网络信息安全总复习级队资料 No.1

2017年考试卷详细解析串联知识点

一、单项选择题（每小题3分，共24分）

（1） DES 是一种（ ）↵

A） 对称的分组加密方案 B） 抗冲突的散列方案 C） 数字签名方案 D） 流加密方案↵

1. 解析：四种常见的加密方案和他们具体的实现算法

加密方案	实现算法
对称的分组加密方案	DES
抗冲突的散列方案	Hash函数
数字签名方案	使用用户的私钥加密消息的Hash值
流加密方案	将明文转换为二进制位串，逐位使用加密算法进行加密得到密文二进制串

所以本题选 A。

（2）数字证书的本质目的在于（ ）↵

A）发布用户的公钥↵

B）发布用户的身份标识↵

C）发布用户公钥并以一种可核实的方式将该公钥与其合法持有者的身份标识联系起来↵

D）发布用户私钥并以一种可核实的方式将该私钥与其合法持有者的身份标识联系起来↵

2. 解析：数字证书的本质是什么？

数字证书的本质：一个用户以一种安全的方式将它的公钥交给可信第三方并获得证书，任何需要该用户公钥的人都可以获得该证书，并通过查看附带的可信签名来验证证书的有效性。

数字证书的要求

1. 任何通信方可以读取证书并确定证书拥有者的*姓名*和*公钥*
2. 任何通信方可以验证该证书出自证书管理员，不是伪造的
3. 只有证书管理员可以产生并更新证书
4. 任何通信方可以验证证书的时效性

所以本题选C。

（3）A 方有一对密钥（$K_{A\,公开}$，$K_{A\,秘密}$），B 方有一对密钥（$K_{B\,公开}$，$K_{B\,秘密}$），A 方向 B 方发送数字签名 M，对信息 M 加密为：M'= $K_{B\,公开}$（$K_{A\,秘密}$（M））。B 方收到密文的解密方案是（　）

A）$K_{B\,公开}$（$K_{A\,秘密}$（M'））　　B）$K_{A\,公开}$（$K_{A\,公开}$（M'））

C）$K_{A\,公开}$（$K_{B\,秘密}$（M'））　　D）$K_{B\,秘密}$（$K_{A\,秘密}$（M'））

3. 解析：已知加密算法，怎么找到解密算法？

想要分析出B的解密方案就必须分析透A的加密方案：

1. A的明文内容是M
2. 对M首先使用A的私钥进行加密——这是对明文签上A的数字签名，以实现消息的不可否认性和A身份的真实性
3. 对签名后消息使用B的公钥进行加密——这是实现对消息的保密性

所以对应的解密过程应该与加密过程相反：

1. 使用B的私钥解密出被A签名后的明文
2. 使用A的公钥验证A的签名，确定A身份的真实性

所以应该选择C。

（4）ϕ(N)是N的Euler函数, ϕ(15)的值是（ ）

A）14；　B）8；　C）6；　D）16

4. 解析：怎么计算欧拉数？

求欧拉数的算法流程：

```
对于Euler(N)（N是括号里的那个数）：

if(N是一个素数)
  Euler(N) = N - 1;
else
  将N分解成两个素数P、Q的乘积，即 N = P · Q;
  Euler(N) = (P-1)·(Q-1);
```

故本题Euler（15）=Euler（3*5）=（3-1）·（5-1）=8；

所以应该选择B。

（5）X = 5 mod 9, X =2 mod 7, X =4mod 19 则X=( )

A）14； B）41； C）32； D）23

5. 解析：选择题中如何快速作答中国剩余定理?

本题考察中国剩余定理。

这是一道选择题，不必使用中国剩余定理公式计算。

14 ÷ 9 余 5，14 ÷ 7 余 0 排除

41 ÷ 9 余 5，41 ÷ 7 余 6 排除

32 ÷ 9 余 5，32 ÷ 7 余 4 排除

23 ÷ 9 余5， 23 ÷ 7 余 2，23 ÷ 19 余 4，正确

所以本题选D。

（6）*Diffie-Hellman*协议所协商的会话密钥的保密性质基于( )

A）合数模的二次剩余问题难解

B）多项式求根问题难解

C）离散对数问题难解

D）因子分解问题难解

6. 解析：因子分解问题难解和离散对数问题难解是什么东西?

我们目前所学习的加密协议所协商的会话密钥不过是基于两个难解的数学问题：

1. 因子分解问题难解：就是说想要将一个大素数（2的256次方级别）分解成两个大素数乘积，求着两个大素数因子目前没有一个有效的算法。
2. 离散对数问题难解：就是说对于方程

$$y = g^x \ mod \ p$$

对给定的x、g、p，求解y是容易的；但是给定y、g、p求解x就是非常困难的。

对于因子分解问题难解的应用是RSA算法，对于离散对数问题难解的应用是Diffie-Hellman算法和El Gamal算法，El Gamal算法不过是在Diffie-Hellman算法的基础上使发送方的公钥随机产生，使之成为了概率密码算法。

（7）数字签名的使用一般不解决下面哪种安全需求（ ）

A）机密性

B）完整性

C）认证性

D）不可否人性

7. 解析: 数字签名的安全需求

四种安全需求的含义

安全需求一共有以下四种：

1. 机密性：消息能否保密传送
2. 完整性：消息如果遭到篡改能否在接收端被及时发现
3. 认证性：消息接收方能否确定该消息一定是由消息发送方发送的
4. 不可否认性：接收方收到发送方的消息，如果发送方想要抵赖自己没有发送过这条消息，接收方可以展示证据证明发送方发送过，即源不可否认性；发送方发送消息给接收方，如果接收方在接收后想要抵赖自己没有接受过这条消息，发送方可以展示证据证明接收方已经接收到了消息；

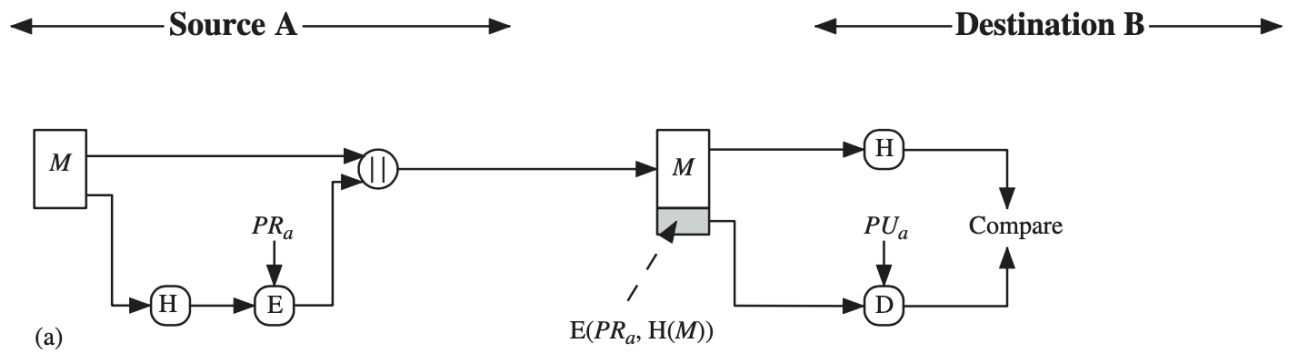
数字签名能满足的安全需求

1. 数字签名能保证完整性：

数字签名过程中，发送方使用自己的私钥加密消息的Hash值，其他任何用户都知道发送方的公钥，所以都能通过数字签名来验证消息的完整性。这是为什么呢？如果有人想要篡改消息，它篡改的是私钥加密过的Hash值，又因为Hash值是通过散列函数多对一映射得来，所以一旦被修改就会导致接收方解密出的明文的Hash值完全无法与被加密的Hash值匹配，便知道消息遭到了篡改。

2. 数字签名能保证认证性：

使用发送方的私钥，利用公钥密码算法进队Hash码进行加密可以提供认证性。这是为什么呢？因为只有发送方能够使用自己的私钥产生加密后的Hash码。所以既然得到了Hash码就说明一定是发送方发送的。

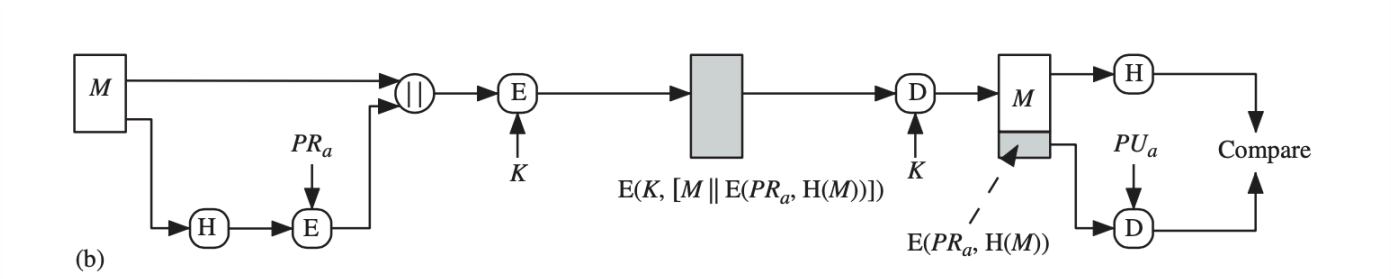


3. 数字签名能保证不可否认性

由于发送方的公钥是与发送方的证书关联的，所以既然接收方可以使用发送方的公钥进行身份验证，就能够在发送方抵赖时提供发送方的证书作为证据

4. 数字签名不能保证保密性

因为数字签名是用私钥进行加密的，而公钥是众所周知的，所以数字签名当然就无法对消息进行保密。如果希望既保证保密性又希望有数字签名，则先用发送方的私钥对Hash码加密，再用对称密码中的密钥对数字签名过的明文进行加密。这和第三题的加密算法时一致的。



（8）哪一项不是在X.509证书中所包含的项（ ）

A）用户的公钥

B）证书的有效期

C）用户的私钥

D）主体唯一标志

8. 解析：什么是X.509?

X.509是一个标准。这个标准定义了管理用户信息数据库的服务器都提供哪些认证服务。认证服务的核心是与每个用户相关的公钥证书。这些证书由可信第三方签发，而X.509规定了用户该如何存储和取得这些证书。

X.509证书

不管什么证书，它的本质都是将用户的身份和公钥关联在一起的数据结构。由于它是所有有该证书查阅权限的用户都能访问的，所以证书所有者的私钥信息必然不会在证书内。证书包含以下信息：

1. X.509的版本
2. 序列号：这本证书在可信第三方那里的唯一标识
3. 有效期
4. 证书主体名：证书所有者的用户名，证明拥有相应死要的主体是公钥的所有者
5. 发行商
6. 证书主体唯一标识符
7. 签名：用CA死要对证书的所有域即对这些域的Hash值一起加密

所以这道题应该选择C。

二、证明题

1. 现有以下公钥加密方案，其中：公钥pk=(e，N，H，G)、N是两个(保密的)素数的乘积，e是和Euler函数ϕ(N)互素的一个正整数；私钥sk=d，d是满足方程 ed=1 mod ϕ(N) 的一个正整数，ϕ(N)保密。明文消息M是1到N-1之间的整数，加密算法E(pk, M)如下：计算y = M……e mod N；

   输出密文y；(25分)

- （1）请写出相应的解密算法D(sk, y)。（5分）
- （2）证明以上你所给出的解密算法是正确的，即若y=E(pk, M)则必有D(sk, y)=M。（10分）
- （3）若两个素数p=3,q=11,e=7, 求其私钥d；（5分）
- （4）对消息M=7，计算其密文。（5分）

1. 做题技巧解析

第一、二问

本题考察RSA算法解密算法的数学表达形式，解密算法的数学证明，私钥的计算方法以及算法的应用。

RSA是公钥密码的一种，所以想要解密密文必定是使用接收者的私钥进行解密。我们看到在算法中利用了这样的一种奇妙的知识：

$$ed = 1\ mod\ \varphi(N)$$

其中，e是由通信的两个人各自挑选的公钥，而d是私钥，它是公钥关于ϕ(N)的乘法逆元。而e在加密明文时是位于明文的幂位置的，所以，接收方在解密时一定要凑出ed的形式，将M的幂化为1，才能解出明文，这也就是为何解密时要使用：

$$C^d\ mod\ N$$

以达到：

$$\begin{aligned}
&C^d \mod N \\
&= M^{ed} \mod N \\
&= M^{k\varphi(N)+1} \mod N \\
&= ((M^{\varphi(N)})^k \bullet M) \mod N \\
&= (M^{\varphi(N)} \mod N)^k \bullet (M \mod N) \\
&= 1^k \bullet (M \mod N) \\
&= M \mod N
\end{aligned}$$

第三问

在第三问中，如果我们知道p、q，我们就能直到N，因为：

$$N = p \bullet q$$

如果我们直到N，我们就能求出ϕ(N)，因为根据欧拉公式：

$$\varphi(N) = (p-1) \bullet (q-1)$$

如果我们求出ϕ(N)，就能求出e关于它的乘法逆元d：

$$d = e^{-1} \mod \varphi(N)$$

即找到一个数d，它乘以e除以ϕ(N)的余数是1.

第四问

对于第四问，我们只需要将M和e代入加密公式：

$$C = M^e \mod N$$

便可以求出密文C。

2. 阐述Diffie-Hellman密钥协商机制（可通过图示说明），并分析其安全机制，说明所存在的中间人攻击方式。（15分）

2. 做题思路解析

Diffie-Hellman密钥协商机制的原理是这样的，

先由通信双方选择大素数q和大素数q的本原根a，这对信息对所有其他用户可见；

然后由通信双方分别寻找自己的私钥X，这个私钥X可以使小于q的任何整数；

在生成自己的私钥X后，利用私钥X作如下运算得到自己的公钥Y：

$$Y = a^X \mod q$$

这个公钥会被其他用户所见；

如果用户A希望和用户B进行通信，那么AB两人便需按如下方法计算出会话密钥K：

$$\begin{aligned}
&对A而言：K = (Y_B)^{X_A} \mod q \\
&对B而言：K = (Y_A)^{X_B} \mod q \\
&\because (Y_B)^{X_A} = (a^{X_B})^{X_A} = a^{X_A X_B} \\
&= (a^{X_A})^{X_B} = (Y_A)^{X_B} \\
&\therefore (Y_B)^{X_A} \mod q = (Y_A)^{X_B} \mod q = K
\end{aligned}$$

请记住，两个用户通过公钥和私钥所要传递的消息不是明文，而是他们二者之间的会话密钥，所以这个被称为”密钥协商机制“。

由于DH算法没有依赖可靠第三方来授权证书，所以这套算法会遭到”中间人攻击“：

1. 中间人可以看到用户A和用户B的公开信息大素数q和本原根a。他会根据大素数q来生成两个自己的密钥XD1和XD2。
2. 中间人会利用运算：

$$\begin{aligned}
Y_{D1} = a^{X_{D1}} \mod q \\
Y_{D2} = a^{X_{D2}} \mod q
\end{aligned}$$

   计算出两对公钥YD1和YD2。中间人已经做好分别和A、B用户通信的准备了。

3. 当用户A发送自己的公钥YA给用户B时，中间人截获这条消息，得到了用户A的公钥YA；中间人将事先准备好的公钥YD1发送给用户B。用户B由于没有通过辨别公钥是不是用户A的公钥的能力，所以用户B理所当然的接收中间人的公钥YD1并认为这就是用户A的公钥。
4. 当用户B发送自己的公钥YB给用户A时，中间人截获这条消息，得到了用户B的公钥YB；中间人将事先准备好的公钥YD2发送给用户A。用户A由于没有通过辨别公钥是不是用户B的公钥的能力，所以用户A理所当然的接收中

间人的公钥YD2并认为这就是用户B的公钥。

5. 当用户A和用户B都分别获得了中间人的公钥后，它们和中间人都开始分别计算会话密钥K1和K2。其中K1是用户A和中间人的会话密钥，K2是用户B和中间人的会话密钥，K1和K2的运算如下：

$$K_1 = (Y_{D1})^{X_A} \mod q = (Y_A)^{X_{D_1}} \mod q$$
$$K_2 = (Y_{D2})^{X_B} \mod q = (Y_B)^{X_{D_2}} \mod q$$

6. 如此，用户A和用户B都以为自己在和对方使用会话密钥通信，实际上，他们是分别在和中间人通信。

3. 一个公钥加密方案如下：↵

P 是一个素数，g 是与 P 互素的整数，1≤g≤P−1；1≤X≤P−2 是一个整数，↵ $Y=g^X \bmod P$；公钥 pk=（g，P，Y），私钥 sk=（X）。↵

消息 M 是一个满足 1≤M≤P-1 的数，加密算法 E（pk, M）如下：↵

在 1 到 P−2 之间取随机数 r；↵

$U=g^r \bmod P$；↵

$V=MY^r \bmod P$；↵

密文 Z=（U，V）↵

（1）请给出相应的解密算法 D（sk, Z）并证明你的算法是正确的，即：若 y=E(pk, M)则必有 D(sk, y)=M. （10 分）↵

（2）已知 Z=（U，V）是某个消息 M 的密文（M 本身未知），问 $Z^*=(U^8, V^8)$ 所对应的消息 M*和 M 有什么关系？请写出关系式并证明这一关系。（5 分）↵

3. 做题技巧解析

第一问

本题使用的算法是El Gamal算法。El Gamal算法是对Diffie-Hellman算法的增强，它使用概率密码，相同的明文和密钥每一次得到的密文都不相同。

针对明文对(U, V), U是为我们提供会话密钥K的信息的，这是因为：

$$\because U = g^r \mod P$$
$$\therefore K = Y^r \mod P$$
$$= (g^X)^r \mod P$$
$$= (g^r)^X \mod P$$
$$= U^X \mod P$$

V可以让我们在通过U求出会话密钥K后得到明文，完成解密，这是因为：

$$\because V = MK \mod P$$
$$\therefore M = V \times K^{-1} \mod P$$

这里，明文等于V乘上K关于素数P的乘法逆元再模P即可，K的乘法逆元就是K乘上这个数除以P余数为1的那个数。

所以，解密算法的完整形式应该是如下的：

$$M = V \times (U^X)^{-1} \mod P$$

为什么相同密钥、相同明文却会得到不同的密文呢？这是因为随机数r是每次通信由其中发送方随机生成的，由于离散对数问题难解，所以接收方和攻击方都很难通过U来计算出r的值。接收方无需知道r的值，因为他可以直接使用U和自己的私钥X，利用：

$$K = U^X \mod P$$

计算出K值，进而再利用V值求出明文，实现解密。

第二问

解决本问关键的两个变量是：明文M和随机数r。这两个变量都有可能前后两次不同，导致最终得到的密文不同。由于在第一问中我们得到：

$$M = V \times (U^X)^{-1} \mod P$$

那么如果出现V和U分别变为原来的8次幂，明文又会是怎样变化呢？

$$M^* = V^8 \times ((U^8)^X)^{-1} \mod P$$

根据模运算的性质可以将上式化简为：

$$\begin{aligned} M^* &= (V \times (U^X)^{-1})^8 \mod P \\ &= M^8 \mod P \end{aligned}$$

三、计算题

2. 签名方案

公钥：p=19， g<p, g 是 p 的原根，g =10, $y=g^x \pmod p$

私钥：x<p-1, x=16

签名：随机选取, k=5, k 属于[1,p-1] 且 k 与 p-1 互素，

a（签名）$=g^k \mod p$

b（签名）满足 $M = (xa+kb) \mod (p-1)$, M=14

(即有：$b = (M- xa)k^{-1} \mod (p-1)$)

(1)计算 a, b (6 分)

(2)验证：如果 $y^a a^b \pmod p = g^M \pmod p$，则签名有效（5 分）

2. 做题技巧解析

本题的签名算法是基于离散对数问题难解。a签名的值类似于证明题第3题中的El Gamal算法关于密文U的计算。b签名的值在a的基础上配合私钥对明文进行计算。

第一问

计算a的值只需要代入题目公式计算即可：

$$
\begin{gathered}
a = 10^5 \mod 19 \\
\because 10^2 \mod 19 = 5 \\
\therefore 10^4 \mod 19 = (10^2)^2 \mod 19 = 25 \mod 19 = 6 \\
\therefore 10^5 \mod 19 = (10^4) \times 10 \mod 19 = 6 \times 10 \mod 19 = 3 \\
\therefore a = 3
\end{gathered}
$$

计算b的值同样只需要代入题目公式(b) 计算即可：

$$
\begin{gathered}
b = (M - xa)K^{-1} \mod (p-1) \\
= (14 - 16 \times 3) \times K^{-1} \mod (19-1) \\
\because K \times 11 \mod 18 = 1 \\
\therefore K^{-1} = 11 \\
\therefore (-34) \times 11 \mod 18 = 4 \\
\therefore b = 4
\end{gathered}
$$

第二问

我们可以迁移一下我们证明Diffie-Hellman和El Gamal算法时的思想，尝试利用欧拉定理进行化简，并且把所有包含离散对数型的变量展开计算，如本题中的y和作为底数的a：

$$
\begin{gathered}
y^a = (g^x)^a \mod p = g^{xa} \mod p \\
a^b = (g^k)^b = g^{kb} \mod p \\
y^a k^b \mod p = g^{xa+kb} \mod p
\end{gathered}
$$

我们下面需要证明：

$$
g^{xa+kb} \mod p = g^M \mod p
$$

这时我们发现这个式子的指数位置的形式我们似曾相识，我们应该立刻想到题目中有关M的等式有：

$$
M = (xa + kb) \mod (p-1)
$$

这更加坚定了我们证明它的信息，因为我们现在需要证明：

$$
g^{xa+kb} \mod p = g^{(xa+kb) \mod (p-1)} \mod p
$$

我们回想起在证明模运算性质时用到过的技巧：

$$
(xa + kb) \mod (p-1) \rightarrow (xa+kb) = n(p-1) + r, n \wedge r\text{是整数}
$$

代入到等式中，看看会有什么效果：

$$
g^{n(p-1)+r} \mod p = (g^{(p-1)})^n \mod p \times g^r \mod p
$$

根据欧拉定理，并且g与p互素，所以有

$$
g^{p-1} = 1 \mod p
$$

故证得：

$$g^{n(p-1)+r} \mod p = g^r \mod p$$

即原式得证。