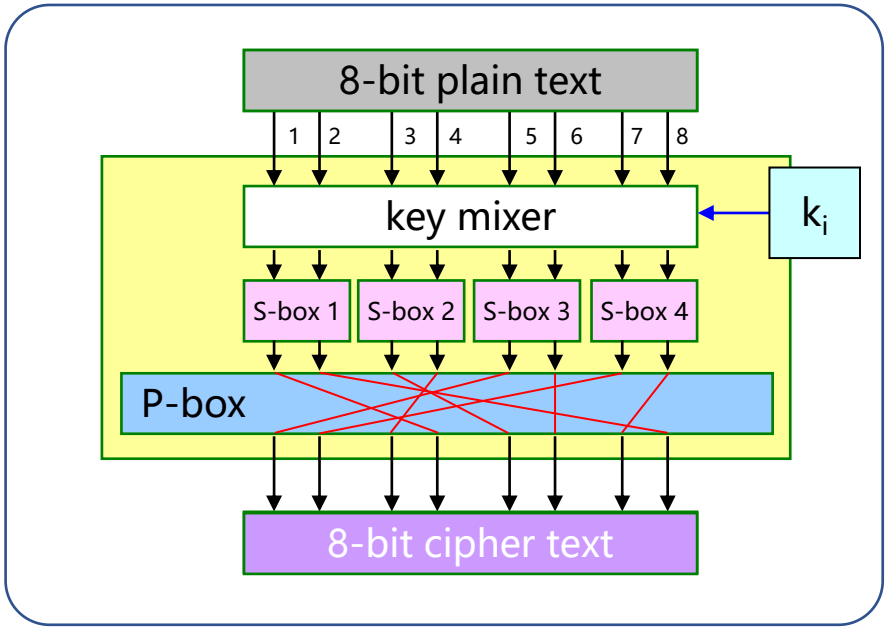
信息安全导论

现代密码学原理与实践

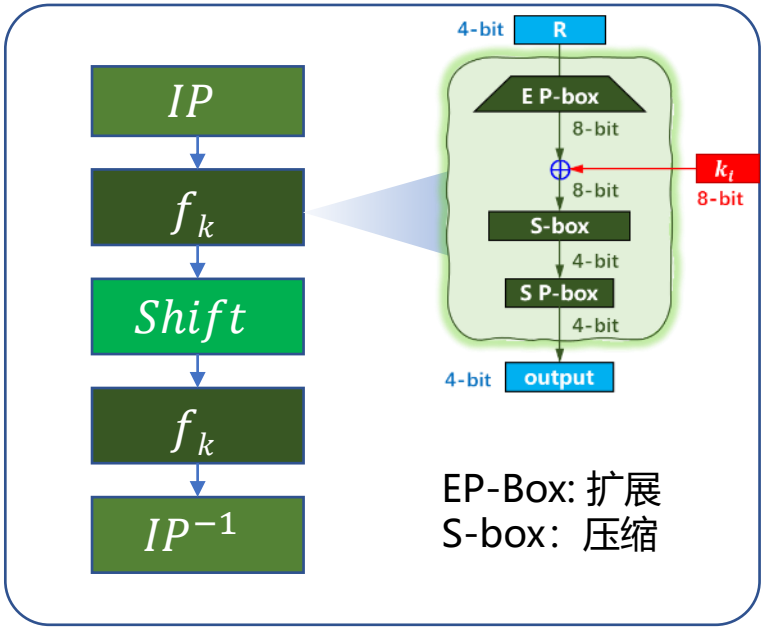
第6讲：数据加密标准(2)

- 重庆大学大数据与软件学院
- 开课时间：2025年秋季

课程回顾



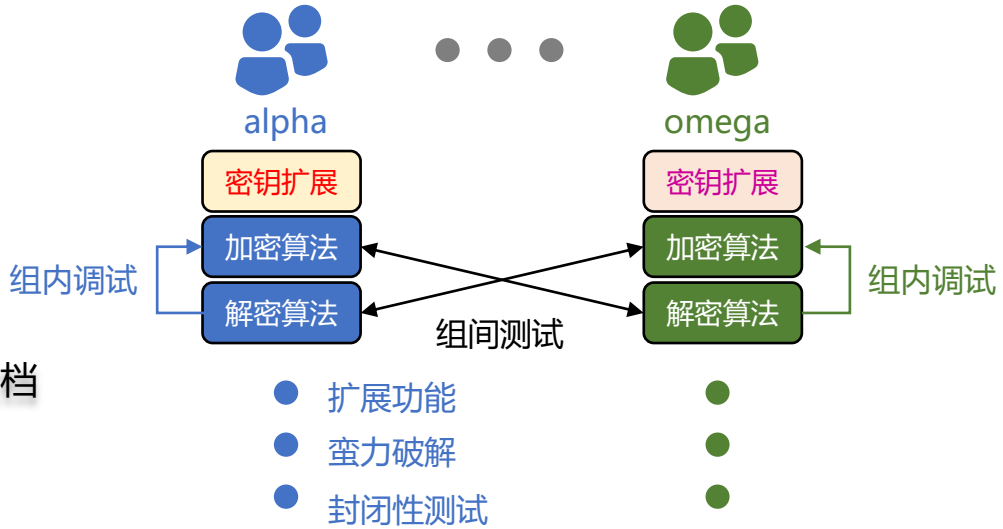
Sandwich



S-DES

课外作业

- **S-DES算法程序实现**
  - 2人一组共同完成
  - 使用编程语言不限
  - 调试测试：过关模式
  - 提交方式：Github链接→石墨文档
  - 截止时间：2025.10.8 23:00
  - 详情请访问石墨文档：
    - https://shimo.im/docs/m5kvdlMaKvcENy3X/
    - 《作业1：S-DES算法实现》可复制链接后用浏览器或石墨文档 App 打开



目录 | CONTENTS

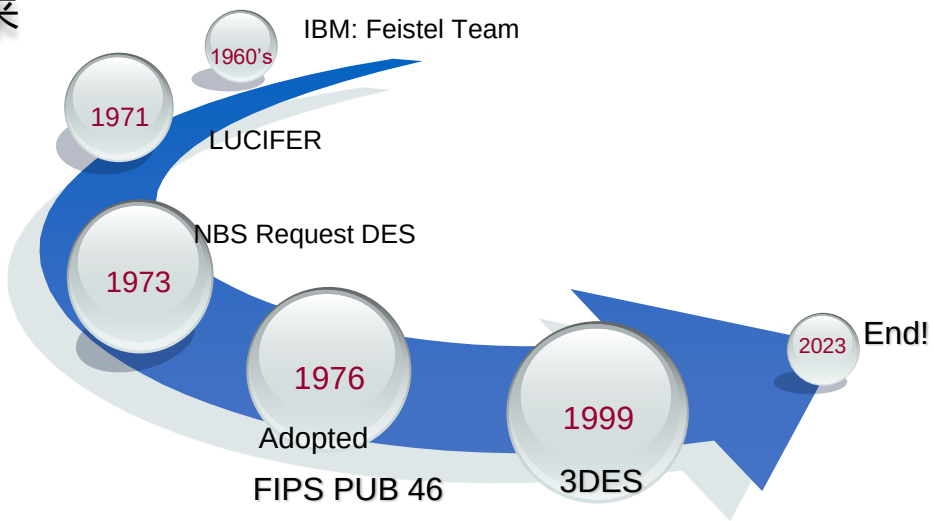
1 • **数据加密标准: DES** ➔参考书v8~P71

2 • **Feistel 密码体系结构**

3 • **分析和讨论**

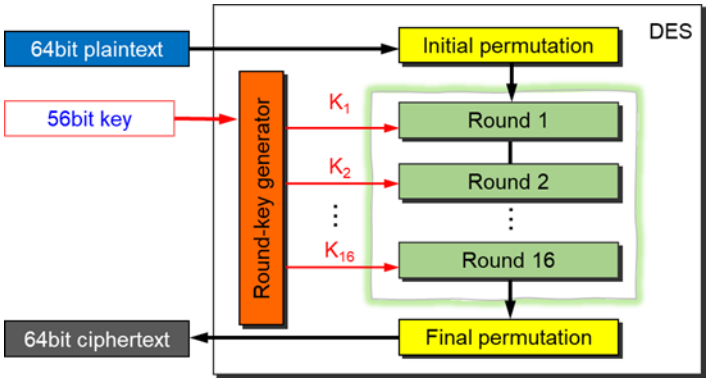
1 数据加密标准: DES

- **数据加密标准:**
  - Data Encryption Standard (DES)
  - IBM 公司 LUCIFER 算法 简化而来
  - FIPS PUB 46



1 数据加密标准: DES

- **数据加密标准（DES）：**
  - 64bit 分组明文输入/密文输出
  - 56bit 密钥
  - 生成16把 48bit 子密钥
  - F函数对32bit分组进行加密
  - 8个S盒，每个均为4行16列矩阵

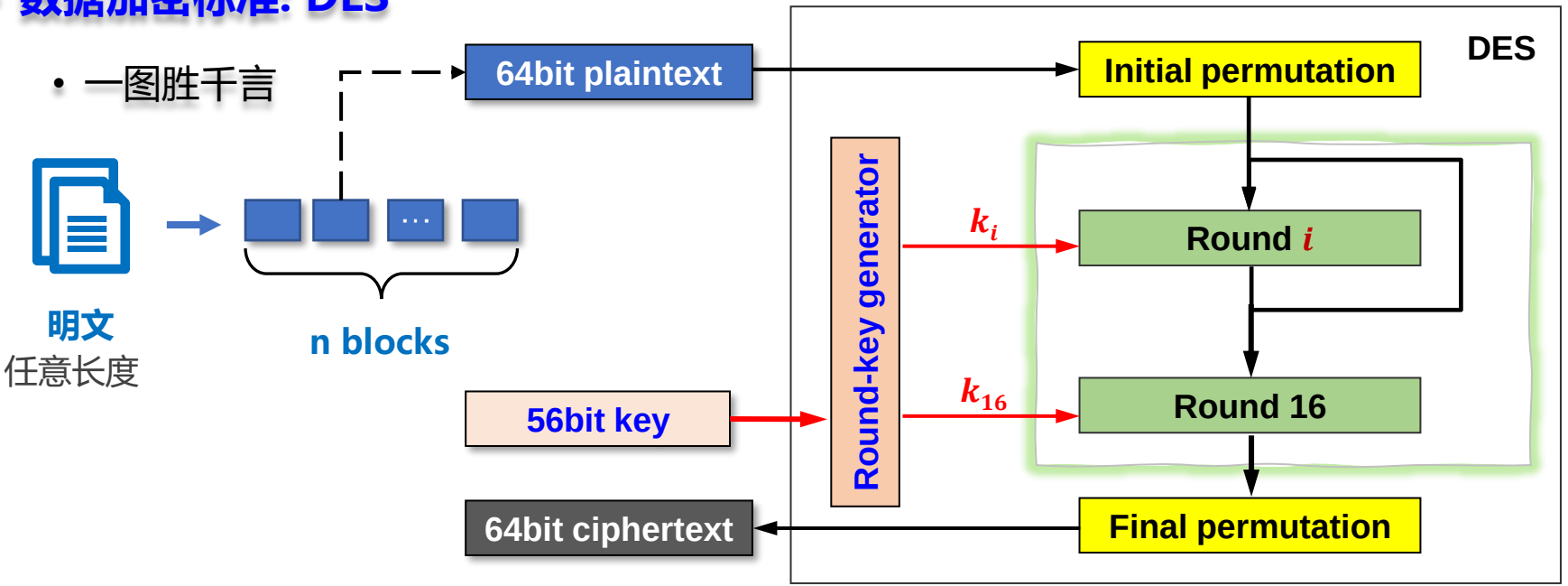


$$C = E_K(P) = IP^{-1} \circ f_{K_{16}} \circ SW \circ f_{K_{15}} \circ \cdots \circ f_{K_1} \circ IP$$

$$P = D_K(C) = IP^{-1} \circ f_{K_1} \circ SW \circ f_{K_2} \circ \cdots \circ f_{K_{16}} \circ IP$$

1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言



1 数据加密标准: DES

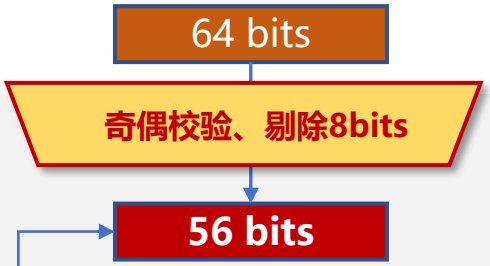
- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - **伪代码示范**

```
Cipher(plainBlock[64], RoundKeys[16,48],cipherBlock[64])
 {
  permute(64,64,planBlock, inBlock, initial_PBox)
  split(64,32,inBlock, leftBlock, rightBlock)
  for(round=1 to 16)
   {
    mixer(leftBlock, rightBlock, RoundKeys[round])
    if (round!=16) swapper(leftBlock, rightBlock)
   }
  combine(32,64,leftBlock, rightBlock, outBlock)
  permute(64,64,outBlock, cipherBlock, final_PBox)
 }
```

1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - **密钥扩展**
    - 加密过程
    - 解密过程

- **密钥生成**
  - **密钥 K:**
    - 随机生成 64 bits
    - 奇偶校验 8 bits
    - **密钥长度 56 bits**
    - 通讯双方事先密钥共享

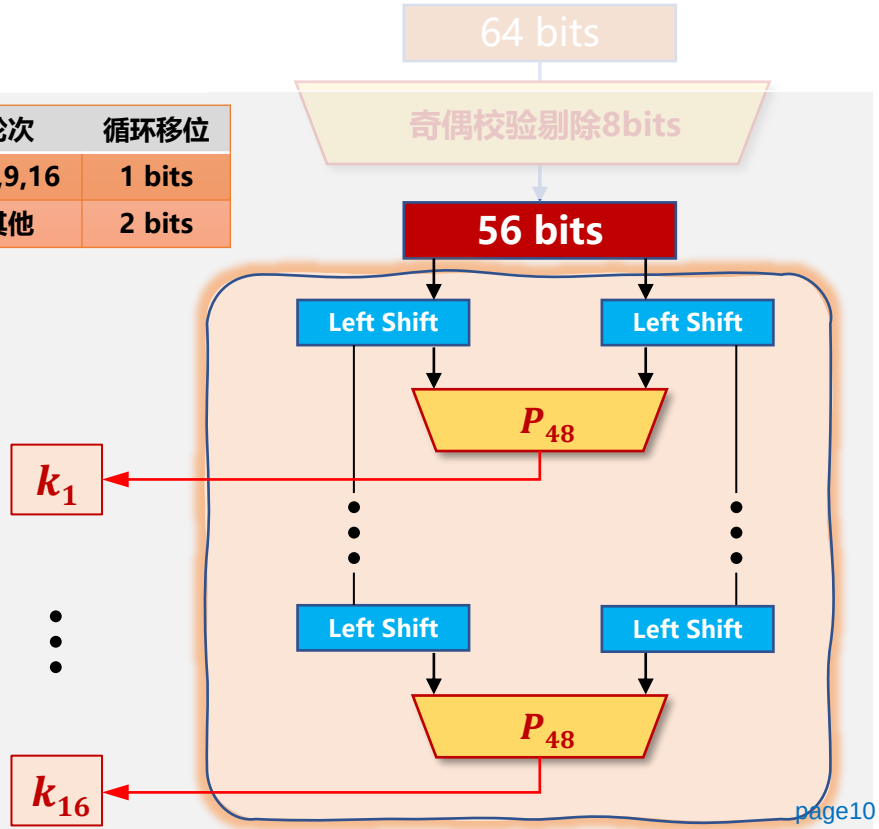


1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - **密钥扩展**
    - 加密过程
    - 解密过程

- **密钥生成**
  - 密钥 K:
  - **轮密钥 k_i**

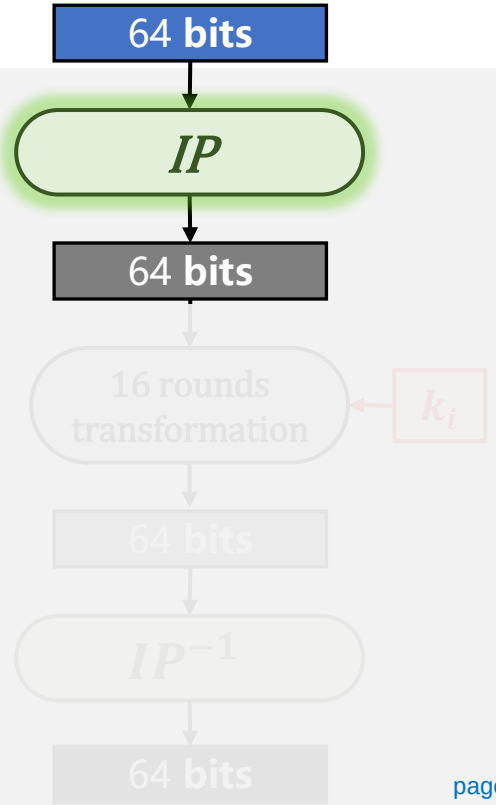
轮次	循环移位
1,2,9,16	1 bits
其他	2 bits



1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程

- 密钥生成
- **初始置换**

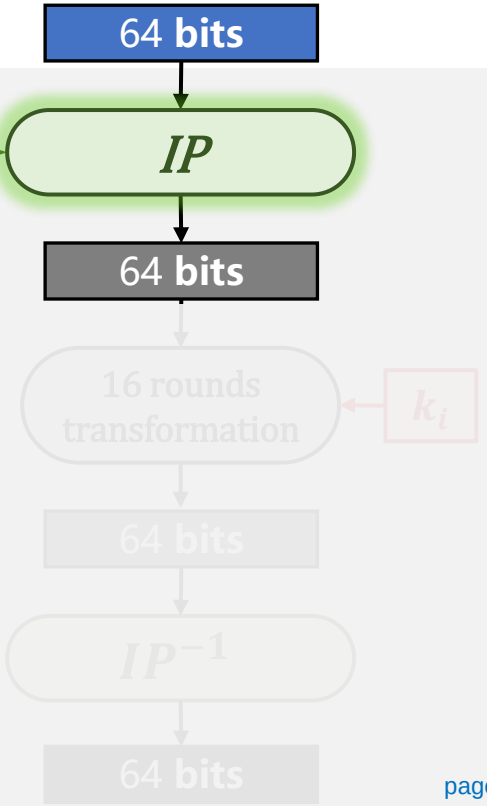


1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程

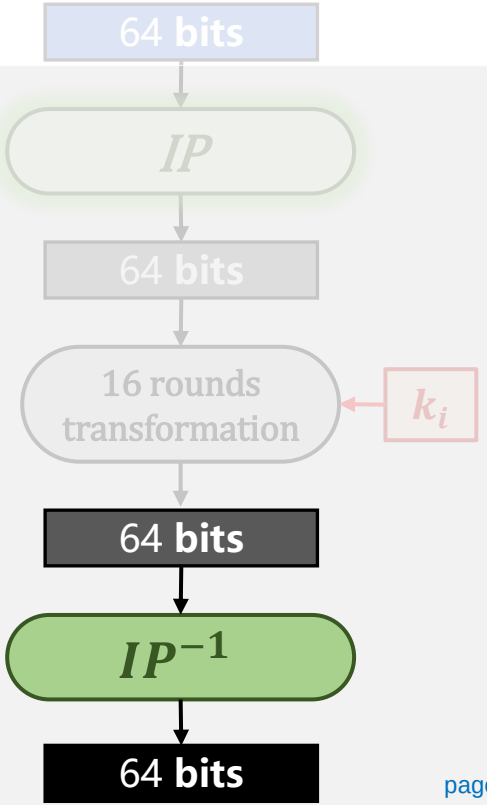
- 密钥生成
- **初始置换**

58,	50,	42,	34,	26,	18,	10,	02
60,	52,	44,	36,	28,	20,	12,	04
62,	54,	46,	38,	30,	22,	14,	06
64,	56,	48 ,40 ,32,	24,	16,	08		
57,	49,	41,	33,	25,	17,	09,	01
59,	51,	43,	35,	27,	19,	11,	03
61,	53,	45,	37,	29,	21,	13,	05
63,	55,	47,	39,	31,	23,	15,	07



1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程
- 密钥生成
- 初始置换
- **最终置换**

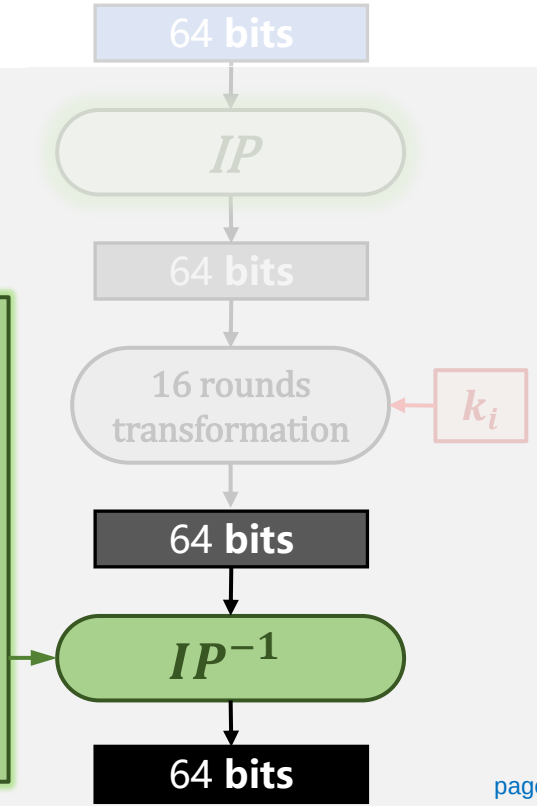


1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程

- 密钥生成
- **最终置换**

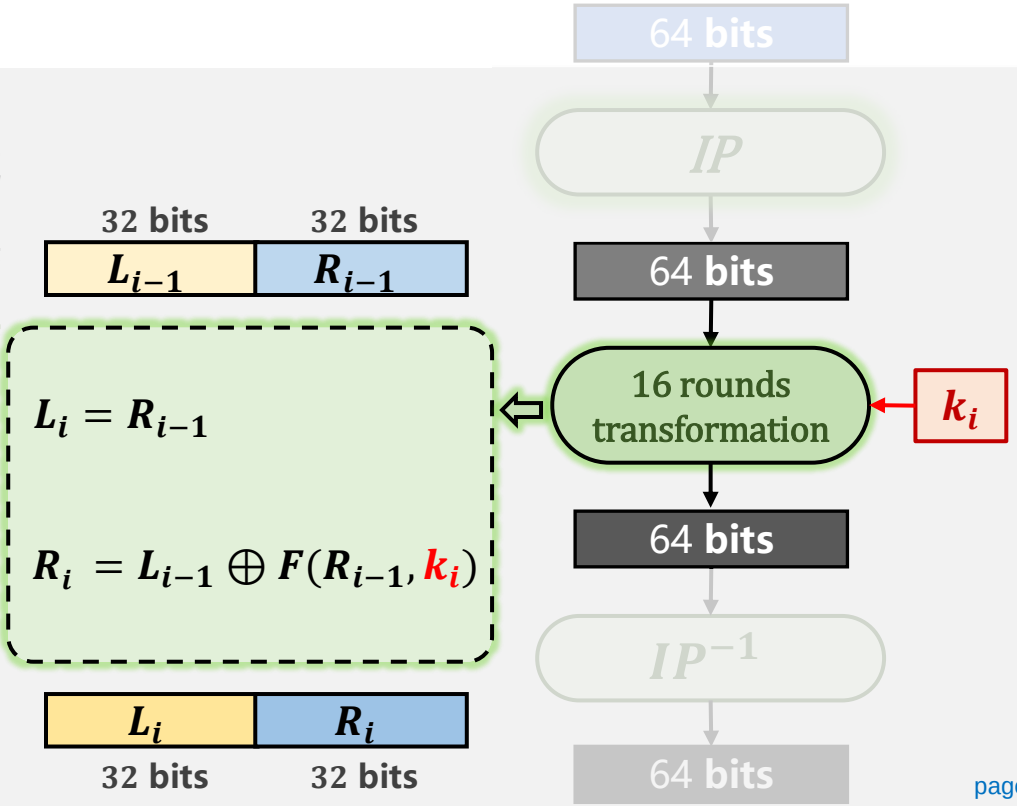
40,	08,	48,	16,	56,	24,	64,	32
39,	07,	47,	15,	55,	23,	63,	31
38,	06,	46,	14,	54,	22,	62,	30
37,	05,	45,	13,	53,	21,	61,	29
36,	04,	44,	12,	52,	20,	60,	28
35,	03,	43,	11,	51,	19,	59,	27
34,	02,	42,	10,	50,	18,	58,	26
33,	01,	41,	09,	49,	17,	57,	25



1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程

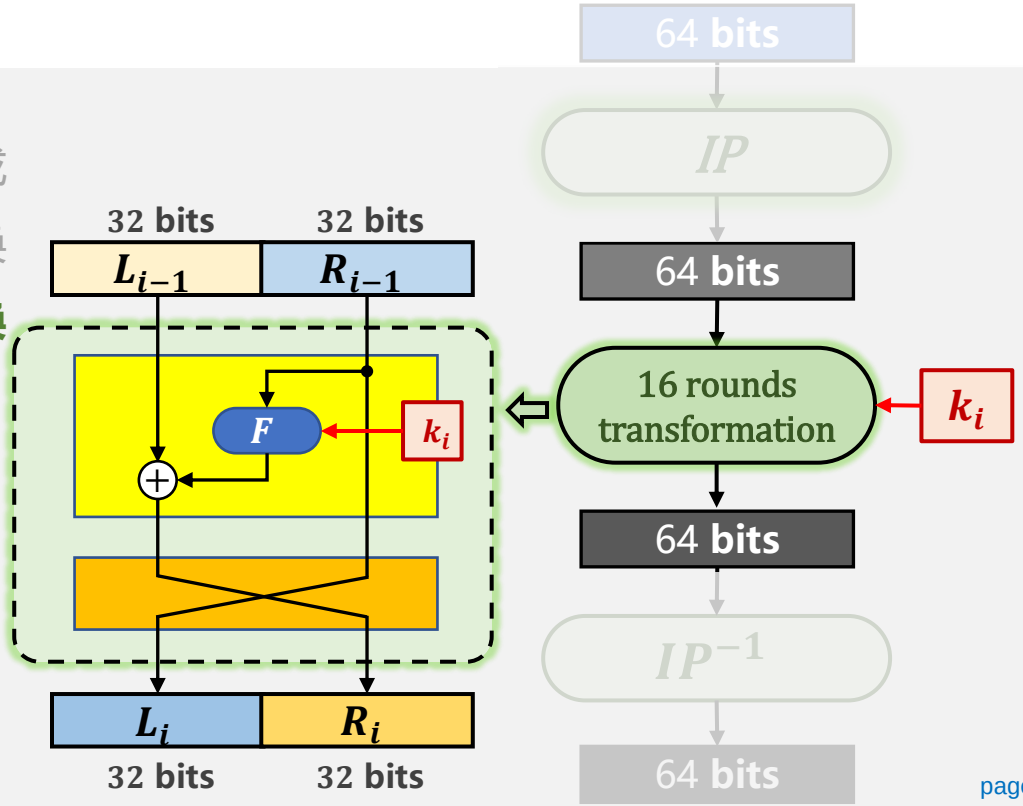
- 密钥生成
- 初始置换
- **多轮变换**



1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程

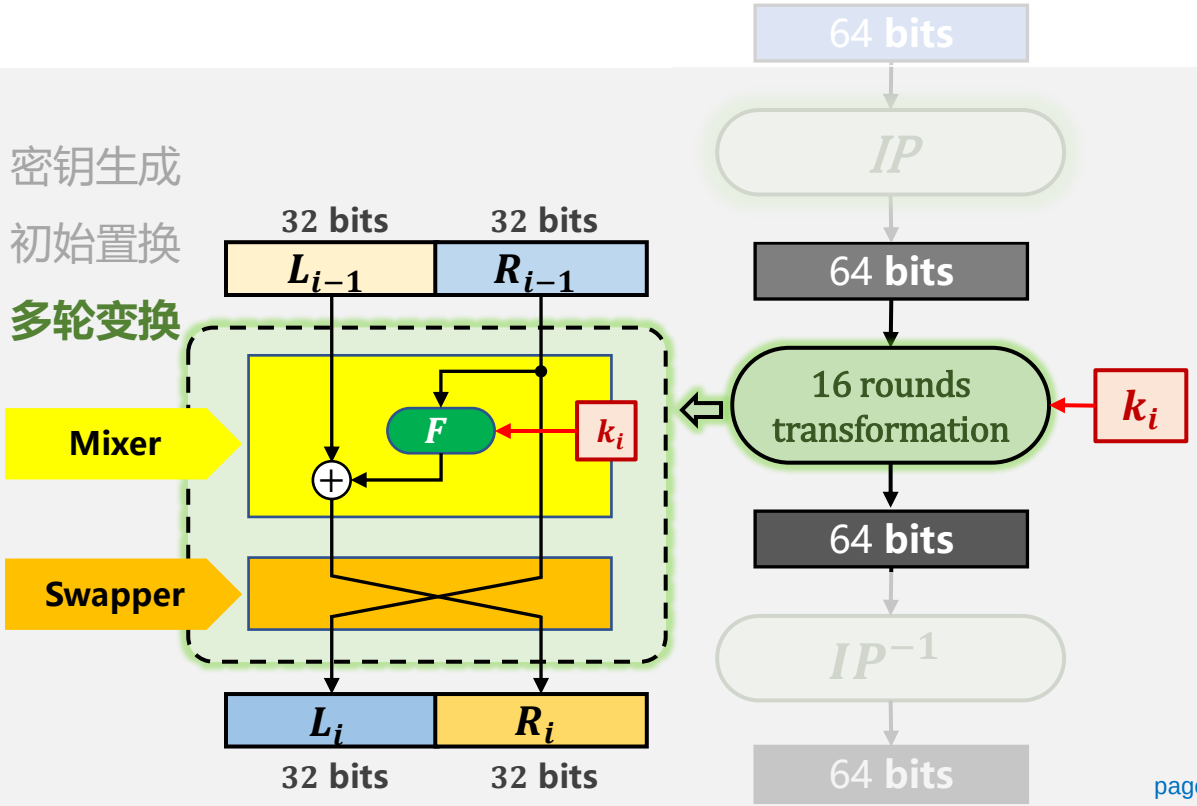
- 密钥生成
- 初始置换
- **多轮变换**



1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程

- 密钥生成
- 初始置换
- **多轮变换**



1 数据加密标准: DES

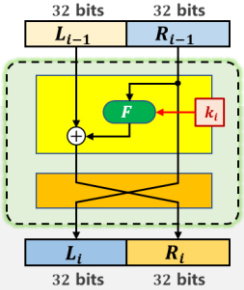
- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程
- 密钥生成
- 初始置换
- **多轮变换**
  - **伪代码**

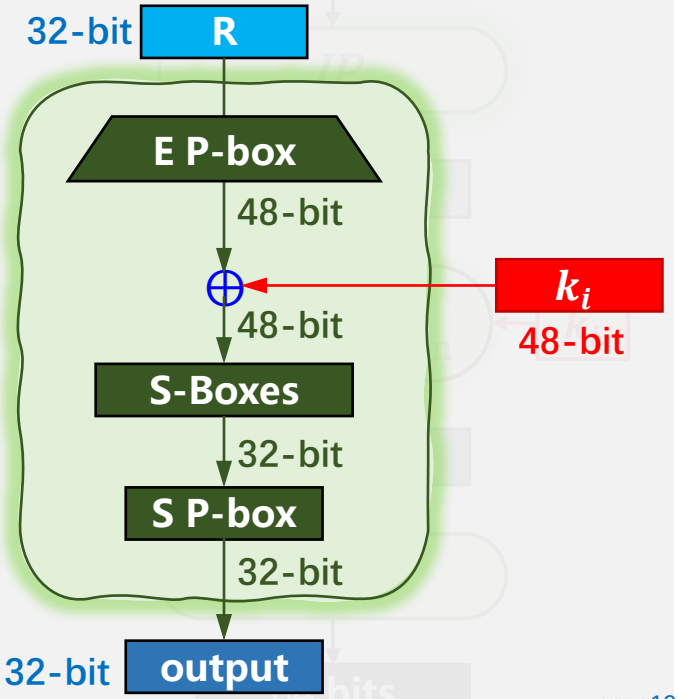
```
mixer(leftBlock[32],rightBlock[32],RoundKey[48])
{
   copy (32,rightBlock,T1)
   function(T1,RoundKey,T2)
   exclusiveOr(32,leftBlock,T2.T3)
   copy(32, T3,rightBlock)
}
swapper(leftBlock[32], rigthBlock[32])
{
   copy(32, leftBlock, T)
   copy(32, rightBlock, leftBlock)
   copy(32, T, rightBlock)
}
```

1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程

- 密钥生成
- 初始置换
- **多轮变换**
  - **轮函数 F**
  - **四个转换步骤**





1 数据加密标准: DES

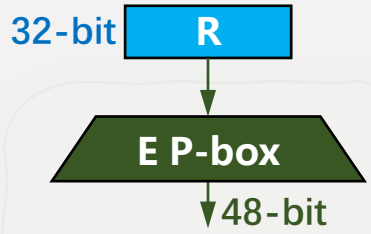
- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程

- 密钥生成
- 初始置换
- **多轮变换**
  - **轮函数 F**
  - **伪代码**

```
function(inBlock[32], RoundKey[48],outBlock[32])
{
    permute(32, 48, inBlock, T1, Extend_PBox)
    exclusiveOr(48, T1, RoundKey, T2)
    substitute(T2, T3, SBox)
    permute(32,32,T3, outBlock, Straight_PBox)
}
```

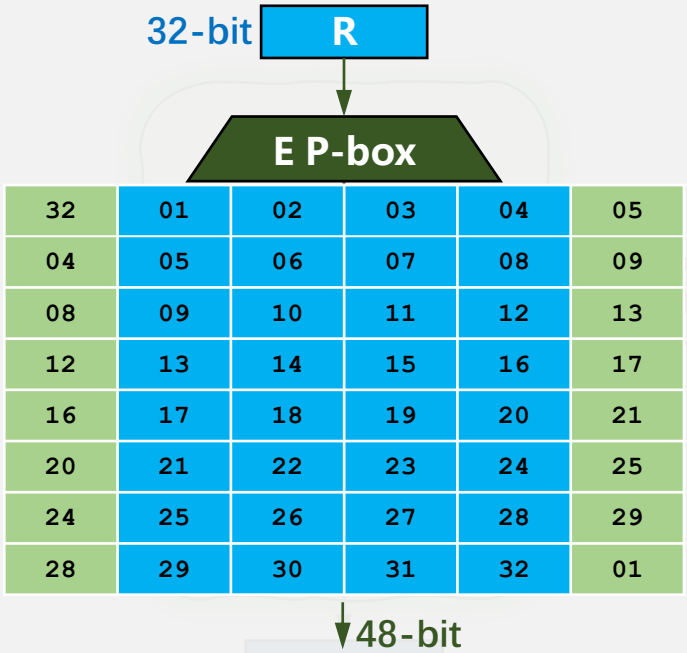
1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程
  - 密钥生成
  - 初始置换
  - **多轮变换**
    - 轮函数 F
      - **扩展置换**



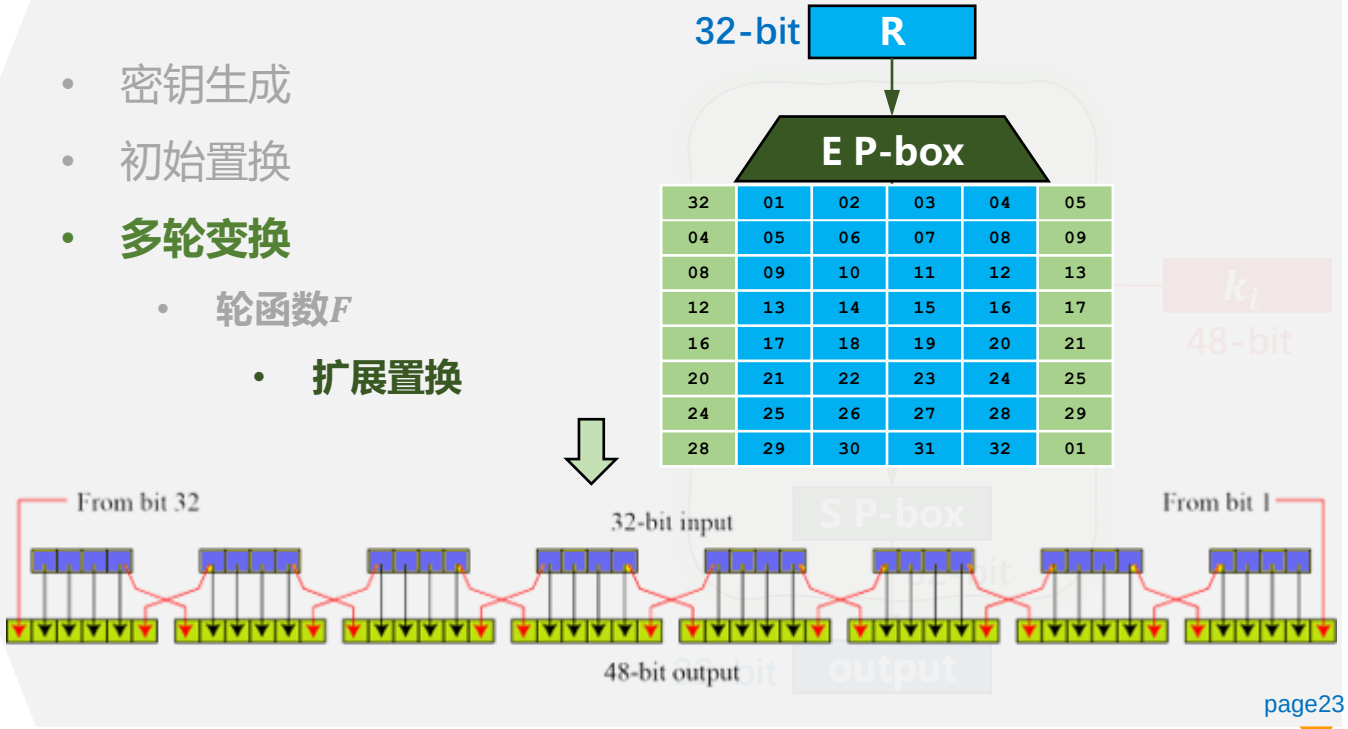
1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程
  - 密钥生成
  - 初始置换
  - **多轮变换**
    - 轮函数F
      - **扩展置换**



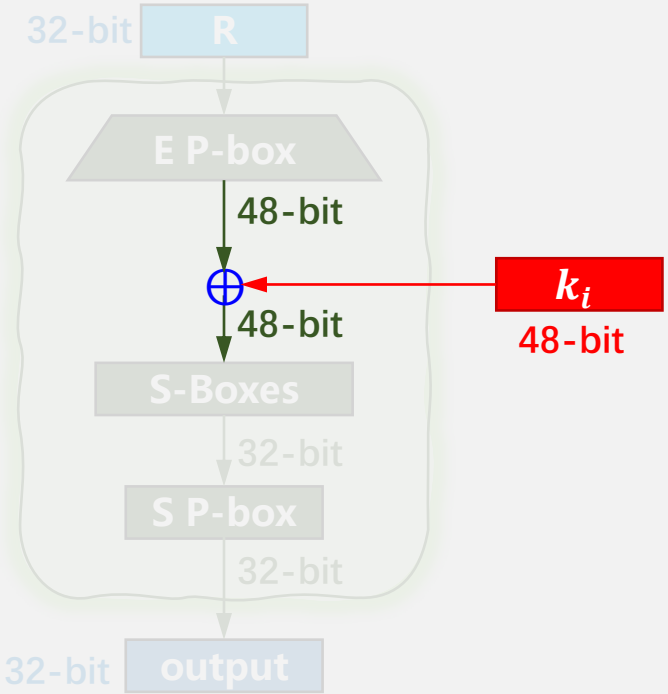
1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程
  - 密钥生成
  - 初始置换
  - **多轮变换**
    - 轮函数F
      - **扩展置换**



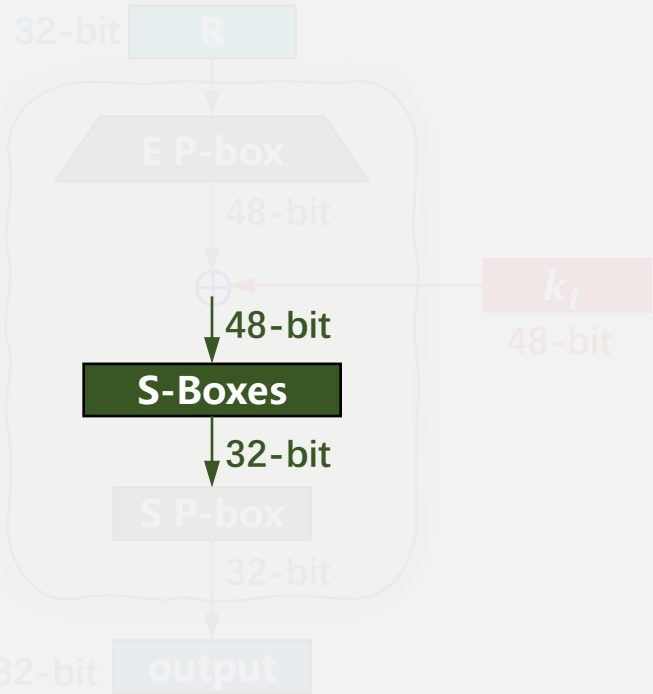
1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程
  - 密钥生成
  - 初始置换
  - **多轮变换**
    - 轮函数F
      - 扩展置换
      - **加轮密钥**



1 数据加密标准: DES

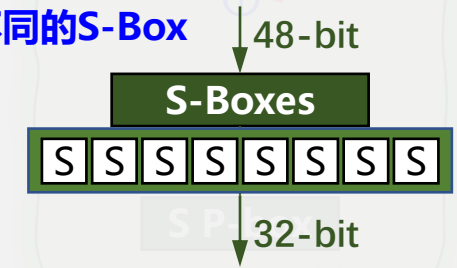
- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程
  - 密钥生成
  - 初始置换
  - **多轮变换**
    - **轮函数F**
      - 扩展置换
      - 加轮密钥
      - **压缩替换**



1 数据加密标准: DES

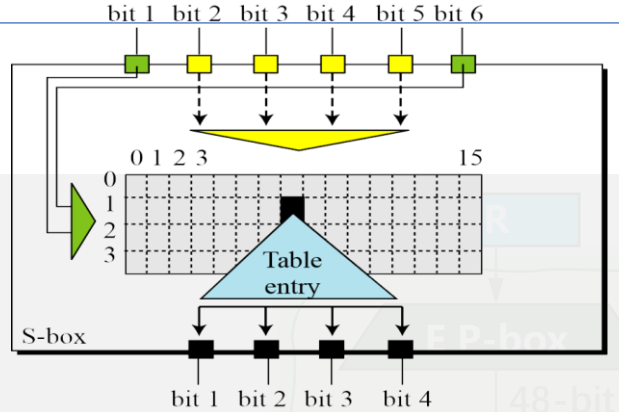
- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程
  - 密钥生成
  - 初始置换
  - **多轮变换**
    - 轮函数F
      - 扩展置换
      - 加轮密钥
      - **压缩替换**

使用8个不同的S-Box

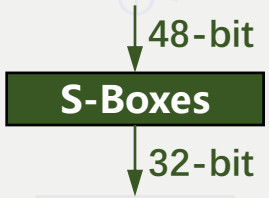


1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程
  - 密钥生成
  - 初始置换
  - **多轮变换**
    - **轮函数F**
      - 扩展置换
      - 加轮密钥
      - **压缩替换**

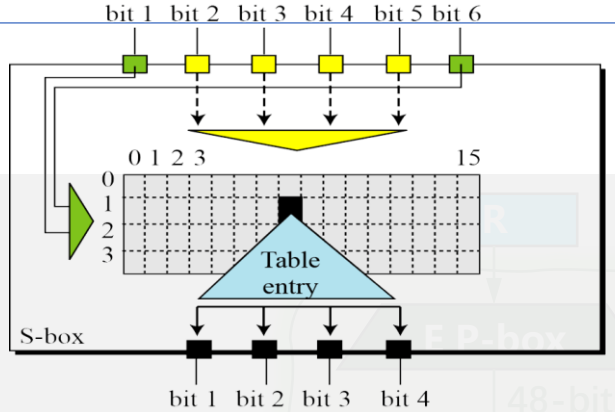


S-Box转换规则



1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程
  - 密钥生成
  - 初始置换
  - **多轮变换**
    - 轮函数F
      - 扩展置换



输入 110100

输出 ? 1001

1010

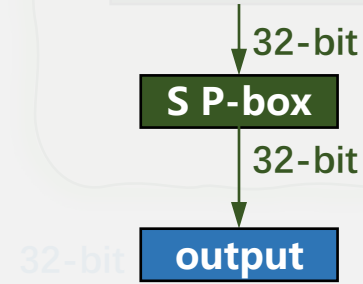
10

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程
- 密钥生成
- 初始置换
- **多轮变换**
  - **轮函数F**
    - 扩展置换
    - 加轮密钥
    - 压缩替换
    - **直接置换**

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25



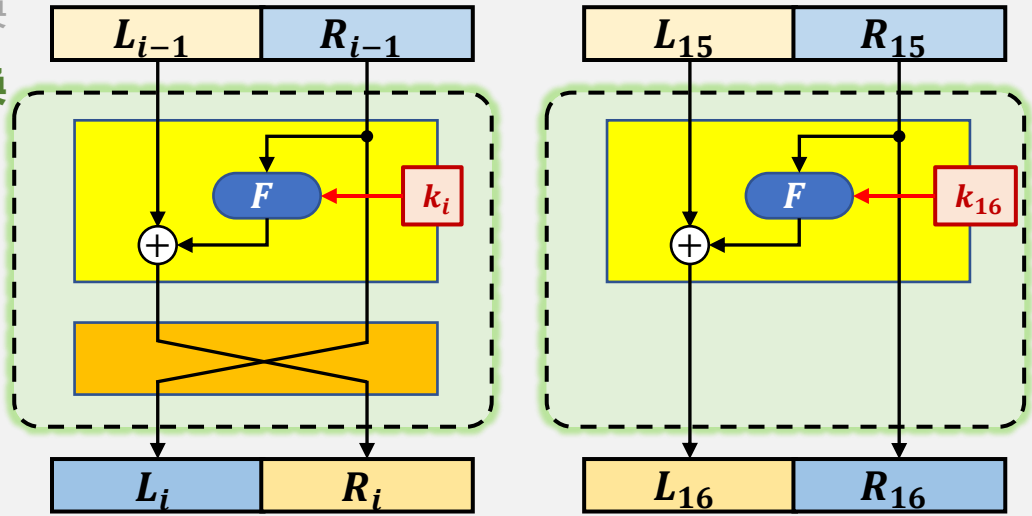
1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - 解密过程

完备的系统总需要一个“bug”，例如0!=1

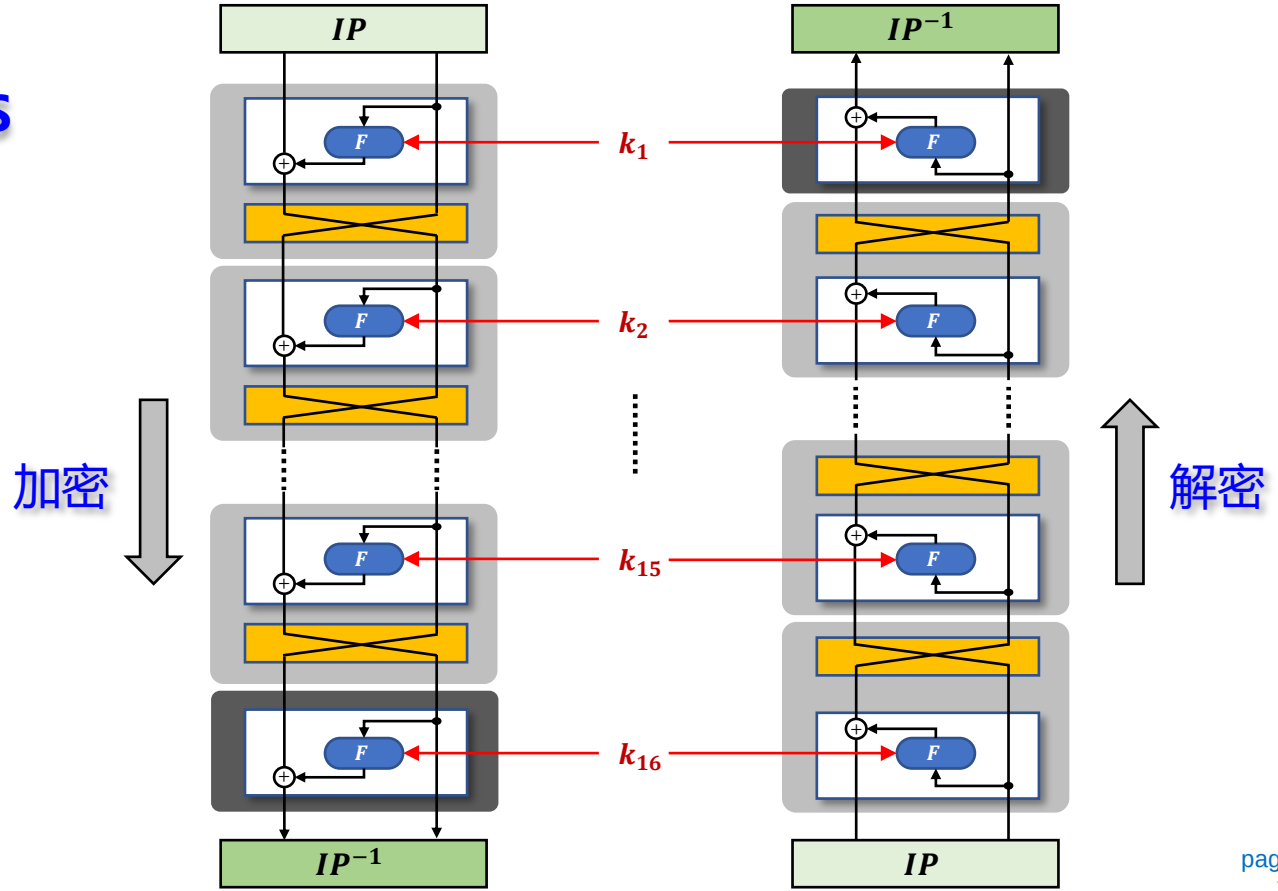
- 密钥生成
- 初始置换
- **多轮变换**

第16轮没有Swapper!



1 数据加密标准: DES

- **数据加密标准: DES**
  - 一图胜千言
  - 代数表达式
  - 伪代码示范
  - **算法流程**
    - 密钥扩展
    - **加密过程**
    - **解密过程**



目录 | CONTENTS

1 • 数据加密标准: DES

2 • Feistel 密码体系结构 ➔教材v8~P65

3 • 分析和讨论

2 Feistel 密码体系结构

- **Feistel密码**
  - 是一种体系结构
  - 可逆变换(非奇异变换)
    - 给定一个密钥Key
    - 每个明文分组唯一地对应一个密文分组
  - 加密解密过程一致
    - 加解密一体
    - 可以使用代数+递推法进行证明

Horst Feistel
1915-1990

2 Feistel 密码体系结构

- **Feistel密码**
  - 置换替换网络：SPN
  - 组合变换

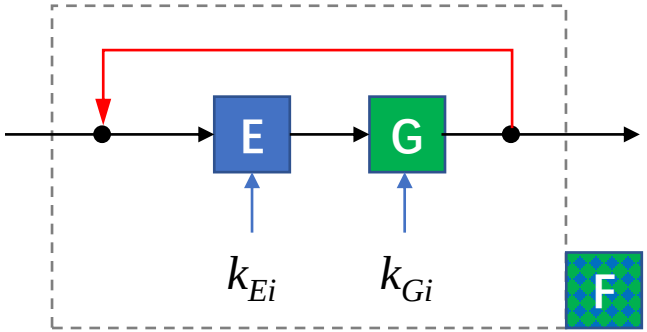
Horst Feistel
1915-1990

2 Feistel 密码体系结构

- **Feistel密码**
  - 置换替换网络：SPN
  - 组合变换

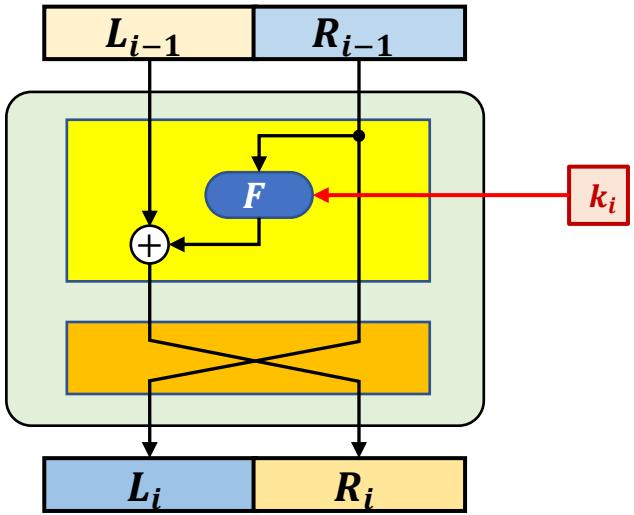
“香农的论文说明了一切”

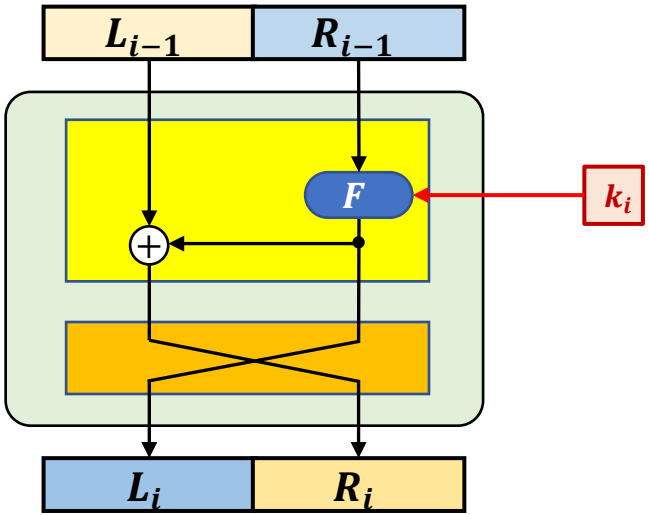
Horst Feistel
1915-1990



2 Feistel 密码体系结构

- **Feistel密码**
  - 轮函数F中可以使用 不可逆变换(E-Pbox、S-box)

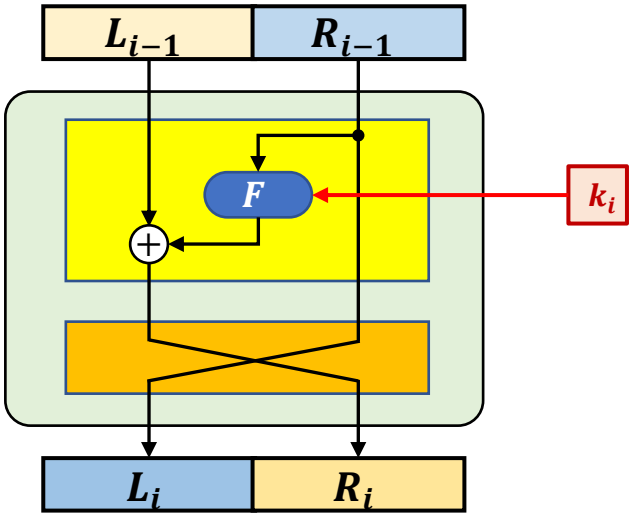




第8版教科书的改动

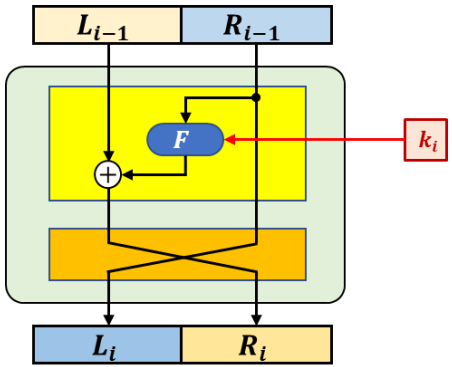
2 Feistel 密码体系结构

- **Feistel 密码体系**
  - 设计时应该考虑的特性或参数
    - 分组尺寸
    - 密钥尺寸
    - 轮数
    - 轮密钥生成
    - 轮函数设计
    - 快速软硬件实现
    - 易于分析



2 Feistel 密码体系结构

- **Feistel密码体系**
  - 对现代商用密码的深远影响



- Blowfish
- Camellia
- CAST-128
- DES
- FEAL
- GOST 28147-89
- ICE

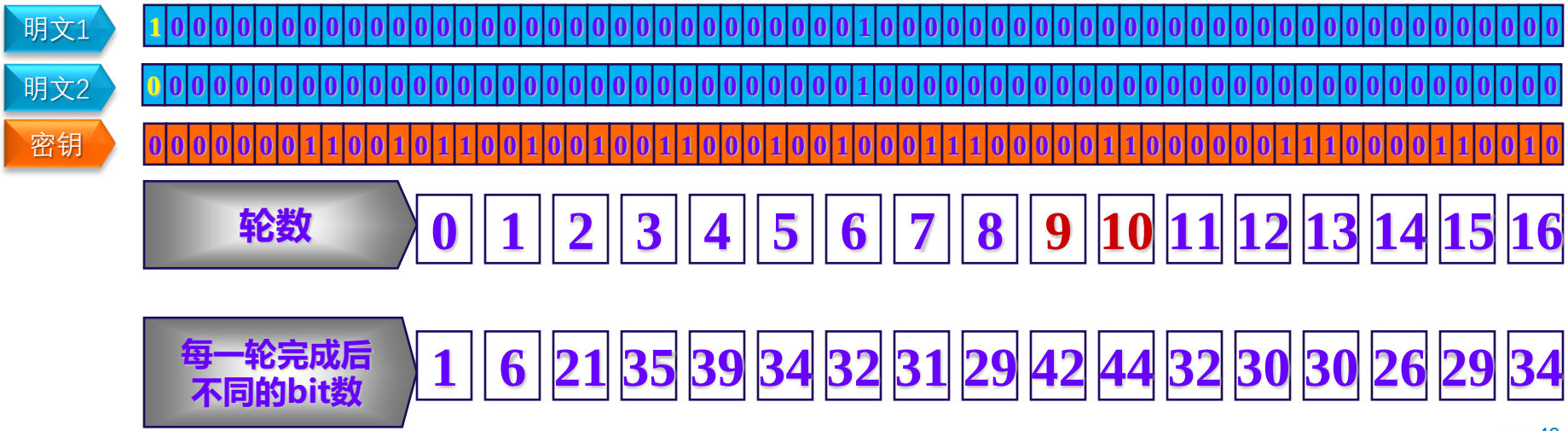
Generalised Feistel:

- CAST-256
- CLEFIA
- MacGuffin
- RC2
- RC6
- Skipjack
- SMS4
- KASUMI
- LOKI97
- Lucifer
- MARS
- MAGENTA
- MISTY1
- RC5
- Simon
- TEA
- Triple DES
- Twofish
- XTEA

目录 | CONTENTS

3 分析和讨论

- 数据加密标准：DES
  - 扩展（Diffusion）：效果显著
  - 雪崩效应：明文输入发生微小变化，密文输出就会截然不同



3 分析和讨论

- **数据加密标准：DES**
  - **混淆（Confussion）：效果显著**
  - **雪崩效应：密钥输入发生微小变化，密文输出就会截然不同**

明文 0 1 1 0 1 0 0 1 0 0 0 1 0 0 0 0 1 1 0 0 0 1 0 1 0 0 1 1 0 0 1 0 0 1 1 0 0 0 0 0 0 1 0 1 0 0 0 1 1 0 0 0 0 1 1 0 0 0 1 1 0 0 1 0

密钥1 1 1 1 0 0 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 1 0 0 0 0 1 1 1 0 1 0 0 1 1 1 0 0 1 0 0 0 1 0 0 1 1 1 0 0 0 1 0 1 1 0 1 1 1 0 0 0

密钥2 0 1 1 0 0 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 1 0 0 0 0 1 1 1 0 1 0 0 1 1 1 0 0 1 0 0 0 1 0 0 1 1 1 0 0 0 1 0 1 1 0 1 1 1 0 0 0

轮数	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
每一轮完成后不同的bit数	0	2	14	28	32	30	32	35	34	40	38	31	33	28	26	34	35

3 分析和讨论

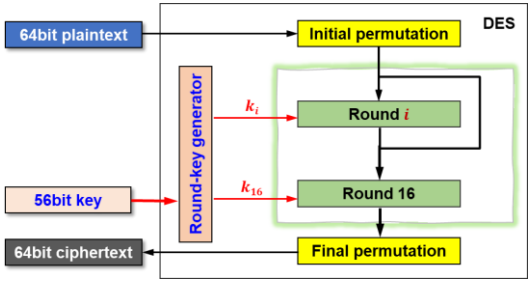
- **数据加密标准：DES**
  - 混淆和扩展
  - 雪崩效应
  - **主要问题**
    - **S-Boxes的设计方案没有公布**
    - **密钥长度56 Bits太短**
      - **难以抵御蛮力攻击：当今最强的超算可以毫秒杀**
      - **可以考虑使用多重加密(3DES)来解决 (1999~2023)**

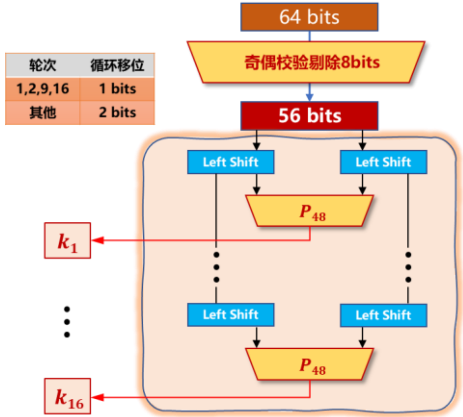
DES最终被谁给替换了？

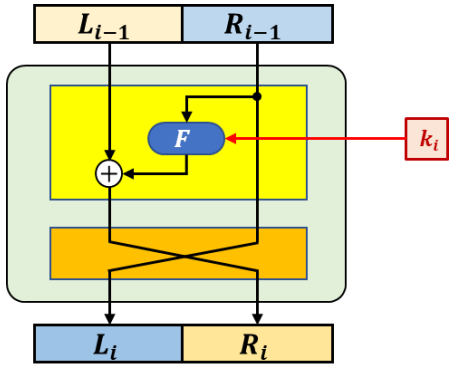
我们将在下节进行探索...

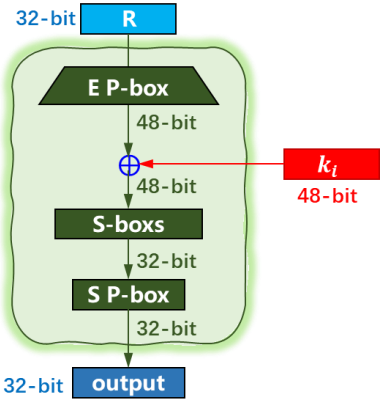
课堂小结

- DES 加密算法
  - 算法流程
  - 密钥扩展
  - 轮函数
    - 扩展置换
    - 加轮密钥
    - 压缩替换
    - 直接置换
- Feistel密码结构
  - 主要特性









Thanks!