密 码 学

第十八讲　复习

张焕国

武汉大学计算机学院

空天信息安全与可信计算教育部重点实验室

内容简介

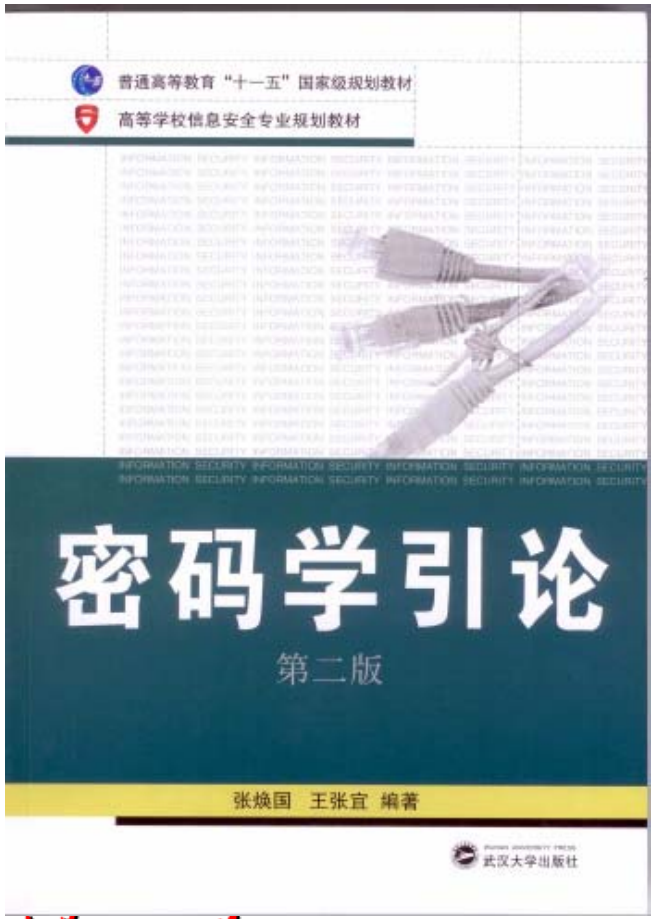
第一讲 信息安全概论
第二讲 密码学的基本概念
第三讲 数据加密标准（DES）
第四讲 高级数据加密标准（AES）
第五讲 中国商用密码（SMS4）
第六讲 分组密码的应用技术
第七讲 序列密码
第八讲 复习
第九讲 公钥密码（1）

内容简介

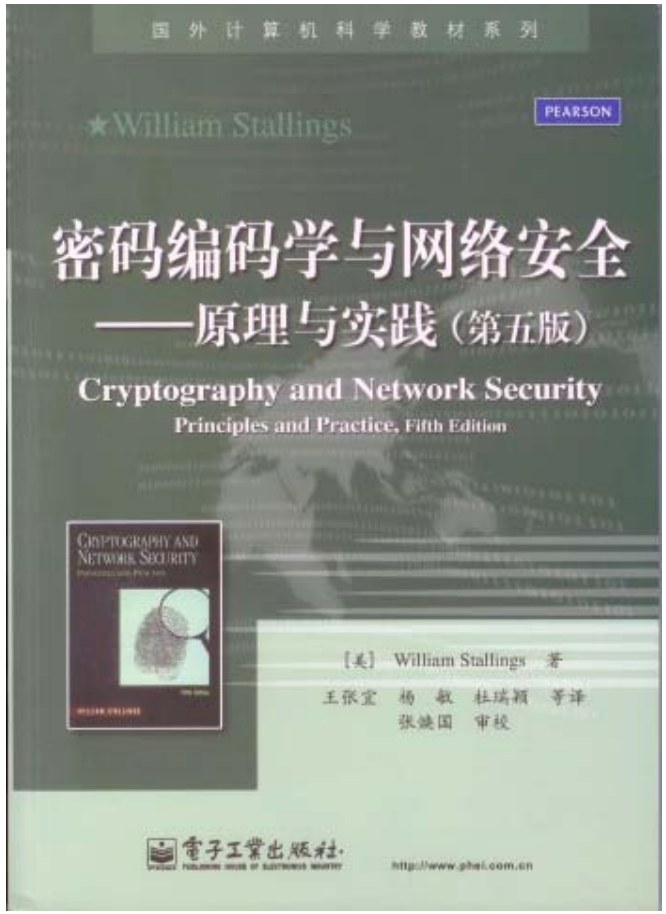
第十讲 公钥密码（2）
第十一讲 数字签名（1）
第十二讲 数字签名（2）
第十三讲 HASH函数
第十四讲 认证
第十五讲 密码协议
第十六讲 密钥管理（1）
第十七讲 密钥管理（2）
第十八讲 复习

教材与主要参考书

教材



参考书



第九讲　复习题

●RSA密码

①证明RSA密码加解密算法的可逆性

② 证明RSA密码加解密算法的可交换性

③ 说明对于RSA密码从公开加密钥不能求出保密的解密钥

④令p=3,q=11,d=7,m=5,手算密文C 。

⑤设RSA密码的 e=31,n=35,C=10,手算明文M 。

第九讲　复习题

●RSA密码

⑥设A，B为正整数，D=(A,B)。试证明：$\phi(AB)=D\,\phi(A)\,\phi(B)/\,\phi(D)$

⑦RSA密码的快速运算

- 分析反复平方乘算法的效率
- 说明 Montgomery算法为什么效率高？它适合哪些情况下应用？

⑧编程实现RSA密码的加解密运算。

⑨ 在RSA中使用e=3作为加密指数有和优缺点？使用d=3作解密指数的做法好吗？为什么？

第十讲　复习题

- **ELGamal密码**

①证明**ELGamal**密码的可逆性。

②为什么**ELGamal**密码要求参数 **K**是一次性的？

③设**p=5**，**m=3,**构造一个**ELGamal**密码，并用它对**m**加密。

④编程实现**ELGamal**密码。

第十讲　复习题

- 椭圆曲线密码

①证明椭圆曲线密码的可逆性。

②为令**p=5**,求出椭圆曲线 $y^2=x^3+4x+2$的全部解点

③以教材例**5-5**为例，分别以**G=(2,7)**和**G=(5,2)**构造椭圆曲线密码，并设**m=3**，分别进行加密和解密。

第十一、十二讲　复习题

- 数字签名

①为什么数字签名能够确保真实性？

②说明对于**RSA**的数字签名，为什么先加密后签名不安全？

③说明**HASH**函数在**RSA**数字签名中的作用。

④深入理解**ELGamal**密码和椭圆曲线密码的数字签名。

⑤说明在**ELGamal**密码签名中，参数**k**为什么必须是次性的。

⑥说明在椭圆曲线密码签名中，参数**k**有无一次性的要求。

第十三、十四、十五讲　复习题

- 认证

①设计一个综合报文认证方案，包括报文源、报文宿、报文顺序、报文内容的认证。

- **HASH函数**

①安全**HASH**函数 要满足那些条件？为什么？

②编程实现**SHA-1** 和**SM3**。

- 密码协协议

①分别使用对称密码和公钥密码设计一个安全的双向认证协议。

第十六、十七讲　复习题

- 密钥管理

①深入理解传统密码体制的密钥管理方案。

②深入理解**PKI** 。

③ 分析**PKI**的优缺点。

综合复习题

●公钥密码学的基本概念

1、掌握以下基本概念：

- 公开密钥密码体制
- 公开加密钥
- 保密解密钥
- 大合数的因子分解问题
- 离散对数问题
- 椭圆曲线
- 椭圆曲线上的离散对数问题
- 单向函数
- 单向陷门函数

综合复习题

2、解释以下基本概念：

① **RSA密码**　椭圆曲线密码　**ELGamal密码**

② 签名　签名的技术条件　数字签名　盲签名

③ 认证　站点认证　报文源认证　报文宿认证

④ 报文顺序认证　报文内容认证　**MAC**

⑤ 密码协议　密码协议安全问题

⑥密钥管理　密钥分配　密钥管理的主要原则

谢　谢！