

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

2.2 Feistel密码结构流程图

加密： 进行16次迭代后就得到密文组：

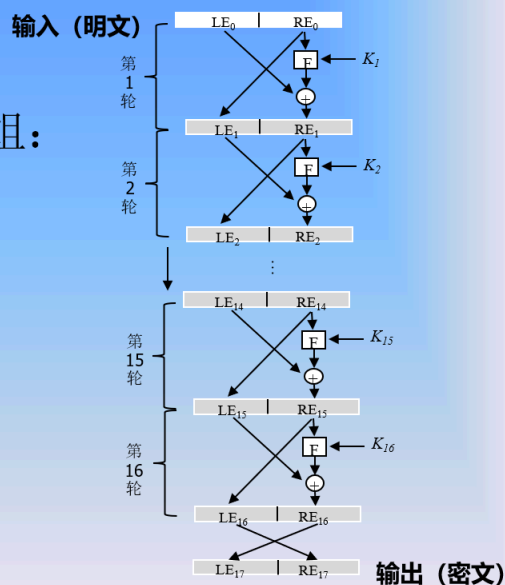
输入： LE_0RE_0

for $i=1, \dots, 16$

$LE_i \leftarrow RE_{i-1}$

$RE_i \leftarrow LE_{i-1} \oplus F(RE_{i-1}, K_i)$

输出：〈密文〉 $\leftarrow LE_{17}RE_{17}$



2.2 Feistel密码结构流程图

解密： 进行16次迭代后就得到明文组：

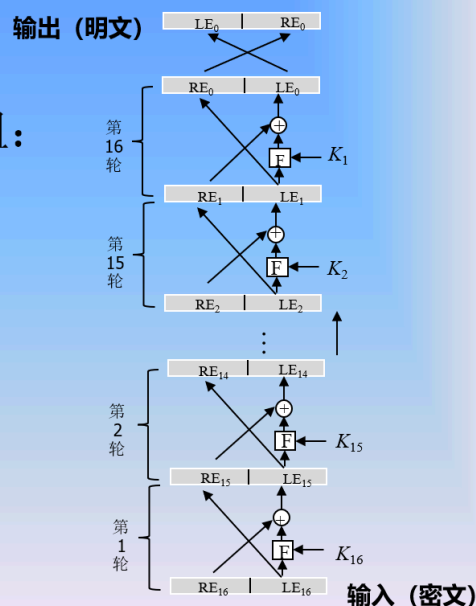
输入： $RE_{16}LE_{16}$ ($LE_{17}RE_{17}$)

for $i=16, \dots, 1$

$RE_{i-1} \leftarrow LE_i$

$LE_{i-1} \leftarrow RE_i \oplus F(LE_i, K_i)$

输出：〈明文〉 $\leftarrow LE_0RE_0$

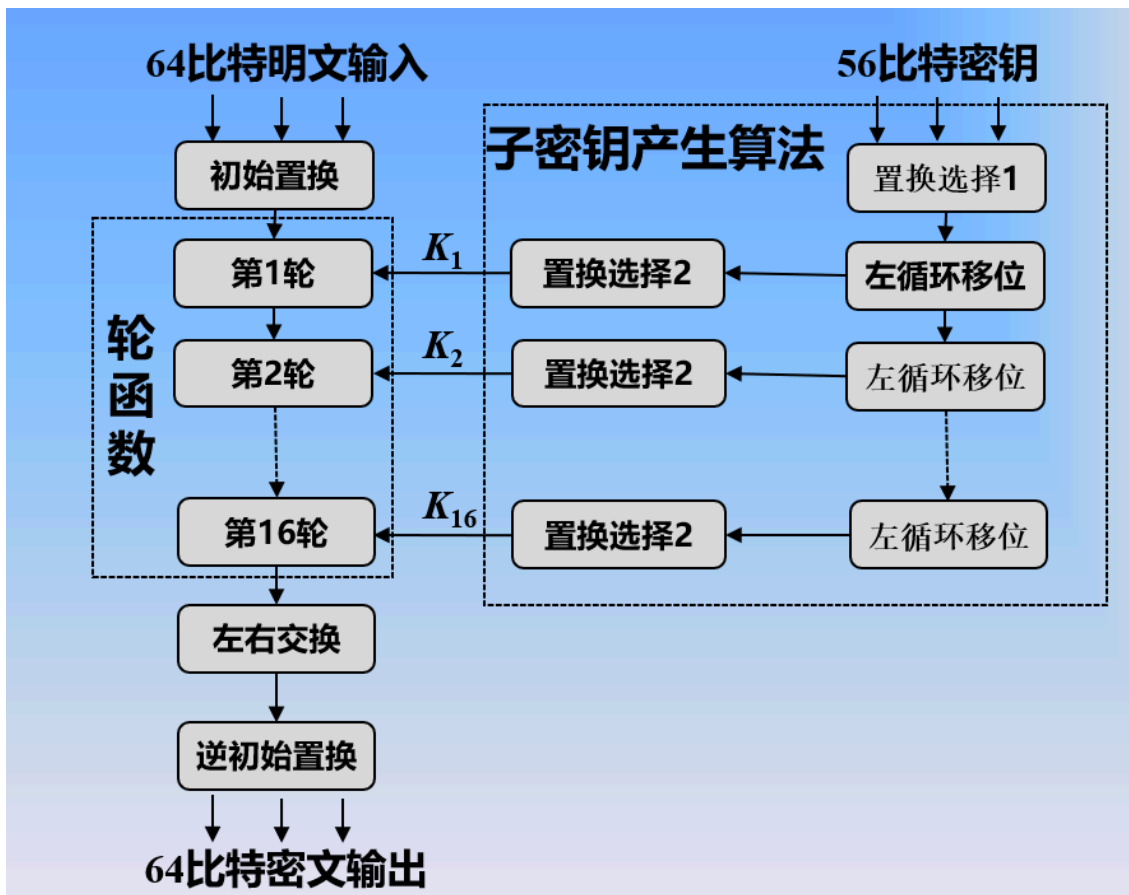


- 设计要素
 - 分组大小：分组越大，安全性越高，加解密速率越慢。
 - 密钥大小：密钥越长，安全性越高，加解密速率也许会减小。
 - 迭代次数：多轮处理能提供更高的安全性。
 - 子密钥产生算法：算法复杂度越高，密码破译难度越高。

- 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

3.2 DES介绍 (初始置换)

置换矩阵

置换

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

置换矩阵

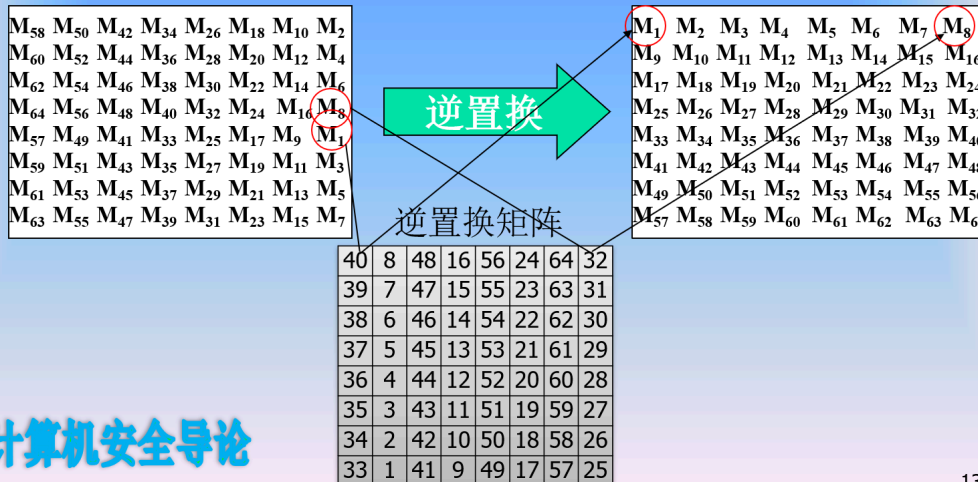
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

计算机安全导论

置换矩阵

逆置换矩阵

3.2 DES介绍 (初始逆置换)



计算机安全导论

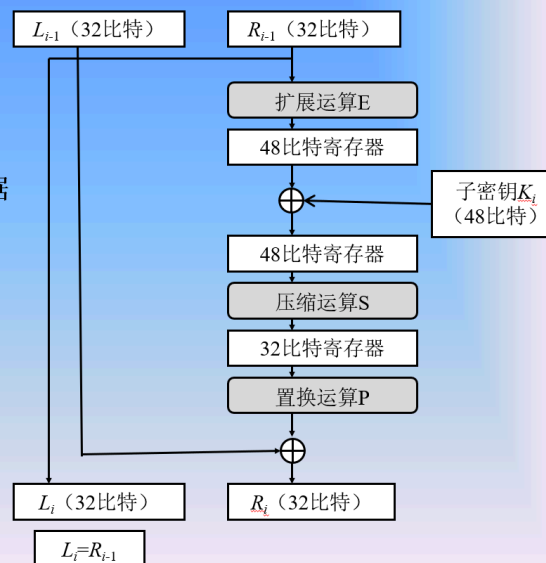
13/71

轮函数操作

3.2 DES介绍 (轮函数)

对右半部分数据 R_{i-1} 进行如下操作：

1. R_{i-1} 通过选择扩展运算E扩展成48-bit数据
2. 与子密钥 K_i 异或生成新的48-bit数据
3. 经过压缩运算S变成32-bit数据
4. 进行置换运算P
5. 与左半部分数据 L_{i-1} 进行异或



计算机安全导论

14/71

- 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）。

3.2 DES介绍 (扩展运算)

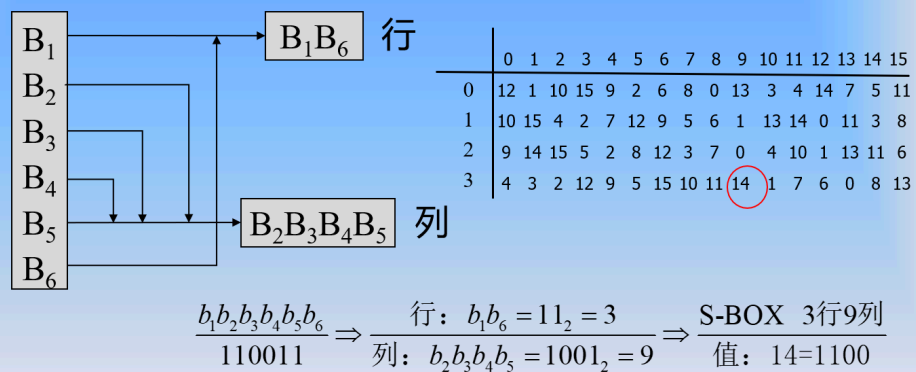


计算机安全导论

15/71

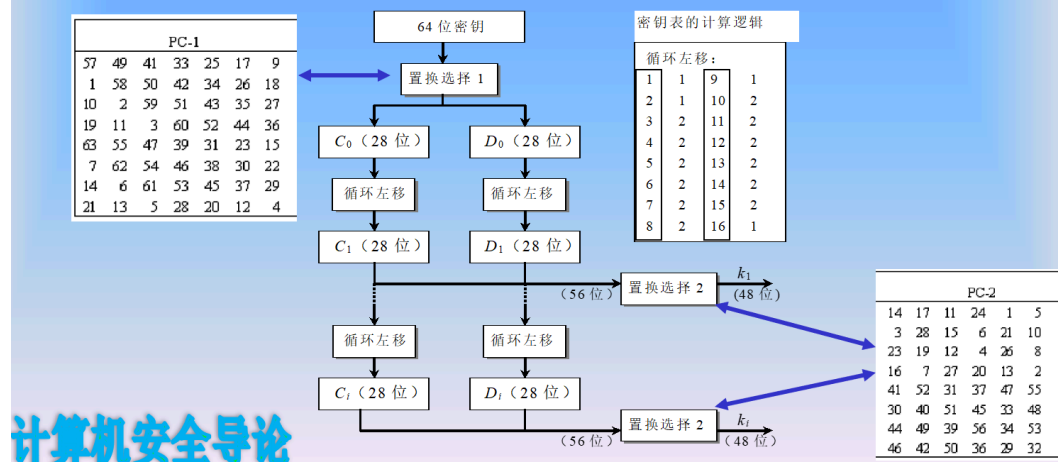
- 压缩运算：非线性，不可逆

3.2 DES介绍 (压缩运算S-BOX)



- 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 $i=1, 2, \dots, 16$ ，对于 C_i 和 D_i ，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）。

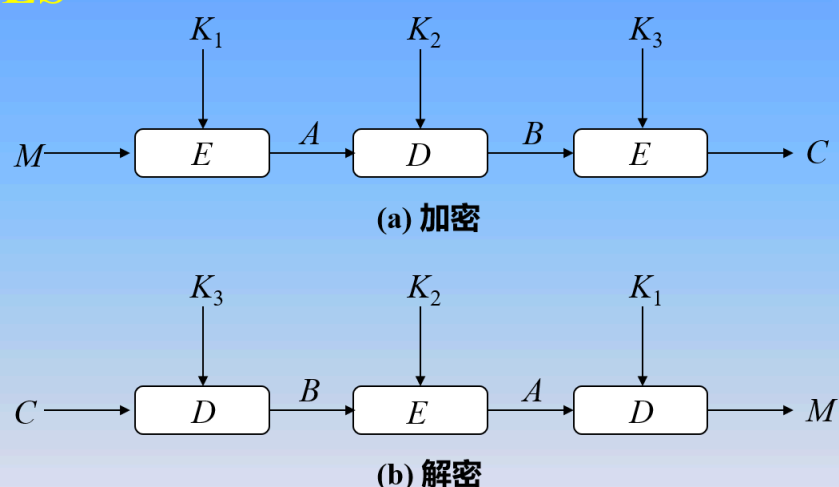
3.2 DES介绍 (子密钥生成)



- 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



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

$$K1=K2, \text{ 相当于单个DES}$$

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：

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