



信息安全

智慧课程
认证学习

国家精品

期末不挂科

升级认证学习
学习时长

李景涛

课程进度提醒



评价课程

返回

帮助

单元测试1

本次得分为： /16.00, 本次测试的提交时间为：2024-09-24, 如果你认为本次测试成绩不理想，你可以选择 再做一次。

分享

1 单选 (2分) 19世纪荷兰人A.Kerckhoffs就提出了一个在密码学界被公认为基础的假设，也就是著名的“Kerckhoffs假设”：秘密必须全寓于（ ）。

得分/总分

A. 密钥

B. 密文

C. 明文

D. 加密算法

正确答案：A 你选对了

提问

2 单选 (2分) 以下哪个要素不属于对称密钥密码系统？（ ）

得分/总分

A. 明文

B. 数字签名

C. 密文

D. 密钥

正确答案：B 你选对了

提问

3 单选 (2分) 古罗马时代使用的恺撒密码属于（ ）。

得分/总分

A. 分组密码

B. 行序列密码

C. 置换密码

D. 替代密码

正确答案：D 你选对了

提问

4 单选 (2分) Vigenère是一种多字母表密码，若被发现（ ）则很容易遭到攻击。

得分/总分



- A. 密钥数量
- B. 偏移量
- C. 密钥长度
- D. 字母频率

🔒 □□□□□□

正确答案：C 你错选为D

提问

5 单选 (2分) 下面关于无条件安全和计算安全，说法不正确的是（ ）。 得分/总分

- A. 假设攻击者时间有限计算资源有限的情况下，密码不能被破解称之为计算上安全。
- B. 假设攻击者有无限的时间，无限的资源，密码都不能被破解称之为无条件安全。
- C. 如果密钥序列真正随机，且明文序列长度相同，那么该密码无条件安全。
- D. AES密码是无条件安全的。

🔒 □□□□□□

正确答案：D 你选对了

提问

6 单选 (2分) 以下古典密码系统中，属于置换密码的是（ ）。 得分/总分

- A. 凯撒密码
- B. 羊皮传书
- C. Vigenère密码
- D. PlayFair密码

🔒 □□□□□□

正确答案：B 你选对了

提问

7 单选 (2分) 相对最容易遭受词频统计分析攻击的是（ ）。 得分/总分

- A. Autokey密码
- B. 维吉尼亚密码
- C. DES密码
- D. 单字母表密码

🔒 □□□□□□

正确答案：D 你选对了

提问

8 单选 (2分) 下面说法不正确的是（ ）。 得分/总分

- A. 有些公开密钥系统中，密钥对互相之间可以交换使用。
- B. 对称密钥体制中，密钥需要事先由发送方和接收方实现共享。
- C. 若知道公钥密码的加密算法，从加密密钥得到解密密钥在计算上是可行的。

🔒 □□□□□□

D. 密码体制包括对称密钥密码和非对称密钥密码两种。

正确答案： C 你选对了

提问



信息安全

智慧课程

认证学习

国家精品

期末不挂科

升级认证学习



学习时长

李景涛

课程进度提醒



评价课程

返回

帮助

单元测试2

本次得分为： /10.00, 本次测试的提交时间为：2024-10-18, 如果你认为本次测试成绩不理想，你可以选择 再做一次。

分享

1 单选 (2分) ____算法只能用于实现密钥交换，算法的安全性依赖于有限域上的离散对数问题。（ ） 得分/总分

A. AES

B. Diffie-Hellman



C. 椭圆曲线公钥密码

D. RSA

正确答案：B 你选对了

提问

2 单选 (2分) 下面关于公开密钥密码体制，不正确的是（ ）。 得分/总分

A. 若知道加密算法，从加密密钥得到解密密钥在计算上是不可行的。

B. 加密与解密由不同的密钥完成，并且可以交换使用。

C. 通信双方掌握的秘密信息(密钥)是一样的。



D. 一般情况下，公钥密码加密和解密速度较对称密钥密码慢。

正确答案：C 你选对了

提问

3 单选 (2分) 1976年，Diffie和Hellman在论文“密码学新方向（New Direction in Cryptography）”中首次提出了公开密钥密码体制的思想；“公开密钥密码体制”的意思是（ ）。 得分/总分

A. 将公钥公开,将私钥保密



B. 将私钥公开,将公钥保密

C. 将公钥和私钥都公开

D. 将公钥和私钥都保密


正确答案：A 你选对了

提问

4 单选 (2分) 以下哪项不是分组加密算法？（ ） 得分/总分



- A. DES
- B. RSA
- C. AES
- D. RC4

 □□□□□□

正确答案：D 你选对了

提问

5 单选 (2分) 以下哪些不属于RSA算法的应用（ ）。

得分/总分

- A. 数字签名
- B. 密钥交换
- C. 数据加密
- D. 可靠传输

 □□□□□□

正确答案：D 你错选为B

提问



信息安全

智慧课程
认证学习

国家精品

期末不挂科

升级认证学习
学习时长

李景涛

课程进度提醒



评价课程

返回

帮助

单元测试3

本次得分为： ☐ ☐ ☐ ☐ ☐ ☐ /20.00, 本次测试的提交时间为：2024-10-18, 如果你认为本次测试成绩不理想，你可以选择 再做一次。

分享

1 单选 (2分) 信息安全需求包括 ()。

得分/总分

- A. 以上都是
- B. 完整性
- C. 保密性
- D. 抗抵赖性

☐ ☐ ☐ ☐ ☐ ☐

正确答案：A 你选对了

提问

2 单选 (2分) 报文的 ()，即验证报文在传送和存储过程中是否被篡改、错序等。

得分/总分

- A. 保密性
- B. 完整性
- C. 身份认证
- D. 抗抵赖性

☐ ☐ ☐ ☐ ☐ ☐

正确答案：B 你选对了

提问

3 单选 (2分) 若发送者使用对称密钥加密报文，则无法实现 ()。

得分/总分

- A. 完整性
- B. 保密性
- C. 抗抵赖性
- D. 身份认证

☐ ☐ ☐ ☐ ☐ ☐

正确答案：C 你选对了

提问

4 单选 (2分) 以下哪一项不属于哈希函数的特性 ()。

得分/总分

- A. 固定长度的输出
- B. 抗碰撞性



C. 单向性

D. 可逆性

🔒 □□□□□

正确答案：D 你选对了

提问

5 单选 (2分) 对于报文M若找到M’使____，即找到碰撞能够构成对哈希函数H的攻击。（ ） 得分/总分

A. $M=M'$ 且 $H(M') = H(M)$

B. $M' \neq M$ 但 $H(M') = H(M)$

🔒 □□□□□

C. $M' \neq M$ 且 $H(M') \neq H(M)$

D. $M' = M$ 但 $H(M') \neq H(M)$

正确答案：B 你选对了

提问

6 单选 (2分) 要找到两个不同的报文x, y, 使 $H(y)=H(x)$, 在计算上是不可行的。则哈希函数H具有（ ）。

A. 压缩性

B. 单向性

C. 弱抗碰撞性

D. 强抗碰撞性

🔒 □□□□□

正确答案：D 你选对了

提问

7 单选 (2分) 发送者用____对报文签名，然后使用____加密，同时提供保密性和报文鉴别的所有三种安全服务。（ ） 得分/总分

A. 自己的公钥，自己的私钥

B. 自己的私钥，自己的公钥

C. 自己的公钥，接收者的私钥

D. 自己的私钥，接收者的公钥

🔒 □□□□□

正确答案：D 你选对了

提问

8 单选 (2分) 以下不属于Hash算法的是（ ）。

A. RSA

🔒 □□□□□

B. RIPEMD-160

C. SHA-1

D. MD5

正确答案：A 你选对了

提问

9 单选 (2分) 发送者使用接收者的公钥加密报文传递给接收者，能实现（ ）。 得分/总分

- A. 保密与部分报文鉴别
- B. 仅报文鉴别
- C. 保密且报文鉴别
- D. 仅保密

🔒 □□□□□□

正确答案：D 你选对了

提问

10 单选 (2分) 以下的描述中，对报文的数字签名不能实现的是（ ）。 得分/总分

- A. 防止报文发送者抵赖
- B. 保护报文的完整性
- C. 验证报文发送者的身份
- D. 保证报文传输过程中的保密性

🔒 □□□□□□

正确答案：D 你选对了

提问



信息安全

智慧课程

认证学习

国家精品

期末不挂科

升级认证学习



学习时长

李景涛

课程进度提醒



评价课程

返回

帮助

单元测试4

本次得分为： ☐ ☐ ☐ ☐ ☐ ☐ /12.00, 本次测试的提交时间为：2024-10-18, 如果你认为本次测试成绩不理想, 你可以选择 再做一次。

分享

1 单选 (2分) PKI通过引入___解决如何相信公钥与身份的绑定关系的问题。

得分/总分

- A. 数字签名
- B. 密钥共享
- C. SET协议

D. 证书



☐ ☐ ☐ ☐ ☐ ☐

正确答案：D 你选对了

提问

2 单选 (2分) 不属于PKI系统的组件的是___。

得分/总分

- A. 认证服务器AS
- B. CA
- C. RA
- D. 证书发布系统



☐ ☐ ☐ ☐ ☐ ☐

正确答案：A 你选对了

提问

3 单选 (2分) 不属于PKI系统的典型信任模型的是___。

得分/总分

- A. 网状(Mesh)信任模型
- B. 交叉认证
- C. 层次结构信任模型
- D. 社交网络信任模型



☐ ☐ ☐ ☐ ☐ ☐

正确答案：D 你选对了

提问

4 单选 (2分) 关于层次结构信任模型描述不正确的是___。

得分/总分

- A. 对于安全主体(End-Entity) 而言，仅需要信任给它的签发证书的CA或该CA的父节点CA
- B. 根CA有一个自签名的证书



C. 要维护层次结构，在每个CA节点上，需要保存前向证书和后向证书

🔒 □□□□□□

D. 根CA为它每个孩子节点的CA签发证书

正确答案：A 你错选为C

提问

5 单选 (2分) 以下说法不正确的是____。 得分/总分

- A. 无论层次结构信任模型还是交叉认证，要完成证书的验证，都需要证书链上的所有证书的签名验证都通过
- B. RA可作为层次结构信任模型的叶节点
- C. 交叉认证时可能会有路径长度约束
- D. 交叉认证包括单向交叉认证和双向交叉认证

正确答案：B 你选对了

提问

6 单选 (2分) 以下说法不正确的是____。 得分/总分

- A. CRL(证书注销列表)可以通过HTTP方式发布
- B. 没有到期的证书不会被提前撤销
- C. CA有时会发布分段CRL(证书注销列表)
- D. CA有时会发布增量CRL(证书注销列表)

正确答案：B 你选对了

提问



信息安全

智慧课程

认证学习

国家精品

期末不挂科

升级认证学习



学习时长

李景涛

课程进度提醒



评价课程

返回

帮助

单元测试5

本次得分为： /12.00, 本次测试的提交时间为：2024-10-18, 如果你认为本次测试成绩不理想，你可以选择 再做一次。

分享

1 单选 (2分) 关于UNIX密码文件中的Salt，以下说法不正确的是（ ）。

得分/总分

A. Salt可以提高离线字典攻击的穷举空间

B. Salt值是随机数

C. Salt可以重复使用

D. 使用Salt，一个口令字符串的hash值最多可以有2^12种不同的输出

正确答案：C 你选对了

提问

2 单选 (2分) 以下说法不正确的是（ ）。

得分/总分

A. 质询/应答身份认证技术中，可以利用对称密钥加密实现双向认证

B. 基于口令的认证是弱的认证方法

C. 动态口令可以完全避免重放攻击

D. 质询/应答身份认证技术中，质询也可以称为Nonce

正确答案：C 你选对了

提问

3 单选 (2分) _____是构造更复杂的交互式认证协议的基本组件。（ ）

得分/总分

A. 口令

B. 质询与应答

C. KERBEROS协议

D. Needham-Schroeder协议

正确答案：B 你选对了

提问

4 单选 (2分) _____解决了Kerberos协议中的授权问题。（ ）

得分/总分


A. AS

B. 共享的对称密钥



c. 数字证书

D. TGS

 ☐ ☐ ☐ ☐ ☐ ☐

正确答案：D 你选对了

提问

5 单选 (2分) 面哪项是由Needham-Schroeder协议解决的最主要问题？（ ）


得分/总分

A. 密钥分发和认证

B. 保密性和可用性

C. 认证和完整性

D. 保密性和完整性

 ☐ ☐ ☐ ☐ ☐ ☐

正确答案：A 你选对了

提问

6 单选 (2分) 对于身份认证协议最大的威胁是（ ）。


得分/总分

A. 重放攻击

B. 社会工程攻击

C. 穷举攻击

D. 字典攻击

 ☐ ☐ ☐ ☐ ☐ ☐

正确答案：A 你选对了

提问



信息安全

智慧课程

认证学习

国家精品

期末不挂科

升级认证学习



学习时长

李景涛

课程进度提醒



评价课程

返回

帮助

单元测试6

本次得分为： ☐ ☐ ☐ ☐ ☐ ☐ /10.00, 本次测试的提交时间为：2024-10-18, 如果你认为本次测试成绩不理想，你可以选择 再做一次。

分享

1 单选 (2分) 比特币的两个主要支撑技术是（ ）。

得分/总分

A. 区块链和P2P网络



☐ ☐ ☐ ☐ ☐ ☐

B. 账本和匿名性

C. 数字签名和哈希算法

D. 区块链和公开密钥技术

正确答案：A 你选对了

提问

2 单选 (2分) 区块链利用____技术解决了账本完整性需求。（ ）

得分/总分

A. P2P网络

B. 公开密钥技术

C. 可拥有多个公钥

D. 数字签名和哈希算法



☐ ☐ ☐ ☐ ☐ ☐

正确答案：D 你选对了

提问

3 单选 (2分) 区块的区块头中记录着当前区块的元信息，其中前一区块头Hash保障交易历史的完整性，____保障交易本身的完整性。（ ）

得分/总分



A. 前一区块头Hash

B. 区块版本号

C. Merkle树根Hash



☐ ☐ ☐ ☐ ☐ ☐

D. Nonce

正确答案：C 你选对了

提问

4 单选 (2分) 为了维持区块生成速度，区块链被设计为平均每____分钟生成一个新区块，这____需要每隔____个区块定期更新难度值E。（ ）

得分/总分

A. 30, 2016

B. 10, 2016

C. 30, 1024

D. 10, 1024

🔒

□□□□□□

提问

5

单选 (2分)

区块链中运用了什么基础技术来实现隐私保护？ ()

得分/总分

A. 数字签名

B. 公开密钥技术

C. 参与者可拥有多个公钥

D. 哈希算法

🔒

□□□□□□

提问

正确答案： C 你错选为B



期末不挂科



信息安全

智慧课程

认证学习

国家精品

升级认证学习



学习时长

李景涛

课程进度提醒



评价课程

返回

帮助

选择题

本次得分为： 解锁得分情况 /100.00, 本次测试的提交时间为：2024-11-12。

1 单选 (2分) 对于报文M若找到M'使____，即找到碰撞能够构成对哈希函数H的攻击。（）

得分/总分

- A. $M=M'$ 且 $H(M')=H(M)$
- B. $M'\neq M$ 且 $H(M')\neq H(M)$
- C. $M'\neq M$ 但 $H(M')=H(M)$
- D. $M'=M$ 但 $H(M')\neq H(M)$

☐ ☐ ☐ ☐ ☐ ☐

正确答案：C 你选对了

提问

2 单选 (2分) 要找到两个不同的报文x, y, 使 $H(y)=H(x)$, 在计算上是不可行的。则哈希函数H具有（）。

得分/总分

- A. 单向性
- B. 弱抗碰撞性
- C. 强抗碰撞性
- D. 压缩性

☐ ☐ ☐ ☐ ☐ ☐

正确答案：C 你选对了

提问

3 单选 (2分) 发送者使用接收者的公钥加密报文传递给接收者，能实现（）。

得分/总分

- A. 仅保密
- B. 保密且报文鉴别
- C. 保密与部分报文鉴别
- D. 仅报文鉴别

☐ ☐ ☐ ☐ ☐ ☐

正确答案：A 你选对了

提问

4 单选 (2分) 以下的描述中，对报文的数字签名不能实现的是（）。

得分/总分

- A. 保证报文传输过程中的保密性

☐ ☐ ☐ ☐ ☐ ☐



- B. 保护报文的完整性
- C. 验证报文发送者的身份
- D. 防止报文发送者抵赖

正确答案：A 你选对了

提问

5 单选 (2分) 关于UNIX密码文件中的Salt，以下说法不正确的是（ ）。

得分/总分

- A. Salt值是随机数
- B. Salt可以重复使用
- C. Salt可以提高离线字典攻击的穷举空间
- D. 使用Salt，一个口令字符串的hash值最多可以有2¹²种不同的输出

🔒 □□□□□□

正确答案：B 你选对了

提问

6 单选 (2分) 以下说法不正确的是（ ）。

得分/总分

- A. 基于口令的认证是弱的认证方法
- B. 动态口令可以完全避免重放攻击
- C. 质询/应答身份认证技术中，质询也可以称为Nonce
- D. 质询/应答身份认证技术中，可以利用对称密钥加密实现双向认证

🔒 □□□□□□

正确答案：B 你选对了

提问

7 单选 (2分) _____是构造更复杂的交互式认证协议的基本组件（ ）。

得分/总分

- A. 口令
- B. 质询与应答
- C. Needham-Schroeder协议
- D. KERBEROS协议

🔒 □□□□□□

正确答案：B 你选对了

提问

8 单选 (2分) _____解决了Kerberos协议中的授权问题。（ ）

得分/总分

- A. 共享的对称密钥
- B. AS
- C. TGS
- D. 数字证书

🔒 □□□□□□

正确答案：C 你选对了

提问

9 单选 (2分) 下面哪项是由Needham-Schroeder协议解决的最主要问题？（）

得分/总分

- A. 密钥分发和认证

B. 保密性和完整性

C. 认证和完整性

D. 保密性和可用性
- 🔒

□□□□□□

正确答案：A 你选对了

提问

10 单选 (2分) 对于身份认证协议最大的威胁是（）。

得分/总分

- A. 穷举攻击

B. 重放攻击

C. 字典攻击

D. 社会工程攻击
- 🔒

□□□□□□

正确答案：B 你选对了

提问

11 单选 (2分) SSL协议中的_____可以实现客户和服务端之间的相互认证，协商会话的密钥等参数。（）

得分/总分

- A. ssl记录协议

B. ssl握手协议

C. ssl密码变化协议

D. ssl警告协议
- 🔒

□□□□□□

正确答案：B 你选对了

提问

12 单选 (2分) 下面关于SSL/TLS协议，不正确的是（）。

得分/总分

- A. 该协议可以提供的安全服务包括保密性,数据完整性,身份认证

B. TLS与SSL在网络层对网络连接进行加密

C. ssl记录协议使用加密算法提供连接安全性

D. ssl握手协议一般在应用数据传输之前先开始工作
- 🔒

□□□□□□

正确答案：B 你选对了

提问

13

单选 (2分)

SET协议中使用_____技术来秘密传输对称密钥? ()

得分/总分

- A. 双重哈希

B. 数字信封

C. 双重数字签名

D. Merkle哈希树
- 🔒

□□□□□□

正确答案: B 你选对了

提问

14

单选 (2分)

下面关于SET协议，说法不正确的是 ()。

得分/总分

- A. SET是为在线信用卡交易设计的安全协议，不是第三方支付系统

B. SET协议可以保障通信的保密性和完整性

C. SET协议用对称密钥密码解决身份认证问题

D. SET中使用的密码技术包括对称密钥加密、数字签名、数字信封等
- 🔒

□□□□□□

正确答案: C 你选对了

提问

15

单选 (2分)

IPSec协议是在__层实现的安全解决方案。()

得分/总分

- A. 应用层

B. 网络层

C. 数据链路层

D. 传输层
- 🔒

□□□□□□

正确答案: B 你选对了

提问

16

单选 (2分)

比特币的两个主要支撑技术是 ()。

得分/总分

- A. 区块链和公开密钥技术

B. 区块链和P2P网络

C. 数字签名和哈希算法

D. 账本和匿名性
- 🔒

□□□□□□

正确答案: B 你选对了

提问

17

单选 (2分)

区块链利用_____技术解决了账本完整性需求。()

得分/总分

- A. 公开密钥技术

B. 数字签名和哈希算法

C. 可拥有多个公钥

D. P2P网络

正确答案: B 你选对了

提问

18 单选 (2分) 区块的区块头中记录着当前区块的元信息，其中前一区块头Hash保障交易历史的完整性，____保障交易本身的完整性。（）

A. 区块版本号

B. 前一区块头Hash

C. Merkle树根Hash

D. Nonce

正确答案: C 你选对了

提问

19 单选 (2分) 为了维持区块生成速度，区块链被设计为平均每____分钟生成一个新区块，这需要每隔____个区块定期更新难度值E。（）

A. 10, 2016

B. 30, 2016

C. 10, 1024

D. 30, 1024

正确答案: A 你选对了

提问

20 单选 (2分) 区块链中运用了什么基础技术来实现隐私保护？（）

A. 哈希算法

B. 数字签名

C. 参与者可拥有多个公钥

D. 公开密钥技术

正确答案: C 你选对了

提问

21 多选 (4分) 下列哪项不是现代对称密钥加密所经常使用技术？（）

A. 扩散（Diffusion）

B. 扰乱（Confusion）

C. 大数因子分解（Factoring）

提问

D. 哈希（hash）

🔒 □□□□□□

正确答案：C、D 你选对了

提问

22 多选 (4分) 为保证安全性，在设计分组密码时应该考虑以下哪些问题？（） 得分/总分

A. 加密、解密变换要足够复杂

A. 加密、解密变换要足够复杂 🔒 □□□□□□

B. 分组长度要足够大

B. 分组长度要足够大 🔒 □□□□□□

C. 密钥量要求足够大

C. 密钥量要求足够大 🔒 □□□□□□

D. 加密、解密时间要足够长

正确答案：A、B、C 你选对了

提问

23 多选 (4分) 公钥加密体制中，每个用户设定一把公钥，由本人公开，用它进行（）。 得分/总分

A. 加密

A. 加密 🔒 □□□□□□

B. 验证签名

B. 验证签名 🔒 □□□□□□

C. 签名

D. 解密

正确答案：A、B 你选对了

提问

24 多选 (4分) 小李托小王把作业交给老师，小王把作业署名改成自己的，然后交给老师，这破坏了下列哪些安全属性？（） 得分/总分

A. 保密性

B. 完整性

B. 完整性 🔒 □□□□□□

C. 不可抵赖性

C. 不可抵赖性 🔒 □□□□□□

D. 可认证

D. 可认证 🔒 □□□□□□

正确答案：B、D 你错选为B、C、D

提问

25 多选 (4分) C为MAC算法，K为对称密钥，下图所示的加密方案可以提供哪些安全服务？（） 得分/总分

A. 保密性

B. 完整性

C. 认证发送者身份

D. 抗抵赖性

🔒

□□□□□□

🔒

□□□□□□

正确答案：B、C 你选对了

提问

26 多选 (4分) 证书授权中心（CA）的职能有（ ）。

得分/总分

A. 验证信息

B. 识别用户身份

C. 签发数字证书

D. 签发证书撤销列表

🔒

□□□□□□

🔒

□□□□□□

🔒

□□□□□□

🔒

□□□□□□

正确答案：C、D 你错选为A、B、C、D

提问

27 多选 (4分) 以下哪些认证技术是基于加密技术的身份认证？（ ）

得分/总分

A. 质询与应答

B. Unix口令

C. Needham-Schroeder协议

D. KERBEROS协议

🔒

□□□□□□

🔒

□□□□□□

🔒

□□□□□□

🔒

□□□□□□

正确答案：A、C、D 你选对了

提问

28 多选 (4分) 关于Kerberos协议，下面说法中正确的有（ ）。

得分/总分

A. Kerberos协议要求参与方的系统时钟较为精确同步

B. Kerberos是基于可信第三方的安全协议

C. Kerberos协议交互中用到了质询与应答技术

D. 客户机请求获取票据许可票时，AS会生成一个客户机和应用服务器V的会话密钥，并把该密钥加密后发送给客户机

🔒

□□□□□□

🔒

□□□□□□

🔒

□□□□□□

正确答案：A、B、C 你选对了

提问

29 多选 (4分) 下面说法不正确的有（ ）。

得分/总分

A. 使用诸如SHA-1之类的哈希函数来计算数据项的哈希值需要有正确的密钥

B. PKCS标准提供对“在线信用卡交易”的安全保障

C. 哈希函数常与公钥密码配合使用来构造数字签名

D. 哈希函数具有单向性

正确答案：A、B 你选对了

提问

30 多选 (4分) 数字证书内部格式包含的主要内容除了版本信息、证书序列号、证书有效期之外，还包括（ ）。 得分/总分

A. 证书持有者的公钥内容

B. 证书持有者的公钥算法

C. 证书持有者的私钥内容

D. CA的公钥内容

正确答案：A、B 你选对了

提问

31 多选 (4分) 下面哪些属于信息安全的安全技术？（ ） 得分/总分

A. 防火墙技术

B. 漏洞扫描技术

C. 入侵检测技术

D. 防病毒技术

正确答案：A、B、C、D 你选对了

提问

32 多选 (4分) 区块链中运用了哪些技术来实现完整性保护？（ ） 得分/总分

A. 哈希算法

B. 数字签名

C. 对称密钥密码加密

D. Merkle树

正确答案：A、B、D 你选对了

提问

33 多选 (4分) 在一次在线交易中通过SET协议中采用的双重数字签名技术，能够保证（ ）。 得分/总分

A. 商家能看到订单信息原文和持卡人的支付信息原文

B. 商家不能看到订单信息原文和持卡人的支付信息原文

C. 商家能看到订单信息原文，但不能看到持卡人的支付信息原文

🔒 □□□□□

D. 收单银行不能看到订单信息原文，但能看到持卡人的支付信息原文

🔒 □□□□□

正确答案：C、D 你选对了

提问

34 多选 (4分) 下面说法不正确的是（ ）。

得分/总分

A. 密码体制可分为对称密钥密码和非对称密钥密码两种

B. 对称密钥密码体制中，密钥需要在通信开始之前由发送方和接收方实现共享

C. 对称密钥密码算法和非对称密钥密码算法的实现原理一样，只是参与者拥有的密钥数量不一样

🔒 □□□□□

D. 一般情况下，非对称密钥密码比对称密钥密码加密速度更快

🔒 □□□□□

正确答案：C、D 你选对了

提问

35 多选 (4分) 下面关于加密的说法不正确的是（ ）。

得分/总分

A. 加密就是基于数学算法的程序和保密密钥对信息进行编码，生成难以理解的字符串

B. 如果没有加密所用的密钥，知道加密程序的算法也能解开加密的信息
秘密必须全寓于密钥

🔒 □□□□□

C. 秘密必须全寓于密钥

D. 选择密钥和加密算法的原则是：在攻击者不知道加密算法的前提下密文不可能被破解

🔒 □□□□□

正确答案：B、D 你选对了

提问