第二次作业

作业2-习题1

① (William中文第八版)P152页习题7.4

- 在DES的ECB模式中，若在密文的传输过程中，某一块发生了错误，则只有相应的明文分组会有影响，然而，在CBC模式中，这种错误具有扩散性，比如传输时C_1发生错误将会影响明文分组P_1和P_2，

a．P_2以后的分组是否会受到影响?

b．假设P_1本来就有一位发生了错误，则这个错误要扩散多少个密文分组，对接受者解密后的结果有何影响?

作业2-习题2

② (William中文第八版)P153页习题7.6

- CBC-pad是RC5中的一种分组加密工作模式，它可以用于任何分组密码，并处理任意长度的明文，得到的密文最多比明文长一个分组的长度。填充的作用是保证输入明文是分组长度的整数倍。假设原始明文是整数字节，尾部填充1到bb个字节，这里bb为分组的字节长度。填充的字节相同，其值为填充的字节数。例如，若有8字节填充，则每个字节为00001000。那么为何不允许0字节的填充？若原始明文是分组大小的整数倍，为什么不省区填充？

作业2-习题3

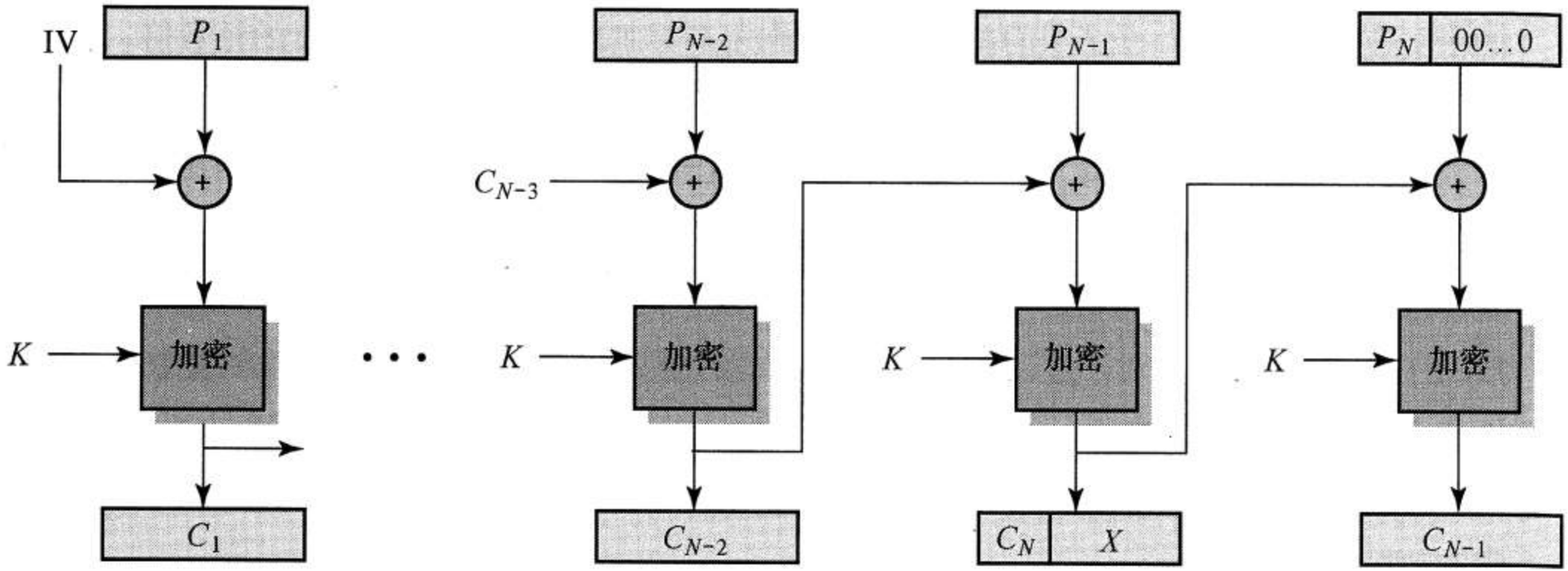
③ (William中文第八版)P153页习题7.11

- 填充并不总是合适的，例如，我们希望使用相同的内存缓冲区（明文最初存储在这里）来存储加密的数据，这时密文必须与明文的长度相同。密文挪用模式（CTS）是满足这种要求的一种工作模式。图7.18（a）为该模式的实现过程，

a. 解释CTS是如何工作的；

b. 描述如何解密C_{n-1}和C_n

图7.18(a)



(a) 密文窃取模式

作业2-习题4

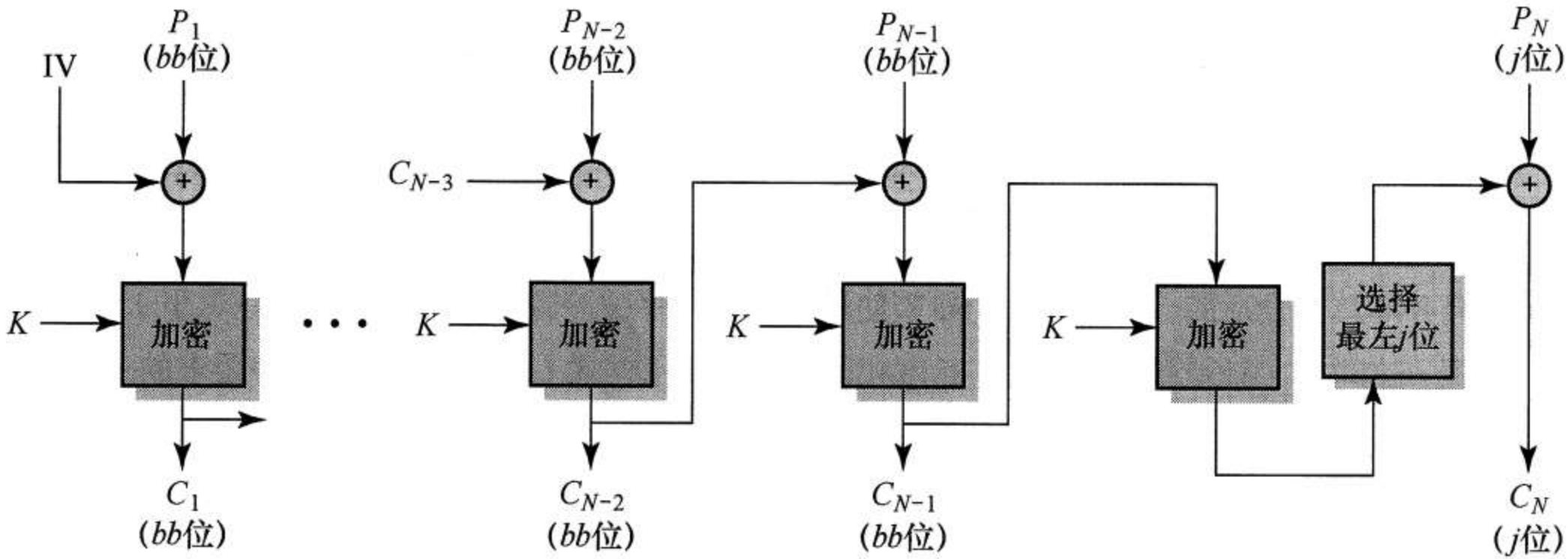
④ (William中文第八版)P153页习题7.12

- 图7.18(b)中给出了一种CTS的替换方案，使得当明文不是分组长度整数倍时产生的密文长度与明文长度相等

a. 解释该算法

b. 解释为何CTS算法比图7.18(b)中的方法更可取?

图7.18(b)


IV
P_1
(bb位)
P_{N-2}
(bb位)
P_{N-1}
(bb位)
P_N
(j位)
C_{N-3}
K
加密
选择
最左j位
C_1
(bb位)
C_{N-2}
(bb位)
C_{N-1}
(bb位)
C_N
(j位)

(b) 替换方法

作业2-习题5

⑤ 分组密码作用于n位明文分组，产生n位密文分组，当n=64或者更大时，为什么使用n位分组的任意可逆代替密码不可行？

提交要求

- 通过教学网提交，由助教张昱琪负责批改
- 如果包含多个文件，压缩为一个文件，提交作业的文件名采用“学号+姓名+第几次作业”
- 例“1300048400杨帆第1次作业.rar”或“1300048400杨帆第1次作业.zip”
- 按时提交截止时间:10月23日23：30前提交