一、填空题

1. 一个可信平台必须包括三个可信根：**可信度量根，可信存储根，可信报告根**。

2. 平台证明引入了**AIK**对**PCR值**和**随机数N**在TPM的控制下的签名，保证了平台配置信息的**完整性**和**新鲜性**，从而大大提高了通信的**安全性**。

3. TPM只允许两种操作来修改PCR的值：**重置操作和扩展操作**。

4. **RTM**是平台启动时首先执行的一段程序，它是由**CRTM**控制的计算引擎。

二、选择题

1. 可信计算的安全属性不包括：（**B**）

A．可鉴别性。B. 可视性。C．完整性。D. 机密性。

2. 可信计算中，一次度量就是一个度量事件，不包括如下度量事件：（ **A**）

A．完整性报告。B. 嵌入式数据。C. 程序代码的特征值。D. 被度量值的散列值。

3. TCG认为可信平台不包含的可信根是：（**C**）

A. RTM B. RTS C. PCR D. RTR

4．下列说法正确的是：（**ABD**）

A．RTR由TPM芯片中的PCR和背书密钥组成。

B. EK可用于创建TPM的拥有者。

C. RTS不包含PCR。

D. EK可用于创建AIK及其授权数据。

5．下列可信根中包含PCR：（**BC**）

A. RTM。B. RTS。C．RTR。D. SRK。

三、简答题

1. 详细分析PCR在TPM所起到的作用。

**PCR是TPM内部的平台配置寄存器，大小只有160bits用于存储组件的散列值，将散列值同期望值比较，就可以维护组件的完整性。TPM只允许两种操作来修改PCR的值:重置操作和扩展操作。重置操作发生在机器断电或者重新启动之后，PCR的值自动重新清零（但TCG 1.2新引入的寄存器除外）。只能通过扩展操作来改变PCR的内容。扩展操作是不可交换的，即先扩展度量值A再扩展度量值B所得到的PCR值跟先扩展B再扩展A的结果是不同的。理论上PCR能够记录一个无限长的度量值序列,这个度量值序列反映了系统状态的变迁。如果扩展序列中的某个度量值被改变了,那么后续的度量序列都会受到影响。**

2. 简述可信计算中的信任根。

**可信根是系统的安全基础也是安全起点，在可信网络环境中所有安全设备都信任该可信根。可信应用将会从下层获得安全支撑，而非可信应用可以运行于可信系统之上，但不能获得安全支撑。**

**可信计算中包含可信度量根（RTM）、可信存储根（RTS）、可信报告根（RTR）三个可信根：**

**RTM是平台启动时首先执行的一段程序，它是由CRTM控制的计算引擎。在理想状态下，CRTM存储在TPM内部，但根据实现的需要，它可能需要加载到其他固件中，如：BIOS；**

**RTS由TPM芯片中的PCR和存储根密钥组成。处于密钥树根部的密钥是最高级存储密钥，即存储根密钥SRK，它是2048位的RSA密钥对，主要用于对由TPM使用，但存储在TPM之外（如：硬盘）的密钥进行保护。同时，它作为父密钥对其子密钥进行加密保护；**

**RTR由TPM芯片中的PCR和背书密钥组成。EK仅用于以下两种操作：一是创建TPM的拥有者；二是创建AIK及其授权数据。**

3. 可信计算的基本功能是什么？

**验证用户的身份:验证使用者的合法身份，可以使用该系统；**

**验证平台软硬件配置的正确性:使用者可以信任平台的运行环境，软硬件配置没有问题；**

**验证应用程序的完整性和合法性:在平台上运行的应用程序是可信的，是正版软件且未受破坏；**

**平台之间的可验证性:在网络环境下运行的多个平台之间是可以相互信任的，即这些平台本身各自可信，且可以合法地相互访问，相互通信不存在安全问题；**