

“网络安全综合实验（I）”实验报告

**题目： 加密与解密实验**

院 系 网络空间安全学院

专业班级 信安1901班

姓 名 李欣宇

学 号 U201911658

日 期 2020 年 12 月

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 评分表 | 加密与解密实验报告评分 （50分） | | | | 完成（50分） | 成绩 | |
| 评分 项目 | 过程 | 分析与小结 | 撰写 | 创新 | 完成任务 | 合计 | 教师 |
| 分值 | 20 | 20 | 5 | 5 | 50 | 100 | 签名 |
| 评分 |  |  |  |  |  |  |  |

报告要求及评分规则

1.请按照模板给出的格式，包括行距、字体、段落格式等，完成报告；

2.报告封面保持一致(如实填写基本信息及完成日期)；

3.实验报告内容应包括：封面、评分规则、实验过程记录、实验问题分析与总结、参考文献及资料列表；

4提交：电子材料应包括本实验电子版（doc）、实验参考文献资料的电子资源文件（pdf）。

5.主要考察能力： 实验动手能力、问题分析与归纳能力、文档规范撰写能力、创新能力；

6.其他要求：可按各指导老师要求的时间和提交方式提交；每次课实验报告可以单独提交；如果需要最终纸质报告的，可去掉模板中说明文字（斜体）之后，双面打印；

7.总评分=课程每次实验分数之和/课程实验次数。

其中：

每次实验分=实验完成分（50分）+实验报告分（50分）-扣分+加分；

计算方法：

实验完成分=（完成任务数量/总任务数量）\*50；

实验报告分=以下1-4项合计；

1）过程（要求：实验过程完整、清晰）(满分20)（优秀：18+ 良好：16+ 一般：14+）；

2）问题分析与小结（要求：有条理、细致）（满分20）（优秀：18+ 良好：16+ 一般14+）；

3）撰写（要求：语句通畅、格式规范）（满分5）（优秀：4+ 良好：3+ 一般：2+）；

4）创新（要求：见解独到、有创意）（满分5）（优秀：4+ 良好：3+ 一般：2+）；

扣分=报告迟交天数\*2分（满分10分）  （发现雷同抄袭的内容，该次实验不得分）；

加分=搜集整理与实验相关的学习资料作为附件，资料能帮助同学更好掌握相关知识的；获得同组人互评优秀的；提交最终报告时间为班级前3名。（满分5分）（项数\*1分）；

同组评价：

本实验中你的同组人姓名： 刘颖 学号： U201911663

你给同组人评价： 优 （优 良 中 及格）；

理由： 善于思考，合作意识较强，知识储备和信息检索能力强。

# 

# 加密与解密实验

## 实验环境及要求

### 实验平台及说明

虚拟机：Vmware 15或者VirtualBox；

操作系统：虚拟机内安装kali Linux；

已安装：kali Linux虚拟机；按实验一，启动mysql、apache2,ssh服务；

其他配置：实验中主机IP 192.168.155.1 ；

**实验分组**

本实验2人一组，同组成员： 李欣宇 、 刘颖 ；

### 实验场景设置

2022年秋天，上次你为了减少损失而撤销了Bob对Galaxy数据库的访问权限，并对数据进行了保护。Bob学会使用系统中的工具，发现了系统的一些不安全因素，并提醒你注意；另外，你被派往芝加哥出差，公司要求你和Bob远程通信时，采取一些安全防护技术，比如文件加密、邮件加密等，保障公司信息不被泄露；

## 过程记录/实验任务（共10个任务，25个小关卡）

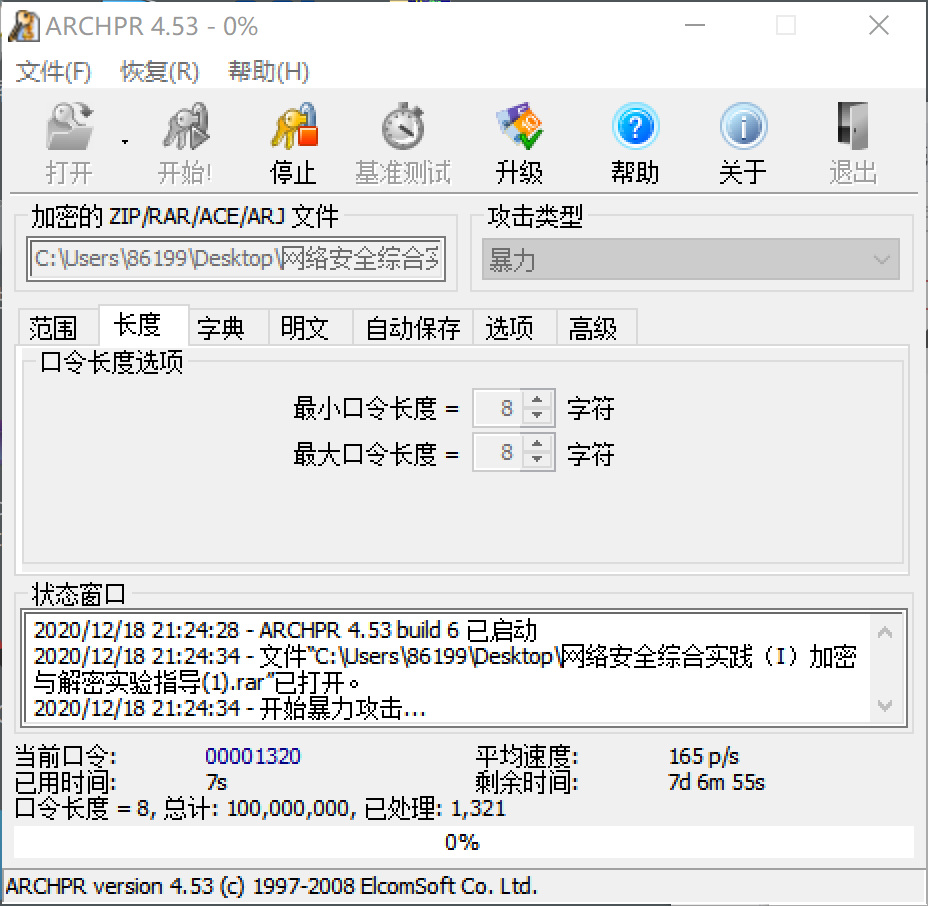
* + 1. **任务1 达芬奇密码**

**1）密码恢复**

公司内部用于培训数据的资料（指导手册），被压缩软件加上了密码进行了保护，这个文件是已经辞职的管理员留下的，你安排Bob想办法恢复文件的内容。样例可以从网络环境中获取，格式如：XXXX.rar。采用工具Advanced Archive Password Recovery（ARCHPR）对该zip文件破解：

**过程记录:**

根据提示信息Call the Hospital ，考虑校医院电话，开头为87，长度为8，暴力破解。



* + 1. **任务2 友谊的小船**

**2）互换文件破解**

同组两位同学，各自压缩并设置密码保护某文件，相互交换后，尝试破解；

**过程记录:**

同伴发来code.zip带密码压缩包，使用ARCHPR暴力破解，时间较长



**3）强度削弱**

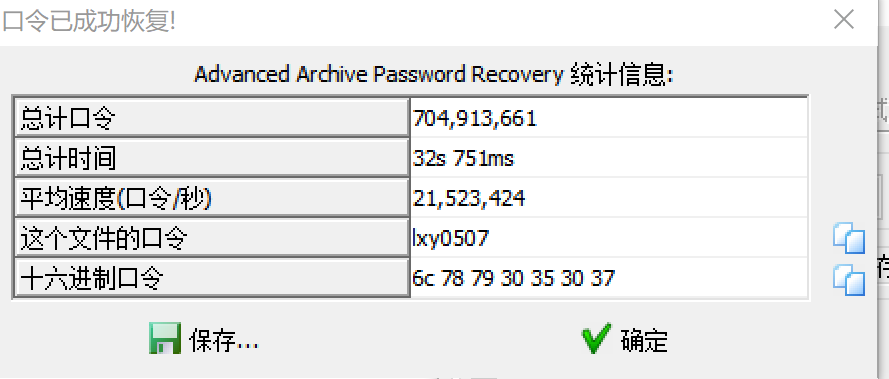
如果10分钟后，某一方未能完成任务2，请对方给出提示，记录对方给出的提示。

**过程记录:**

提示：以该口令的长度为结尾，选取范围为36个字符

根据提示，使用掩码破解，从???4 开始尝试，逐次增加位数到??????7 ，最终破解的口令为lxy0507





* + 1. **任务3 好记性不如烂笔头**

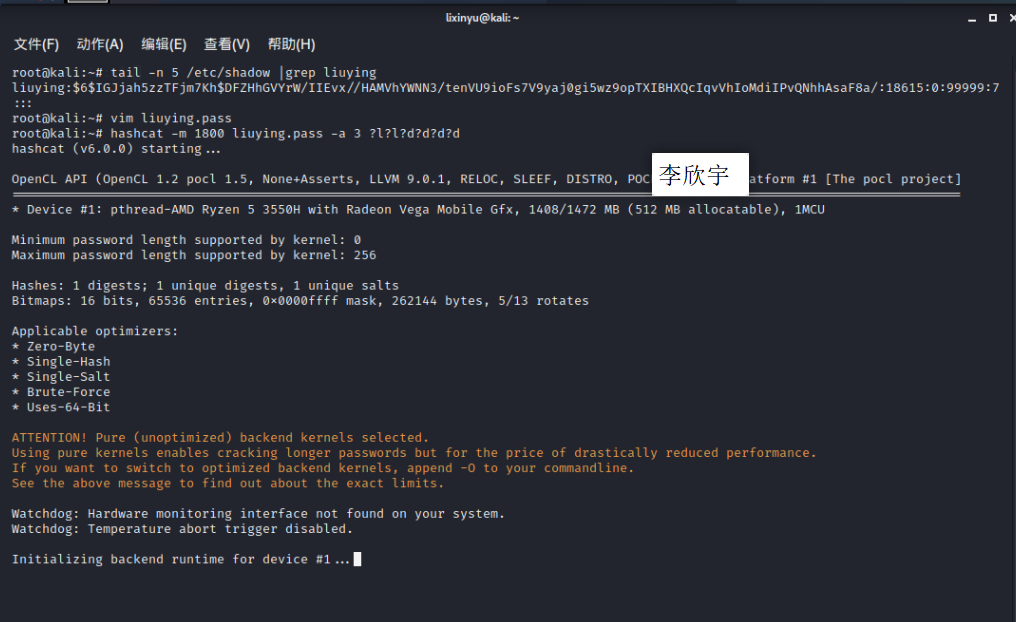
口令恢复：还记得前面Linux基础实验任务1.2.3中，kali系统里，增加了用户Bob吗？假设Bob自己登录系统后，修改了自己的密码；但因为太长时间没有登录系统，Bob不慎遗忘了以前的密码。如果Bob希望找回原始密码，Kali系统有这项功能吗？你能帮助Bob找回密码吗？完成以下关卡（不是重置密码）。

**4）获取密文**

从虚拟机中/etc/shadow中获得该同学用户密码的密文。

**过程记录:**

使用 tail -n 5 /etc/shadow |grep liuying 获得liuying 用户的密码密文



**5）暴力破解**

使用kali中的Hashcat工具，直接用掩码模式，尝试暴力破解。

如果破解5分钟，还没有结果，记录保存当时的状态截图，记录如下：

之后，再尝试用字典破解。

**过程记录：**

暴力破解几分钟无结果



**6）生成字典**

请同组成员，给出提示信息，记录提示信息：

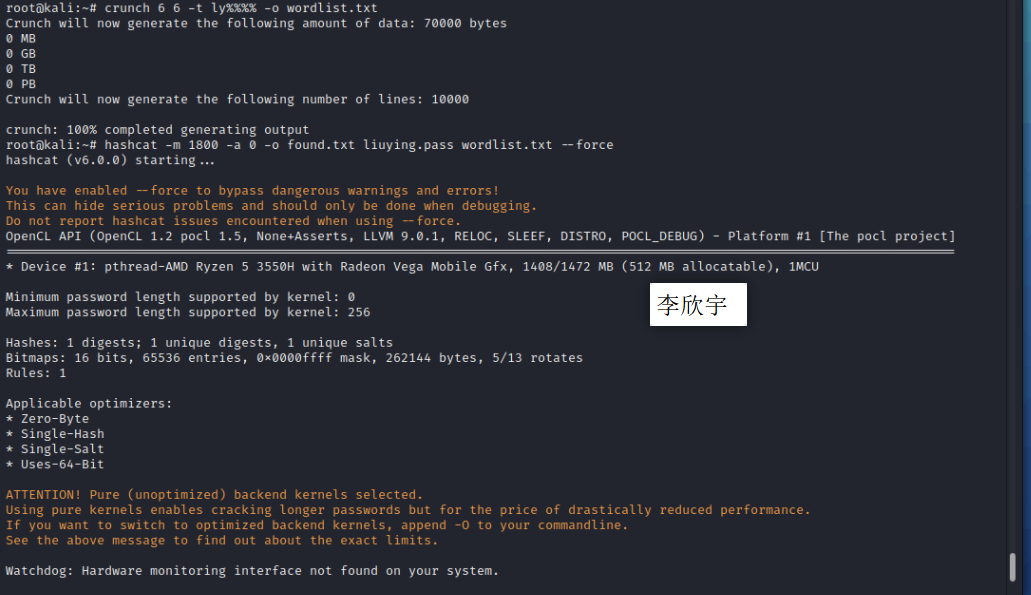
前两个字母为同伴名字首字母，后四位为数字

根据提示信息，使用字典的工具：crunch，生成字典。

**过程记录：**

1）使用crunch 6 6 -t ly%%%% -o wordlist.txt 生成字典存储在woordlist.txt 中

2)再次使用hashcat借用字典暴力破解，成功得到口令，在found.txt中查看为ly2001







**7）用字典继续完成破解**

如果5分钟不能破解成功，先保存截图，然后请对方给出更多提示信息，再尝试。

**8）独立思考**

回答问题：hashcat能否破解前面数据库实验中你进行保护的部分密文字段信息吗？假如你用MD5、AES加密了某些字段。

填写你的答案： 只能破解MD5加密的字段，不能破解AES加密的字段

你同组人同意吗？ 同意

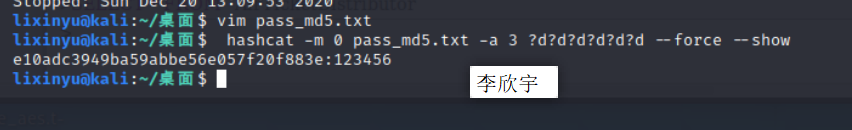
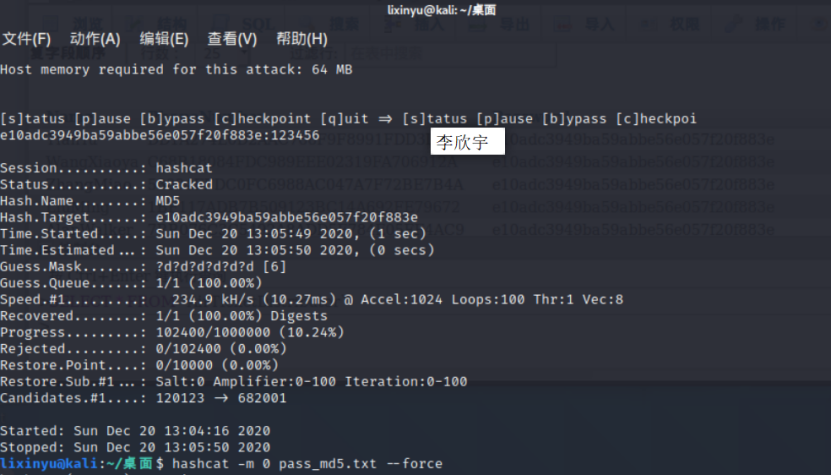
尝试用前面的工具，进行实验，证明你的想法并记录：

**过程记录：**

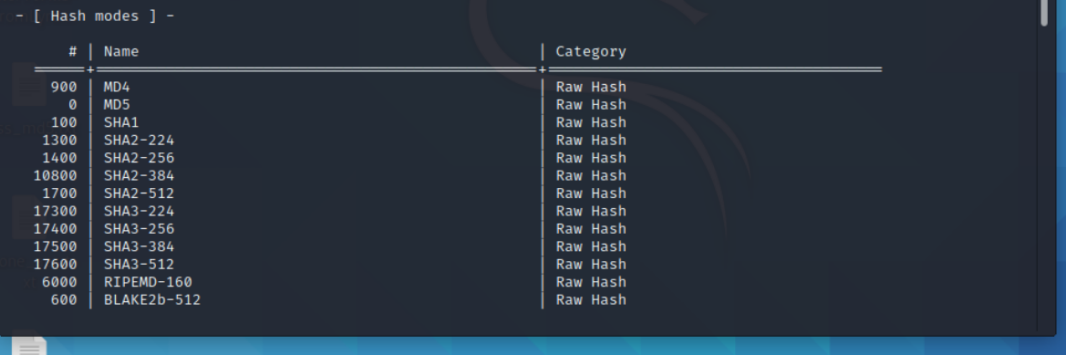
1）去上一次实验备份数据库中的一组数据，以TianYu这一商户为例，分别将加密后的PhoneNumber和Password放入phone\_aes.txt和pass\_md5.txt中。

NX69Q37~LS08541G9Y9MJQA

2）查阅相关hashcat的资料，使用以下命令对password进行解密，过程与结果如下，得到的口令是123456

****

3）通过查阅hashcat -h ，其中的hashmode并无与aes相关的，故不能对aes加密的字段进行解密。

****

* + 1. **任务4 十八般兵刃**

天下安全，唯密不破（防护）；

从前面的过程中，你应该发现了安全中的一些问题或者原则。现在需要用更强大的工具，对一些内容进行安全防护。掌握好openssl及密码算法的名称。

openssl 使用

**9）查看已安装的openssl版本**

通过命令查看并记录版本信息。

**10）查看帮助**

查看openssl联机帮助，了解其功能。

查看帮助后，回答问题：openssl命令分为哪几类命令？

1、Standard commands ；

2、Message Digest commands ；

3、Cipher commands ；

**过程记录：**

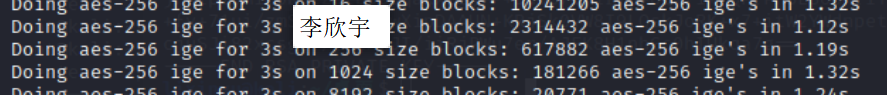


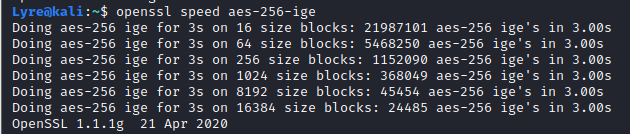
**11）加密速度测试** Benchmarking

对比一下你机器使用openssl加密的速度与你同伴的差异，记录两台主机的配置，虚拟机的配置，同一种算法的速度：

**过程记录：**

以下速度依次为本机与同伴的





以下本机和虚拟机配置分别为本机与同伴的





* + 1. **任务5 Digest摘要算法**

**12）被篡改了吗？**

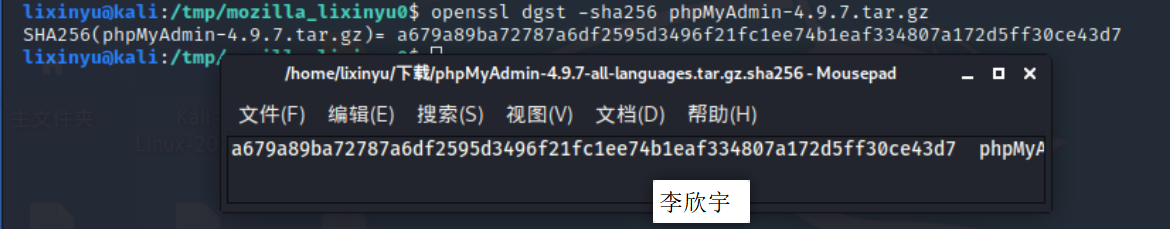
从课程群下载的linux是官方发布的正式版吗?有没有被篡改过？想办法利用openssl来检测一下，说明你测试的过程和结果。

**过程记录：**

在phpmyadmin官网下载4.9.7版本和对应的sha256的摘要

使用openssl dgst -sha256查询包的摘要值，看是否被篡改。

该文件未被篡改。



**13） Shell编程**

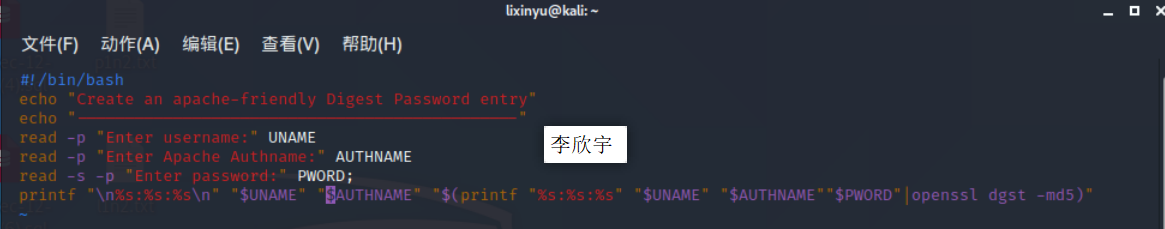
尝试写一个模拟登录过程的脚本：

用vim或其他编辑器写个shell脚本，功能：读取用户键盘输入的姓名、密码、认证串三个符号串参数，然后用openssl命令，计算输入的三项内容对应的md5摘要值，输出到控制台屏幕上。想办法运行你的脚本文件，输入你自己的姓名等信息，创建摘要并记录结果。

运行并测试你写的脚本，总结你的发现。

**过程记录：**

shell脚本与运行结果如下

****



* + 1. **任务6 Symmetric cryptography对称密码**

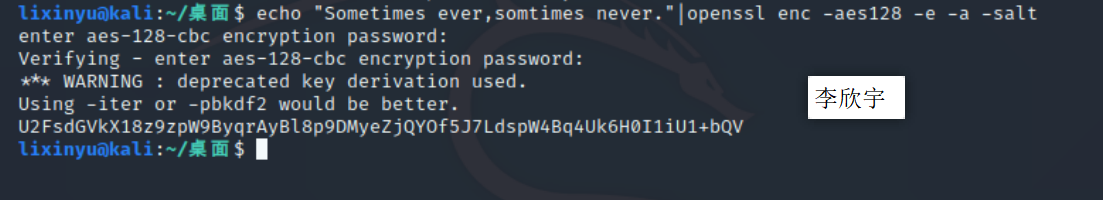
**14）对称密码加密/解密字符串**

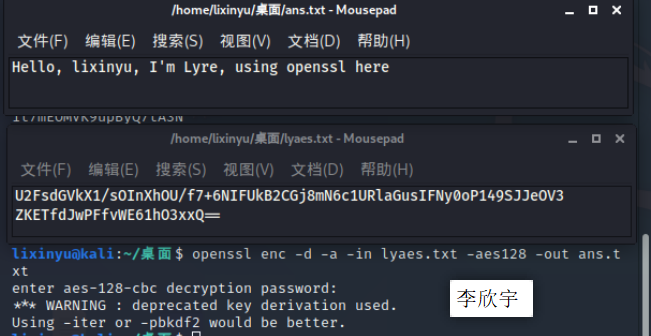
和你的同伴约定好通讯的方法之后，请你的同伴，利用课程的群，发一条用openssl加密信息串，你解密它，并记录结果；

**过程记录：**

1）使用aes128加密，密钥为-abc

2）解密同伴给的密文，密钥为??!，结果如下截图

****



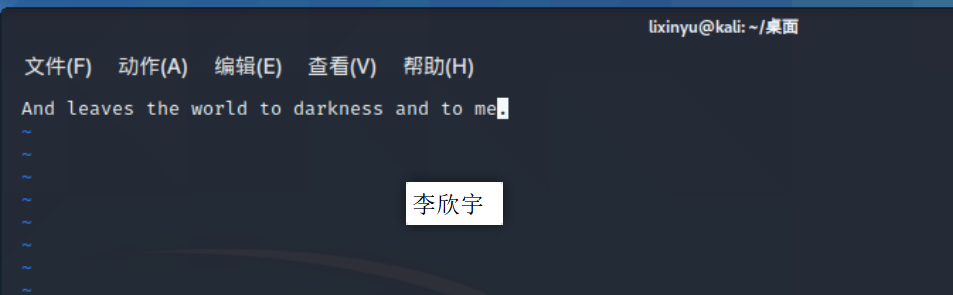
**15）加密文本**

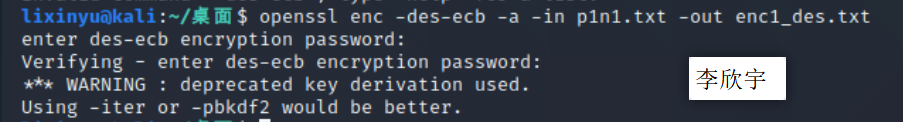
与14类似的方法，但换一种加密算法，传递一个简短的文本文件，并记录收到的密文、解密出来的明文内容：

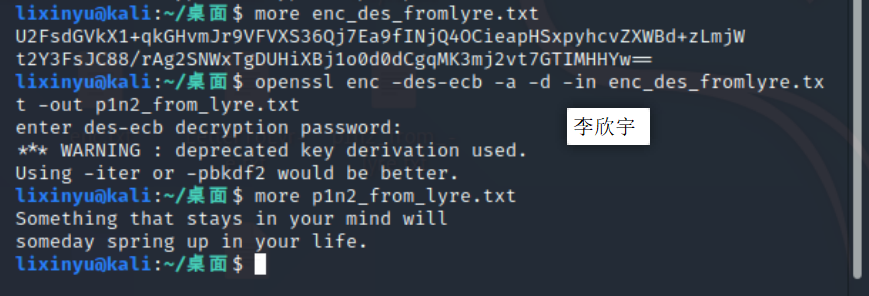
**过程记录：**

1）使用aes256加密，加密内容为And leaves the world to darkness and to me.存储在p1n1.txt中 密钥为-abc，密文存储在enc1\_des.txt中

2）使用openssl enc对同伴传来的密文进行解密，密钥为on，解密出来的明文内容为”Something that stays in your mind will.someday spring up in your life.”





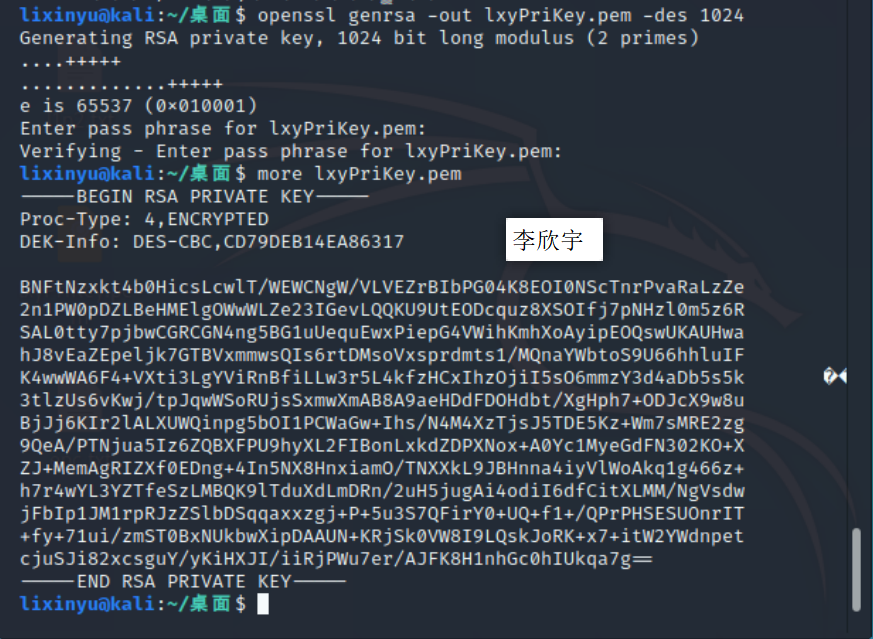


* + 1. **任务7 Asymmetric cryptography非对称密码**

**16）生成私钥**

生成一个私钥，保存到文件 lxyPriKey.pem中

**过程记录：**

**

**17）加密文件**

利用openssl加密一个文件。

**18）解密文件：**

利用openssl解密一个文件。

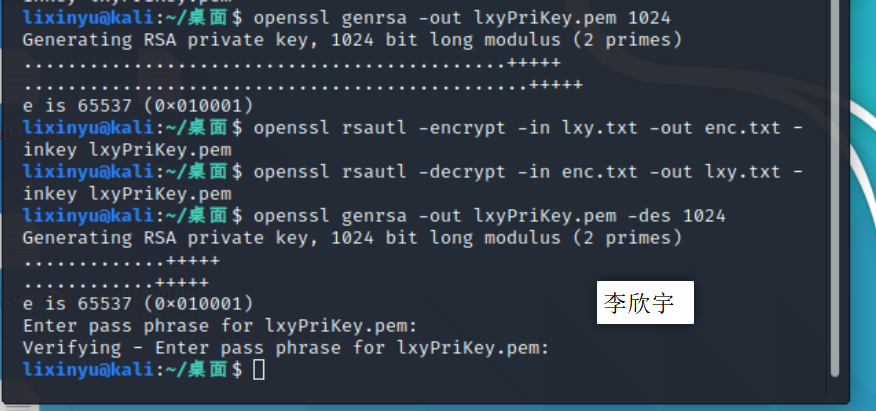
**19）保护密钥**

现在的问题，你的密钥文件包含的私钥，没有任何保护，任何人如果取得，都可以使用；所以需要加密存放密钥文件本身。请生成rsa私钥并选一种密码算法，保护你的私钥。可以选DES、DES3、IDEA、AES128、AES192、AES256。

**过程记录：**

1）使用openssl根据私钥加密、解密一个文件

2）使用des将私钥加密

****

* + 1. **任务8 星际通讯**

公司派你出差到了芝加哥，你需要与你在Galaxy公司的伙伴Bob（你的同组人），进行加密通讯，你们将公钥通过钉钉群，公开传递，互换公钥，之后用对方的公钥，加密你们要交换的文件。并检查结果是否正确。

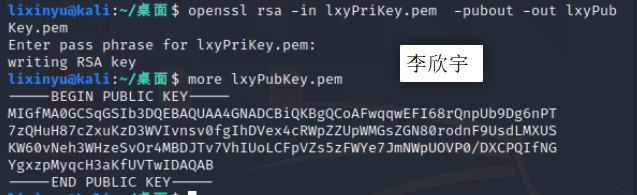
**20）分离公钥**

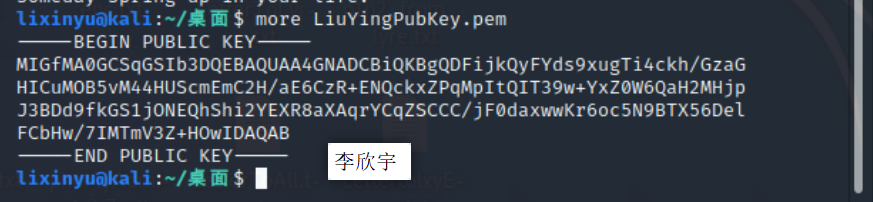
同组人，分别分离出自己的公钥，保存到自己的文件中，发到课程群内，并保存另一方的公钥文件；显示自己公钥的内容；

**过程记录：**

1）使用openssl rsa 命令分离出自己的公钥，存在lxyPubKey.pem中

2）交换公钥，同伴公钥内容如下

****

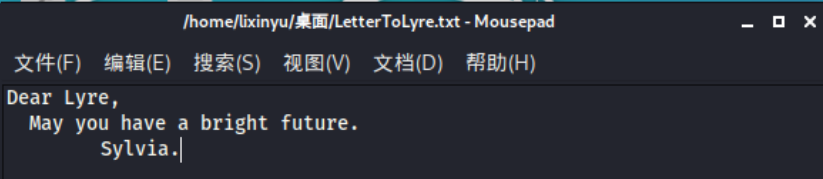
****

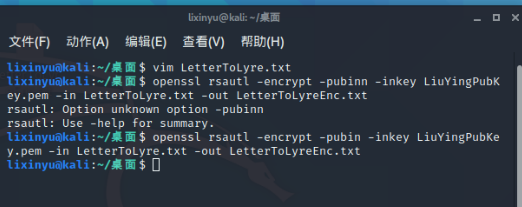
**21）加密邮件**

准备一封写给对方的信，然后使用对方的公钥，加密信件，并通过邮件和课程群，公开发出给同组伙伴Bob；

**过程记录：**

使用vim编辑一封给同伴的信，使用同伴的公钥把LetterToLyre.txt进行加密并发给同伴

****

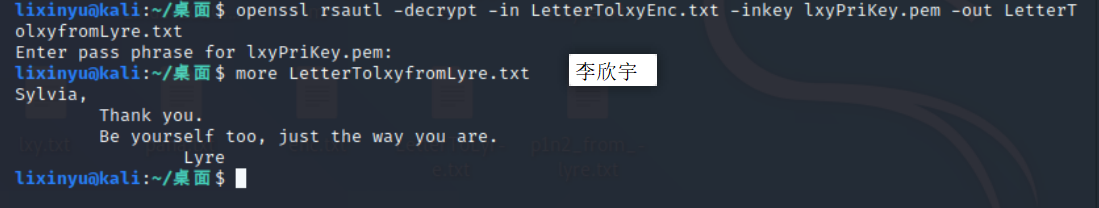
****

**22）私钥解密**

你公开获得密文邮件后，能解密出你的同伴给你发的内容，请记录：

**过程记录：**

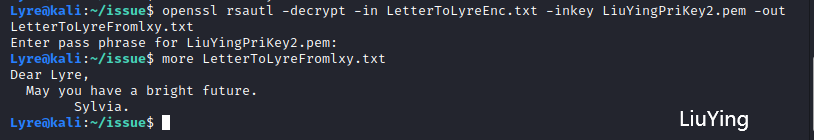
使用自己的私钥对密文邮件进行解密，获得的明文如下



**23）团队合作**

你的伙伴能还原出你发给他的加密邮件吗？

记录： 我的小伙伴能还原，截图如下



* + 1. **任务9 May The Cryptography Force Be With U**

**24)数字签名**

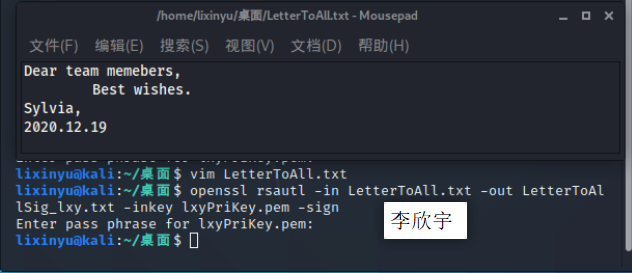
你担任某地区市场经理了，给你的员工发一封公开信，鼓励他们，例如：“Dear XXXX, the most difficult time is about to pass, with a bright future---XXXXXXX”。员工Bob收到后，如何能确认信是你发出的。

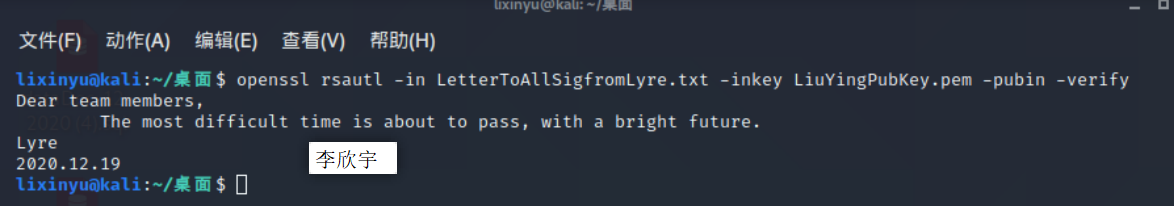
同组两位同学，互相验证对方的签名信件，并记录信件的内容：

**过程记录：**

1）使用私钥对信件进行签名处理并公开发给同伴Lyre

2）使用同伴的公钥对同伴公开发送的信件进行验证





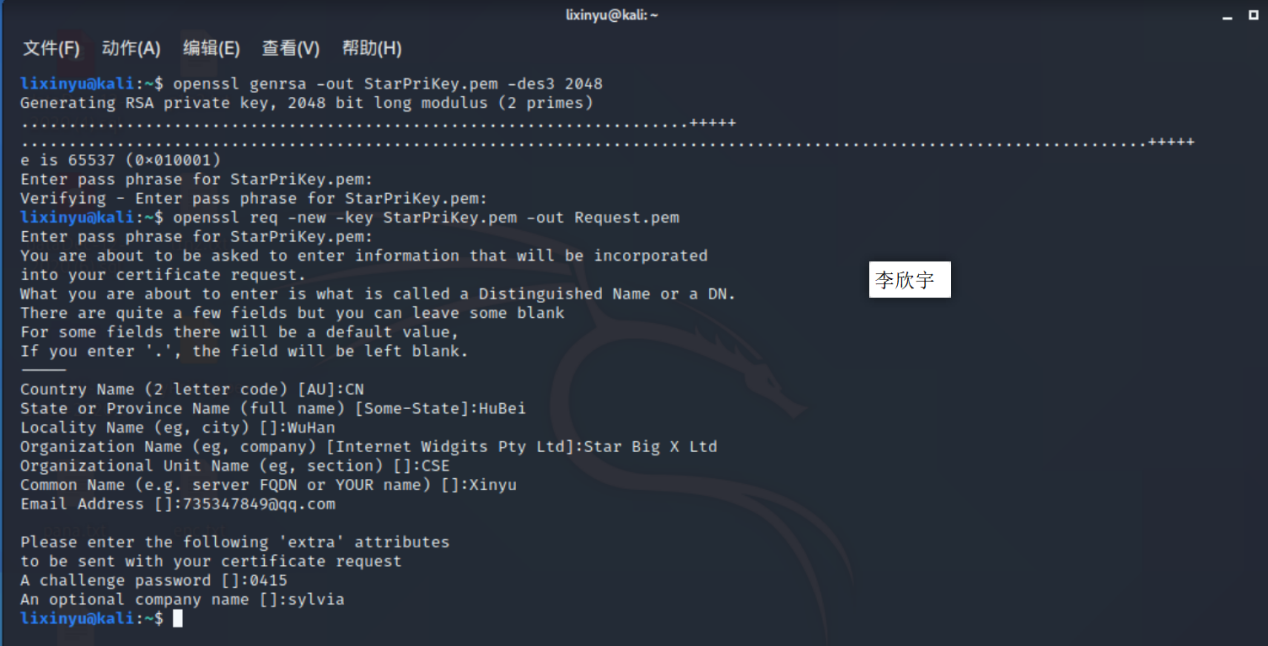
* + 1. **任务10 待下回分解To be continued**

**25)请求证书**

你毕业后，准备成立自己的初创公司，得取一个响亮的名字吧，比如：Universe，给自己的公司网站签发证书。你的公司一样，可能也需要一个密钥对。请利用openssl生成公司的私钥，另外，完成签发证书的请求。

**过程记录：**

为公司生成私钥并完成签发证书

****

* + 1. **扩展阅读及参考**

1. <Https://luv.asn.au/overheads/security/index.html>
2. [OpenSSL与网络信息安全-基础、结构和指令.pdf](file:///E:\\2020分级培养一\\2%20加密解密（GnuPG、Hashcat、advanced%20archive%20password%20recovery）\\OpenSSL与网络信息安全-基础、结构和指令.pdf)
3. [Openssl man1.pdf](file:///E:\\2020分级培养一\\2%20加密解密（GnuPG、Hashcat、advanced%20archive%20password%20recovery）\\openssl%20man1.pdf)
4. [Openssl开发手册.chm](file:///E:\\2020分级培养一\\2%20加密解密（GnuPG、Hashcat、advanced%20archive%20password%20recovery）\\openssl开发手册.chm)
5. [Hashcat.pdf](file:///E:\\2020分级培养一\\2%20加密解密（GnuPG、Hashcat、advanced%20archive%20password%20recovery）\\hashcat.pdf)
6. [Crunch.pdf](file:///E:\\2020分级培养一\\2%20加密解密（GnuPG、Hashcat、advanced%20archive%20password%20recovery）\\crunch.pdf)
7. <Http://www.linuxguruz.com/forum/security-f554.html>

\*思考：

1、Openssl里面有没有我们国家自己的标准算法？

2、暴力破解关卡中能否提高速度？

## 实验问题分析与总结

本次实验较为简单，并未遇到问题，但是非常有意思，与同伴在交互模式下的解密加密更能快速的了解对称加密和非对称加密，尤其是写邮件这种形式会更进一步增强我们之间的合作默契度。而关于hashcat的自主探究对aes、md5加密的字段的解密很具有探索趣味。

## 参考文献及资料列表

[1]crunch命令详解 以及使用方法（综合我的经验） , https://blog.csdn.net/qq\_42025840/article/details/81125584

[2]openssl 对称加密算法enc命令详解 , https://www.cnblogs.com/gordon0918/p/5317701.html

[3]hashcat详细使用教程 , https://smling.blog.csdn.net/article/details/106111493?utm\_medium=distribute.pc\_relevant.none-task-blog-BlogCommendFromBaidu-1.control&depth\_1-utm\_source=distribute.pc\_relevant.none-task-blog-BlogCommendFromBaidu-1.control