密码学复习提纲

2024年

目　录

第一章　密码学复习要点

1.1 考试方式和题型

以理解为主，不需要死记硬背。
基本要求：

- 理解基本概念
- 能看懂密码算法(分组密码、公钥密码、流密码、Hash函数)和基本密码协议（签名方案）
- 能做初步的安全分析

考题来源：

- 课本基本内容。越是基础的越容易被考到。
- 课本例子。
- 平时作业。

题型：

- 选择题（单选题）：考察基本知识点和计算
- 判断题：主要考察基本知识点
- 填空题：计算题为主。第一章的较多。
- 问答题：题型有密码分析、证明、解密。

1.2 每章的复习要点

其中红字部分所占分数较高，大部分问答题来自红字部分。

1. 第1章古典密码：
    - 密码体制的基本概念
    - 古典密码：包括移位密码、仿射密码、代换密码、置换密码、维吉尼亚密码和希尔密码，掌握它们的加密和解密运算，以及密码空间计算。
    - 流密码：重点掌握LFSR的基本原理、周期计算等。
    - 密码分析的基本概念：Kerchhoff假设、唯密文分析、已知明文分析、选择明文分析和选择密文分析，理解强力攻击（或穷搜素攻击）的原理和计算复杂度。

2. 第2章Shannon信息论：

- 理解三种安全性的度量准则（计算安全性、可证明安全性和无条件安全性）
- 掌握完善保密性概念及基本的证明方法
- 了解一次一密加密体制的优缺点
- 唯一解距离和乘积密码对现代密码学设计的指导意义，其结论的推导不考。

3. 第3章分组密码：

- 理解分组密码的迭代加密方式
- 2种主要加密结构（SPN和Feistel）的特点
- 了解2种线性密码分析和差分密码分析的基本情况（对具体思路不做考试要求）
- 能看懂DES、AES算法（不需要死记硬背算法细节），了解其安全现状。了解如何快速实现分组密码算法。
- 理解4种分组密码的工作方式的安全性和特点。

4. 第4章Hash函数：

- 理解Hash函数的安全用途（即消息完整性），以及Hash函数、消息认证码和签名的安全用途区别（最后者可以解决消息完整性和不可否认性，前二者只能解决消息完整性）。
- 安全要求：即对三个问题是难解的，对三个问题的基本攻击方法（例如生日攻击）和成功概率计算
- Hash函数的迭代设计思路。
- 能看懂SHA-1算法
- 了解消息认证码的特点、对消息认证码的假冒攻击。
- 能对简单的Hash函数和消息认证码做安全性分析：题型来自课本例题和布置的习题。
- 4.2.3、4.3.1、4.5节不考，4.4.1和4.4.2节中安全性分析不考。

5. 第5章RSA密码体制：

- 理解公钥密码体制的特点和基本构造方法（限门单向函数）
- 熟悉RSA密码体制。
- 理解图灵规约的概念，见课本P167。
- 理解5.9节(课本P168-169）中关于语义安全的概念。

- RSA的安全性分析：5.7.1、5.7.2、5.9.1节。
- 5.2节不考，但这节涉及到的数论和代数知识是公钥密码学的数学基础。
- 5.4、5.5、5.6、5.7.3、5.8、5.9.2节不考。

第6章公钥密码学和离散对数：

- 6.1、6.6节：理解群上的离散对数问题、ElGamal公钥密码体制、以及一般群上ElGamal公钥密码体制。
- 6.7.3节：$\mathbb{Z}_p^*$上的离散对数、CDH问题、DDH问题和Elgamal解密之间的关系。
- 6.2、6.3、6.4、6.5、6.7.1、6.7.2节不考。

第7章签名方案：

- 签名方案的安全要求，签名和加密的顺序
- Hash函数在签名中的使用和对Hash函数的要求
- RSA签名方案的安全性分析
- 其余部分不考

第二章　本课程总结

部分概念列出详细定义，部分只简略提及，没有详细写的不代表不重要，只限于时间和篇幅缘故，细节参考复习课本或课件。

2.1 密码学的体系结构

以Shannon信息论的提出为分界，分为：

- 古典密码(第1章)
- 现代密码

现代密码学的基本密码算法有：

- 加密算法：保护消息私密性。分为对称（私钥）和非对称（公钥）两类。
- Hash函数：保护消息完整性。分为不带密钥的和带密钥（消息认证码）的两类。
- 伪随机数生成器：生成看起来“随机”的比特流（不做考试要求）

由基本密码算法可构造各种密码方案（协议）：

- 签名方案（第7章）
- 身份认证（识别）（不做考试要求。第9章）
- 密钥建立和管理方案（不做考试要求）：
  - 公钥基础设施（PKI）（见第12章）：用于非对称密钥的建立和管理，公钥以证书形式保存（见第9章）。不做考试要求。
  - 密钥分配和协商方案（见第10-11章）：用于对称密钥的建立和管理。不做考试要求。
- 其它各种用途的密码协议（不需要掌握）
  - 秘密共享
  - 组播安全和版权保护
  - 零知识证明
  - 电子选举
  - 电子现金
  - 多方计算
  - 。。。

把密码协议应用到通信安全中并标准化，就形成了满足各种需要的安全标准。

2.2 加密算法设计和分类

根据加密密钥和解密密钥的关系，加密算法分为：

- 对称密码体制：从加密密钥推出解密密钥是容易的，一般加解密钥一致或相似，其密钥也因此称为秘密密钥。分为以下2类：
  - 分组密码：每一分组加密的密钥一样，一般采用迭代加密，需要设计轮函数、密钥编排方案，根据轮函数的结构主要分为2类：
    - Feistel结构：代表算法为DES，也因此称为DES-like结构
    - 代换－置换网络(SPN)：代表算法为AES
  - 序列密码（或称为流密码）：用种子密钥生成密钥流，再用密钥流加密明文流。线性反馈移位寄存器(LFSR)是序列密码的基本构造部件。
- 非对称密码体制（也称为公钥密码体制）：从加密密钥推出解密密钥是困难的，通过单向限门函数构造，单向限门函数又通过数学困难问题构造，主要分为：
  - 基于整数因子分解问题：代表算法为RSA
  - 基于离散对数问题：代表算法为ElGamal

2.3 Hash函数设计和分类

Hash函数可分为：

- 不带密钥的。根据输入消息长度限制分为：
  - 输入消息长度有限，也称为压缩函数，采用迭代函数构造。例：SHA系列算法。
  - 输入消息长度可任意长，可基于压缩函数构造，如Merkle-Damgard结构
- 带密钥的，也称为消息认证码（MAC），构造方法有
  - 基于不带密钥的Hash函数构造，如HMAC
  - 基于对称加密构造，如CBC-MAC

2.4 安全准则

安全准则，即我们如何评价一个密码体制的安全性。
评价密码体制的安全性，有以下三个准则（见p.36）

(a) 计算安全性：破译密码体制需要N次计算量，N是某个很大的数。如公钥密码体制建立在计算上困难的问题上。

(b) 可证明安全性：在某个假设下，可证明是安全的。例子：1）基于碰撞稳固的压缩函数compress，用Merkle-Damagard结构构造的Hash 函数也是碰撞稳固的(见p103 定理4.6)。2）如果Computation Diffie-Hellman问题是难解的，则ElGamal密文也是难解的（见p.216，解CDH问题的算法，可用于解密ElGamal密文，反之亦然）。

(c) 无条件安全性：安全性不依赖于攻击者所掌握的计算资源。具有完善保密性(见p.38)的密码体制是无条件安全的，一次一密密码体制(p.42)是完善保密的，但是不实用。其它例子：对参数k的Blom密钥预分配方案，任意k个用户联合起来也无法给出其它两个用户的会话密钥（p.310），这是无条件的安全性质。

Hash函数的安全准则：安全的Hash函数应该对以下三个问题是难解

(a) 原像问题（Preimage）：给定Hash函数h和输出y，求输入x满足$h(x) = y$。如对该问题困难则称为原像问题稳固。

(b) 第二原像：给定Hash函数h和输入x，求另一输入x'满足$h(x') = h(x)$。如对该问题困难则称为第二原像稳固。

(c) 碰撞：给定Hash函数h，求x, x'满足$h(x) = h(x')$。如对该问题困难则称为碰撞稳固。对碰撞问题的最简单的攻击是生日攻击。

消息认证码的安全准则：

(a) 假冒者：如果攻击者知道Q个MAC的输入输出对$(x_1, y_1), \ldots, (x_Q, y_Q)$，能够计算出未知的MAC输入输出对$(x, y)$，即$x \notin \{x_1, \ldots, x_Q\}$，且$x = MAC_k(y)$，那么$(x, y)$称为假冒者，如果成功概率为$\epsilon$，则该攻击者称为$(\epsilon, Q)$假冒者。对足够大的$Q$，安全的MAC应该不存在高概率的假冒者。

签名方案的安全准则：

(a) 签名者无法否认有效的签名

(b) 其它人无法伪造有效的签名

2.5 密码分析方法

密码分析是密码编码学的对立面，分析密码的安全性是为了设计出安全的密码体制。

密码分析的Kerchhoffs假设(p.19)：假设密码分析者已有密码算法及其实现的全部细节，密码的安全性只依赖于密钥而不是对算法的保密。

密码分析的攻击模型分类(p.19)：

(a) 唯密文攻击

(b) 已知明文攻击

(c) 选择明文攻击

(d) 选择密文攻击

对签名方案的攻击模型分类(p.224)：

(a) 唯密钥攻击

(b) 已知消息攻击

(c) 选择消息攻击

攻击者对签名方案的目标分类(p.224)

(a) 完全破译

(b) 选择性伪造

(c) 存在性伪造

对密码算法的基本攻击：

- 穷搜索密钥分析，也称为强力攻击：即穷尽搜索所有密钥直到解密成功，对长度为n的密钥， 密钥空间大小为2^n，因此平均搜索复杂度为$O(2^{n-1})$。穷搜索分析是最基本的分析，适合于所有密码算法，如果一种分析方法的计算复杂度低于穷搜索，我们才能称之攻击“成功”。

分组密码的基本分析方法（不要求掌握）

(a) 差分分析：为选择明文分析

(b) 线性分析：为已知明文分析

对Hash函数的基本攻击：

- 生日攻击

对RSA的安全性分析：

(a) 分解n（不要求掌握）

(b) 计算$\phi(n)$，等价于分解n（5.7.1节）

(c) 计算解密指数，等价于分解n（5.7.2节）

(d) RSA的语义安全（5.9.1节）

对ElGamal密码体制的安全性分析：

(a) 离散对数的比特安全性(6.7.1节，不考)

(b) Diffie-Hellam问题（6.7.3节）

数字签名的分析（详见课件或课本）：

(a) 签名方案结合加密、hash函数的安全性分析(7.1，7.2.1节)

(b) RSA签名方案的3种伪造(7.2节)

(c) ElGamal签名的2种伪造，若知签名中的随机数k的攻击方法，若知签名中的随机数相等的攻击方法(7.3.1节)