

密码学

第八讲 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

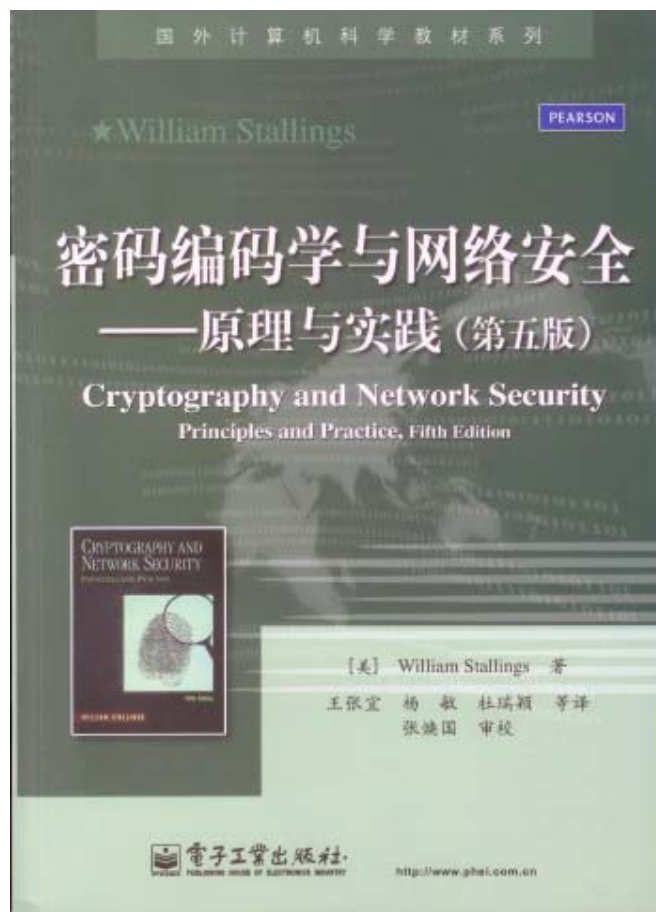


教材与主要参考书

教材



参考书



武汉大学



要求

- ① 同学们书面作业为所有奇数号的题目，要交作业。
- ② 偶数号的题目中的一部分由辅导老师在作业课上讲解，一部分点学生上台解答。
- ③ 期末验收大作业。





第一讲 复习题

- ① 解释信息安全的含义。
- ② 密码的基本思想是什么？
- ③ 密码体制分哪些类型？各有什么优缺点？
- ④ 什么是密码分析？密码分析有哪些类型？
- ⑤ 为什么说理论上，任何实用的密码都是可破的？
- ⑥ 计算机的程序文件和数据库文件加密容易受到什么攻击？为什么？





第二讲 复习题

① 已知置换如下：

$$P = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 4 & 2 \end{bmatrix}$$

明文=642135,密文=?

密文=214365, 明文=?

②使加法密码算法称为对合运算的密钥k称为对合密钥，
以英文为例求出其对合密钥。





第二讲 复习题

③ 已知一个加法密码的密文如下：

**BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHC
QD**

用穷举法求出明文。

④ 以英文为例，用加法密码，取密钥常数 $k=7$ ，对明文
INFORMATION SECURITY，进行加密，求出密文。

⑤ 证明，在置换密码中，置换 p 是对合的，当且仅当对任意的 i 和 j ($i, j=1, 2, 3, \dots, n$)，若 $p(i)=j$ ，则必有 $p(j)=i$ 。

⑥ 编程实现 Vigenre 密码。

⑦ 分析仿射密码的安全性。





第三讲 复习题

大作业

- 以3DES作为加密算法开发出文件加密软件系统：
 - 具有文件加密和解密功能；
 - 具有加解密速度统计功能；
 - 采用密文反馈链接和密文挪用短块处理技术；
 - 具有较好的人机界面。





第三讲 复习题

- ①分析**DES**的弱密钥和半弱密钥。
- ②分析**DES**的互补对称性。
- ③证明**DES**的可逆性。
- ④证明**DES**的对合性。
- ⑤画出3密钥 **3DES**的框图。





第四讲 复习题

大作业

- 以AES作为加密算法开发出文件加密软件系统：
 - 具有文件加密和解密功能；
 - 具有加解密速度统计功能；
 - 采用密文反馈链接和密文挪用短块处理技术；
 - 具有较好的人机界面。





第四讲 复习题

- 1、对比AES和DES有什么不同？
- 2、AES的解密算法与加密算法有什么不同？
- 3、在 $GF(2^8)$ 中，01的逆元素是什么？
- 4、对于字节“00”和“01”计算S盒的输出。
- 5、证明 $c(x)$ 与 $d(x)$ 互逆，模 x^4+1 。
- 6、证明： $x^i \bmod (x^4+1) = x^{i \bmod 4}$





第四讲 复习题

①复习有限域理论。

②证明： $C(x)=03x^3+01x^2+01x+02$

$$D(x)=0Bx^3+0Dx^2+09x+0E$$

互逆。

③利用AES的对数表或反对数表计算ByteSub(25)。

④求出AES的 S盒的逆矩阵。





第五讲 复习题

- ① 计算机数据加密有些什么特殊问题？它对加密的安全性有什么影响？
- ② 分析**ECB**、**CBC**、**CFB**、**OFB**、**X CBC**、**CTR**工作模式的加解密错误传播情况。
- ③ 为什么说填充法不适合计算机文件和数据库加密应用？
- ④ 密文挪用方法有什么优缺点？





第六讲 复习题

- ① 设 $g(x)=x^4 +x^3 +1$ ， $g(x)$ 为本原多项式，以其为连接多项式组成线性移位寄存器。画出逻辑图，写出输出序列及状态变迁。
- ② 令 $n=3$ ， $f(s_0,s_1,s_2)=s_0 \oplus s_2 \oplus 1 \oplus s_1 s_2$ ，以其为连接多项式组成非线性移位寄存器。画出逻辑图，求出非线性移位寄存器的状态变迁及输出。





第六讲 复习题

③令 $n=3$, $f(s_0, s_1, s_2) = 1 \oplus s_0 \oplus s_1 \oplus s_2 \oplus s_0 s_1 \oplus s_1 s_2 \oplus s_2 s_3$, 以其为连接多项式组成非线性移位寄存器。画出逻辑图, 求出非线性移位寄存器的状态变迁及输出。

④证明: $GF(2)$ 上的 n 级移位寄存器共有 2^n 个状态, 因此共有 2^{2^n} 种不同的反馈函数, 其中线性反馈函数只有 2^{n-1} 种, 其余均为非线性。






第七讲 复习题

- 1、分析SMS4在密码结构上与DES和AES有何异同？
- 2、编程研究SMS4的S盒的以下特性：
 - ①输入改变1位，输出平均改变多少位？
 - ②对于一个输入，连续施加S盒变换，变换多少次时出现输出等于输入？
- 3、我国公布商用密码算法有何意义？





第七讲 复习题

大作业

- 以SMS4作为加密算法开发出文件加密软件系统：
 - 具有文件加密和解密功能；
 - 具有加解密速度统计功能；
 - 采用密文反馈链接和密文挪用短块处理技术；
 - 具有较好的人机界面。





谢 谢！



武汉大学