

“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

姓 名

学 号

日 期 2021 年 6 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.请参考模板给出的格式，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： 学号：

你给同组人评价： 优 （优 良 中 及格）；

请描述具体理由： 操作较为熟练，在缺课请假的情况下根据资料自学完成了任务；

# 

# 加密与解密实验（通关）

## 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；

本实验2人一组，同组成员： 、 ；

### 实验场景设置

还记得上次数据库关卡吗？你撤销了Bob对Galaxy数据库的访问权限，并对数据进行了保护，包括用MD5、AES等。这次Bob通过一些渗透工具的使用，发现了一些不太安全的因素，会提醒你注意；另外，假如你被派往上海出差，你和Bob远程通信时，采取适当的安全防护，比如文件加密、邮件附件加密等。

## 过程记录/实验任务（共10个关卡，25个小任务）

* + 1. **关卡1 达芬奇密码**

**1）密码恢复**

公司内部用于培训数据的资料，被压缩软件winrar压缩，并加上了密码进行保护，但这个文件是已经辞职的管理员留下的，原密码已经丢失；请你想办法恢复该密码。

提示：采用工具Advanced Archive Password Recovery（ARCHPR）进行密码恢复：

*提示信息：如果直接恢复15分钟，仍未成功，可以利用信息“Call the Hospital of HUST”削弱破解难度。*

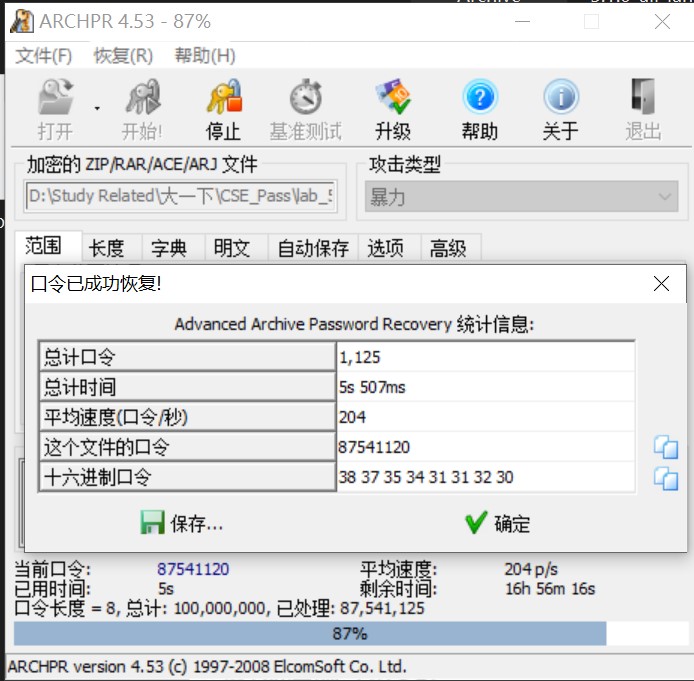


图1 利用提示破解.rar压缩文件

* + 1. **关卡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；

**3）强度削弱**

如果10分钟后，某一方未能完成关卡2，可请对方给出提示以缩小尝试的范围；请记录对方给出的提示。

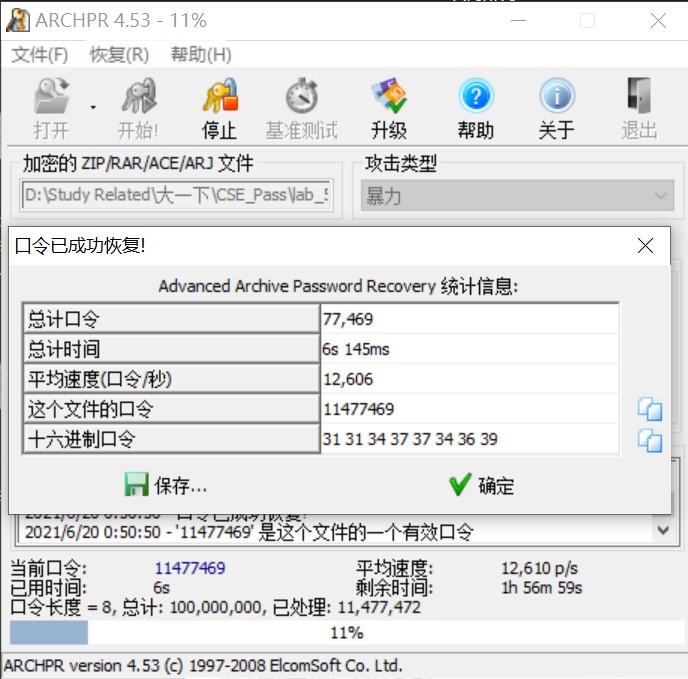


图2 利用提示破解搭档提供的加密文件

* + 1. **关卡3 好记性不如烂笔头**

口令恢复：前面Linux基础关卡中，kali系统里，增加的你同伴Bob的账号吗？ 请Bob自己登录系统后，修改自己的密码；现在，假设Bob太长时间没有登录系统，遗忘了该密码。

如果希望找回原始密码，Kali系统有这项功能吗？

答案： 有；在开机界面选择高级功能，可还原root用户的密码；root用户可查看 ；

请你按小任务4）-7）找回你同组人Bob的原始密码。

**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；



图3 使用tail和grep获取搭档的密码

**5）暴力破解**

使用kali中的Hashcat工具，用掩码模式，尝试暴力破解；

如果破解10分钟，还没有结果，

记录保存当时的状态截图，记录如下；

之后，再尝试用用字典破解。

**6）生成字典**

请同组成员，给出提示信息，记录提示信息：

/

根据提示信息，使用字典的工具：crunch，生成字典。

**解答：**Kali已经更改了保存用户密码的加密算法，Google后没有得到确切的答案，故此项任务暂时无法进行；

**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能否破解数据库安全基础关卡中，采用MD5、AES加密了某些字段？

填写你的答案： 查询hashcat支持列表知，hashcat无法破解aes

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： hashcat的哈希模式选择0即可破解md5；

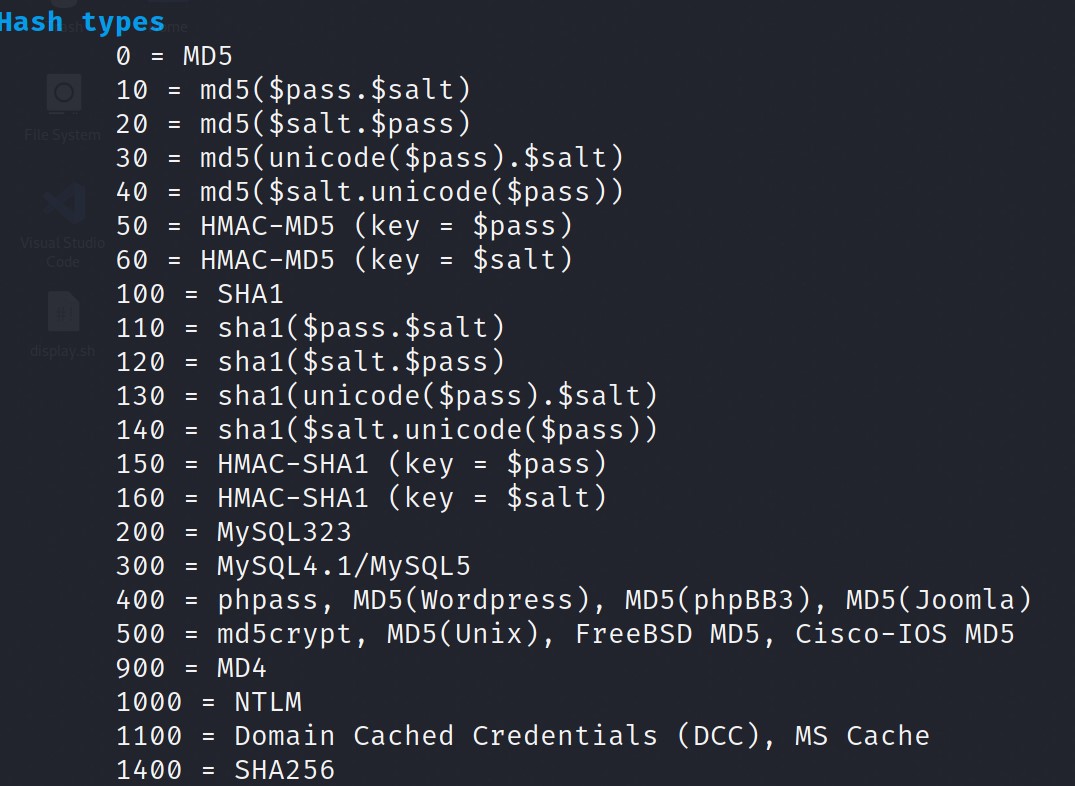


图4 hashcat支持的哈希模式列表（部分）

* + 1. **关卡4 十八般兵刃**

天下安全，唯密不破；

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。

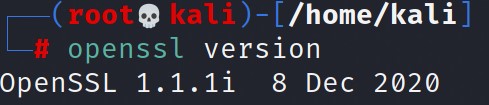


图5 查看openssl版本

**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、 **标准 standard** ；

2、 **摘要 digest** ；

3、 **加密 cipher** ；

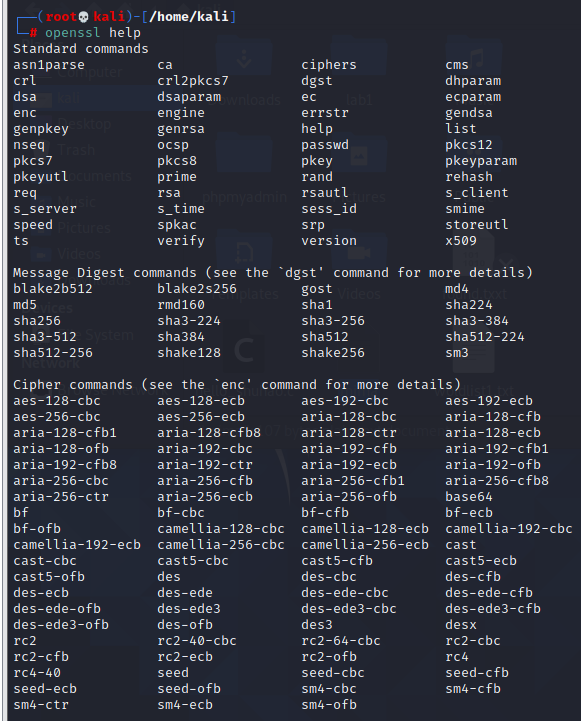


图6 查看openssl命令

**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：

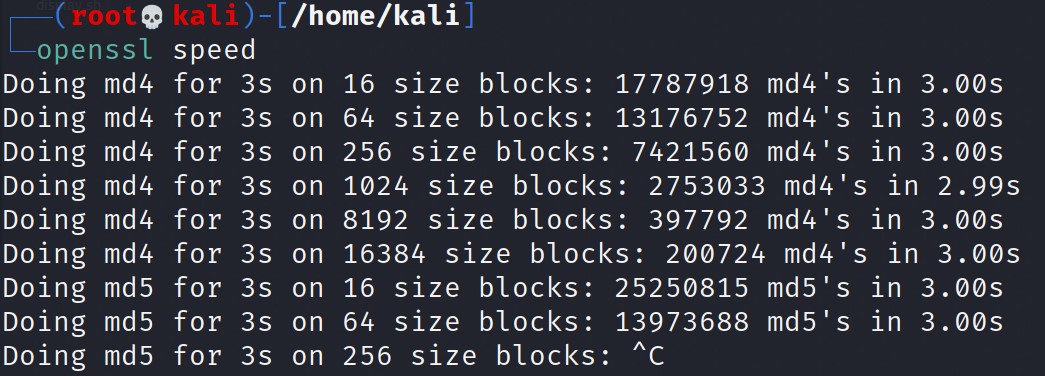


图7 测试openssl速度

* + 1. **关卡5 Digest摘要算法**

**12）被篡改了吗？**

从课程群下载的phpmyadmin压缩包，你能确定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。

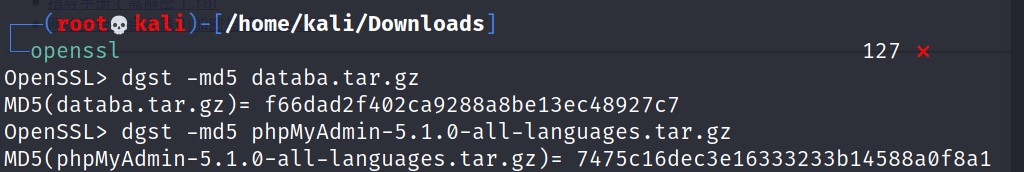


图8 md5对比

对比发现并不相同；原因是下载了不同的语言包版本。

**13） Shell编程**

灵活运用你掌握的技术，假设需要你写一个小程序，读取用户输入的一些信息，并加密它们。比如写一个模拟登录过程的脚本：

用vi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拼接成的符号串对应的md5值，输出到控制台屏幕上。

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。

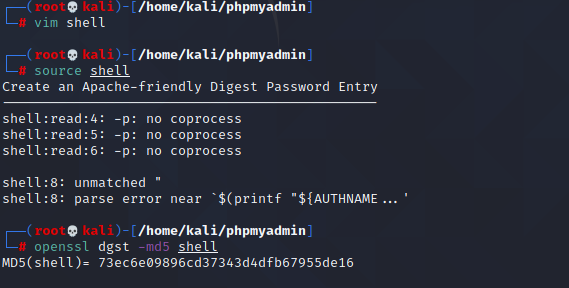


图9 运行模拟的shell脚本

* + 1. **关卡6对称密码**（Symmetric cryptography）

**14）对称密码加密/解密字符串**

先和你的同伴约定好通讯用的密码，再请你的同伴，利用openssl命令加密后发送到课程群，@你；你尝试解密这条信息，并记录结果；

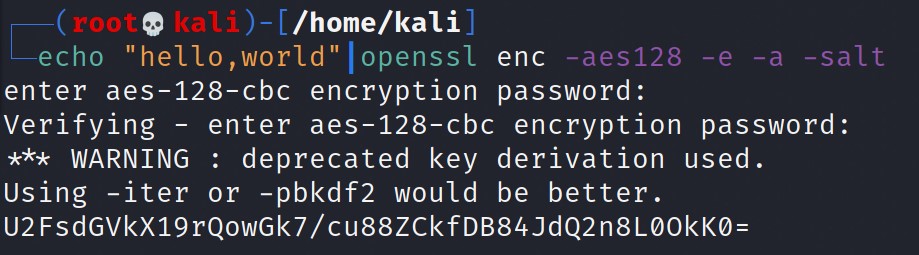


图10 使用aes123加密一段文字

**15）加密文本**

与小任务14类似，但换一种加密算法参数，传递一个简短的文本文件：

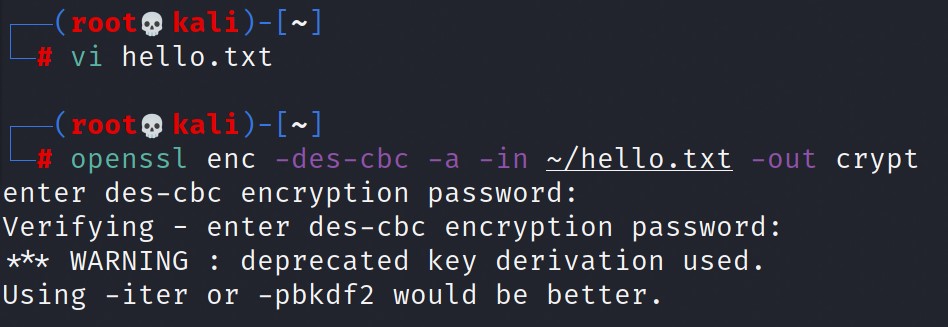


图11 使用另一种指令加密一段文本

* + 1. **关卡7非对称密码**（Asymmetric cryptography）

**16）生成私钥**

前面双方商量并交换password，实现起来安全吗？

回答： **不安全，有被窃听的可能；**

公钥密码不需要密码商议，就能完成关卡8中的通讯。

首先，自己生成一个私钥，保存到文件中；



图12 创建私钥

**17）非对称密码加密文件**

利用openssl rsautl加密一个文件。

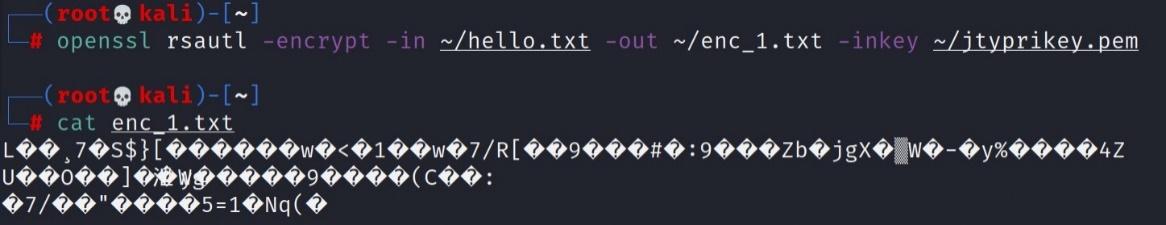


图13 利用rsautl加密文件

**18）非对称密码解密文件：**

利用openssl rsautl解密一个文件。

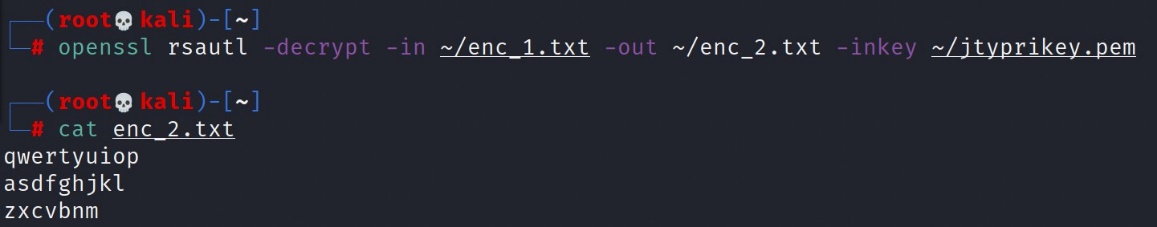


图14 利用rsautl解密文件

**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。

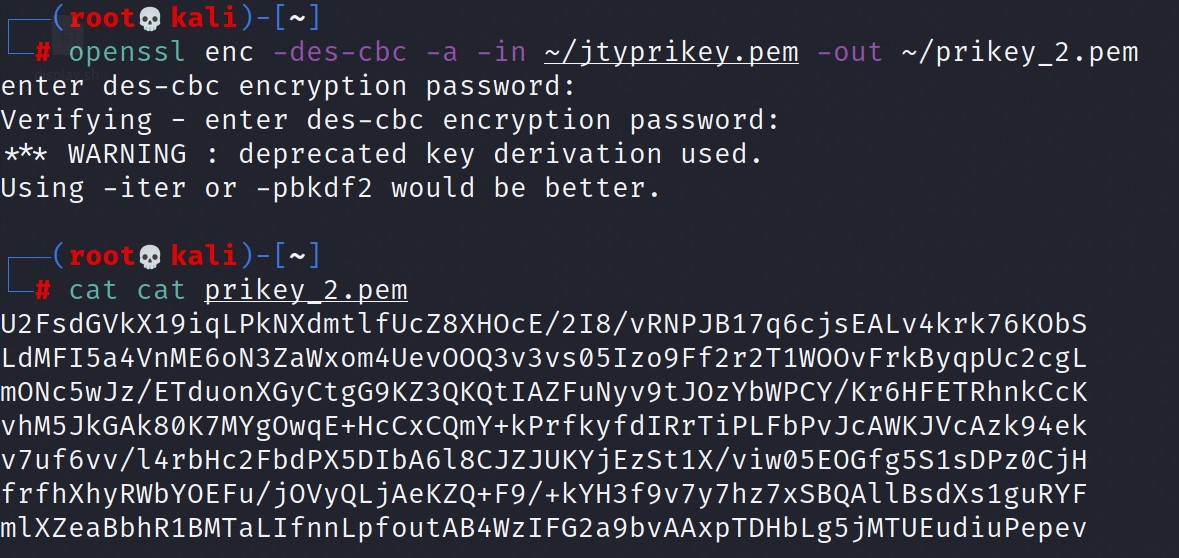


图15 利用des加密私钥

* + 1. **关卡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；

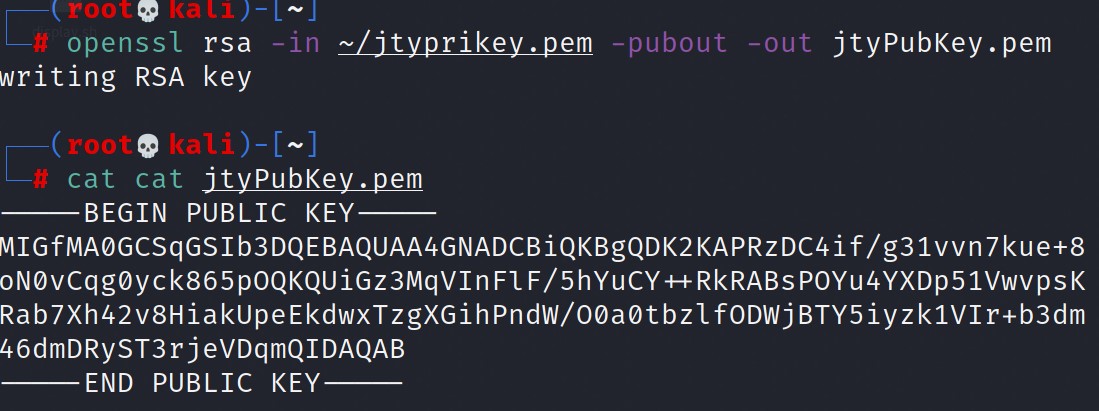


图16 显示公钥

**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；

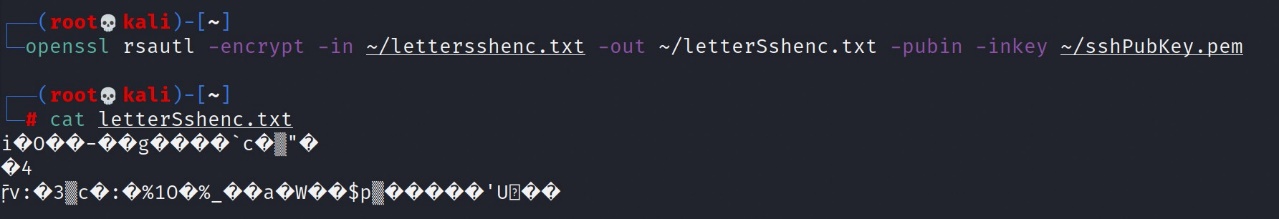


图17 使用对方公钥加密信件

**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：



图18 解密对方邮件

**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： 可以，如下所示

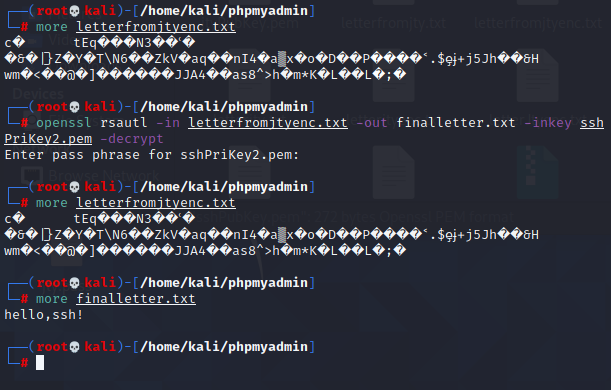


图18 解密对方邮件

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

**24)数字签名**

假如你担任了华东市场的经理，发一封邮件给你的团队：“Dear team members, the most difficult time is about to pass, with a bright future---：XXXXX”。员工Bob收到后，如何能确认邮件是你发出的？

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：

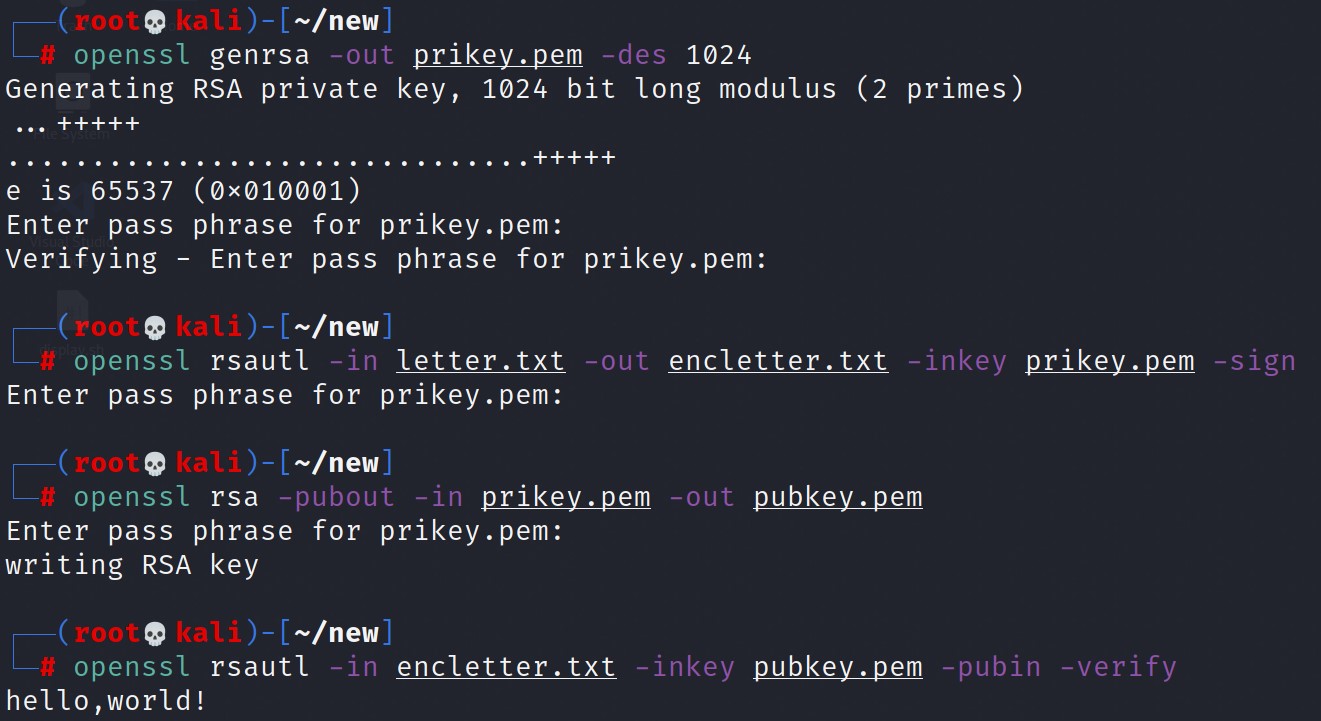


图19 验证签名

* + 1. **关卡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。

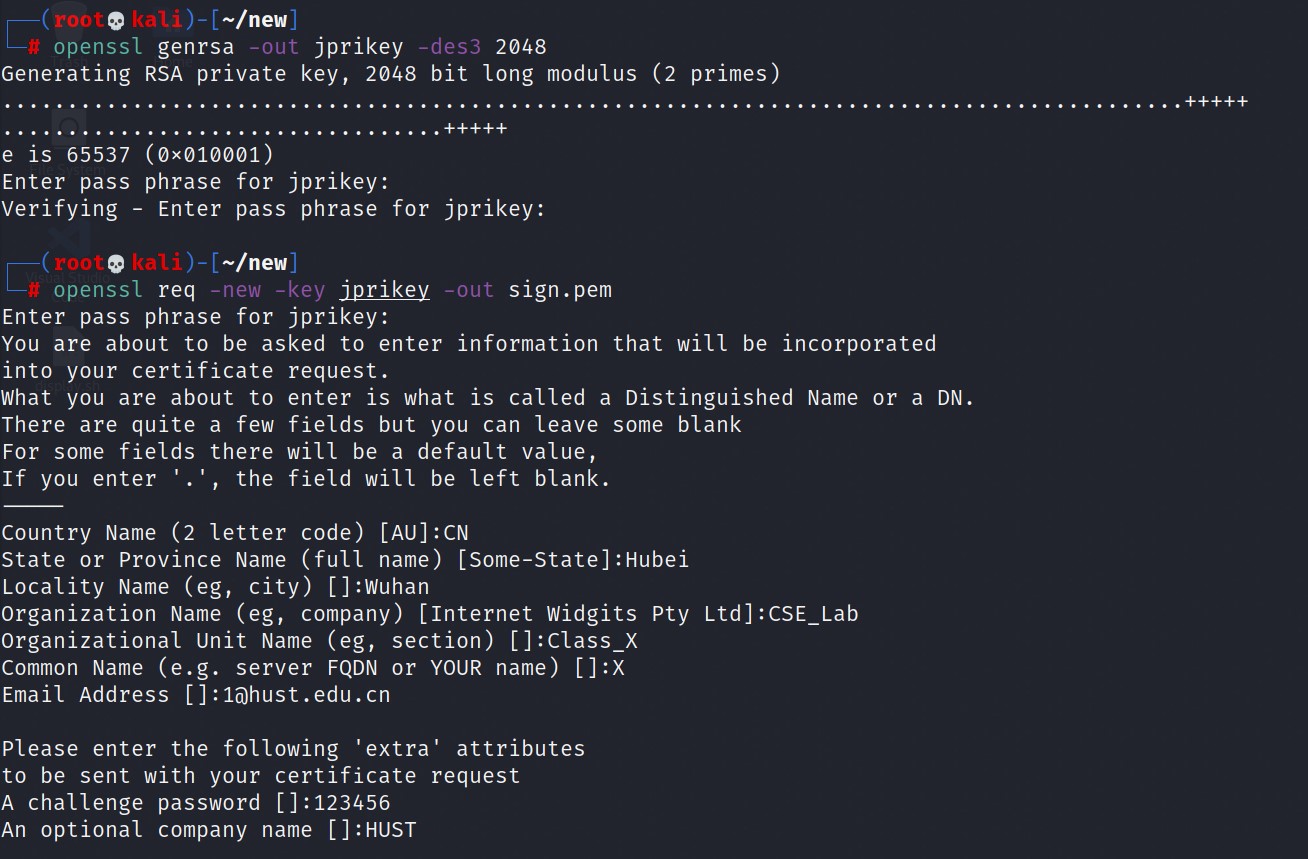


图20 生成私钥并签发证书

* + 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>

\***可选关卡**：

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，能否提高破解速度？

## 实验问题分析与总结

本次实验的主要难点在于openssl工具的使用，其功能非常强大，但同时存在带来了命令行参数过多，难以掌握的问题；正常的加解密操作有规律可循，基本为源文件，目标文件，加解密方法和其他参数，但这一规律不能完全适用于其他操作（比如签发证书）这给掌握它的使用造成了很大难度。实际使用中，如果能配套GUI使用可能效果更好。