1. **选择题**
2. 以下算法中属于非对称算法的是（ B ）**p81**
3. Hash算法 B.RSA算法

C.IDEA D.三重 DES

1. 以下不属于非对称密码算法的特点是（ D ）**p80**
2. 计算量大 B.处理速度慢

C.运算过程复杂 D.适合大量数据加密

1. 就目前计算机设备的计算能力而言，数据加密标准DES不能抵抗对密钥的穷举搜索攻击，其原因是（　Ｂ　）**p69**
2. DES 算法是公开的
3. DES的密钥较短
4. DES除了其中S盒是非线性变换外，其余变换均为线性变换
5. DES算法简单
6. **判断题**
7. 分组密码体制允许反复使用同一密钥，但需要将明文分割成固定长度的数据段后，再进行加密运算。**V**
8. 流体密码体制每一次加密过程使用不同的密钥，且这些密钥之间没有相关性.**V**

３.RAS的加密密钥可以公开，解密密钥也是公开的**。X P81**

1. **名词解释**
2. 凯撒密码：凯撒密码是一种通过用其他字符替代明文中的每一个字符，完成将明文转化为密文过程的加密算法。**p58**
3. 换位密码：换位密码是一种通过改变明文中每一个字符串的位置，完成将明文转换成密文的过程。**P58**
4. 流密码体制：流密码体制，也称序列密码体制，是一次一密钥的加密运算过程。**P71**
5. **计算题**
6. 设英文字母A, B, C, … , Z分别编码伪0, 1, 2, 3, … , 25。已知单表加密变换为  
   c＝5m＋7（mod 26）  
   其中m表示明文，c表示密文。试对明文HELPME加密。  
   明文H  E  L  P  M  E对应的编码值分别是  7  4  11  15  12  4。用加密变换将上述6个编码值分别加密并转换为字母是  
   c＝5×7＋7 （mod 26）＝16 ...... Q  
   c＝5×4＋7 （mod 26）＝1 .....  B  
   c＝5×11＋7 （mod 26）＝10 ..... K  
   c＝5×15＋7 （mod 26）＝4 ....  E  
   c＝5×12＋7 （mod 26）＝15 ...... P  
   c＝5×4＋7 （mod 26）＝1  ..... B  
   从而得到密文QBKEPB。
7. 设 素数P=71，原根α=7，用户A选择XA=1，用户B选择XB=2，求用户A和用户B用Diffie-Hellman密钥交换算法同步密钥K。**P77**
8. XA=1,求出YA=α¹mod p = 7¹ mod 71 = 64
9. XB=2,求出YB=α²mod p = 7² mod 71 = 22
10. 用户A求出KA=YB¹mod p = 22¹ mod 71= 49
11. 用户B求出KB=YA²mod p =64² mod 71 = 49
12. KA=KB=K=49

3.使用RSA算法进行加密**p79**  
(1）p=3,q=11,e=7,M=5

M=5是明文，计算过程如下：  
n=p\*q=33;  
求出欧拉函数：(p-1)\*(q-1)=20;  
加密：y=密文，x=明文=5;  
y=x^e mod n = 5^7 mod 33 = 14;

1. **简述题**
2. WEP加密机制的缺陷**p75**
3. 由于用伪装随机数生成器来产生密钥，无法保证这些密钥之间没有任何相关性。
4. 作为随机种子一部分的原始数据密钥K是不变的，增加了这些密钥之间的相关性。
5. 初始向量的长度只有24位，密钥集中的密钥数<=2的24次方，如果原始密钥K较长一段时间内保持不变，加密用的一次性密钥很容易重复，破坏流密码体制一次一密钥的原则。
6. 对称密钥和公开密钥的特点**p80**

对称密钥加密算法的优势是加密解密运算过程相对简单，计算量相对较少，劣势是密钥的分发比较困难。公开密钥加密算法的劣势是加密解密过程比较复杂，计算量相对较大，因此，不适合大量数据加密的应用坏境。优势是密钥分发简单，可以通过有公信力的传播媒介公告公钥。

1. 公开密钥加密算法密钥分发原则**p80**
2. 成对生成加密密钥和解密密钥。

加密密钥和解密密钥是一一对应的，用加密密钥的密文只能通过对应的解密密钥解密。因此，需要成对生成加密密钥和解密密钥。

1. 公告加密密钥和，保密解密密钥。

所有需要向指定接收者传输密文的发送者，可以用同一个加密密钥对明文进行加密运算。如果只有该接收者知道解密密钥，则只有该接收者能够解密所有发送者发送的密文。因此，加密密钥可以通过有公信力的媒介公告，解密密钥必须只有密文接收者知道。

1. 需要证明密文接收者与加密密钥之间的绑定关系。

接收者A为了能够解密发送者发送给接收者B的密文，生成一对密钥PKA和SKA，并将加密密钥PKA作为接收者B的加密密钥给予公告。当发送者需要向接收者B传输密文时，错误地用PKA对明文进行加密运算。由于只有接收者A知道加密密钥PKA对应的解密密钥SKA，因此，接收者A可以解密发送者用PKA加密的密文。因此，为了防止某个接收者通过冒充其他接收者公告加密密钥的情况，加密密钥与密文接收者之间的绑定关系必须得到有公信力的权威机构的证明。