密码编码学与网络安全课后答案

第一章计算机与网络安全的概念

1.什么是OSI安全架构？(p6)

OSI 安全框架是提供安全的一种组织方法，而且因为这个框架是作为国际标准而开发的， 所有计算机和通信商已经在他们的产品和服务上开发了这些安全特性，这些产品和服务与安 全服务是和安全机制的结构化定义相关联的。OSI安全框架主要关注安全攻击、机制和服务。

安全攻击:任何危及信息系统安全的行为

安全机制:用来检测、阻止攻击或从攻击状态恢复到正常状态的过程(或实现该过程的设备)。

安全服务:加强数据处理系统和信息传输的安全性的一种处理过程或通信服务，目的在于利用一种或多种安全机制进行反攻击。

2.被动安全威胁与主动安全威胁有何区别？(书上没找着，参考p6-p7的主动攻击和被动攻击)

被动威胁的本质是窃听或监视数据传输,主动威胁包含数据流的改写和错误数据流的添加。

3.列出并简要定义安全服务的种类。(p8)

①认证:保证通信的实体是它所声明的实体

②访问控制:阻止对资源的非授权使用(即这项服务控制谁能访问资源，在什么条件下可以访问，这些访问的资源可用于做什么)

③数据保密性:保护数据免于非授权泄露

④数据完整性:保证收到的数据的确是授权实体发出的数据(即未修改、插入、删除或重播)

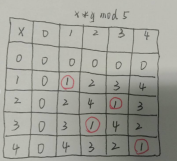
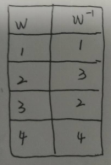
⑤不可否认性:防止整个或部分通信过程中，任一通信实体进行否认的行为。

4.列出并简要定义安全机制的种类。(p10)

①特定安全机制:可以并入适当的安全协议层提供一些OSI安全服务

②普遍的安全机制:不局限与任何特定的OSI安全服务或协议层的机制

第二章数论基础

1. 求Z5中各非0元素的乘法逆元。(p25)

第4章 分组密码和数据加密标准

1.什么是乘积密码(p74)

乘积密码是指依次使用两个或两个以上的基本密码，所得结果的密码强度将强与所有单个密码的强度.

2.混淆和扩散的区别(p75)

扩散(Diffusion):明文的统计结构被扩散消失到密文的,使得明文和密文之间的统计关系尽量复杂.即让每个明文数字尽可能地影响多个密文数字

混淆(confusion):使得密文的统计特性与密钥的取值之间的关系尽量复杂，阻止攻击者发现密钥

3.哪些参数与设计决定了实际的Feistel密码算法？(p75-p77)

①分组长度:分组越长意味着安全性越高，但是会降低加/解密的速度。

②密钥长度:密钥越长意味着安全性越高，但是会降低加/解密的速度。

③迭代轮数:Feistel密码的本质在于单轮不能提供足够的安全性，而多轮加密可- 取的很高的安全性。

④子密钥产生算法:子密钥产生越复杂，密码分析就越困难。

⑤轮函数:轮函数越复杂，抗攻击能力就越强

⑥快速软件加/解密:加密算法被嵌入到应用程序中，以避免硬件实现的麻烦，因此，算法执行的速度很重要。

⑦简化分析难度:如果算法描述起来简洁清楚，那么分析其脆弱性也就容易一些，因而可以开发出更强的算法。

第六章高级加密标准

3. 对如下所述的DES中的元素，指出AES中与之相对应的元素，或解释AES中为什么不需要该元素：

①f函数的输入与子密钥相异或；

轮密匙加

②f函数的输出与分组最左的部分相异或；

不需要，∵每轮都使用代替和混淆将整个数据细分为一个单一的矩阵处理

③f函数

字节代替、行移位、列混淆、轮密匙加

④置换P;

行移位

⑤交换分组长度相等的两部分

不需要，∵每轮都使用代替和混淆将整个数据细分为一个单一的矩阵处理

第七章

第7章 分组加密的工作方式

1.什么是中间相遇攻击？(p137)

是密码学上以空间换取时间的一种攻击。中途相遇攻击(meet-in-the-middle attack)可成倍减少解密已被多个密钥加密的文本所进行的蛮力排列操作。这种攻击可以使入侵者更容易获取数据。

2.在三重加密中一个用到了几个密匙(p138)

2个

3.为什么3DES的中间部分采用了解密而不是加密？(p138)

第二步采用解密运算并没有什么密码学上的含义，这仅仅是为了使用三重DES的用户可以利用该算法解密单DES加密的数据。

4. DES的ECB模式和CBC模式

在DES的ECB模式中，若在密文的传输过程中，某一块发生错误则只有相应的明文分组会有影响。然而，在CBC模式中，这种错误具有扩散性。比如，图7.4中传输C1时发生的错误将会影响明文分组P1,P2

a.P2以后的所有块是否会受到影响

b.假设P1本来就有一位发生了错误。则这个错误要扩散至多少个密文分组？对接收者解密后的结果有什么影响

参考答案

a.不会受到影响

b.会在加密过程中传递到每一个密文分组。对接收者解密后，P1与加密前一样有一位的错误，而对其他Ci能够解密得到无错误的密文。

1. DES的CBC模式和CFB模式

安全性，密文分组是否会泄露关于明文分组的信息等

6. 在8位的cfb模式中，若传输中一个密文字符发生了一位错，这个错误将传播多远

参考答案

9个明文字符受到影响，因为除了与密文字符和对应的一个明文字符受影响外，受影响的该明文字符进入移位寄存器，直到接下来的8个字符处理完毕后才移出。

第8章 伪随机数的产生和流密码

1.伪随机数发生器

a.下述的伪随机数发生器可获得的最大周期是多少？

Xn + 1 = ( a ∗ Xn ) m o d 24

参考答案：最大周期为4

b.这时a为多少？

参考答案：3、5、11、13

c.对种子有什么要求？

参考答案：种子必须为奇数，即X0=1,3,5,7,9,11,13,15

第9章 公钥密码学与RSA

1.什么是单向函数？(p198-p199)

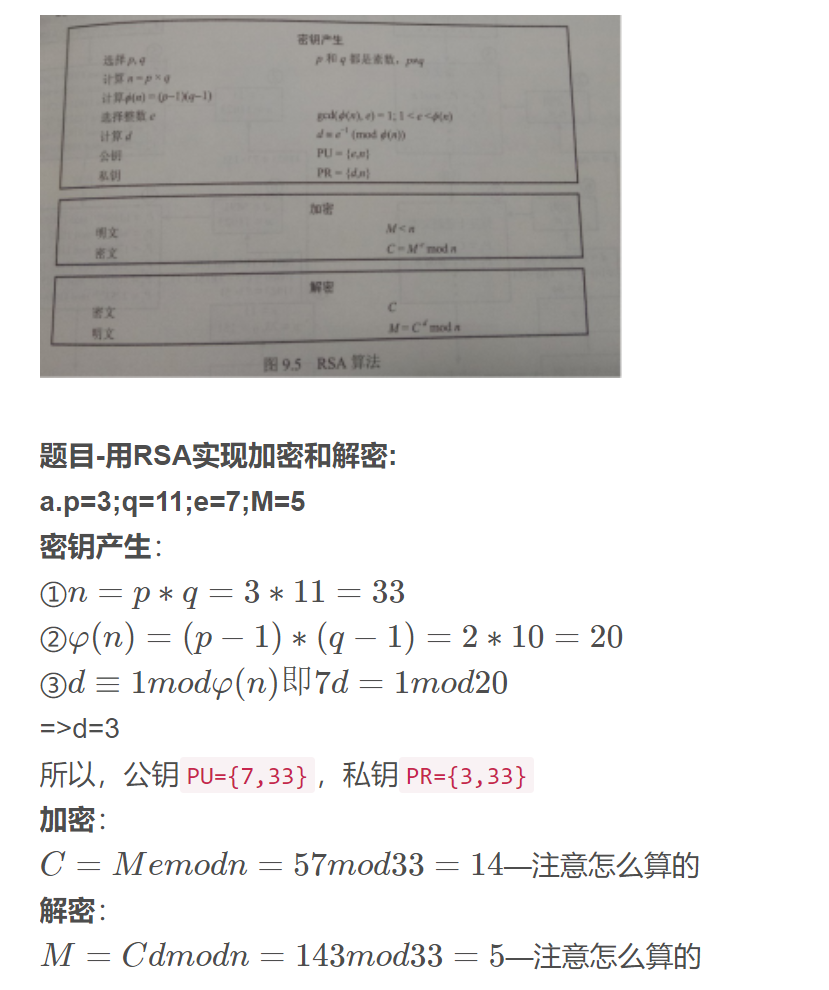
课本上自己画

2.什么是单向陷门函数？(p199)

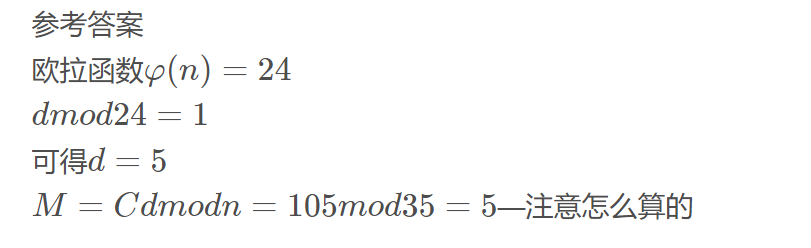
课本上自己画

3.RSA秘钥生成及加密解密的计算

涉及知识(打印版看不清可以看课本p201)

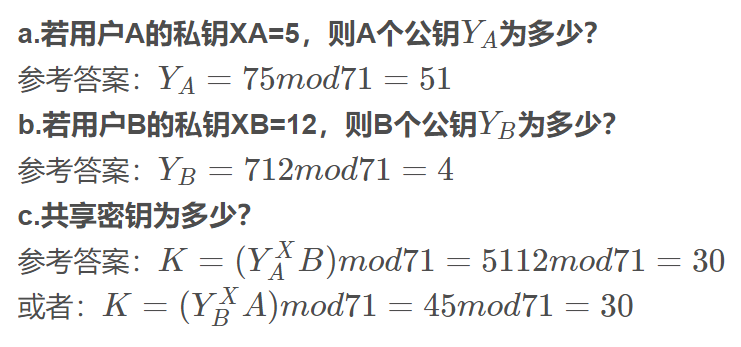


1. 在使用RSA的公钥体制中，已截获发给用户的密文C=10，该用户的公钥e=5,n=35，那么明文M是多少

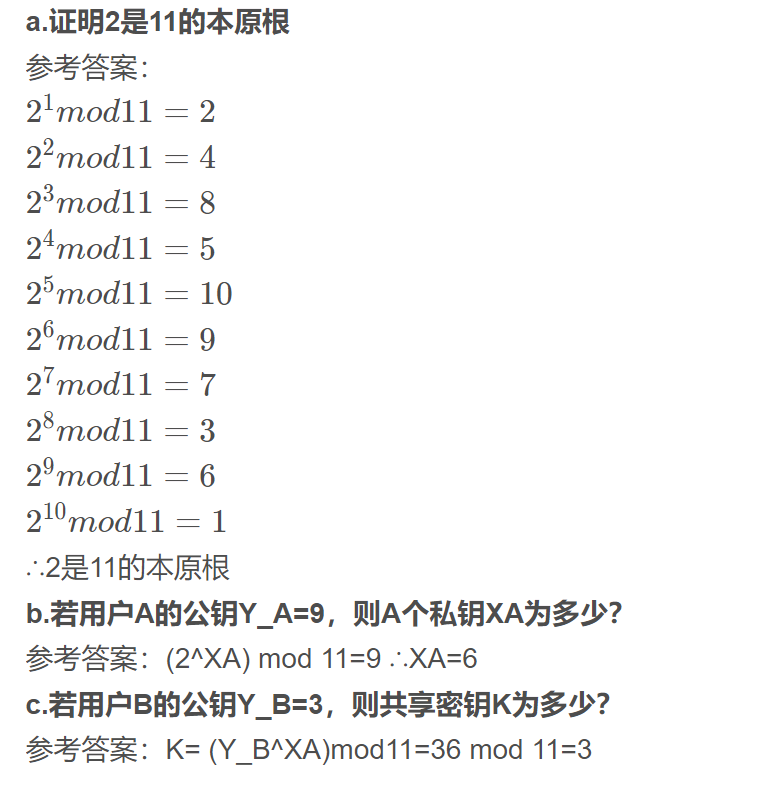


第10章 密钥管理和其他公钥密码体制

1.用户A和B在使用Diffie-Hellman密匙交换技术来交换密匙，设公钥的素数q=71，本原根α=7



1. 设Diffie-Hellman方法中，公钥素数q=11，本原根α=2。



第11章 密码学Hash函数

1.安全Hash函数需要具有哪些特征？(p240)

①输入长度可变

②输出长度固定

③效率

④抗原像攻击(单向性)

⑤抗第二原像攻击(抗弱碰撞性)

⑥抗碰撞攻击(抗强碰撞性)

⑦伪随机性

2.抗弱碰撞性和抗强碰撞之间的区别是什么？(p240)

见课本

3.Hash函数的压缩函数的作用是什么？

压缩函数将一个较长的、固定长度的输入处理后返回一个较短的、固定长度的输出。

第12章 消息认证码

1.消息认证是为了对付哪些类型的攻击？(p264-p265)

①伪装

②内容修改

③顺序修改

④计时修改

2.产生消息认证有哪些方法？(p265)

①Hash函数

②消息加密

③消息认证码(MAC)

3.对称加密和错误控制码一起用于消息认证时，这两个函数必须以何种顺序执行？

先错误控制码，后对称加密

4.为提供消息认证，应以何种方式保证Hash值的安全？

a.用对称密码对消息及附加在其后的Hash码加密。

b.用对称密码仅对Hash加密。

c.用公钥密码和发送方的密钥仅对Hash加密。

d.若寄希望保证保密性有希望有数字签名，则先用发送方的密钥对Hash码加密

e.该方法使用Hash函数但不使用加密函数来进行消息认证。

f.如果对整个消息和Hash码加密，则(e)中的方法可提供保密性。

第12章 消息认证码

1.消息认证是为了对付哪些类型的攻击？(p264-p265)

①伪装

②内容修改

③顺序修改

④计时修改

2.产生消息认证有哪些方法？(p265)

①Hash函数

②消息加密

③消息认证码(MAC)

3.对称加密和错误控制码一起用于消息认证时，这两个函数必须以何种顺序执行？

先错误控制码，后对称加密

4.为提供消息认证，应以何种方式保证Hash值的安全？

a.用对称密码对消息及附加在其后的Hash码加密。

b.用对称密码仅对Hash加密。

c.用公钥密码和发送方的密钥仅对Hash加密。

d.若寄希望保证保密性有希望有数字签名，则先用发送方的密钥对Hash码加密

e.该方法使用Hash函数但不使用加密函数来进行消息认证。

f.如果对整个消息和Hash码加密，则(e)中的方法可提供保密性。

第13章 数字签名

1.签名函数和保密函数应以何种顺序作用与消息？为什么？

先执行签名函数，再执行加密函数。这样在发生争执时，第三方可以查看消息及其签名。这种先后次序非常重要，如果先对消息加密，然后再对消息的密文签名，那么第三方必须知道解密密钥才能读取原始消息。

第14章 密钥管理和分发

1.会话密钥和主密钥之间有什么不同？

主密钥是被客户机和服务器用于产生会话密钥的一个密钥。这个主密钥被用于产生客户端读密钥，客户端写密钥，服务器读密钥，服务器写密钥。主密钥能够被作为一个简单密钥块输出。

会话密钥是指：当两个端系统希望通信，他们建立一条逻辑连接。在逻辑连接持续过程中，所以用户数据都使用一个一次性的会话密钥加密。在会话和连接结束时，会话密钥被销。

2.公钥目录的必要要素是什么?

一是目录管理员的私钥安全，二是目录管理员保存的记录安全。

3.X.509标准的用途是什么？(p319)

X.509标准是一个广为接受的方案，用来规范公钥证书的格式。证书在大部分网络安全应用中都有使用，包括IP安全、传输层安全(TLS)和S/MIME。

4.什么是证书链？

数字证书由颁发该证书的签名。多个证书可以绑定到一个信息或交易上形成证书链，证书链中每一个证书都由其前面的数字证书进行鉴别。最高级的必须是受接受者信任的、独立的机构。

第15章 用户认证

1.列出三个常用的防止重放攻击的方法(p332)

①对每一个用于认证交互的消息附上一个序列号。

②时间戳：只有当消息中包含一个时间戳时，A才接收该消息。

③挑战/应答：A想要一个来自B的新消息，首先发给B一个临时交互号，并要求后面从B收到的消息(回复)中包含正确的临时交互号。

2.在网络或者Internet上，和用户认证相关联的三个威胁是什么？

①用户可能通过某种途径进入工作站并假装成其他用户操作工作站。

②用户可以通过变更工作站的网络地址，从该机上发送伪造的请求。

③用户可以静听信息或使用重放攻击，以获得服务或破坏正常操作。

第17章 传输层安全

1.TLS连接和TLS会话的区别是什么？(p381)

书上自己画

2.HTTPS的目的是什么？

在 http 的基础上结合 ssl 来实现网络浏览器和服务器的安全通信。

3.哪些应用程序可以使用SSH？

远程登录工具，文件传输工具等

第20章 IP安全性

1.IPSec提供哪些服务？

①访问控制

②连接完整性

③数据源认证

④拒绝重放包(部分顺序完整性格式)

⑤保密性(加密)

⑥限制流量保密性

2.哪些参数标识SA，哪些参数刻画一个特定SA的本质？

由安全参数索引、IP目的地址、安全协议标识三个参数确定一个SA。由“序列号计数器，序列计数器溢出，反重放窗口，AH信息，ESP信息，此安全关联的生存期，IPSec 协议模式，最大传输单元路径”等参数表示一个特定的SA。

3.指出传输模式和隧道模式的区别

传输模式是对IP数据包的载荷(上层协议)、IPV6报头的扩展部分进行保护和认证；隧道模式是对整个内部IP包、IPV6报头的扩展部分进行保护和认证。

4.什么是重放攻击？

重放攻击就是一个攻击者得到了一个经过认证的包的副本，稍后又将其传送到其希望被传送到的目的的站点的攻击。

5.IPSec中的Oakley密钥确定协议和ISAKMP的作用是什么？

IPSec的密钥管理部分包括密钥的确定和分发。分手动密钥管理和自动密钥管理两种类型。Oakley和ISAKMP就是IPSec的自动密钥管理协议。