《现代密码学》第四讲

分组密码（四）

上讲内容回顾

- AES算法的整体结构
- AES算法的轮函数
- AES算法的密钥编排算法
- AES的解密变换

分组密码的运行模式

分组密码在加密时,明文分组的长度是固定的，而实际应用中待加密消息的数据量是不定的，数据格式多种多样.

1）为了能在各种应用场合使用DES，美国在FIPS PUS 74和81中定义了DES的4种运行模式: ECB, CBC, CFB, OFB

2）FIPS PUB 140-2 推荐了AES的另外一种运行模式：CTR

本节主要内容

- 分组密码算法的运行模式
  - ECB
  - CBC
  - CFB
  - CTR

分组密码的运行模式

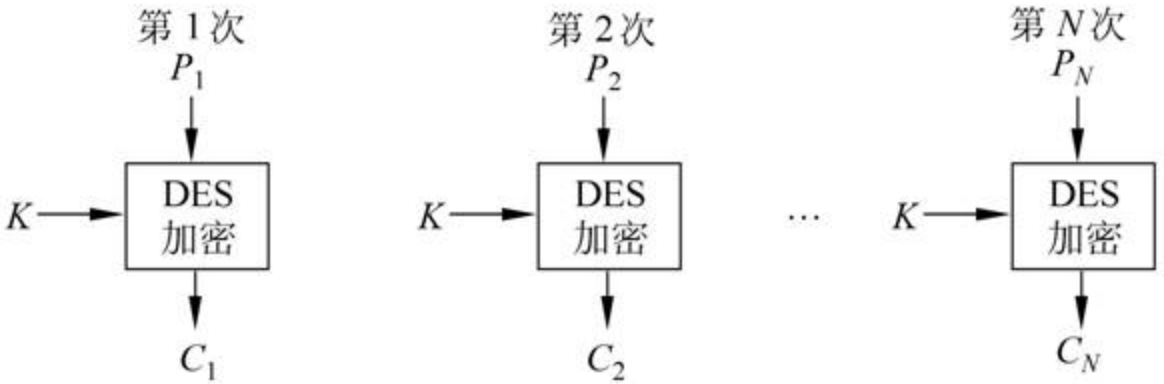
- 1 ECB (electronic codebook) 模式

最简单的运行模式，首先将明文分为64比特（调用的分组密码算法的分组长度）的明文块，它一次对一个64比特长的明文分组加密，每次的加密密钥都相同.

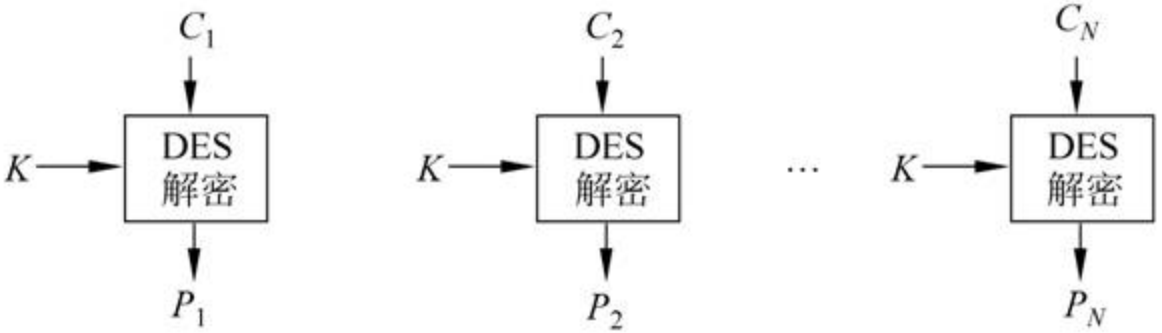
加密：$C_i = E(P_i, K)$.

解密：$P_i = D(C_i, K)$.

分组密码的运行模式



(a) 加密



(b) 解密

分组密码的运行模式

- 如果明文长于64比特，首先将其分为长为64比特的分组；若最后一个分组如果不够64比特，则需要填充；
- 明文加密过程和解密过程分别调用加密算法和解密算法.
- 无额外的初始向量.

分组密码的运行模式

- 密文块可以分别独立解密，无顺序要求.

- 不存在错误传播，一块密文传送错误只导致对应明文解密错误；

- 密钥相同时，明文中相同的64比特分组产生相同的64比特密文块；主要用于发送少数量的分组数据.

分组密码的运行模式

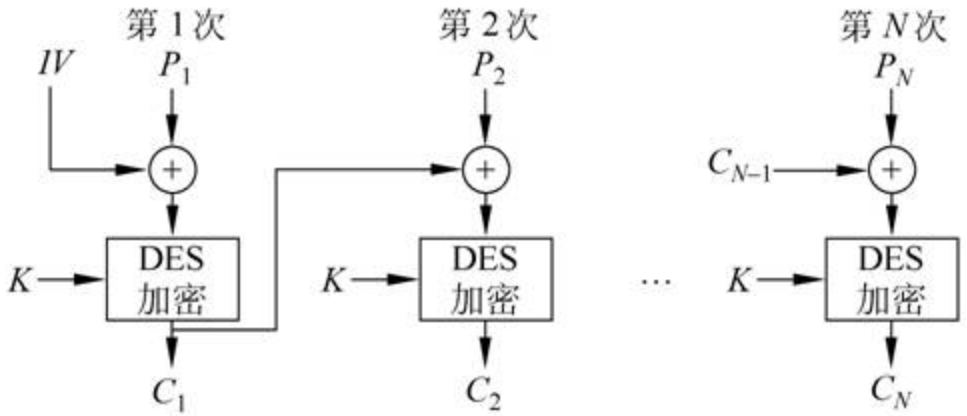
2 CBC（cipher block chaining）模式

首先对明文分组，它一次对一个明文分组加密，加密算法的输入是当前明文分组和前一次密文分组的异或.

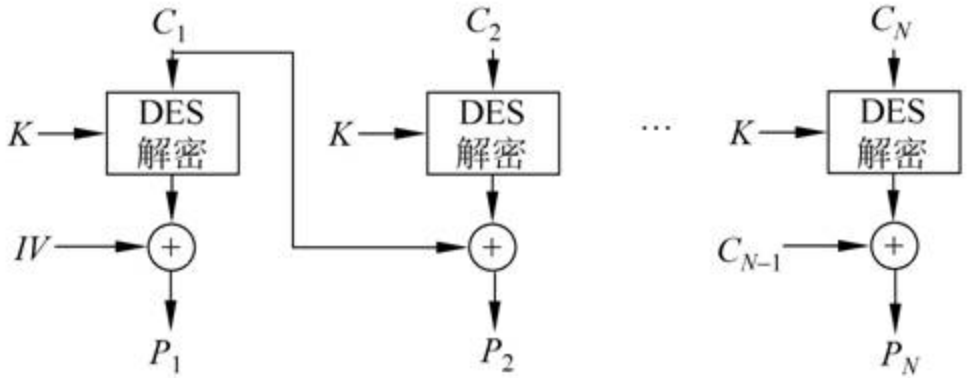
加密：$C_i = E(P_i \oplus C_{i-1}, K)$.

解密：$P_i = D(C_i, K) \oplus C_{i-1}$.

分组密码的运行模式



(a) 加密



(b) 解密

分组密码的运行模式

注：IV对于收发双方都应是已知的（和密文一起在信道上传送），如果敌手能欺骗接收方使用不同的IV值，则接收方收到的P1中相应的比特也发生了变化.

$$C_1 = E_K[IV \oplus P_1]$$

$$P_1 = IV \oplus D_K[C_1] \qquad P_1' = IV' \oplus D_K[C_1]$$

为使安全性最高，IV应像密钥一样被保护（可使用ECB加密模式来发送IV).

分组密码的运行模式

- 如果消息长于64比特，首先将其分组，最后一个分组如果不够64比特，则需要填充.
- 明文加密过程和解密过程分别调用加密算法和解密算法.
- 有额外的随机初始向量，与密文一同传送；
- 密文块需按顺序逐一解密.
- 存在错误传播，一块密文传输错误会导致下一块密文解密失败
- 密钥相同时，明文中相同的64比特分组产生不相同的64比特密文块；适合加密长度大于64比特的消息

分组密码的运行模式

- 3 CFB（cipher feedback）模式

设传送的每个单元（如一个字符）是j比特，0<j<64长，通常取j=8.

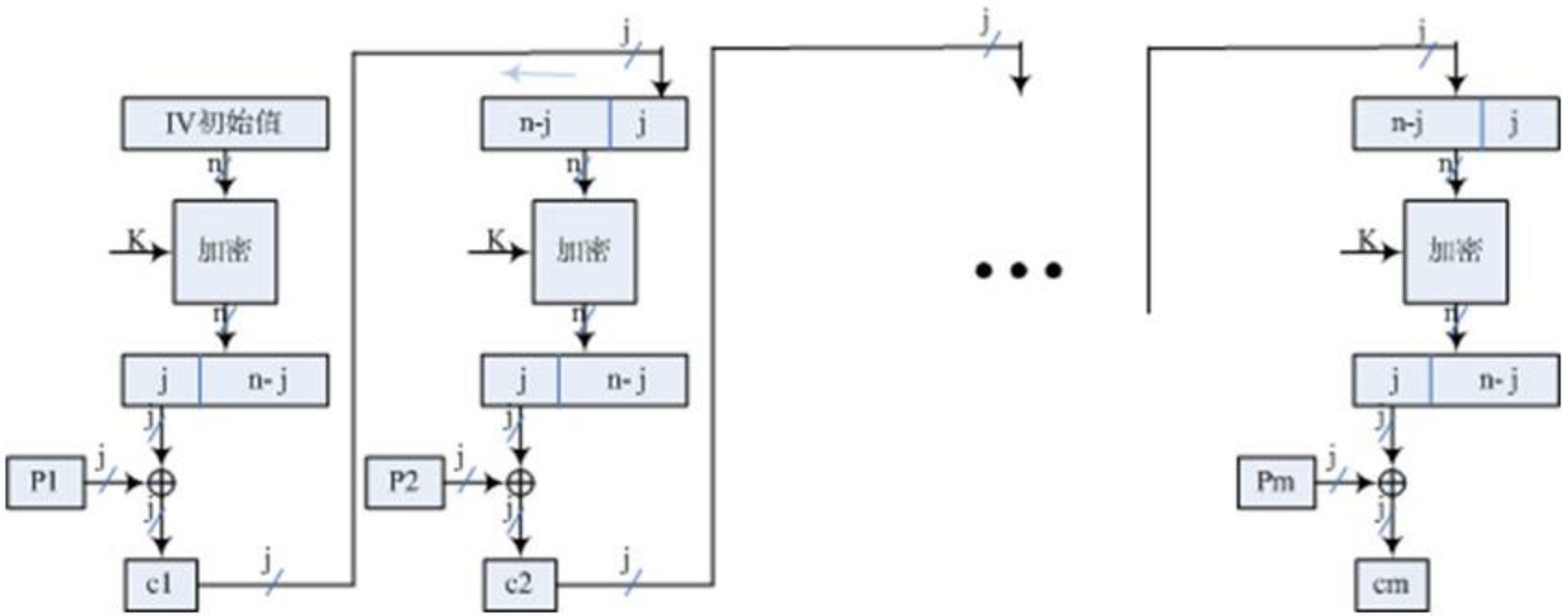
加密时，设加密算法的输入是64比特移位寄存器，其初值为某个初始向量IV. 加密算法输出的最左（最高有效位）j比特与明文的第一个单元P_1进行异或，产生出密文的第1个单元C_1. 传送该单元并将输入寄存器的内容左移j位，用C_1补齐最右边（最低有效位）j位.

解密时，将加密算法输出的最左（最高有效位）j比特与密文的相应单元异或，产生明文. 反馈输入到输入寄存器的值为密文单元.

分组密码的运行模式

- CFB加密模式

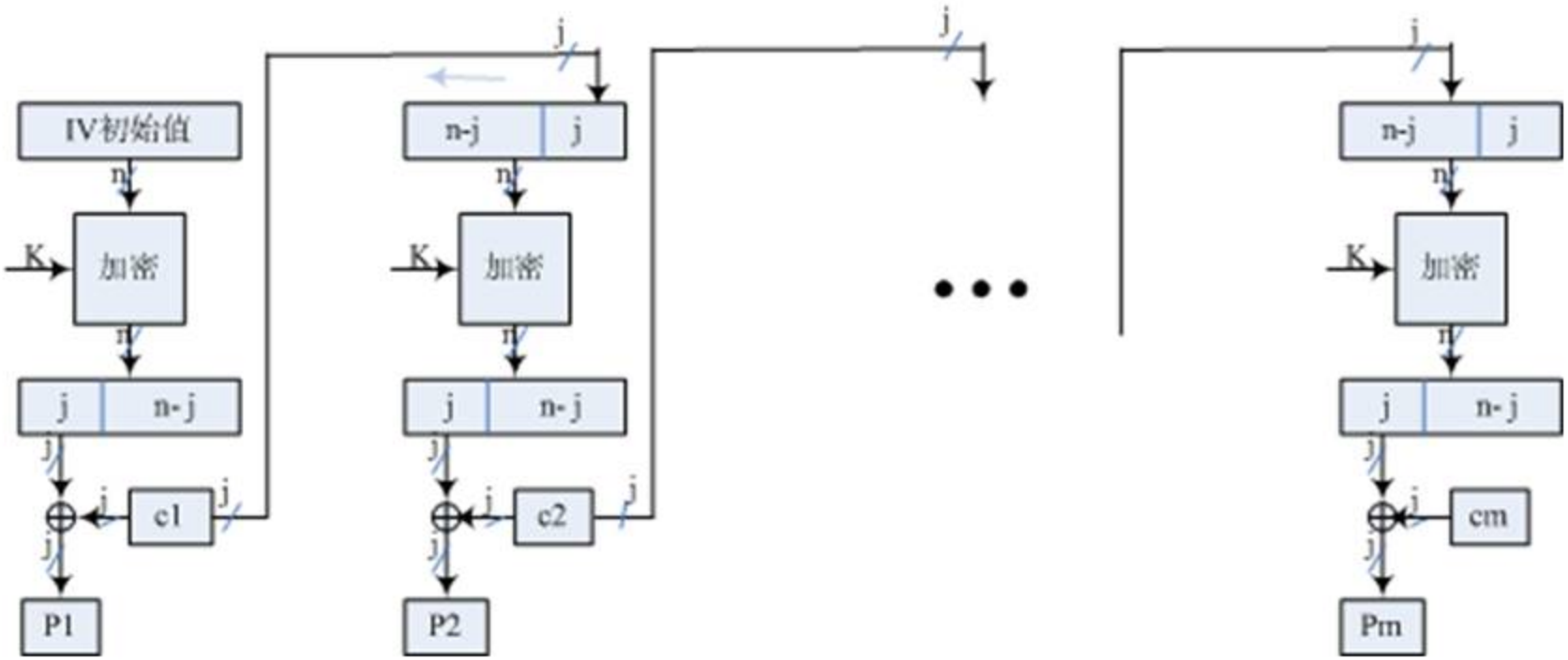
加密：$C_i = E(C_{i-1}, C_{i-2}, \cdots, C_{i-n/j}; K) \oplus P_i$.



分组密码的运行模式

- CFB解密模式

解密： $P_i = E(C_{i-1}, C_{i-2}, \cdots, C_{i-n/j}; K) \oplus C_i$.



分组密码的运行模式

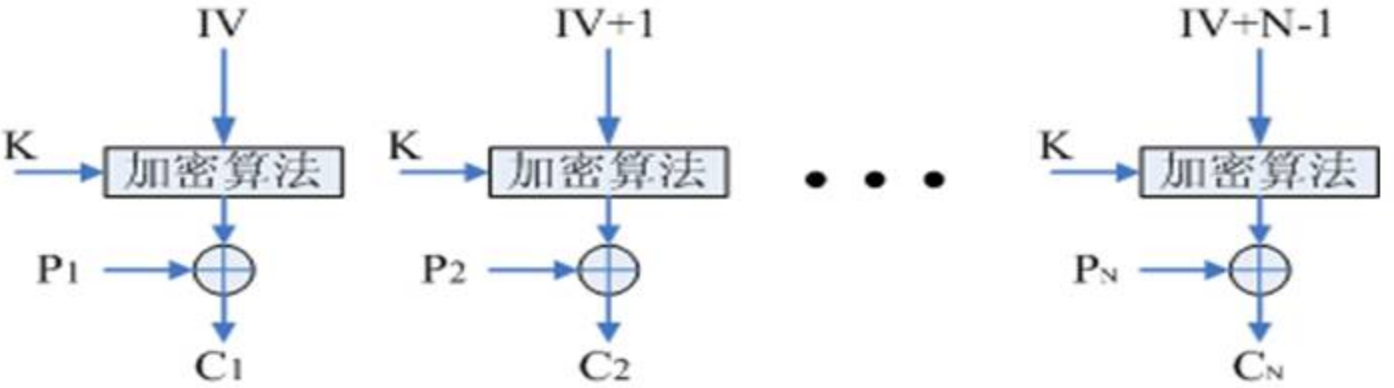
- 消息被看作bit流，无须分组填充；适合数据以比特或字节为单位出现标准允许反馈任意比特(1,8 or 64 or whatever)记作 CFB-1, CFB-8, CFB-64
- 只使用DES加密算法，且所有加密都使用同一密钥.
- 有额外的初始向量，若初始向量公开，攻击者可以通过篡改，使前几块（与错误比特几次移出寄存器有关）明文解密错误.

分组密码的运行模式

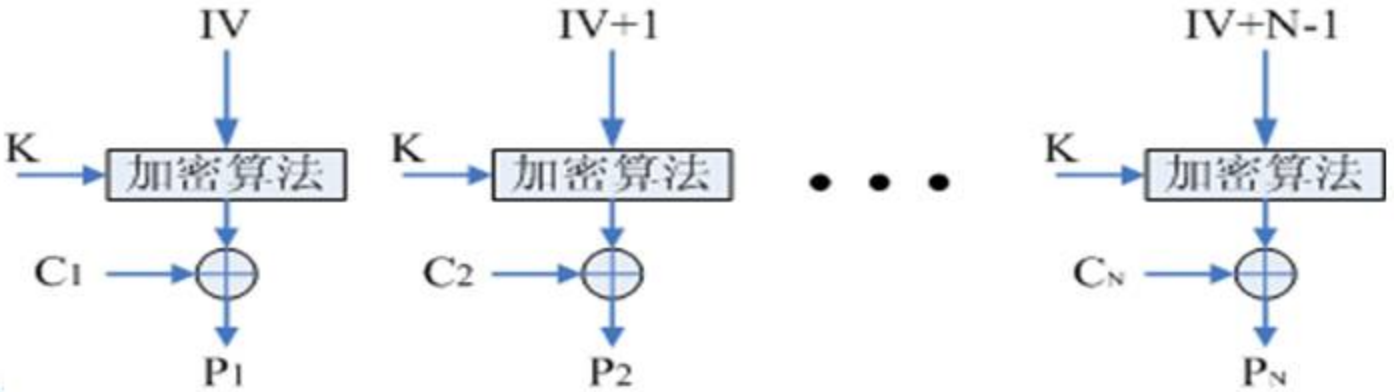
- 密文块需按顺序逐一解密.
- 密钥相同时，明文中相同的64比特分组产生不相同的64比特密文块.
- 存在错误传播（只传播后面的几块）.

分组密码的运行模式

4. 计数器模式 Counter(CTR)



加密过程



解密过程

分组密码的运行模式

- 消息被看作比特流，无须分组填充.
- 只使用加密算法，且所有加密都使用同一密钥.
- 密钥流可以在已知消息之前计算，不需要按顺序解密. 并行计算。
- 有额外的随机初始向量，密钥相同时，明文中相同的64比特分组产生不相同的64比特密文块.
- 不存在比特错误传播.

主要知识点小结

分组密码的运行模式

- **Block Modes**
  - **ECB, CBC**
- **Stream Modes**
  - **CFB, OFB, CTR**

THE END!