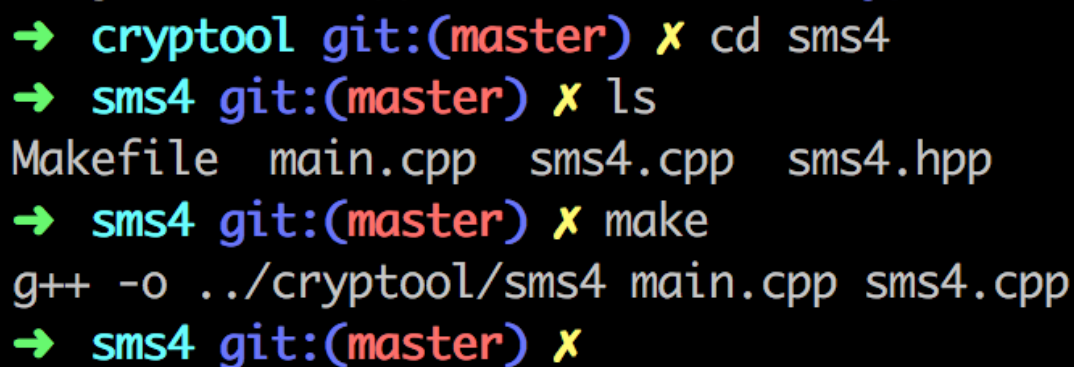


网络与系统安全实验课——加密1

环境说明

编译sm4命令行工具

```
cd sms4  
make
```



```
→ cryptool git:(master) X cd sms4  
→ sms4 git:(master) X ls  
Makefile  main.cpp  sms4.cpp  sms4.hpp  
→ sms4 git:(master) X make  
g++ -o ../cryptool/sms4 main.cpp sms4.cpp  
→ sms4 git:(master) X
```

加密过程

```
cd cryptool/  
python encrypt_qrcode.py
```

生成二维码

按照格式生成二维码。



扫码后得到秘钥

扫码后接收到长度129的data，前16位为KR，后113位为PK，保存PK，通过KR和随机字符串异或可以得到Key。

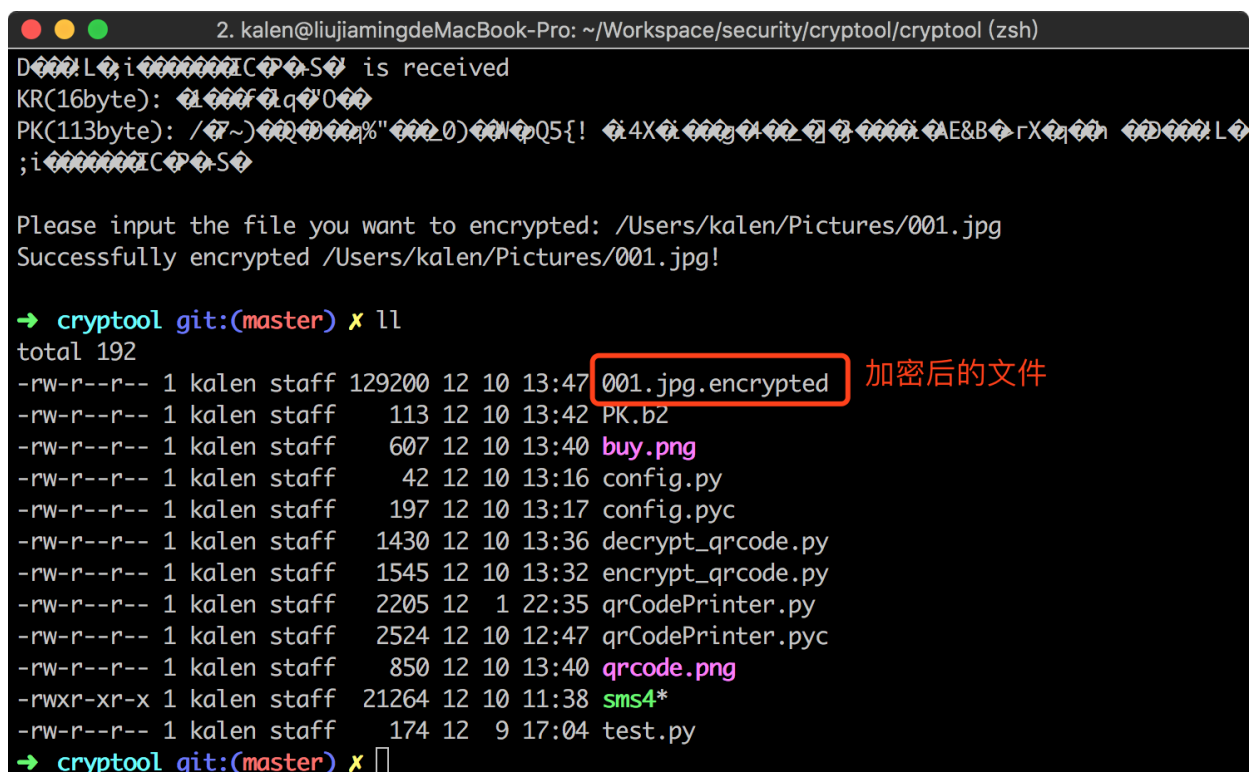


加密文件

选择一张要加密的文件，这里以图片为例。



点击回车后，在当前路径下生成加密后的文件，在文件名后面添加.encrypted作为标识。



解密过程

```
cd cryptool/  
python decrypt_qrcode.py
```

生成二维码

同样按照格式生成二维码。



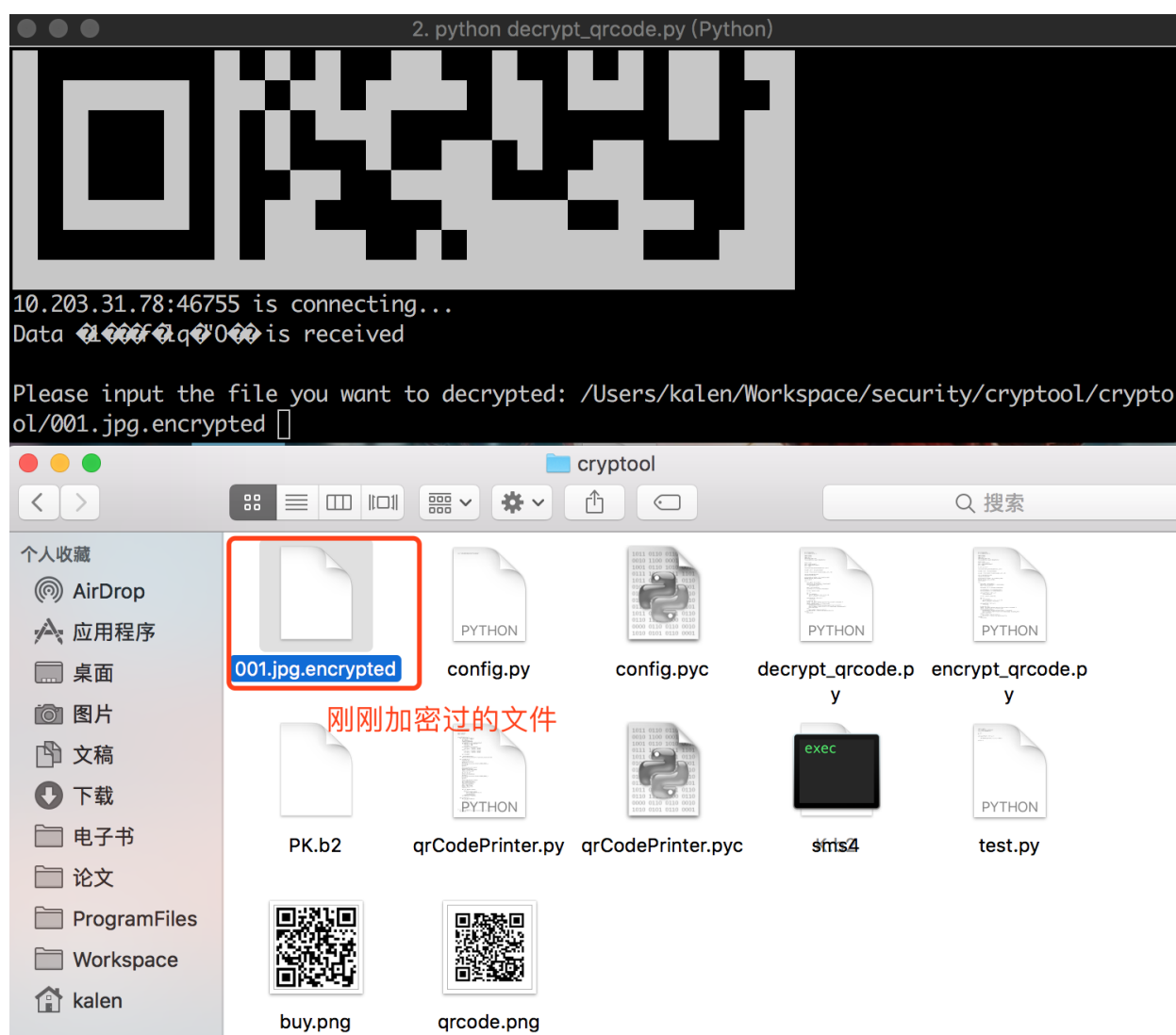
扫码后得到密钥

扫码后把PK发送给手机端，然后得到KR，通过KR和随机字符串疑惑可以得到Key。



解密文件

输入刚刚加密的文件001.jpg.encrypted。



点击回车后解密得到原来的图片。

```
2. kalen@liujiamingdeMacBook-Pro: ~/Workspace/security/cryptool/cryptool (zsh)

10.203.31.78:46755 is connecting...
Data 1000f000 is received

Please input the file you want to decrypted: /Users/kalen/Workspace/security/cryptool/cryptool/001.jpg.encrypted
Successfully decrypted /Users/kalen/Workspace/security/cryptool/cryptool/001.jpg.encrypted!

→ cryptool git:(master) x
```

