第 2 章习题

1. 对于整数39 和63，回答下面问题

(1) 它们是否互素；

(2) 用欧几里德算法求它们的最大公因子；

2．用费马定理求$3^{201} \pmod{11}$

3．计算下面欧拉函数；

$\phi(41)$ 、$\phi(27)$、$\phi(231)$

4． 求7^{803}的后三位数字。（用欧拉定理）

5．已知 a =97， r = 1001，如果 $a \cdot b \equiv 1 \bmod r$

求a的乘法逆元b，写出计算过程。

第三章习题

1． 已知 DES 算法 S-盒代替表如下：

代替函数 S_i	行号	列 号														
	↓	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_2	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

当S_2 盒的输入分别为101011和110100时，写出S_2 盒的输出（要求写出具体过程）

第四章 习题

1． 利用RSA 算法运算，如果p=11，q=13, 公钥e=11, 对明文2 进行加密.求私钥d 及密文。

2． 在使用RSA 的公钥体制中，已截获发给某用户的密文为c=10，该用户的公钥e = 5， n =35，那么明文m 等于多少？为什么能根据公钥可以破解密文？

第五章 习题

3． 为什么需要消息认证？

4． 散列函数和消息认证码有什么区别？各自可以提供什么功能？

5． 简述HMAC算法的过程；

6． 数字签名需要满足哪些条件？写出数字签名的典型使用方案；

第7章 习题

7． 简述Kerberos的基本工作过程。

8． 简述SSL握手的过程。

第8章 习题

9．PKI 的主要组成是什么？它们各自的功能各是什么？

10． 请给出案例，说明基于PKI 的SSL 是如何工作的？

考试说明

考试重点：第二章、第四章、第 5 章、第七章、第八章；

（公钥技术、网络安全协议）

考试类型：开卷。

参考资料：课件+教材+作业

教材：（信息安全原理与技术 郭亚军编著　清华大学出版社 ）

总评成绩=成绩期末试卷*70%+平时成绩（点名+作业5次+实习报告3次）30分

注：要参加考试的学生必须交作业（5次）+实习报告（3次）

考试题型（判断题、选择题、计算题、简答题，综合应用题）

判断题示例

1． 在对称密码体制中有 n 个成员的话，就需要 n(n-1)/2 个密钥。而在公开密钥体制中只需要 2n 个密钥。（　　）

2． 利用欧几里德算法，求乘法逆元算法时，即重复使用带余数除法：每次的余数为除数除上一次的除数，直到余数为 0 时为止。 （　　）

选择题示例

1． 在开始进入一轮 DES 时先要对密钥进行分组、移位。 56 位密钥被分成左右两个部分，每部分为 28 位。根据轮数，这两部分分别循环左移_____。

A．1 位或 2 位　　B．2 位或 3 位

C．3 位或 4 位　　D．4 位或 5 位

2.PGP 加密算法是混合使用_____算法和 IDEA 算法，它能够提供数据加密和数字签名服务，主要用于邮件加密软件。

A．DES　　B．RSA　　C．IDEA　　D．AES

答案

第一章 习题

1． 对于整数39 和63，回答下面问题

(1) 它们是否互素；

解：由于gcd(39,63)=3,所以他们不互素。

(2) 用欧几里德算法求它们的最大公因子；

解：用欧几里德算法的计算过程如下：

63= 1 *39 +24

39= 1* 24 +15

24= 1* 15 +9

15= 1* 9+ 6

9 =1* 6+ 3

6= 2 *3+ 0

所以39和63的最大公因子是3.

2． 用费马定理求3^{201} (mod 11)

由于 gcd(3,11) =1， 3与11互素，

则根据费马定理

$3^{10} \equiv 1 \bmod 11$

$3^{201} = 3^{10} * 3^{10} * 3^{10} * \ldots. *3^{10} *3^{1}$

$3^{201} \bmod 11 \equiv 1*1*1*\ldots.*1*3 \pmod{11}$

$\equiv 3 \pmod{11}$

3． 3．计算下面欧拉函数；

ϕ(41) 、ϕ(27)、ϕ(231)

- (1) $\varphi(41) = 41-1 = 40$
- (2) $\varphi(27) = \varphi(3^3) = 3^{3-1} 3^{2} = 18$
- (3) $\varphi(440) = \varphi(5*8*11) = \varphi(5) * \varphi(8) * \varphi(11)$
- $= 4*10*(2^3-2^2) = 160$

4． 求7^{803}的后三位数字

解： 7^{803}（mod 1000）的结果

ϕ(1000) = 1000(1-1/2)(1-1/5) = 400，

有$7^{803} \equiv (7^{400})^2 7^3 \equiv 343 \pmod{1000}$

5． 求 a=97,m=1001 ,求a在模 1001 时的乘法逆元。

1001=97*10+31

97=31*3+4

31=4*7+3

4=3*1+1

3=3*1+0

gcd(97,1001)=1

- 逐项回代

1 =4-3*1

=4-(31-4*7) 回代

=4*8-31

- =(97-31*3)*8-31 回代
- =97*8-31*25

- =97*8-(1001-97*10)*25　　回代
- =97*258+1001*(-25)
- 则 258 是97 在模1001下的乘法逆元。

三．S_2盒的输入为101011时，a1a6=$(11)_2$=3，a2a3a4a5=7, S2盒的输出=2=$(0010)_2$
S_2盒的输入为110100时，a1a6=2，a2a3a4a5=10, S2盒的输出=12=$(1100)_2$

四．

1. (1)n=p*q=11*13=143;
   $\phi(n)=(p-1)(q-1)=10*12=120$
   $e*d \equiv 1 \bmod \phi(n)$
   $11*d \equiv 1 \bmod \phi(n)$
   求出11在模120 时的乘法逆元 d=11 ，所以私钥为11；
   （2）求密文 $c= m^e \bmod n=2^{11} \bmod 143=2048 \bmod 143=46$

2． n=p*q (p 和q 都是素数)，n=35 故解出p=5 ，q=7 ；
$\phi(n)$=（p-1）*(q-1)=24 ；
又因为$e*d \equiv 1 \bmod \phi(n)$，而e=5 故可解出d=5；
$m= c^d \bmod n=10^5 \bmod 35=5$ 。

因为RSA 密码体制的安全性是基于分解大整数的困难性设计的。
RSA 算法的加密函数
$c= m^e \bmod n$ 是一个单项函数，故对于解密密文的陷门是分解n=p*q ，只要知道这个分解就可以计算$\phi(n)$=（p-1）*(q-1) ，然后用扩展欧几里德算法来求计算解密私钥d。

五． 1。为什么需要消息认证？
答：网络安全的威胁来自于两个方面：一是被动攻击，攻击者只是通过侦听和截取等手段被动的获取数据，并不对数据进行修改；一是主动攻击，攻击者通过伪造、重放、篡改、改变顺序等手段改变数据。对于这些应用中，仅提供保密性是远远不够的。认证则是防止主动攻击的重要技术。认证的目的主要有两个：第一，验证消息的发送者是合法的，不是冒充的，这称为实体认证，包括对信源、信宿等的认证和识别；第二，验证信息本身的完整性，这称为消息认证，验证数据在传送或存储过程中没有被篡改、重放或延迟等。
4． 散列函数和消息认证码有什么区别？各自可以提供什么功能？
答：消息认证码和散列函数都属于认证函数。简单来说，消息认证码是一种使用密钥的认证技术，它利用密钥来生成一个固定长度的短数据块，并将该数据块附加在消息之后。而散列函数是将任意长的消息映射为定长的hash值的函数，以该hash值作为认证符。散列函数也称为消息的“指纹”。但是散列函数用于认证时，通常和数字签名结合使用。
它们都可以提供消息认证，认证内容包括：消息的源和宿；消息内容是否曾受到偶然的或有意的篡改；消息的序号和时间栏。
5． 简述HMAC算法的过程(以分组为512位为例)；
（1）在密钥K的后面填充0，得到512位的K+
（2）K+和ipad进行异或运算产生512位的分组Si,ipad 为00110110 重复64次，共为512

（64*8）位；
（3）将M附于si后面；
（4）将散列函数H作用于步骤3所得的结果，得到散列值；
（5）K+和opad执行异或运算产生512位的分组S0，opad 为01011100 重复64次，共为512（64*8）位；
(6) 将步骤4的散列值附在S0 的后面。
（7）将散列函数作用于第（6）步的结果，得到最终的结果为消息鉴别码。

6． 数字签名需要满足哪些条件？写出数字签名的典型使用方案；

答：：数字签名需要满足的条件包括：

[1] 签名的结果必须是与被签名的消息相关的二进制位串；
[2] 签名必须使用发送方某些独有的信息（发送者的私钥），以防伪造和否认；
[3] 产生数字签名比较容易；
[4] 识别和验证签名比较容易；
[5] 给定数字签名和被签名的消息，伪造数字签名在计算上是不可行的。
[6] 保存数字签名的拷贝，并由第三方进行仲裁是可行的。

第7章 习题

7． 简述Kerberos的基本工作过程。

Kerberos的基本认证过程描述为：

①用户想要获取访问某一应用服务器的许可证时，先以明文方式向认证服务器AS发出请求，要求获得访问TGS的许可证。

②AS以证书（credential）作为响应，证书包括访问TGS的许可证和用户与TGS间的会话密钥。会话密钥以用户的密钥加密后传输。

③用户解密得到TGS的响应，然后利用TGS的许可证向TGS申请应用服务器的许可证，该申请包括TGS的许可证和一个带有时间戳的认证符（authenticator）。认证符以用户与TGS间的会话密钥加密。

④TGS从许可证中取出会话密钥、解密认证符，验证认证符中时间戳的有效性，从而确定用户的请求是否合法。TGS确认用户的合法性后，生成所要求的应用服务器的许可证，许可证中含有新产生的用户与应用服务器之间的会话密钥。TGS将应用服务器的许可证和会话密钥传回到用户。

⑤用户向应用服务器提交应用服务器的许可证和用户新产生的带时间戳的认证符（认证符以用户与应用服务器之间的会话密钥加密）。

⑥应用服务器从许可证中取出会话密钥、解密认证符，取出时间戳并检验有效性。然后向用户返回一个带时间戳的认证符，该认证符以用户与应用服务器之间的会话密钥进行加密。据此，用户可以验证应用服务器的合法性。

简述SSL握手的过程。

答：SSL握手的详细过程如下：

第一步：客户发出一个带有客户HELLO信息的连接请求。

第二步：服务器评估客户方发来的HELLO信息中的各项参数，并且返回一个服务器方的HELLO信息，其中含有服务器选来用于SSL会话的各项参数。在服务器HELLO信息之后，服务器发出如下信息：①服务器证书，如果服务器需要被鉴别的话。②服务器密钥交换信息，如果得不到证书或证书仅仅用作签名的话。③证书请求，如果客户要求被鉴别的话。然后，服务器发出一个服务器HELLO DONE信息，开始等待客户的回音。

第三步：客户发送下列信息：①如果服务器发出了一个证书请求，那么客户方必须发

送一个证书或非证书信息。②如果服务器发送了一个服务器密钥交换信息，那么客户方就发送一个基于公钥算法的由HELLO信息决定的密钥交换信息。③如果客户方已经发送了一个证书，那么客户方就需验证服务器方的证书并且发出一个证书验证信息指明结果。然后，客户方发出一个结束信息，指出协商过程已经完成。客户方还发送一个修改密文规约信息来产生共享的常规密钥。应该注意这部分工作不是由握手协议控制，是由修改密文规约协议管理的。
第四步：服务器发出一个结束信息指出协商阶段完成。然后服务器发出一个密文修改规约信息。
第五步：会话双方分别产生一个加密密钥，然后他们再根据这些密钥导出会话主密钥。
握手协议改变状态至连接状态。所有从应用层的来的数据传输作为特定信息传输给对方。__
第8章 习题
9．PKI 的主要组成是什么？它们各自的功能各是什么？
：PKI 主要组成部分包括：包括PKI 策略、软硬件系统、认证机构（Certificate Authority，简称CA）、注册机构（Register Authority，简称RA）、证书发布系统和PKI 应用接口等。各自的功能如下：
PKI 安全策略建立和定义了一个信息安全方面的指导方针，同时也定义了密码系统使用的处理方法和原则。
证书机构CA 是PKI 的信任基础，它管理公钥的整个生命周期，其作用包括：发放证书、规定证书的有效期和通过发布证书撤销列表（Certificate Revocation Lists，简称CRL）确保必要时可以撤销证书。
注册机构RA 提供用户和CA 之间的一个接口，它获取并认证用户的身份，向CA 提出证书请求。
证书发布系统负责证书的发放，如可以通过用户自己，或是通过目录服务。目录服务器可以是一个组织中现存的，也可以是PKI 方案中提供的。
PKI 应用接口是提供在PKI 平台之上为所有应用提供一致、可信的使用公钥证书及相关服务的接口。
一个PKI 系统还必须包括相应的证书库存储证书。证书存储库包括LDAP 目录服务器和普通数据库，用于对用户申请、证书、密钥、CRL 和日志等信息进行存储和管理，并提供一定的查询功能。
10． 请给出案例，说明基于PKI 的SSL 是如何工作的？
答：在两个实体进行通信之前，先要建立SSL连接，以此实现对应用层透明的安全通信。利用PKI技术，SSL协议允许在浏览器和服务器之间进行加密通信。此外服务器端和浏览器端通信时双方可以通过数字证书的交互确认对方的身份。基于PKI技术，结合SSL协议和数字证书，则可以保证Web交易多方面的安全需求，使Web上的交易和面对面的交易一样安全。
基于B/S 结构的应用系统，客户端通过HTTP 协议或SSL 协议进入WebServer，使用WebServer 兼做SSLserver。用户使用的证书交给后台的应用服务器进行解析，由应用服务器转向CA 的LDAP 目录进行查询，同时CRL 也在应用服务器中存储和查询，对用户的签名的验证也是在应用服务器中完成。这样的应用适合用户量较少的情况。