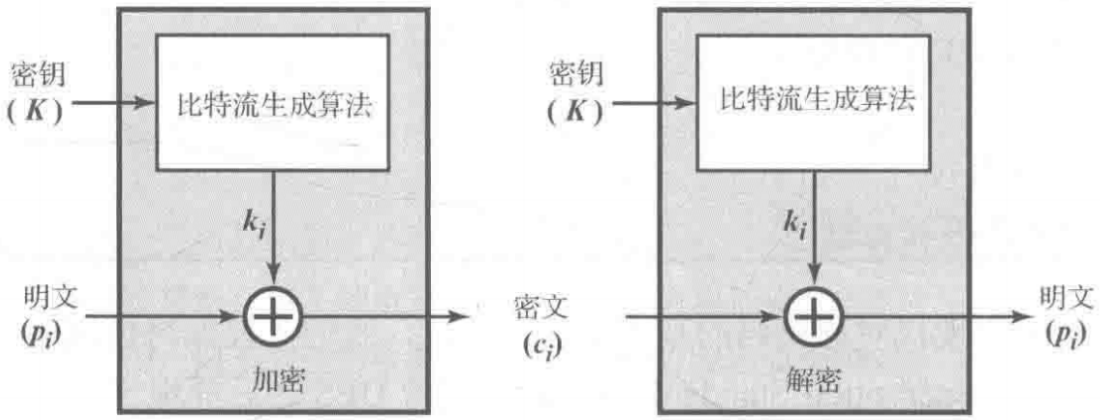
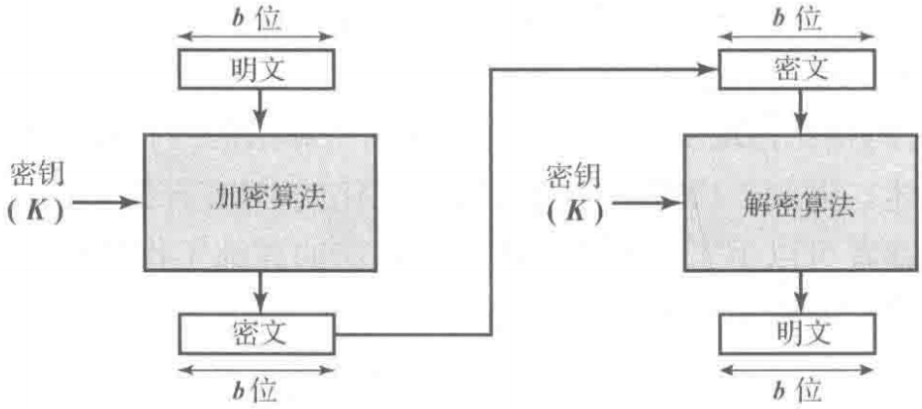
> 教材第四章

流密码与分组密码

- 都是对称加密范围内的
- 流密码的加解密过程为异或，而分组密码的加解密过程比较复杂



(a) 使用算法比特流发生器的流密码

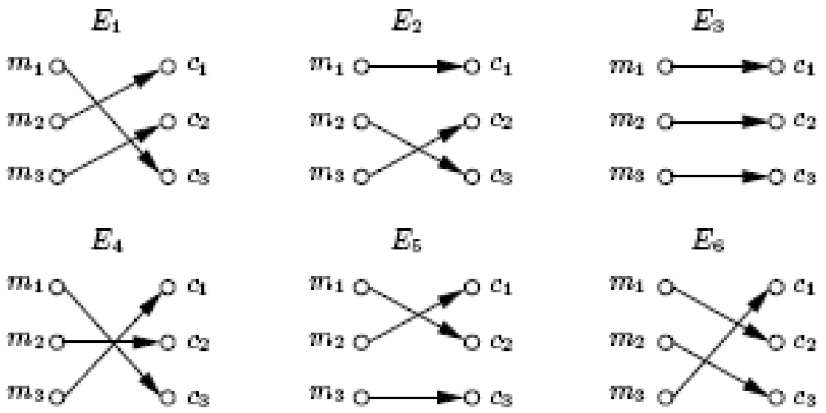


(b) 分组密码

图 4.1　流密码和分组密码

课件中的问题：

- **Assume M={m1,m2,m3}, C={c1,c2,c3}, K={1,2,3,4,5,6} and $C=E_k(M)$, $M=D_k(C)$**

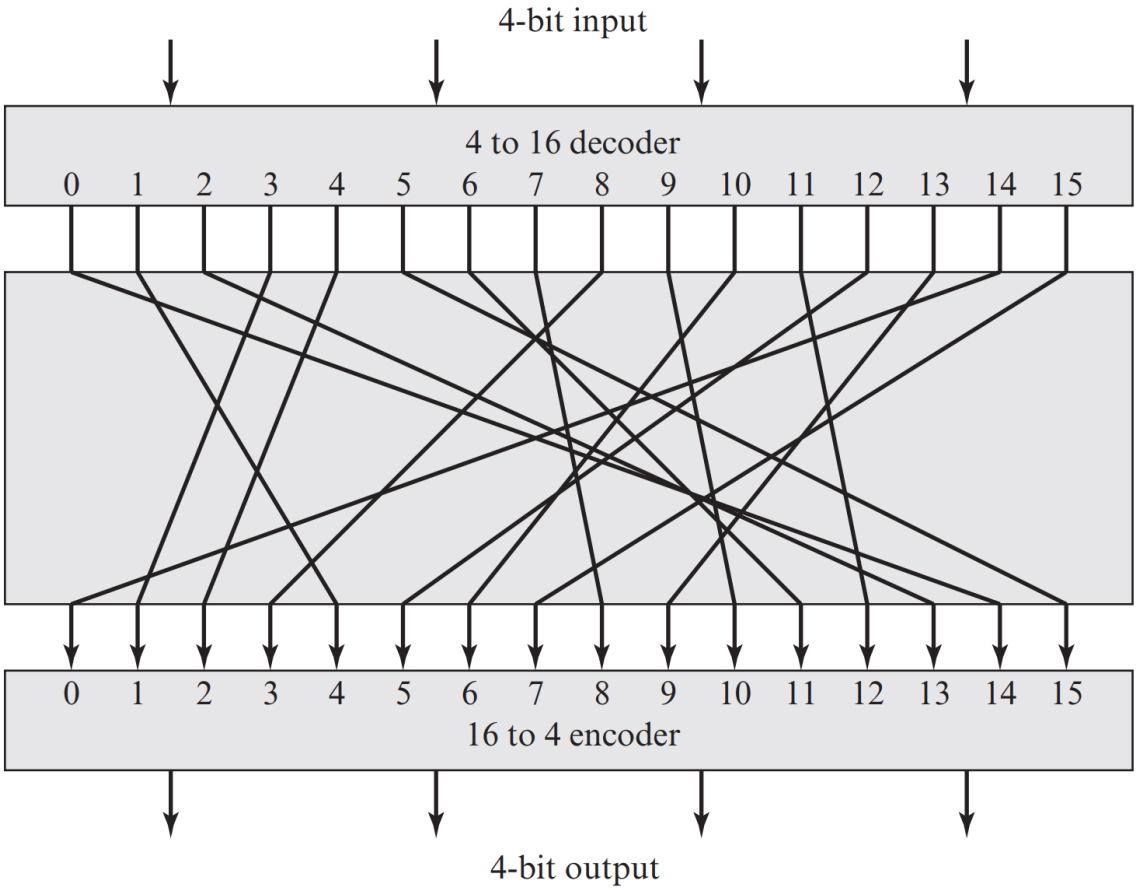


Number of substitution tables: 3!= 6
number of keys: 6

1. 密钥空间如何计算?
   - $3! = 6$
2. 需要几对明密文才能找到真正的钥匙?
   - $(3-1)! = 2$

理想分组密码

分组密码作用在 n 位明文组上，而产生 n 位密文组。n 位明文组可以组合出 2^n 个不同明文组，且由于加密是可逆的，每一个明文组将唯一对应一个密文组。这样的变换称为可逆变换，不同变换的总数（即密钥空间）是 $2^n!$ 个。下图为 $n = 4$ 时的一个普通代替密码的结构，4 位的输入有 16 种可能的输入状态：



对应的加解密表

Plaintext	Ciphertext
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

Ciphertext	Plaintext
0000	1110
0001	0011
0010	0100
0011	1000
0100	0001
0101	1100
0110	1010
0111	1111
1000	0111
1001	1101
1010	1001
1011	0110
1100	1011
1101	0010
1110	0000
1111	0101

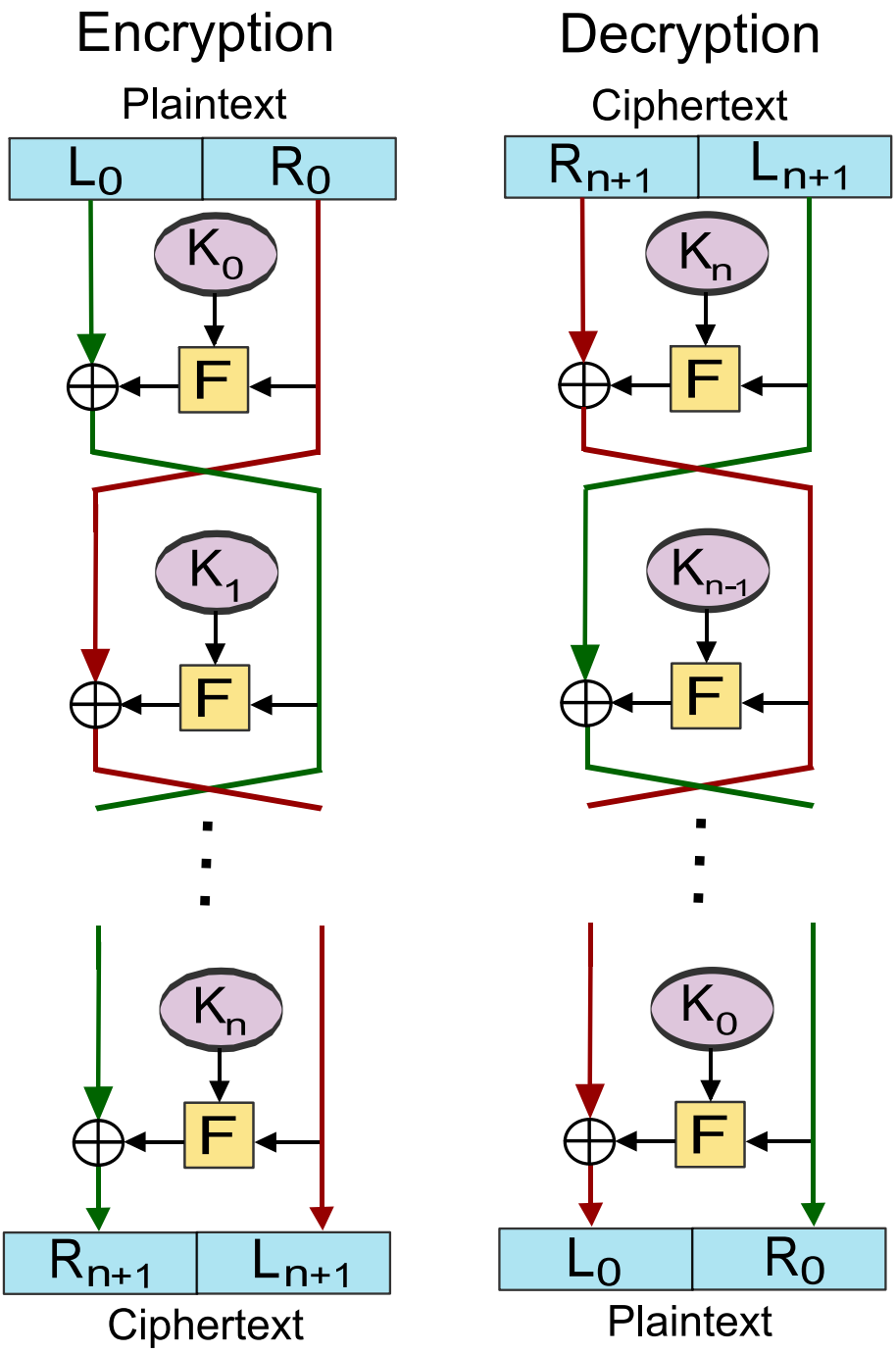
Feistel 称这种密码为理想分组密码，因为它允许生成最大数量的加密映射来映射明文分组。**然而**在实现角度，这样的分组密码是不可行的。对于这样的变换，映射本身就是密钥。如上例，密钥长度为 4 位 $\times 16$ 种 $= 64$ 位。一般地，对于 n 位的代替分组密码，密钥长度是 $n \times 2^n$ 位。一个 64 位的分组密码，若分组有抵抗统计攻击的理想长度，其密钥大小将需要 $64 \times 2^{64} = 2^{70} \approx 10^{21}$ 位。考虑到这些困难（Feistel 密码结构的设计动机在此），在实践中只能使用理想分组密码体制的近似体制。

Feistel 结构

是密码设计的一个主要原则，而不是一个特殊的密码。Feistel 建议使用乘积密码的概念来逼近理想分组密码，乘积密码是指依次使用两个或两个以上基本密码（如代替、置换）。

- 如何挫败基于统计方法的密码分析?
    - 扩散（diffusion）：扩散指使明文的统计特征消散在密文中，可以让每个明文数字尽可能地影响多个密文数字获得，等价于说每个**密文**数字被许多**明文**数字影响。例如：通过使用置换和线性替换的方法。
    - 混淆（confusion）：其目的在于使作用于**密钥**和**密文**之间的关系复杂化，是明文和密文之间、密文和密钥之间的统计相关特性极小化，从而使统计分析攻击不能奏效。例如：通过使用非线性替换。

Feistel 密码结构（Feistel 结构的对合性保证加解密可逆）：



Feistel 的具体实现依赖以下参数：分组长度、密钥长度、迭代次数、子密钥（$K_0, \cdots, K_n$）产生算法、轮函数（F）。

DES

- DES 细节不要求掌握，https://www.bilibili.com/video/BV1QW411B7A4/
- DES 的明文分组长度为 64 位，AES 为 128 位
- 雪崩效应（验证扩散和混淆）：明文或密钥的某一位发生变化会导致密文的很多位发生变化，这被称为雪崩效应（教材 P80）

DES 强度

从暴力破解和互补方面分析。

差分分析：通过适当选择明文得到密文比较它们的差异以推导出使用的密钥（**不考**）

思考题

4.3

> 为什么使用表 4.1 所示的任意可逆代替密码不实际?

上面有解释，当明文位数很大时，密钥体积过大。

4.5

> 混淆与扩散的差别是什么?

混淆：使密钥和密文之间的统计关系变得复杂。
扩散：使明文和密文之间的统计关系变得复杂。

4.6

> 哪些参数与设计选择决定了实际的 Feistel 密码算法?

分组长度、密钥长度、迭代次数、子密钥（$K_0, \cdots, K_n$）产生算法、轮函数（F）。

习题

4.1

> (a) 在 4.1 节名为“Feistel 密码结构的设计动机”的小节里说到，对于 n 个位的分组长度，理想分组密码的不同可逆映射个数为 $2^n!$ 个。请证明。

对于一个 n 位的分组，有 2^n 个可能的不同明文块和 2^n 个可能的不同密文块。明文到密文的双射的种数可理解为 2^n 个元素进行全排列，因此共有 $2^n!$ 种可能性。

> (b) 在同样的小节里说到，对于理想分组密码，若允许所有可逆映射，则密钥的长度为 $n \times 2^n$ 位。但是，如果有 $2^n!$ 个映射，则应该需要 $\log_2 2^n!$ 个位就可以区分这 $2^n!$ 个映射。所以密钥长度应为 $\log_2 2^n!$。然而，$\log_2 2^n! < n \times 2^n$。请解释这种差别。

理论上，密钥长度可以是 $\log_2 2^n!$ 位。例如，为每个映射分配一个从 0 到 $2^n - 1$ 的数字（比如密文 0010 对应密钥 10，而之前的方案中密文和密钥都是 0010），并维护一个表来显示每个这样的数字的映射。而之前的方案则把密钥的值直接当作密文，无需维护映射表。