> 教材第七章，第八章第四节、第五节。主要考查工作模式，参考文章

为了将分组密码应用于各种各样的实际应用，NIST 定义了五种“工作模式”。从本质上讲，工作模式是一项增强密码算法或者使算法适应具体应用的技术，如将分组密码应用于数据块组成的序列或者数据流。这五种模式实际上覆盖了大量使用分组密码的应用。

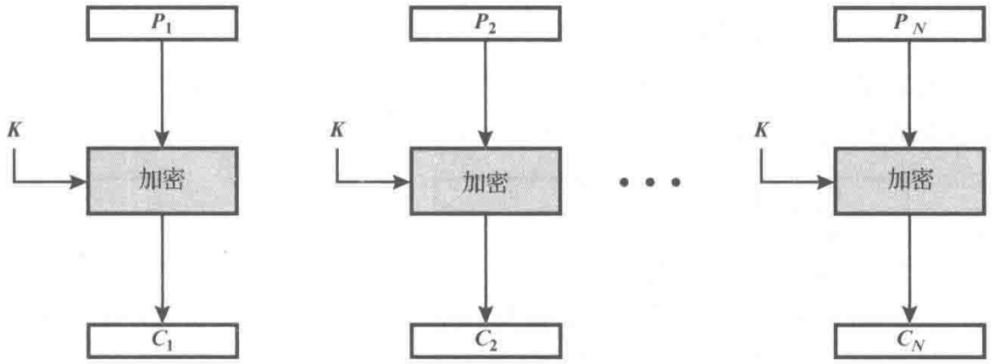
五种工作模式

模式	描述	典型应用
电码本（ECB）	用相同的密钥分别对明文分组独立加密	单个数据的安全传输（如一个加密密钥）
密文分组链接（CBC）	加密算法的输入是上一个密文组和下一个明文组的异或	1. 面向分组的通用传输 2. 认证
密文反馈（CFB）	一次处理 s 位，上一块密文作为加密算法的输入，产生的伪随机数输出与明文异或作为下一单元的密文	1. 面向数据流的通用传输 2. 认证
输出反馈（OFB）	与 CFB 类似，只是加密算法的输入是上一次加密的输出，且使用整个分组	噪声信道上的数据流的传输（如卫星通信）
计数器（CTR）	每个明文分组都与一个经过加密的计数器相异或。对每个后续分组计数器递增	1. 面向分组（？）的通用传输 2. 用于高速需求

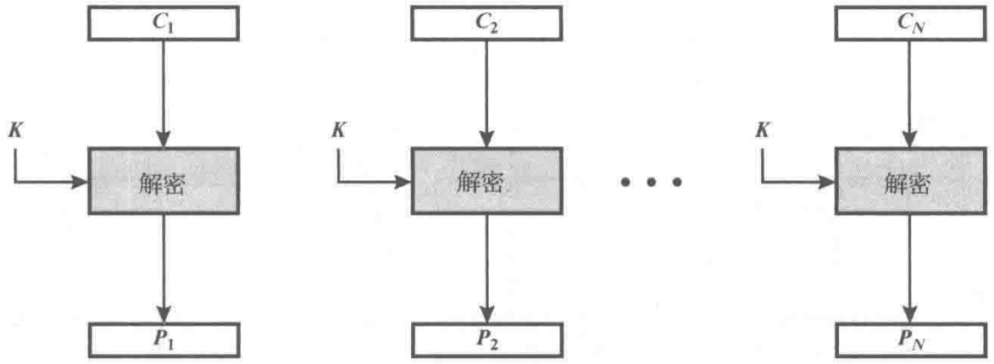
工作模式的评价标准：

- 总体比较：与 ECB 模式相比，用于加密和解密需要额外的操作
- **错误恢复**：第 i 个密文分组的错误会只被模式同步后的一些（少数）明文分组继承
- ☆☆☆ **错误传播**：第 i 个密文分组的错误会被第 i 组及其后所有明文分组继承
- 扩散：明文统计如何反映在密文中
- 安全性：密文分组是否会泄露关于明文分组的信息

电码本（ECB）



(a) 加密



(b) 解密

- 每个消息块都使用相同的密钥独立加密，因此相同的明文块会被加密成相同的密文块，不能很好地隐藏数据模式

> [!NOTE|label:错误传播] 密文传输中的比特错误会在相应的明文分组中造成比特错误，不过这种错误对其他分组没有影响（参考解密流程图）

Given $C_i = E_K(P_i)$ $(i \geq 1)$

$C'_i = E_K(P'_i)$ $(i \geq 1)$

$$P=P_0P_1P_2P_3P_4P_5 \ \cdots \ ; \ C=C_0C_1C_2C_3C_4C_5 \ \cdots$$

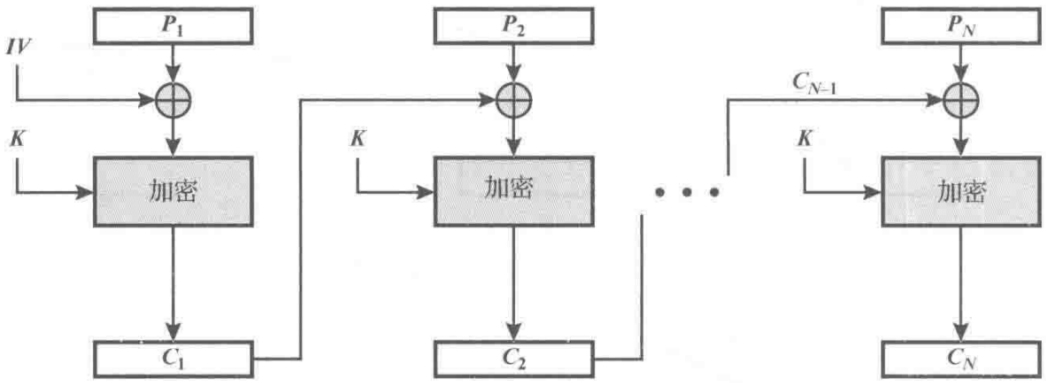
$$P^*=P_0P_1P_1P_1P_4P_5 \ \cdots$$

$$P'=P_0P_1P'_2P'_3P'_4P'_5 \ \cdots$$

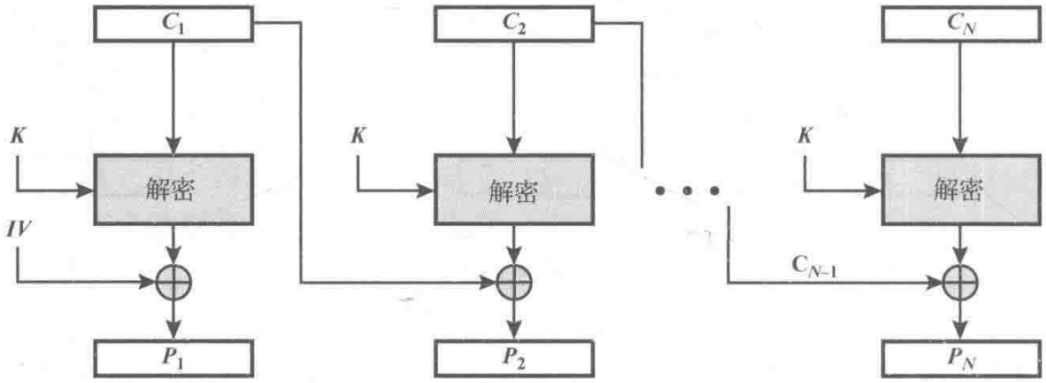
Then, $C^*=C_0C_1C_1C_1C_4C_5 \ \cdots$

$C'=C_0C_1C'_2C'_3C'_4C'_5 \ \cdots$

密文分组链接（CBC）



(a) 加密



(b) 解密

IV（Initialization Vector，初始向量）

- 它的主要缺点在于加密过程是串行的，无法被并行化
- 和 ECB 一样，CBC 下的消息必须被填充到块大小的整数倍，解决这个问题的一种方法是利用密文窃取

> [!NOTE|label:错误传播] 传送过程中密文分组 C_i 的比特错误，在解密时会造成明文分组 P_i 以及下一个明文分组 P_{i+1} 的比特错误，不会影响到其它明文分组。密文分组重复和分组缺失情况见下图：

Example

$C_0 = IV$

$C_i = E_K(P_i \text{ XOR } C_{i-1}) (i \geq 1)$

$P_i = D_K(C_i) \text{XOR } C_{i-1} \ (i \geq 1)$

$C=C_1C_2C_3C_4C_5 \ \ldots$

$P=P_1P_2P_3P_4P_5 \ \ldots$

Case1:

$C'=C_1C'_2C_3C_4C_5C_6 \ldots$

$P'=P_1P'_2P'_3P_4P_5P_6 \ldots$

Case2:

$C'=C_1C_2C_2C_3C_4C_5C_6 \ldots$

$P'=P_1P_2P'_2P_3P_4P_5 \ldots$

Case3:

$C'=C_1C_2C_4C_5C_6 \ldots$

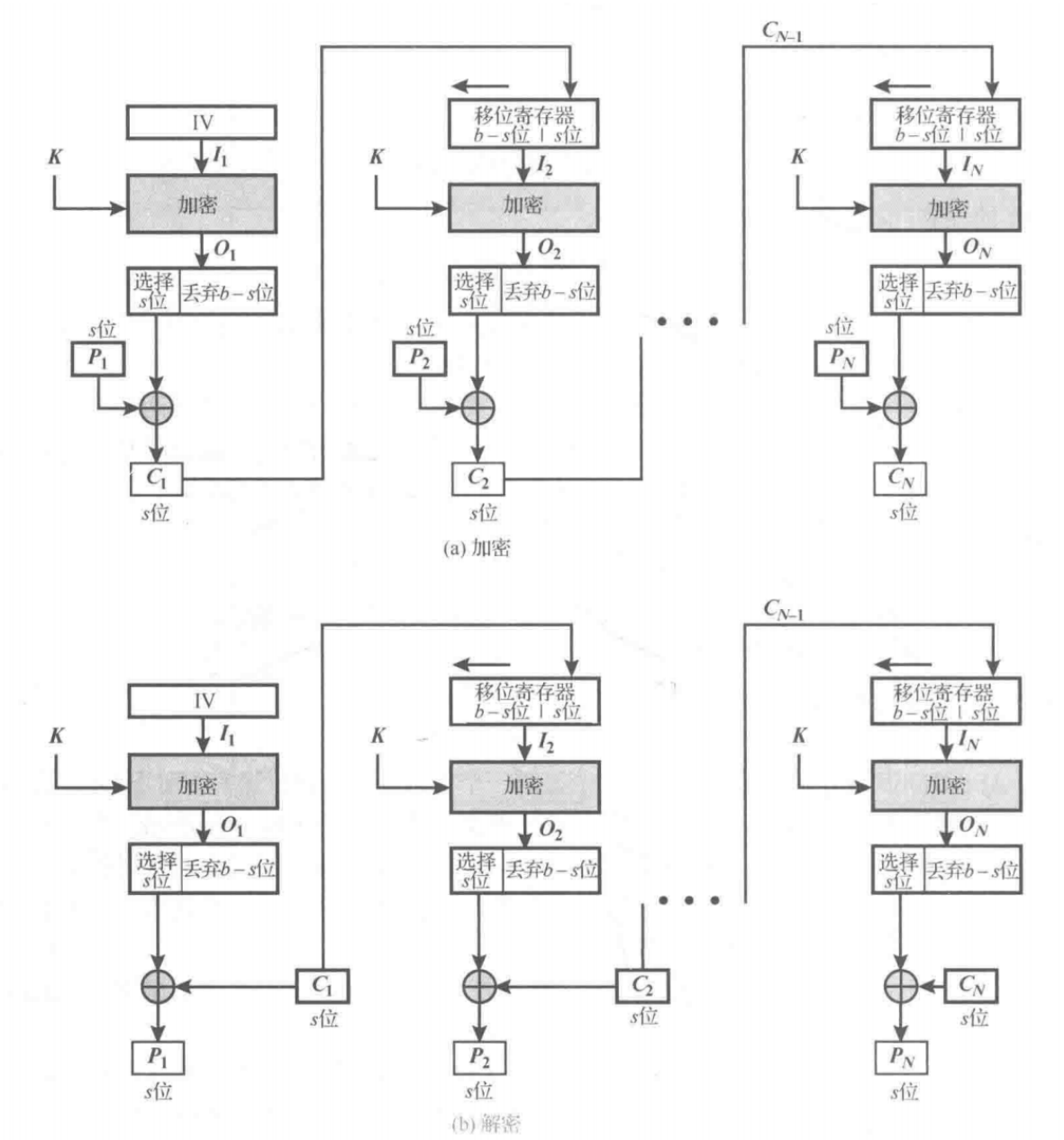
$P'=P_1P_2P'_4P_5P_6 \ldots$

Q:

$C'=C_1C'_2C'_3C'_4C_5C_6C_7C_8 \ldots$

$P'= P_1P'_2P'_3P'_4P'_5P_6P_7P_8 \ldots$

密文反馈（CFB）



- 与 CBC 相似，明文的改变会影响接下来所有的密文，因此加密过程不能并行化，但解密过程是可以并行化的

> [!NOTE|label:错误传播] 密文中一位数据的改变会影响 $1+b/s$ 个明文分组：对应明文分组中的一位数据与后 b/s 分组中全部的数据。密文分组重复和分组缺失情况见下图：

Example

Use CFB-8 for DES

It means that b=64bits and S=8bits

$P_i=f(C_i,C_{i-1},...,C_{i-b/s})$

$C=C_1C_2C_3C_4C_5$ …

$P=P_1P_2P_3P_4P_5$ …

Case1:

$C'=C_1C'_2C_3C_4C_5C_6$ …

$P'=P_1P'_2P'_3P'_4P'_5P'_6P'_7P'_8P'_9P'_{10}P_{11}$ ·

Case2:

$C'=C_1C_2C_2C_3C_4C_5C_6$ …

$P'=P_1P_2P'_2P'_3P'_4P'_5P'_6P'_7P'_8P'_9P'_{10}P_{10}$ ··

Case3:

$C'=C_1C_2C_4C_5C_6$ …

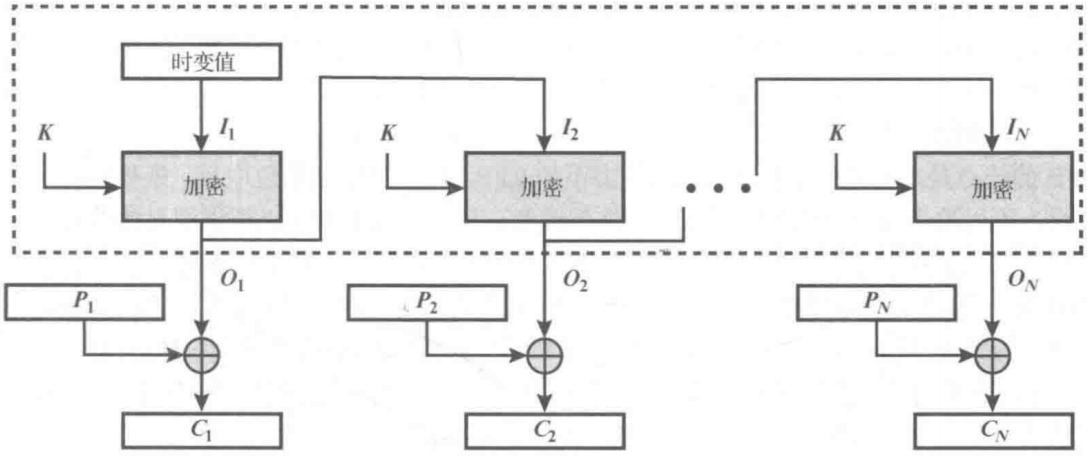
$P'=P_1P_2P'_4P'_5P'_6P'_7P'_8P'_9P'_{10}P'_{11}P_{12}$…

Q:

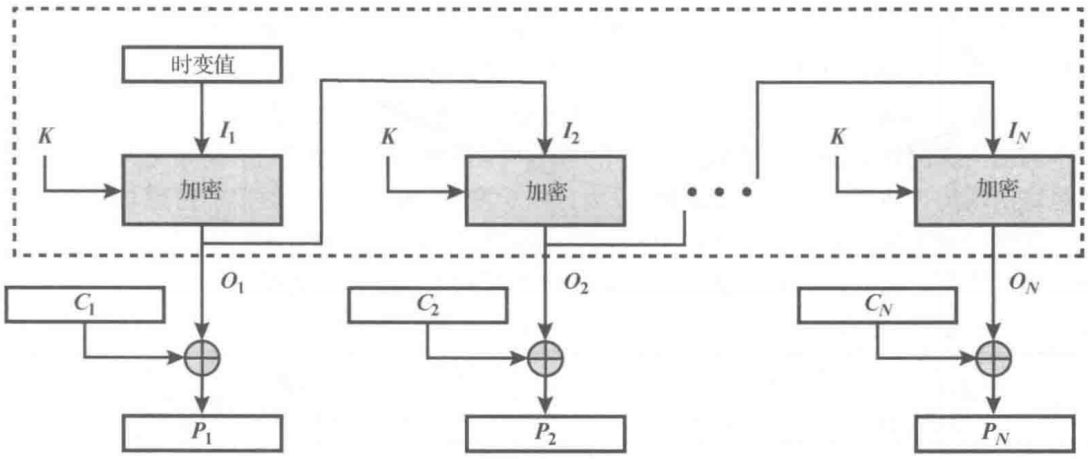
$C'=C_1C'_2C'_3C'_4C_5C_6C_7C_8$ …

$P'=P_1P'_2P'_3P'_4P'_5P'_6P'_7P'_8P'_9P'_{10}P'_{11}P'_{12}P_{13}$ …

输出反馈（OFB）



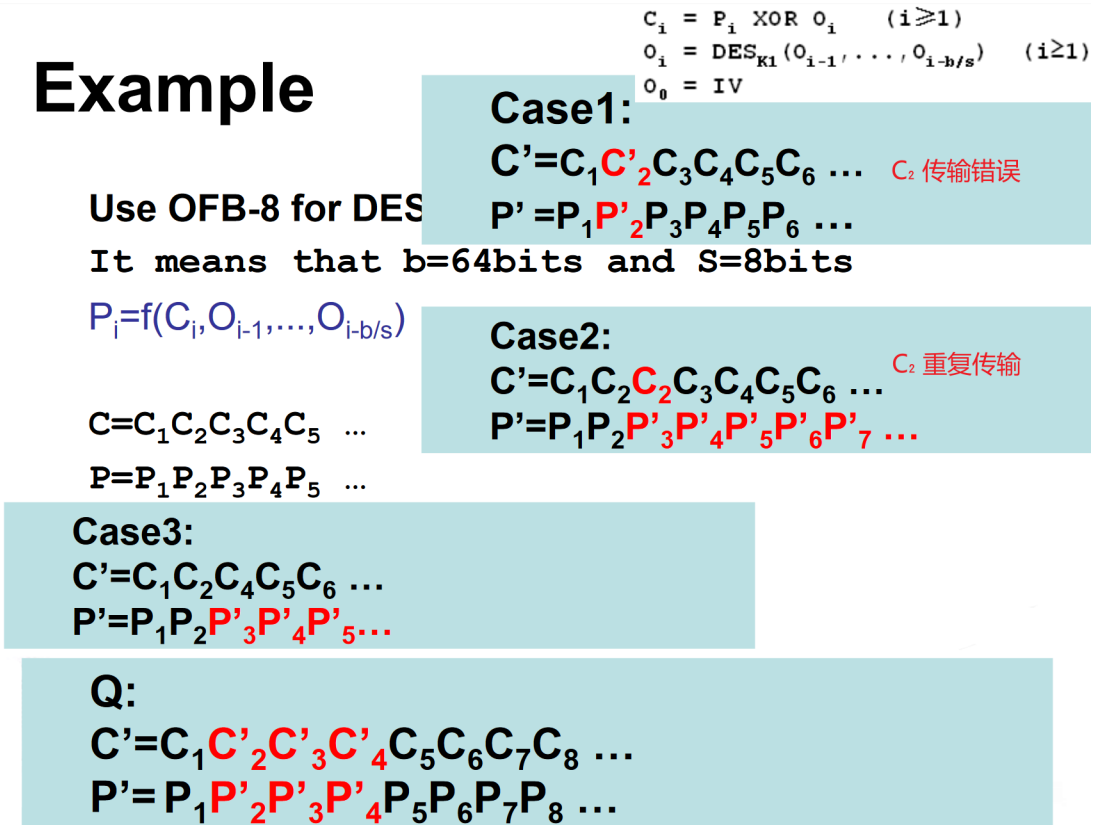
(a) 加密



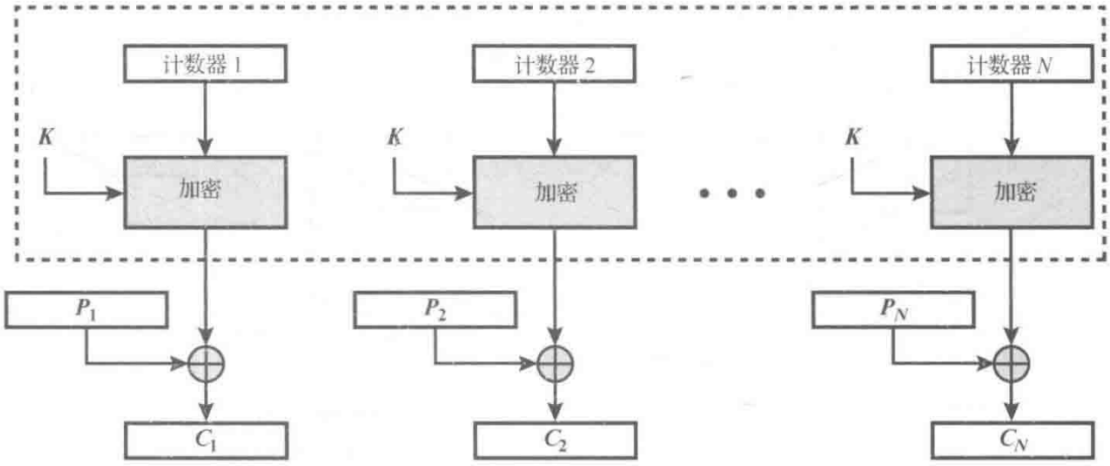
(b) 解密

- 每个使用 OFB 的输出块与其前面所有的输出块相关，因此上图中“加密”部分不能并行化处理，但事先算好“加密”部分后，“异或”部分可以并行处理

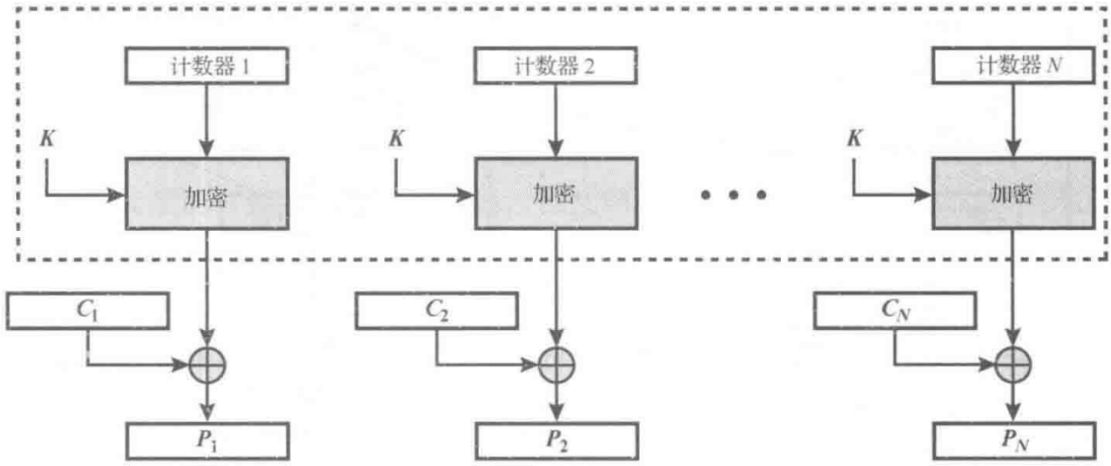
> [!NOTE|label:错误传播] 密文中一位数据的改变仅会影响对应的明文分组。密文分组重复和分组缺失会导致后续解密全错，如下图：



计数器（CTR）



(a) 加密



(b) 解密

- 加密和解密过程均可以并行处理，CTR 是高速的 OFB

> [!NOTE|label:错误传播] 密文中一位数据的改变仅会影响对应的明文分组。密文分组重复和分组缺失会导致后续解密全错（后续每个计数器的值都错了），如下图：

Example

$C=C_1C_2C_3C_4C_5 \ \cdots$

$P=P_1P_2P_3P_4P_5 \ \cdots$

$C_i = P_i \ XOR \ O_i$

$O_i = E_K(i)$

Case1:

$C'=C_1C'_2C_3C_4C_5C_6 \ \cdots$

$P' =P_1P'_2P_3P_4P_5P_6 \ \cdots$

Case2:

$C'=C_1C_2C_2C_3C_4C_5C_6 \ \cdots$

$P'=P_1P_2P'_3P'_4P'_5P'_6P'_7 \ \cdots$

Case3:

$C'=C_1C_2C_4C_5C_6 \ \cdots$

$P'=P_1P_2P'_3P'_4P'_5 \cdots$

Q:

$C'=C_1C'_2C'_3C'_4C_5C_6C_7C_8 \ \cdots$

$P'= P_1P'_2P'_3P'_4P_5P_6P_7P_8 \ \cdots$

- ECB 和 CBC 的结果类型是分组密码，而 CFB，OFB 和 CTR 的结果类型是流密码

思考题

7.1

> 什么是三重加密?

对明文分组进行三次加密，上一次加密的输出结果，作为下一次加密的输入。典型的情况是，第二阶段使用解密算法而不是加密算法。

7.2

> 什么是中间相遇攻击?

这是针对双重加密算法的攻击，需要已知的明密对。明文在双重加密中被加密以产生中间值并存入哈希表，而密文在双重加密中被解密以产生中间值，再查表判断表中是否有相同值。

7.3

> 在三重加密中用到多少个密钥?

两个或三个。

7.4

> 为什么 3DES 的中间部分采用了解密而不是加密?

为了代码复用，上一节中提及。

7.5

> 为什么某些分组密码的**操作模式**仅使用加密算法而其他的模式既使用加密算法又使用解密算法?

在某些模式下，明文不通过加密函数，而是与加密函数的输出进行异或运算。数学计算得出，对于这些情况下的解密，必须仍使用加密函数。如：CFB、OFB、CTR。

习题

7.4

> 在 DES 的 ECB 模式中，若在密文的传输过程中，某一块发生了错误，则只有相应的明文分组会有影响。然而，在 CBC 模式中，这种错误具有扩散性。比如，图 7.4 中传输 C_1 时发生的错误将会影响明文分组 P_1 和 P_2。
>
> (a) P_2 以后的所有块是否会受到影响?
>
> (b) 假设 P_1 本来就有一位发生了错误。则这个错误要扩散至多少个密文分组？对接收者解密后的结果有什么影响?

(a) 无影响。

(b) P_1 中的错误影响 C_1。但由于 C_1 被输入到 C_2 的计算中，C_2 受到影响，以此类推，所有的密文块都会受到影响。由于不是传输过程中的错误，接收端解密的结果也是 P_1 中有一位发生了错误。

7.8

> 在 8 位的 CFB 模式中，若传输中一个密文字符发生了一位错，这个错误将传播多远?

九个明文字符受影响。上面 CFB 中有解释。