**可信计算**

1. 选择题  
   1.下列哪一个为身份认证密钥的英文简写（ B ）  
   A.EK  B.AIK  C.LK  D.AK

2.下列哪一个不是静态信任链的运行特点( D )  
A.以CRTM为可信根  
B.平台的一次运行对应于一个信任链，一个起点一个终点  
C.一旦平台进入不可信状态，从信任链角度，平台以后的所有状态都是不可信的  
D.主要采用DRTM技术

3.远程证明过程不包括哪个阶段（ D ）

A .完整性度量

B.完整性报告

C 完整性测评

1. 完整性验证

4.下面哪个不是可信计算平台的可信根（ C ）

A.可信度量根

B.可信报告根

C.可信反馈根

D.可信存储根

5.基于信任链的可信计算机模块的启动顺序是（ B ）

A.行为监测模块—身份认证模块—加密模块—数字签名模块BIOS

B.身份认证模块—行为监测模块—加密模块—数字签名模块BIOS

C.行为检测模块—加密模块—身份认证模块—数字签名模块BIOS

D.身份认证模块—加密模块—行为监测模块—数字签名模块BIOS

6. 信任不可以是（ C ）的关系

A.一对一 B.一对多 C.多对一 D.多对多

7.下列哪一选项关于可信计算是正确的（ D ）

A. 可信计算的核心思想是软件安全模块支持下的可信计算平台

B. 可信计算平台由可信链、 硬件平台、操作系统和应用系统组成

C. 可信计算不能从根本上阻止病毒和黑客等软件的攻击。

D. 可信计算可以用来打击在线游戏作弊。

解析：

A. 是硬件 P7

B. 可信计算平台由可信根、 硬件平台、操作系统和应用系统组成。 P7

C. 确保系统具有免疫能力,从根本上阻止病毒和黑客等软件的攻击。 P8

D. 可信计算可以用来打击在线游戏作弊。P12

8.基于密钥的身份认证协议中，引入时间戳可以( B )。

A.实现时钟同步.  
B.防止重放攻击  
C.防止中间人攻击  
D.防止窃听

9.在以下认证方式中，最常用的认证方式是（ A ）。

A.基于账户名/口令认证

B.基于摘要算法认证

C.基于PKI认证

D.基于数据库认证

10.下列哪些算法不能用于数字签名算法? （ D ）

A. DSS/DSA B.RSA C.EIGamal D.RC5

11.管理数字证书的权威机构CA是( D )。

1. 解密方  
   B.加密方
2. 双方  
   D.可信任的第三方

12. 哪个不是TCG制定规范中定义的可信计算的属性？( D )

A可鉴别性 B完整性 C私密性 D真实性

13.TPM密钥的身份证明密钥（AIK）的目的是替代（ B ）来提供平台的证明。

A．存储密钥 B. 背书密钥

C．签名密钥 D. 绑定密钥

14.（ C ）不由TSS核心服务（TCS）模块提供。

A．密钥和证书管理 B. 事件管理

C．TSP上下文管理 D.审计管理

15.以下关于公钥基础设施(PKI)的说法中，正确的是( A )

A.PKI可以解决公钥可信性问题

B.PKI不能解决公钥可信性问题

C.PKI只能有政府来建立

D.PKI不提供数字证书查询服务

16.以下关于可信计算说法错误的是:( D )

A.可信的主要目的是要建立起主动防御的信息安全保障体系

B.可信计算机安全评价标准(TCSEC)中第一次提出了可信计算机和可信计算基的概念

C.可信的整体框架包含终端可信、终端应用可信、操作系统可信、网络互联可信、互联网交易等应用系统可信

D.可信计算平台出现后会取代传统的安全防护体系和方法

17.以下关于可信存储根管理功能包含以下（ D ）

A.密钥管理

B.密钥产生

C.加密和解密

D.以上都是

18.MD5文摘算法得出的文摘大小是？（ A ）  
A 128位   B 160位  C 128字节  D 160字节

19. 构建可信计算平台的基础模块是（ A ）  
A. 安全启动系统  
B. 可信平台模块  
C. 安全协处理器  
D. 密码加速器

20.在TSS中，以下哪些不是可信核心服务层TCS提供的核心服务？ （ C ）

A.上下文管理 B.密钥与证书管理 C.设备驱动管理 D.事件管理

21.下列哪一项不是TPM的核心功能（ C ）

A.远程证明 B.数据保护 C.储存器屏蔽 D.密钥管理

**二、填空题**1.TPM部件体系结构可包括为:分离部件、通信接口、防篡改攻击封装 三大类。

2.可信计算的发展阶段：硬件可信阶段、综合可信阶段、深入发展阶段。

3.可信机制分为可信度量机制、可信存储机制、可信报告和可信认证机制。

4. 一个CA创建的凭证通常称为认证密钥证书。

5. 可信计算的核心问题可以归结为 信任问题 。 P7

6. 在可信计算平台中，一般有24个PCR寄存器。每个寄存器都存储特定的散列值0到7用于系统启动，8到15给操作系统使用，16到23用于动态可信根的建立

7. Diffie-Hellman算法是第一个公钥算法。

8. 信任链分为静态信任链和动态信任链。

9. 平台身份证明分为Privacy CA方案和DAA方案

10.CA是PKI的核心执行机构，是PKI的主要组成部分，业界人士通常称他为 认证中心 。

11.信任链的核心和起点是 计算机可信根 。

12.数字证书是将证书持有者的身份信息和其所拥有的公钥进行绑定的文件。

13.身份信任采用静态验证机制，常用的技术包括认证、授权、加密等。

14.在TSS结构体系中，TPM设备驱动库（TDDL）以 用户 模式运行

15.可信计算平台通用体系架构分为3个层次：基础硬件层、可信服务层、安全应用层。

16.公钥基础设施(PKI):是一个用非对称密码算法（或公钥密码)原理和技术来实现并提供安全服务的、具有通用性的安全基础设施。

17.TPM安全管理密钥的生成、使用和存储，包括背书密钥、存储密钥、签名密钥、身份证明密钥、绑定密钥、继承密钥、验证密钥。

18.TPM可信平台模块，本身是一种 SOC 芯片，是可信计算平台的 信任 根。

**三、判断题**

1.信任可以分为身份信任和直接信任两部分。（×）

2.每个TPM拥有唯一的EK 。 （√）

3.可信机制是保障可信计算平台安全可行的机制。（√）

4.一个实体如果它的行为总是以预期的方式，达到预期的目标，则这个实体就是可信的。 （√）

5.可信强调行为结果可预期，但并不等于确认行为是安全的。（√）

6.TPM密钥的签名密钥是对称密钥。 （ × ）

7.远程证明是通过“挑战”-“应答”协议来实现的。 （ √ ）

8.公钥基础设施时刻一个用非对称密码算法原理和技术实现的、具有通用性的安全基础设施。（√ ）

9.TSS模块中，TSP（可信服务提供者）的功能是提供公共服务的集合。（×）

（正确功能应该是本地和远程的可信代理，位于书P51）