现代密码学（第4版）习题参考答案

第1章 引言

1、设仿射变换的加密是：



对明文“THE NATIONAL SECURITY AGENCY”加密，并使用解密变换



验证你的解密结果。

解：①明文m=THE NATIONAL SECURITY AGENCY用数字表示为：

m=[19 7 4 13 0 19 8 14 13 0 11 18 4 2 20 17 8 19 24 0 6 4 13 2 24 ]

根据E11,23(m)≡11\*m+23(mod 26)，对明文中的每一个字符计算出相应的密文字符

c=[24 22 15 10 23 24 7 21 10 23 14 13 15 19 9 2 7 24 1 23 11 15 10 19 1 ]

由此得到密文c=YWPKXYHVKXONPTJCHYBXLPKTB

②使用解密变换验证加密结果过程如下：

由11\*19≡1 (mod 26)知11-1=19

(注：求模逆元可以通过欧几里得算法或者直接穷举1~25)

根据D11,23(c)≡11-1\*(c-23) (mod 26)≡19\*(c-23) (mod 26)，对密文中的每一个字符计算出相应的明文字符

m=[19 7 4 13 0 19 8 14 13 0 11 18 4 2 20 17 8 19 24 0 6 4 13 2 24 ]

由此得到m=THE NATIONAL SECURITY AGENCY，解密结果与明文一致，正确。

2、设由仿射变换对一个明文加密得到的密文为：edsgickxhuklzveqzvkxwkzzukvcuh。又已知明文的前两个字符为“if”，对该明文解密。

解：设加密变换为c=Ea,b(m)≡a\*m+b(mod 26)

由题目可知，明文前两个字符为if，相应密文为ed，即有：

E(i)=e，4≡a\*8+b(mod 26) ，(i=8，e=4)，

E(f)=d，3≡a\*5+b(mod 26) ，(f=5，d=3)，

由上述两式可求得，a=9，b=10

因此解密变换为D9,10(c)≡9-1\*(c-10) (mod 26)

又由3\*9≡1 (mod 26)可知9-1=3

密文对应的数字表示为：

c=[4 3 18 6 8 2 10 23 7 20 10 11 25 21 4 16 25 21 10 23 22 10 25 20 10 21 2 20 7 ]

根据D9,10(c)≡9-1\*(c-10) (mod 26)≡3\*(c-10) (mod 26)，对密文中的每一个字符计算出相应的明文字符

c=[8 5 24 14 20 2 0 13 17 4 0 3 19 7 8 18 19 7 0 13 10 0 19 4 0 7 2 4 17 ]

由此得到明文m=ifyoucanreadthisthankateahcer

1. 设多表代换密码中



加密为：

对明文“PLEASE SEND ME THE BOOK,MY CREDIT CARD NO IS SIX ONE TWO ONE THREE EIGHT SIX ZERO ONE SIX EIGHT FOUR NINE SEVEN ZERO TWO”

用解密变换 

验证你的结果，其中



解：加密时，先将明文分组，每四个一组：



再代入加密变换：，得到计算结果：



知密文为：NQXB BTWB DCJJ IJDT XDCF YFSG

LYGD MOXN LLGN HAPC QZZQ ZCRG

ZEZJ UIEB RRSQ NEMV QDJE MXNA

IERP XAKM YRBY TQFM NEMV OME

同上，解密时，先将密文分组，再代入解密变换：

得到明文：PLEA SESE NDME THEB OOKM YCRE

DITC ARDN OISS IXON ETWO ONET

HREE EIGH TSIX ZERO ONES IXEI

GHTF OURN INES EVEN ZERO TWO

解密验证结果与明文相符。

4、设多表代换密码中，A是2×2矩阵，B是零矩阵，又知明文“dont”被加密为“elni”，求矩阵A。

解：设矩阵

由m=dont=(3,14,13,19)，c=elni=(4,11,13,8)可知:





解得：

第2章 流密码

1. 3级线性反馈移位寄存器在时可有4种线性反馈函数，设其初始状态为，求各线性反馈函数的输出序列及周期。

解：设3级线性反馈特征多项式为，若则共有种可能，对应初态。4种线性反馈函数分别记为：

 输出序列，由定义2-2得周期

 由定义2-3得是不可约多项式，输出序列由定理2-5周期是m序列

 不可约多项式，输出序列，周期 是m序列

 输出序列，得周期

1. 设n级线性反馈移位寄存器的特征多项式为，初始状态为，证明输出序列的周期等于的阶。

解：的阶定义为 的最小的。

因为初始状态不为零，设为序列的最小周期。又因为，所以必存在，使得。

又因为定理2-1有,

则

而的次数为，的次数不超过，的次数不超过。所以，是正整数，都有。

设，，。

即周期为的阶，若是n次不可约多项式，则序列的最小周期等于的阶。

生成函数，，的次数不超过。





不可约，所以，。又因为，所以。

1. 设，，初始状态为，求此非线性反馈移位寄存器的输出序列及周期。

解：由，初态为 。线性递归可得：













可以得到输出序列为，周期为。

4.设密钥流是由级的LFSR产生，其前个比特是,即个01。问第m+3个比特有无可能是1，为什么？

解：第m+3个比特上不可能出现1，这是由于：

根据线性移位寄存器的的递推关系有：



5.设密钥流是由n级LFSR产生，其周期为,是任一整数，在密钥流中考虑以下比特对



问有多少形如的比特对。试证明你的结论。

解：根据p23定理2-7，在上的n长m 序列在周期为的m序列中对于,长为i的游程有个，且0，1游程各半，那么就有：

1的2游程：

1的3游程：

……

1的n-2游程：

那么就有：

 ①

①/2得

 ②

①-②得



从而有

即共有个形如的比特对。

6.已知流密码的密文串1010110110和相应的明文串0100010001，而且还已知密钥流是使用3级线性反馈移位寄存器产生的，试破译该密码系统。

解：由已知可得相应的密钥流序列为1110100111，又因为是3级线性反馈移位寄存器，可得以下方程：

将值代入得: 

 , 



由此可得密钥流的递推关系为：。

7.若GF(2)上的二元加法流密码的密钥生成器是n级线性反馈移位寄存器，产生的密钥是m序列。2.5节已知，敌手若知道一段长为2n的明密文对就可破译密钥流生成器。若敌手仅知道长为2n-2的明密文对，问如何破译密钥流生成器。

解：如果敌手仅仅知道长为2n-2的明密文对，他可以构造出以下的长为2n的明密文对：

不妨设：明文：

密文：

其中：为已知的，为未知的。

为已知的，为未知的。

的可能取值为{00,01,10,11}。的可能取值为{00,01,10,11}。共有16种组合方案，分别破解得到密钥流，在破解的结果中符合m序列的性质密钥流即为正确的方案，有可能不唯一。

8.设J-K触发器中和分别为3级和4级m序列，且，求输出序列及周期。

解：由J-K触发器可知



此时和分别为3级和4级m序列，则的周期为。

。

9.设基本钟控序列生成器中和分别为2级和3级m序列，且，求输出序列及周期。

解：令基本钟控序列生成器中的周期为，的周期为，则输出序列的周期为，，，

。

记LFSR2产生，其状态向量为，可得的变化情况如下：



输出序列

第3章 分组密码体制

1. (1) 设M’和M的逐比特取补，证明在DES中，如果对明文分组和加密密钥都逐比特取补，那么得到的密文也是原密文的逐比特取补，即：

如果Y=DESK(X)，那么Y’=DESK’(X’)

提示：对任意两个长度相等的比特串A和B，证明。

1. 对DES进行穷搜索攻击时，需要在由256个密钥构成的密钥空间进行，能否根据(1)的结论减少进行穷搜索攻击时所用的密钥空间。

（1）证明：

设Li和Ri分别不是第*i*轮DES变换的左右部分，*i*=0,1,…,16, 则加密过程为:



若将明文和密钥*k*同时取补，则加密过程为：



其中，的作用是将数据的左、右半部分扩展后与密钥进行逐比特异或运算，因此，再经过S盒，并将输出结果进行置换运算P之后有：*，*而*，*所以有**。同时有，所以明文*P*与密钥*K*同时取补后有*。*

（2）答：根据(1)的结论进行穷搜索攻击, 可将待搜索的密钥空间减少一半，即255个。因为给定明文*x*，则，由(1)知，则一次搜索就包含了*x*和*x’* 两种明文情况。

2. 证明DES解密变换是加密变换的逆。

证明：

令为左右位置交换函数，,则第*i*次迭代变换为:

,

又∵ 有,

同时，,

即，

∴ ,

DES加密过程在密钥*k*作用下为:

,

解密过程为:

,

所以，，即解密变换是加密变换的逆。（得证）

3.在DES的EBC模式中，如果在密文分组中有一个错误，解密后仅相应的明文分组

受到影响。然而在CBC模式中，将有错误传播。例如在图3-11中*C1*中的一个错误明显地将影响*P1*和*P2*的结果。

(1) *P2*后的分组是否受到影响？

(2) 设加密前的明文分组*P1*中有一个比特的错误，问这一错误将在多少个密文分组中传播？对接收者产生什么影响？

答：

（1）在CBC模式中，若密文分组中有一个错误*C1*，则解密时明文分组中都将受到影响，而后的分组都不受影响，即CBC的错误传播长度为2，具有自恢复能力。

（2）若明文分组P1有错误，则以后的密文分组都将出现错误，但对接收者来说，经过解密后，除P1有错误外，其余的明文分组都能正确恢复。

4. 在8比特CFB模式中，如果在密文字符中出现1比特的错误，问该错误能传播多远？

答：

在8比特CFB模式中，若密文有1比特错误，则会影响当前分组以及后续分组的解密，会使解密输出连续9组出错，即错误传播的长度为9。

5. 在实现IDEA时，最困难得部分是模乘法运算。以下关系给出了实现模乘法的一种有效方法，其中a和b是两个n比特的非0整数：

(1) 证明存在唯一的非负整数q和r使得；

(2) 求q和r的上下界；

(3) 证明;

(4) 求关于q的表达式；

(5) 求关于q和r的表达式；

(6) 用(4)和(5)的结果求r的表达式，说明r的含义。

(1) 证明：

假设存在使得，有 因为，所以，

因此，只能有。

（2）解：，

显然，a和b的最大值均为，则有

所以，

(3)证明：

(4)解：根据，得



(5)解：根据，得



1. 解：当****时，根据及得，

，

同理，当 时，



余数r表示ab的n个最低有效位与ab右移位数n之差。

6. (1) 在IDEA的模乘运算中，为什么将模乘取为而不是？

(2) 在IDEA的模加运算中，为什么将模乘取为而不是？

答：

(1) 在IDEA模乘运算中，必须保证运算构成一个群，因此模数必须为素数，故不能取216。

(2) 同一群内的分配律和结合律都成立，但IDEA算法中要保证模数的加法和模数的乘法，比特异或之间分配律和结合律不成立，因此模加运算不能和模乘运算在同一个群内，即不能选模216+1，而216在模加运算中必为一个群.

1. 证明SM4算法满足对合性，即加密过程和解密过程一样，只是密钥使用的顺序相反。

证明：

SM4算法的加密轮函数分为加密函数G和数据交换E。其中G对数据进行加密处理，E进行数据顺序交换。即加密轮函数

其中，

因为，

因此，加密函数G是对合的。

E变换为：

显然，E是对合运算。

综上，加密轮函数是对合的。

根据加密框图，可将SM4的加密过程写为：

根据解密框图，可将SM4的解密过程写为：

比较SM4与SM4-1可知，运算相同，只有密钥的使用顺序不同。

所以，SM4算法是对合的。

第4章 公钥密码

1. 证明以下关系：

(1) ，则；

(2) ，则；

(3) ，，则。

解：(1)设，由题意得，且存在整数，使得

，即，证得。

(2)已知，则存在整数，使得，证得。

(3)已知，则存在整数，使得

，证得。

2. 证明以下关系：

(1) ；

(2) 。

解：(1)设，则存在整数，使得



即。

(2)设，则存在整数，使得



即。

3. 用Fermat定理求。

解：因为是素数，且，则由Fermat定理可得：

；

又根据性质，可得：

。

4. 用推广的Euclid算法求的逆元。

解：运算步骤如下表所示：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 循环次数 | Q | X1 | X2 | X3 | Y1 | Y2 | Y3 |
| 初值 | ~ | 1 | 0 | 119 | 0 | 1 | 67 |
| 1 | 1 | 0 | 1 | 67 | 1 | -1 | 52 |
| 2 | 1 | 1 | -1 | 52 | -1 | 2 | 15 |
| 3 | 3 | -1 | 2 | 15 | 4 | -7 | 7 |
| 4 | 2 | 4 | -7 | 7 | -9 | 16 | 1 |

所以。

5. 求。

解：由Euclid算法，得：



所以。

6. 求解下列同余方程组：

解：根据中国剩余定理求解该同余方程组，记，，则有

，

所以方程组的解为



7. 计算下列Legendre符号：

**(1) ； (2) ； (3) 。**

解：(1)

(2)



(3)



8. 求的所有本原根。

解：因为，所以的所有不同的素因子为，即对每个，只需计算。又因为，所以有8个本原根。

 

满足且的为的本原根，即。

9. 证明当且仅当是素数时，是域。

证明：(1)若是域，则，均为Abel群。显然为Abel群，与*n*是否为素数无关；但若为Abel群，其条件之一必须保证对任意有模乘法逆元，即对任意，有，使得，所以，即，为素数。

(2)若不是素数，则，即至少存在一个，使得，即无模乘法逆元，因此不能保证均为Abel群，即****不是域。

10. 设通信双方使用RSA加密体制，接收方的公开钥是，接收到的密文是，求明文。

解：因为，则，所以

，即明文。

11. 已知的运行时间是，用中国剩余定理改进RSA的解密运算。如果不考虑中国剩余定理的计算代价，证明改进后的解密运算速度是原解密运算速度的4倍。

证明：RSA的两个大素因子的长度近似相等，约为模数的比特长度的一半，即，而在中国剩余定理中，需要对模和模进行模指数运算，这与的运行时间规律相似，所以每一个模指数运算的运行时间仍然是其模长的三次幂，即。

在不考虑中国剩余定理计算代价的情况下，RSA解密运算的总运行时间为两个模指数运算的运行时间之和，即，证得改进后的解密运算速度是原解密运算速度的4倍。

12. 设RSA加密体制的公开钥是

(1) 用重复平方法加密明文，得中间结果为：



若敌手得到以上中间结果就很容易分解，问敌手如何分解。

(2) 求解密密钥。

解：(1)由以上中间结果可得：

。

由，可知分解为。

(2)解密密钥，由扩展的Eucild算法可得。

13. 在ElGamal加密体制中，设素数，本原根，

(1) 如果接收方B的公开钥是，发送方A选择的随机整数，求明文所对应的密文。

(2) 如果A选择另一个随机整数，使得明文加密后的密文是，求。

解：(1)密文，其中：

。

所以明文对应的密文为。

(2)由，穷举法可得。

所以。

14. 设背包密码系统的超递增序列为，乘数，模数，试对good night加密。

解：由，乘数，模数，可得。

明文“good night”的编码为“00111”，“01111”，“01111”，“00100”，“00000”，“01110”，“01001”，“00111”，“01000”，“10100”，则有：



所以明文“good night”相应的密文为。

15. 设背包密码系统的超递增序列为，乘数，模数，试对解密。

解：因为，则。

所以其对应的明文分组为，由课本120页表4-7可得明文为“ADRA”。

16. 已知，都是素数，，其Jacobi符号都是，其中，证明：

(1) 是模的平方剩余，当且仅当都是模的平方剩余或都是模的非平方剩余。

(2) 是模的平方剩余，当且仅当都是模的平方剩余或都是模的非平方剩余。

证明：(1)①必要性：若是模的平方剩余，即存在使得，而，显然必有，所以也同时是模和模的平方剩余，即。

又由题意得，即。所以：

当时，有，即同时是模和模的平方剩余，也同时是模和模的平方剩余，即都是模的平方剩余；

当时，有，即同时是模和模的非平方剩余，也同时是模和模的非平方剩余，即都是模的非平方剩余。

②充分性：若都是模的平方剩余，则也是模和模的平方剩余，即，即同时是模和模的平方剩余，所以是模的平方剩余；

若都是模的非平方剩余，则它们对于模和模至少有一种情况是非平方剩余，不妨设，则有，即也都是模和模的非平方剩余。所以，同理，即同时是模和模的平方剩余，所以是模的平方剩余。

(2)若是模的平方剩余，则同时是模和模的平方剩余，所以，由于勒让德符号的偶数次方肯定为（情况除外），即有，余下证明同(1)。

提示：

****

****

17. 在Rabin密码体制中设：

(1) 确定在模下的4个平方根。

(2) 求明文消息所对应的密文。

(3) 对上述密文，确定可能的4个明文。

解：(1)已知，由中国剩余定理可得到等价方程组：



因为，所以。经组合可得到以下四个方程组：

   

根据中国剩余定理，则有：

第一个方程组的解为；

第二个方程组的解为；

第三个方程组的解为；

第四个方程组的解为。

所以，的四个平方根为。

(2)对应的密文为。

(3)解密即解，由中国剩余定理可得到等价方程组：



因为，所以，经组合可得到以下四个方程组：

   

根据中国剩余定理，则有：

第一个方程组的解为；

第二个方程组的解为；

第三个方程组的解为；

第四个方程组的解为。

所以，四个可能的明文为。

18. 椭圆曲线表示，求其上的所有点。

解：模的平方剩余有。

时，，无解，曲线无与这一相对应的点；

时，，无解，曲线无与这一相对应的点；

时，，无解，曲线无与这一相对应的点；

时，；

时，；

时，；

时，。

所以椭圆曲线上的所有点为：

。

19. 已知点在椭圆曲线上，求和。

解：(1)求。



所以。

(2)易知。



所以。

20. 利用椭圆曲线实现ElGamal密码体制，设椭圆曲线是，生成元，接收方A的秘密钥。

(1) 求A的公开钥。

(2) 发送方B欲发送消息，选择随机数，求密文。

(3) 显示接收方A从密文恢复消息的过程。

解：(1)易知公开钥。

①求。



所以。

②由题19可得，即。



所以。

(2)密文。

①求：。

②求：。



所以。

③求：。



所以。

综上：。

(3)从密文恢复消息的过程如下：



其中：

a)计算

①先计算。



所以。

②计算。



所以。

③计算。



所以。

④计算。



所以。

b)计算。



所以。

第5章 密钥分配与密钥管理

1. 在公钥体制中，每一用户U都有自己的公开钥和秘密钥。如果任意两个用户A,B按以下方式通信，A发给B消息，B收到后，自动向A返回消息，以使A知道B确实收到报文m，

（1）问用户C怎样通过攻击手段获取报文m？

解：当A发给B消息时，A的身份“A”并没有认证，而B在收到消息后也无法对发送者进行检验，且身份A，B均明文传输，因此用户C可通过如下手段获得报文m：

当A发给B消息时，C截取该消息并将身份A替换为自己的身份C，将修改后的消息发给接收者B；

B提取消息后，根据身份“C”将返回消息；

C再次劫取B返回的消息，用自己的私钥解密出消息m，并用A的公钥对m加密后将消息发给A。

这样，用户C获得了报文m而没有影响A,B之间的正常通信，实现了攻击。

（2）若通信格式变为：

A发给B消息

B向A返回消息

这时的安全性如何？分析这时A、B如何相互认证并传递消息m。

解：根据消息格式，先对消息m进行了签名，然后再进行加密，传送的消息具有了保密性和认证性，敌手无法获得报文明文，安全性提高。

A，B之间相互认证传递消息的过程如下：

B收到消息时，先用B自己的私钥解密得到消息，然后根据提取的身份信息A，用A的公钥对消息m的签名的正确性进行验证，如果验证通过，则说明消息确实来自A。反之A用相同的方法可验证确实来自B，从而实现了相互认证。

1. Diffie-Hellman密钥交换协议易受中间人攻击，即攻击者截获通信双方通信的内容后可分别冒充通信双方，以获得通信双方协商的密钥。详细分析攻击者如何实施攻击。

解：虽然Diffie-Hellman密钥交换算法十分巧妙，但由于没有认证功能，存在中间人攻击。当Alice和Bob交换数据时，Trudy 拦截通信信息，并冒充Alice欺骗Bob，冒充Bob欺骗Alice。其过程如下：

（1）Alice选取大的随机数*x*，并计算，Alice将*g、P、X*传送给Bob，但被Trudy拦截；

（2）Trudy冒充Alice选取大的随机数z，并计算，Trudy将Z传送给Bob；

（3）Trudy冒充Bob，再将传送给Alice；

（4）Bob选取大的随机数y，并计算，Bob将Y传送给Alice，但被Trudy拦截。

由（1）、（3）Alice与 Trudy 共享了一个秘密密钥，由（2）、（4）Trudy与Bob共享了一个秘密密钥。

以后在通信过程中，只要Trudy作中间人，Alice和 Bob不会发现通信的异常，但 Trudy可以获取所有通信内容。

1. Diffie-Hellman密钥交换过程中，设大素数p=11，a=2是p的本原根，

（1）用户A的公开钥，求其秘密钥。

解：满足即，所以有=6。

（2）设用户B的公开钥，求A和B的共享密钥K。

解：由Diffie-Hellman协议可知。

1. 线性同余算法，问：

（1）该算法产生的数列的最大周期是多少？

解：由于模因此它没有原根，又由递推式不难得知。因此该算法产生的序列的最大周期为的最大阶*l*，而，但。若l=4，则不难验证，，时，数列周期为4，因此该算法产生数列的最大周期是4。

（2）a的值是多少？

解：a必须满足，所以a在中取值。

周期为4的有，即为a的取值

（3）对种子有何限制？

解：种子必须满足。

1. 在Shamir秘密分割门限方案中，设k=3，n=5，q=17，5个子密钥分别是8、7、10、0、11，从中任选3个，构造插值多项式并求秘密数据s。

解：取，，构造插值多项式





1. 在基于中国剩余定理的秘密分割门限方案中，设，，，，，三个子秘钥分别是6、3、4，求秘密数据s。

解： 由题设可得s应满足

因为，，，，，3个子密钥分别是6，3，4，那么

，

，

，

由， 可得

===48

由，可得

===48

由，可得

=

即秘密数据s为48

第6章 消息认证和哈希函数

1．6.1.3节介绍的数据认证算法是由CBC模式的DES定义的，其中初始向量取为0，试说明使用CFB模式也可获得相同结果。

6.1.3节用CBC模式的DES设计数据认证算法为：



如果改用CFB模式来实现，由于输出为64位，所以必须取，也就是每次移位寄存器左移整个64位。为了达到相同的结果，可取CFB模式中，则有：



比较两式，作为消息认证码，结果相同。



2．有很多哈希函数是由CBC模式的分组加密技术构造的，其中的密钥取为消息分组。例如将消息M分成分组M1, M2,…,MN，H0=初值，迭代关系为(i=1,2,…,N),哈希值取为HN，其中E是分组加密算法。



（1）设E为DES，第3章的习题已证明如果对明文分组和加密密钥都逐比特取补，那么得到的密文也

是原密文的逐比特取补，即如果Y=DESK（X），那么Y’=DESK’（X’）。利用这一结论证明在上述哈希

函数中可对消息进行修改但却保持哈希值不变。

答：敌手主要是通过修改函数的输入值和来构造碰撞。



利用和两个性质可知，若敌手同时对和逐比特取补，则由性质一知也被逐比特求补，由性质二知保持不变，所以也都不受影响，所以有：



（2）若迭代关系，证明仍可对其进行上述攻击。

答：改迭代关系为，则敌手也可同时对和逐比特取补，由性质一知



也被逐比特求补，由性质二知都不受影响，故仍可进行上述攻击。



3．考虑用公钥加密算法构造哈希函数，设算法是RSA，将消息分组后用公开钥加密第一个分组，加密结果与第二个分组异或后，再对其加密，一直进行下去。设一消息被分成两个分组B1和B2，其哈希值为

H(B1, B2)=RSA(RSA(B1)⊕B2)。证明对任一分组C1可选C2，使得H(C1, C2)= H(B1, B2)。证明用这种攻击法，可攻击上述用公钥加密算法构造的哈希函数。

证明：

对任一分组，可构造如下：



，则



设哈希函数的输入消息分组为，则可任取替代，并由上述方法构造替代，可得，攻击成功。



1. 在图6-11中，假定有80个32比特长的字用于存储每一个Wt，因此在处理信息分组前，可预先计算出这80个值。为节省存储空间，考虑有16个字的循环移位寄存器，其初值存储前16个值（即W0，W1，…, W15），设计一个算法计算以后的每一个Wt。。

答：

XOR

CLS1



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| W0 | W1 | W2 | W3 | W4 | W5 | W6 | W7 | W8 | W9 | W10 | W11 | W12 | W13 | W14 | W15 |

为消息分组的16个字，初始放在移位寄存器中，如上图连接电路。的输出反馈到移位寄存器右边的输入端，则每个时钟到来时，移位寄存器从左边输出端移出一个字。



5.对SHA，计算W16，W17，W18，W19

答：

6．设a1a2a3a4是32比特长的字中的4个字节，每一给ai可看作由二进制表示的0~255之间的整数，在大端方式中，该字表示整数a1224+a2216+a328+a4，在小端结构中，该字表示整数a4224+a3216+a228+a1。

（1）MD5使用小端结构，因消息的摘要值不应依赖于算法所用的结构，因此在MD5中为了对以大端

方式存储的两个字X=x1x2x3x4和Y=y1y2y3y4进行模2加法运算，必须要对这两个字进行调整，问如

何进行？

答：由于MD5使用little-endian结构，而X，Y使用的是big-endian存储结构，因此必须把X，Y转换成little-endian格式，设转换成：，，则有



（2）SHA使用大端方式，问如何对以小端结构存储的两个字X和Y进行模2加法运算。

答：由于SHA使用big-endian结构，而X，Y使用的是little-endian存储结构，因此必须把X，Y转换

成big-endian格式，设转换成：，，则有



第7章 数字签名和认证协议

1. 在DSS数字签名标准中，，于是，若取，则。在对消息签名时，选择，计算签名并进行验证。

解：(1)签名过程：为了简化，用代替，则用户对消息的签名为。计算

，

，

。

所以签名。

(2)验证过程：接收方收到的消息为，签名为。计算

，

，

，

。

因为，所以认为签名有效，即验证通过。

2. 在DSA签名算法中，参数泄露会产生什么后果？

解：若攻击者得到了一个有效签名，并且知道了DSA签名算法中的参数，那么在签名方程中只存在一个未知数，即用户的秘密钥，所以攻击者可以求得秘密钥。因此，参数泄漏将导致签名秘密钥的泄漏，攻击者可以伪造任意消息的签名。

第8章 密码协议

1. 假设你知道一个背包问题的解，试设计一个协议，以零知识证明方式证明你的确知道问题的解。

解一：设背包向量为，证明者P知道一个背包容积的解，即，P以零知识证明方式向验证者证明自己掌握秘密的协议如下：

① P随机选取一向量，计算，将发给V。

② V随机选，将发给P；

③ P计算，即时，；时，，将发给V。

注：如果，P展示的解，即；如果，P展示被加密的的解，即。

④ 若，V接受P的证明。

协议的完备性、正确性和安全性

(1) 完备性：如果P和V遵守协议，且P知道的解，则应答使得，V接受P的证明。

(2) 正确性：假冒的证明者E可按以下方式以的概率骗得V接受自己的证明：

① E随机选取一向量和，计算，将发给V。

② V随机选，将发给E；

③ E将发给V。

V的验证方程为。当时，方程成立，V接受E的证明，E欺骗成功。因的概率是，所以E成功的概率是。

另一方面，是E成功的最好概率，否则假定E以大于的概率使V相信自己的证明，那么E知道一个，对这个，他可以正确回答V的两个询问和，意味着E能计算，由此可计算，因此得秘密。

(3) 安全性：根据以上的讨论知，假冒的证明者E欺骗V成功的概率为，这个概率太大了。为减少这个概率，可以将协议重复执行多次，设执行次，则欺骗成功的概率将减少到。

解二：

(1)构造背包问题

先选大素数，， ，是素数，且 也为素数，为的本原根。P随机选取个整数，，…， (不用超递增序列)，计算





┇



式中，，…，为秘密密钥；，，，，…， 为公开。

(2)零知识证明协议

1)P随机选择，计算 ，并将传送给V；

2)V随机选择个二进制比特序列，，…，，并将其传送给P；

3)P计算，，并将其传送给V。

4)V验证，计算

 



比较是否成立，若成立，说明P了解秘密密钥，，…，；反之，P为假冒。

(3)安全性

此类算法的安全威胁主要来自P欺骗V或V假冒P。假如使用的背包和离散对数没有问题，P欺骗V和V假冒P成功的概率都基于 的随机性，若每一个的选取为0或1的概率为，则假冒或欺骗成功的几率为；若该协议重复次，成功的几率为。

1. 在8.1.4节，基于大数分解问题的“多传一”不经意传输协议中为什么要求？设，B选择，且想获得A的秘密，分析B是否能成功获得。

解：

(1) 要求是为了保证同一数在模下的两个平方根有相反的Jacobi符号。

(2) B先计算Jacobi符号和，，将发给A。

接下来A计算4 mod55的平方根，求出4在mod 5时的平方根为2，4在mod11时的平方根为2，可得以下四个方程组：

   

由

第一个方程组的解为；

第二个方程组的解为；

第三个方程组的解为；

第四个方程组的解为；

因，A将42或53发给B。

当A将42发给B时，B由得到的一个因子，从而得到的分解式，从而获得A的秘密。

当A将53发给B时，因,所以B不能计算出的一个因子，没有得到任何新信息，从而不能获得A的秘密。

1. 设是素数，群的元素是群的生成元，当且仅当对每一，存在一整数，使得。

(1) 在中均匀、随机选取一元素，证明，如果不是的生成元，则存在一整数，使得成立的概率至多是。

(2) 给出是的生成元的零知识证明。

(3) 在(2)中的零知识证明中，证明者能否在多项式时间内完成证明，为什么？

解：(1) 因为不是的生成元，记循环群为，显然是的子群，且，设，是一个大于1的正整数，所以。

在中均匀、随机选取一元素，若，则可在上找到一个，使得成立。而的概率至多是，所以成立的概率至多是。

(2) ① V在中任意取一个元素，发送给P。

② P知道，使得。P在中随机取一个元素，计算并发送给V。

1. V随机选，将发给P；
2. P计算并发送给V
3. V验证，若成立，则接受P的证明。
4. P和V重复以上过程次。

(3) 以上的证明可以在多项式时间内完成。因为，是一个有限值，可以在多项式时间内完成。

1. 设是两个未知大素数和的乘积，且其中至少一个是模的二次剩余。又设模的Jacobi符号都为1，考虑下面交互证明系统，其中和作为输入，P为证明者，V为验证者：
2. P随机选择，计算及，将发送给V。
3. V随机选择，将发送给P。
4. P计算，将发送给V。
5. V检查和是否成立，或和是否成立。如果不成立，则拒绝并终止。

以上过程重复次。

1. 证明以上协议证明了中至少有一个是模的二次剩余。
2. 证明以上协议是完备的。

解：

1. 对于给定的,证明者P都能够回答的两个挑战；

故说明都是模的二次剩余或者都是模的二次剩余；

根据数论知识可得：至少有一个是模的二次剩余。

1. 若Prover和Verifier都是诚实的，且(1)是正确的，显然，验证者最终会接受证明者的证明。

第9章 可证明安全

1、解释主义安全的概念，这一概念可用于抵抗如下攻击吗？

1）、被动的多项式时间有界敌手；

2）、被动的多项式时间无界敌手；

3）、主动的多项式时间有界敌手。

答：语义安全：一个安全的加密方案应使敌手通过密文得不到任何信息，即使是1比特的信息。

此概念可用于抵抗被动的多项式时间有界敌手和主动的多项式有界敌手，但不能抵抗被动的多项式无界敌手。

2. Rabin密码体制是IND-CPA安全的吗？是IND-CCA安全的吗？是IND-CCA2安全的吗？

答：Rabin密码体制Rabin密码体制是RSA密码体制的一种修正，假定模数不能被分解，该类体制对于选择明文攻击是计算安全的。因此，Rabin密码体制提供了一个可证明安全的密码体制的例子：假定分解整数问题是整数上不可行的，那么Rabin密码体制是安全的。

**Rabin密码体制：**

1. 密钥生成

设，其中和是素数，且，即这两个素数形式为，计算。

为公钥，为私钥。

1. 加密



其中 是明文分组，是对应的密文分组。

1. 解密

解密也就是求模的平方根，即解，该方程等价于方程组：



由于，所以可以解出每个方程有两个解：



两两组合可得4个同余方程组：

①、

②、

③、

④、

由中国剩余定理可解出每一个方程组的解，共四个，即每一密文对应的明文不唯一。

为有效确定明文一般在中加入某些代表性信息，如：发送者身份号、接受者身份号、时间、日期等

下面证明，当时，两个方程，的平方根都很容易求出。

由得，，即是一个整数。因是模的平方剩余，故

设的根为，即，则



所以和是方程的两个根。

同理，和是方程的两个根。

当时，求解方程与分解是等价的，所以破译Rabin密码体制的困难程度等价于大整数的分解。

所以Rabin密码体制对选择明文攻击是可证明安全的，然而该体制对选择密文攻击是完全不安全的，因谕言机用实际解密算法来代替，就可以攻破密码体制。

所以Rabin密码体制是IND-CPA安全的，但不是IND-CCA安全的，也不是IND-CCA2安全的。

3.计算性Diffie-Hellman问题（Computational Diffie-Hellman,CDH问题）是已知，计算。离散对数问题（Discrete Logarithm问题，DL问题）是已知，计算。证明如下关系：

证明：1）、证明

定义DDH假设: 设是阶为大素数的群，为的生成元。则以下两个分布：

随机四元组。

四元组（称为Diffie-Hellman四元组，简称DH四元组）。

是计算上不可区分的，称为DDH假设。

具体地说，对任一敌手，区分和的优势是可忽略的。

设是构成的集合，是构成的集合

下面构造一个敌手，利用来攻击CDH问题。

设,,

输入四元组,目标是判断还是

，



如果则说明，输出；

否则则说明，终止。

此时选中t的概率是，故获胜的概率是

2）、证明

由CDH问题可知，对任一敌手，在已知情况下，计算的优势是可忽略的。

那么下面构造一个敌手，利用来攻击DL问题。

则已知，目标是计算。

设，且；





如果：，则;

或,则；

否则终止。

此时敌手选中的概率为

又因为计算的优势是，所以获胜的概率为。

4.设是单钥加密方案，将9.2.2节中的加密方案修改如下：

输入公开钥和消息，选择一个随机数，输出密文 。

证明如果RSA问题是困难的，则修改后的加密方案是IND-CPA安全的公钥加密方案。

证明：设GenRSA是RSA加密方案的密钥生成算法，它的输入为，输出为模数（为2个比特素数的乘积），整数满足。又设是一个哈希函数，其中是一个任意的多项式。

加密方案如下：

密钥产生过程：

：

；

，。

加密过程（其中）

:

；

；

输出（，）

解密过程：

:

；

输出。

定理：设是一个随机谕言机，如果与方案GenRSA相关的RSA问题是困难的，则方案是IND-CPA安全的。

即，设存在一个IND-CPA敌手以的优势攻破方案，那么一定存在一个敌手至少以的优势解决RSA问题。

证明：的IND-CPA游戏如下：

:

;

,;

;

;

，其中；

，；





如果，则返回1，否则返回0

敌手的优势定义为安全参数的函数：



下面证明方案可归约到RSA假设。

敌手已知，以（攻击方案）作为子程序，进行以下过程，目标是计算。

1. 选取一个随机串，作为的猜测值，将公钥发给。
2. H询问：建立一个表（初始为空），元素类型，在任何时候都能发出对的询问，做如下应答（设询问为）

* 如果已经在，则以中的应答；
* 如果以应答，将存入表中，并记下。
* 否则随机选择以应答，并将存入表中。

1. 挑战：输出两个挑战的消息和，随机选择，

并令，

将给作为密文。

1. 在执行结束后（在输出其猜测之后），输出第2）步记下的。

设表示事件：在模拟中发出询问，即出现在中。

**断言1**：在以上模拟过程中，的模拟是完备的。

证明 在以上模拟中，的视图与其在真实攻击中的视图是同分布的，这是因为

1) 的询问中的每一个都是用随机值来回答的。而在对的真实攻击中，得到的是的函数值，由于假定是随机谕言机，所以得到的的函数值是均匀的。

2）对来说，为对做一次密加密。由的随机性，对来说是随机的。

所以两种视图不可区分。

断言2：在上述模拟攻击中。

证明：显然有。

又由在真实攻击中的定义，可知的优势大于等于，得在模拟攻击中的优势也为。



=









又知：









所以

即模拟攻击中。

由以上两个断言，在上述模拟过程中以至少的概率出现在。若发生，则在第（2）步可找到满足，即。所以成功的概率与发生的概率相同。

5.Cramer-Shoup密码体制也使用哈希函数，其安全性证明为什么不是随机谕言机模型？

答：首先回顾随机谕言机的定义。在对方案进行安全性分析时，将其中的哈希函数视为随机谕言机。随机谕言机是一个魔盒 ，对用户（包括敌手）来说，魔盒内部的工作原理及状态都是未知的。用户能够与这个魔盒交互，方式是向魔盒输入一个比特串，魔盒输出比特串（对用户来说，是均匀分布的）。这一过程称为用户向随机谕言机询问。由于这种哈希函数工作原理和内部状态是未知的，因此不能用通常的公开哈希函数。在安全性的归约证明中，敌手需要哈希函数值时，只能由敌手为他产生。之所以以这种方式使用哈希函数，是因为要把欲攻击的困难问题嵌入到哈希函数值中。这种安全性称为随机谕言机模型下的。如果不把哈希函数当作随机谕言机，则安全性称为标准模型下的。

而Gramer-Shoup的证明过程无需把困难问题嵌入到哈希函数中，所以它是标准模型下的证明过程。

6.（1）在Paillier方案1中，设，，，在对加密时，取，计算密文，并验证解密过程。

（2）在Paillier方案2中，设，，计算的密文，并验证解密过程。

答：因为在Paillier方案1中，

加密算法为：

解密算法为：

所以当，，，时，其密文为：





解密过程：

解密为：

即

第10章 网络加密与认证

1. 下面是X.509三向认证的最初版本







假定协议不使用时间戳，可在其中将所有时间戳设置为0，则攻击者C如果截获A、B之前执行协议时的消息，就可假冒A和B，以使A(B)相信通信的对方是B(A).请提出一种不使用时间戳的、防中间人欺骗的简单方法。

答：方案如下：







需要交互的用户A和B提前设置一个只有双方知道的口令password。其中的。

当接收方收到发送方的消息之后进行：，若得的值为之前商定好的password值，则说明发送方的可信的。上述过程即是不使用时间戳的、防止中间人欺骗的一种简单方法。

1. 在PGP中，若用户有N个公开钥，则密钥ID至少有两个重复的概率有多大？

解：在PGP中，用公开钥中64个最低有效位表示该密钥的ID，即公开钥的ID是。由于64位已经足够长，所以不同密钥ID重复的概率非常小。

密钥ID 的可能取值共有种，则当用户有N个公开钥时，ID取值共有种，密钥ID至少有两个重复的概率为。

1. 在PGP中，先对消息签名再对签名加密，请详细说明这一顺序为什么优于先加密再对加密结果签名。

答： 将签字与明文消息在一起存储比与密文消息在一起存储会带来很多方便，同时也给第三方对签字的验证带来方便。如果先加密消息再对消息签字，签字将和密文消息放在一起，这不利于存储消息，也不利于第三方验证签字。另外，加密之前需要压缩，对不压缩的消息签字，可便于以后对签字的验证。如果对压缩后的消息签字，则为了以后对签字的验证，需存储压缩后的消息 或在验证签字时对消息重做压缩。并且，zip压缩算法是不确定性的，该算法在不同的实现中会由于在运行速度和压缩率之间产生不同的折中，产生出不同的压缩结果。

1. 在PGP的消息格式中，消息摘要的前两个8比特位组以明文形式传输。

（1）说明这种形式对哈希函数的安全性有多大程度的影响。

答：首先，哈希函数满足如下几个性质（1）输入为任意长度，输出为固定长度，便于计算与实现。（2）哈希函数具有单向性。（3）哈希函数具有抗碰撞性。在PGP中，消息摘要有SHA对签名的时间戳链接上本身后求得的160比特哈希函数输出结果。公开的消息摘要的前两个8比特位数组（哈希结果的前两个8比特位数组内容），对哈希函数的安全性没有影响。

（2）接收方用消息摘要的前两个8比特位组，确定自己在验证发送方的数字签名时是否正确地使用了发送方的公开钥，其可信程度有多大？

答：消息摘要是对签名的时间戳链接上消息本身后求得的160比特函数输出，然后再由发送方使用秘密要进行签名所得。接收方验证签名时，即为使用对应发送方公钥进行签名验证，其可信程度与签名算法的安全性相关，如果使用的签名算法具有不可伪造性，那么这种验证方式就是可信安全的。

1. 在表10-2中，公钥环中的每一项都有一个拥有者可信字段，用以表示这一公钥的属主(即拥有这一公钥的用户)的可信程度。这一字段能否充分表达PGP对这一公钥的信任？如果不能，则如何实现PGP对这一公钥的信任？

解：

PGP是一个网络，每个人在信任链中都作为到另一个人的介绍人。PGP把密钥签名作为一种介绍形式。当某个人签署了一个密钥时，他就成为那个密钥的潜在介绍人。例如，假设Alice签署了Bob的密钥，而Bob签署了Charlie的密钥。

Alice现在就有了一个到Chrlie的证明路径。Alice现在有一种方式知道Charlie的密钥确实是Charlie的，因为上面有Bob的签名，而且Alice知道Bob的密钥确实是Bob的。这是一种在密钥中提供可传递的信任。

这个设计中有一个明显的问题。如果有人作为介绍人，但是并不真正知道他所介绍的人会怎么样呢？例如，如果Bob非常粗心，虽然签署了Doug的密钥，却宣称是Charlie的。不仅Bob认为这处密钥属于Charlie（尽管是Doug但却宣称它属于Charlie），而且因为对受托性没有一种度量，Alice也会相信。

这就是PGP信任网中所发生的。通过信任网（Web of Trust），用户定义了对一个密钥的信任量，作为介绍人。在前面的例子中，Alice给予Bob的密钥尽可能多的信任，而且如果他相信Bob正确地签署了其他人的密钥，他也会相信这个密钥。如果Alice知道Bob对于密钥验证很松懈，他就不会再信任Bob作介绍人了。其结果是，Alice不会再相信Bob为Doug签署的但宣称为Charlie的密钥。

当然，信任网也不是绝对安全。如果有人被欺骗签署了一个错误的密钥，它就会使得其他人错误地相信它。PGP信任网被认为是一个声誉系统，受到尊敬的人给出好的签名，其他人则给出不好的签名。当存在错误的声誉时，系统就可能失效。

综上所述，我们可知，PGP的信任字段并不能充分表达用户对这一公钥的信任。用户要根据证书链以及信誉系统来计算对特定公钥的信任程度。

如果使用用户充分信任的第三方机构或个人为特定公钥签字，可以实现用户对这一公钥的充分信任。