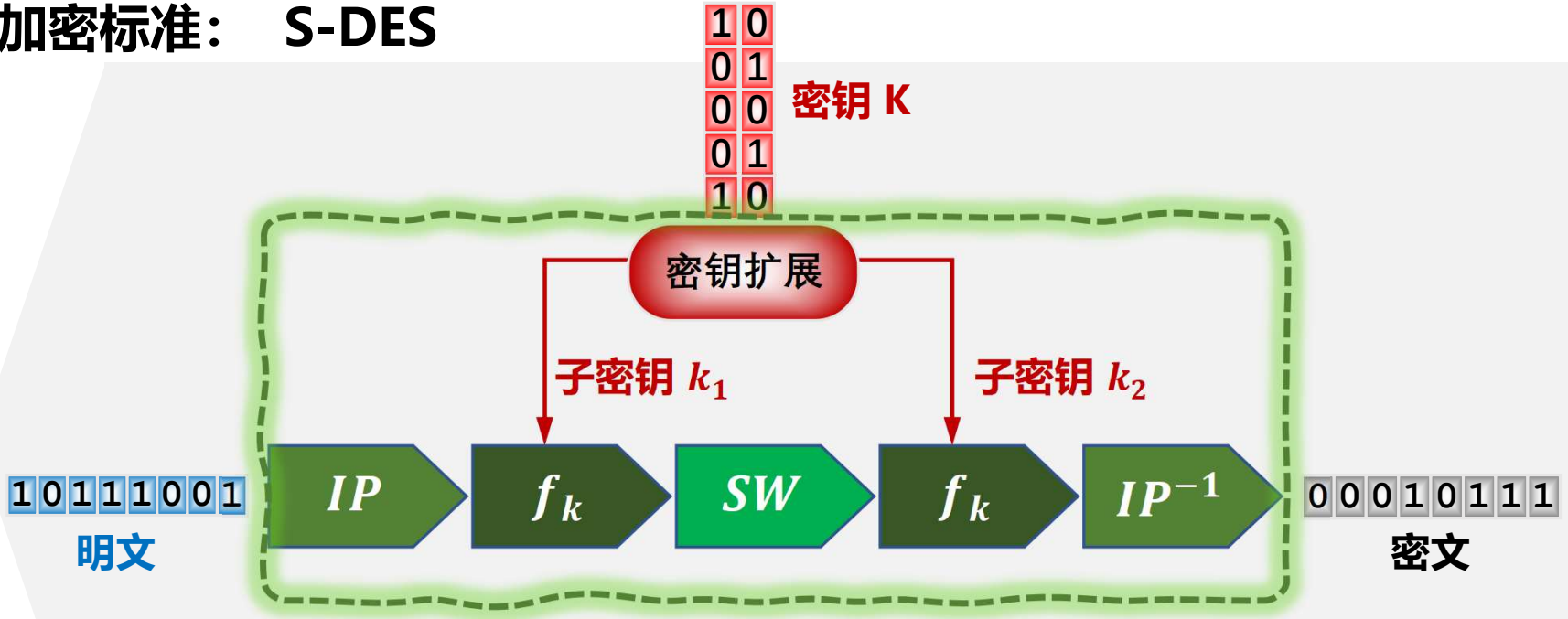
- **简化的数据加密标准： S-DES**
  - 基本设定
  - **加密机制**

IP	初始置换，Initial Permutation
f_k	S-DES 加密函数
SW	交换/轮换，Swap
IP^{-1}	最终置换，是初始置换的逆运算

3 数据加密标准：S-DES

- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - **算法流程**

S-DES
加密过程

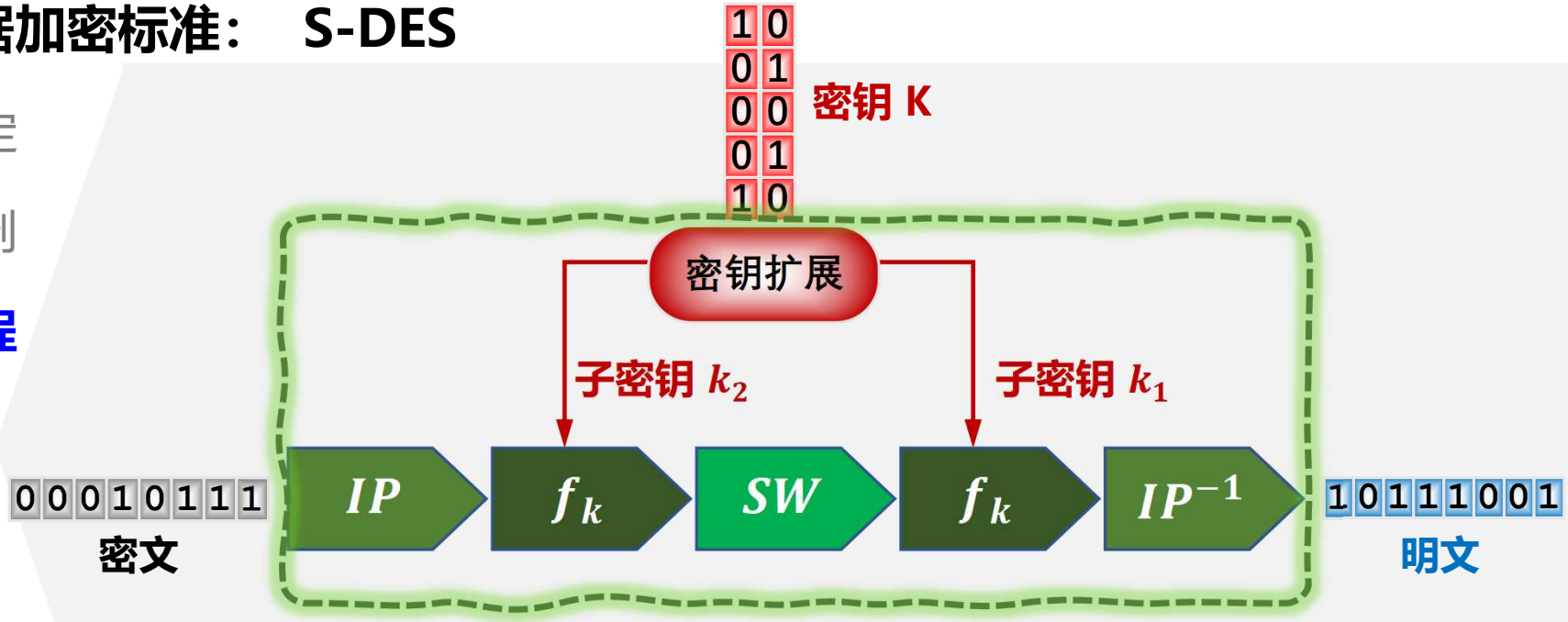


$$C = IP^{-1}(f_{k_2}(SW(f_{k_1}(IP(P)))))$$

3 数据加密标准：S-DES

- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - **算法流程**

S-DES
解密过程



$$P = IP^{-1}(f_{k_1}(SW(f_{k_2}(IP(C)))))$$

3 数据加密标准：S-DES

- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - 算法流程
  - **详细步骤**

- **密钥生成**
  - **密钥 K:**
    - 随机生成器获取
    - 长度为 10bits
    - 通讯双方事先密钥共享

1	0
0	1
0	0
0	1
1	0

3 数据加密标准：S-DES

- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - 算法流程
  - **详细步骤**

- **密钥生成**
  - 密钥 K
  - **子密钥 k_i**
    - 由密钥K 进行扩展
    - 用于S-DES函数的输入
    - 长度为8 bits

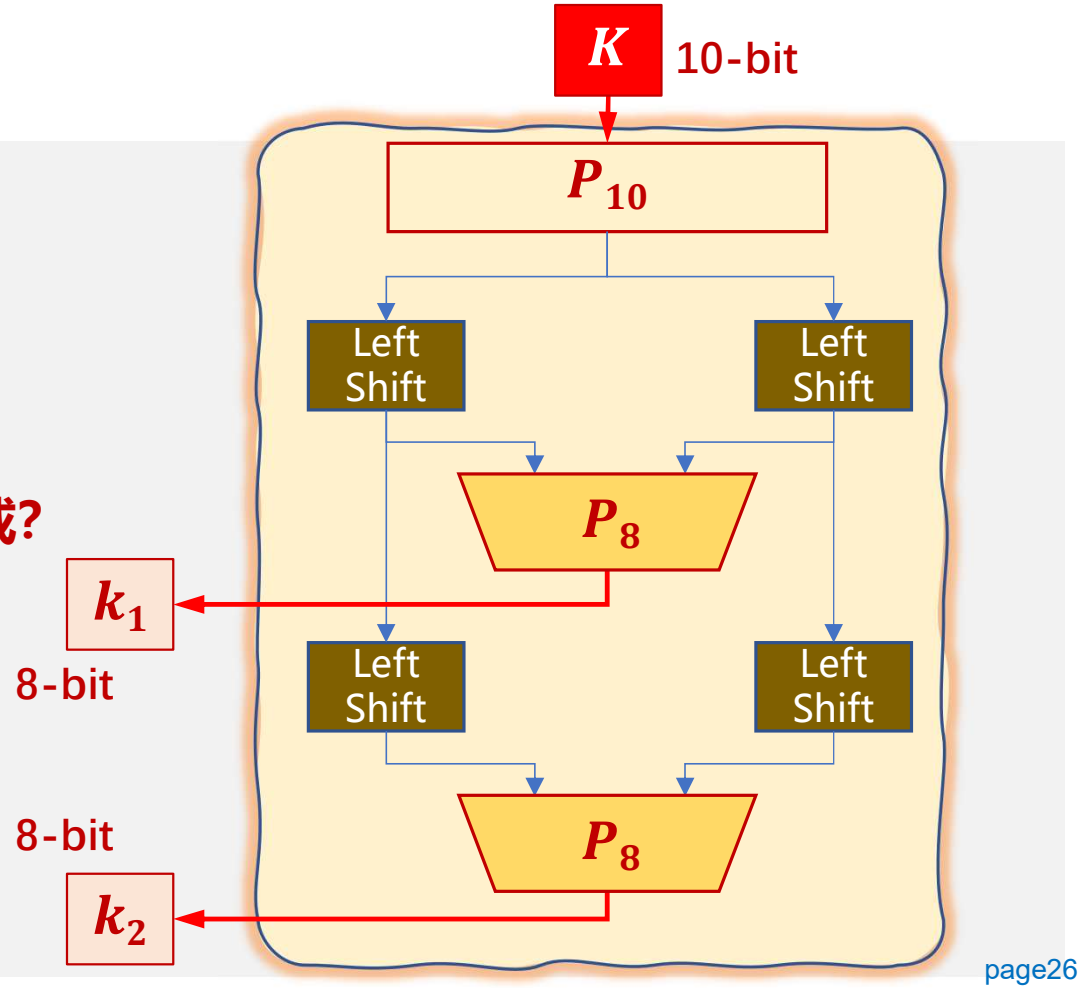
k_i

1	0
0	0
0	0
1	1

3 数据加密标准：S-DES

- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - 算法流程
  - **详细步骤**

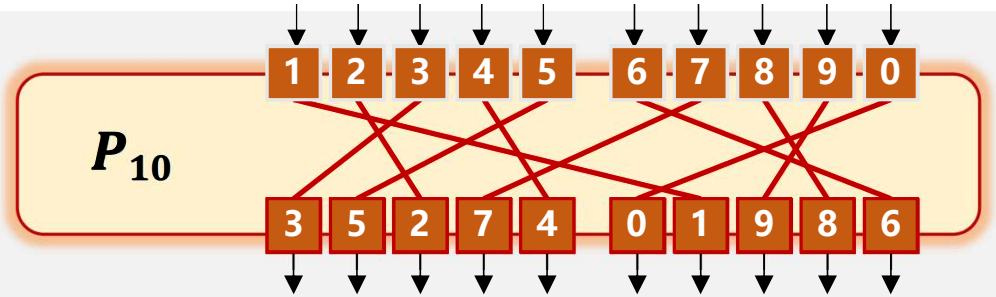
- **密钥生成**
  - 密钥 K
  - **子密钥 k_i**
    - **如何生成?**

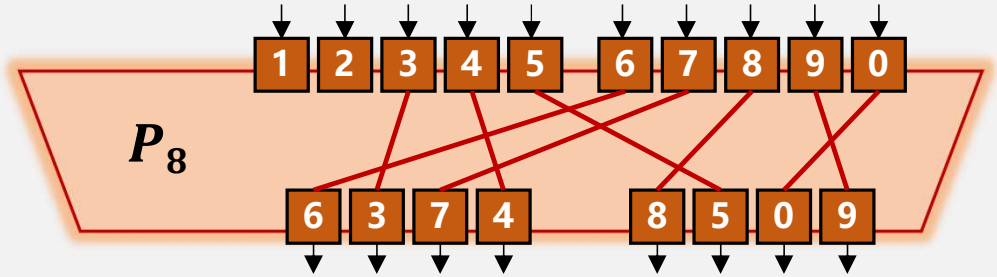


3 数据加密标准：S-DES

- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - 算法流程
  - **详细步骤**

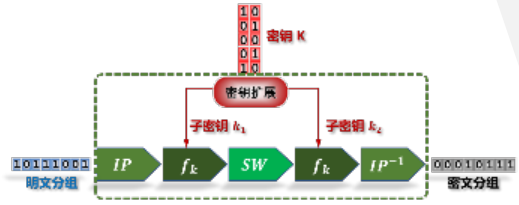
- **密钥生成**
  - 密钥 K
  - **子密钥 k_i**
    - 如何生成?
    - **两个P-Box**



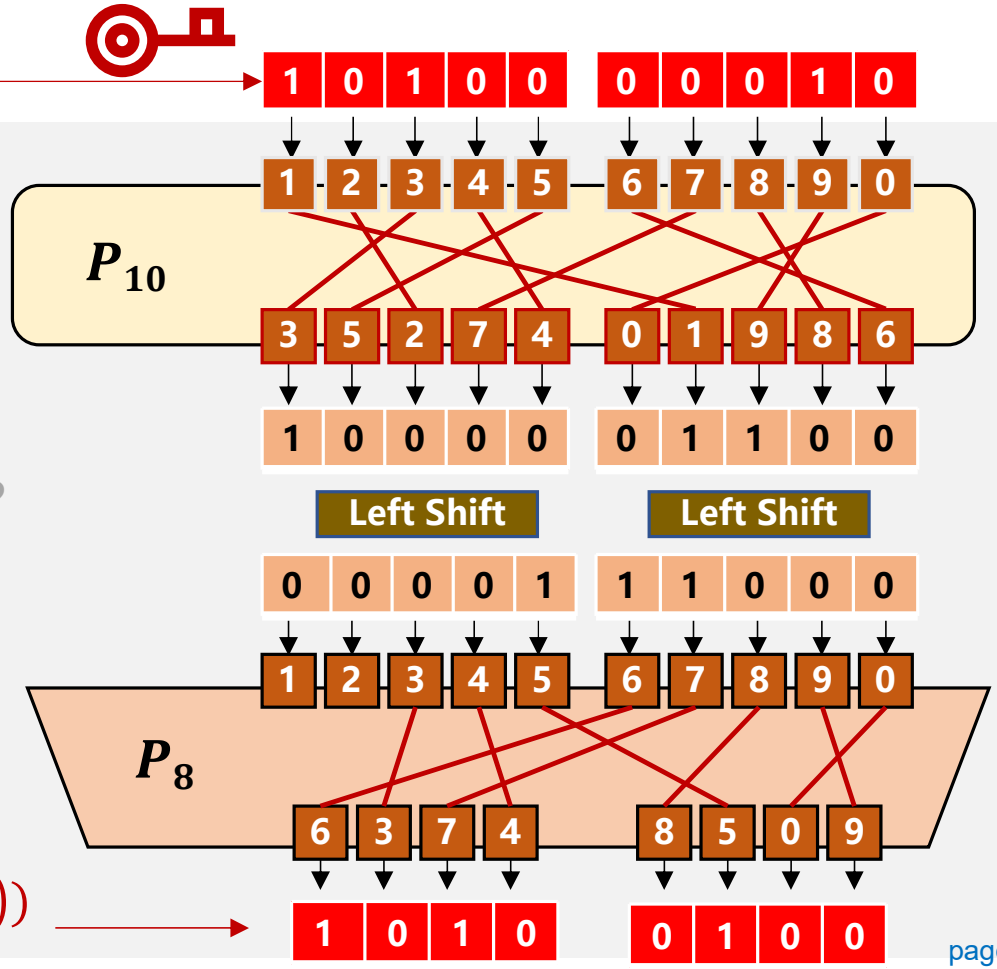


3 数据加密标准：S-DES

- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - 算法流程
  - **详细步骤**



- **密钥生成**
  - 密钥 K
  - **子密钥 k_i**
    - 如何生成?
    - **示例**



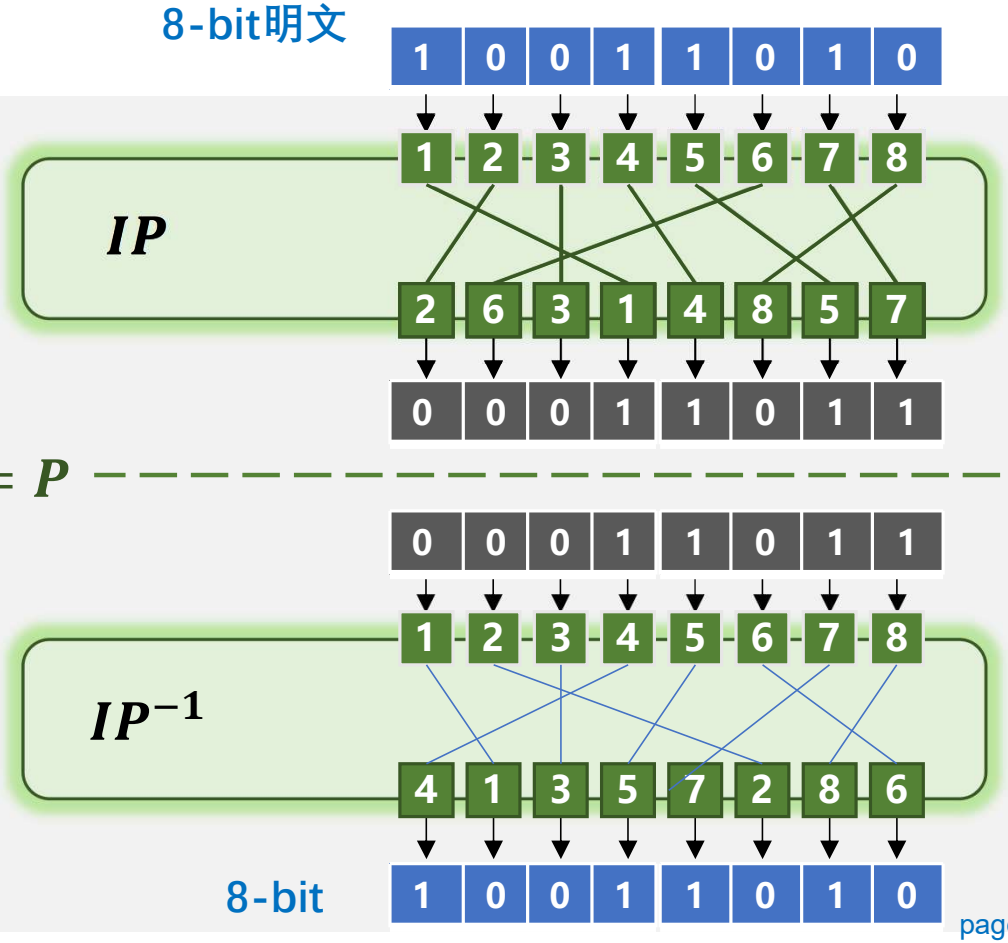
$$k_1 = P_8(Shift(P_{10}(K)))$$

3 数据加密标准：S-DES

- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - 算法流程
  - **详细步骤**

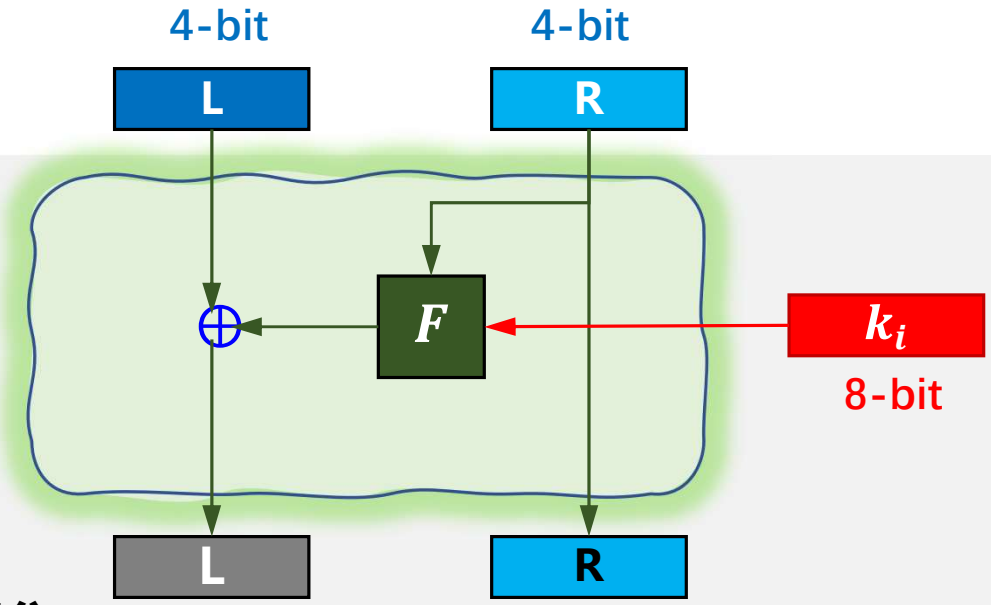
- 密钥生成
- **初始置换**
- **最终置换**

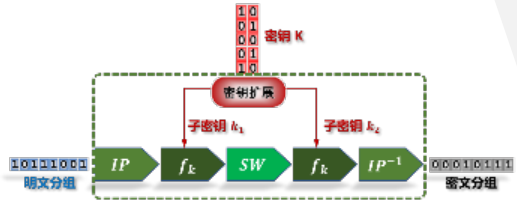
$$IP^{-1}(IP(P)) = P$$



3 数据加密标准：S-DES

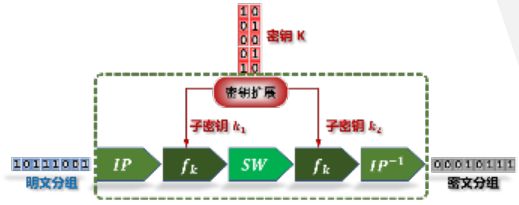
- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - 算法流程
  - **详细步骤**
    - 密钥生成
    - 初始置换
    - 最终置换
    - **S-DES 函数 f_K**
      - **分成左、右两部分**
      - $f_K(L,R) = (L \oplus F(R, k_i), R)$
      - F **是算法最核心的环节：轮函数**
      - $\oplus$ **是按位异或运算**

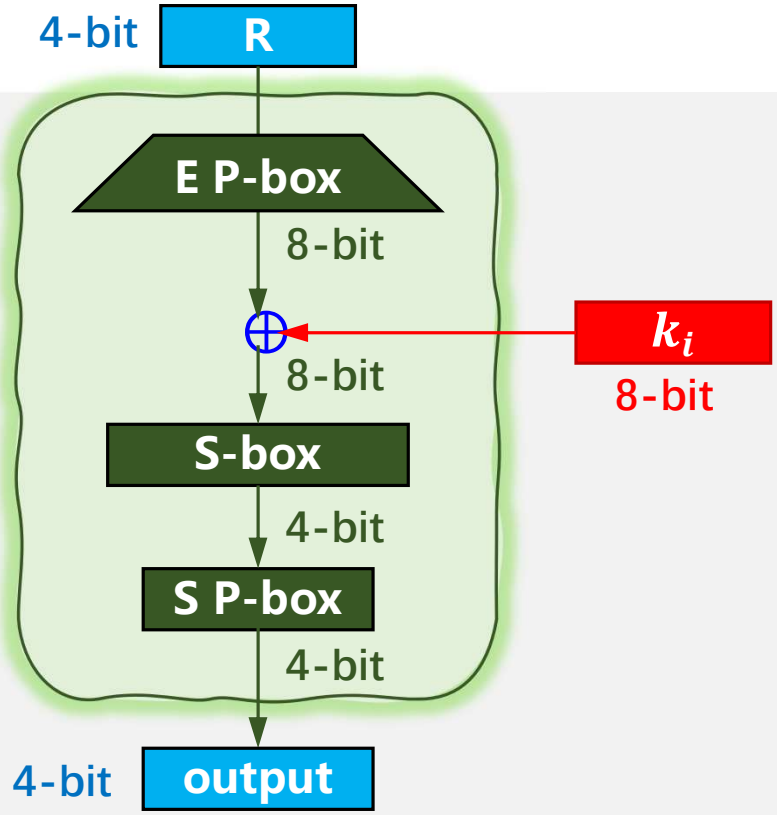




3 数据加密标准：S-DES

- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - 算法流程
  - **详细步骤**
    - 密钥生成
    - 初始置换
    - 最终置换
    - **S-DES 函数 f_K**
      - **轮函数F**
      - **四个转换步骤**

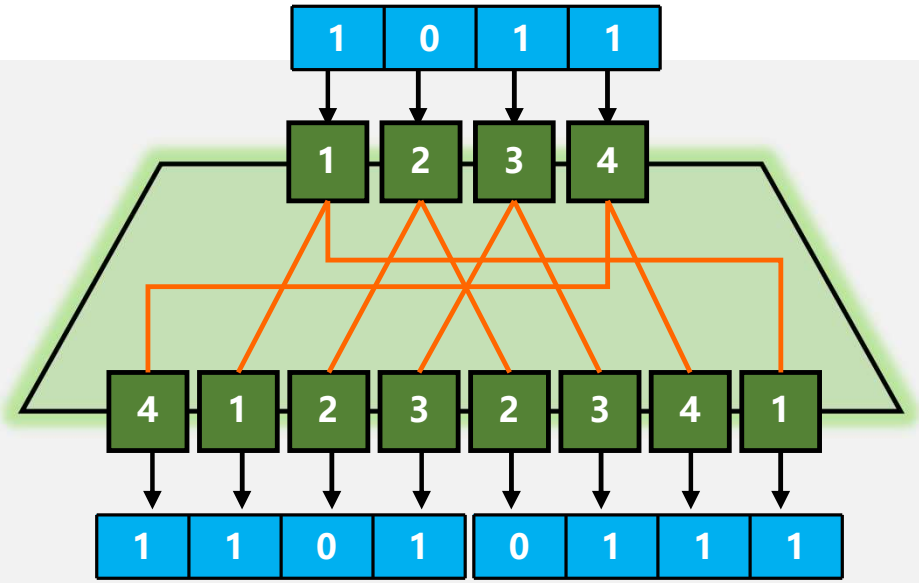




3 数据加密标准：S-DES

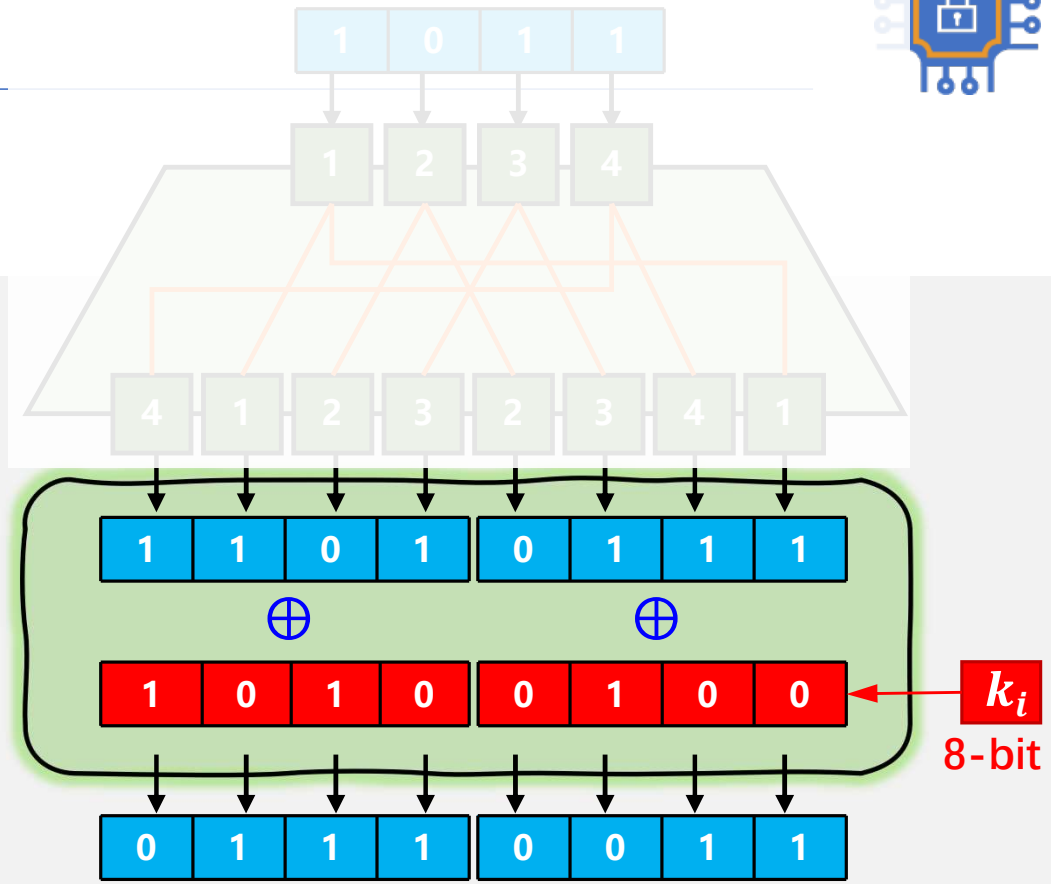
- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - 算法流程
  - **详细步骤**
    - 密钥生成
    - 初始置换
    - 最终置换
    - S-DES 函数 f_K
      - **轮函数*F***

(1) 扩展置换



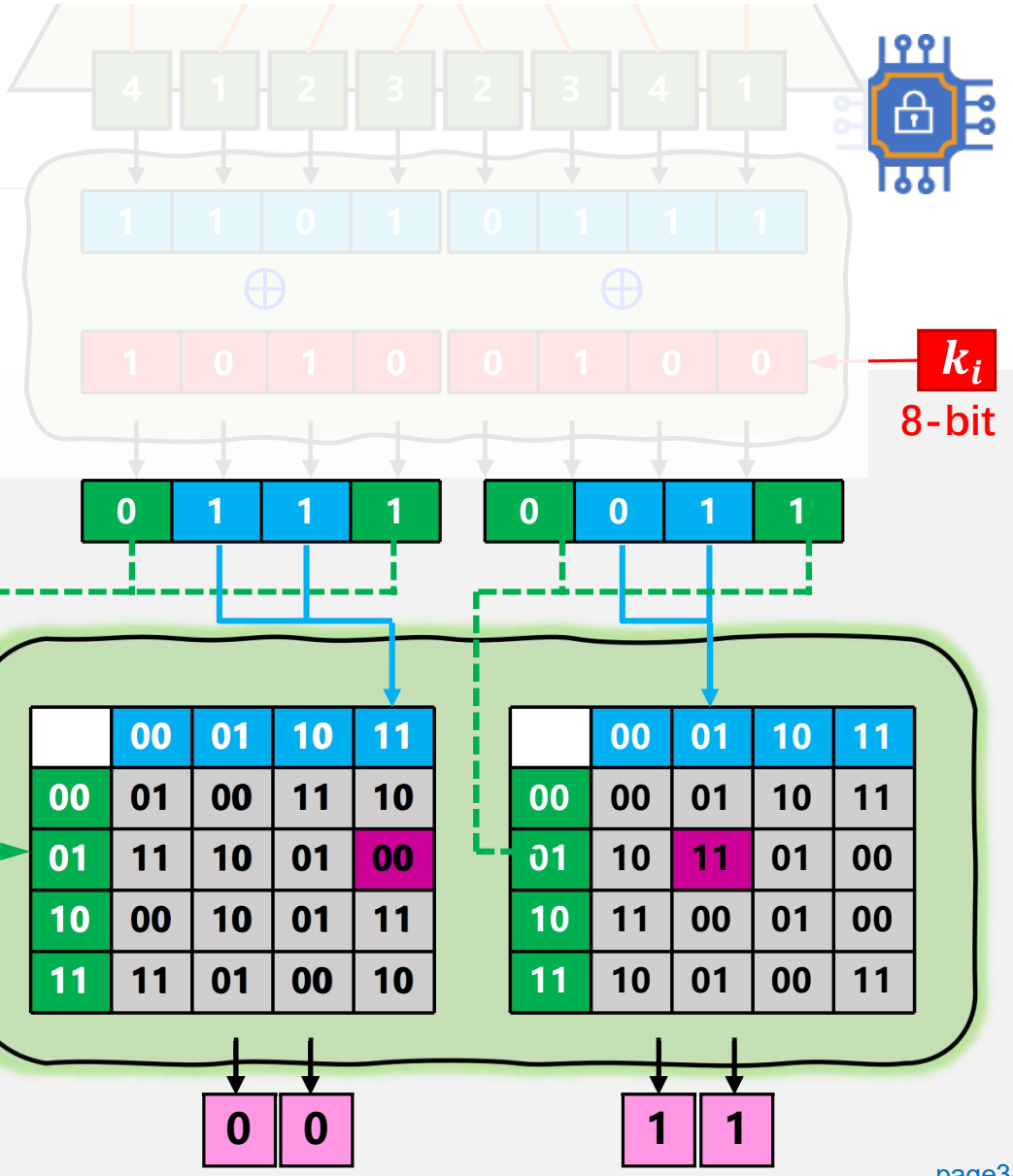
3 数据加密标准：S-DES

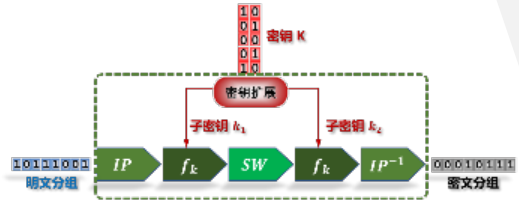
- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - 算法流程
  - **详细步骤**
    - 密钥生成
    - 初始置换
    - 最终置换
    - S-DES 函数 f_K
      - **轮函数*F***
      1) 扩展置换
      2) 用轮密钥



3 数据加密标准：S-DES

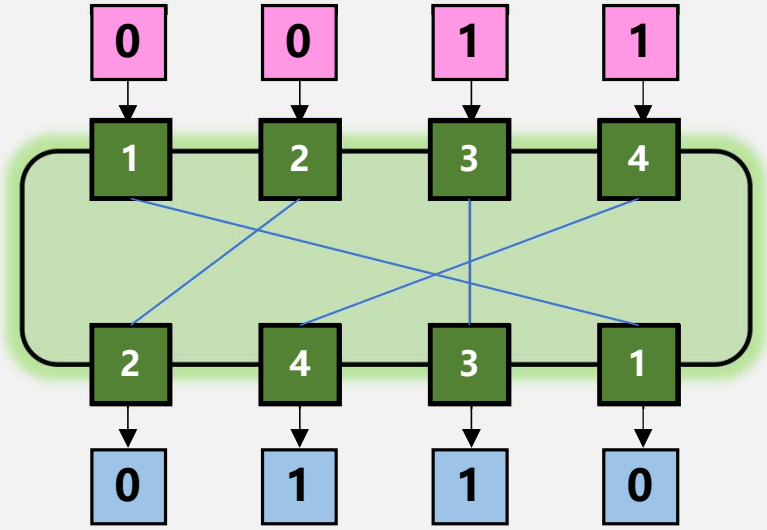
- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - 算法流程
  - **详细步骤**
    - 密钥生成
    - 初始置换
    - 最终置换
    - S-DES 函数 f_K
      - **轮函数*F***
      - 1) 扩展置换
      - 2) 用轮密钥
      - **3) 替换盒S-Boxs**





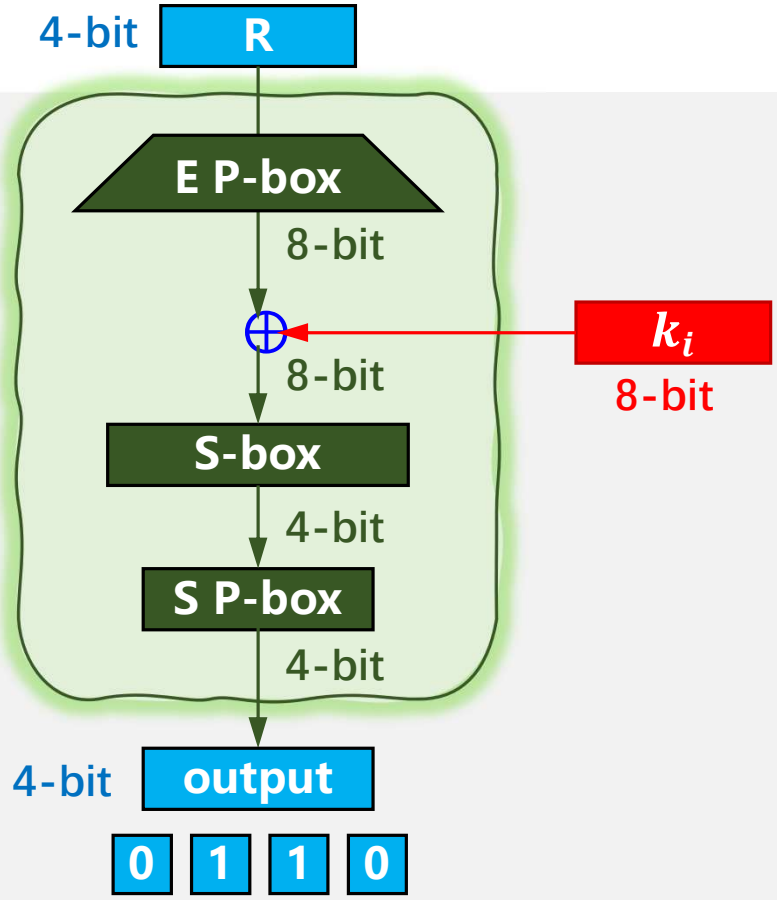
3 数据加密标准：S-DES

- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - 算法流程
  - **详细步骤**
    - 密钥生成
    - 初始置换
    - 最终置换
    - S-DES 函数 f_K
      - **轮函数*F***
      - 1) 扩展置换
      - 2) 用轮密钥
      - 3) 替换盒S-Boxes
      - **4) 直接置换**



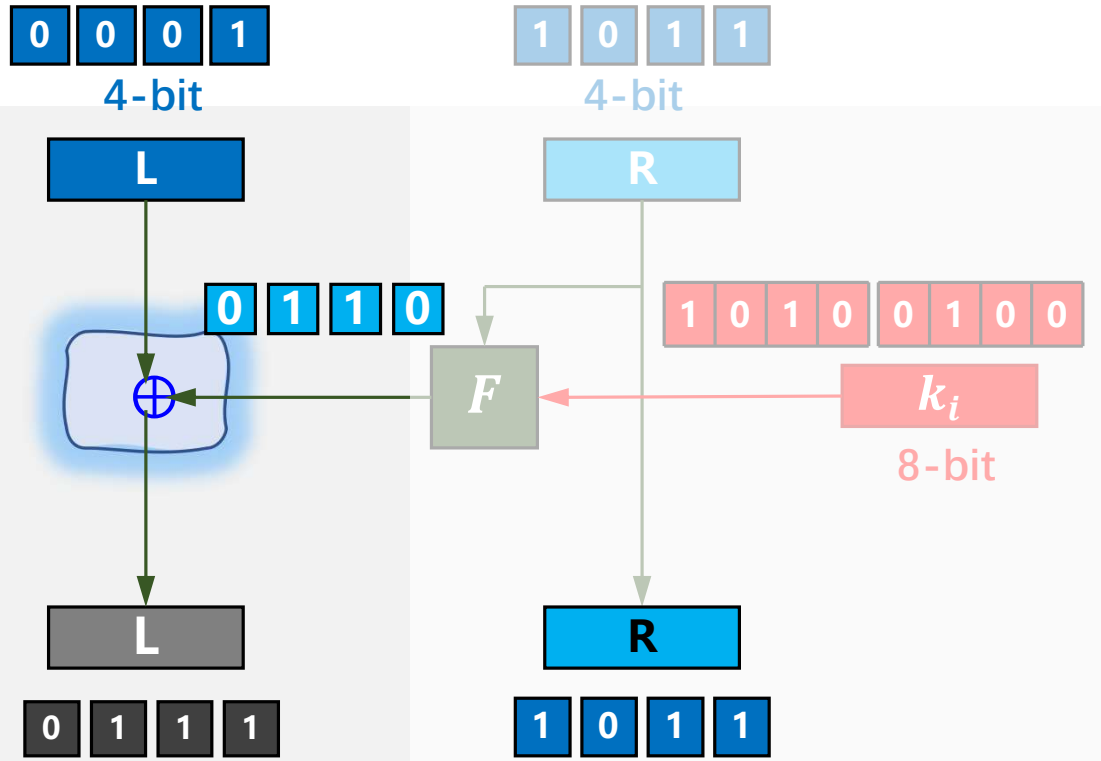
3 数据加密标准：S-DES

- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - 算法流程
  - **详细步骤**
    - 密钥生成
    - 初始置换
    - 最终置换
    - **S-DES 函数 f_K**
      - **轮函数F**
        - **输出结果**



3 数据加密标准：S-DES

- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - 算法流程
  - **详细步骤**
    - 密钥生成
    - 初始置换
    - 最终置换
    - S-DES 函数 f_K
      - 轮函数F
      - 异或

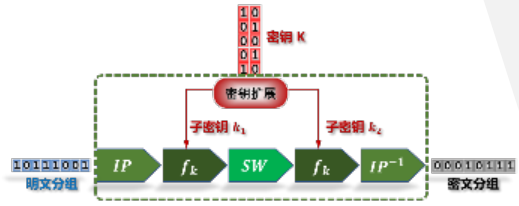


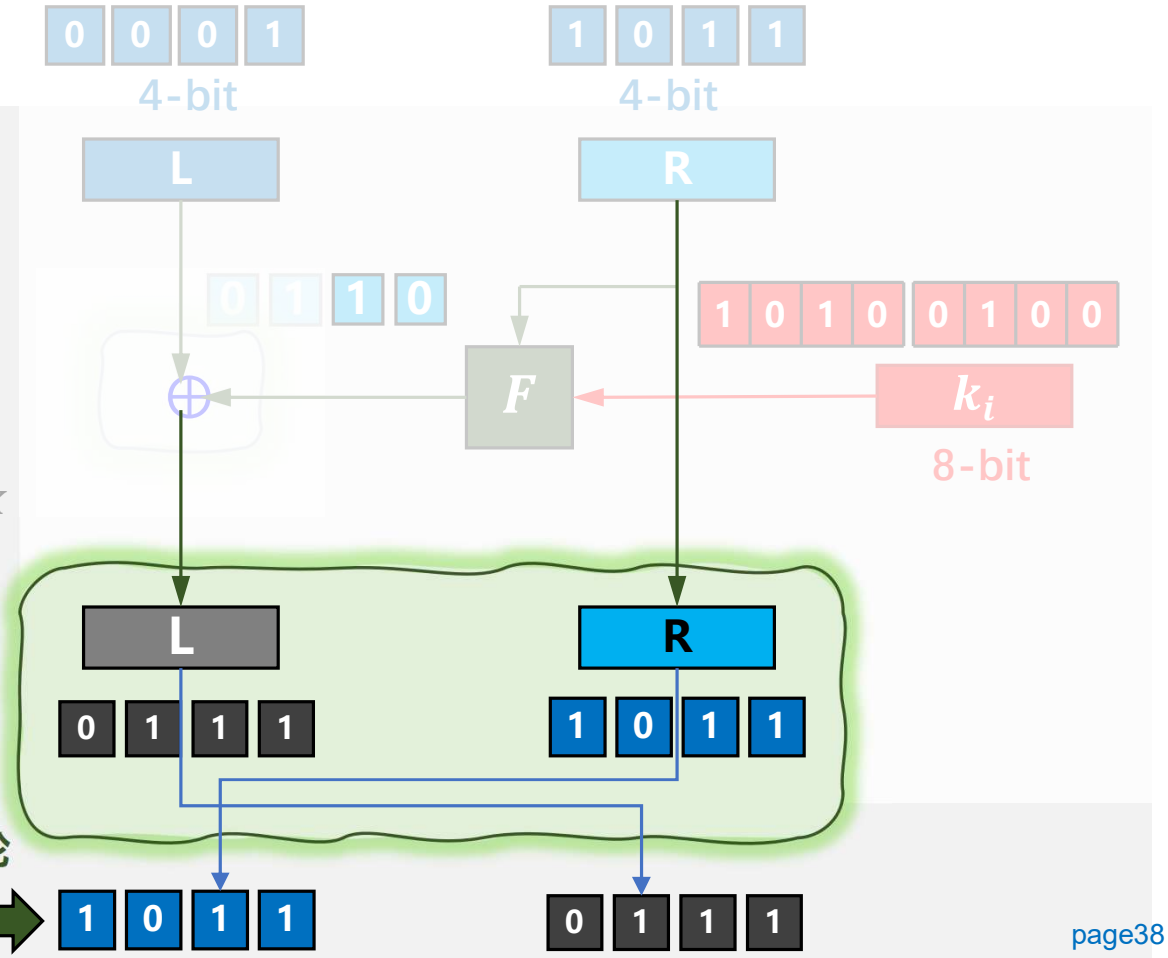
3 数据加密标准：S-DES

- **简化的数据加密标准： S-DES**
  - 基本设定
  - 加密机制
  - 算法流程
  - **详细步骤**
    - 密钥生成
    - 初始置换
    - 最终置换
    - S-DES 函数 f_K
      - 轮函数F
      - 异或
    - **左右互换SW**

相当于Enigma转轮

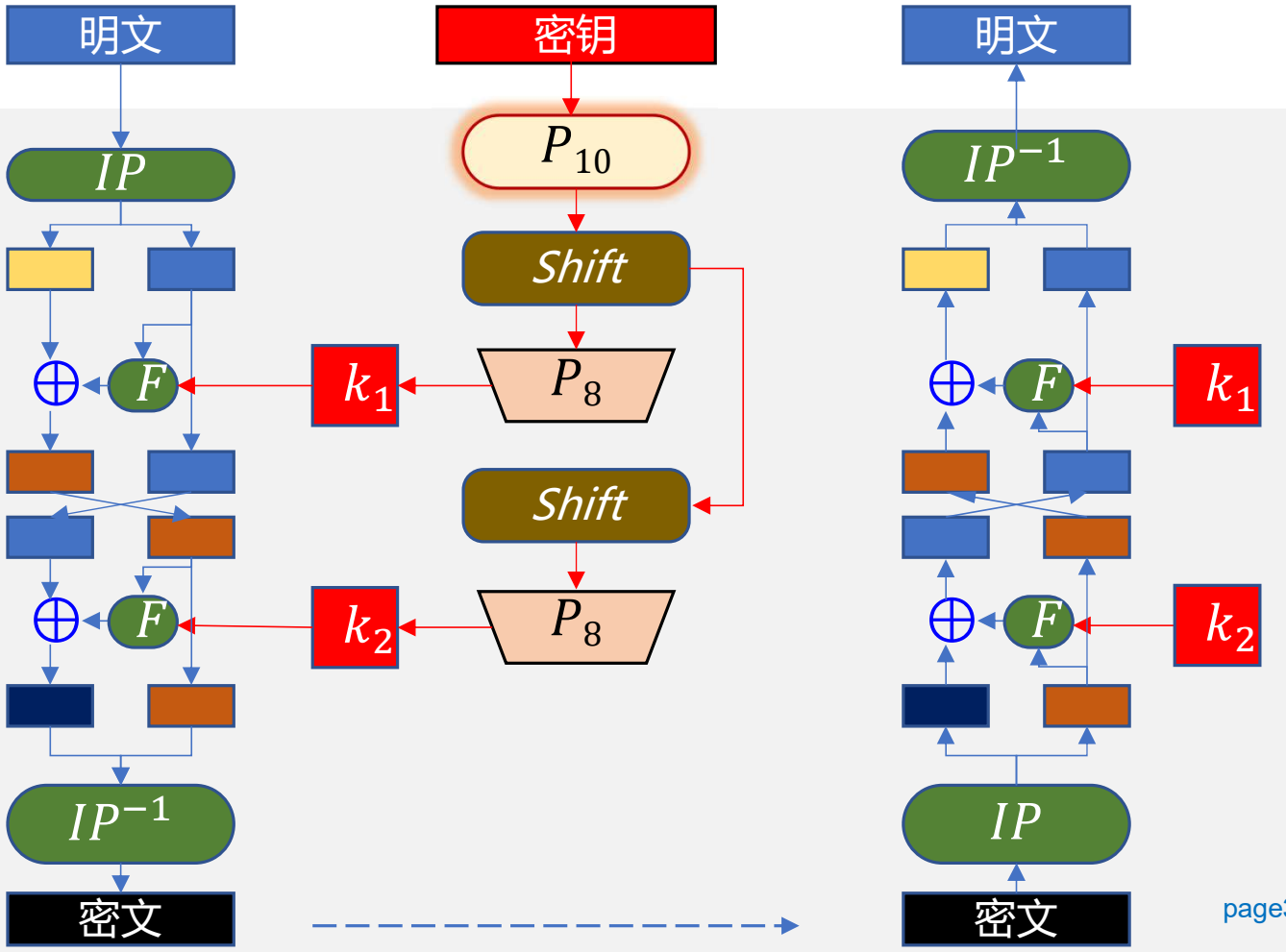
重复上述流程





3 数据加密标准：S-DES

- **简化的数据加密标准：**
  - 基本设定
  - 加密机制
  - 算法流程
  - **详细步骤**



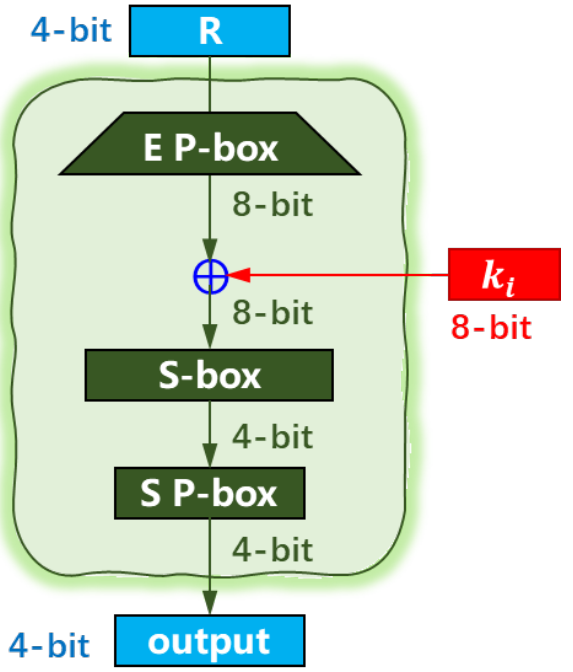
目录 | CONTENTS

3 数据加密标准：讨论

- 为什么S-DES中存在 不可逆的变换 单元
- 但算法方面又能够实现加解密一体呢?

究竟有什么奥秘?

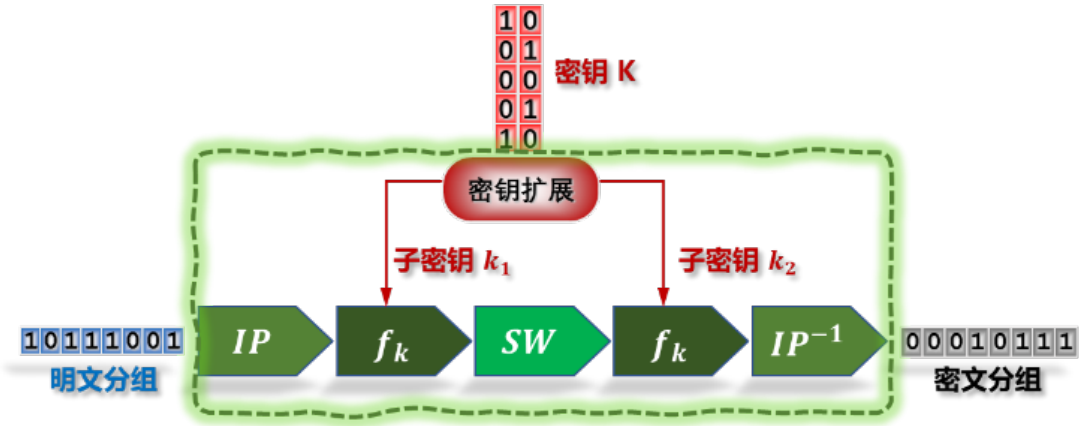
我们将在下节进行探索...



EP-Box: 扩展
S-box：压缩

课堂小结

- 对称分组加密的基本概念
- 分组加密的转换机制
  - P-Box
  - S-Box
  - XOR
  - 转轮
  - 分组加密标准
  - 简单算法：S-DES



$$C = IP^{-1}(f_{k_2}(SW(f_{k_1}(IP(P)))))$$

Thanks!