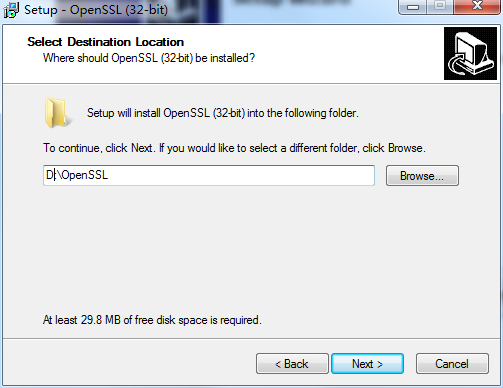
## 1.安装OpenSSL(Win32) 0.9.8l

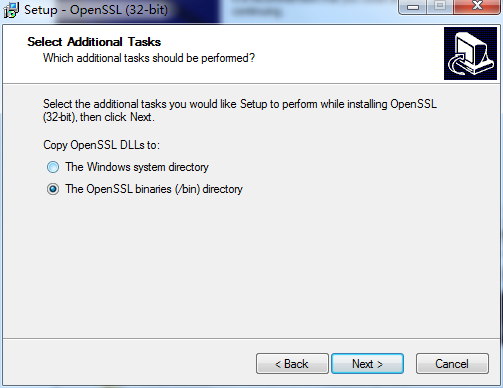
解压压缩包, 双击exe文件:



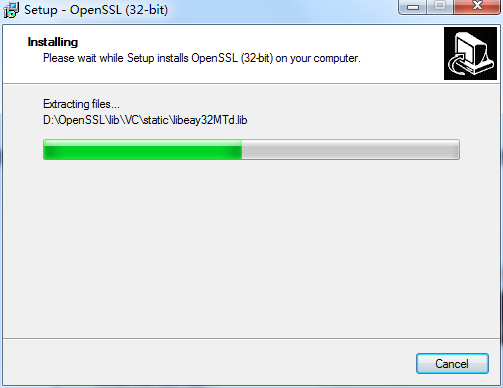
选择安装路径:



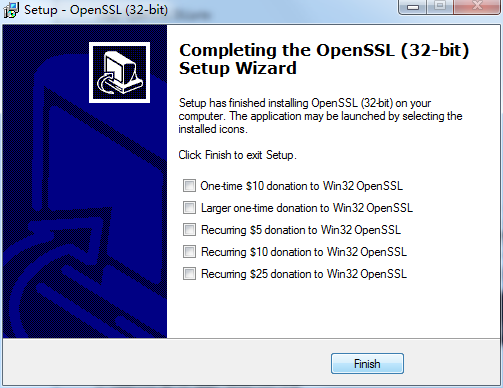
选择工具安装位置:



安装中:



安装完成:



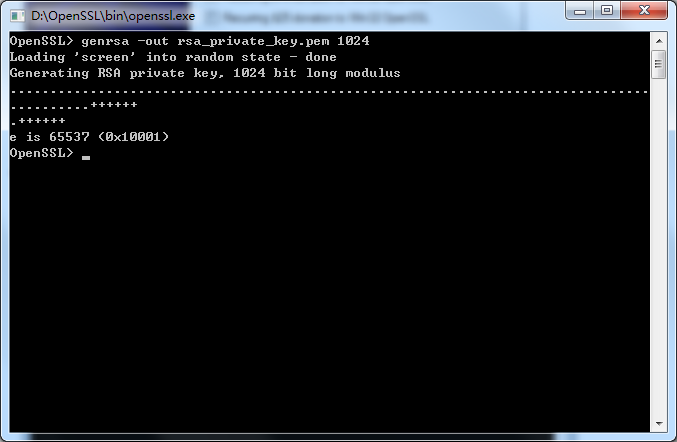
## 2.生成RSA密钥

进入OpenSSL安装目录的bin文件夹, 双击openssl.exe:

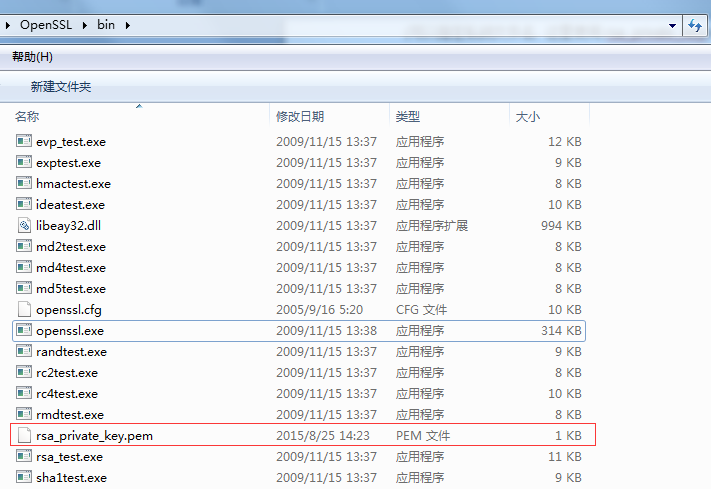


输入genrsa -out rsa\_private\_key.pem 1024:

(可以指定私钥文件名, 这里使用rsa\_private\_key)



在bin目录下生成了RSA私钥:



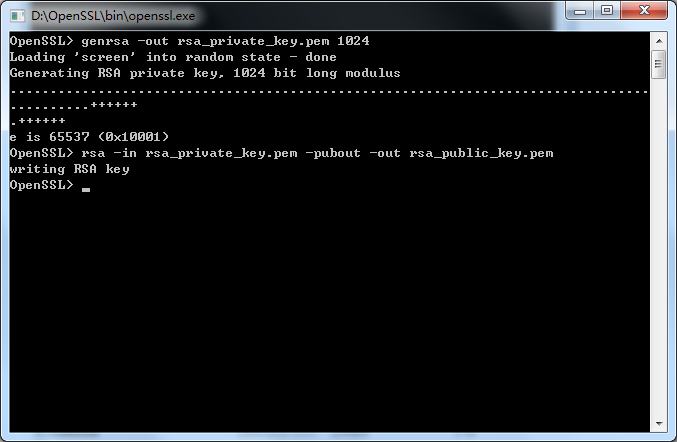
如果使用JAVA语言开发，需要将PKCS1格式私钥转换成PKCS8格式：

openssl pkcs8 -topk8 -in rsa\_private\_key.pem -out pkcs8\_rsa\_private\_key.pem -nocrypt

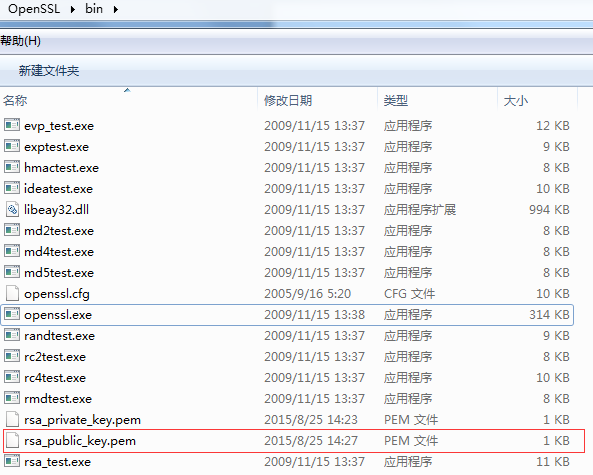
## 3.生成RSA公钥

在刚才打开的窗口继续输入 rsa -in rsa\_private\_key.pem -pubout -out rsa\_public\_key.pem

(可以指定私钥文件名, 这里使用rsa\_public\_key)



在bin目录下生成了RSA公钥:



私钥仅供商户自己使用, 请妥善保存, 不要轻易泄露. 公钥则给国采使用.