



《密码学》

期末速成课



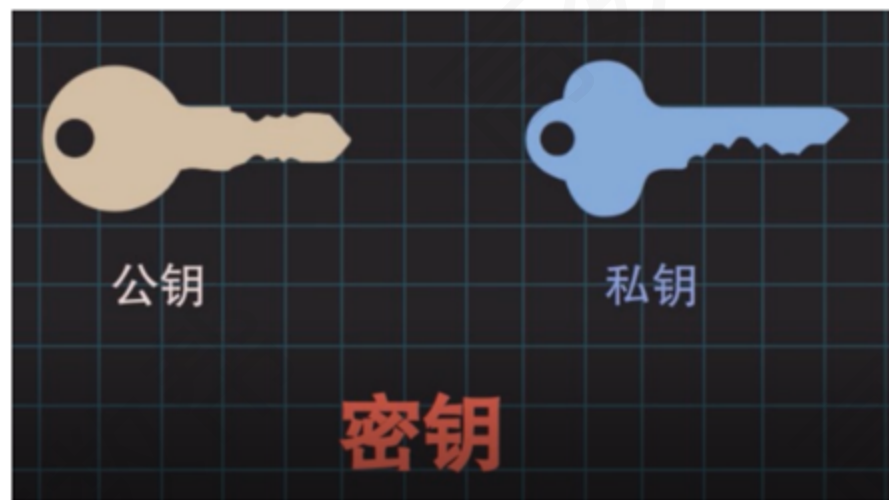
考点	重要程度	占分	题型
1. 密码学体系/分类	★★★★	4 - 6	选择/填空
2. 密码学五要素	★★	0 - 2	选择/填空
3. 信息安全五大属性	★★★★★	0 - 3	填空/问答
4. 哈希函数	★★★★★★	3 - 5	选择/填空/简答
5. 数字签名	★★★★★	5 - 8	填空/简答
6. 密码学两次飞跃	★★★★★	3 - 4	填空

1.1 密码学概论

一、密码学体系

密码学分为对称密码体制和公钥密码体制

- (1) 对称/私钥 密码体制：加解密使用相同的密钥【门锁】
- (2) 非对称/公钥 密码体制：加解密使用不同的密钥



1.1 密码学概论

一、密码学体系



二、密码学五要素

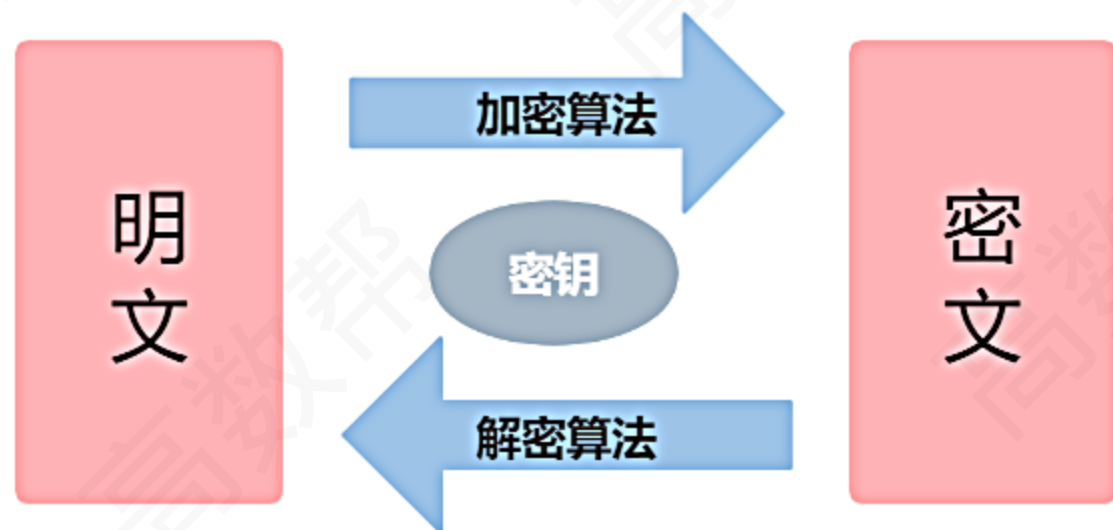
明文空间M

密文空间C

密钥空间K

加密算法E

解密算法D



三、密码学分类

密码学分类:密码分析学和密码编码学

(1) **密码分析学:** 是指在没有加密密钥的情况下,攻击密文的过程


密码分析学中, 设计和使用密码必须遵守**柯克霍夫准则**

- 柯克霍夫准则——算法必须公开, 对密钥进行保护

(2) **密码编码学:** 对信息进行变换, 保护信息在信道中的安全

三、密码学分类

攻击方式：唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击



攻击类型	攻击者拥有的资源
唯密文攻击	加密算法截获的部分密文
已知明文攻击	加密算法，截获的部分密文和相应的明文
选择明文攻击	加密算法加密黑盒子，可加密任意明文得到相应的密文
选择密文攻击	加密算法解密黑盒子，可解密任意密文得到相应的明文

唯密文攻击最困难，上述攻击的强度是递增的

四、信息安全五大属性

机密性: 与你说话时, 消息不能被别人偷听

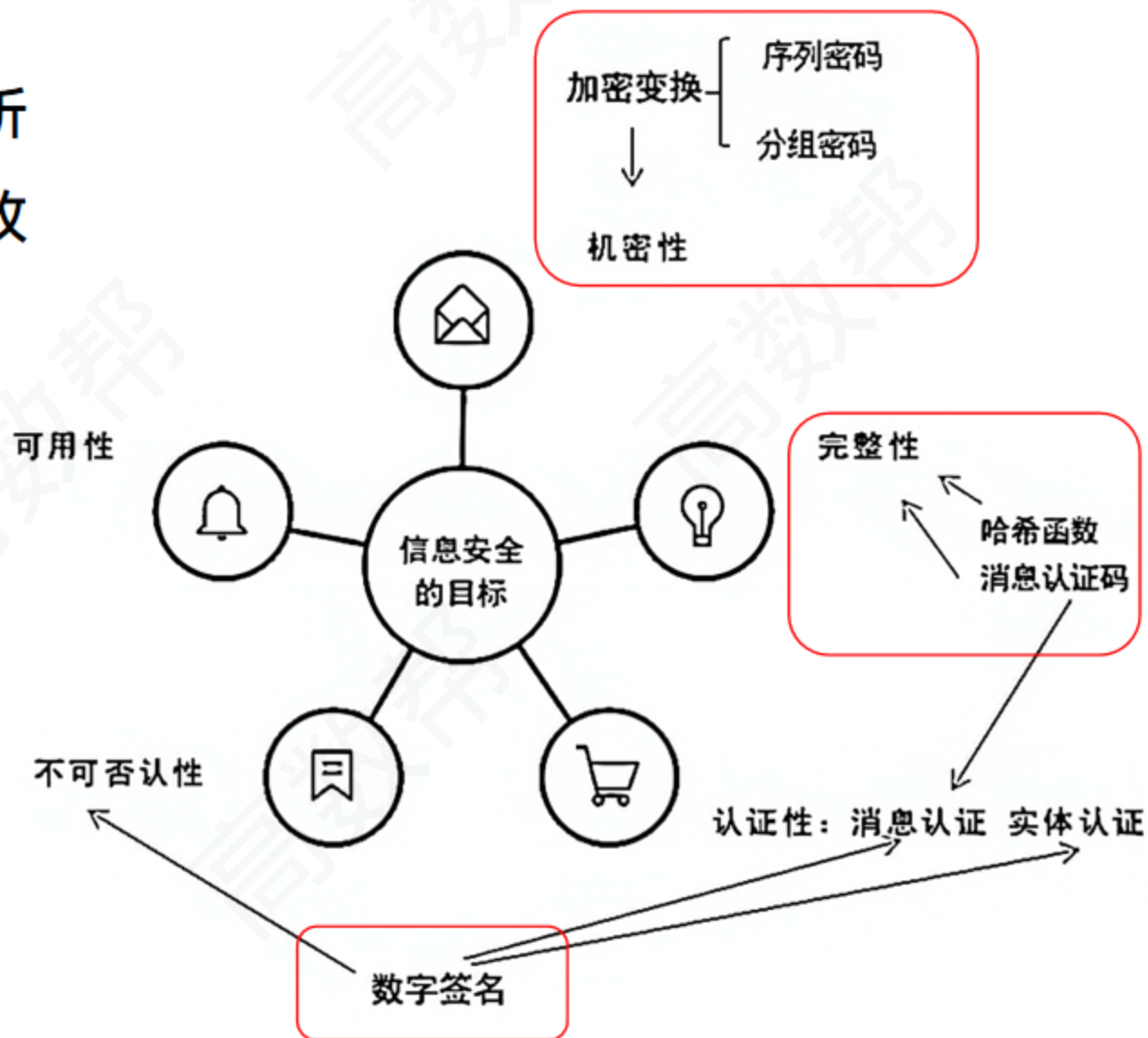
完整性: 信息中途传送过程中别人有无篡改

认证性: 你是谁, 我怎么相信是你,

你怎么证明是你

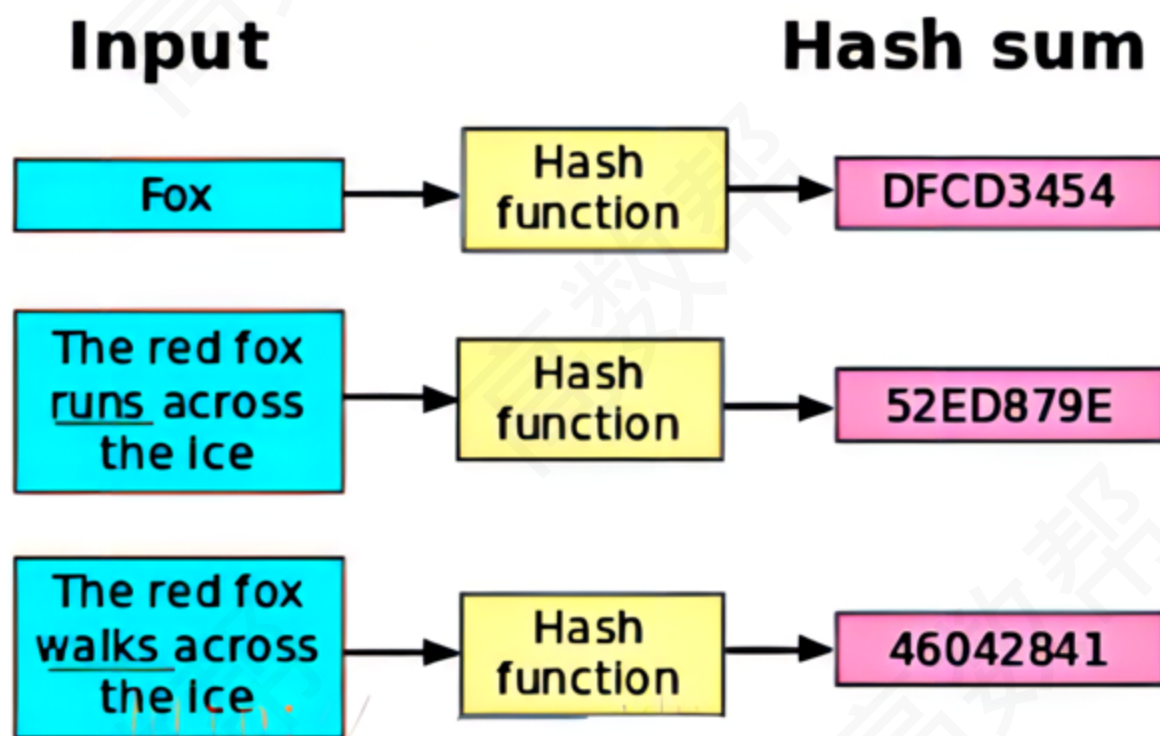
不可否认性: 我收到货, 不想付款想抵赖

可用性



五、哈希函数

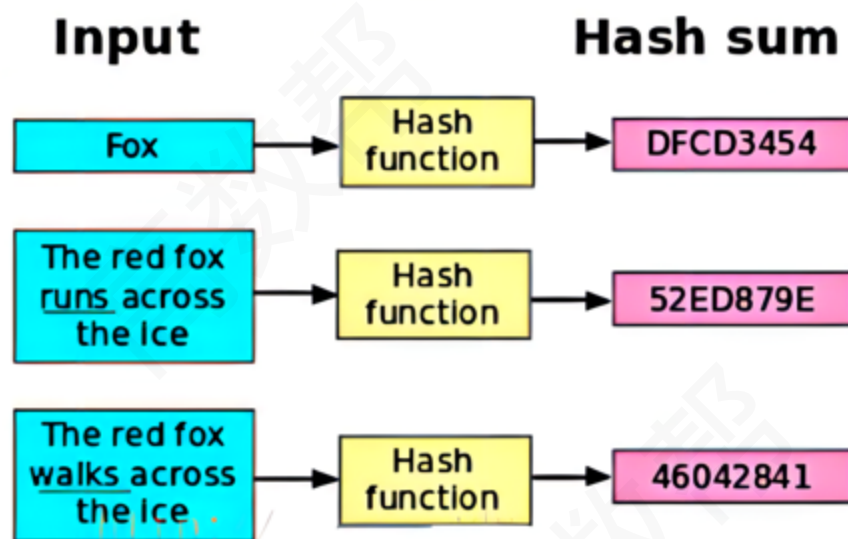
- 哈希函数是以任意长度的数据为输入，输出相应**固定长度的值**



- 常见哈希函数:** MD5、MD4、SHA-1、SHA-256、SHA-3、SM3

五、哈希函数

- 哈希函数/散列函数/杂凑算法
- 消息/数据—>哈希值/散列值/摘要



哈希函数性质：单向性、抗碰撞性、雪崩效应

单向性：对于给定的哈希值 h ，要找到 M 是的 $H(M)=h$ 在计算上是不可行的。

抗碰撞性：一种是弱抗碰撞性，即对于给定的消息，要发现另一个消息，满足在计算上是不可行的；另一种是强抗碰撞性，即对于任意一对不同的消息，使得在计算上也是不可行的。

雪崩效应：当一个输入位发生变化时，输出位将有一半会发生变化。

六、数字签名

- 私钥加密、公钥解密

加密通信

公钥加密

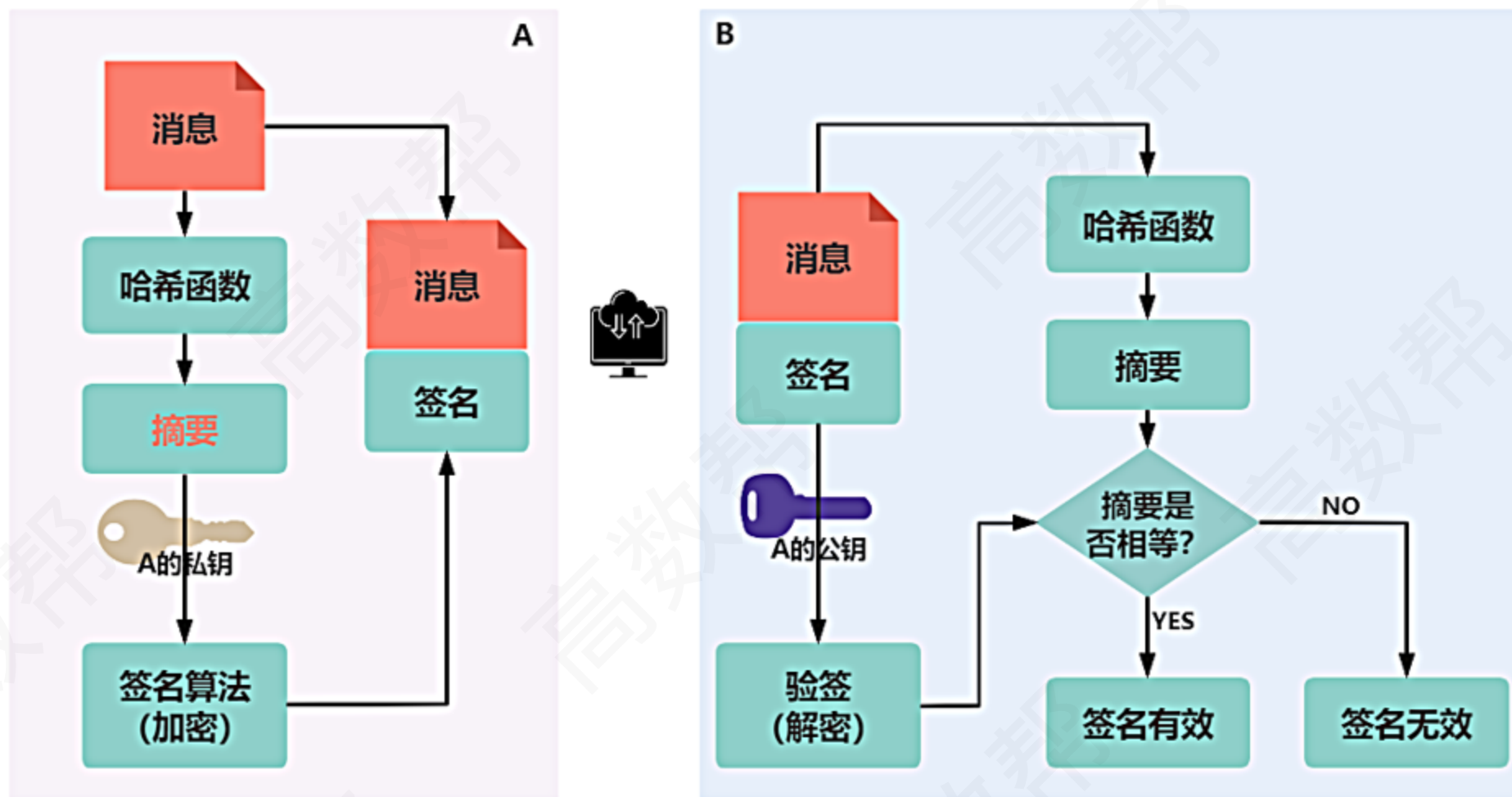
私钥通信

数字签名

私钥加密

公钥通信

六、数字签名

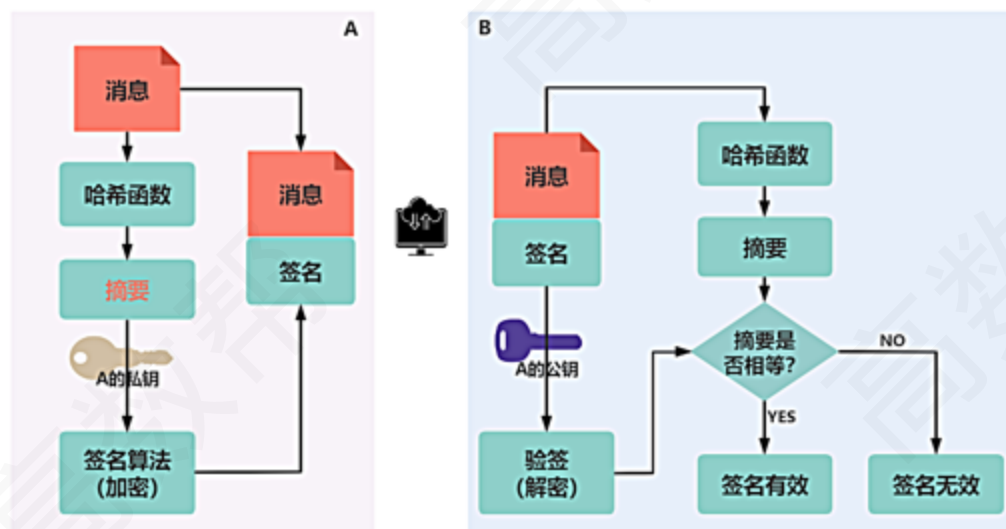


- ① 用户A使用私钥加密的是**摘要**而不是文件
- ② 用户B验证签名实际上是比较得出的两份摘要是否相等
- ③ 没有加密功能

六、数字签名

基本特征

- 报文鉴别——接收者能够核实发送者对报文的签名;
- 报文完整性——接收者不能伪造对报文的签名或更改报文内容。
- 不可否认——发送者事后不能抵赖对报文的签名



七、密码学两次飞跃

第一次质的飞跃 1949年香农发表《保密系统的通信理论》——密码学学科

第二次质的飞跃 1976年Diffie和Hellman发表《密码学的新方向》——公钥密码

八、密码学发展的三个阶段

传统密码时期 { 古典密码时期：凯撒密码、维吉尼亚密码
近代密码时期：转轮密码

现代密码时期：DES、RSA



扫码观看
视频讲解更清晰

【题1】 1949年，（ A ）发表题为《保密系统的通信理论》的文章，为密码系统建立了理论基础，从此密码学成了一门科学。

A、Shannon

B、Diffie

C、Hellman

D、Shamir

【题2】 一个密码系统至少由明文、密文、加密算法、解密算法和密钥5部分组成，而其安全性是由（ D ）决定的。

A、加密算法

B、解密算法

C、加解密算法

D、密钥

【题3】 密码分析是研究密码体制的破译问题，根据密码分析者所获得的数据资源，可以将密码分析（攻击）分为：唯密文攻击、已知明文攻击、选择明文攻击、选择密文攻击。

【题4】 （ A ） 用于验证消息完整性。

A、消息摘要 B、加密算法 C、数字信封 D、都不是

【题5】 下列 （ D ） 算法不具有雪崩效应。

A、DES 加密 B、序列密码的生成
C、哈希函数 D、RSA加密



扫码观看
视频讲解更清晰

【题6】 下列算法属于Hash算法的是（ C ）。

- A、DES B、IDEA C、SHA D、RSA。
-

【题7】 下面关于密码算法的阐述，（ C ）是不正确的。

- A、对于一个安全的密码算法，即使是达不到理论上的不破的，也应当为实际上是不可破的。即是说，从截获的密文或某些已知明文密文对，要决定密钥或任意明文在计算机上是不可行的。
- B、系统的保密性不依赖于对加密体制或算法的保密，而依赖于密钥（这就是著名的Kerckhoff原则）。安全性在于密钥，而不是算法。
- C、公钥密码体制下，加密的人也能解密。
- D、数字签名的理论基础是公钥密码体制。

【题8】 公钥密码学的思想最早由（ B ）提出。

A . 欧拉 (Euler)

B . 迪菲 (Diffie) 和赫尔曼 (Hellman) C . 费马 (Fermat)

D . 里维斯特 (Rivest) 、沙米尔 (Shamir) 和埃德蒙 (Adleman)

【题9】 下面的说法（ D ）是错误的。

A . 传统的密钥系统的加密密钥和解密密钥相同

B . 公开密钥系统的加密密钥和解密密钥不相同

C . 报文摘要适合数字签名但不适合数据加密

D . 数字签名系统一定具有数据加密功能



扫码观看
视频讲解更清晰

【题10】在非对称加密技术实现数据安全传输的应用中，发送方对明文加密后发送给接收方，接收方使用（ D ）对明文解密。

- A、发送方的公钥
 - B、发送方的私钥
 - C、接收方的公钥
 - D、接收方的私钥
-

【题11】在以下密码系统的攻击方法中，哪一种方法的实施难度最高的（ A ）。

- A. 唯密文攻击
 - B. 已知明文攻击
 - C. 选择明文攻击
 - D. 选择文本攻击
-

【题12】哈希函数的特点？

特点：单向性、抗碰撞性



扫码观看
视频讲解更清晰

【题13】 公钥密码体制与对称密码体制相比有什么优点和不足？

优点:

- (1) 密钥的分发相对容易
- (2) 密钥管理简单;
- (3) 可以有效地实现数字签名。

缺点:

- (1) 与对称密码体制相比，非对称密码体制加解密速度比较慢;
- (2) 同等安全强度下，非对称密码体制要求的密钥位数要多一些;
- (3) 密文的长度往往大于明文长度。