北京郵電大學
BEIJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

《现代密码学》第四讲

分组密码（四）

信息安全中心
BUPT ISC

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算法的解密变换

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

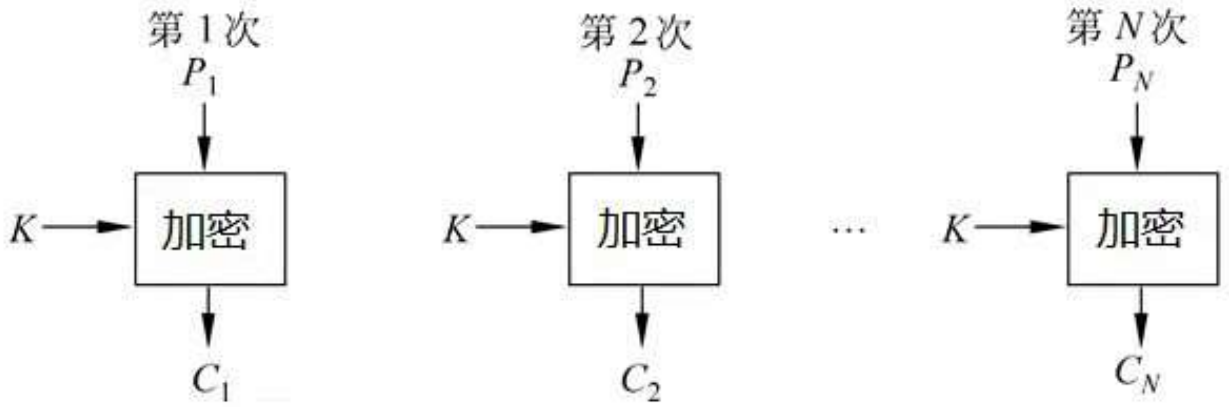
分组密码的运行模式

1. ECB（electronic codebook）模式

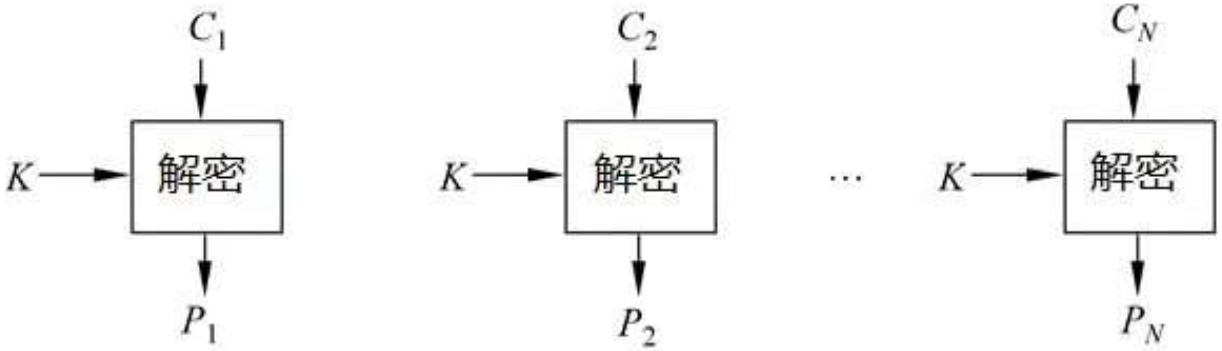
加密：$C_i = E(P_i, K)$.

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

- 将长消息分块，若最后一个分块不足分组长度，则需要填充；
- 加密过程和解密过程分别调用加密算法和解密算法；
- 存在密文扩展(明文填充带来的扩展)；
- 密文块分别独立解密，无顺序要求；
- 不存在错误传播；
- 适合一个分组长度的短数据加密.

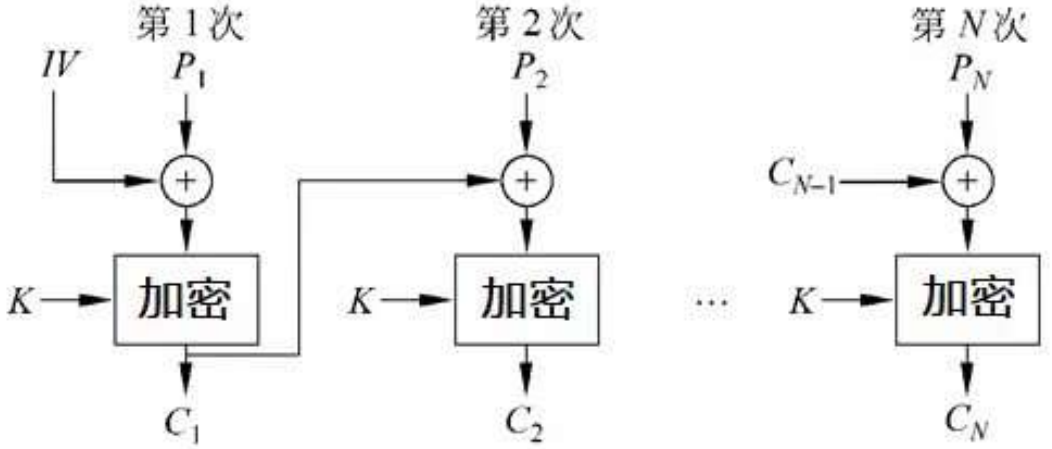
分组密码的运行模式

2. CBC（cipher block chaining）模式

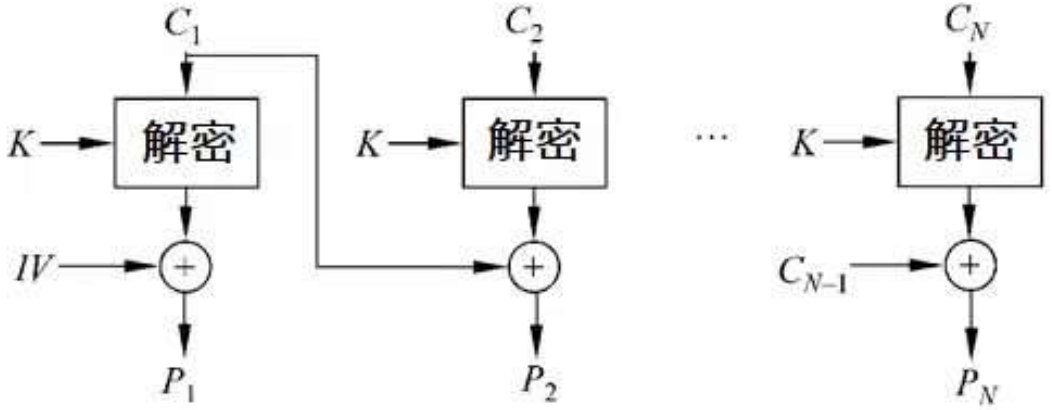
加密：$C_i = E(P_i \oplus C_{i-1}, K)$.

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.

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

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

对于收发双方都已知的IV，可以不在信道上传送.

分组密码的运行模式

- 将长消息分块，若最后一个分块不足分组长度，则需要填充；
- 加密和解密过程分别调用加密算法和解密算法；
- 存在密文扩展(明文填充带来的扩展和IV传输的扩展)；
- 密文块需按顺序逐一解密；
- 存在错误传播(只传播下一块密文)；
- 适合大于一个分组长度的长数据加密.

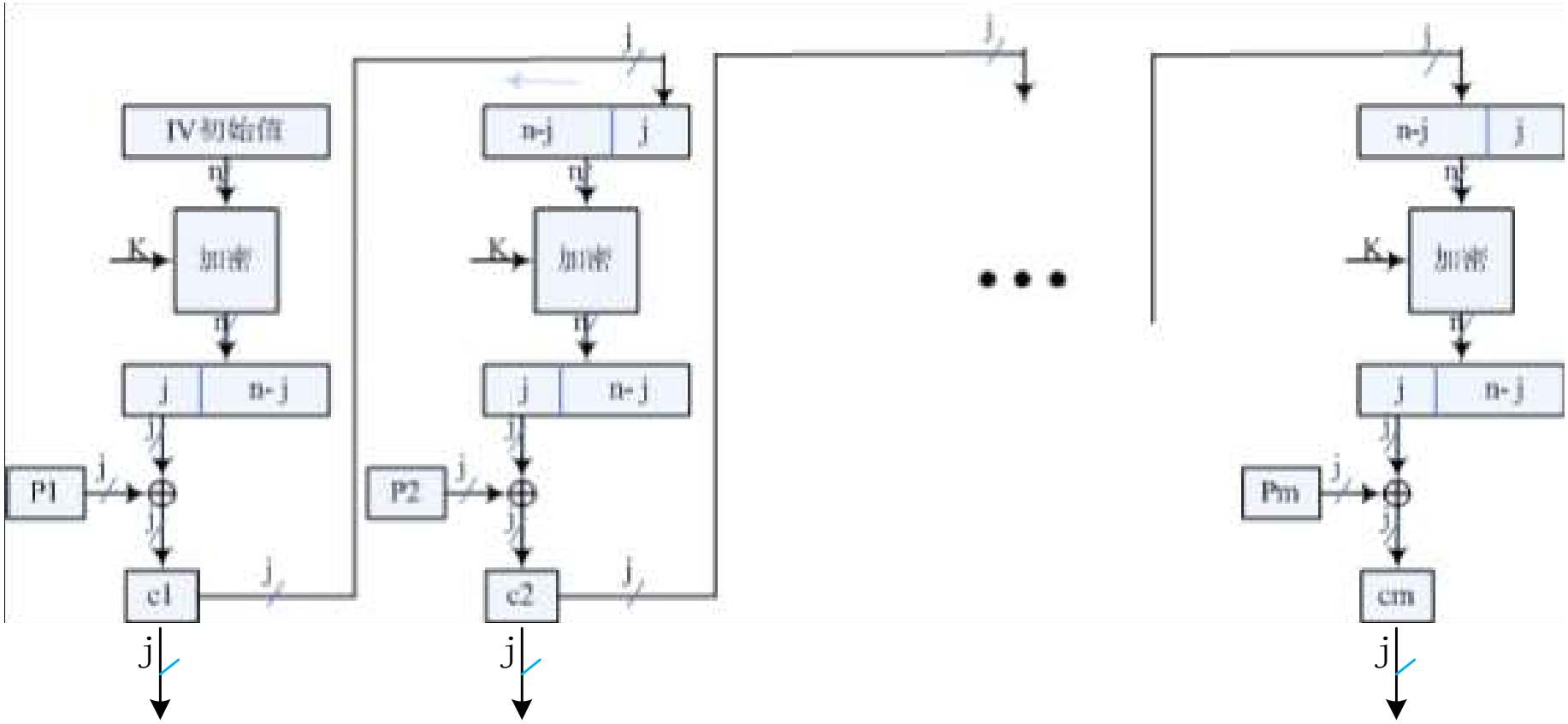
分组密码的运行模式

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.

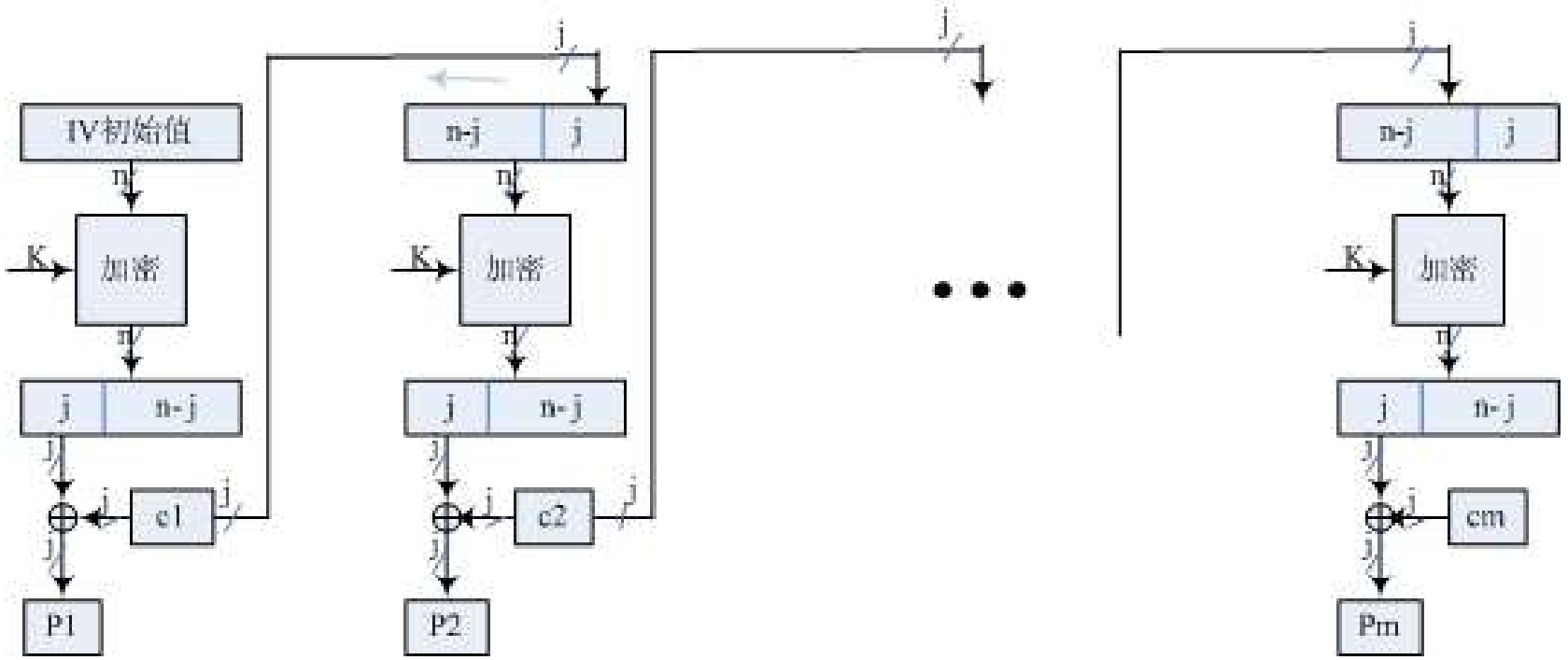
分组密码的运行模式

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

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

- 消息作为比特流进行加密，无须分组填充；

标准允许反馈任意比特（1,8 or 64 or whatever，前几种分别记作 CFB-1，CFB-8，CFB-64）；

- 加密和解密过程只调用加密算法；
- 存在密文扩展(IV传输的扩展)；
- 密文块需按顺序逐一解密；
- 存在错误传播（只传播后面的几块）；
- 适合大于一个分组长度的长数据加密.

分组密码的运行模式

- 练习
- 设分组长度为64，j=8，若C1存在传输错误，会导致哪几块明文不能正确解密？

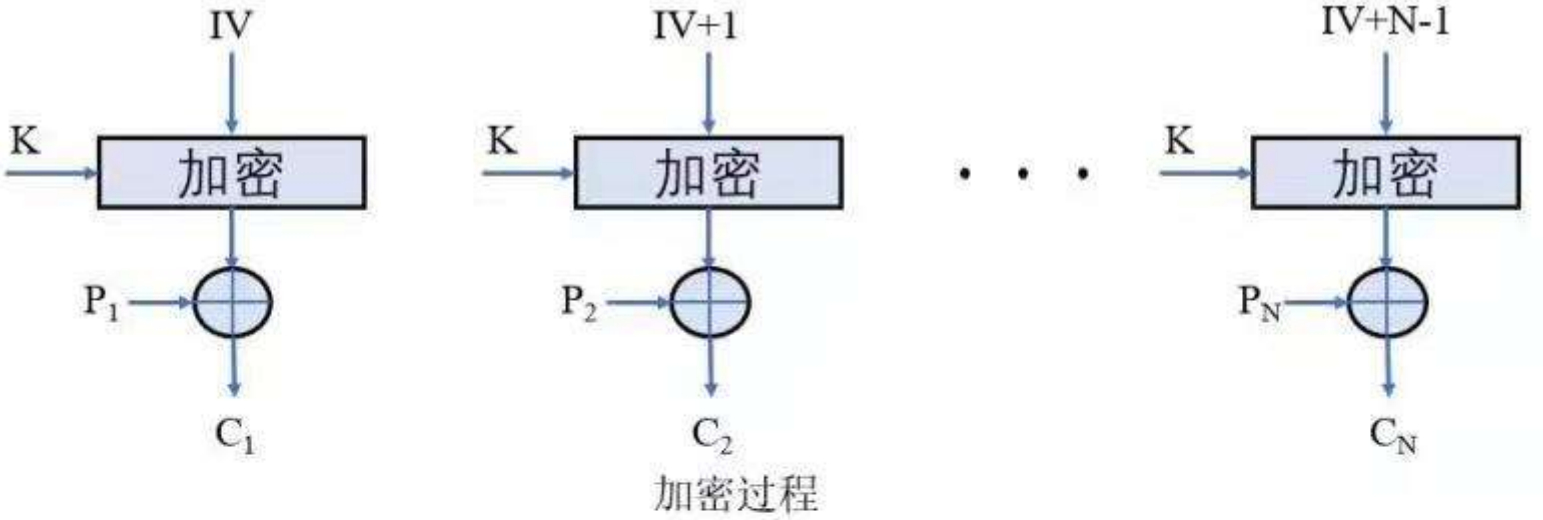
分组密码的运行模式

4. 计数器模式 Counter (CTR)

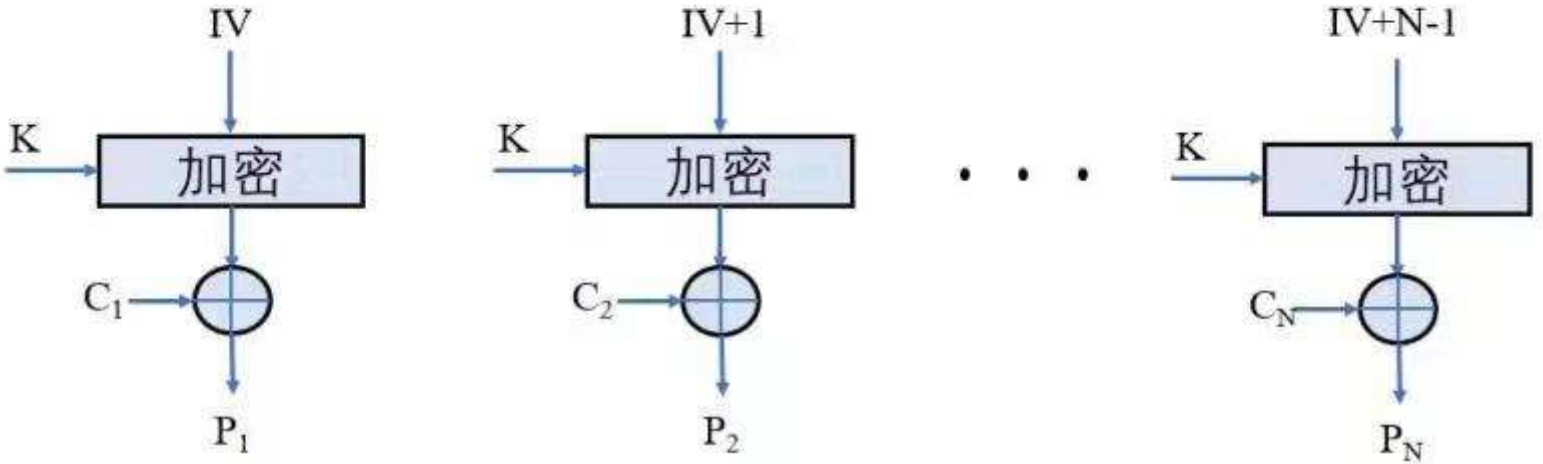
加密：$C_i = E(IV+i-1, K) \oplus P_i$.

解密：$P_i = E(IV+i-1, K) \oplus C_i$.

分组密码的运行模式



加密过程



解密过程

分组密码的运行模式

- 消息作为比特流进行加密，无须分组填充；
- 加密和解密过程只调用加密算法；
- 存在密文扩展(IV传输的扩展)；
- 密文块分别独立解密，无顺序要求(并行计算)；
- 不存在错误传播；
- 适合大于一个分组长度的长数据加密.

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 !