

现代密码学

第二十四讲 分组密码的工作模式1

信息与软件工程学院

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the title.

为什么需要工作模式？

- 分组密码的工作模式是：根据不同的数据格式和安全性要求，以一个具体的分组密码算法为基础构造一个分组密码系统的方法
 - 分组密码的工作模式应当力求简单，有效和易于实现
 - 需要采用适当的工作模式来隐蔽明文的统计特性、数据的格式等
 - 降低删除、重放、插入和伪造成功的机会
-

A decorative blue horizontal bar with a series of parallel lines is positioned to the left of the title.

分组密码的主要工作模式

1. 电码本 (ECB) 模式
 2. 密码分组链接 (CBC) 模式
 3. 密码反馈 (CFB) 模式
 4. 输出反馈 (OFB) 模式
 5. 计数器模式
-

A decorative vertical bar with horizontal blue stripes is positioned on the left side of the slide.

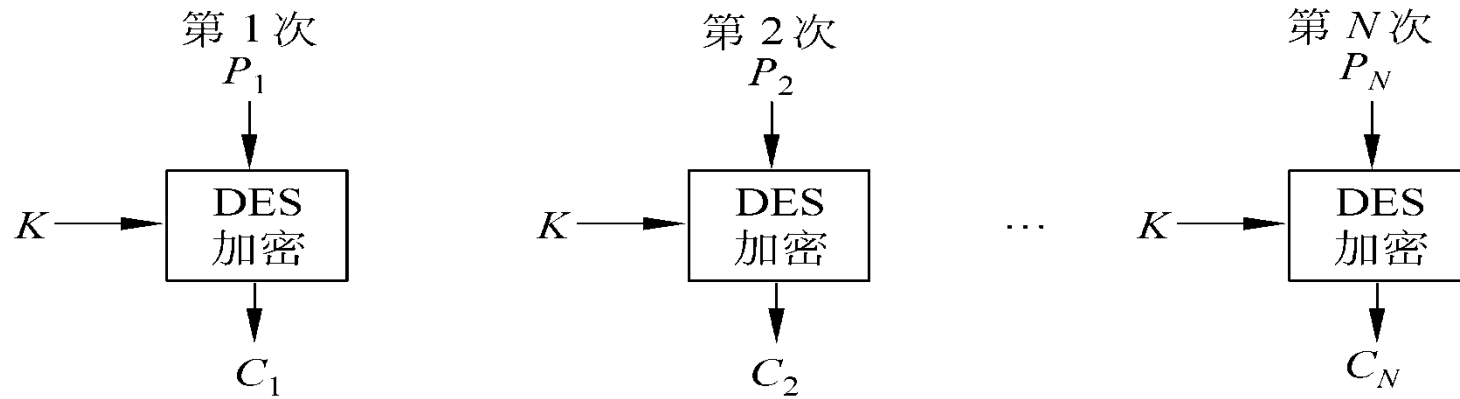
第二十四讲 分组密码的工作模式1

A diagram on the left side of the slide shows a vertical line with two circles. The top circle is connected to a blue horizontal bar containing the text '电码本(ECB)模式'. The bottom circle is connected to another blue horizontal bar containing the text '密码分组链接(CBC)模式'.

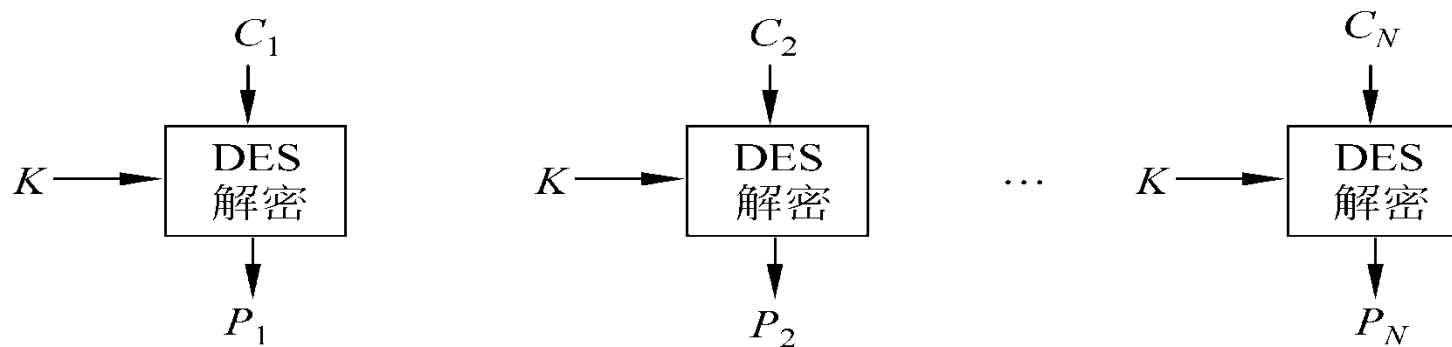
电码本(ECB)模式

密码分组链接(CBC)模式

电码本ECB (Electronic Code Book) 模式



(a) 加密



(b) 解密

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the title.

ECB模式的优、缺点

- 优点：
 - (1) 实现简单;
 - (2) 不同明文分组的加密可并行实施, 尤其是硬件实现时速度很快
 - 缺点:
 - (1) 相同明文分组对应相同密文分组
 - (2) 不能隐蔽明文分组的统计规律和结构规律, 不能抵抗替换攻击
 - 应用:
 - (1) 用于随机数的加密保护
 - (2) 用于单分组明文的加密
-

电码本模式缺陷的例子

- 例：假设银行A和银行B之间的资金转帐系统所使用报文模式如下：

1	2	3	4	5	6	7	8	9	10	11	12	13
时间 标记	发送 银行		接收 银行	储户姓名 1						储户帐号 1		存款 金额

1	2	3	4	5	6	7	8	9	10	11	12	13
时间 标记	发送 银行		接收 银行	储户姓名 2						储户帐号 2		存款 金额

- 敌手C通过截收从A到B的加密消息，只要将第5至第12分组替换为自己的姓名和帐号相对应的密文，即可将别人的存款存入自己的帐号。



第二十四讲 分组密码的工作模式1

A diagram showing two encryption modes. On the left, a vertical line has two white circles. Each circle is connected to a horizontal blue bar on the right. The top bar contains the text '电码本(ECB)模式' and the bottom bar contains '密码分组链接(CBC)模式'.

电码本(ECB)模式

密码分组链接(CBC)模式

密码分组链接CBC (Cipher Block Chaining) 模式

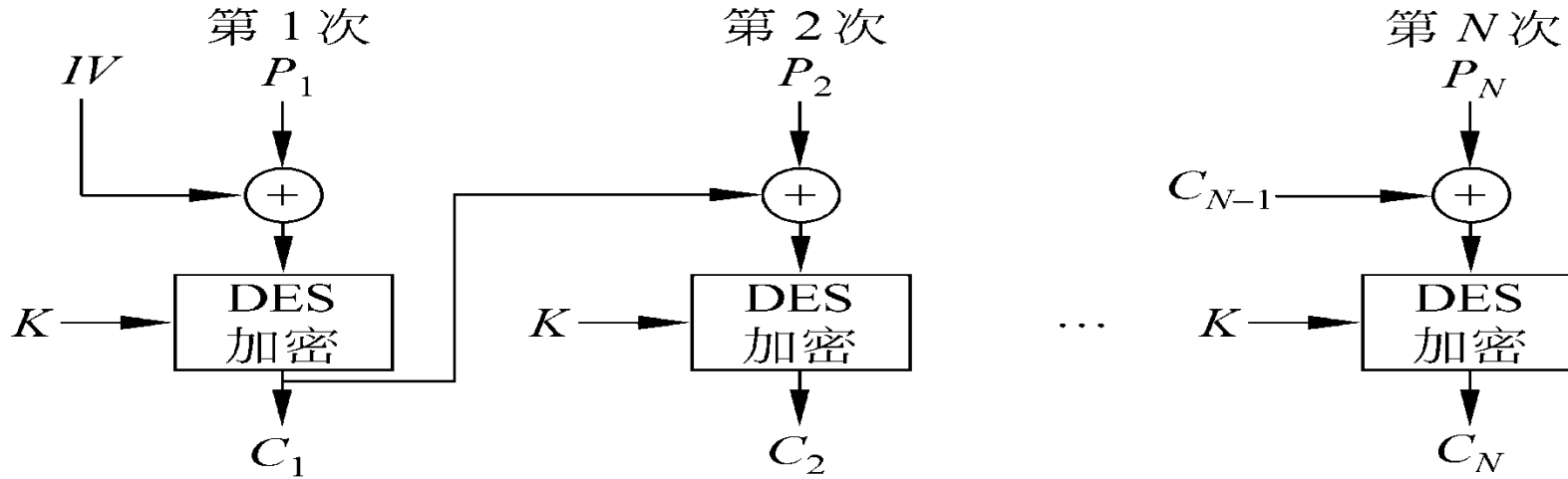
- 这种模式先将明文分组与上一次的密文块进行按比特异或，然后再进行加密处理。这种模式必须选择一个初始向量 $c_0=IV$ ，用于加密第一块明文。
- 加密过程为

$$c_i = E_k(m_i \oplus c_{i-1})$$

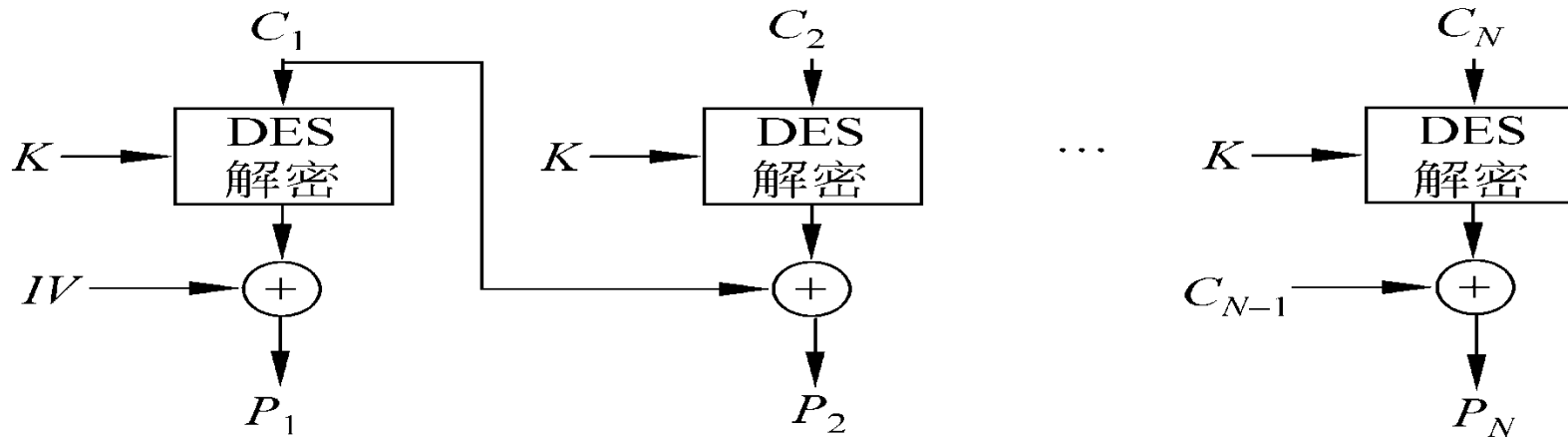
- 解密过程为

$$m_i = D_k(c_i) \oplus c_{i-1}$$

密码分组链接CBC (Cipher Block Chaining) 模式



(a) 加密



(b) 解密

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the title.

CBC模式的特点

1. 明文块的统计特性得到了隐蔽

- 由于在CBC模式中，各密文块不仅与当前明文块有关，而且还与以前的明文块及初始化向量有关，从而使明文的统计规律在密文中得到了较好的隐藏

2. 具有有限的(两步)错误传播特性

- 一个密文块的错误将导致两个密文块不能正确解密

3. 具有自同步功能

- 密文出现丢块和错块不影响后续密文块的解密. 若从第 t 块起密文块正确，则第 $t+1$ 个明文块就能正确求出
-

利用CBC模式实现报文的完整性认证

- 目的:检查文件在(直接或加密)传输和存储中是否遭到有意或无意的篡改.
- 关键技术:
 - (1) 文件的制造者和检验者共享一个密钥
 - (2) 文件的明文必须具有检验者预先知道的冗余度
 - (3) 文件的制造者用共享密钥对具有约定冗余度的明文用**CBC**模式加密
 - (4) 文件的检验者用共享密钥对密文解密, 并检验约定冗余度是否正确

A decorative blue horizontal bar with white horizontal stripes is positioned to the left of the title.

报文完整性认证的具体实现技术

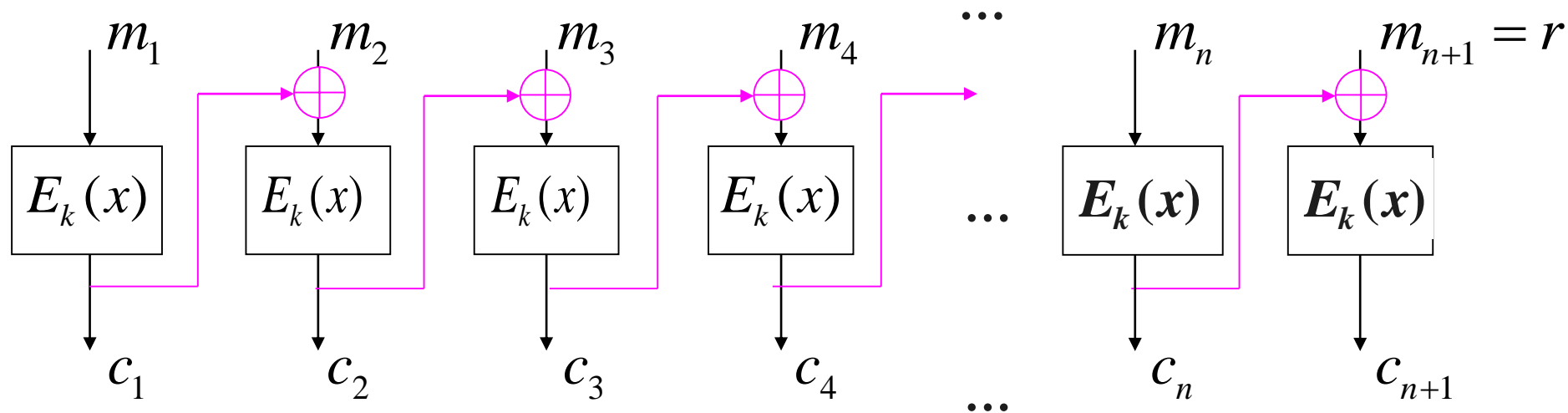
- (1) 文件的制造者和检验者共享一个密钥;
- (2) 利用文件的明文 m 产生一个奇偶校验码 r 的分组;
- (3) 采用分组密码的**CBC**模式, 对附带校验码的已扩充的明文 (m, r) 进行加密, 得到的最后一个密文分组就是认证码

认证码生成

n 个分组明文 $m = (m_1, \dots, m_n)$, 校验码为

$$r = m_{n+1} = m_1 \oplus \dots \oplus m_n$$

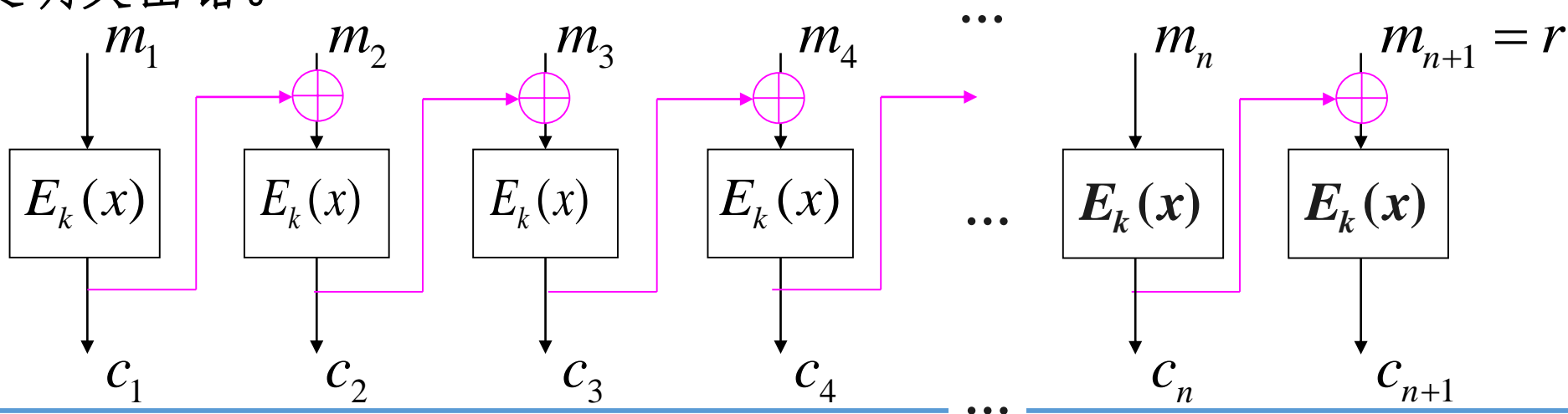
C_{n+1} 为认证码。



- (1) 仅需对明文认证,而不需加密时,传送明文 m 和认证码 C_{n+1} , 此时也可仅保留 C_{n+1} 的 t 个比特作为认证码;
- (2) 既需对明文认证,又需要加密时,传送密文 C 和认证码 C_{n+1}

认证码检验

- (1) 仅需对明文认证而不需加密时,此时验证者仅收到明文 \mathbf{m} 和认证码 C_{n+1} , 他需要:
- **Step1** 产生明文 \mathbf{m} 的校验码 $r = m_{n+1} = m_1 \oplus \dots \oplus m_n$
- **Step2** 利用共享密钥使用CBC模式对 (\mathbf{m}, r) 加密, 将得到的最后一个密文分组与接收到的认证码 C_{n+1} 比较, 二者一致时判定接收的明文无错; 二者不一致时判定明文出错。





感谢聆听!

xynie@uestc.edu.cn
