第 2 章：分组密码体制

2.7 分组密码的工作模式

赵俊舟

junzhou.zhao@xjtu.edu.cn

2025 年 3 月 12 日

分组密码的工作模式

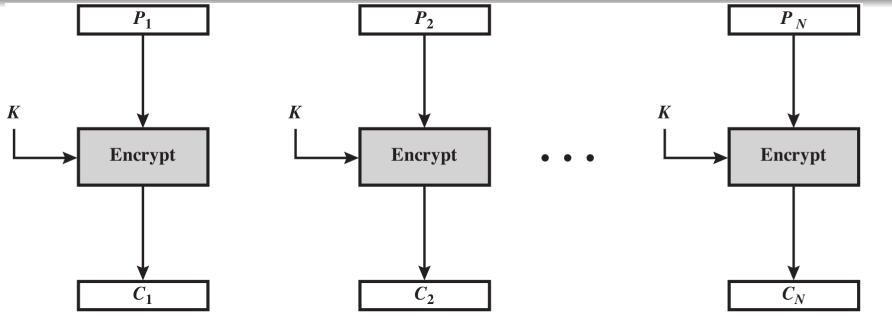
- 分组密码输入 b 位明文分组，输出 b 位密文分组。
- 若明文长度大于 b，则需要将明文分成 b 位一组的块。
- 每次使用相同的密钥对多个分组加密，会引发安全问题。
- 为了将分组密码应用于各种各样的应用，NIST 定义了五种工作模式。
- 本质上，工作模式是一项增强密码算法或者使算法适应具体应用的技术。
- 五种工作模式可使用包括 DES 和 AES 在内的任何分组密码。

目录

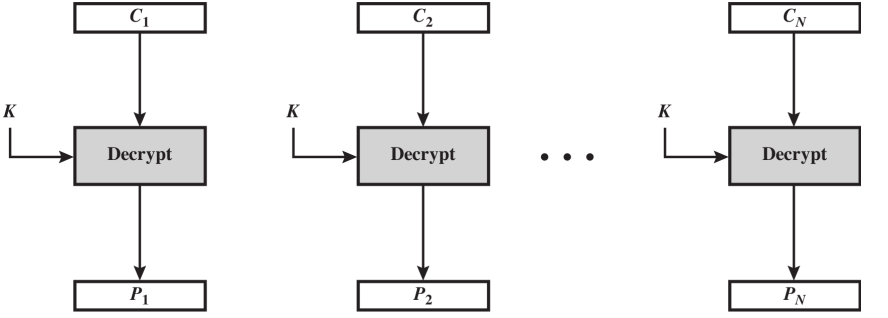
目录

电码本（Electronic Codebook, ECB）

加密：



解密：



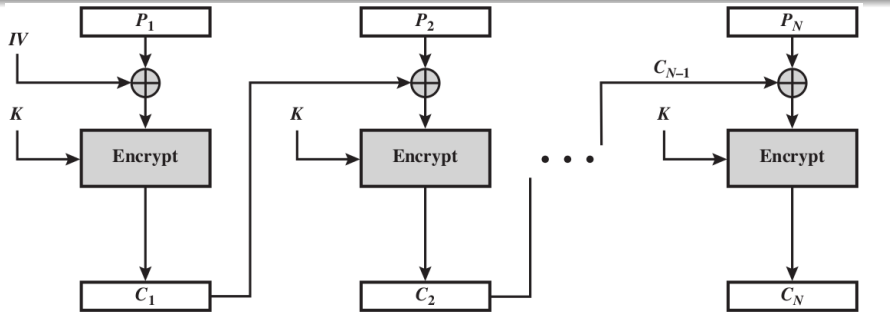
ECB 的局限性

- 给定密钥，任何 b 位明文分组有唯一密文分组，类似于在一个很厚的密码本里查明文的相应密文，所以叫电码本模式。
- ECB 模式特别适合数据较少的情况，例如传输 DES 密钥。
- 一段明文消息中若有几个相同的明文分组，则密文也将出现几个相同的片段。
- 对于很长的消息，ECB 是不安全的，如果消息是非常结构化的，密码分析可能利用其结构特征来破解。
- ECB 的弱点来源于其加密过的密文分组互相独立。

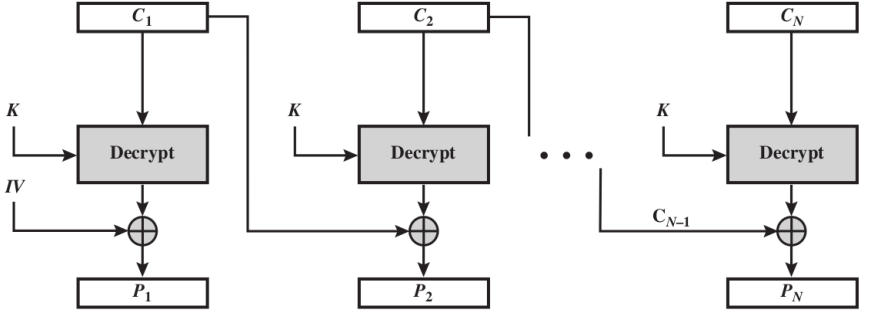
目录

密文分组链接（Cipher Block Chaining, CBC）

加密：



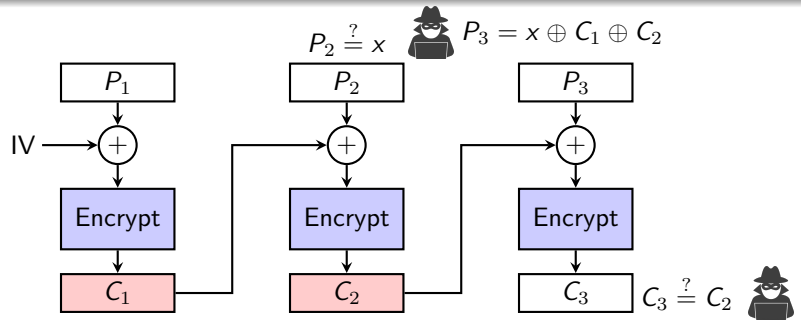
解密：



CBC 的优缺点

- 加密算法的输入是当前明文分组与上一个密文分组的异或。
- 每个密文分组依赖于所有之前的明文分组。
- 明文消息中的任何一点变化都会影响之后所有的密文分组。
- 发送方和接收方需要共享初始向量（Initial Value, IV）。
  - 如果 IV 被明文传送，则攻击者可以通过改变 IV 进而改变则接收者收到的 P_1。
  - 因此，IV 必须是定值或者必须用 ECB 方式在消息之前加密传送。
- 如果最后一个分组不是完整的分组，则需要填充：可以填充已知非数据值，或者在最后一块补上填充位长度。
  - eg., [b1 b2 b3 0 0 0 0 5], i.e., 3 data bytes, then 5 bytes pad+count.

CBC 的一个潜在漏洞



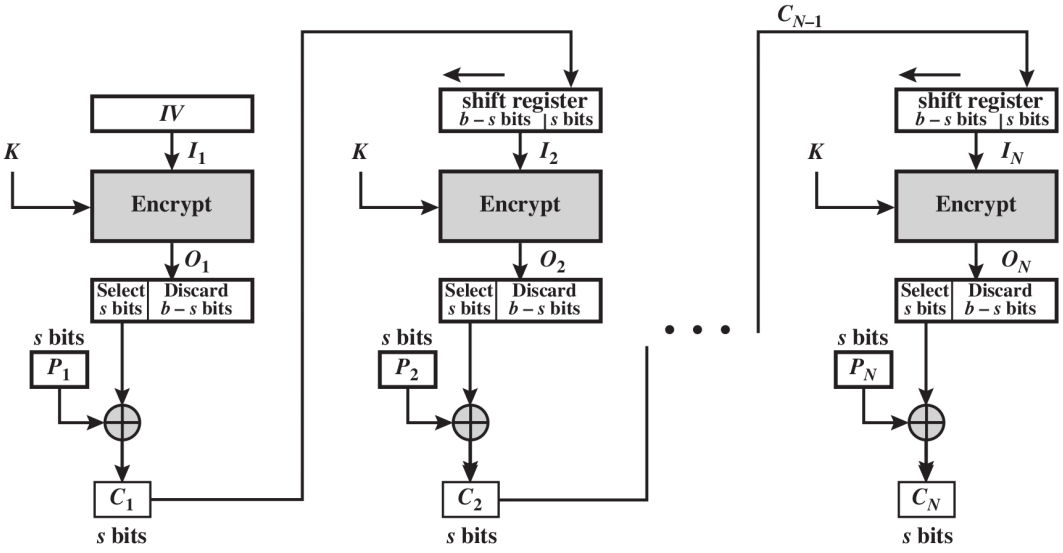
- 如果攻击者能观察连续两个密文分组 C_1 和 C_2，那么通过选择下一个明文分组 $P_3 = x \oplus C_1 \oplus C_2$，便可以判断第二个明文分组 P_2 是否等于 x。
- 因为

$$C_3 = E(C_2 \oplus P_3) = E(C_2 \oplus x \oplus C_1 \oplus C_2) = E(x \oplus C_1)$$

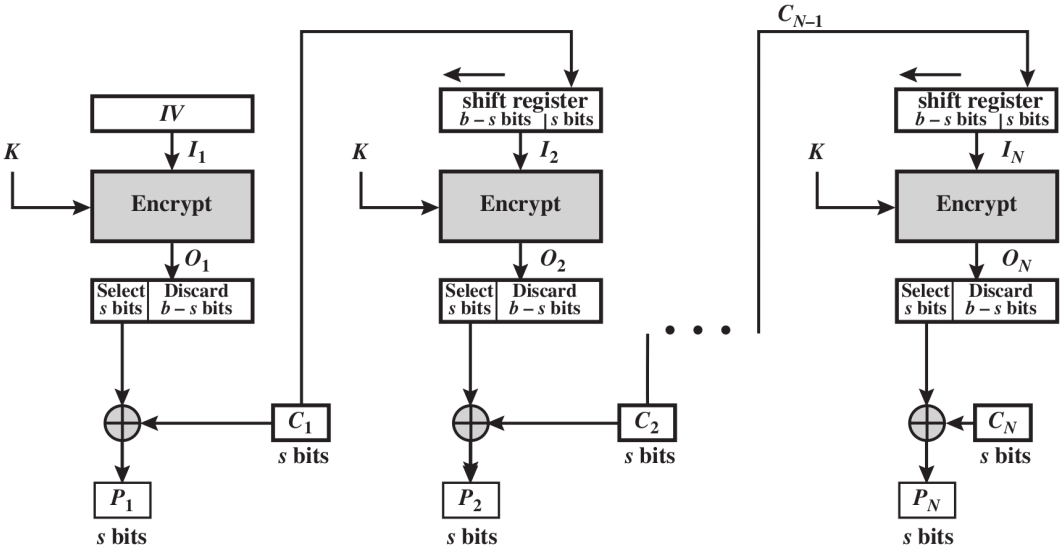
当 $P_2 = x$ 时，有 $C_3 = C_2$。

目录

密文反馈（Cipher Feedback, CFB）：加密



密文反馈（Cipher Feedback, CFB）：解密



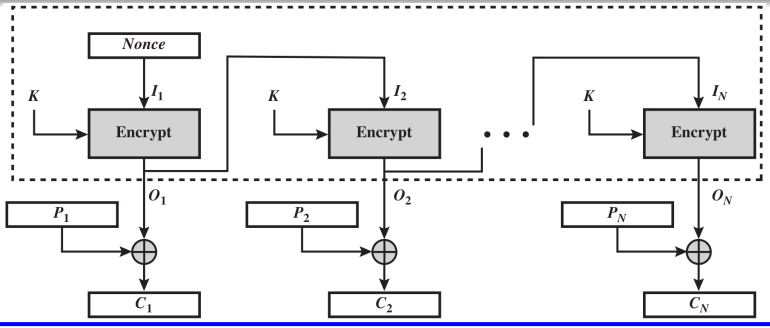
CFB 的优缺点

- 可以将分组密码转化成流密码的技术。
- 不再要求报文被填充成整个分组，数据以位或字节形式到达时都适用。
- 加解密使用相同方案，注意解密时仍使用加密函数。
- 密文在传输过程中发生错误时，会得到错误明文，错误会传播几个分组。

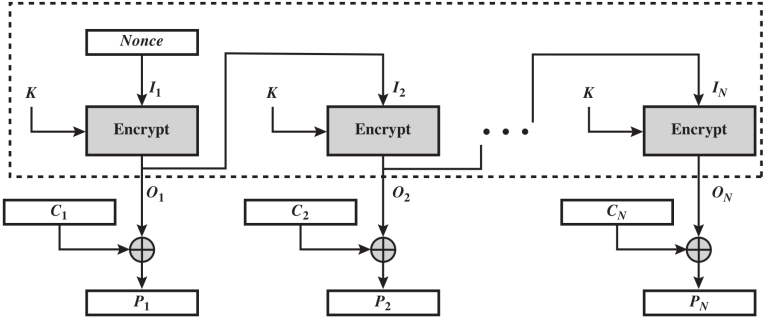
目录

输出反馈（Output Feedback, OFB）

加密：



解密：



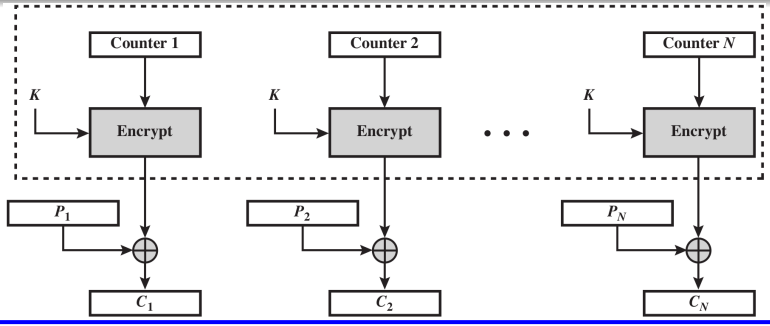
OFB 的优缺点

- 优点：密文传输过程中某位上发生的错误不会影响其他明文的恢复。
- 例如，C_1 中有一位发生了错误，只会影响 P_1 的恢复，不会影响后续明文的恢复。
- 缺点：抗消息流篡改能力不如 CFB，即如果密文某位取反，则恢复出来的明文相应位也取反。

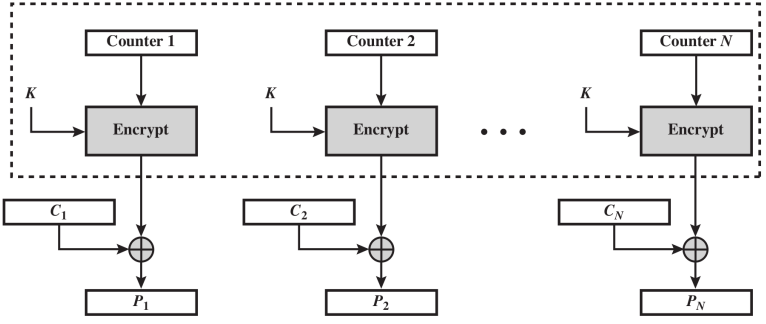
目录

计数器（Counter, CTR）

加密：



解密：



CTR 的优缺点

- 高效，可以做并行加密，可以用于高速网络加密中。
- 可以对被加密的分组进行随机存取。
- 相当安全。
- 简洁。
- 必须决不重复使用密钥和计数器值。

小结

1. 电码本
2. 密文分组链接
3. 密文反馈
4. 输出反馈
5. 计数器