密码期末复习课

勿传

选择：20

填空：20

简答：30

计算：18

综合、分析、设计：12

“基本上大部分是基本概念，考的是比较细的，需要复习的细致一些”

“题里饶了很多弯”

“考试的知识点是讲过的，但是出题会经过转换而不是直接就见过的”

第一讲

- 密码学目的
  - 五个基础的密码学需要保证的体系：
    - 保密性、完整性、不可否认性、实体认证性、可用性
      - 保密性、完整性都有对称的、非对称的
      - 不可否认性只讲了对称的
      - 实体认证 指的是身份鉴别
      - 而消息认证码、指的是消息的原认证性，而非实体认证性
- 密码学的分类
  - 分析学、设计学的分类
    - 分析学
    - 设计学：协议、密码学源语、基本算法

- 哈希函数在被动攻击下，能保证完整性（因此哈希函数不作为密码学的源语）
- 非对称
  - 保密：
  - 完整：数字签名，并且还能保证不可否认性
- 协议：
  - 密钥分配、密钥协商
  - **身份鉴别协议（这个不考了，第十章不算在考试范围内）**

第二讲

- 代换密码体系、置换密码体系
- 一定要会求逆，考试的时候可以带计算器
- 那些古典密码都要会算
- 转轮密码主要体现了迭代结构，代换置换代换置换代换置换，混乱。这是为了突出分组密码的一个设计思想。
- 关于古典密码，穷举搜索的分析方法，复杂度到底是多少，关键的分析因素是秘钥空间大小
- 唯密文攻击：
  - 频率攻击
- 已知明密文攻击
- 计算复杂度
- 空间复杂度
- 数据复杂度

第三讲

- Shannon的通信保密系统
  - 加密密钥、解密密钥、加密算法、解密算法、明文、密文、DE=I ，其中I为恒等映射

    - 假设密钥信道是安全信道
- 公开信道能拿到什么？
    - 保密系统：密文
    - 认证系统：消息、认证码
    - 签名系统：消息、签名
- 三种安全性
    - 熵和无条件保密
        - H(P)-H(P|C)=0
        - 这个评估方式肯定不用了，只是理论的一个开山成果
            - 那他的价值呢？
                - 密码学：从艺术→技术
                - 香农
    - 计算安全性
        - 现代密码学所用
    - 实际安全性
        - 代价>信息本身价值
        - 现代密码学所用

中国的密码：

SM4，分组

SM3，哈希

公钥， SM2、SM9

第四讲

- 分组密码的定义
    - 每一块分组长度是一样的，每一块都去运算

- 分组密码算法设计思想（香农）
  - 迭代结构
  - 扩散
  - 混淆：非线性的体现
    -
- DES
  - 迭代结构 Festiel ：
    - 加解密相似
  - 分组长度64bit，密钥长度的实际有效位56bit
  - 运算
    - E扩展：
      - 怎么扩展的？
      - 怎么收缩的？
    - ？
    - S盒（混淆、非线性）
    - P盒
  - 轮密钥长度：48bit
  - 密钥拓展简单，列表
  - 具体怎么算的，步骤要明确
- AES
  - 迭代架构SPN
  - AES有三个版本，每个版本的分组长度都是128bit
  - 三个版本对应的是密钥长度不同，128、192、256
  - 根据密钥不同，迭代轮数不同。其中128是10轮迭代，最后一轮少一个运算。
  - 每一轮的运算
    - 字节代换（混淆、非线性）

            - 求逆运算
            - 仿射运算
        - 行移位
        - 列混合
            - 列和矩阵的乘法↔有限域上的运算
            - “两个多项式的乘法mod x^4 +1 …这个推理的过程”
        - 密钥加
    - 最后一轮少哪儿个？
    - 轮密钥长度：128bit
    - 密钥拓展不简单，用代换、移位、加常数
    - 具体怎么算的，步骤要明确
    - **AES重点讲了一个快速运算**
        - **有限域上字节的加法、乘法**

- SM4对标AES，分组、密钥长度都是128bit
- 攻击者
    - 主动
        - 选择明文攻击
        - 选择密文攻击
    - 被动
        - 唯密文攻击（利用密文有冗余）
        - 已知明密文攻击
    - 攻击者的攻击目的（从强到弱）：
        - 攻击出密钥
        - 攻击出某些明文
        - 攻击出明文的某些信息（某bit信息）

    - **安全的保密体制的评估条件：**
        - 最强能力的攻击者（选择密文攻击CCA），即使达到最简单的攻击（某比特信息IND）都不可行
- 分组密码的工作模式：
    - ECB模式
        - 对相同明文、相同密文会泄露信息（因为没有IV嘛，因此不能抗选择明文攻击），不安全，不推荐用来加密长信息。
    - 流模式和分组模式的区分：
        - 是否要填充分组
    - …之类的模式不能选择密文攻击，不过能抗选择明文攻击。

第五讲流密码

- OTP与伪随机数生成器
    - 伪随机性使用随机性检测标准检测
    - 如何设计生成的过程[伪随机生成器PRG]
- 同步流密码与自同步的流密码
    - 自同步是密文要参与到下一次密钥流的生成的过程
    - 同步跟密文完全没关系，仅跟初始密钥流有关
        - 我们上课上的都是同步的
- 算法实现：硬件实现、软件实现
- 硬件实现的基础，反馈移位寄存器
- 线性反馈移位寄存器
    - 两个参数
        - 存储单元的个数（级数n）
        - 反馈函数(f)
    - 如何设计一个m序列

- 初始状态填什么？
  - 密钥、随机数
- 生成m序列如何设计寄存器
  - 选择合适的n →2^{n-1}的序列
  - n阶本原多项式，多项式的高次项对应反馈函数低次项的数值
- 生成的数据是不安全的
  - 已知明密文攻击（这是一个被动攻击）：
    - 密文 异或 明文 = 密钥流
    - 已知n级的寄存器，得到2n长的密钥流，就可以列出方程组。
      - 可以得到反馈函数
      - 然后后续的密钥流、前面的密钥流可以恢复
    - 就算不知道n，也可以通过BM算法得到级数n以及其生成多项式
    - 因此如果使用基于线性反馈移位寄存器的方法，要使用：
      - 线性反馈移位寄存器s + 非线性
      - 驱动部分 + 非线性部分(滤波、走停)

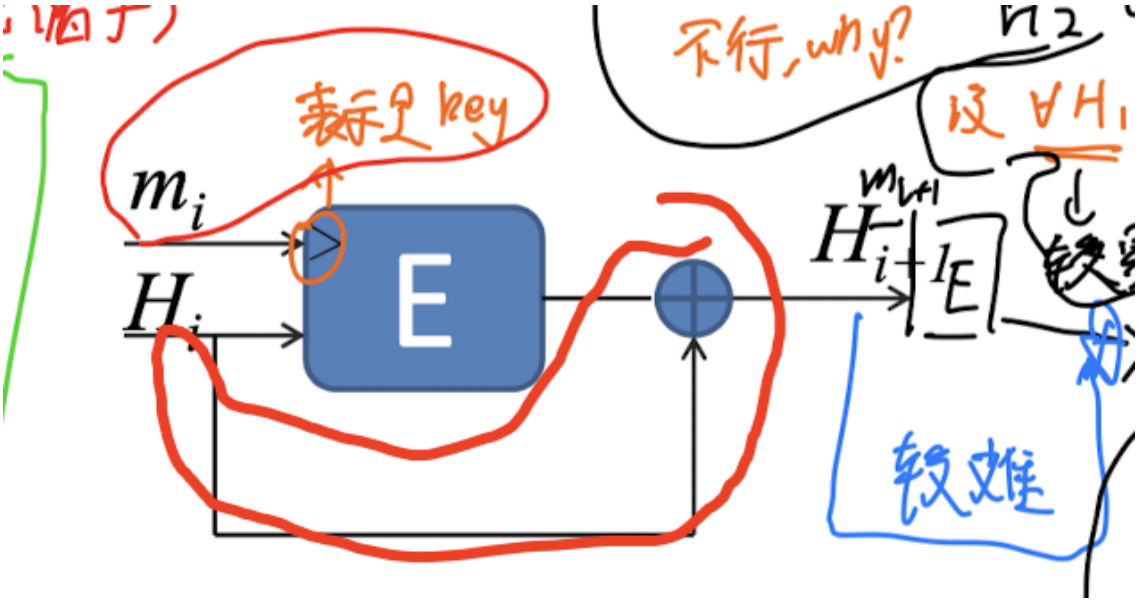
- 软件算法：RC4
  - 生成一个大的表，每次从表里调出一个位置的值来输出，同时将表中两个位置交换
- Estream算法
  - 看了一个软件的和一个硬件的
- 重点：关于如何设计一个反馈移位寄存器，以及如何使用反馈移位寄存器设计一个密码算法
- PRG的安全问题：相同明文↔相同密文，因此不抗选择明文攻击，为了让他抗选择明文攻击，因此里面需要融入初始向量IV
- 对PRG的选择密文攻击：
  - 密文 异或 随机数 → oracle

    - oralce解密 →攻击者
    - 攻击者将收到的值，与随机数异或
- 如何防止选择密文攻击？
    - 之前的密码源语/工作模式+消息鉴别码

消息鉴别码

- 攻防体系
    - 攻击拥有：
        - 已知(m,mac)对
        - 选择消息攻击，从oracle上得到mac值
    - 攻击结果：
        - 选定消息，得到MAC(选择性伪造)
        - 存在性伪造，能找到存在的(m,MAC) s.t.
            - Var(m',MAC',key)=1
            - (m',MAC') 不属于 {(m1,MAC1),(m2,MAC2)……}，即这是一个新的
    - 安全的消息鉴别码的定义：
        - 最强的攻击能力（选择消息攻击），最弱的攻击结果（存在性伪造）不可行
- 哈希函数定义及其安全目标
    - 哈希函数只能防止被动攻击，而不能防止主动攻击
    - 定义
    - 单向：穷举攻击，暴力搜索 $O(2^n)$
    - 二次原象：穷举攻击，暴力搜索 $O(2^n)$
    - 碰撞：生日攻击 $O(2^{n/2})$
- 消息鉴别码：

- 消息鉴别码的安全性由两个因素保障
  - min{ |KEY|,|OUTPUT|}，若k长m， output长n，则min{ 2^m,2^n}
- MD结构：
  - 填充消息长度
- DM压缩函数：
  - 要把链接变量反馈回来做运算
  -



- SHA系列
  - SHA-数字，数字表示的是输出的长度

- 消息鉴别码可以防主动攻击
- 消息鉴别码的构造
  - CBC分组模式构造
    - 输出跟分组的算法有关
    - 与CBC加密的不同地方，没有IV这个随机数的向量

        - 在输出的时候，一定要记得对输出的处理，来防止一些攻击。老师上课讲了两种攻击，如果做了输出处理就不可以实现了。

    - 基于HMAC构造
        - ….去看看
- 认证加密模式：
    - E then MAC
    - E & MAC
    - MAC then E

非对称密码体制

- 为什么提出非对称密码体制
    - 对称密码体制不可以的地方：
    - 初始密钥分发
    - 消息的不可否认性
    - 密钥管理
- 发展
    - DF提出思想
    - …提出RSA算法
- 重点是RSA、ElGmal
- RSA:
    - **密钥生成过程、加密过程、解密过程一定要非常非常熟悉**
    - RSA基于整数分解问题困难
    - **参数选择的问题，一定要比较清晰，讲过的参数要求一定要非常清晰**
        - 整数足够长

        - p和q的要求
        - e的要求
        - d的要求
        - 不能共模…
    - RSA是确定性加密，RSA有同态性，不安全
        - 在真正使用的时候，是OAEP模式
- ElGmal：
    - 有限域的离散对数问题
    - 加密过程有选随机数，是随机算法，相同的明文在不同次加密的时候得到了不同的密文
        - 不过不抗选择..攻击，不可以直接使用，还需要封装
    - **参数误用**
        - **泄露**
        - **复用**
- 椭圆曲线：
    - 完全类比ElGmal，从有限域→群
    - 基于椭圆曲线上的离散对数问题
    - 椭圆曲线在参数的长度上具有绝对优势，存储设备上占有优势
    - SM2，基于椭圆曲线构造的
    - **不需要会计算，不考他的计算**
- **RSA的快速运算的问题，平方乘的方法**

第八讲数字签名

- 公钥在很多时候，是没有选择明文攻击的，而是有一个唯密钥（指只有公开密钥），只拿到公开密钥就攻击
- 首先要拿到密钥，然后再进行伪造

    - 选择性伪造
    - 存在性伪造
    - 一致性伪造
- 安全的
    - 选择性消息的攻击情况下，存在性伪造不可行。
- 算法：
    - RSA
        - 谁的XX加密，谁的XX解密，谁的XX签名，不要弄混了
        - 参数选择
            - p、q
    - DSA
        - 怎么计算
        - k泄露了的问题、有签名等式如何验证签名
    - 椭圆曲线
        - 完全比对DSA
        - 好处仍然是参数长度短，也不要求相关计算
- 加密认证方式
    - 保证保密性、完整性、不可否认性
    - 先加密、再密文签名
    - 先对明文签名、再明文及签名一起加密

第九讲

- 密钥管理
    - 首先要知道，有很多很多的环节，从密钥的生成，一直到密钥的销毁，每一个环节需要有什么安全保护需要知道

    - 密钥管理还涉及到分层的管理方式，主密钥、密钥加密密钥、会话密钥，他的好处是什么？
        - 会话密钥不需要保存，生成周期小
        - 主密钥使用的次数可以不用那么频繁，不用经常去换主密钥
- 秘钥分配和密钥协商协议
    - 中间人攻击
        - 消息源的认证
    - 重放攻击
        - 时间戳、随机数
    - 一致性：
        - 告诉对方已经达成了一致的密钥
- 不同场景下，如何安全部署系统
- 密钥协商，一步一步搭建，怎么看中间人的攻击，怎么看如何防止中间人的攻击 ：使用公钥、公钥用证书认证
- 数字证书
    - CA完成颁发、签名
    - RA的主要工作是验证申请证书的人的身份是否是相同的。
    - RA不掌握私钥，CA才掌握私钥
    - CA证书的生命周期
    - 真正认证的时候需要检查哪儿些检查项
- 秘密共享
    - <t个人一定不行，≥t一定能恢复
    - 秘密分割、秘密合成，大致了解一下
- 密钥托管：
    - 对通信进行监听，对密钥加密密钥做了一个备份的技术
    - 了解一下他的目标就行了

AES、DES的加密过程要会算

计算器用来干啥？
模、求逆，AES的快速运算一定考，DES的P、S都是靠表，要知道怎么查表

以老师PPT讲的为主，不需要去背课本

所有题都会绕点小弯

为了让同学们思考怎么回答这些问题，题目的数量不是特别多，不过难度…