作业

对称密码

第一讲

- 密码学的五个安全属性（目标）
- 对称密码体制和非对称密码体制的区别是什么

第二讲

- 举例说明古典密码体制体现下列技术的分别是哪个密码？代换、置换、扩散、分组/填充
- 维吉尼亚密码的惟密文分析都有哪些方法？
- 惟密文分析的前提条件是什么？

第三讲

- 完善保密的定义是什么?
- 计算安全的含义是什么?
- 实际安全的含义是什么?
- 满足完善保密的密码体制是哪些算法?

第四讲

- 对称密码的五要素是什么?
- 分组密码的设计技术主要是什么?
- DES和AES的迭代结构分别是什么?
- 2DES为什么不安全?
- 为什么DES迭代的轮数比AES迭代的轮数多?
- AES算法中承担扩散作用和混淆作用的函数分别是哪些?
- 为什么ECB模式不能加密长消息?
- 说明分组模式和流模式的主要区别?

第五讲

- 为什么一次一密不在现实中使用?
- 流密码分为同步和自同步流密码，常用的是哪一种?
- 硬件实现的流密码的主要技术是什么?
- m序列是什么？如何设计一个生成m序列的LFSR?
- LFSR为什么不能直接用来生成密钥序列?
- 如何基于LFSR设计安全的流密码?
- 为什么流密码的随机数要不可预测且足够长?
- 保密体制的攻击者按照目的分为哪些?
- 满足什么条件的保密体制是安全的?

第六讲

- Hash函数的三个安全要求是什么？
- 生日攻击用于求碰撞的复杂度是多少？
- 目前推荐使用的SHA-2（或SM3）使用的是什么迭代结构？压缩函数又是什么结构？
- 消息鉴别码用于保护消息的什么属性？
- 完整性保护角度来说，hash函数和消息鉴别码的区别是什么？
- 消息鉴别码的攻击者的攻击目标分为哪些？
- 满足什么条件的消息鉴别码是安全的？
- CBC-MAC的输出处理和截断有什么作用？
- HMAC的设计中，如何防止消息延展攻击的？
- 如何保障保密体制达到选择密文攻击下的安全性？