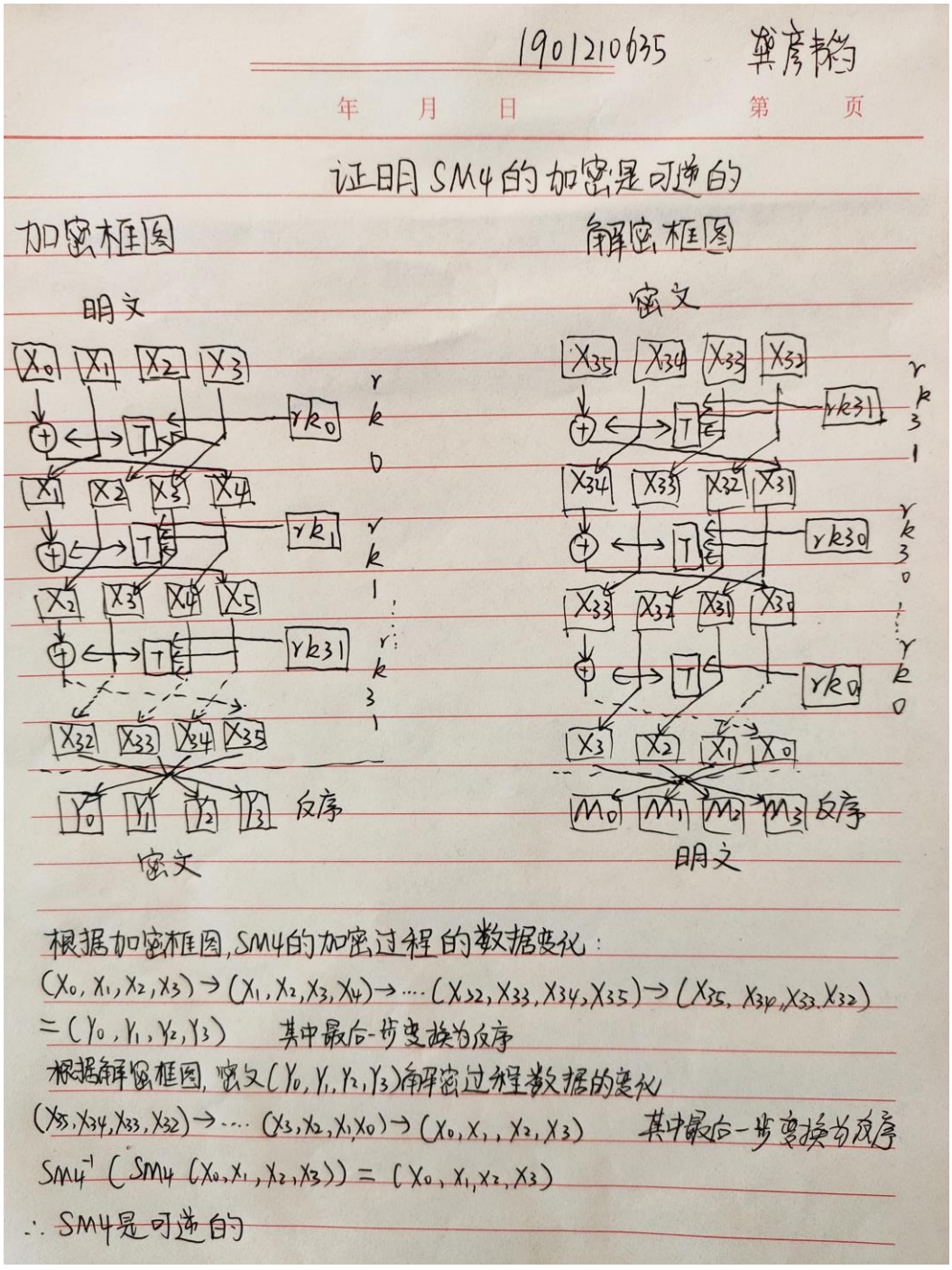
应用密码学第二次作业

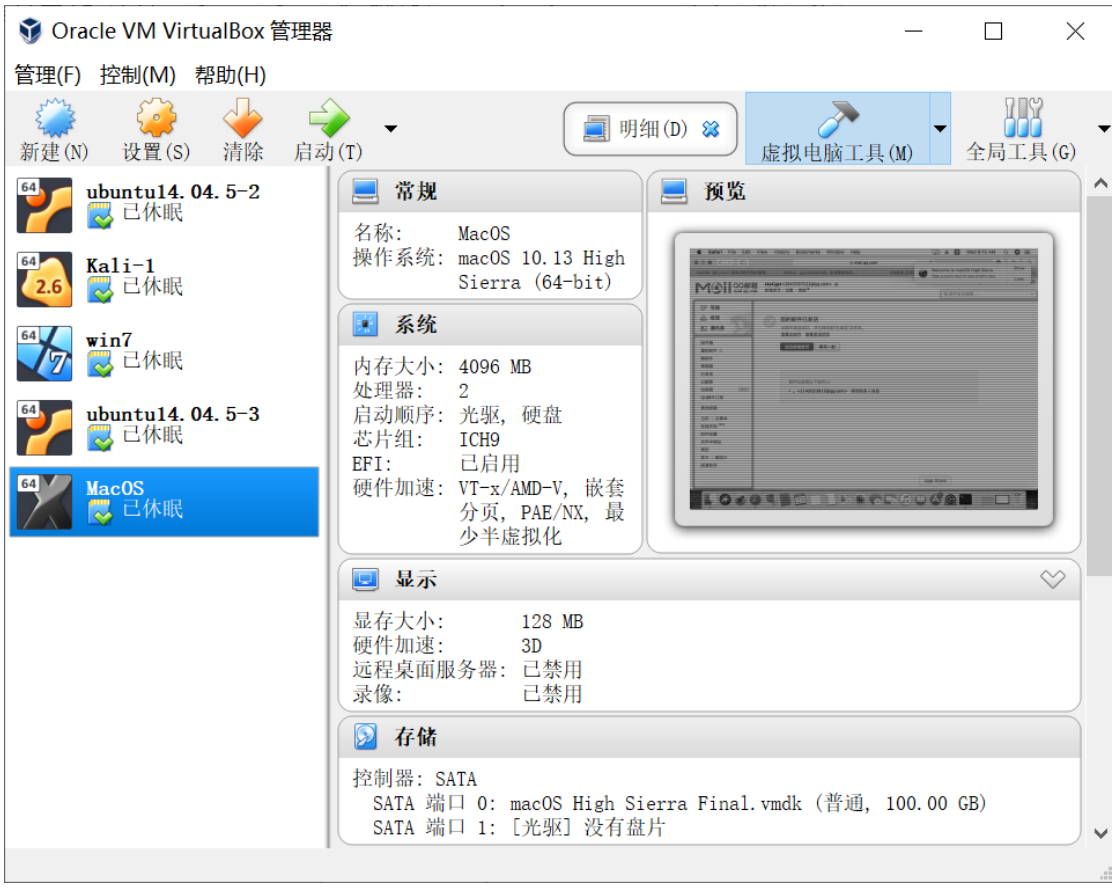
1901210635 龚彦韬

1、 Proof that encryption of SM4 is reversible 证明 SM4 的加密是可逆的

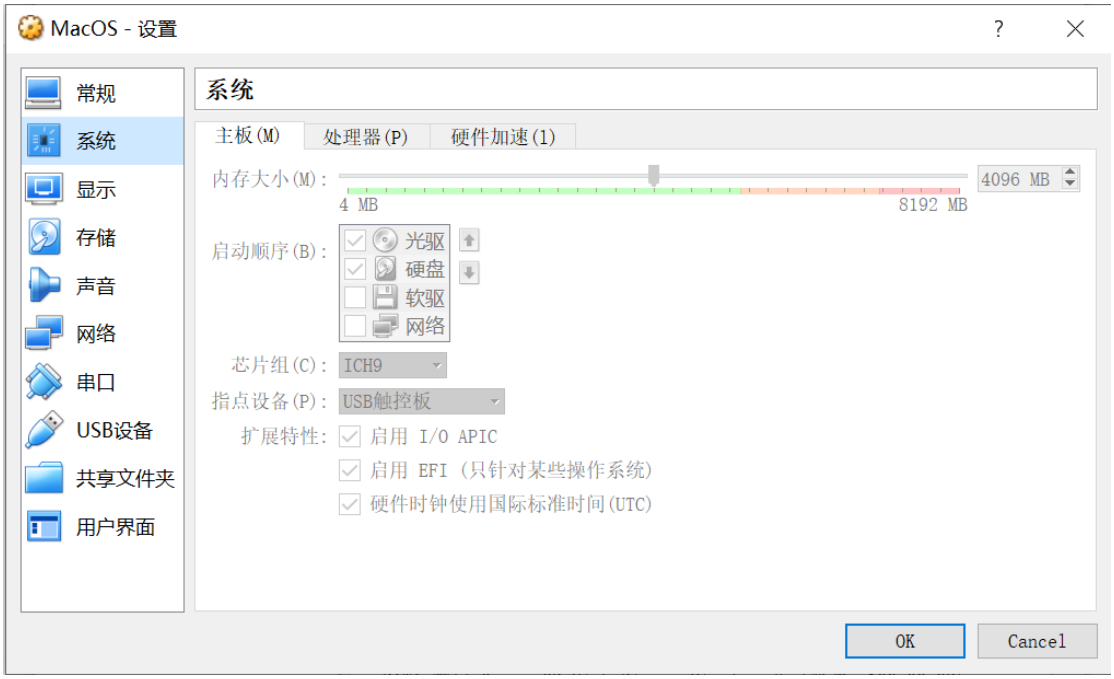


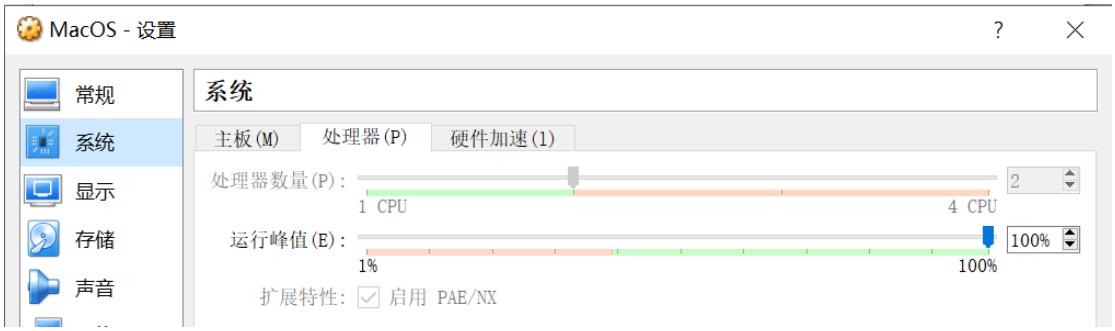
2、 Encrypt a PKU logo with SM4/ECB and other modes 使用 SM4/ECB 和其他模式加密 PKU logo

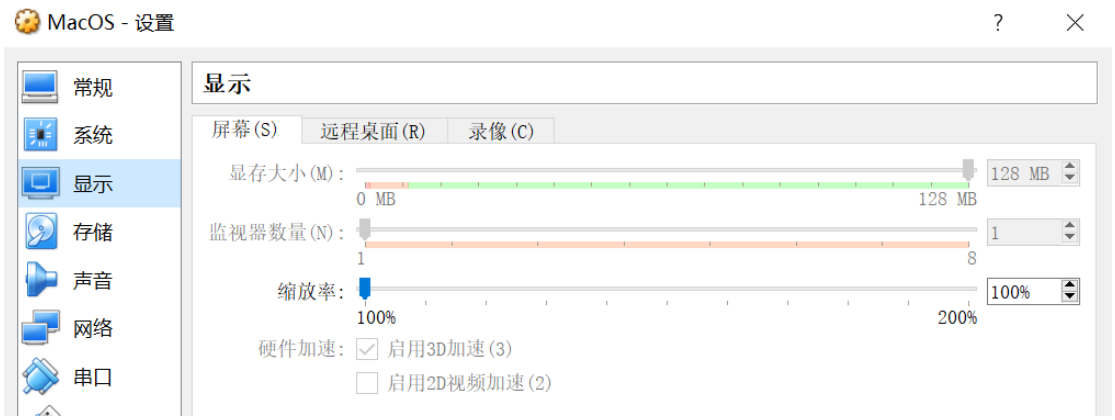
1） 在 VirtualBox 上安装 MAC 虚拟机

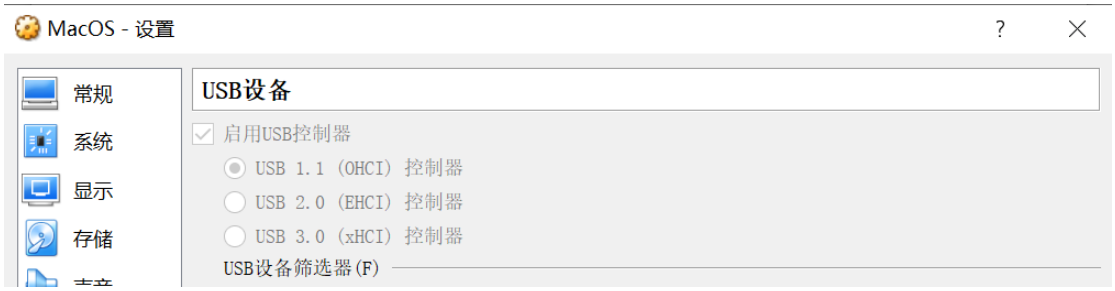

Oracle VM VirtualBox 管理器
管理(F) 控制(M) 帮助(H)
新建(N) 设置(S) 清除 启动(T)
明细(D)
虚拟电脑工具(M)
全局工具(G)
ubuntu14.04.5-2
已休眠
Kali-1
已休眠
win7
已休眠
ubuntu14.04.5-3
已休眠
MacOS
已休眠
常规
名称: MacOS
操作系统: macOS 10.13 High Sierra (64-bit)
预览
系统
内存大小: 4096 MB
处理器: 2
启动顺序: 光驱, 硬盘
芯片组: ICH9
EFI: 已启用
硬件加速: VT-x/AMD-V, 嵌套分页, PAE/NX, 最少半虚拟化
显示
显存大小: 128 MB
硬件加速: 3D
远程桌面服务器: 已禁用
录像: 已禁用
存储
控制器: SATA
SATA 端口 0: macOS High Sierra Final.vmdk (普通, 100.00 GB)
SATA 端口 1: [光驱] 没有盘片

相关设置如下


MacOS - 设置
常规
系统
显示
存储
声音
网络
串口
USB设备
共享文件夹
用户界面
系统
主板(M)
处理器(P)
硬件加速(1)
内存大小(M):
4 MB
8192 MB
4096 MB
启动顺序(B):
光驱
硬盘
软驱
网络
芯片组(C):
ICH9
指点设备(P):
USB触控板
扩展特性:
启用 I/O APIC
启用 EFI (只针对某些操作系统)
硬件时钟使用国际标准时间(UTC)
OK
Cancel







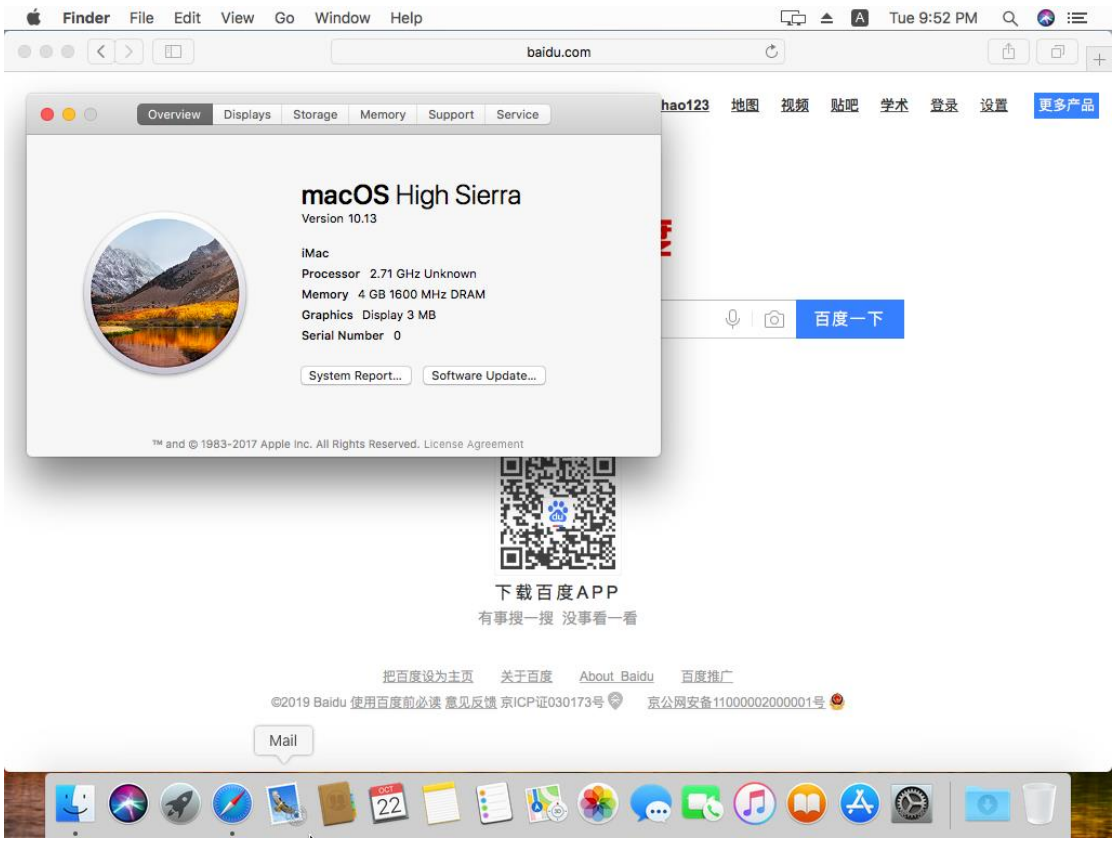
进入 VirtualBox 安装目录，输入如下命令；其中 MacOS 是虚拟机名字

```
VBoxManage.exe modifyvm MacOS --cpuidset 00000001 000106e5 00100800
0098e3fd bfebfbff
VBoxManage setextradata MacOS
"VBoxInternal/Devices/efi/0/Config/DmiSystemProduct" "iMac11,3"
VBoxManage setextradata MacOS
"VBoxInternal/Devices/efi/0/Config/DmiSystemVersion" "1.0"
VBoxManage setextradata MacOS
"VBoxInternal/Devices/efi/0/Config/DmiBoardProduct" "Iloveapple"
VBoxManage setextradata MacOS "VBoxInternal/Devices/smc/0/Config/DeviceKey"
"ourhardworkbythesewordsguardedpleasedontsteal(c)AppleComputerInc"
```

```
VBoxManage setextradata MacOS
"VBoxInternal/Devices/smc/0/Config/GetKeyFromRealSMC" 1
```

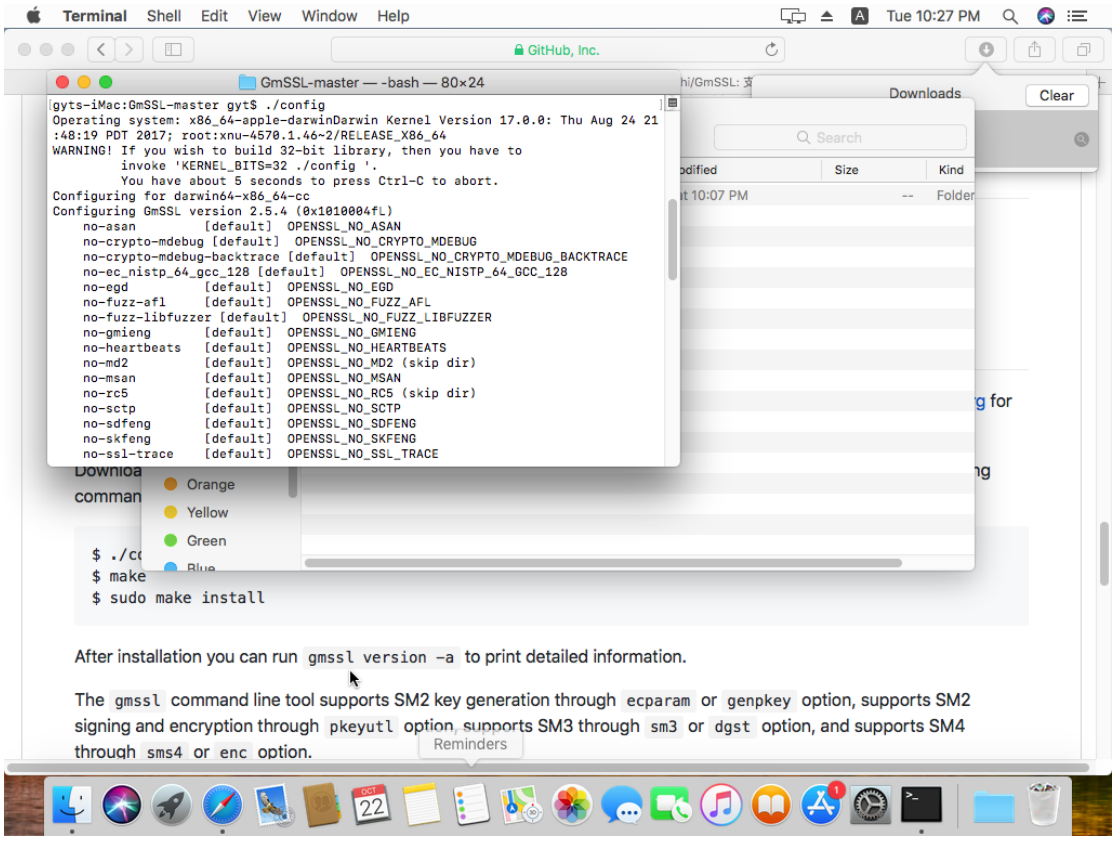
下载好 macOS High Sierra 10.13 VMDK 镜像，在虚拟机中添加硬盘

安装完成后效果图

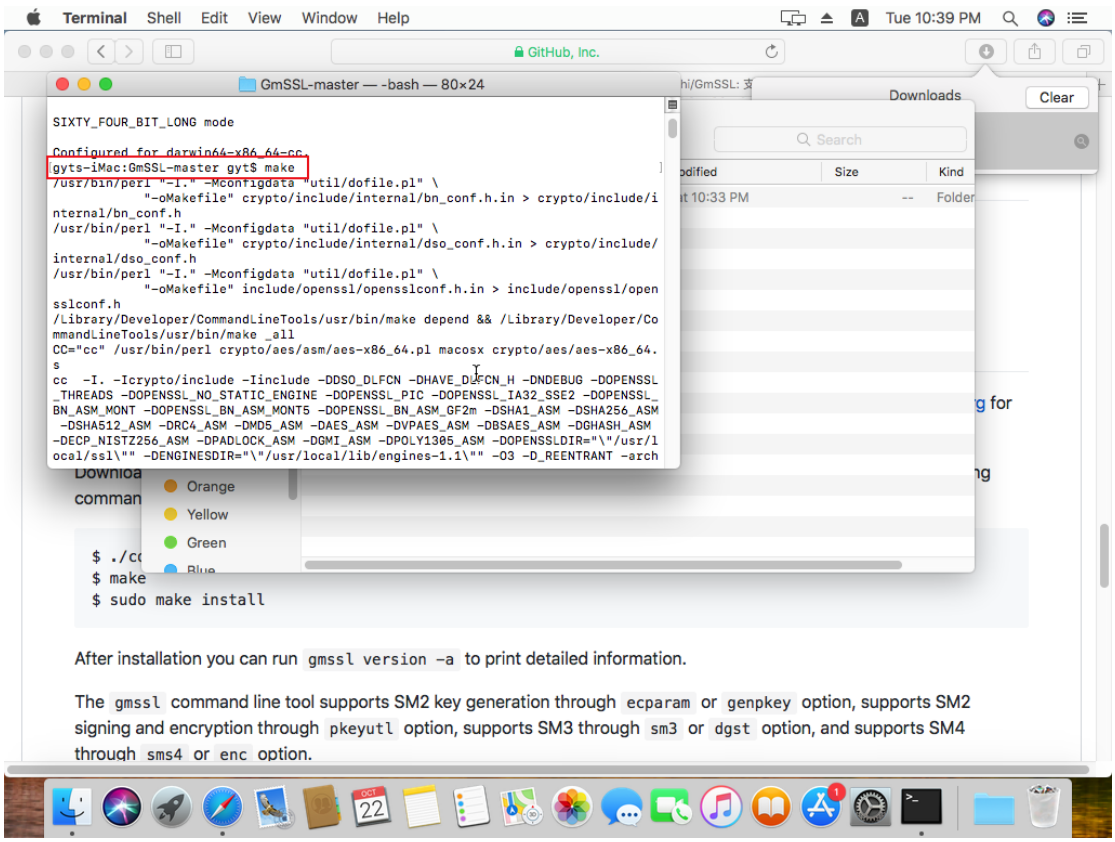


2） 安装必要的软件包

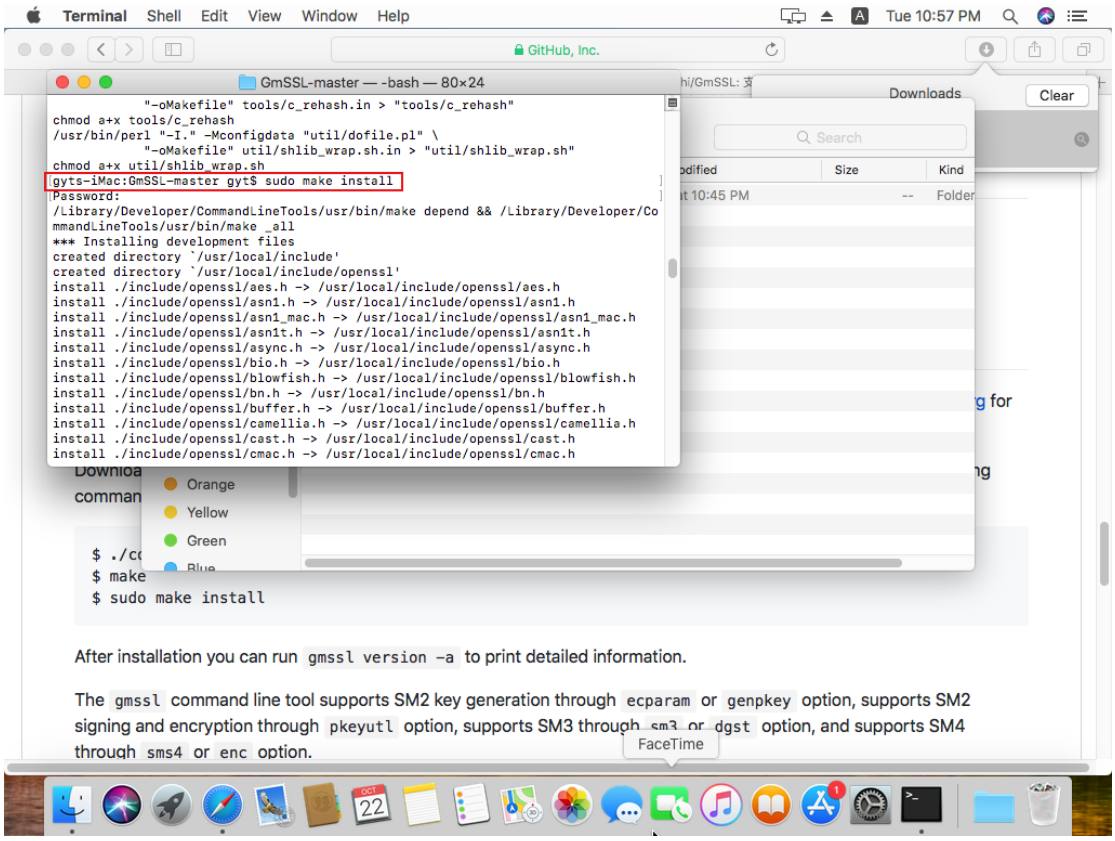
下载 GmSSL，进入其主目录执行./config



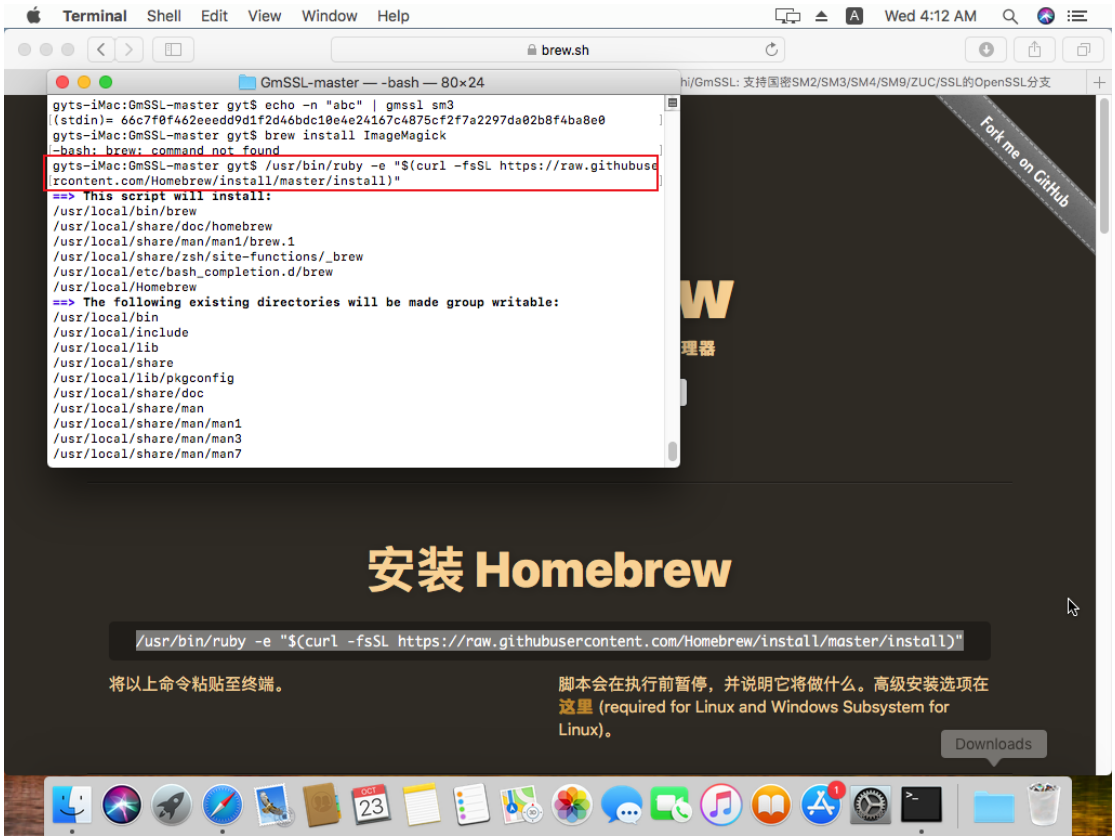
执行 make



执行 sudo make install



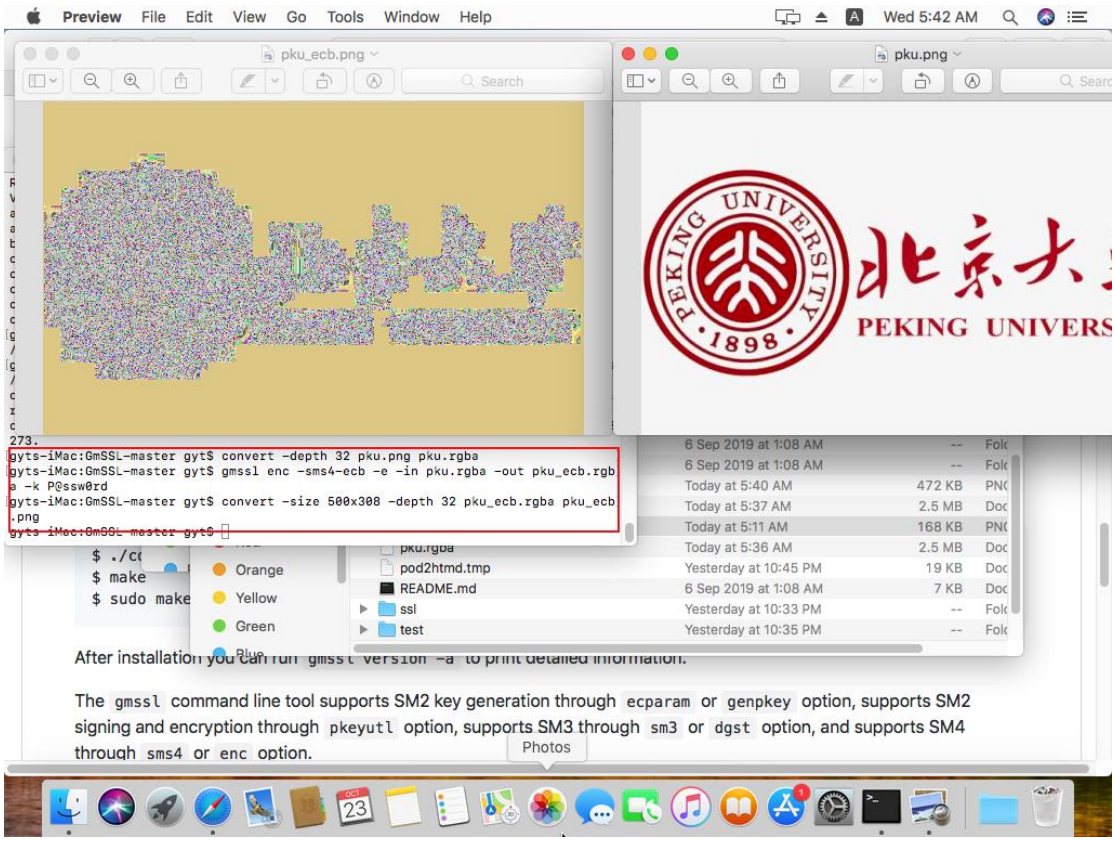
安装包管理工具 Homebrew



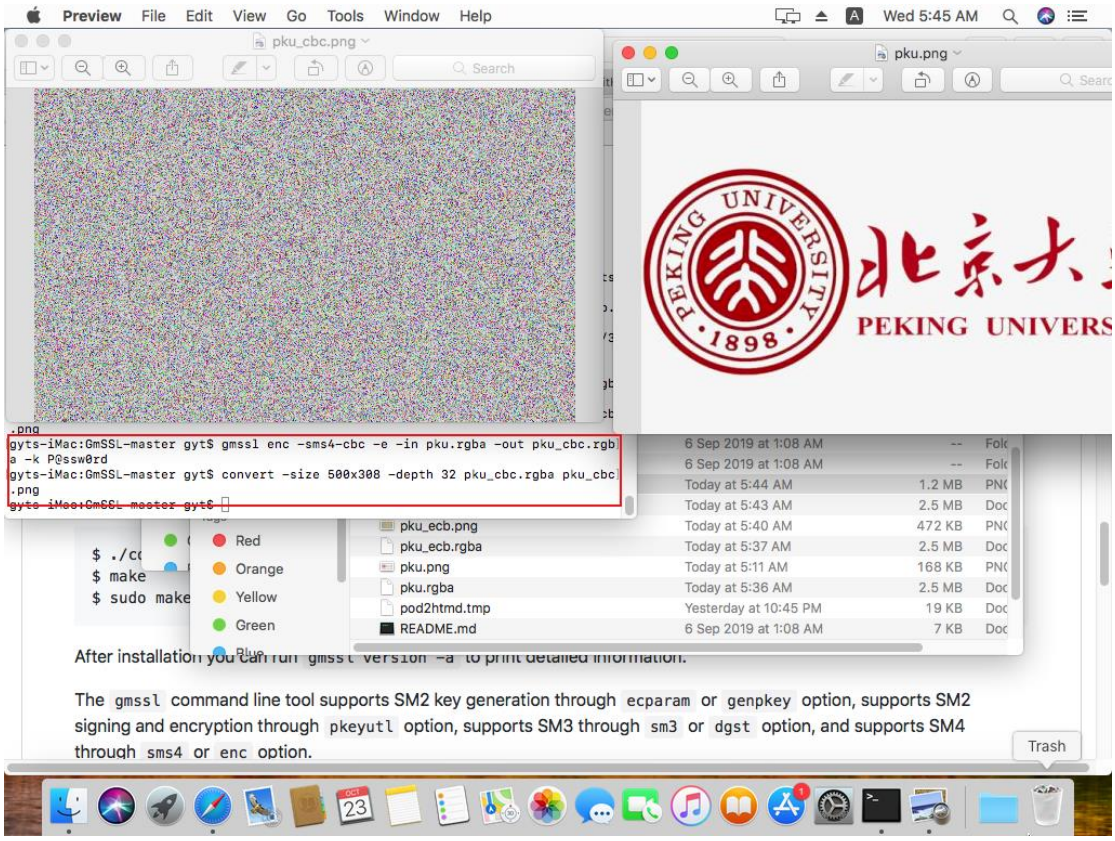
安装 ImageMagick 软件包

3） 实验结果展示

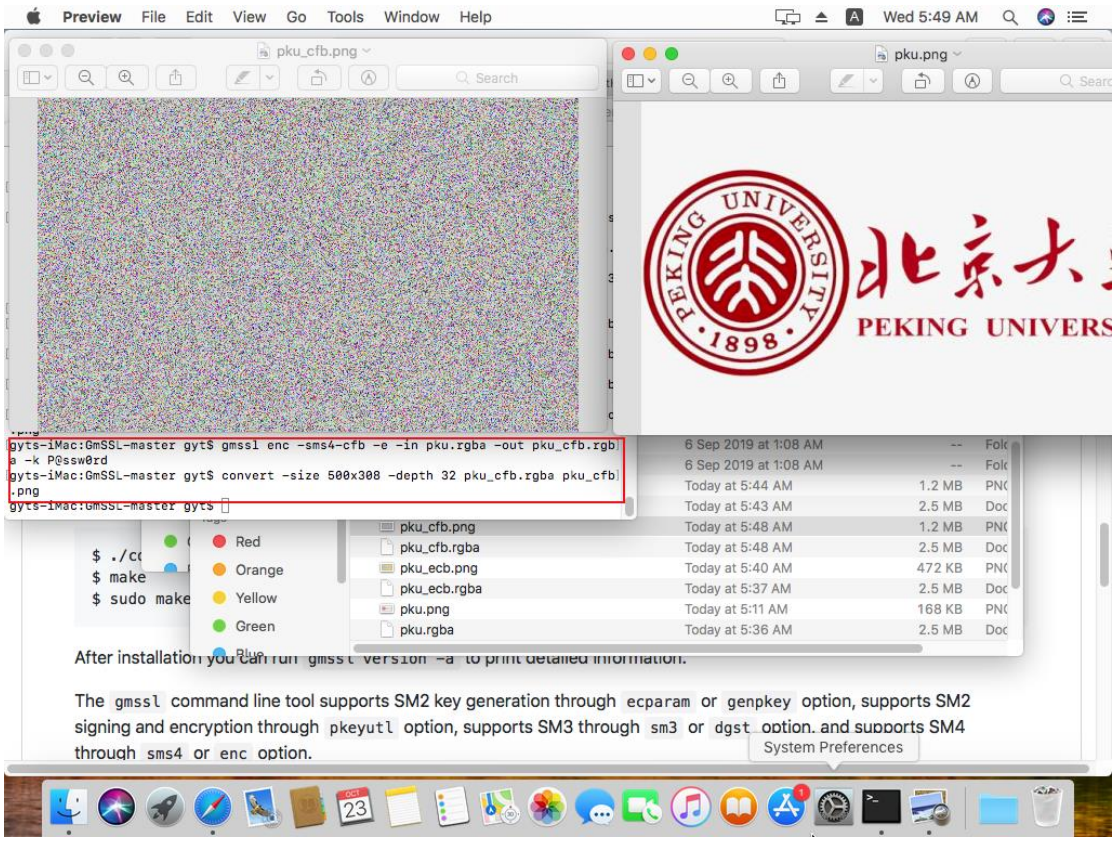
SMS4-ECB



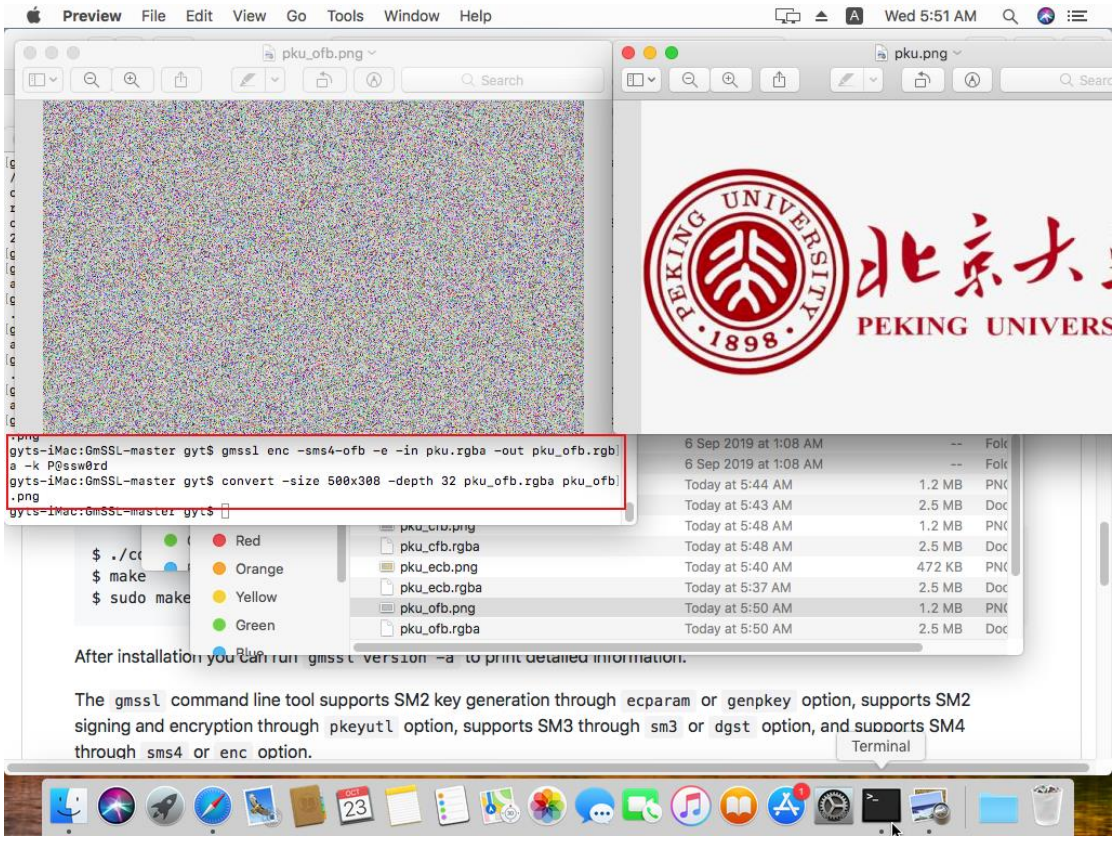
SMS4-CBC



SMS4-CFB



SMS4-OFB



SMS4-CTR