**集美大学计算机工程学院实验报告**

|  |  |  |
| --- | --- | --- |
| **课程名称**： 嵌入式系统应用 | **班级**：计算2114 | **实验成绩**： |
| **指导教师**： 刘晋明 | **姓名**： 庄佳强 |  |
| **实验项目名称**： 可信计算验证 | **学号**： 202121331104 | **上机实践日期**：5.30 |
| **实验项目编号**： 008 | **组号**：001 | **上机实践时间**： 5.30 |

**一、实验目的**（本次实验所涉及并要求掌握的知识点）

1. **实验内容与设计思想**（设计思路、主要数据结构、主要代码结构、主要代码段分析、电路图等）

**2.4.3检验可信计算模块是否被操作系统识别**

**2.4.4查看可信计算模块的错误详情**

**2.4.5获取可信计算模块的内部随机值**

**2.5.1-基于主密钥的 context 创建子密钥**

**2.5.2基于主密钥创建带有口令的子密钥**

**2.5.3解密封装的加载数据**

**2.5.4基于对称密钥的上下文对数据加密和解密**

**2.5.5可信计算模块非对称加密解密实验**

**2.5.6使用可信计算模块签名**

**2.5.7使用可信计算模块进行签名及验**

**2.6.1查看可信计算模块内部PCR值**

**三、实验使用环境**（本次实验所使用的平台和相关软件）

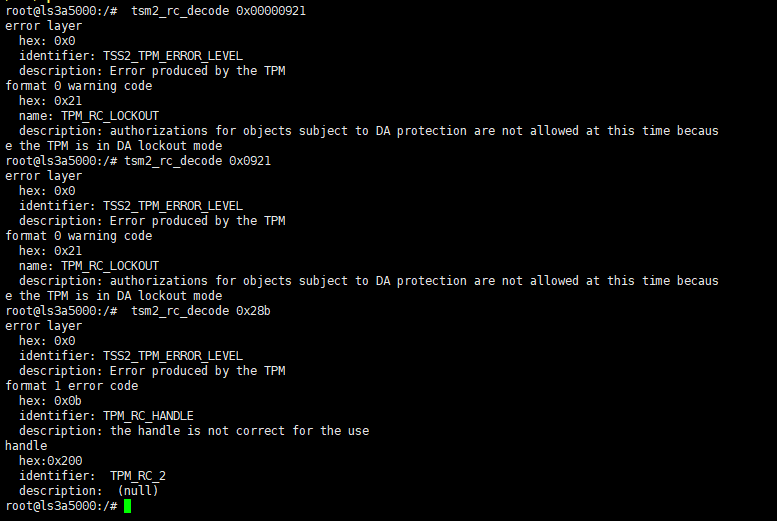
龙芯平台，可信模块，Putty,Windows11

**四、实验步骤和调试过程**（实验步骤、测试数据设计、测试结果分析）

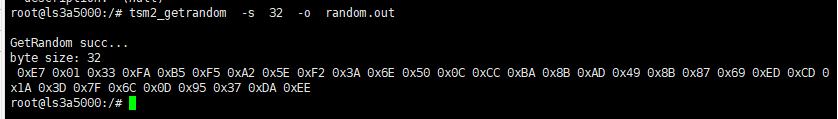
**2.4.3检验可信计算模块是否被操作系统识别**

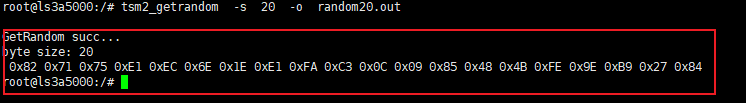


**2.4.4查看可信计算模块的错误详情**



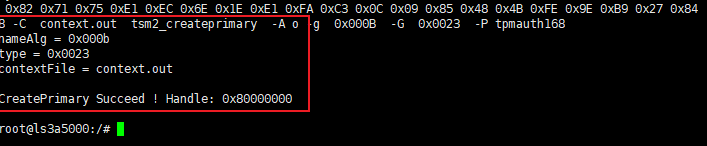
**2.4.5获取可信计算模块的内部随机值**



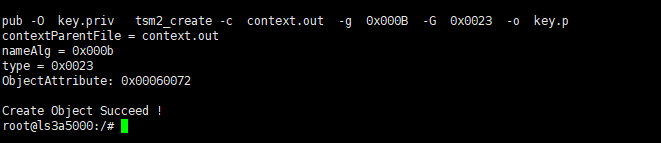


**2.5.1-基于主密钥的 context 创建子密钥**

建立主密钥

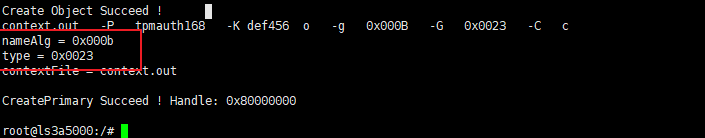


生成子密钥



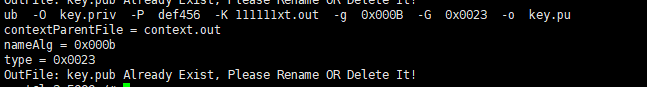
**2.5.2基于主密钥创建带有口令的子密钥**

生成主密钥

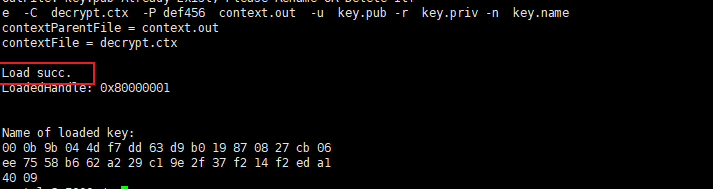


生成子密钥

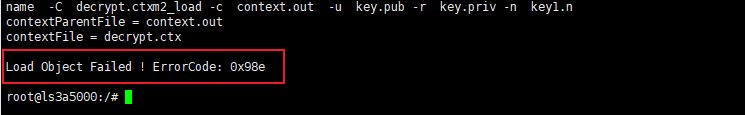
已经存在。



使用主密钥的口令时，可以加载到 TCM



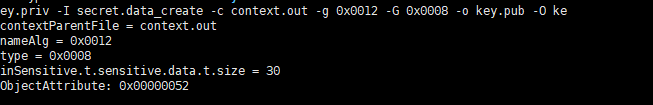
使用口令可以正确的生成。

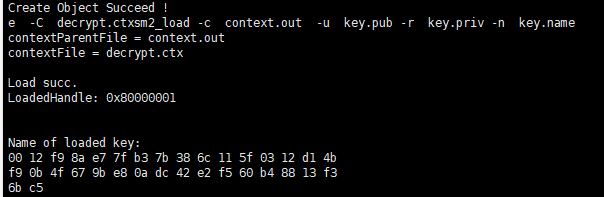


若口令不正确，无法正确生成。

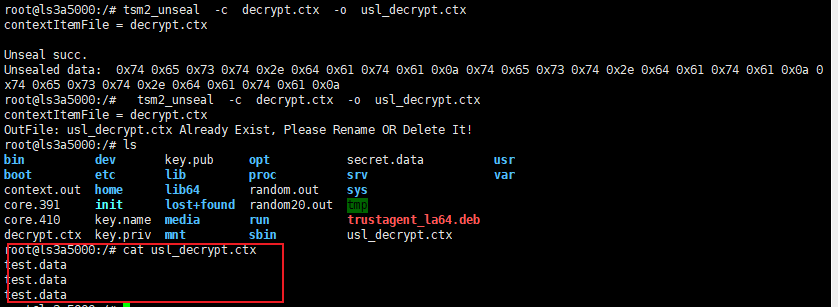
**2.5.3解密封装的加载数据**

封装数据



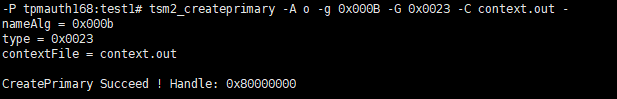


解密数据

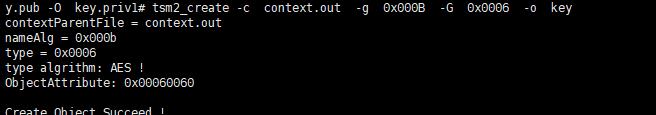


**2.5.4基于对称密钥的上下文对数据加密和解密**

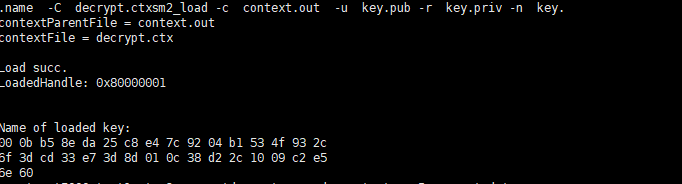
主密钥



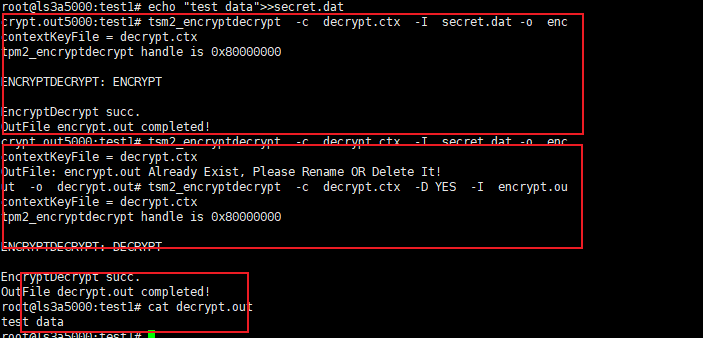
子密钥



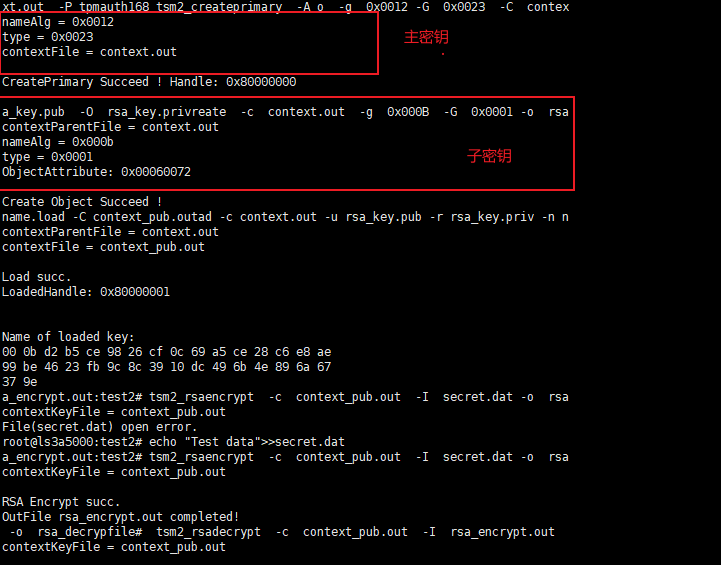
获得上下文

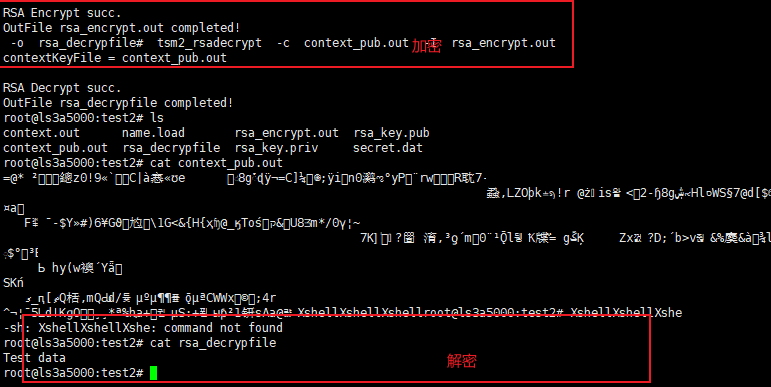


进行加密和解密

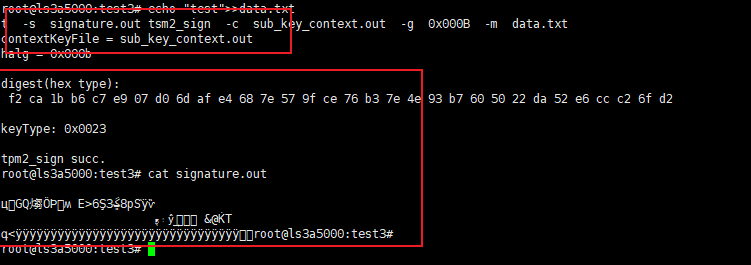


**2.5.5可信计算模块非对称加密解密实验**





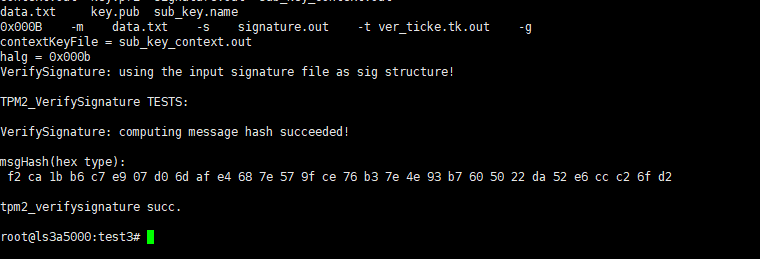
**2.5.6使用可信计算模块签名**

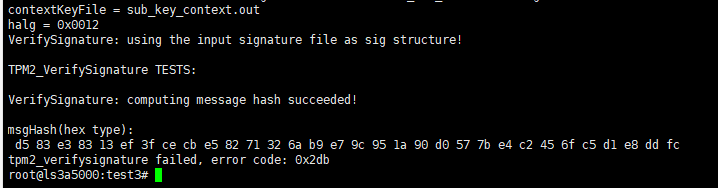


**2.5.7使用可信计算模块进行签名及验证**

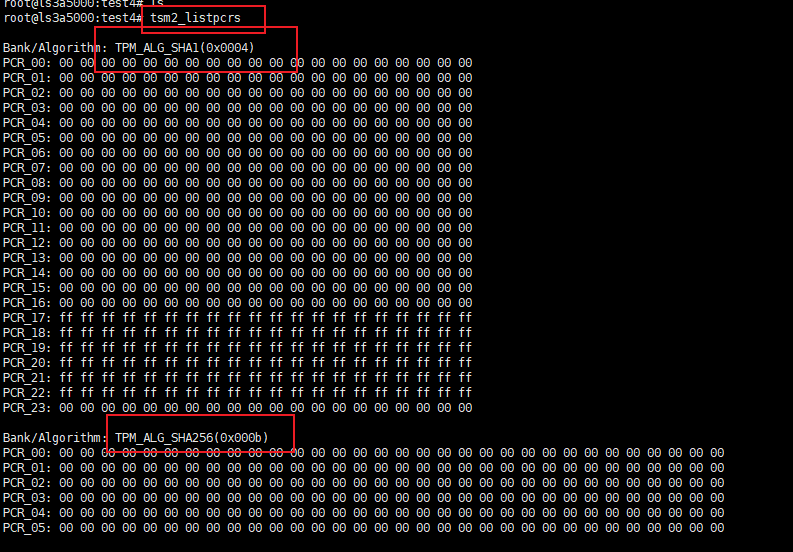
签名之前进行过了。

验证签名。





**2.6.1查看可信计算模块内部PCR值**



2.6.2下课了，先做到这里吧。

1. **实验小结**（实验中遇到的问题及解决过程、实验中产生的错误及原因分析、实验体会和收获）

在进行可信模块实验的过程中，复习了相关理论知识。我逐渐熟悉了TPM的基本操作。随后，通过生成和存储密钥、数据加密解密、数字签名验证等功能验证实验，我确认了TPM的主要功能和实际效果。在进行安全性测试时，如抗攻击性测试和密钥管理安全性测试，我评估了TPM的安全性能。整个实验过程中，我不仅掌握了TPM的配置与使用方法，还对其在实际应用中的效果有了深入认识，并总结了在信息安全中的重要作用和潜在应用场景。