第一章

**1. 什么是主动攻击和被动攻击，各有何特点？**

主动攻击：对信息的篡改和伪造；被动攻击：对传输进行窃听和检测。

特点：被动攻击的目的是获得信息，不对信息做任何改变，如消息内容的流露和流量分析等；主动攻击：主要威胁信息的完整性、可用性和真实性。

**2. 试述网络安全的特征？**

保密性：信息不泄露给非授权用户、实体或过程，或供其利用的特性。

完整性：数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

可用性：可被授权实体访问并按需求使用的特性。即当需要时能否存取所需的信息。例如网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击；

可控性：对信息的传播及内容具有控制能力。

可审查性：出现安全问题时提供依据和手段。

**3. 什么是网络安全？**

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

**4. 简述主动攻击与被动攻击的特点，并列举主动攻击与被动攻击现象。**

被动攻击时系统的操作和状态不会改变，因此被动攻击主要威胁信息的保密性。主动攻击则意在篡改或者伪造信息、也可以是改变系统的操作状态和操作，因此主动攻击威信信息的完整性、可用性和真实性。

**第二章**

**1. 什么是单向函数？什么是单向陷门函数？**

单向函数是一种具有下述特点的单射函数：对于每一个输入，函数值都容易计算，但是给出一个随机输入的函数值，算出原始输入却比较困难。

单向陷门函数是有一个陷门的一类特殊单向函数。单向陷门函数包含两个明显特征：一是单向性，二是存在陷门。

2. 用欧拉定理求 。

**3. 用欧几里德算法求gcd (1997, 57)。**

1997 = 57 \* 35 + 2

57 = 2 \* 28 +1

28 = 1 \* 28 + 0 所以 gcd(1997,57) =1

**4. 用欧几里德算法求gcd(24140, 16762)。**

24140 = 1 \*16762 + 7378

16762 = ７３７８ \* 2 + ２００６

7387 =２００６×３ + １３６０

２００６＝１３６０×１＋６４６

１３６０＝６４６×２＋６８

６４６＝６８×９＋３４

６８＝３４×２＋０

所以ｇｃｄ（２４１４０，１６７６２）＝３４

**5. 用扩展欧几里德算法求1234 mod 4321的乘法逆元。**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Ｑ | Ｘ１ | Ｘ２ | Ｘ３ | ｙ１ | Ｙ２ | Ｙ３ |
| 初始值 |  | １ | ０ | ４３２１ | ０ | １ | １２３４ |
| １ | ３ | ０ | １ | １２３４ | １ | －３ | ６１９ |
| ２ | １ | １ | －３ | ６１９ | －１ | ４ | ６１５ |
| ３ | １ | －１ | ４ | ６１５ | ２ | －７ | ４ |
| ４ | １５３ | ２ | ７ | ４ | －３０７ | １０７５ | ３ |
| ５ | １ | －３０７ | １０７５ | ３ | ３０９ | －１０８２ | １ |

**6. 用扩展欧几里德算法求550 mod 1769的乘法逆元。**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Ｑ | Ｘ１ | Ｘ２ | Ｘ３ | Ｙ１ | Ｙ２ | Ｙ３ |
| 初始值 |  | １ | ０ | １７６９ | ０ | １ | ５５０ |
| １ | ３ | ０ | １ | ５５０ | １ | －３ | １１９ |
| ２ | ４ | １ | －３ | １１９ | －４ | １３ | ７４ |
| ３ | １ | －４ | １３ | ７４ | ５ | －１６ | ４５ |
| ４ | １ | 5 | -16 | 45 | -9 | 29 | 29 |
| ５ | １ | -9 | 29 | 29 | 14 | -45 | 16 |
| ６ | １ | 14 | -45 | 16 | -23 | 74 | 13 |
| ７ | １ | -23 | 74 | 13 | 37 | -119 | 3 |
| ８ | ４ | 37 | -119 | 3 | -171 | 550 | 1 |

550 mod 1769的乘法逆元是550

**7. 用扩展欧几里德算法求1513 mod 1618的乘法逆元。**

**8. 用快速指数模运算方法计算200837 mod 77。**

**9. 用快速指数模运算方法计算319971 mod 77。**

**10. 用快速指数模运算方法计算3037 mod 73。**

|  |  |  |
| --- | --- | --- |
| ａ | ｂ | ｃ |
| ３７ | ３０ | １ |
| ３６ | ３０ | ３０ |
| １８ | ２４ | ３０ |
| ９ | ６５ | ３０ |
| ８ | ６５ | ５２ |
| ４ | ６４ | ５２ |
| ２ | ８ | ５２ |
| １ | ６４ | ５２ |
| ０ | ６４ | ４３ |

**11. 计算下面数的欧拉函数值（写明详细计算步骤）：**

（1） 53 （2）231 （3）108

（１）５３-1=52

（２）＝２×６×１０＝１２０

（３）＝２＊１８＝３６

**12. 用费马定理求3201 (mod 11)。**

由于gcd(3,11)

由费马定理得

３２０１≡３×３２００ｍｏｄ１１≡（３１０ｍｏｄ１１）＊（３１０ｍｏｄ１１）．．．（３１０ｍｏｄ１１）＝３ｍｏｄ１１＝３

13. 利用中国剩余定理求满足下面同余方程的解x。

x≡1(mod 5)，

x≡5(mod 6)，

x≡4(mod 7)，

x≡10(mod 11)

**第三章**

**什么是密码学、密码编码学、密码分析学？**

密码学:密码学是以研究学秘密通信为目的，即对所要传送的信息采取一种秘密保护，以防第三者对信息进行窃取的一门学科。

密码编码学：密码编码学是研究加密原理与方法，是保密的技术和科学，它的目的是掩盖消息内容。

密码分析学：密码分析学则是研究密码破解密文的原理与方法

**一个密码系统的五个组成部分是什么？各自有什么含义？**

1. 密码空间M，表示全体明文的集合
2. 密文空间C，表示全体密文的集合
3. 密钥空间K，表示全体密钥的集合，包括加密密钥和解密密钥
4. 加密算法，表示用铭文到密文的变换
5. 解密算法，表示由密文到明文的变换

**根据密码分析者所知的信息量，可将对密码的攻击分为哪几类？什么是穷举攻击？**

分类：唯密文攻击、已知明文攻击、选择密文攻击、选择文本攻击。

穷举攻击：穷举攻击是指尝试所有的密钥，只有有足够的资源，任何密码体制都可以用穷举攻击将其攻破。

**什么是置换密码？什么是代换密码？**

置换密码：是将明文中的元素重新排列

代换密码：是将明文中的每个元素映射成另外一个元素

**密码分析主要有哪些方式？简述其中任意一种攻击方式的特点。**

方法：线性密码分析和差分密码分析。

线性密码分析是一种统计攻击，它要求以线性近似为基础。通过寻找现代密码算法变换的线性近似来攻击。

已知仿射密码的加密变换*c*= (*3m*+*5*) mod 26，试求：

（1）该密码的密钥空间是多少；

（2）求消息“security”对应的密文。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| s | e | c | u | r | i | t | y |
| 18 | 4 | 3 | 20 | 17 | 8 | 19 | 24 |

s->(18\*3+5)mod26=7

e->（3\*4+5）mod26=17

c->(3\*3+5)mod26=14

u->(3\*20+5)mod26=13

r->(17\*3+5)mod26=4

i->(8\*3+5)mod26=3

t->(19\*3+5)mod26=10

y->（24\*3+5）mod26=25

密文：rotedkz

已知乘法密码的加密变换*c*= *3m* mod 26，试求：

1. 写出它的解密变换。
2. 试对密文VMHHQ进行解密。

**设密钥字是network, 使用维吉尼亚密码加密明文串now we are having a test，求密文。**

密文：AYPSYKHMGCOKOPX

**用维吉尼亚密码加密明文“we are discovered save yourself”，密钥是：deceptive，求密文。**

密文：ZICVTWQGMRZGVTWKVAHCOYOBQH

**用Playfair算法加密明文“Playfair cipher was actually invented by wheatstone”，密钥是：fivestars。**

**设密钥是network，使用Playfair算法加密Playfair cipher，求密文。**

|  |
| --- |
| N E T W O  R K X A B  C D F G H  I/J L M P Q  S U V Y Z |

密文：QMGWGXSCISQGKN  
 **用列置换加密方法，使用密钥network，加密明文“we are discovered save yourself”，求密文。**

密文:ECSRIOWSDUELDRYFAOASRVVE

**使用穷举搜索法，破译如下利用凯撒密码加密的密文：**

**BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD**

**试述对称密码体制的原理和特点。**

对称密码特点是发送方和接收方共享一个密钥，解密算法是加密算法的逆运算。

对称密码的解密算法通常是加密算法的逆运算，加密密钥和解密密钥相同，属于只使用一个密钥的加密体制，加密速度快，但密钥的强度一般不高。它保密强度高但开放性差，要求发送者和接收者在安全通信之前，需要有可靠的密钥信道传递密钥，而此密钥也必须妥善保管。

**试述对称密码算法存在的问题？**

对称密码系统的安全只依赖于密钥的保密，不依赖于加密算法和解密算法的保密。

所以进行安全通信前需要以安全的方式进行密钥交换，它的规模复杂。

适用于封闭系统，其中的用户是彼此相关并相互信任的，所要防范的是系统外攻击。随着开放网络环境的安全问题日益突出，而传统的对称密码遇到很多困难：密钥使用一段时间后需要更换，而密钥传送需要可靠的通道；在通信网络中，若所有用户使用相同密钥，则失去保密意义；若使用不同密钥N个人之间就需要N(N-1)/2个密钥，密钥管理困难。无法满足不相识的人之间私人谈话的保密性要求。对称密钥至少是两人共享，不带有个人的特征，因此不能进行数字签名。

**设计密码算法的两个主要方法混淆与扩散的区别是什么？**

混淆是为了保证密文不会反映出明文的线索，防止密码分析员从密文中找到模式，从而求出相应的明文；扩散是通过扩展明文的行和列来增强明文的冗余度。

1、扩散 (diffusion)：将明文的统计特性散布到密文中去，实现方式是使得明文的每一位影响密文中多位的值，使得每一字母在密文中出现的频率比在明文中出现的频率更接近于相等。其目的是使明文和密文之间的统计关系变得尽可能复杂，使敌手无法得到密钥。

2、混淆 (confusion)：其目的在于使作用于明文的密钥和密文之间的关系复杂化，是明文和密文之间、密文和密钥之间的统计相关特性极小化，从而使统计分析攻击不能奏效。

**设DES密码中的初始密钥是K=（b0,b1,,b63），记DES加密算法中16轮加密过程中所使用的子密钥分别为K1,K2,…,K16。请写出第一个子密钥K1的生成算法。**

1. 将k64位密钥变成k56位
2. 首先经过置换1将其位置打乱
3. 将k56循环左移一位，在经过置换选择2,
4. 挑去48位作为这一轮的子密钥。

试述在DES算法中，如何从56位的密钥计算出48位的子密钥。

^^56位密钥首先经过置换选择1将其位置打乱重拍，并将前28位作为C0，后28位作为C1，接下来经过16轮，产生16个子密钥。每一轮迭代中Ci-1和Di-1循环左移一位或者两位变成Ci和Di，将Ci和Di合在一起的56位，经过置换选择2从中挑出48位作为这一轮的子密钥。

试述使用两个密钥的三重DES的加解密过程。

简述DES的加密过程。

对输入的密钥进行变换

计算16个子密钥，计算方法C[i][28] D[i][28]为对前一个C[i-1][28], D[i-1][28]做循环左移操作。

串联计算出来的C[i][28] D[i][28] 得到56位，然后对它进行如下变换得到48位子密钥K[i][48]

对64bit的明文输入进行换位变换。

加密过程，对R[i][32]进行扩展变换成48位数

将E(R[i][32])与K[i][48]作异或运算，得到48位数，将48位数顺序分成8份，6位一份，B[8][6]

使用S[i]替换B[i][6]。过程如下: 取出B[i][6]的第1位和第6位连成一个2位数m， m就是S[i]中对应的行数(0-3)，取出B[i][6]的第2到第5位连成一个4位数n(0-15)，n就是S[i]中对应的列数，用S[i][m][n]代替B[i][6]。

将从B[i][6]经过S得到的8个4位数连起来得到32位数

把R[i-1][32]的值赋给L[i]，从5开始循环。直到K[16][48]结束。

将最后的L,R合并成64位，然后进行如下转化得到最后的结果。

已知DES算法使用的S2盒如下所示：

|  |  |
| --- | --- |
|  | 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 |
| 0  1  2  3 | 15 1 8 14 6 11 3 4 9 7 2 13 12 0 5 10  3 13 4 7 15 2 8 14 12 0 1 10 6 9 11 5  0 14 7 11 10 4 13 1 5 8 12 6 9 3 2 15  13 8 10 1 3 15 4 2 11 6 7 12 0 5 14 9 |

**当S2 盒的输入分别为111011和110100时， 计算S2 盒的输出。**

5 12

假设DES算法的输入密钥K=（01000011 00101001 10100001 01110010 10110011 01011101 11010110 11111010），使用如下的置换选择1对K进行置换打乱重排，置乱后的信息是多少？并简述生成第一轮子密钥的步骤。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 |
| 1 | 58 | 50 | 42 | 34 | 26 | 18 |
| 10 | 2 | 59 | 51 | 43 | 35 | 27 |
| 19 | 11 | 3 | 60 | 52 | 44 | 36 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 |
| 7 | 62 | 54 | 46 | 38 | 30 | 22 |
| 14 | 6 | 61 | 53 | 45 | 37 | 29 |
| 21 | 13 | 5 | 28 | 20 | 12 | 4 |

对于DES，回答如下问题：

1. 简述DES的基本原理。

其入口参数有三个：key、data、mode。key为加密解密使用的密钥，data为加密

解密的数据，mode为其工作模式。当模式为加密模式时，明文按照64位进行分组，形成明文组，key用于对数据加密，当模式为解密模式时，key用于对数据解密。实际运用中，密钥只用到了64位中的56位，这样才具有高的安全性。

(2) 当DES的一个S盒如下图所示，如果输入为110110，求二进制形式的4位输出。 1000

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 |
| 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 |
| 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
| 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 |

(3) 假设R为（0000 1001 0001 0010 0011 1101 0110 1010），使用如下扩展置换对R进行置换，写出扩展后的48位值（需有详细中间过程，如矩阵形式的中间结果）。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 32 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 30 | 31 | 32 | 1 |

000001 010010 100010 100100 000111 111010 101101 010100

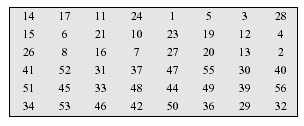
用DES加密，密钥K=（133457799BBCDFF1）16。使用的置换选择1和2分别如下图所示。

K=0001 0011 0011 0100 0101 0111 0111 1001 1001 1011 1011 1100 1101 1111 1111 0001

1111 0011 0011 0010 1010 1011 1111 1101 1111 0111 0101 0101 0101 1001 10

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 |
| 1 | 58 | 50 | 42 | 34 | 26 | 18 |
| 10 | 2 | 59 | 51 | 43 | 35 | 27 |
| 19 | 11 | 3 | 60 | 52 | 44 | 36 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 |
| 7 | 62 | 54 | 46 | 38 | 30 | 22 |
| 14 | 6 | 61 | 53 | 45 | 37 | 29 |
| 21 | 13 | 5 | 28 | 20 | 12 | 4 |

置换选择1



置换选择2

1. **求密钥K经过置换选择1的结果。**
2. **求置换选择2的第一轮输入。**

循环左移一位

**(3) 求经过置换选择2获得的第一个子密钥K1。**

**什么是流密码和分组密码？**

序列密码是一种对明文中的单个位（有时对字节）运算的算法。分组密码是把明文信息

分割成块结构，逐块予以加密和解密。块的长度由算法设计者预先确定。

**简述分组密码和流密码的区别。**

分组密码是针对固定大小的分组进行加密的。当明文的长度超过分组大小时，需要将明文划分成多个分组，采用一定的工作模式来对每个分组进行加密和解密。流密码是对明文以一位或者一个字节为单位进行操作。流密码实现简单、加密速度快、密文传输中的错误不会在明文中扩散。

简述AES的加密过程。

AES的分组长度和密钥长度不相同时，加密过程将迭代不同的轮数，以及使用比轮数多1个的子密钥，如分组长度和密钥长度均为128位时，AES共迭代10轮，需要11个子密钥。每一轮包括4个阶段，分别是：字节代换、行移位、列混淆和轮密钥加，最后一轮只有三个阶段，缺少列混淆。轮密钥加将矩阵中的每一个字节都与该次轮秘钥做XOR运算；每个子密钥由密钥生成方案产生。字节代换通过非线性的替换函数，用[查找表](http://baike.baidu.com/view/1627735.htm" \t "_blank)的方式把每个字节替换成对应的字节。行移位将矩阵中的每个横列进行循环式移位。列混淆使用线性转换来混合每列的四个字节。

分组密码的工作模式主要有哪几种？简述任一种模式的工作原理。

主要有电子密码本模式、密码分组链接模式、密码反馈模式、输出反馈模式以及计数器模式五种。电子密码本模式是将明文分割成独立大小的分组，最后一组在必要时需要填充，每次使用相同的密钥对各个分组进行加密。密码分组链接模式将各个分组链接在一起进行加密操作，加密输入是当前明文分组和前一密文分组的异或，每次加密使用相同的密钥。

简述中国商用密码算法SM4的基本加密过程。

每个分组128位明文分为4个32位的字，经过32轮加密变换，每一轮的加密变换为：循环左移，最后一个字经过轮函数F得到，32轮的加密变换结束后，将4个字反序变化后，得到128位密文。

简述无中心的对称密码密钥分配过程。

两个用户A和B在无中心的情况下建立会话密钥需要经过3个步骤：1、A向B发出建立会话密钥的请求，包括A和B的身份标识和临时交互号N1。2、B用A共享主密钥MK对应答的消息加密，并发送给A。应答的消息中包括选取的会话密钥Ks、B的身份标识、f(N1)和另一个临时交互号N2。3、A使用新建立的会话密钥Ks对f(N2)加密后返回给B。

简述DES和AES中使用S盒的区别。

DES中的S盒是4行16列的矩阵，总共使用了8个S盒，输入为6比特，输出为4比特。代换规则是第一比特和第6比特输入的组合为行号，中间4比特为列号，行列交叉点处的数据即为输出。

AES中的S盒是16\*16的矩阵，固定的8比特输入8比特输出的置换。代换规则是前半个字节为行号，后半个字节为列号，行列交叉点处的数据即为输出。

简述流密码的主要类型并列举典型的流密码算法。

主要有两种类型：同步流密码和自同步流密码。前者密钥流的产生完全独立于明文流或密文流。后者密钥流的产生与明文或者密文相关。典型的流密码算法有：RC4。

简述RC4加密算法的基本原理。

密钥长度可变的面向字节流的加密算法，以随机置换为基础，利用密钥流与明文流异或得密文流。流密钥的生成需要两个处理过程：一个是密钥调度算法(KSA);二是伪随机产生算法(PRGA)。密钥调度算法用来设置数据表S的初始排列，伪随机产生算法用来选取随机元素并修改S的原始排列顺序。

当AES加密的密钥长度为128位，行移位的规则是什么？假设行移位前的状态矩阵State的值为，求行移位后的State的值？

当AES加密的密钥长度为128位，行移位的规则是什么？假设行移位后的状态矩阵State的值为

|  |  |  |  |
| --- | --- | --- | --- |
| D4 | E0 | B8 | 1E |
| 27 | BF | B4 | 41 |
| 11 | 98 | 5D | 52 |
| AE | F1 | E5 | 30 |

求行移位前的State的值。

|  |  |  |  |
| --- | --- | --- | --- |
| D4 | E0 | B8 | 1E |
| BF | B4 | 41 | B4 |
| 5D | 52 | 11 | 98 |
| 30 | AE | F1 | E5 |

利用AES中的倍乘函数分别计算{02}{87}、{03}{6E}。注：。

{02}{87} = x \* {x7 + x2 + x + 1} = x8+x3+x3+x

｛x8+x3+x3+x｝mod m(x) =｛x4+x3+1｝= ｛19｝

AES中使用的S盒如下图所示，问：

1. **简述S盒的代换规则。**

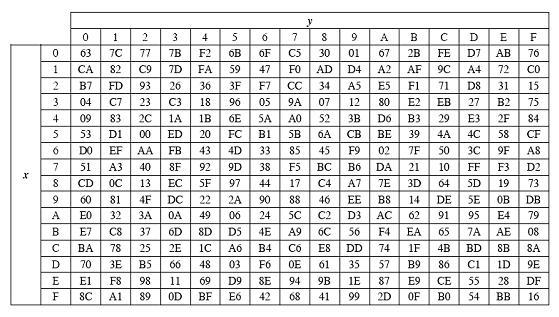
例如十六进制{95}对应的S盒行值是9，列值是5

1. **依次输入十六进制的19、3D时，求对应的十六进制输出结果。**

D4 27

1. **依次输入二进制的1110 0011、1011 1110时，求对应的二进制输出结果。**

11 8B



采用AES加密，密钥为2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C，明文为32 43 F6 A8 88 5A 30 8D 3131 98 A2 E0 37 07 34

(1) 写出最初的State的值

(2) 出密钥扩展数组中的前8个字节

(3) 写出初始轮密钥加后State的值

下图是一个密钥分配协议



请回答下面问题：

1. **该密钥分配协议是针对哪一种密码的分配？**

对称密码体制

1. **密钥分配中心的作用是什么？若密钥分配中心有n个用户，则需要分配的Ks总数是多少？**

密钥分配中心：为用户分配密钥；总数：n

1. **步骤3中，A向B发送的消息是什么？**

加密后的A和B的一次性会话密钥和A的身份标识

1. **详细说明密钥分配过程，在说明过程中需解释清楚各变量的含义。**

IDA、IDB分别是用户A、B的身份标识

Ks分配给A和B的一次性会话密钥

N1时临时会话号，用于防止重放攻击

Es(Ks,IDa)是加密后的一次会话密钥和Ida

1. **步骤4和步骤5的主要目的是什么？**

A和B双方相互认证，确认密钥一定只给对方，防止重放攻击。

下图是一个密钥分配协议，请回答下面问题：



1. **解释步骤2中各变量的含义。**

IDA、IDB分别是用户A、B的身份标识

Ks分配给A和B的一次性会话密钥

N1时临时会话号

Es(Ks,IDa)是加密后的一次会话密钥和Ida

1. **由谁产生的？它的作用是什么？**

密钥分配中心，时A、B建立通信

1. **若密钥分配中心有个用户，则需要分配的的总数是多少？**

n（n-1）/2

1. **步骤1和步骤2的目的是什么？**

给用户分配密钥

1. **步骤3中，A向B发送的消息是什么？目的是什么？**

加密后的A和B的一次性会话密钥和A的身份标识。

1. **步骤4和步骤5的主要目的是什么？**

A和B双方相互认证，确认密钥一定只给对方。

**对于AES算法，回答如下问题：**

**（1）当AES加密的密钥长度为128位，假设行移位前的状态矩阵State的值为，求行移位后的State的值。，**

**（2）行移位后的State矩阵将进行列混淆变换。设行移位后State矩阵的第一列的四个元素，从上到下依次为：*s*0，*s*1，*s*2，*s*3，求*s*0经过列混淆变换的结果，其中变换公式为：，不可约多项式为：。**

**对于AES算法，回答如下问题：**

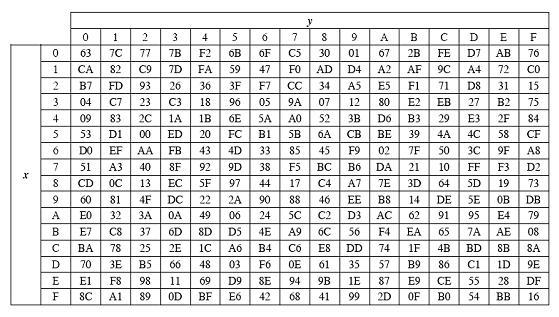
1. **当AES加密的密钥长度为128位，假设行移位前的状态矩阵State的值为，求行移位后的State的值。**

**(2) 行移位后的State矩阵将进行列混淆变换。设行移位后State矩阵的第一列的四个元素，从上到下依次为：*s*0，*s*1，*s*2，*s*3，求*s*2经过列混淆变换的结果，其中变换公式为：，不可约多项式为：。**

S2 = {87}{6E}{02}\*{46}{03}\*{A6}

S2 = {10000111}{01101110}{10001100}{11101001} = {10001100}={8C}

**采用AES加密，密钥为2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C，S盒为：**

****

1. **写出最初的密钥矩阵K0=（W0，W1，W2，W3）的值。**

2B 28 AB 09

7E AE F7 09

15 D2 15 4F

16 A6 88 3C

1. **简述密钥扩展原理。**

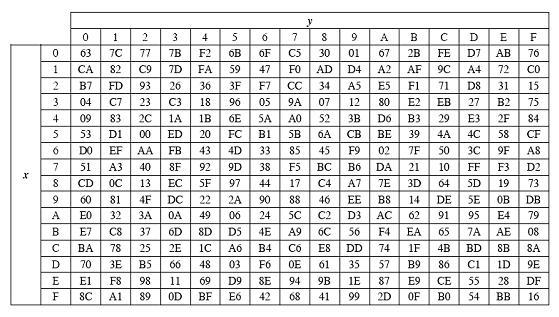
**(3) 求扩展密钥数组的下一个密钥字W4。**

A0FAFE17

**(4) 求扩展密钥数组的后续密钥字W5，W6，W7。**

88542CB1 23A33939 2A6C7605

采用AES加密，明文为32 43 F6 A8 88 5A 30 8D 3131 98 A2 E0 37 07 34，S盒为：



1. 写出最初的明文矩阵State的值。

32 88 31 E0

43 5A 31 37

F6 30 98 07

A8 8D A2 34

1. 若字节代换前State的值为：，写出字节代换后State的值。

D4 E0 B8 1E

1A BF B4 41

11 98 5D 52

AE F1 E5 30

1. 写出行移位后的State的值

D4 E0 B8 1E

BF B4 41 1A

5D 52 11 98

30 AE F1 E5

第4章

简述公钥密码体制的原理和特点。

^^公钥密码体制是使用具有两个密钥的加密和解密算法，加密和解密的密钥是分开的；这两个密钥一个保密，另一个公开。根据应用的需要，发送方可以使用接收方的公开密钥加密消息，或使用发送方的私有密钥签名消息，或两个都使用，以完成某种类型的加密和认证功能。公钥密码算法基于数学函数（如单向陷门函数）而不是基于代换和置换。在这两个独立的密钥中，任何一个都可以用来加密，另一个用来解密。

**解释对称密码体制和公钥密码体制，并阐述这两种密码体制的优缺点。**

对称密钥密码：对称密钥加密又称私钥加密，即信息的发送方和接收方用一个密钥去加密和解密数据。它的最大优势是加/解密速度快， 适合于对大数据量进行加密，但密钥管理困难。

非对称密钥密码：非对称密钥加密又称公钥密钥加密。它需要使用一对密钥 来分别完成加密和解密操作，一个公开发布，即公开密钥，另一 个由用户自己秘密保存，即私用密钥。信息发送者用公开密钥去 加密，而信息接收者则用私用密钥去解密。公钥机制灵活，但加密和解密速度却比对称密钥加密慢得多。

简述对称密码体制与公钥密码体制的异同与优缺点。

**简述利用公钥证书进行公钥分配的基本原理。**

事先由CA对用户的证书签名，证书中包含有与该用户的私钥对应的公钥及用户身份等信息。所有的数据项经CA用自己的私钥签名后就可形成证书

**简述对称密码系统模型的组成和基本过程。与公钥密码体制的主要区别是什么？**

1. 在对称密钥体制中，它的加密密钥和解密密钥的密码体制是相同的，收发方共享密钥（即一个密钥）**，**对称密码的密钥是保密的，没有密钥，解密就不可能。知道算法和若干密文不足以确定密钥。
2. 公钥密码体制中，使用不同的加密密钥和解密密钥，并且加密密钥是公开的，解密密钥是保密的，发送方拥有加密密钥或者解密密钥，而接受方拥有另一个密钥**，**（相对而要，其实接发方都有两个密钥，自己的加密密钥，以及对方分享的解密密钥），两个密钥之一是保密的，无解密密钥，解密不可行。知道算法和其中一个密钥以及若干的秘闻不能确定另一个密钥。

**简述公钥密码体制的公钥加密模型的组成和基本过程。**

**公钥和私钥的作用是什么？**

用公钥加密的内容只能用私钥解密；用私钥加密的内容只能用公钥解密。

在公钥加密模型中，接收方的公钥用来进行加密，私钥用来解密。由于公钥是公开的，每个人都可以用接收方的公钥对信息加密后安全地传输信息，即使数据在途中被截获，由于接收方的私有只在他自己手中，因此，只有接收方能用私钥来将密文解密出明文来。

在公钥认证模型中，发送方的公钥用来进行签名，发送方的私钥用来签名验证。这种方式发送方发送的消息有不可抵赖性。因为加密的私有只有发送方有，其他人的公钥是无法解开密文的。

**如何利用公钥密码技术分配对称密钥？**

A产生一对公私钥PUa和PRa，将公钥PUa和自己的身份标识IDa传给B。B产生一个会话密钥Ks，用A的公钥PUa加密后Epua

**公钥密码一般用于传输对称密钥，现假设A和B之间需要传输数据，因此需要共享一个会话钥，请回答下面问题：**

**(1) 在事前通信发信者A应该得到什么密钥？** B的公钥

**(2) 会话钥的作用是什么？**

会话密钥的作用是将需要传送的数据用会话密钥加密

1. **写出一个密钥分配协议，并分析其安全性。**

书p122

**假设A和B之间需要传输数据，利用如下密钥分配协议分配会话钥，请用文字详细阐述该密钥分配过程并分析其安全性。**

1.A→B:EPUb(IDA||N1),

2.B→A:EPUa(N1||N2),

3.A→B:EPUb(N2+1),

4.B→A:EPUa(EPRb(Ks)),

书P122

阐述使用Diffie-Hellman协议产生一个会话密钥的具体过程。

1)两个通信主体Alice及Bob , 希望在公开信道上建立密钥

2)初始化:

3)选择一个大素数p (200 digits)

4)一个生成元

5)Alice选择一个秘密钥( secret key (number) xA <p )

6) Bob)选择一个秘密钥( secret key (number) xB < p

7)Alice and Bob计算他们的公开密钥: yA = axA mod p yB = axB mod p

8)Alice，Bob 分别公开yA，yB9)计算共享密钥:

10) KAB=axA.xBmodp

i. = yAxB mod p which B can compute)

ii. = yBxA mod p which A can compute)11) KAB可以用于对称加密密钥

**在Diffie-Hellman密钥交换协议中，设本原根，公共素数，其中A选择的秘密数为，B选择的秘密数为，计算A和B双方共同的密钥。**

Ya = aXa mod p = 28 mod 11 =3

K = YaXb mod p = 35 mod 11 = 1

**两个用户A和B使用Diffie-Hellman密钥交换协议来交换密钥，假设公共素数*p=*71，本原根*α=*7。A和B选择的秘密数分别为5和12。求A和B共享的密钥。**

Xa = 5 ; Xb = 12

Ya = 75mod 71 = 51

共享会话钥：K = YaXb mod p = 5112 mod 71 = 30

**RSA算法中，选择，，，求私钥。**

φ（n）=10 \* 6 =60

13 \* d ≡1 mod 60

d = 37

定理1:

设m∈Z+, a, b∈Z, a≠0, gcd(a, m)=1, 则同余式

ax≡b (mod m)恰有一个解x≡ba φ (m)-1 (mod m).

**RSA算法中，选择p=5，q=11，e=7，计算其公钥与私钥，并对十进制的明文m=19进行加密，求密文。**

n = p\*q = 11 \* 5 = 55

φ（n）= 10 \* 4 = 40

公钥（7，40）

7 \* d ≡ 1 mod 40 得：d = 23

**假设需要加密的明文信息为m=85，选择：e=7，p=11，q=13，说明使用RSA算法进行加密和解密的过程，并计算密文。**

n = p\*q = 11\*13 = 143

（用快速模指数）c = me mod n = 123

**对于Diffie-Hellman密钥交换协议，设，，A的秘密信息为，B的秘密信息，回答如下问题：**

1. **该协议存在的主要安全威胁是什么？如何解决？**

容易受到中间人攻击；方法：让A和B分别对消息签名。

1. **利用快速指数模运算方法计算A的公开量。**

Ya = aXa mod p = 215 mod 17 =9

**(3) 计算A和B双方共同的密钥。**

K = YaXb mod p = 913 mod 17 = 8

**在使用RSA的公钥体制中，已截获发给某用户的密文为，该用户的公钥，，回答如下问题：**

**(1) 求私钥。**

n = 35 = 5\*7

φ（n）= 4\*6=24

d\*e≡1 mod (φ（n）) =5-1 mod 24 = 5

私钥{5,5,7}

1. **求明文M的值。**

m = cd mod n = 145 mod 35 = 9

1. **为什么能根据公钥和密文能解密明文**？

那么私钥和明文M等于多少？

S = md mod n

M = se‑ mod n

下图是一个公钥分配方案



请回答下面问题：

**(1) 根据上图描述具有公钥管理机构的公钥分配方案的详细过程，并解释每一个变量的含义。**

**(2) 步骤1和步骤2的主要目的是什么？**

用户A获得B的公钥

**(3) 步骤6和步骤7的主要目的是什么？**

双方相互认证确认身份，建立临时会话

第5章

**Hash函数有哪些功能？什么是MD5？**

Hash函数是将任意长的输入消息作为输入生成一个固定长的输出串的函数，即h=H（M）

**试述散列函数应满足的条件** 。

1. H可以应用于任意长度的数据块，产生固定长度的散列值。
2. 对于每一个给定的输入m，计算H（m）是很容易的。
3. 给定Hash函数的描述，对于给定的散列值h，找到满足H（m）=h的m计算上是不可行的。
4. 给定Hash函数的描述，对于给定的消息m1，找到满足m2≠m1且H（m2）=H(m1)的m2在计算上是不可行的。
5. 找到任何蛮子H（m1）=H(m2)且m2≠m1的消息对（m1,m2）在计算上的不可行的。

**试说明数字签名的典型使用方法。**

DDS方法使用Hash函数产生消息的散列值，和随机生成的K作为签名的输入，签名函数依赖于全局公钥PUc。签名由两部分组成，标记为r和s。

接收方对收到消息计算散列值，和收到的签名（r,s）一起作为验证函数的输入，验证函数依赖于全局公钥和发送方公钥，若验证函数的输出等于签名中的r，则签名合法。

试述数字签名的作用，即能解决哪些安全问题？

**消息认证码的原理是什么？它与散列函数有什么区别？**

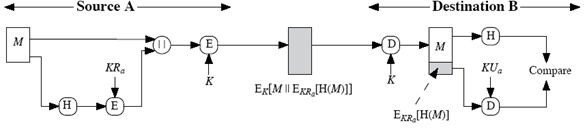
消息认证码和散列函数都属于认证函数。消息认证码是一种使用密钥的认证技术，它利用密钥来生成一个固定长度的短数据块，并将该数据块附加在消息之后。而散列函数是将任意长的消息映射为定长的值的函数，以该值作为认证符。散列函数也称为消息的“指纹”。但是散列函数用于认证时，通常和数字签名结合使用。

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。

**简述数字签名的基本原理。**

数字签名是一种认证机制，是公钥密码算法的典型应用。数字签名包含两个过程：签名过程和验证过程。发送方使用自己的私钥对数据校验和（或）其他与数据内容有关的信息进行加密，完成对数据的合法“签名”，然后将签名信息和原始信息一起发送给接收方。数据接收方则利用发送方的公钥来验证收到的消息上的“数字签名”。若对签名信息解密后获得的信息与接收到的原始信息一致，则签名验证成功，消息确实是发送方所发送，并且消息的内容没有被修改过。否则签名验证不成功。

下图是将Hash函数用于消息认证的一种方法，请回答下面的问题。



**(1) 中各变量及整个公式的含义。**

Eka：A的私钥；M是输入的消息；H（M）：散列值

1. **说明该方法能够同时提供保密性和认证性的原因。**

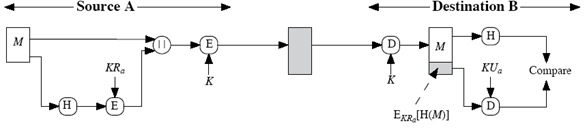
原因：先使用Hash函数得到消息的散列值，再使用发送方法的签名私钥PRa。对代表消息的散列值进行签名。

**(3) 散列函数与消息认证码的相同点和区别是什么？**

消息认证码和散列函数都属于认证函数。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值的函数，以该值作为认证符。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。

下图是将Hash函数用于消息认证的一种方法，请回答下面的问题。



1. **写出图中KRa，H(M)，K和 KUa表示的意思。**

Eka：A的私钥；M是输入的消息；H（M）：散列值，K共享密钥

1. **写出Source A所进行操作的总表达式，并解释其含义和作用。**

Ek（KRa[H（M）]||M），M通过Hash函数得到H（M）之后，再通过A的私钥进行加密。再把加密后的H（M）和M经过共享密钥加密，发送给B，这样可以提供认证行和保密性。

1. **简述B接收到A发送的消息后进行的操作及其作用。**

将消息用K解密之后，将M通过散列函得到H(M); KRa[H（M]同A的公钥解密得到H（M），比较计算出来的H(M)和解密得到的H(M)是否一致，一致则消息没有被篡改。

**(4) 该方法提供了哪些安全服务。**

消息保密、数字签名、消息认证。

综合利用已经学习的密码学技术知识，设计一个具有保密性,同时能够验证消息的完整性以及消息发送方身份的安全通信过程。以Alice和Bob互相通信为例，说明该过程，并简单分析各种密码技术在所设计的通信过程中是如何体现通信安全性的？

第8章

PKI的主要组成是什么？核心部分的功能是什么？

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。

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。

什么是交叉认证？请给出交叉认证的过程。

交叉认证为属于不同 CA域的用户提供一种互相认可对方证书的机制，在原本没有联系 的 CA之间建立信任关系。交叉认证机制保证一个 PKI团体的用户可以验证另一个 PKI团体 的用户证书。它是将这些以前无关的 CA连接在一起的机制，从而使得在它们各自主体群之 间能够进行安全通信。

交叉认证有两个操作：首先在两个域之间建立信任关系，这通常是一次性操作。在双方 交叉认证的情况下，两个 CA 安全地交换他们的验证密钥。这些密钥用于验证他们在证书上 的签名。为了完成这个操作，每个 CA 签发一张包含自己公钥的证书，该证书称为交叉证书。 后续操作由客户端软件完成，这个操作包含了验证已由交叉认证的 CA 签发的用户证书的有 效性，这个操作需要经常执行。该操作被称为跟踪信任链，链指得是交叉证书认证链表，沿 着这个链表可以跟踪所有验证用户证书的 CA 密钥。

如何实现双向的交叉认证证书？

PKI中有哪些常见的信任模型？任选一种模型介绍其特点。

(1)层次模型

(2)分布式信任模型

(3) Web 模型是在环球网(World Wide Web)上诞生的，依赖于流行的浏览器进行构建。在 这种模型中，许多 CA 的公钥被预装在标准的浏览器上。这些公钥确定了一组浏览器用户最 初信任的 CA。尽管这组根密钥可以被用户修改，然而几乎没有普通用户对于 PKI 和安全问 题能精通到可以进行这种修改的程度。Web 模型在方便性和简单互操作性方面有明显的优 势,但是也存在一些安全隐患。

(4)以用户为中心的信任模型

试述CA的主要职责。

验证并标识证书申请者的身份

确保CA用于签名证书的非对称密钥的质量

确保整个认证过程中的安全性，确保签名私钥的安全性

证书资料信息的管理

确定并检查证书的有效期

确保证书主题标识的唯一性，以防重名

发布并维护作废证书列表

对整个证书签发过程做日志记录

向申请人发出通知

数字证书的原理是什么？

数字证书采用公钥体制，即利用一对互相匹配的密钥进行加密、解密。每个用户自己设定一把特定的仅为本人所知的私有密钥（私钥），用它进行解密和签名；同时设定一把公共密钥（公钥）并由本人公开，为一组用户所共享，用于加密和验证签名。当发送一份保密文件时，发送方使用接收方的公钥对数据加密，而接收方则使用自己的私钥解密，这样信息就可以安全无误地到达目的地了。通过数字的手段保证加密过程是一个不可逆过程，即只有用私有密钥才能解密。

试述基于X.509数字证书在PKI中的作用。

1、X.509数字证书是各实体在网络中的身份证明，它证书了实体所声明的身份与其公钥的匹配关系。

2、从公钥管理的机制讲，数字证书是非对称密码体制中密钥管理的媒介。即在非对称密码体制中，公钥的分发、传送是通过数字证书来实现的。

3、通过数字证书，可以提供身份的认证与识别，完整性、保密性和不可否认等安全服务