第六章作业

16337341 朱志儒

思考题

6.1 三重 DES 加密分为两种，①使用两个密钥进行三次加密，具体运算过程是加密-解密-加密，即对明文 P 使用密钥 K_1 加密，再使用密钥 K_2 解密，最后使用密钥 K_1 加密得到密文 C；②使用三个密钥进行三次加密，即对明文 P 使用密钥 K_1 加密，再使用密钥 K_2 解密，最后使用密钥 K_3 加密得到密文 C。

6.3 三重加密中用到 2 个密钥，第一次加密和第三次加密使用相同的密钥。

6.4 第二步采用解密运算没有密码学上的深层含义，仅是为了使用三重 DES 的用户可以利用该算法解密单 DES 加密的数据。

习题

6.4 （a）不会，因为 C_2 以后的所有块的解密与 C_1 无关，所以 P_2 以后的所有块不会受到影响。

（b）这个错误要扩散到所有的密文分组，接受者解密后除了第一个明文分组有错误，其他明文分组均没有错误。

6.5 在 CBC 模式里不可能对多个明文分组进行并行加密，但可以对多个密文分组进行解密。

6.7 因为解密后，最后一个分组的最后一个字节用于确定需要剥离的填充量，所

以，必须至少有一个填充字节。

6.8 这个错误将会影响后续所有密文的解密。