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；

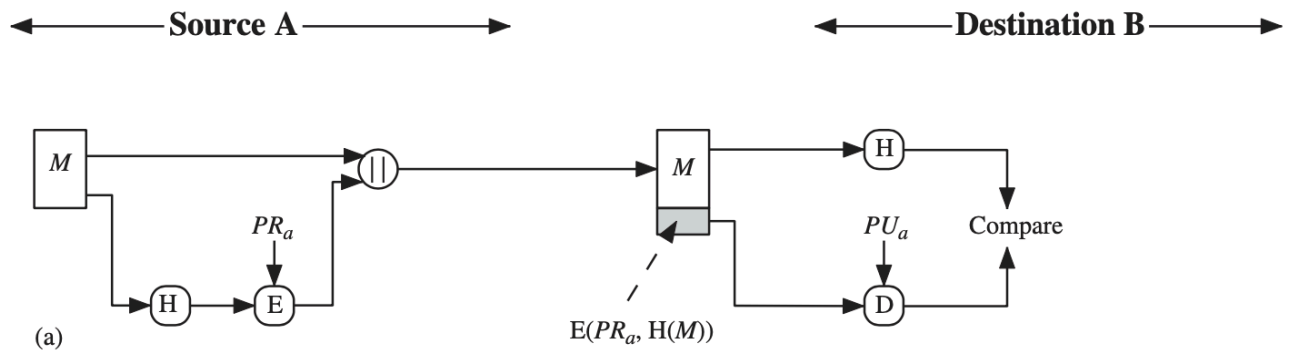
数字签名能满足的安全需求

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。

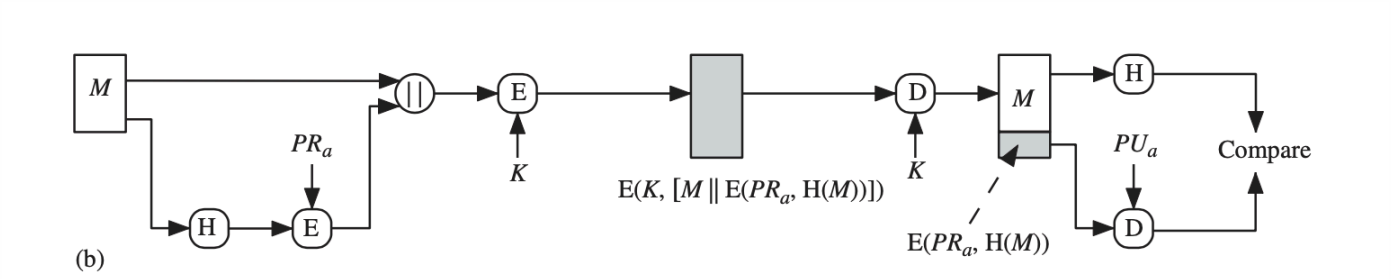


3. 数字签名能保证不可否认性

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。