密码学老师复习

- 考试不用带计算器，手算可以算出来

考试内容

- ①填空题（比如1976年谁谁谁提出了什么什么体制，还有专业的名词解释，攻击方法，敌手的目标和手段，就是树上的**黑体字**，标题、名词和定义之类的，也有**小计算题**）②判断题，书上定义或定理性的东西，可能照搬**定理**，要判断正误。③单项选择题，*（他说一看就会）*④多项选择题，少选扣一点，错选全部扣完，可能会出全部都能选上的题。⑤名词解释，比如什么叫密文不可区分，都是书上的定义。⑥计算题，可以参照书上的例题⑦解答题，*（听说比较简单）*，比如学了对称密码体制可以实现CRA（机密性，完整性，认证性），或者比如基于某个体制给出一个方案

第一章 古典密码学

- 79年以前的密码体制
- 都是对称密码体制，单钥体制。
- 两个基本的技术：①代换②置换 现代密码学依然在用，AES、DES哪个是代换 哪个是置换
- 代换是非线性的，所以是必须的。
- 几个密码要记下来，加密方案和分析方案都要会。
- 一般的密码攻击：①唯密文攻击②已知明文攻击③选择明文攻击④选择密文攻击，后两种古典密码学用不上，用前两种就能破解了。
- 体制：①密钥数量：私钥和公钥②时间：古典密码和现代密码③工作模式：分组密码和流密码

第二章 香农理论

- 完善保密性（考虑敌手有无穷的计算能力，唯密文攻击）：①一次一密，本质②概率角度，拿到密文并不会提升破解的概率
- 熵的定义，并掌握它的计算方法。
- 2.6不考察，其他的都要考

第三章 分组密码与高级加密标准

- SPN网络，也就是代换-置换网络。
    - 乘积密码，需要多轮的迭代，每一轮都有代换-置换操作，形成一个网络
    - 构造现代分组密码的基础。
- DES基本步骤，每一轮的具体操作
    - 分组密码，实际密钥56bit，有校验位。
- AES基本步骤，每一轮的具体操作
    - 四个操作，只有字节代换是非线性的代换。
    - 考虑$GF(2^8)$,要对有限域和元素求逆知道。
- 分析方法：线性分析和差分分析，基本原理都要会。
    - 线性分析是一种已知名密文攻击，优点是线性都能用
    - 差分攻击是选择密文攻击，缺点是需要密文异或差值满足一定条件
- 工作模式：①DMR模式是不安全的，会泄露明文信息。（不满足不可区分性）②CBC模式，概率加密，相同的明文加密得到不同的密文。③还有别的工作模式，也要记住缩写和基本原理。
- 到这里为止还是私钥密码学

第四章 HASH函数

- 原语只有：哈希、加密（公钥，私钥）、认证、伪随机数产生器
- 哈希分不带密钥（只有完整性功能，没有认证性，无法确认消息来源）和带密钥（可以认证），后者又叫MAC
- hash函数就是对不定长输入值产生一个固定长度的消息
- ①原像稳固②第二原像稳固③抗碰撞的
- hash函数的构造也是通过迭代，有MD结构（MD5已攻破）和SHA算法（安全hash算法）
- 消息认证码的定义和安全性定义，假设成立，不可能存在伪造。
  - 构造方法有①用小MAC构造大MAC②CBC-MAC，在选择攻击伪造下依然是安全的，被证明过。
- 4.5不考，考4.1~4.4

第五章 RSA

- 计算题大部分都出在第五章RSA
- 勒让德符号和雅各比符号计算，要会用互反律
- 公钥密码学谁提出的和提出时间?
- 公钥密码学的关键是陷门单向函数
- 欧几里得算法、中国剩余定理、符号、费马小定理、素性检验
- RSA加密方案一定要会描述
- RSA的攻击（计算题不考，掌握名词和基本原理就可以）
  - 分解整数成因子：①穷搜索②pollard p-1②pollard ρ③随机平方算法
  - RSA问题（也叫RSA的逆问题）：告诉你n、b和y，求解x，这与$n=pq$不等价
  - 求出解密指数：①由加密指数
- 需要知道有一些特殊的RSA是不安全的：①小解密指数a
- Rabin密码体制用的是平方，所以一个密文对应四个明文，需要使用中国剩余定理进行求解，选其中一个即可。还有一个很好用的小技巧，用$euler$准则
  - 优点是效率高，而且与$n=pq$等价，能拆解Rabin密码体制，就能解决因子分解问题
- 比特安全性，语义安全性（拿到密文得不到任何明文的信息），RSA密码方案达不到语义安全性，在选择明文和密文攻击下可以知道。书本上有一个RSA构造满足语义安全性（下面的小f变成RSA加密即可）。
  - **密码体制 5.3** 语义安全的公钥密码体制

    设 m, k 为正整数；设 $\mathcal{F}$ 为一族陷门单向置换，且对任意的 $f \in \mathcal{F}$，有 $f: \{0,1\}^k \to \{0,1\}^k$；且设 $G: \{0,1\}^k \to \{0,1\}^m$ 为一个随机谕示器。令 $\mathcal{P} = \{0,1\}^m$，且 $\mathcal{C} = \{0,1\}^k \times \{0,1\}^m$，定义

    $$\mathcal{K} = \{(f, f^{-1}, G): f \in \mathcal{F}\}$$

    对 $K = (f, f^{-1}, G)$，随机选取 $r \in \{0,1\}^k$，且定义

    $$e_K(x) = (y_1, y_2) = (f(r), G(r) \oplus x)$$

    其中 $y_1 \in \{0,1\}^k, x, y_2 \in \{0,1\}^m$。进一步，定义

    $$d_K(y_1, y_2) = G(f^{-1}(y_1)) \oplus y_2$$

    $(y_1 \in \{0,1\}^k, y_2 \in \{0,1\}^m)$。函数 f 和 G 为公钥；函数 f^{-1} 为私钥。
- 确定密码方案没有语义安全性。

第六章 离散对数和公钥密码学

- 计算题也会出在第六章
- ①离散对数问题②$Diffie-Hellman$问题
- $EIGamal$密码体制，语义安全性基于判定性$Diffie-Hellman$问题
- 离散对数问题算法：①$Shanks$算法②pollard ρ③$Pohlig-Hellman$算法④指数演算法（只有在Z_p^*）
- 通用算法的复杂度下界$\Omega(n)$
- 有限域基本运算要会，可以看看之前实现的有限域
- 椭圆曲线：①实数上②模素数上③有限域上， 可以照搬之前的加密方案。
  - 要记住椭圆曲线的定义和运算，再记不住也要记住它的运算的几何意义
  - 会出填空题、选择题或者计算题
  - 点加和倍点要知道，书上的三种情形
- 比特安全性：针对素数阶群才有，其他阶数的群会有泄露的可能。比特安全性等价于求整个x
- $EIGamal$体制＋素数阶群有语义安全性，但是教科书式的体制不满足语义安全性，密文可识别。
- $Diffie-Hellman$问题书上标黑字了，记得看。

第七章 签名方案

- 公钥密码学是公钥加密，私钥解密。而签名方案是私钥加密，公钥认证。
  - 应用在音乐或者其他电子形式的作品，可以认证为正版。
- 签名方案定义的五元组记得要背，可以出填空题
- 签名方案相比加密体制，也有独特的攻击手段和攻击目的，记得背。
- $EIGamal$签名方案和它的变体
- RSA是确定性的，但是离散对数签名不是确定性的，是概率性算法。
- 可证明安全的签名方案：①一次签名，没有选择消息攻击，所以安全。记得定义和构造方法看一下。
- 不可否认签名：不能公开验证，需要借助签名者的帮助。
- 7.7不考

第八章 伪随机数生成

- 伪随机数生成是一个新的原语，只要**任意**有一个**单向函数**，就能构造伪随机数产生器
- 输入定长种子，通过不停地迭代，取其中的每次迭代的某一比特组成输出比特串。
- 不可区分性和下一比特预测器，有定理将它们两个捆绑在一起，有下一比特预测其就能构造区分器。
- 0和1真的完全频率相等的伪随机数生成器，也是不安全的。