第二次书面作业
参考答案

作业2-习题1

①

a．P2之外的分组不会受到影响，假如C1损坏了，P3 只依赖于输入分组 C2 和 C3．

b．假如明文分组 P1出现1比特殊差错，P1影响 C1．由于 C1 被作为输入来计算 C2，C2被影响了．这一影响一直被传播，因此所有的密文分组都会受到影响。但是，在接收端，解密算法能恢复出正确的明文，除了第一个分组。

作业2-习题2

② 解密后，最后一个分组的最后一个字节用于确定必须剥离的填充量。因此必须至少一个字节的填充。

作业2-习题3

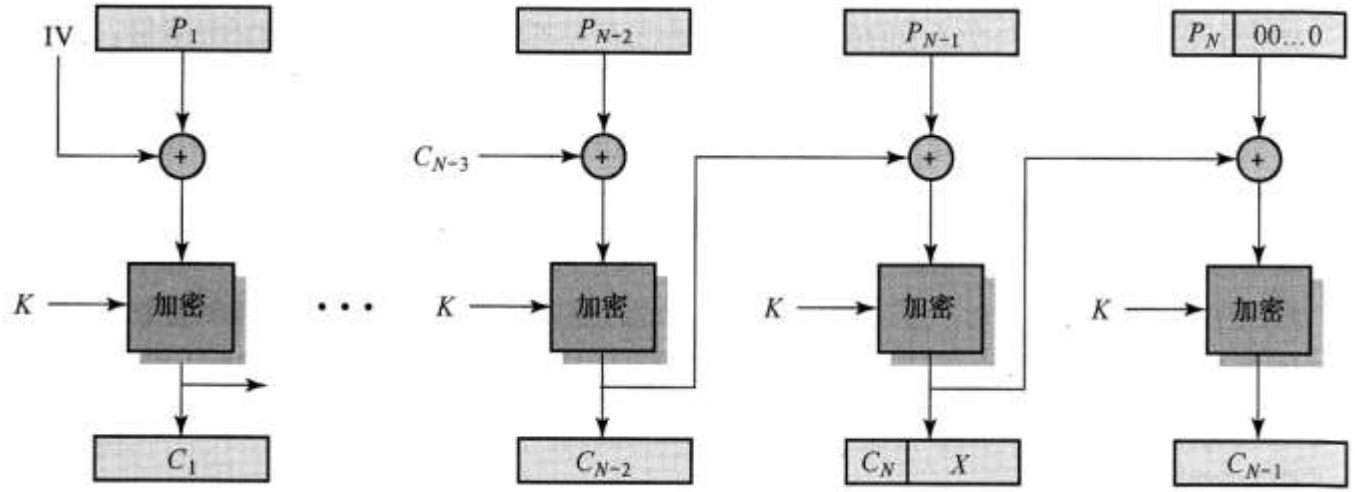
③ 假设明文的最后一块只有L字节长，其中L<2w/8。加密顺序如下：

1. 使用传统的CBC技术加密前（N–2）个分组
2. XOR P_{N-1} 与前一个密文分组C_{N-2} 产生 Y_{N-1}.
3. 加密 Y_{N-1} 产生E_{N-1}
4. 选择E_{N-1} 的前 L 字节产生 C_N
5. 对最后一个分组 P_N在尾端补0，与E_{N-1}XOR 产生Y_N
6. 加密Y_N 产生 C_{N-1}
7. 最后的两个密文分组是C_{N-1} 和 C_N.

作业2-习题3

- $P_N \,||\, X = (C_N \,||\, 00\ldots0) \oplus D(K, [C_{N-1}])$
- $P_N = (P_N \,||\, X)$的左边
- $P_{N-1} = C_{N-2} \oplus D(K, [C_N \,||\, X])$

- 这里|| 表示拼接功能



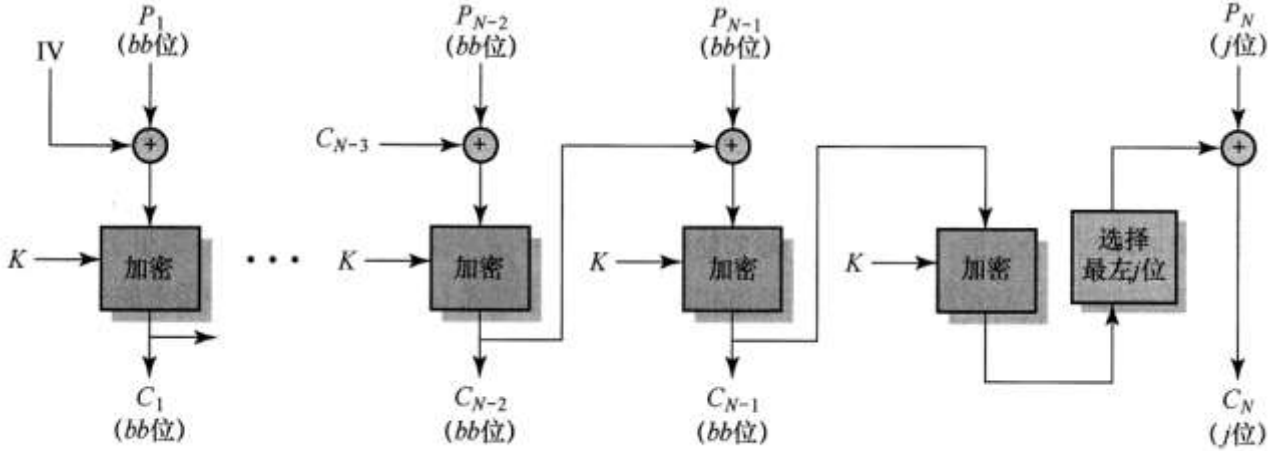
(a) 密文窃取模式

作业2-习题4

④

a. 假定最后一个分组P_N有j 位，加密完最后一个完整分组（P_{N-1}),再次加密密文(C_{N-1}），选择加密的密文最左边的 j 与短分组异或，产生要输出的密文。

b. b. 图7.18(b)给出的方法，当攻击者不能恢复最后一组明文时，他可以通过修改密文的个别位来改变最后一组明文。如果最后n位密文包含有重要信息，这将是一个弱点。如果最后几位只是一些简单的不重要的东西，就无关紧要。图7.18(a)方法的好处是明文消息的所有位都通过了加密算法.



(b) 替换方法

作业2-习题5

⑤ 对于n位分组大小，可能有2^n个不同的明文块和2^n个可能的不同密文块。对于明文和密文，如果我们将分组视为无符号整数，则值范围为0到2^n-1。对于可逆映射，每个明文分组必须映射到唯一的密文分组。因此要枚举所有可能的可逆映射，值为0的分组可以映射到2^n个可能的密文块中的任何一个。对于任何给定的值为0的分组的映射，值为1的分组可以映射到2^n-1个可能的密文分组中的任何一个，依此类推。因此，可逆映射的总数是$(2^n)!$。

理论上，密钥长度可以是$\log_2(2^n)!$位，假设为每个映射分配一个数字，从1到$(2n)!$，对于这样的变换，映射本身就是密钥，我们需要维护一个很大的映射表。在这种情况下，密钥的规模是$n*2^n$，n=64时，$64 * 2^{64} \approx 2^{21}$。从实现和运行的角度看，是不可行的。