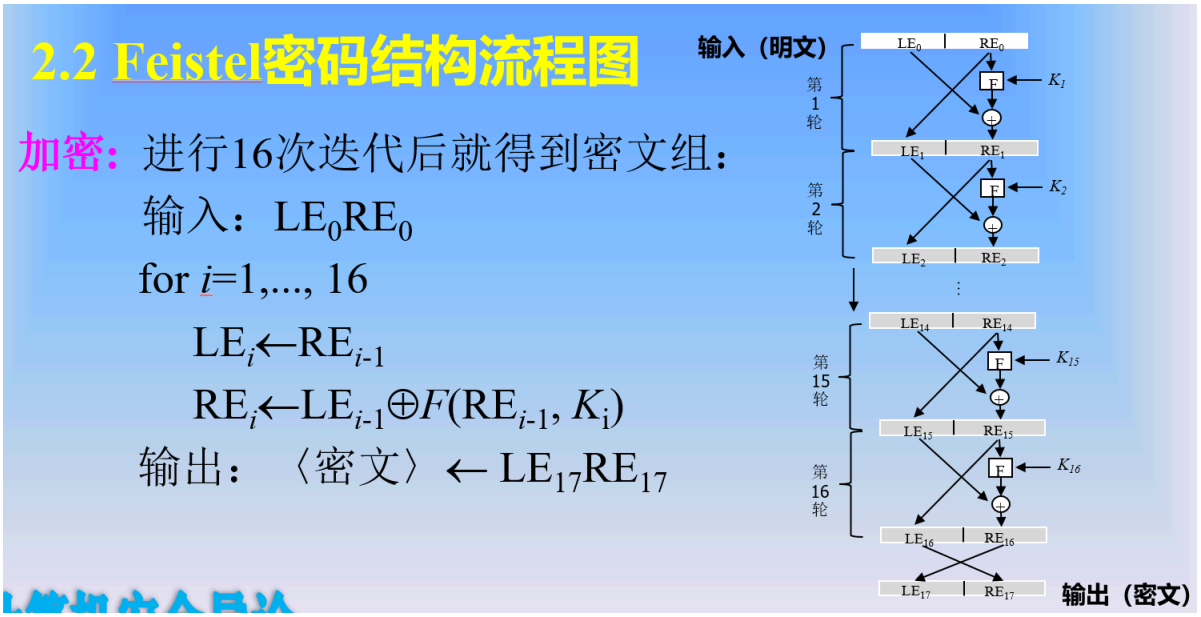
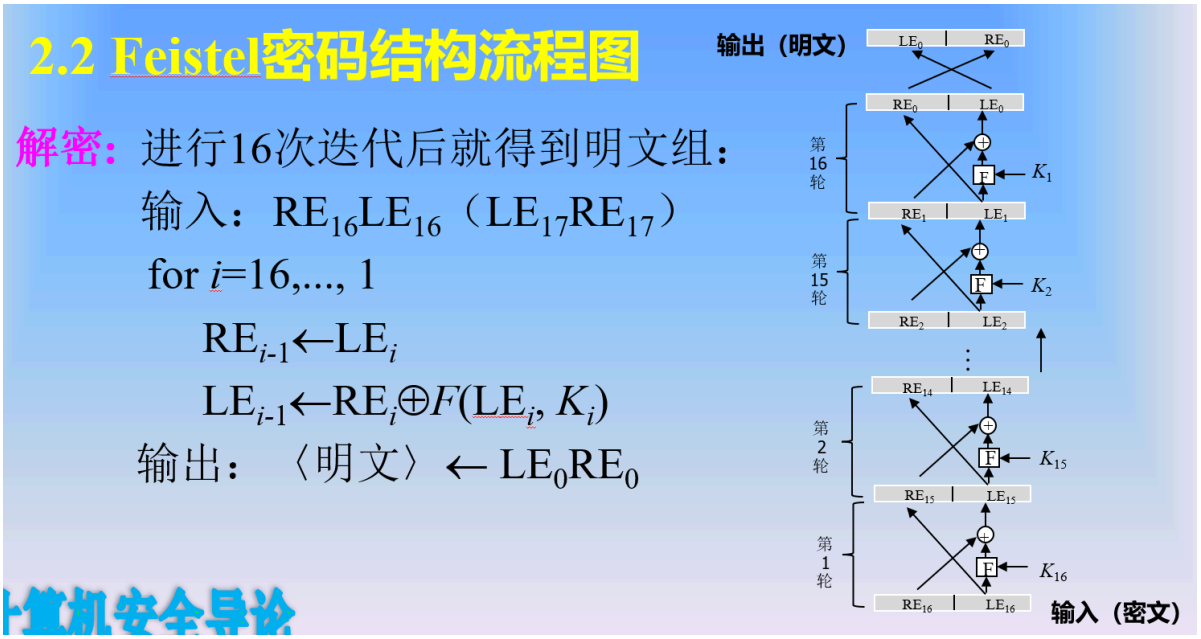
分组密码

分组密码

- 定义：将被加密明文划分成一个一个的分组，输入n比特明文分组，输出n比特密文分组。若映射可逆，具有$2^n!$种替换可能性。
  - 若n较小时：为古典替换密码，易受频度分析法攻击
  - 若n较大时：映射本身构成密钥，密钥长度定义为$n*2^n$比特。实际应用中不大可能传输或保存如此多的密钥。

Feistel密码结构



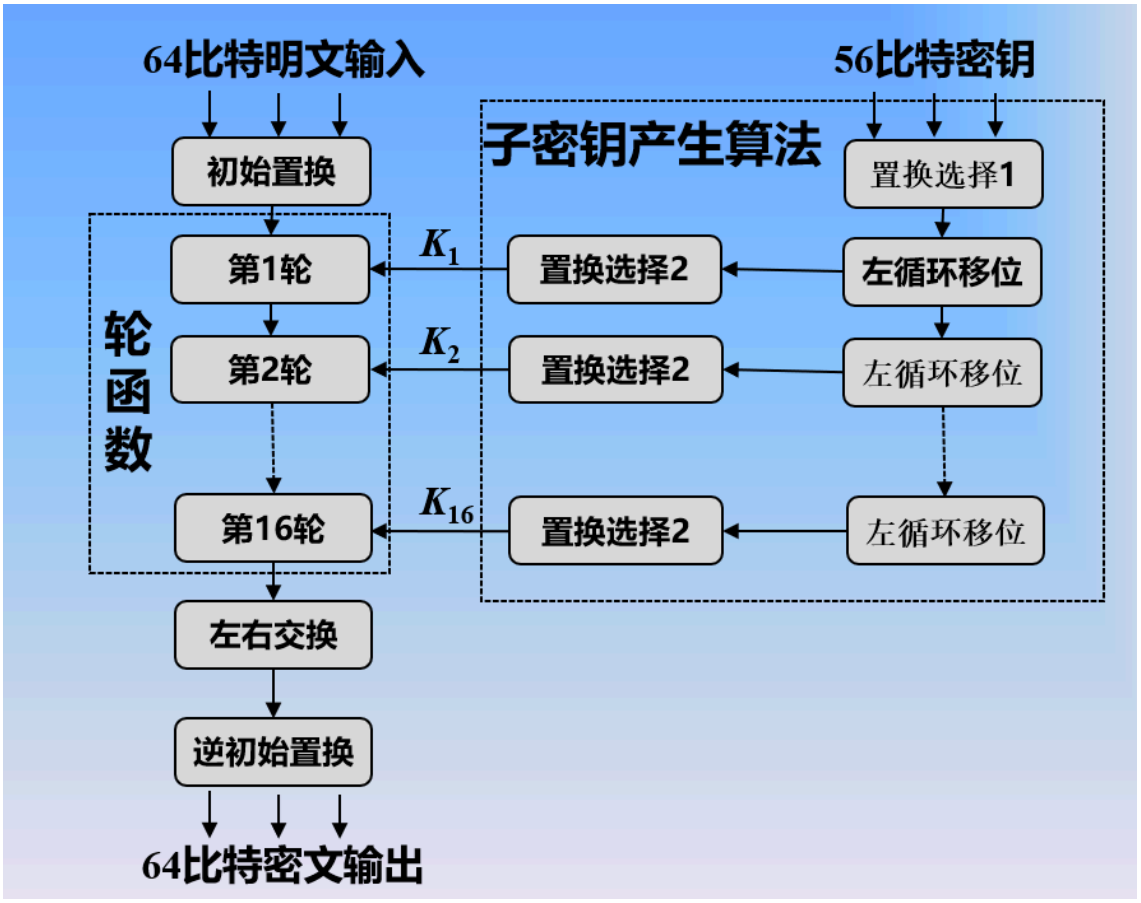


- 设计要素
  - 分组大小：分组越大，安全性越高，加解密速率越慢。
  - 密钥大小：密钥越长，安全性越高，加解密速率也许会减小。
  - 迭代次数：多轮处理能提供更高的安全性。
  - 子密钥产生算法：算法复杂度越高，密码破译难度越高。

- 轮函数：越高的复杂度意味着对破译阻力越大。
- 快速软件加密/解密：容易嵌入到现有的应用程序或实用工具中。
- 容易分析：容易分析该算法的弱点并给出强度更高的保障。

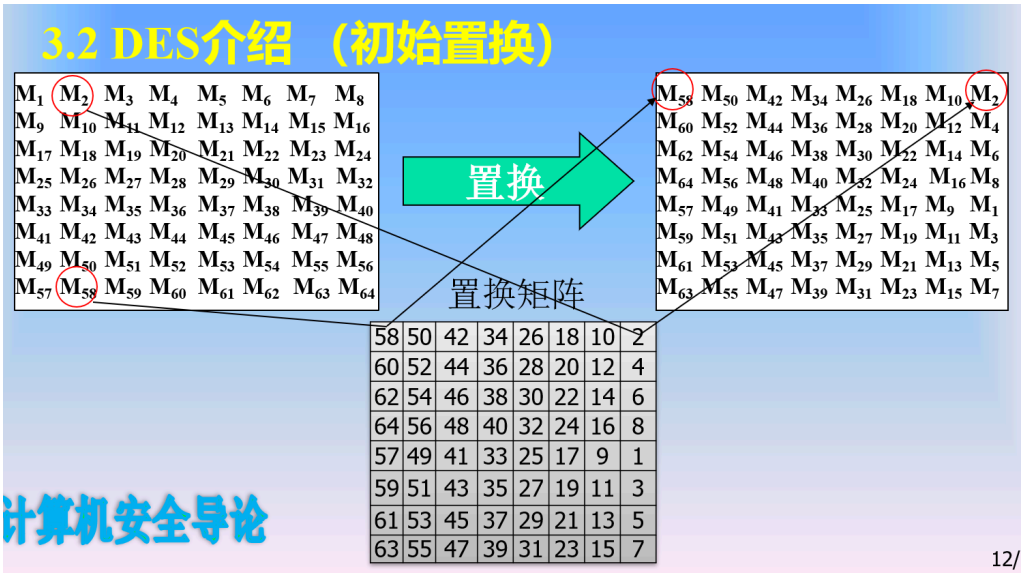
数据加密标准(DES)

- 定义：明文分组长度为 64-bit ，密钥长度为56-bit，在基于Feistel网络的基础上，采用16轮迭代，从原始56-bit密钥产生16组子密钥，每一轮迭代使用一个子密钥。
- DES的三个操作：1）初始置换；2）轮函数操作；3）子密钥产生算法。

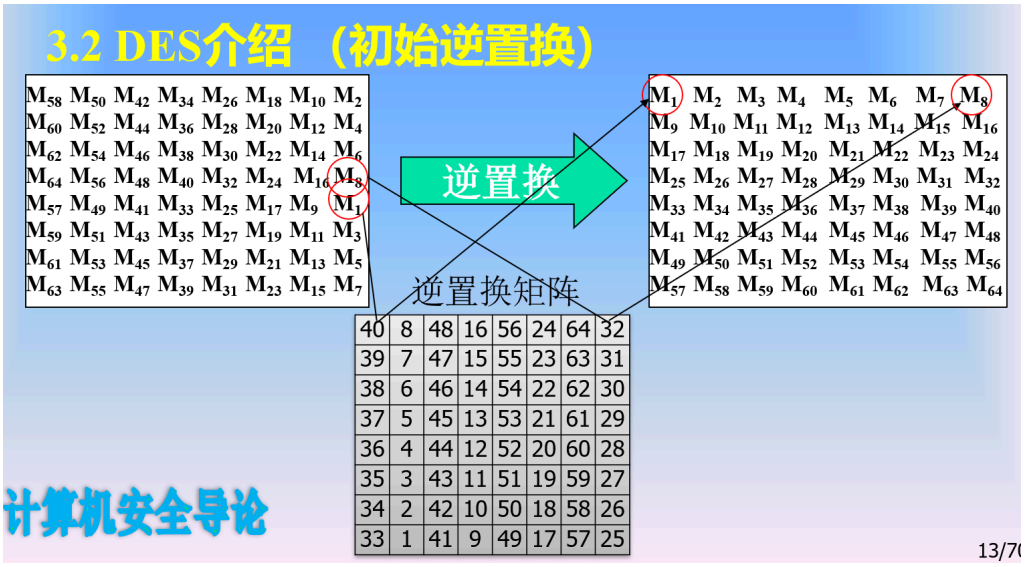


- 初始置换

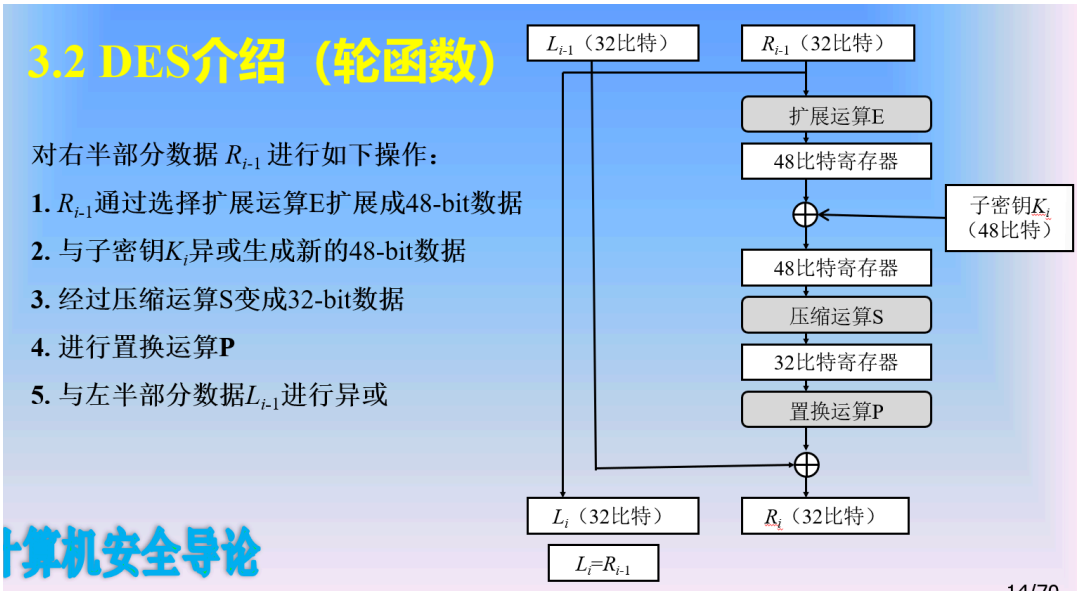
置换矩阵



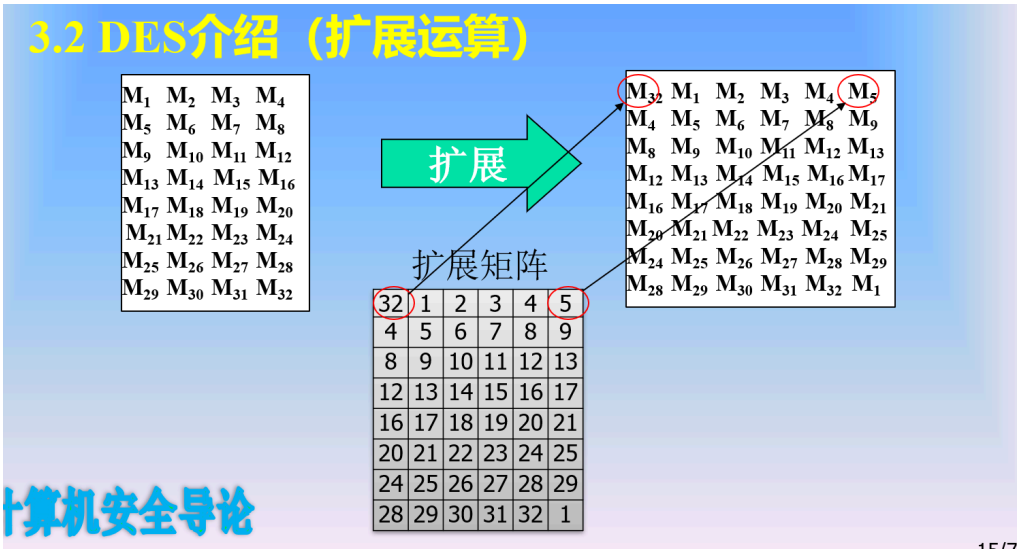
置换矩阵
逆置换矩阵



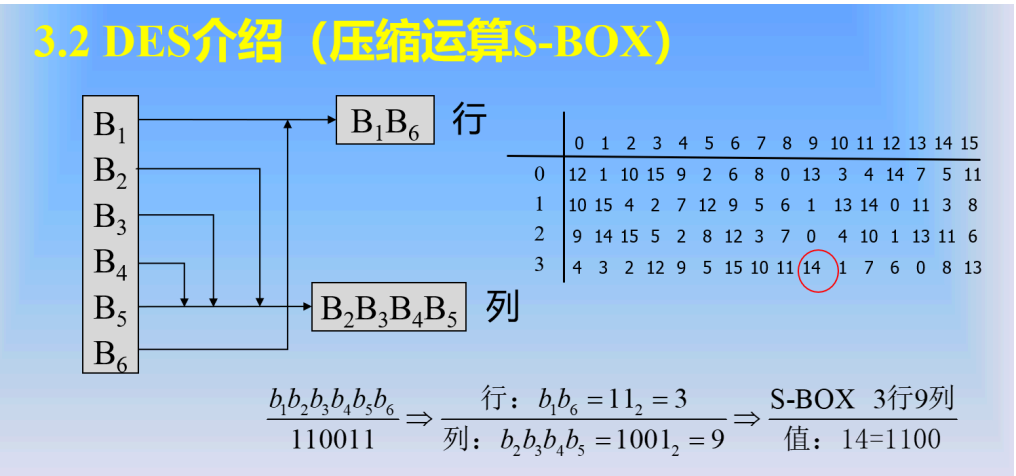
- 轮函数操作



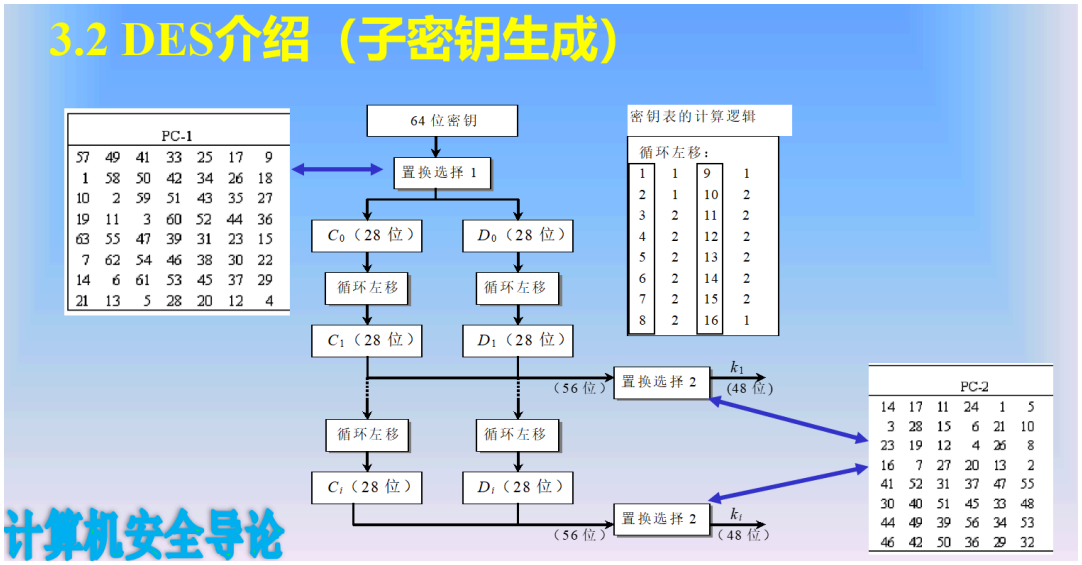
- 拓展运算：32bit按照4*8的矩阵排列，然后左右分别新增一列（共两列）。



- 压缩运算：**非线性，不可逆**

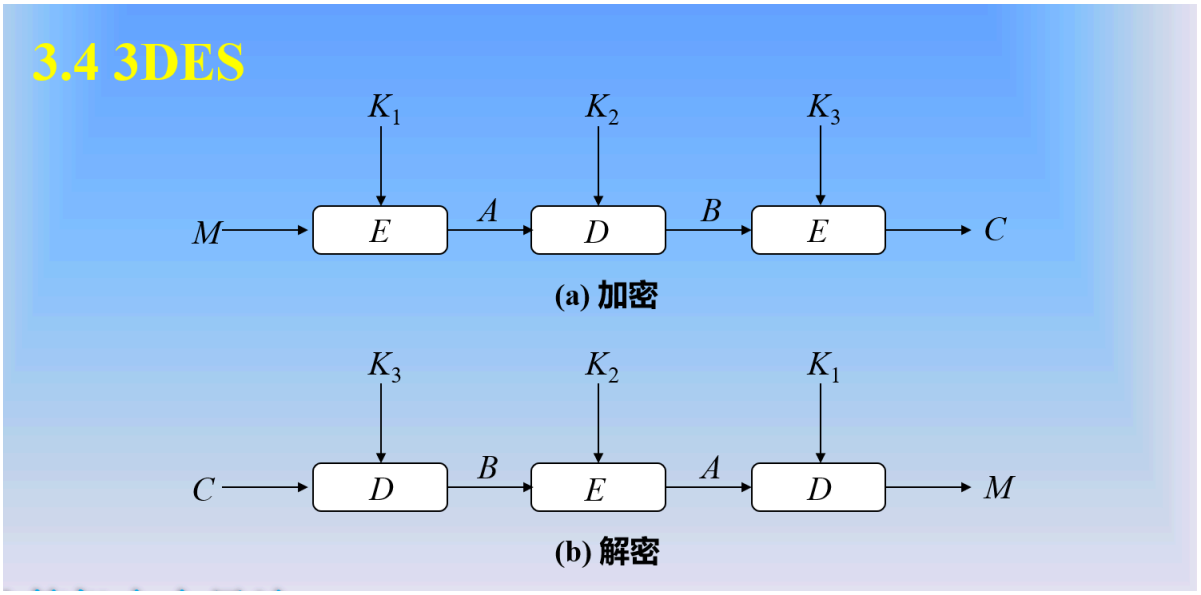


- 子密钥产生算法：首先64位密钥按8*8排列，然后删除最右边的一列（奇偶校验位），即8、16.....64，然后分为左右两半分别进行循环左移（对于i=1，2，...，16，对于Ci和Di，若i为1，2，9或16，则循环左移一位，否则循环左移两位。），置换选择（根据置换表）。



- DES的安全强度
  - 对算法本身的分析：指得是通过研究DES算法的性质而找到破译算法的可能性。DES是现存加密算法中被研究得最彻底的一个，至今没有成功找到DES的致命缺陷。
  - 对使用56-bit密钥的分析：计算速度的提升使得56-bit密钥的使用变得不安全，在有限时间内使用超算技术可以穷举搜索56-bit密钥的所有组合。

三重DES



3.4 3DES（两个密钥）

- 使用3重DES加密，一般需要3个不同密钥，但也可以在*E-D-E*序列下使用2个密钥

$$C = E_{K1}(D_{K2}(E_{K1}(M)))$$

- 在安全上加密和解密是等效的

K1=K2，相当于单个DES

3.4 3DES（三个密钥）

- 采用三个密钥的3DES的加密过程如下所示：

$$C = E_{K3}(D_{K2}(E_{K1}(M)))$$

- 解密过程仅仅是使用相反的密钥顺序进行操作：

$$M = D_{K1}(E_{K2}(D_{K3}(C)))$$