**广州大学学生实验报告**

**开课学院及实验室：**网络空间安全学院 **2023年2月22日**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **学院** | 网络空间安全学院 | **年级/专业/班** | 网安211 | **姓名** |  | **学号** |  |
| **实验课程名称** | 操作系统及安全分析 | | | | | **成绩** |  |
| **实验项目名称** |  | | | | | **指导**  **老师** |  |

1. 实验目的
2. 选择一门语言（C、Python、Java等），熟悉DES和AES密码库的使用；
   1. 使用DES算法CBC模式，通过以下参数产生密文（m均不包含双引号，并验证密文是否为c = cffffa20a73c667b45fec867850a70a382dad87e90ef16a1。

m = ”today\_is\_tuesday”

key = 0x0011223344556677

iv = 0x7766554433221100

* 1. 使用AES算法CBC模式，通过以下参数产生密文（m均不包含双引号，并验证密文是否为c = 6d8e688ec4104ede9e925f49df4eaf79dd829c5b64052aa46a72a202d35b6f1d。

m = ”today\_is\_tuesday”

key = 0x00112233445566770011223344556677

iv = 0x77665544332211007766554433221100

1. 验证以下哪些密钥是DES的弱密钥或半弱密钥？不考虑校验位：

0x0000000000000000 0x00FF00EFF0FF00FF

0x00FF00E100FF00FF 0xE1E1E1E1F0F0F0F0

1. 实验内容

（1）安装；

（2）熟悉Linux常用命令；

（3）安装gcc编程开发环境；

（4）练习使用gcc编译C程序并执行。

1. 实验过程及结果
2. 实验总结