《密码学》课程习题

执笔 张焕国

第一章习题

1、分析信息安全的主要威胁。

2、解释什么是信息系统的设备安全？什么是数据安全？什么是内容安全？什么是行为安全？

3、说明确保信息安全应主要采取哪些措施？

4、为什么说“信息系统的硬件结构安全和操作系统安全是信息系统安全的基础，密码技术和网络安全等技术是关键技术。”？

5、密码的基本思想是什么？

6、上网搜索非数学密码的进展。

第二章习题

1、 解释密码体制的概念。
2、 说明密码体制框图（图 2-1）中攻击者的作用。
3、 说明密码体制的分类，它们各有什么特点？
4、 说明什么是演化密码？它有什么优点？
5、 什么是密码分析？密码分析的方法有哪些类型？它们各有什么特点？
6、 说明什么是“计算上不可破译”？它对我们有什么意义？
7、 为什么说，理论上任何实用的密码都是可破的？
8、 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？
9、 已知置换如下：

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

①设明文 = 642135，求出密文 = ？
②设密文 = 214365，求出明文 = ？

10、 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,…,n)，若 p(i)=j，则必有 p(j)=i 。

11、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。

12、 已知一个加法密码的密文如下：C**SYEVIXIVQMREXIH** 用穷举法求出明文。

13、 编程实现 Vigenre 密码。

14、 分析 Vernam 密码的优缺点。

15、 什么是“一次一密” 密码？为什么它是不实用的?

16、 什么是对合运算？举出 3 种对合运算。

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

18、 分析加法、乘法和仿射密码的安全性。

19、 设明文数据块包含 1024 位，设计一个方案将 64 位的密钥扩展为 1024 位，将明文与扩展密钥进行异或运算，类似一次一密。试问这个密码是否与“一次一密”一样安全？为什么?

20、 从 SuperBase 密码被破译，能给我们什么启示?

第三章习题

1、 说明在 DES 中 S 盒的安全作用。

2、 说明在 DES 中 P 置换的安全作用。

3、 证明 DES 的可逆性和对合性。

4、 分析 DES 的弱密钥和半弱密钥。

5、 分析 DES 的互补对称性。

6、 画出 2DES 的框图，试分析其安全性（提示：考虑中间相遇攻击） 。

7、 画出 3 密钥 3DES 的框图。

8、 大作业：以 3DES 作为加密算法开发出文件加密软件系统，软件要求如下：

①具有文件加密和解密功能；

②具有加解密速度统计功能；

③采用密文反馈链接和密文挪用短块处理技术；

④具有较好的人机界面。

9、 分析 SKIPJACK 的弱密钥。

10、 证明：在 SKIPJACK 密码算法中

1 解密轮函数 1 是加密论函数 1 的逆。

2 解密轮函数 2 是加密论函数 2 的逆。

11、 证明 SKIPJACK 的加解密算法是互逆的。

12、 证明 SKIPJACK 密码算法种加密函数 F 与逆加密函数 F^{-1} 是互逆的。

13、 编程实现 SKIPJACK 的加解密算法。

14、 分析 IDEA 的弱密钥。

15、 实现 IDEA 密码 r= a⊙b 运算的伪代码如下（c 为 32 位无符号数，返回结果为（r AND 0xFFFF））：

```
if (a=0) r←(0x10001-b)
    else if (b=0)  r←(0x10001-a)
            else  { c←a·b;
                    r←((c AND 0xFFFF)-(c>>16));
                    if (r<0) r←(0x10001+r)
                   }
endif
```

分析说明其数学原理。

16、 编程实现 IDEA 密码算法。

17、 比较 AES 和 DES，说明它们各有什么特点？

18、 AES 的解密算法与加密算法有什么不同？

19、 在 GF（2^8）中，01 的逆元素是什么？

20、 在 AES 中，对于字节“ 00”和“ 01”计算 S 盒的输出。

21、 证明：模 x^4+1，c(x)与 d(x)互逆。

22、 证明：$x^i \bmod (x^4+1)=x^{i \bmod 4}$ 。

23、 利用 AES 的对数表或反对数表计算 ByteSub(25)。

24、 求出 AES 的 S 盒的逆矩阵。

25、 设 S 是状态，W 是圈密钥：

①证明：InvShiftRow(InvByteSub(S))= InvByteSub(InvShiftRow(S))。

②证明：InvMixColunm(S ⊕ W)= InvMixColunm(S) ⊕ InvMixColunm(W)。

③说明上述结论对 AES 解密算法的设计有何作用。

26、 大作业：以 AES 作为加密算法开发出文件加密软件系统，软件要求如下：

①具有文件加密和解密功能；

②具有加解密速度统计功能；

③采用密文反馈链接和密文挪用短块处理技术；

④具有较好的人机界面。

27、 编程实现 KASUMI 密码算法。

28、 KASUMI 密码算法是对合运算吗？试证明。

29、 大作业：以 SMS4 作为加密算法开发出文件加密软件系统，软件要求如下：

①具有文件加密和解密功能；

②具有加解密速度统计功能；

③采用密文反馈链接和密文挪用短块处理技术；

④具有较好的人机界面。

30、 比较 SMS4 和 AES，说明它们各有什么特点？

31、 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？

32、 分析 ECB、CBC、CFB、OFB、X CBC、CTR 工作模式的加解密错误传播情况。

33、 画出 CFB 模式的加解密框图。

34、 为什么说填充法不适合计算机文件和数据库加密应用？

35、 密文挪用方法有什么优缺点？

第四章习题

1、设 $g(x)=x^4+x^3+1$，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、设 $g(x)=x^4+x^3+x^2+x+1$，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。并分析与习题 1 的输出序列有什么不同？

3、令 n =3，$f(s_0,s_1,s_2)= s_0 \oplus s_2 \oplus 1 \oplus s_1 s_2$，以其为反馈函数构成非线性移位寄存器。求出非线性移位寄存器的状态变迁及输出。

4、令 n =3，$f(s_0,s_1,s_2)=1 \oplus s_0 \oplus s_1 \oplus s_2 \oplus s_0s_1 \oplus s_1 s_2 \oplus s_2 s_3$ ，以其为反馈函数构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。

5、证明：GF（2）上的 n 级移位寄存器有 2^n 个状态，有种 2^{2^n} 不同的反馈函数，其中线性反馈函数只有 2^{n-1} 种，其余均为非线性反馈函数。

6、说明为什么在 A5 算法中每一时刻至少有两个 LSR 移位。

7、用 MCS-51 单片机实现有限状态自动机密码。

8、说明在 RC4 算法中 S 表初始化的作用。

9、令 n=3，仿照 RC4 设计构造一个类似的密码，并手工演算其加解密过程。

10、编程实现 RC4 密码。

第五章习题

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 。

6、 分析反复平方乘算法的计算复杂度。

7、 分析 Montgomery 算法计算模幂速度快的原因。

8、 在利用函数 **Mon**（A，B，R，n）计算 y=ab mod n 的完整过程中，需要按式(5-18)进行预处理。若将式(5-18)的预处理改为 A＝aR , B=b，即只对 A 进行预处理，有什么优点？又有什么缺点？

9、 在 RSA 中使用 e=3 作为加密指数有何优缺点？使用 d=3 作解密指数

的好吗？为什么？

10、 证明 ELGamal 密码的可逆性。

11、 为什么 ELGamal 密码要求参数 K 是一次性的？

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

13、 证明例 5-8 中 P_{12}= (1000，0001)的阶为 11。

14、 取为 p=29,求出椭圆曲线 $y^2=x^3+4x+20$ 的全部解点。

15、 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。

16、 以教材例 5-8 为例，以 G= P_5= (0010，1111)构造椭圆曲线密码，并设 m= (1010) ，分别进行加密和解密。

第六章习题

1. 为什么数字签名能够确保数据真实性？

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 函数在数字签名中的作用。

4. 编程实现 RSA 数字签名方案。

5. 说明在 ELGamal 密码签名中，参数 k 为什么必须是一次性的。

6. 编程实现 ELGamal 数字签名方案。

7. 说明在椭圆曲线密码签名中，参数 k 有无一次性的要求？

8. 编程实现椭圆曲线密码数字签名方案。

9. 说明 DSS 的签名方案与 ELGamal 密码签名方案有何不同？

10. 编程实现 DSS 数字签名方案。

11. 说明不可否认签名与普通签名有何不同？它在软件知识产权保护方面有何作用？

12. 盲签名与普通签名有何不同？举出一个盲签名的实例。

13. 阅读中国数字签名标准（GB15851-1995）。

第七章习题

1. 什么是 Hash 函数？Hash 函数与一般的压缩函数有何区别？

2. 密码学 Hash 函数的安全性要求有哪些？

3. Hash 函数在密码学中有何作用？带密钥的 Hash 函数和不带密钥的 Hash 函数在应用方面有何不同？

4. 为什么 SHA-1 要求进行填充数据，使数据长度=448 mod 512？

5. 为什么 SHA-512 要求进行填充数据，使数据长度=896 mod 1024？

6. 在 SHA-1 和 SHA-2 的轮函数中使用参数 W_t 和 K_t 有何作用？

7. SHA-1 和 SHA-2 中使用的基本算术和逻辑函数各是什么？

8. 试计算 SHA-512 中 W_{16}，W_{17}，W_{18}，W_{19} 的值。

9. 编程实现 SHA-1 和 SHA-2 算法。

10. 举例介绍 Hash 函数的实际应用。

第八章习题

1. 什么是协议？协议的安全设计原则主要有哪些？

2. 什么是认证？认证与数字签名的区别是什么？

3. 身份认证的途径有哪些？各有什么优缺点？

4. 使用对称密码设计一个安全的双向认证协议。

5. 使用公钥密码设计一个安全的双向认证协议。

6. 根据式（8-4），消息认证码 MAC=C（M，K）。说明密钥 K 在其中起什么作用？

7. 构造消息认证码（MAC）的方法有哪些？

8. 在报文认证中加入序号的作用是什么？

9. 给出一个完整的报文认证方案。

10. Kerberos 系统中的票据有什么作用？

11. 分析 Kerberos 系统的优缺点。

12. 在下述站点认证协议中函数 f 起什么作用？去掉 f 行不行？为什么？

设 A，B 是两个站点，A 是发方，B 是收方。它们共享会话密钥 K_s，f 是公开的简单函数。A 认证 B 是否是他的意定通信站点的协议如下：

1 A 产生一个随机数 RN，并用 K_s 对其进行加密：C＝E（RN，K_s），并发 C 给 B。同时 A 对 RN 进行 f 变换，得到 f(RN)。

2 B 收到 C 后，解密得到 RN＝D（C，K_s）。B 也对 RN 进行 f 变换，得到 f（RN），并将其加密成 C’＝E（f（RN），K_s），然后发 C’给 A。

3 A 对收到的 C’解密得到 f（RN），并将其与自己在第①步得到的 f（RN）比较。若两者相等，则 A 认为 B 是自己的意定通信站点。

否则A认为B不是自己的意定通信站点。

第九章习题

1、 阐述密钥管理的原则，并说明为什么需要这些原则？

2、 阐述传统密码体制的密钥组织的合理性，能否在这一组织结构中加入或删掉一个层次的密钥？

3、 阐述密钥产生的主要方法。

4、 请举出3种电子真随机源的实例。

5、 软件实现基于AES的ANSI X9.17算法。

6、 对于图9-6的初级密钥的网络分配方案中，如果敌手能够截获RN和发送RN，对该方案会构成威胁吗？为什么？

7、 软件实现图9-6初级密钥的网络分配方案。

8、 对Diffie-Hellman密钥分配方案实施中间人攻击，并说明应如何阻止这种攻击。

9、 证明，高级密钥只能以明文形式存储。

10、 阐述密钥更新的原则。

11、 编写一个能够安全删除磁盘数据的程序。

12、 在图9-8（a）中增加一个新的安全类SC_7，使SC_7是SC_2的直接后继。**KMC**要作哪些工作？

13、 从图9-9（a）中删除安全类SC_2。**KMC**需要作哪些工作？

14、 公钥密码体制的公开密钥存在哪些安全威胁？如何对付这些安全威胁？

15、 什么是PKI？它对公钥密码体制的密钥管理有何作用？

16、 讲述一个自己实际应用PKI的实例。

17、 分析PKI的优缺点。

18、 阐述CPK的原理，并分析CPK的优缺点。