

2023 密码学原理与实践 (第三版)

总结

Cryptography Theory and Practice
Third Edition



苏明

[加] Douglas R. Stinson 著

冯登国 等译



第一章 古典密码学

➤ 1. 1 几个简单的密码体制

- 1. 1. 1 移位密码
- 1. 1. 2 代换密码
- 1. 1. 3 仿射密码
- 1. 1. 4 维吉尼亚密码
- 1. 1. 5 希尔密码
- 1. 1. 6 置换密码
- 1. 1. 7 流密码

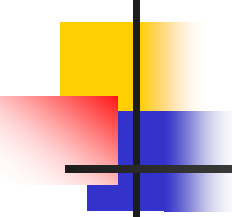
➤ 1. 2 密码分析

- 1. 2. 1 仿射密码的密码分析
- 1. 2. 2 代换密码的密码分析
- 1. 2. 3 维吉尼亚密码的密码分析
- 1. 2. 4 希尔密码的密码分析
- 1. 2. 5 LFSR流密码的密码分析



第二章 Shannon理论

- **2. 1 引言**
- **2. 2 概率论基础**
- **2. 3 完善保密性**
- **2. 4 熵**
- **2. 5 熵的性质**
- **2. 6 伪密钥和唯一解距离**
- **2. 7 乘积密码体制**



第三章 分组密码与高级加密标准

- **3. 1** 引言
- **3. 2** 代换-置换网络
- **3. 3** 线性密码分析
- **3. 4** 差分密码分析
- **3. 5** 数据加密标准
- **3. 6** 高级加密标准
- **3. 7** 工作模式



第4章 Hash函数

- **4. 1 Hash函数与数据完整性**
- **4. 2 Hash函数的安全性**
- **4. 3 迭代Hash函数**
- **4. 4 消息认证码**
- **4. 5 无条件安全消息认证码**



第5章 RSA密码体制和整数因子分解

- **5. 1** 公钥密码学简介
- **5. 2** 更多的数论知识
- **5. 3** **RSA**密码体制
- **5. 4** 素性检测
- **5. 5** 模 n 的平方根
- **5. 6** 分解因子算法
- **5. 7** 对**RSA**的其他攻击
- **5. 8** **Rabin**密码体制
- **5. 9** **RSA**的语义安全性



第6章 公钥密码学和离散对数

- **6. 1 ElGamal密码体制**
- **6. 2 离散对数问题的算法**
- **6. 3 通用算法的复杂度下界**
- **6. 4 有限域**
- **6. 5 椭圆曲线**
- **6. 6 实际中的离散对数算法**
- **6. 7 ElGamal体制的安全性**



第7章 签名方案

- **7. 1 引言**
- **7. 2 签名方案的安全性需求**
- **7. 3 ElGamal签名方案**
- **7. 4 ElGamal签名方案的变形**
 - Schnorr签名方案**
 - 数字签名算法(DSA)**
 - 椭圆曲线DSA**



第8章 伪随机数的生成

- **8. 1 引言与示例**
- **8. 2 概率分布的不可区分性**
- **8. 3 Blum-Blum-Shub生成器**
- **8. 4 概率加密**



Examinations

平时成绩占40%

期末考试闭卷60%

考试时间：1-4 8:00-9:40 星期四

津南公教楼B区304

答疑 1-3 周三 16:00-17:00 计控楼450



Examination

- 判断题、
- 填空题、
- 解答题、
- 综合题、
- 难度题

涉及到算法，请写清楚逻辑结构(如伪码)，并解释