第一章

1. 什么是主动攻击和被动攻击，各有何特点？

被动攻击的特征是对传输进行窃听和监测。被动攻击的目的是获得传输的信息，不对信息做任何改动，如消息内容的泄露和流量分析等。再受到被动攻击时，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。包括监听数据包、流量分析、对通信线路中传输的信号搭线监听。

主动攻击则旨在篡改或者伪造信息，也可以是改变系统的状态和操作，因此主动攻击主要威胁信息的完整性，可用性，常见的主动攻击包括伪装、篡改、重放和拒绝服务。

1. 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与手段

1. 什么是网络安全？

网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。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。

1. 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。

第二章

1. 什么是单向函数？什么是单向陷门函数？

一个可逆函数f：A→B，若它满足：

1. 对所有的x∈A，易于计算f（x）
2. 对于几乎所有的x∈A，由f（x）求x极为困难，以至于实际上不可能做到，则称f为单项函数

单向陷门函数：

一个“可逆函数F”，满足以下两个条件：

1. 对于所有属于域F中的任何一个x，容易计算F(x)=y
2. 对于几乎所有属于域F中的任一y，除非获得陷门信息，否则求出x，使得x=F-1(y)在计算上不可行，F-1为F逆函数
3. 用欧拉定理求。

因为gcd(5,37)=1;

所以5φ（37）≡1 mod 37

所以536=1 mod 37

因为185=36×5+5

所以5185=(536)5×55≡17 mod 37

1. 用欧几里德算法求gcd (1997, 57)。

1997=35×57+2

57=28×2+1

2=2×1+0

因此gcd (1997, 57)=1

1. 用欧几里德算法求gcd(24140, 16762)。

24140=1×16762+7378

16762=2×7378+2006

7378=3×2006+1360

2006=1×1360+646

1360=2×646+68

646=9×68+34

68=2×34+0

所以gcd(24140, 16762)=34

1. 用扩展欧几里德算法求1234 mod 4321的乘法逆元。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 循环次数 | Q | X1 | X2 | X3 | Y1（T1） | Y2（T2） | Y3（T3） |
| 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 |

所以1234 mod 4321≡-1082≡3239 mod 4321

1. 用扩展欧几里德算法求550 mod 1769的乘法逆元。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 循环次数 | Q | X1 | X2 | X3 | Y1（T1） | Y2（T2） | Y3（T3） |
| 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 |

所以550 mod 1769=550

1. 用扩展欧几里德算法求1513 mod 1618的乘法逆元。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 循环次数 | Q | X1 | X2 | X3 | Y1（T1） | Y2（T2） | Y3（T3） |
| 初始值 | / | 1 | 0 | 1618 | 0 | 1 | 1513 |
| 1 | 1 | 0 | 1 | 1513 | 1 | -1 | 105 |
| 2 | 14 | 1 | -1 | 105 | -14 | 15 | 43 |
| 3 | 2 | -14 | 15 | 43 | 27 | -31 | 19 |
| 4 | 2 | 27 | -27 | 19 | -68 | 77 | 5 |
| 5 | 3 | -68 | 67 | 5 | -93 | -262 | 4 |
| 6 | 1 | -93 | -228 | 4 | -53 | 339 | 1 |

所以1513 mod 1618的乘法逆元是339

1. 用快速指数模运算方法计算200837 mod 77。

|  |  |  |  |
| --- | --- | --- | --- |
| a | b | c | n |
| 37 | 2008 | 1 | 77 |
| 36 | 2008 | 6 |  |
| 18 | 36 | 6 |  |
| 9 | 64 | 6 |  |
| 8 | 64 | 76 |  |
| 4 | 15 | 76 |  |
| 2 | 71 | 76 |  |
| 1 | 36 | 76 |  |
| 0 | 36 | 41 |  |

所以200837 mod 77=41

1. 用快速指数模运算方法计算319971 mod 77。

|  |  |  |  |
| --- | --- | --- | --- |
| a | b | c | n |
| 19971 | 3 | 1 | 77 |
| 19970 | 3 | 3 |  |
| 9985 | 9 | 3 |  |
| 9984 | 9 | 27 |  |
| 4992 | 4 | 27 |  |
| 2496 | 16 | 27 |  |
| 1248 | 25 | 27 |  |
| 624 | 9 | 27 |  |
| 312 | 4 | 27 |  |
| 156 | 16 | 27 |  |
| 78 | 25 | 27 |  |
| 39 | 9 | 27 |  |
| 38 | 9 | 12 |  |
| 19 | 4 | 12 |  |
| 18 | 4 | 48 |  |
| 9 | 16 | 48 |  |
| 8 | 16 | 75 |  |
| 4 | 25 | 75 |  |
| 2 | 9 | 75 |  |
| 1 | 4 | 75 |  |
| 0 | 4 | 69 |  |

1. 用快速指数模运算方法计算3037 mod 73。

|  |  |  |  |
| --- | --- | --- | --- |
| a | b | c | n |
| 37 | 30 | 1 | 73 |
| 36 | 30 | 30 |  |
| 18 | 24 | 30 |  |
| 9 | 65 | 30 |  |
| 8 | 65 | 52 |  |
| 4 | 64 | 52 |  |
| 2 | 8 | 52 |  |
| 1 | 64 | 52 |  |
| 0 | 64 | 43 |  |

1. 计算下面数的欧拉函数值（写明详细计算步骤）：
2. 53 （2）231 （3）108
3. 因为53为素数，

所以φ（53）=53-1=52

1. 因为231不是素数

所以φ（231）=φ（3×77）=φ（3）×φ（7×11）=120

1. 因为108不是素数

所以φ（108）=φ（4×27）=φ（4）×φ（27）=2×（2-1）×(33-33-1)=36

1. 用费马定理求3201 (mod 11)。

因为gcd（3,11）=1

又因为201=10×20+1

所以3201=（310）20×3≡3 mod 11

1. 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)

M=5×6×7×11=2310

M1=6×7×11=462

M2=5×7×11=385

M3=5×6×11=330

M4=5×6×7=210

M1-1 mod 5=3

M2-1 mod 6=1

M3-1 mod 7=1

M4-1 mod 11=1

所以x mod 2310 =（3×462×1+1×5×385+1×4×330+1×10×210）mod 2310≡341

第三章

1. 什么是密码学、密码编码学、密码分析学？

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

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

密码分析学：是研究破解密文的原理与方法。

1. 一个密码系统的五个组成部分是什么？各自有什么含义？

答:明文空间M，表示全体明文的集合；

密文空间C，表示全体密文的集合；

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；

加密算法E，表示由明文到密文的集合；

解密算法D，表示由密文到明文的集合。

1. 对明文M用密钥K，使用加密算法E进行加密，常常表示为Ek（M），同样用密钥K使用解密算法D对密文C进行解密时，表示为Dk（C）。在对称加密体制中，解密密钥相同。有：

C= Ek（M）

M= Dk（C）= Dk（C）= Dk（Ek（M））

1. 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？

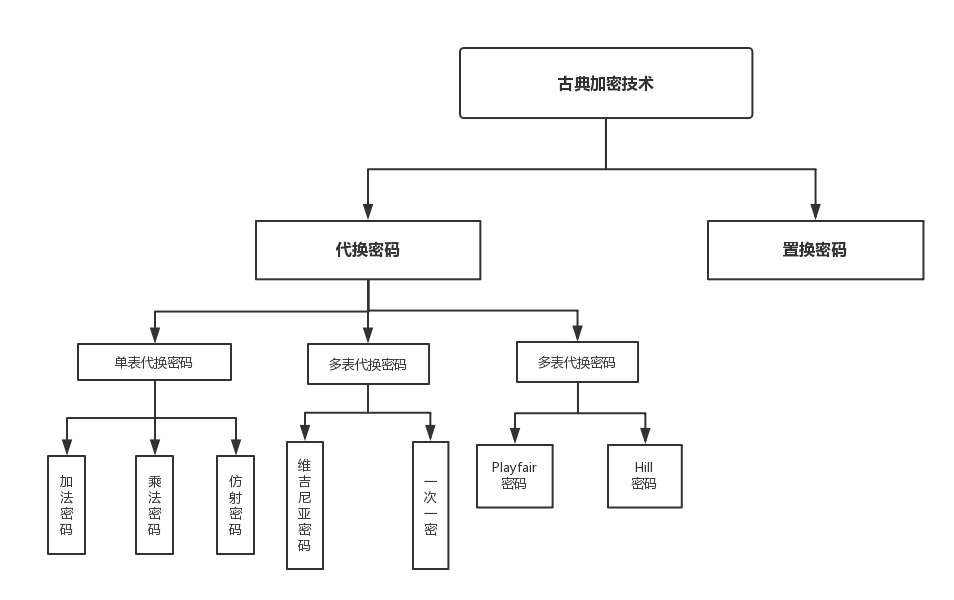
答：唯密文攻击，已知明文攻击，选择明文攻击，选择密文攻击，选择文本攻击。

穷举攻击是试遍所有可能的密钥对所获密文进行解密，直到得到正确的密文，或者用一个确定的密钥对所有可能的明文进行加密，直到得到与所获得的密文一致。

1. 什么是置换密码？什么是代换密码？

答：置换密码：保持明文的所有字母不变，只是打乱明文字母的位置和次序。

代换密码：将明文字母用不同的密文字母代替。



1. 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。

答：线性密码分析和查分密码分析。

线性分析是一种已知明文分析，它以求线性近似为基础，通过寻找现代密码算法变换的线性近似来攻击，是一种统计攻击。

差分密码分析包含了将两个输入的异或与其相对应的两个输出的异或相比较，它的基本思路是通过分析明文对的差值与密文对的差值的影响来回复某些密钥位，差分分析可以用来攻击任何一个拥有固定迭代轮函数结构的密码算法。

1. 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。

答：（1） 密钥空间为26×13=312（n×φ（n），n=26）

（2） （3×18+5） mod 26=7

（3×4+5） mod 26=17

（3×2+5） mod 26=11

（3×20+5） mod 26=13

（3×17+5） mod 26=4

（3×8+5） mod 26=3

（3×19+5） mod 26=10

（3×24+5） mod 26=25

所以密文为：HRLNEDKZ

1. 已知乘法密码的加密变换*c*= *3m* mod 26，试求：
2. 写出它的解密变换。
3. 试对密文VMHHQ进行解密。

答：（1）m=1/3 c mod 26

（2）(1/3 × 21) mod 26 =7

(1/3 × 12) mod 26 =4

(1/3 × 7) mod 26 =11

(1/3 × 16) mod 26 =14

所以明文为hello

1. 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。

答：明文：nowwearehavingatest

密钥：networknetworknetwo

装换成数字相加，再mod 26 得出结果，在转换成数字

1. 用维吉尼亚密码加密明文“we are discovered save yourself”，密钥是：deceptive，求密文。
2. 用Playfair算法加密明文“Playfair cipher was actually invented by wheatstone”，密钥是：fivestars。

首先根据密钥列出5×5的矩阵：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| f | i | v | e | s |
| t | a | r | B | C |
| D | G | h | K | L |
| M | N | O | P | Q |
| U | W | X | Y | Z |

先把密钥放入到表格中，一个字母只出现一次，且之后的字母按字母表顺序填入，j/i一家人

之后把明文两两分组，每一组要求字母不同，如果相同则在中间加x，如果最后只有一位，最后加x

根据两个字母寻找替换

Pl -> qk

Ay=bw

Fa ir ci ph er wa

Wa=ig

处于相同列 则向下找，处于向同行，向又找，不同行不同列找交点。

1. 设密钥是network，使用Playfair算法加密Playfair cipher，求密文。
2. 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。

解：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| N | E | T | W | O | R | K |
| W | A | R | E | D | U | S |
| C | I | V | E | R | E | D |
| S | A | V | E | Y | O | U |
| R | S | E | L | F |  |  |

把密钥字母按顺序排列：eknortw 然后按字母顺序一列一列写出来

AIAS SDU WCSR DRYF RVVE EEEL

1. 使用穷举搜索法，破译如下利用凯撒密码加密的密文：

BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD

1. 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。

1. 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。

1. 设计密码算法的两个主要方法混淆与扩散的区别是什么？
2. 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。
3. 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。

1. 试述使用两个密钥的三重DES的加解密过程。
2. 简述DES的加密过程。
3. 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。

1. 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。

(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。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

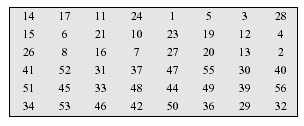
(3) 假设R为（0000 1001 0001 0010 0011 1101 0110 1010），使用如下扩展置换对R进行置换，写出扩展后的48位值（需有详细中间过程，如矩阵形式的中间结果）。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 |

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。

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 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。

(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？

答：流密码也成为序列密码，它是对明文以一位或者一个字节为单位进行操作。

分组密码是针对固定大小的分组进行加密的。

简述分组密码和流密码的区别。

简述AES的加密过程。

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。

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。

简述DES和AES中使用S盒的区别。

简述流密码的主要类型并列举典型的流密码算法。

简述RC4加密算法的基本原理。

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。

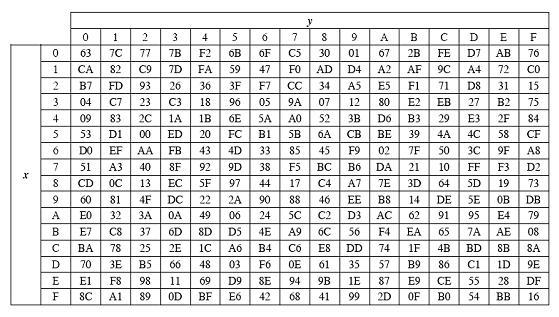
利用AES中的倍乘函数分别计算{02}{87}、{03}{6E}。注：。

AES中使用的S盒如下图所示，问：

（1）简述S盒的代换规则。

（2）依次输入十六进制的19、3D时，求对应的十六进制输出结果。

（3）依次输入二进制的1110 0011、1011 1110时，求对应的二进制输出结果。



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？
2. 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？
3. 步骤3中，A向B发送的消息是什么？
4. 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。
5. 步骤4和步骤5的主要目的是什么？

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。
2. 由谁产生的？它的作用是什么？
3. 若密钥分配中心有个用户，则需要分配的的总数是多少？
4. 步骤1和步骤2的目的是什么？
5. 步骤3中，A向B发送的消息是什么？目的是什么？
6. 步骤4和步骤5的主要目的是什么？

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。

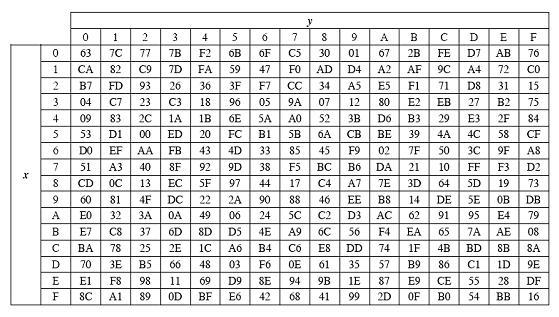
（2）行移位后的State矩阵将进行列混淆变换。设行移位后State矩阵的第一列的四个元素，从上到下依次为：*s*0，*s*1，*s*2，*s*3，求*s*0经过列混淆变换的结果，其中变换公式为：，不可约多项式为：。

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：。

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：



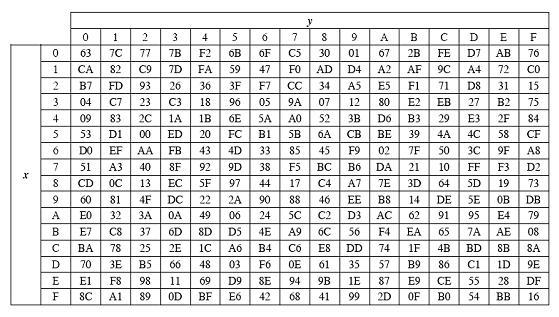
(1) 写出最初的密钥矩阵K0=（W0，W1，W2，W3）的值。

(2) 简述密钥扩展原理。

(3) 求扩展密钥数组的下一个密钥字W4。

(4) 求扩展密钥数组的后续密钥字W5，W6，W7。

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。

(2) 若字节代换前State的值为：，写出字节代换后State的值。

(3) 写出行移位后的State的值

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。

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。

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？

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？

如何利用公钥密码技术分配对称密钥？

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？

(2) 会话钥的作用是什么？

(3) 写出一个密钥分配协议，并分析其安全性。

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)),

阐述使用Diffie-Hellman协议产生一个会话密钥的具体过程。

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。

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。

RSA算法中，选择，，，求私钥。

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。

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。

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？

(2) 利用快速指数模运算方法计算A的公开量。

(3) 计算A和B双方共同的密钥。

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。

(2) 求明文M的值。

(3) 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？

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？

(3) 步骤6和步骤7的主要目的是什么？

第5章

Hash函数有哪些功能？什么是MD5？

试述散列函数应满足的条件 。

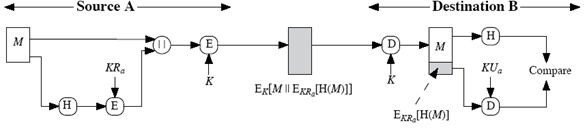
试说明数字签名的典型使用方法。

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？

简述数字签名的基本原理。

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。

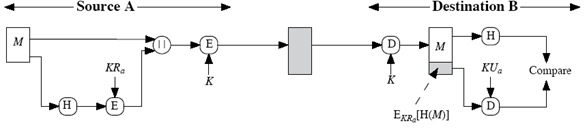


(1) 中各变量及整个公式的含义。

(2) 说明该方法能够同时提供保密性和认证性的原因。

(3) 散列函数与消息认证码的相同点和区别是什么？

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。

(2) 写出Source A所进行操作的总表达式，并解释其含义和作用。

(3) 简述B接收到A发送的消息后进行的操作及其作用。

(4) 该方法提供了哪些安全服务。

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？

什么是交叉认证？请给出交叉认证的过程。

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。

试述CA的主要职责。

数字证书的原理是什么？

试述基于X.509数字证书在PKI中的作用。