

華中科技大學

“网络安全综合实验（I）”实验指导

1 加密与解密实验(通关)

1.1 实验环境及要求

1.1.1 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;

(分组说明: 结合网络教学的实践课程, 便于实验同学间相互讨论、团队协作及相互支持, 要求两位同学一组 (Alice+Bob), 如果学生为单数, 助教可以参与分组。)

参考资料: Linux 自带帮助 man、实验指导教材《网络安全综合实验 (I)》、其他资源。

提交时间及文件名说明: 提交独立实验报告电子版一份, 按指导老师要求的时间和方式提交; 文件名: 姓名.docx

格式说明: 正文宋体小 4 号, 段首缩进 2 字符汉字, 行间距 1 倍行距, 字符间距为标准; 图保证清晰大小合适、每页尽量不留大段空白。

文档中包含内容说明: 1、封面首页信息及作者、完成时间 2、完成任务的过程, 可在任务书基础上进行改写, 补全主要截图及相应的过程说明文字 3、小结: 总体感受、实验中遇到的最突出问题及收获、对实验环节的意见和建议 4、实验中查阅资料的页码、网址作为参考文献部分列表给出 5、参考资料通过浏览器的打印功能, 以 pdf 文件方式保存, 归档为: 姓名.rar, 提交。

虚拟机用户名说明:

Kali 默认 username:kali; password:kali; 自己安装的虚拟机, 用姓名的全拼音作为用户名;

1.1.2 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。

(说明: 实验过程中, 请你们各自保留截图, 关键截图配上相应的说明文字作为实验过程记录; 遇到问题, 尽力寻找解决方案或组内讨论解决, 并做好记录, 最后, 将通关过程、归纳总结, 整理成报告提交。)

1.2 过程记录/实验任务 (共 10 个任务, 24 个小关卡)

1.2.1 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。

参考过程：如图 1-1、1-2 所示。

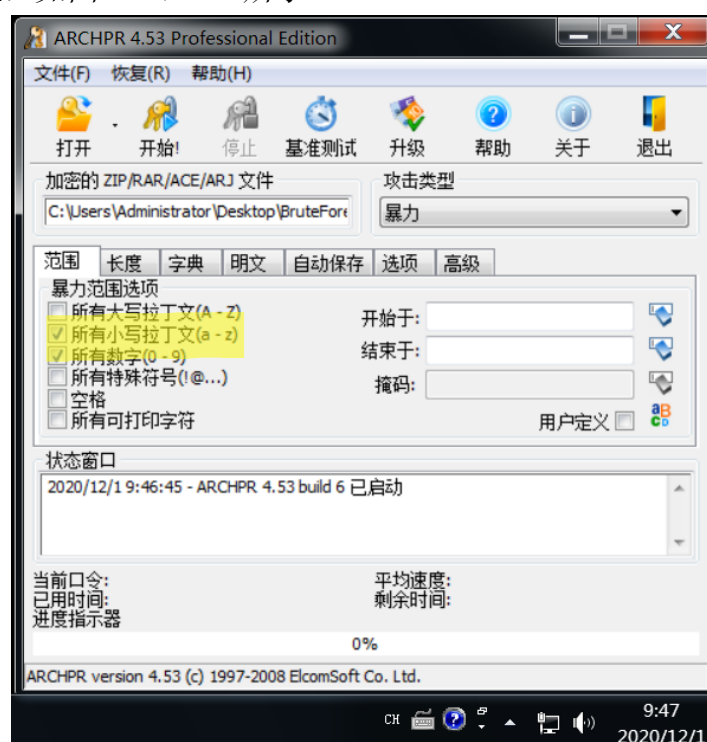


图 1-1 启动密码恢复工具示意图

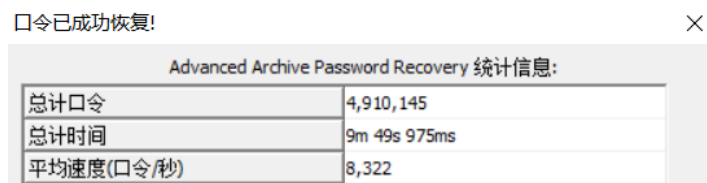


图 1-2 密码恢复运行结果图

提示信息：可以选择不同的如果直接恢复 15 分钟，仍未成功，可以利用信息“密码为 8 位数字，以 87 开头，0 结尾”削弱破解难度。

1.2.2 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，请另一方同学给出提示。记录对方给出的提示如下：

根据该提示，在 ARCHPR 软件中，进行相应配置，缩小搜索范围，再继续；

1.2.3 关卡 3 好记性不如烂笔头

4) 获取密文

从 /etc/shadow 中获得密码的密文

参考命令：`tail -n 5/etc/shadow |grep Bob`

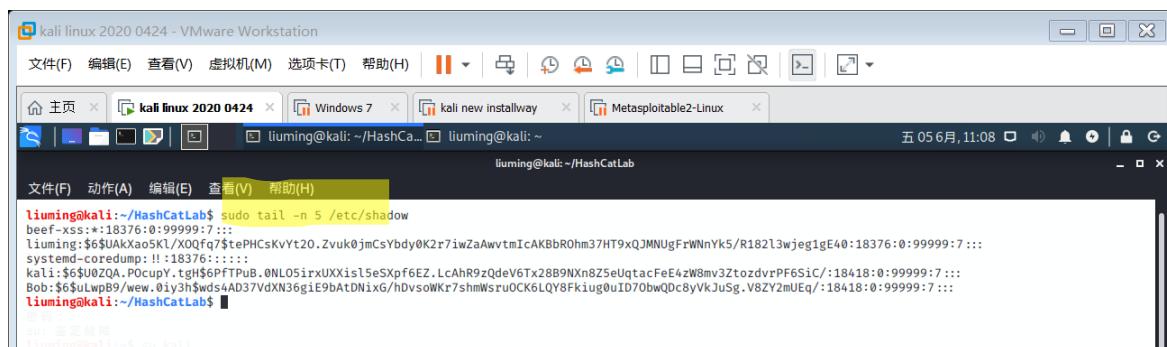


图 1-3 获取用户密码的密文示意图

获得包含待恢复的密码密文后，保存到文件 *Bob.pass* 中；使用 *man* 查找关于 *shadow*、*crypt* 联机帮助，了解 *shadow* 文件中 *\$6\$*、*\$5\$* 前缀的含义；用 *vi* 删除无关内容，‘:’ 为分隔标志，修改后的文件内容可为：

\$6\$uLwpB9/wew.0iy3h\$wds4AD37VdXN36giE9bAtDNixG/hDvsoWKR7shMwSr uOCK6LQY8Fkiug0uID7ObwQDc8yVkJuSg.V8ZY2mUEq/

5) 暴力破解

在了解 *\$6\$* 含义基础上，查看 *hashcat* 的帮助，选择合适的参数进行破解；

参考命令：

man hashcat ；

hashcat -m 1800 ；

参考过程：

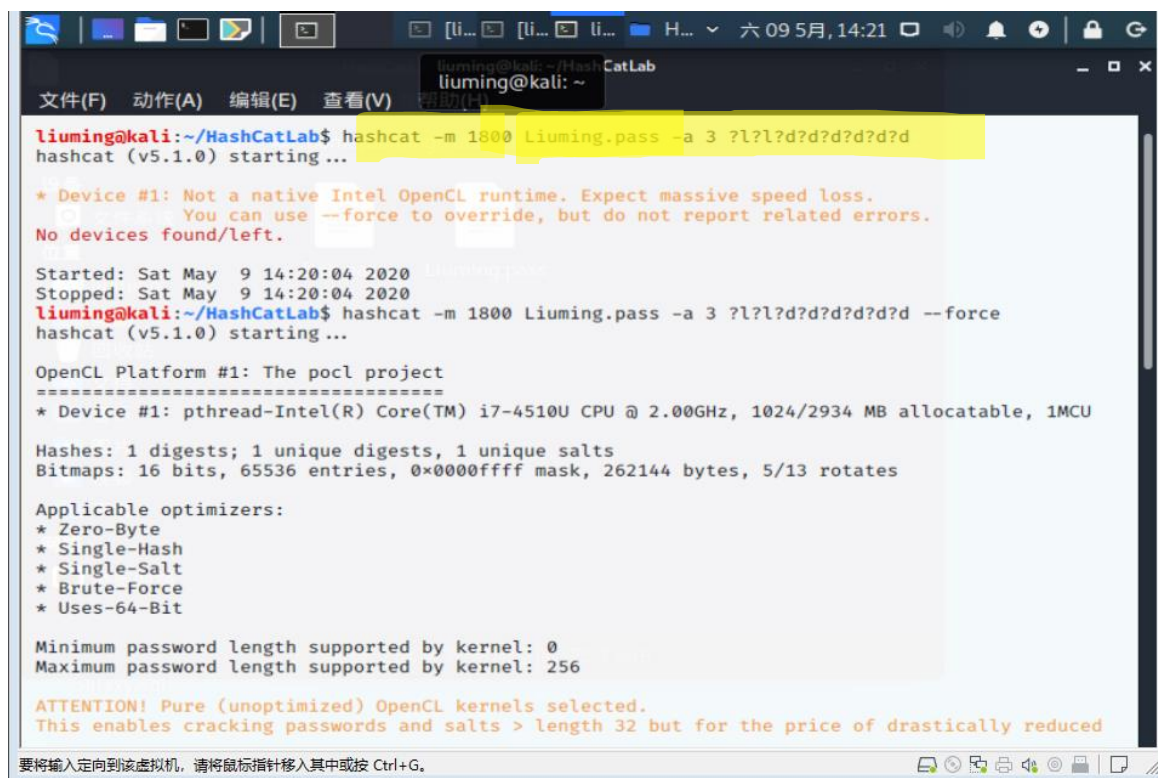
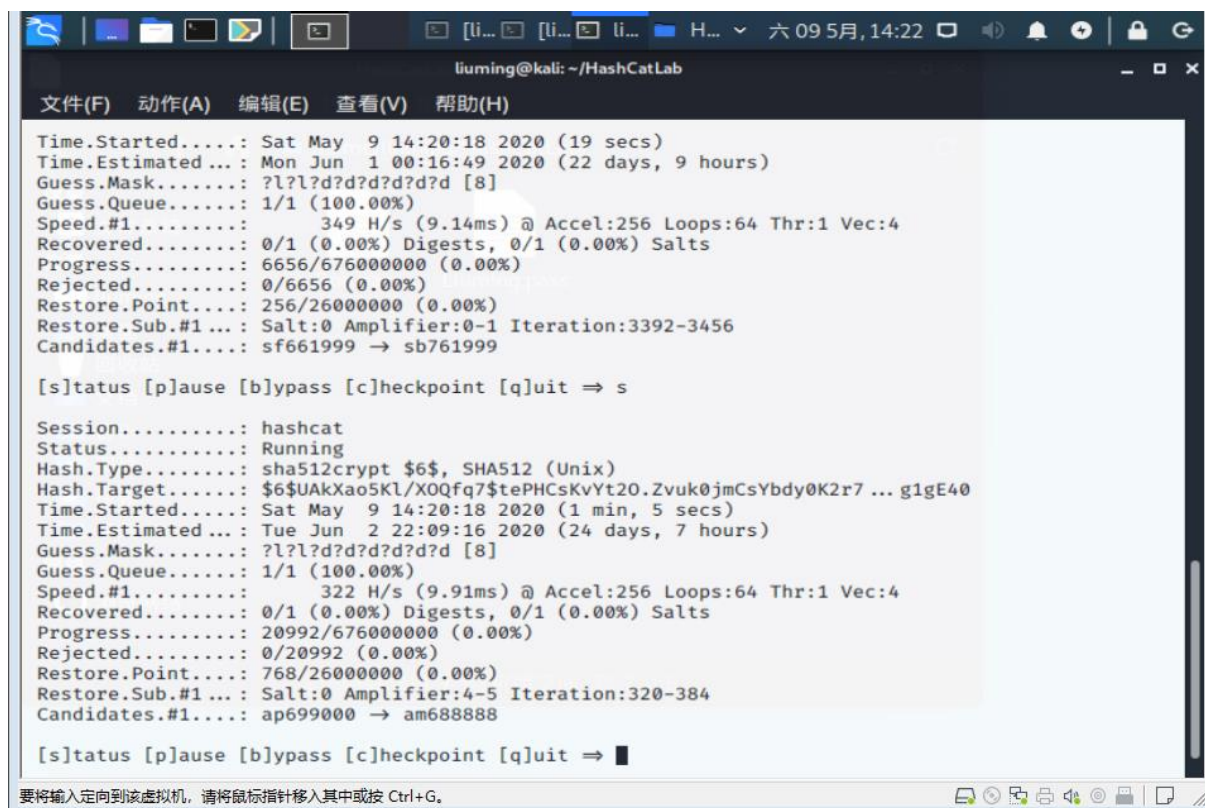


图 1-4 hashcat 破解 shadow 某行密码示意图



```
liuming@kali: ~/HashCatLab
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)

Time.Started.....: Sat May  9 14:20:18 2020 (19 secs)
Time.Estimated....: Mon Jun  1 00:16:49 2020 (22 days, 9 hours)
Guess.Mask.....: ?l?l?d?d?d?d?d [8]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 349 H/s (9.14ms) @ Accel:256 Loops:64 Thr:1 Vec:4
Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 6656/676000000 (0.00%)
Rejected.....: 0/6656 (0.00%)
Restore.Point....: 256/26000000 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:3392-3456
Candidates.#1....: sf661999 -> sb761999

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => s

Session.....: hashcat
Status.....: Running
Hash.Type.....: sha512crypt $6$, SHA512 (Unix)
Hash.Target....: $6$UakXao5Kl/XOQfq7$tePHCsKvYt20.Zvuk0jmCsYbdy0K2r7 ... g1gE40
Time.Started....: Sat May  9 14:20:18 2020 (1 min, 5 secs)
Time.Estimated...: Tue Jun  2 22:09:16 2020 (24 days, 7 hours)
Guess.Mask.....: ?l?l?d?d?d?d?d [8]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 322 H/s (9.91ms) @ Accel:256 Loops:64 Thr:1 Vec:4
Recovered.....: 0/1 (0.00%) Digests, 0/1 (0.00%) Salts
Progress.....: 20992/676000000 (0.00%)
Rejected.....: 0/20992 (0.00%)
Restore.Point....: 768/26000000 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:4-5 Iteration:320-384
Candidates.#1....: ap699000 -> am688888

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => █
```

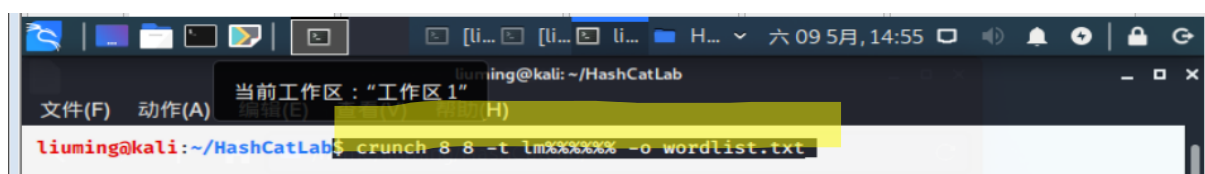
图 1-5 破解过程示意图

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：
再尝试用字典方法破解。

6) 生成字典

请同组成员，给出提示信息，记录提示信息：

查阅 crunch 联机帮助后，根据提示，使用 crunch 生成某字符集对应字典。
参考命令：`man crunch` ; `crunch 6 8 -t lm%-%-%-% -o wordlist.txt`

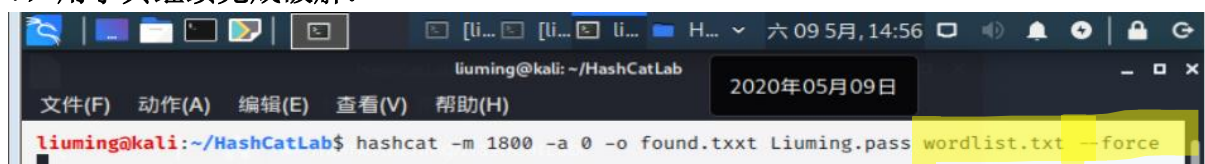


```
liuming@kali: ~/HashCatLab
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)

liuming@kali:~/HashCatLab$ crunch 8 8 -t lm%-%-%-% -o wordlist.txt
```

图 1-6 用工具 crunch 生成字典示意图

7) 用字典继续完成破解：



```
liuming@kali: ~/HashCatLab
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)

liuming@kali:~/HashCatLab$ hashcat -m 1800 -a 0 -o found.txt Liuming.pass wordlist.txt --force
```

图 1-7 利用已生成的字典继续用 hashcat 破解示意图

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 能否破解数据库中用 MD5、AES 加密的串？（这里有小陷阱，同学们注意）

填写你的答案：_____

你同组人同意吗？_____

尝试用前面的工具，进行实验，证明你的想法并记录：_____

1.2.4 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

参考命令：\$ openssl version

参考命令：\$ openssl version -a //查看完整信息

10) 查看帮助

参考命令：\$ openssl help //老师，不对哦！嗯，再看看输出，延展到自己的工具编写

查看帮助后，回答问题：openssl 命令分为哪几类命令？

1、_____；

2、_____；

3、_____；

11) 龟兔赛跑 Benchmarking

对比：记录你虚拟机使用 openssl 进行 md5 算法 3 秒钟、块大小为 1024 时的速度，并与同组成员比较

参考 kali:~\$ openssl speed;

或者：openssl speed md5;

1.2.5 关卡5 Digest 摘要算法

12) 被篡改了吗？

从课程群下载的 phpmyadmin 是官方发布的正式版吗？有没有被篡改过？我们来检测一下！<https://www.phpmyadmin.net/downloads/>

phpMyAdmin 4.9.7

Released 2020-10-15, see [release notes](#) for details.

Older version compatible with PHP 5.5 to 7.4 and MySQL/MariaDB 5.5 and newer.
Currently supported for security fixes only.

File	Size	Verification
phpMyAdmin-4.9.7-all-languages.zip	10.7 MB	[PGP] [SHA256]
phpMyAdmin-4.9.7-all-languages.tar.gz	9.7 MB	[PGP] [SHA256]
phpMyAdmin-4.9.7-all-languages.tar.xz	5.9 MB	[PGP] [SHA256]
phpMyAdmin-4.9.7-english.tar.gz	5.0 MB	[PGP] [SHA256]
phpMyAdmin-4.9.7-english.tar.xz	3.9 MB	[PGP] [SHA256]
phpMyAdmin-4.9.7-english.zip	6.2 MB	[PGP] [SHA256]
phpMyAdmin-4.9.7-source.tar.xz	11.6 MB	[PGP] [SHA256]

图 1-8 phpMyAdmin4.9.7 官网校验 SHA256

参考命令: `openssl dgst` //请将文件复制到虚拟机工作目录下, 然后用 `openssl`, 选择**合适的算法**, 验证其摘要是否与下载网站公布的一致。亦可选其他软件, 从官网自行下载, 检测下载后文件的摘要值(下图 1-9 为 kali 镜像计算 md5 摘要值)。

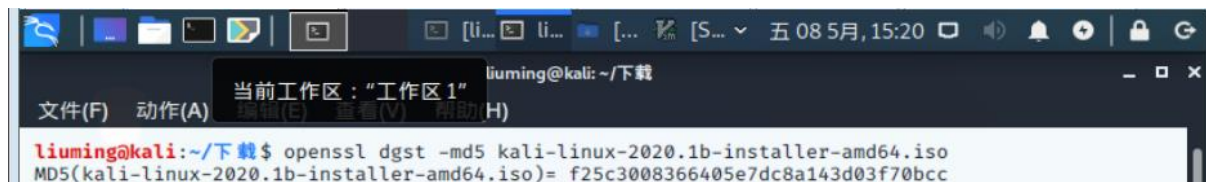


图 1-9 计算 kali 镜像文件 md5 摘要

13) Shell 编程

尝试脚本: 用 vim 写个脚本, 功能是读取键盘输入参数, 然后用 `openssl` 命令, 计算输入的三项内容对应的 md5 摘要。运行你的脚本, 输入你自己的特有信息, 创建摘要并记录结果。

参考命令: `openssl dgst -help`

参考脚本如图 1-10 所示。灵活运用 `chmod` 命令修改 shell 文件文本权限。

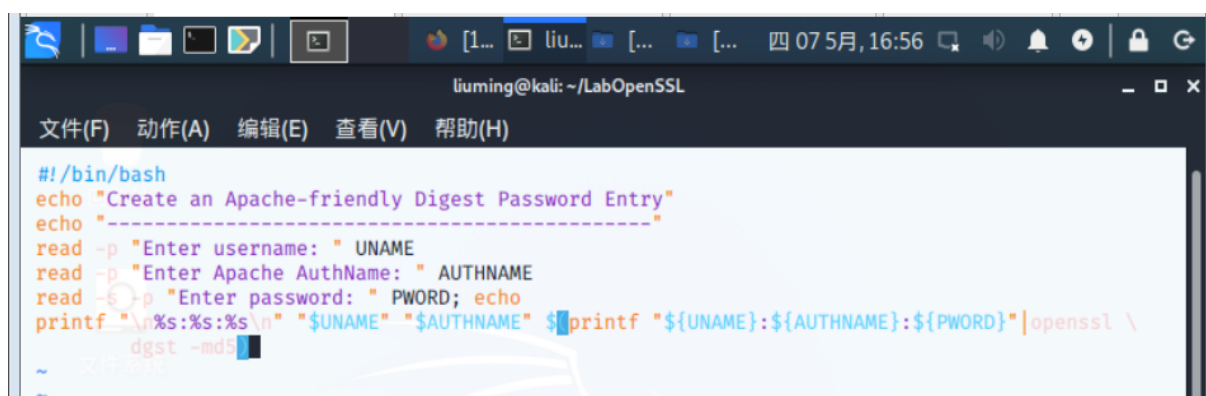


图 1-10 脚本编写过程图

运行并测试你写的脚本, 总结你的发现: _____

1.2.6 关卡 6 Symmetric cryptography 对称密码

14) 对称密码加密/解密字符串

查阅 `openssl` 命令钟关于加密的资料, 了解命令格式;

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;

参考命令: `echo "xxxxxxx" | openssl enc`;

命令中的竖线|表示将 `echo` 的输出通过管道|作为 `openssl` 加密的输入;

参考用 AES128 算法的过程如图 1-11, 加密口令需要告诉你同伴:

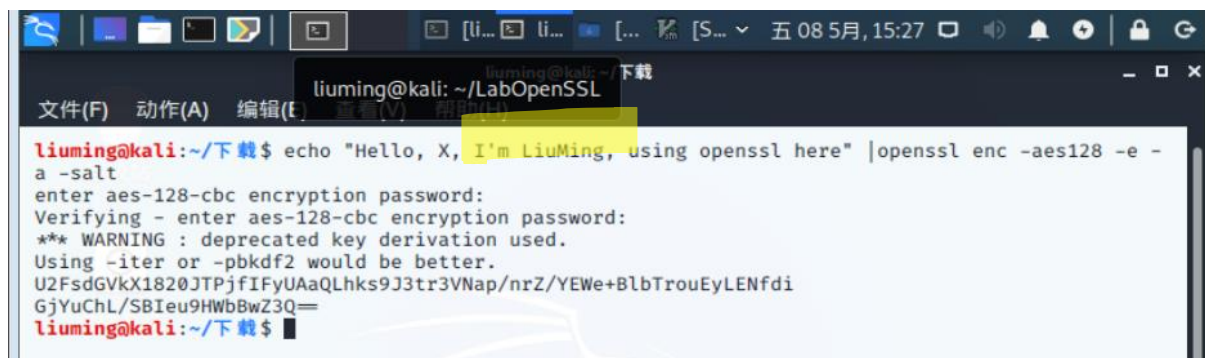


图 1-11 openssl 加密文本过程图

15) 加密文本文件

基本与小任务 14 类似，但换一种对称加密算法，并用文件传递输入、输出内容；同组人传递一个加密过的文件，并记录收到的密文、解密出来的明文内容：

参考选 *des-cbc* 算法的命令：

@kali:~/下载\$ openssl enc -des-cbc -a -in pln1.txt -out enc1_des.txt //产生密文，发给你的伙伴；-a 参数表示用 Base64 处理加密后的内容。

enter aes-256-cbc decryption password:

*** WARNING : deprecated key derivation used.

Using -iter or -pbkdf2 would be better.

liuming@kali:~/下载\$ more enc_des2.txt

//获得你伙伴给你的密文，然后解密；需要双方交换加密密钥 password。

\$ openssl enc -d -des-cbc -a -in enc_des2.txt -out pln2.txt

//供参考解密命令，算法为 *des-cbc*，-d 表示解密

1.2.7 关卡 7 Asymmetric cryptography 非对称密码

16) 生成私钥

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 XXXPriKey.pem 中。 // XXX 为你的姓名

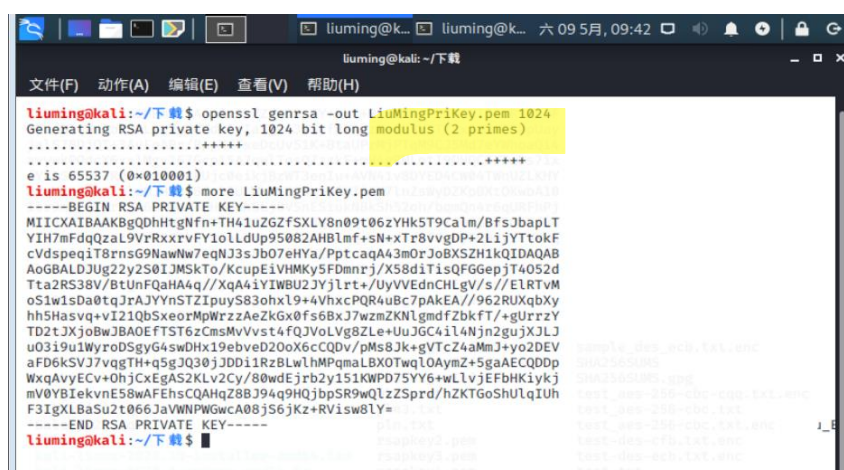


图 1-12 openssl 生成私钥过程图

17) 自己加密文件

参考命令：\$ openssl rsautl -encrypt

参考过程:

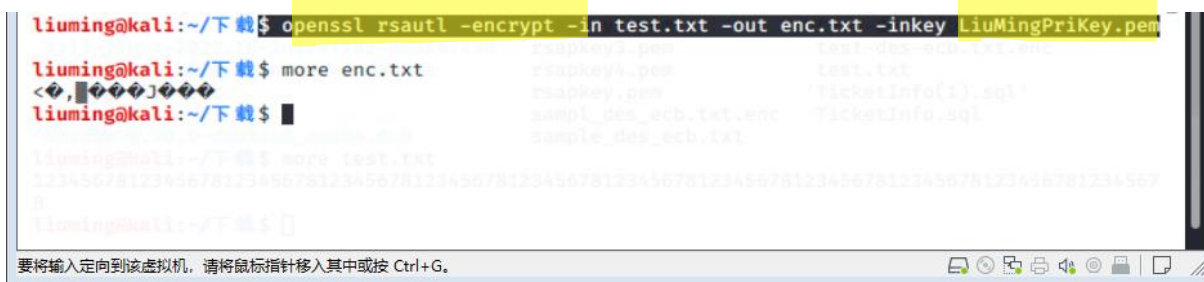


图 1-13 openssl 加密文件过程图

18) 自己解密文件:

参考命令:`$ openssl rsautl -decrypt`

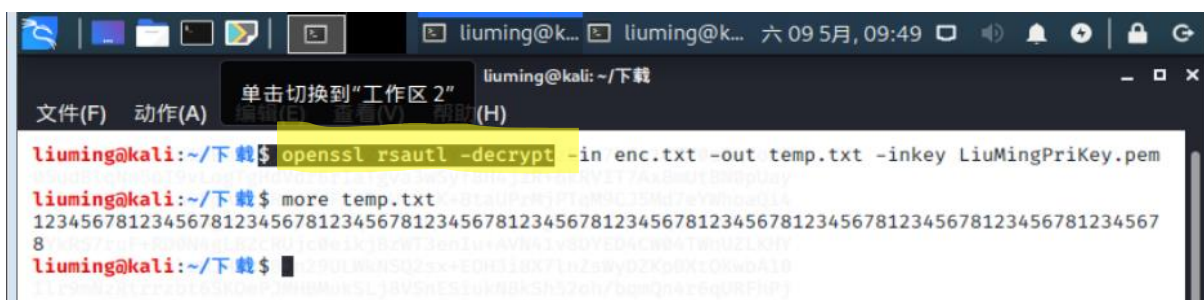


图 1-14 openssl 解密文件 enc.txt 过程图

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。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。

参考命令: `genrsa -des`

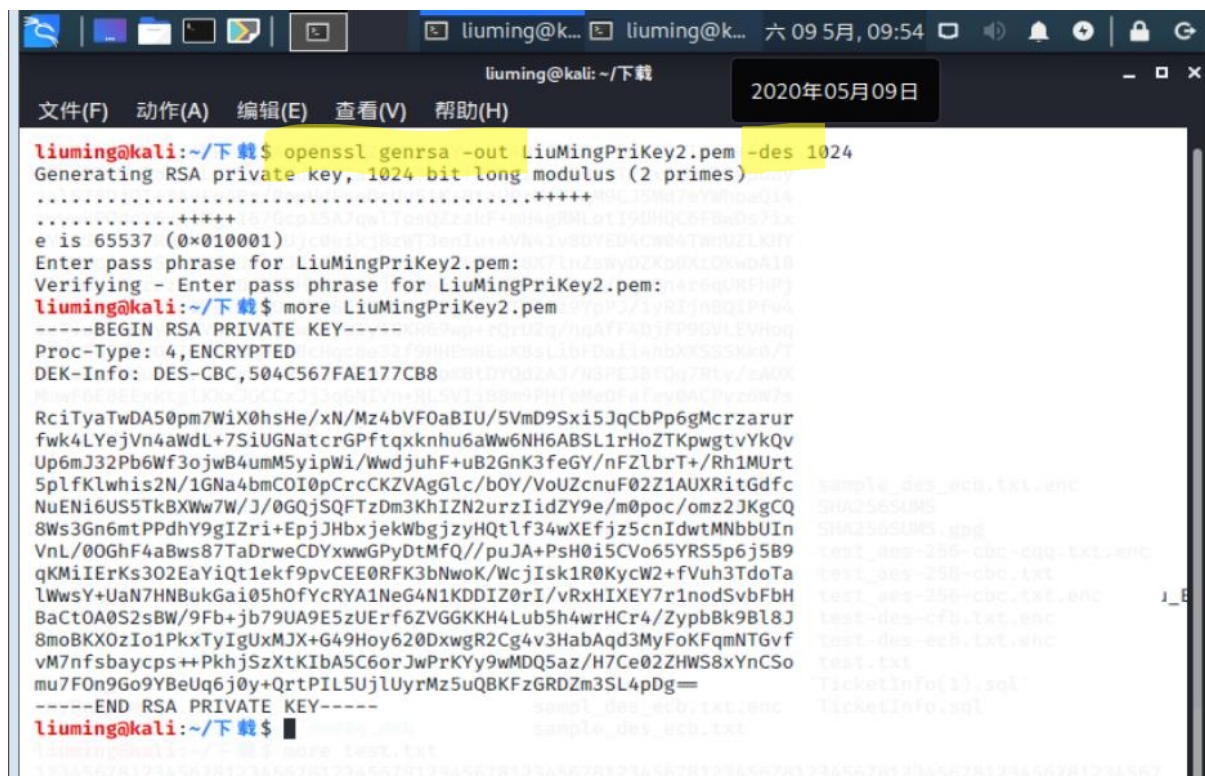


图 1-15 openssl 生成加密私钥文件的过程图

1.2.8 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，你们将公钥通过课程群，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

同组同学，每人已经生成了自己的私钥，目前没有公钥。所以，分别分离出自己的公钥，保存到自己的文件中；将公钥发到课程群内；从课程群内下载同组另一同学的公钥；显示对方公钥的内容；

参考命令：`$ openssl rsa`

参考过程：

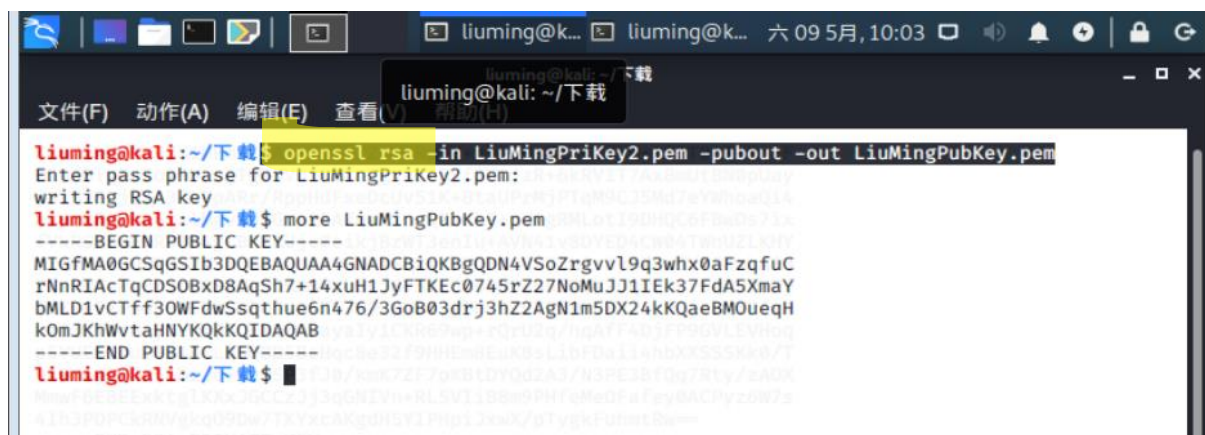


图 1-16 openssl 分离公钥文件的过程图

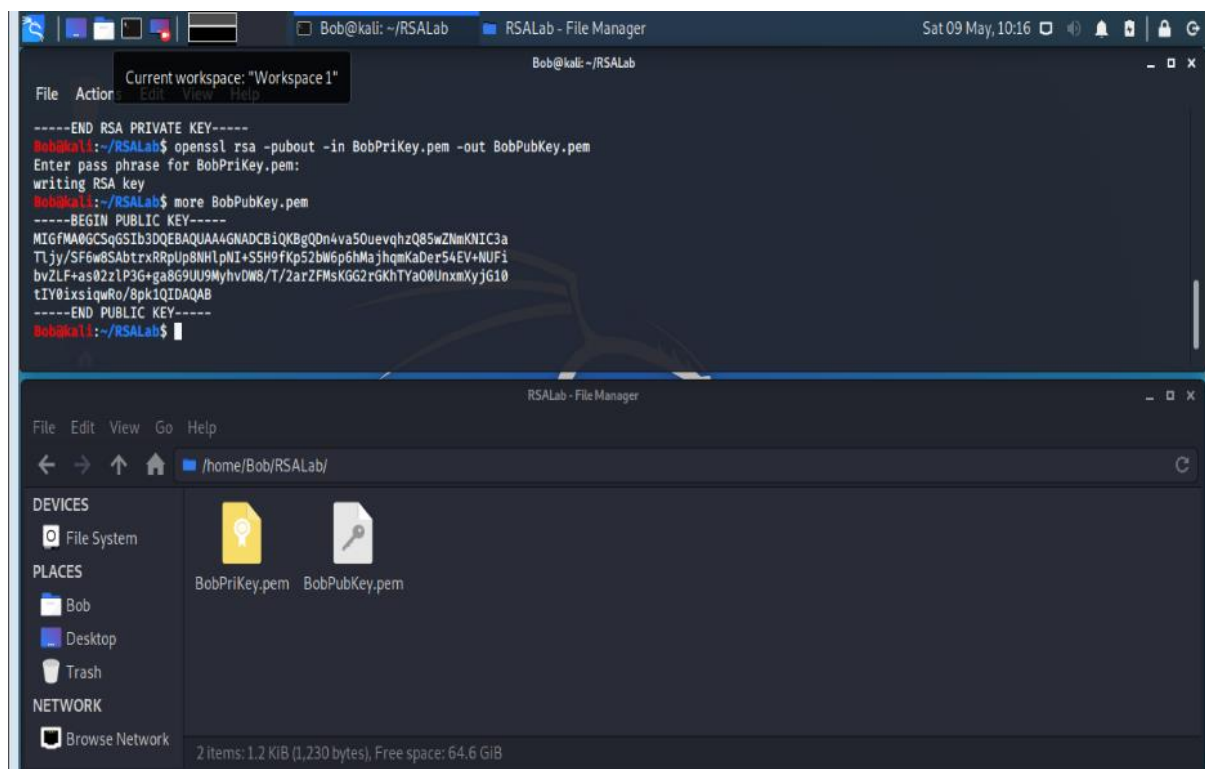


图 1-17 同组人 openssl 分离公钥文件并交换公钥的过程图

21) 加密邮件

获得对方的公钥后，即可进行安全通讯了。准备一封写给对方的信，然后使用对方的公钥，加密该信件，并通过邮件和课程群，公开发出给同组伙伴 Bob；

参考命令: `vi ; openssl rsautl ;`

参考过程:

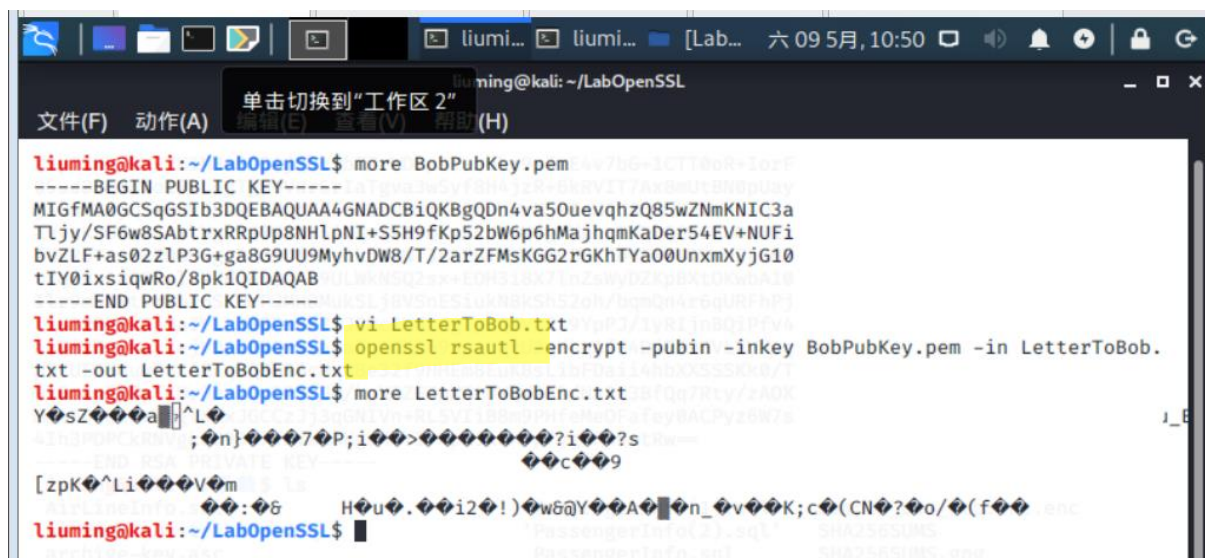


图 1-18 给同组人发加密邮件过程图



图 1-19 对方加密文件的过程图

22) 私钥解密

你也获得了对方给你的密文邮件，请用自己的私钥解密出你的同伴给你发的内容，并记录：

参考命令：*openssl rsautl*

参考过程：

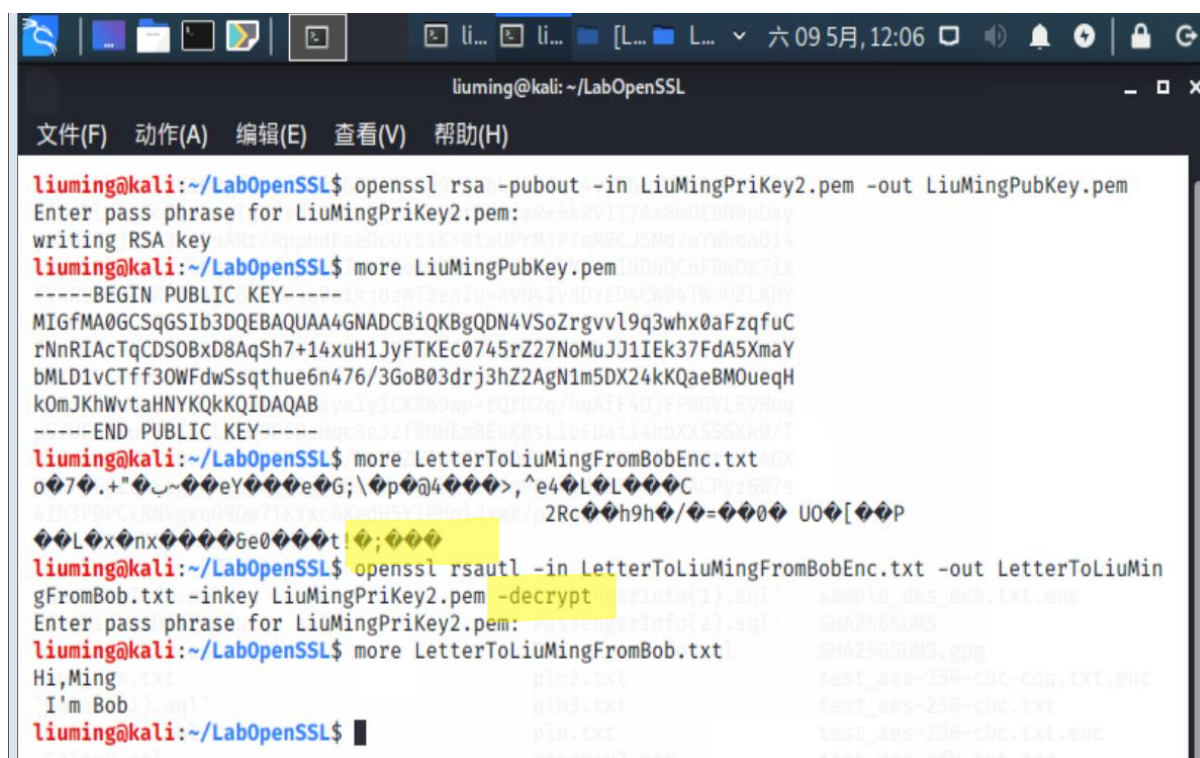


图 1-20 解密收到的文件过程图

23) 团队合作

你的伙伴能还原出你给他的加密邮件吗？

记录：_____

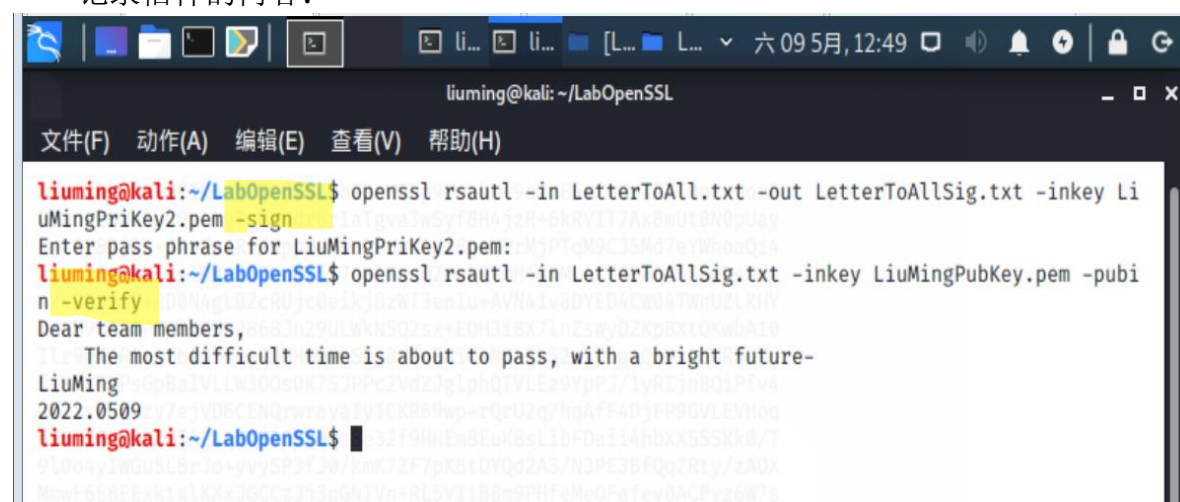
1.2.9 关卡9 密码的力量 (May The Cryptography Force Be With U)

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？

参考命令：`openssl rsautl -sign` //图请同组两位同学，互相验证对方的签名信件。

记录信件的内容：



```
liuming@kali: ~/LabOpenSSL
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)

liuming@kali:~/LabOpenSSL$ openssl rsautl -in LetterToAll.txt -out LetterToAllSig.txt -inkey LiuMingPriKey2.pem -sign
Enter pass phrase for LiuMingPriKey2.pem:
liuming@kali:~/LabOpenSSL$ openssl rsautl -in LetterToAllSig.txt -inkey LiuMingPubKey.pem -pubin -verify
Dear team members,
The most difficult time is about to pass, with a bright future-
LiuMing
2022.0509
liuming@kali:~/LabOpenSSL$
```

图 1-21 利用 openssl 对文件进行数字签名的过程图

1.2.10 关卡10 待下回分解 To be continued

25) 请求证书

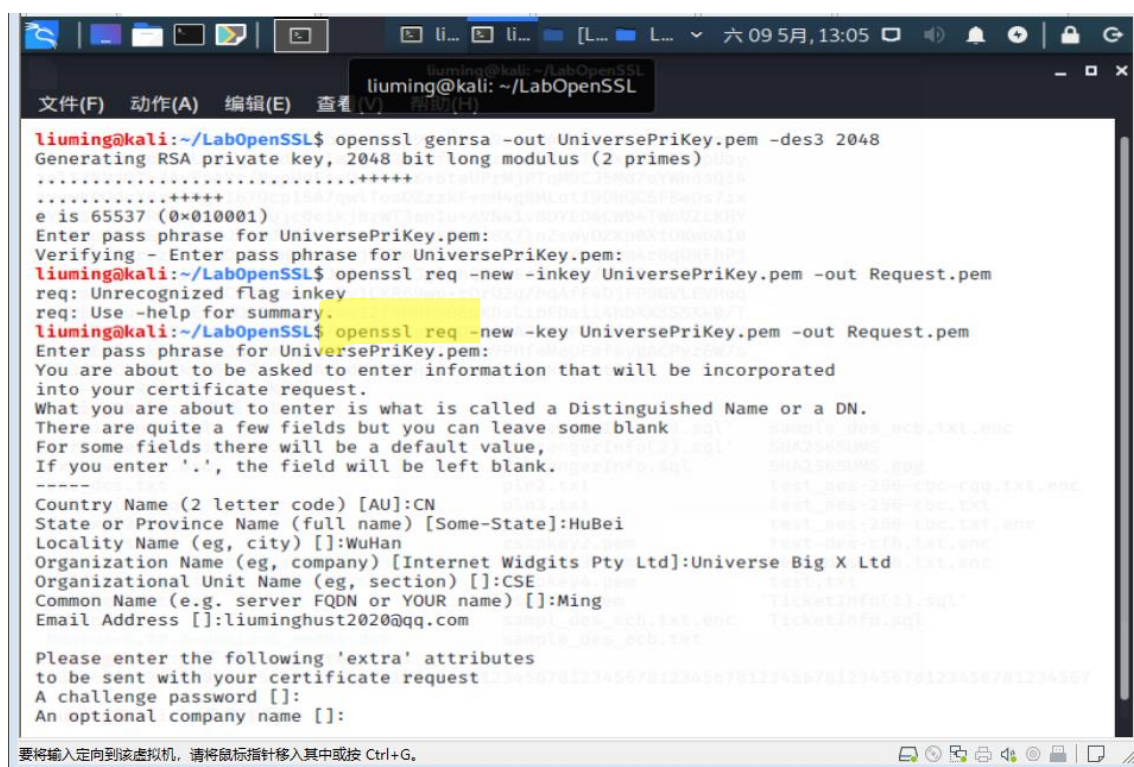
你毕业后，准备成立自己的初创公司，取一个名字，例如：Universe，给自己的公司网站签发证书。你的公司一样，可能也需要一个密钥对。

参考命令：`openssl genrsa;` `openssl req;`

参考操作：

生成公司的私钥，再生成签发证书请求：

`//openssl req -key XXX.pem -new -out Request.pem`



```
liuming@kali: ~/LabOpenSSL
文件(F) 动作(A) 编辑(E) 查看(V) 帮助(H)

liuming@kali:~/LabOpenSSL$ openssl genrsa -out UniversePriKey.pem -des3 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
e is 65537 (0x010001)
Enter pass phrase for UniversePriKey.pem:
Verifying - Enter pass phrase for UniversePriKey.pem:
liuming@kali:~/LabOpenSSL$ openssl req -new -inkey UniversePriKey.pem -out Request.pem
req: Unrecognized flag inkey
req: Use -help for summary.
liuming@kali:~/LabOpenSSL$ openssl req -new -key UniversePriKey.pem -out Request.pem
Enter pass phrase for UniversePriKey.pem:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:HuBei
Locality Name (eg, city) []:WuHan
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Universe Big X Ltd
Organizational Unit Name (eg, section) []:CSE
Common Name (e.g. server FQDN or YOUR name) []:Ming
Email Address []:liuminghust2020@qq.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

图 1-22 准备请求证书的过程图

1.2.11 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](#)
- [3] [Openssl man1.pdf](#)
- [4] [Openssl 开发手册.chm](#)
- [5] [Hashcat.pdf](#)
- [6] [Crunch.pdf](#)
- [7] <http://www.linuxguruz.com/forum/security-f554.html>

1.3 实验问题分析与总结

(说明: 每个实验关卡, 按照实验过程记录在 1.2 节中, 实验中遇到的典型问题、对产生该问题的原因、解决要点的分析过程、本部分实验值得归纳的总结内容、实验的意见和建议, 记录在 1.3 节中)

1.4 参考文献及资料列表