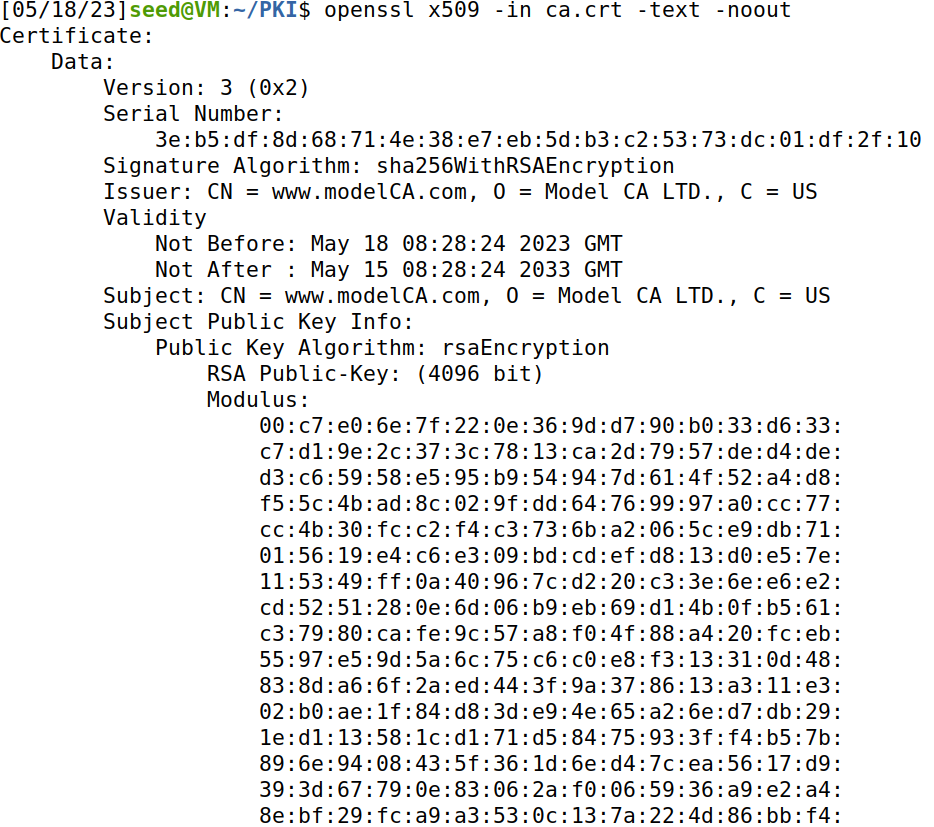
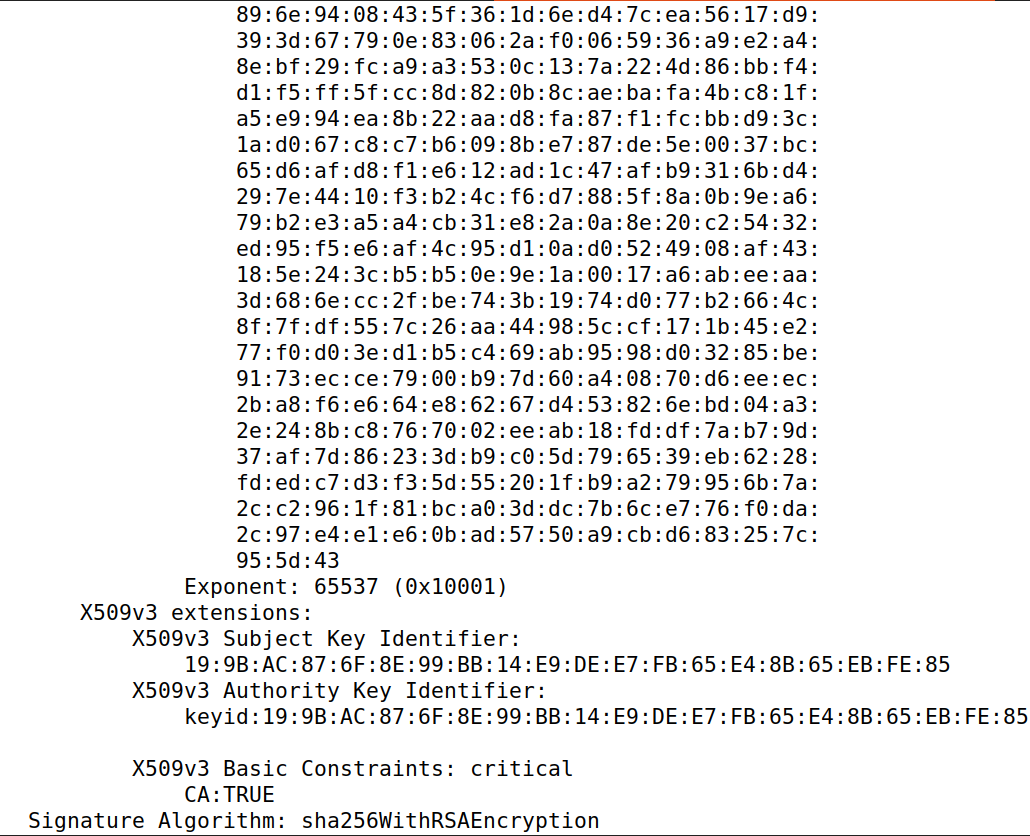
|  |
| --- |
| 哈尔滨工业大学(深圳) |
| **《网络与系统安全》 实验报告** |
|  |
| 实验四  PKI 实验  学 院: 计算机科学与技术   |  |  | | --- | --- | | 姓 名: | 宗晴 | | 学 号: | 200110513 | | 专 业: | 计算机类 | | 日 期: | 2023年5月 | |

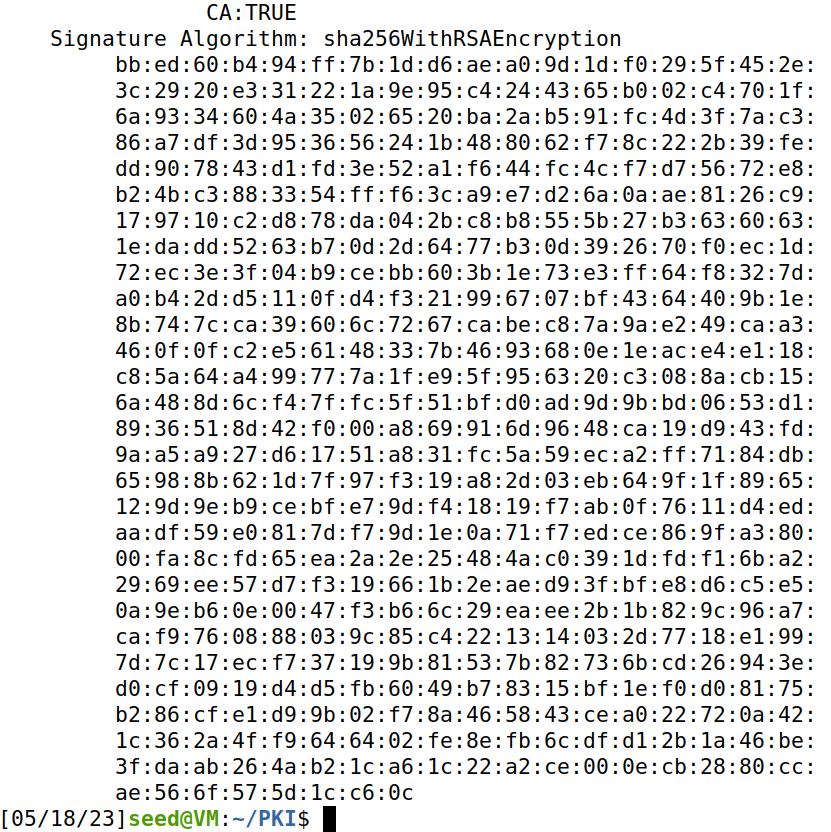
1. 根据如下命令查看证书信息，并回答下面两个问题。

命令为：openssl x509 -in ca.crt -text -noout。

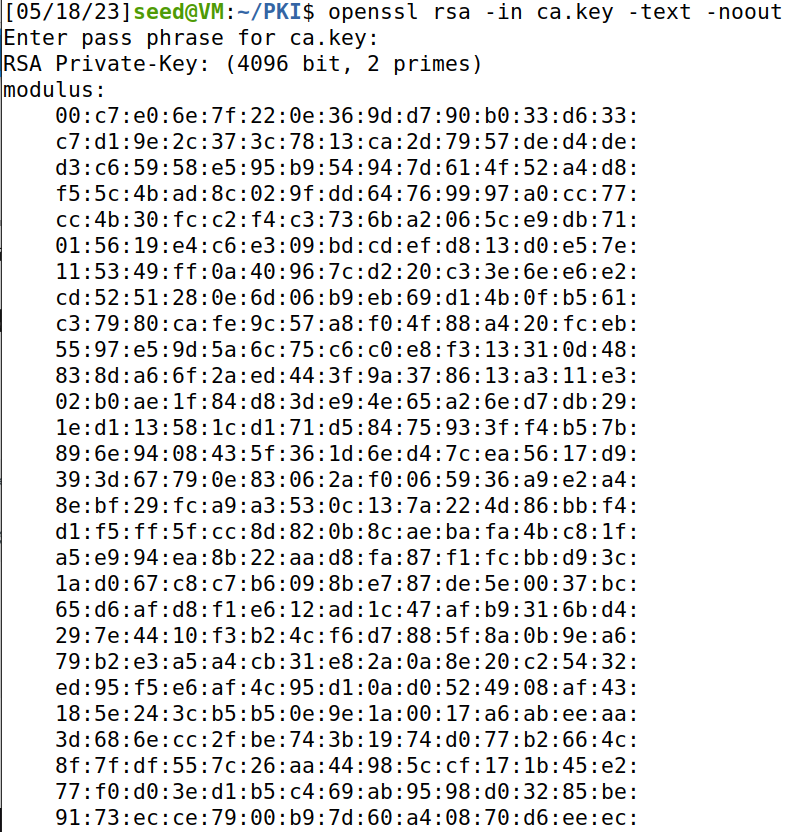
命令openssl x509 -in ca.crt -text –noout的结果如下图所示;

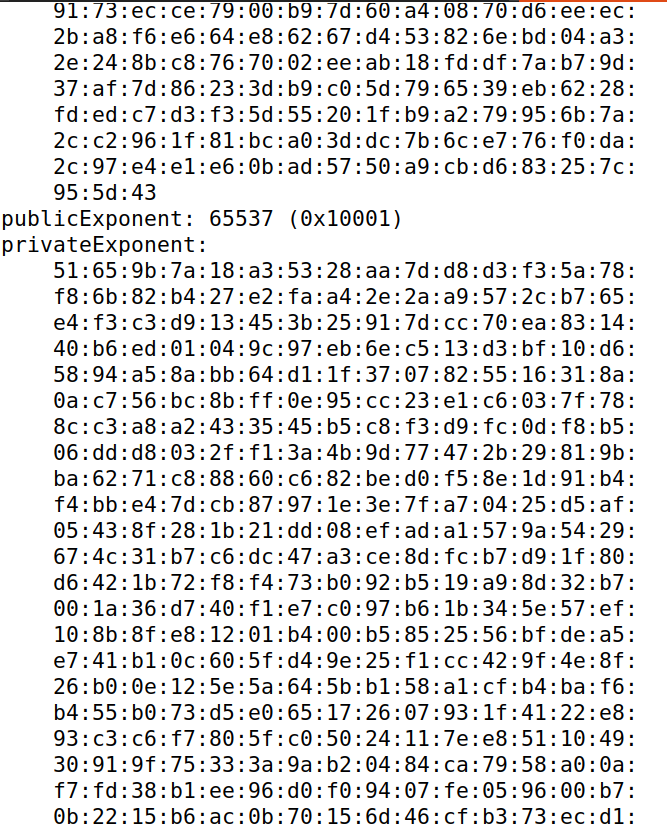


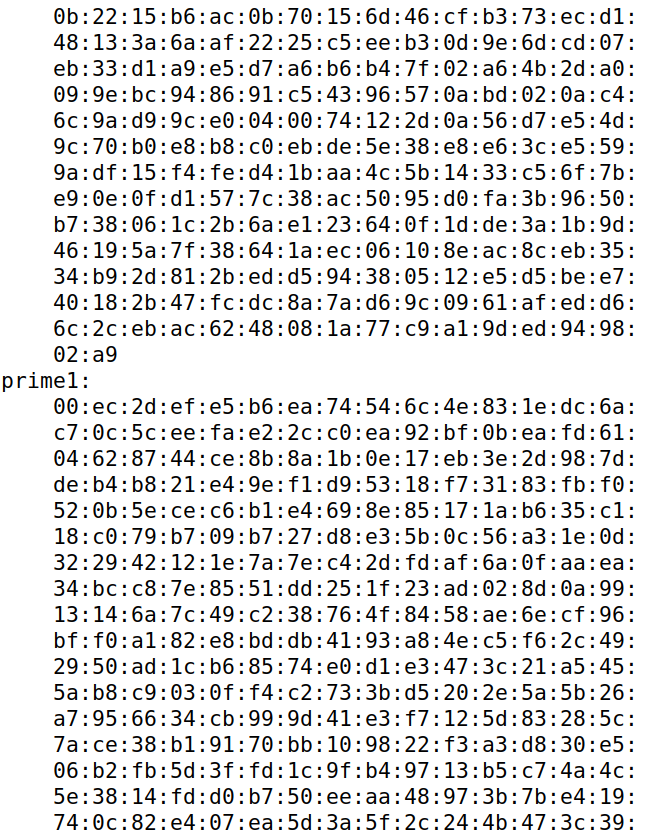


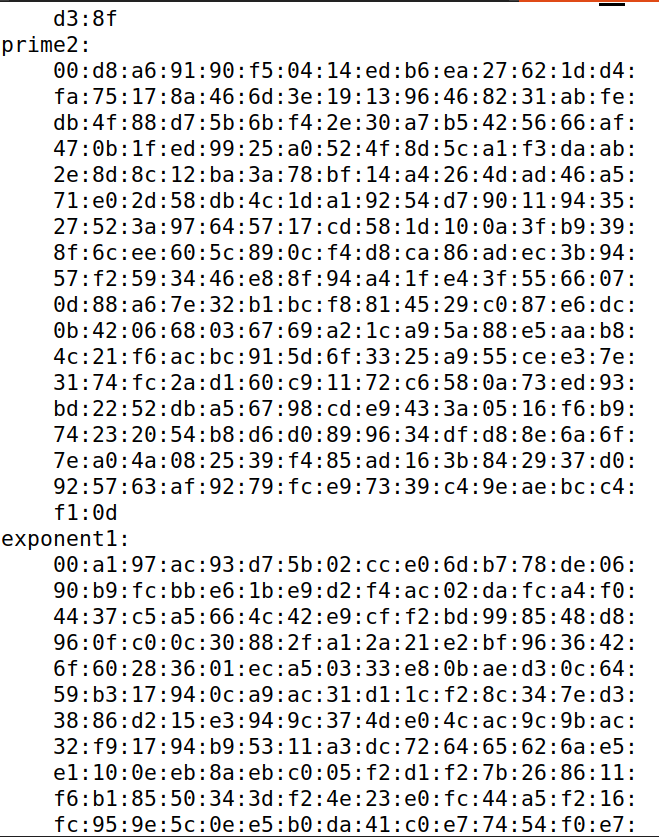


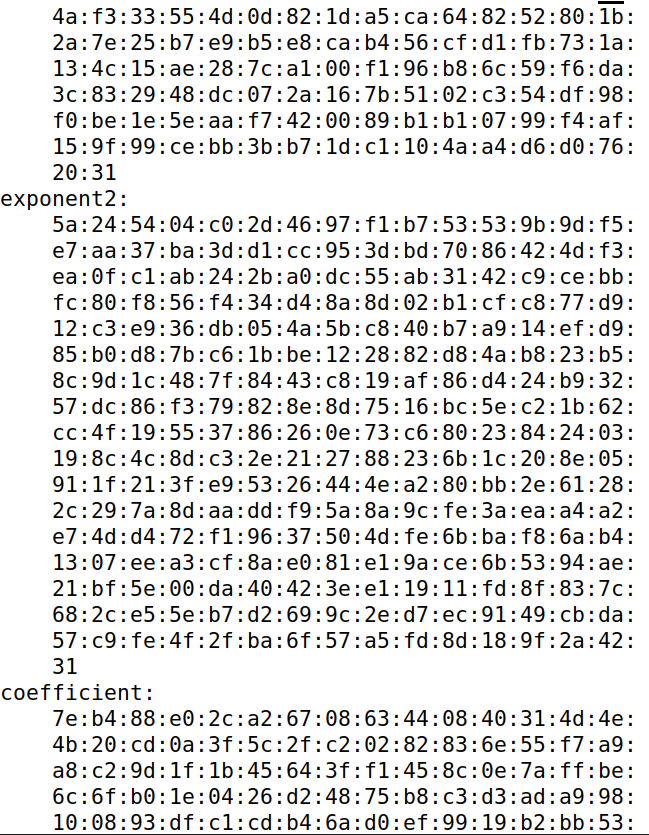
命令openssl rsa -in ca.key -text -noout的结果如下图所示;

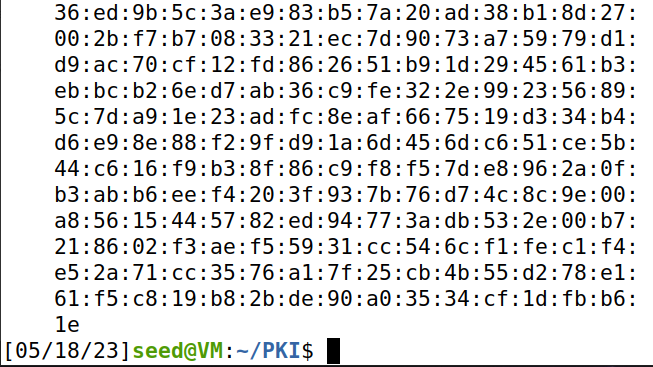












1. 证书的哪部分内容表明这是证书的持有方？

C:\Users\lenovo\AppData\Roaming\Tencent\Users\691745382\QQ\WinTemp\RichOle\8@PQ$L4NL9`AIFTFOD_N9GX.png

如上图所示，证书的该部分内容表明这是证书的持有方。

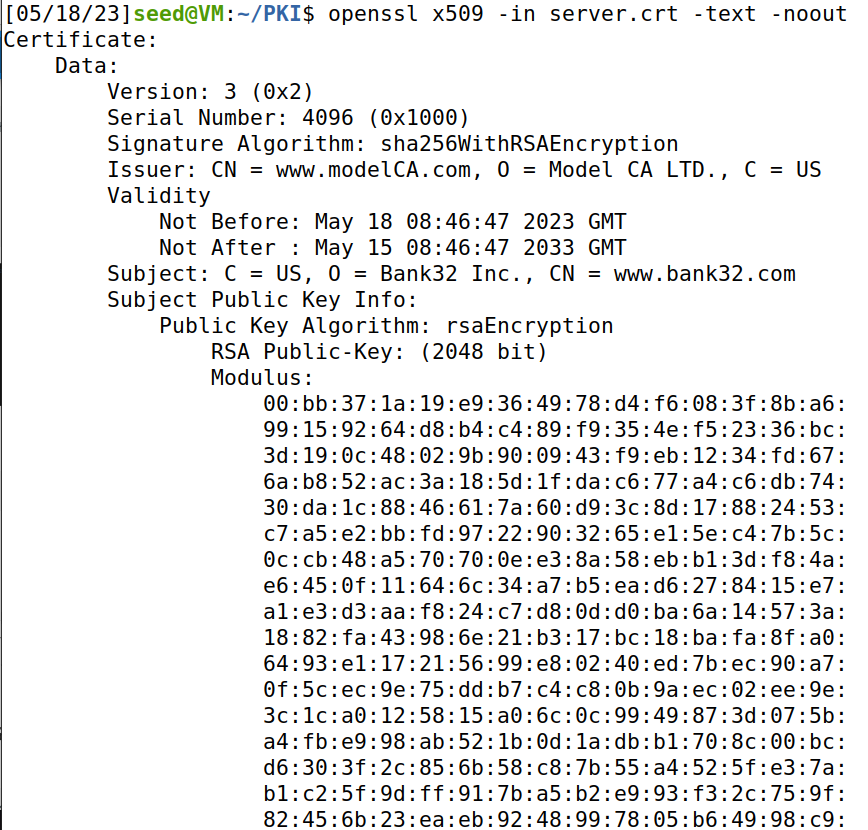
（2）从证书的哪部分内容可以看出这是自签名的证书？

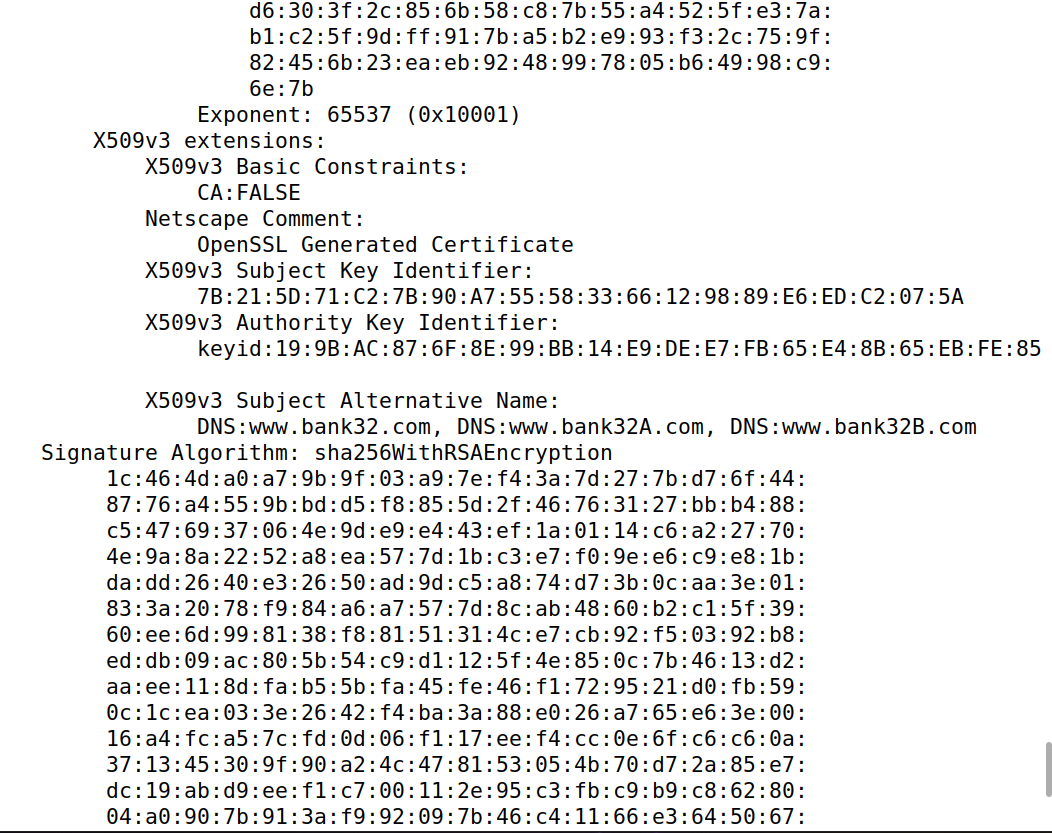
C:\Users\lenovo\AppData\Roaming\Tencent\Users\691745382\QQ\WinTemp\RichOle\EZD7CK%)K~_PI{F[7M[EX2L.png

如上图所示，该行表示证书的签发机构，可以看出与证书的持有方相同，因此表明这是自签名的证书

1. 用如下命令查看[www.bank32.com](http://www.bank32.com)的服务器证书，至少说出与ca.crt的证书的两点不同。

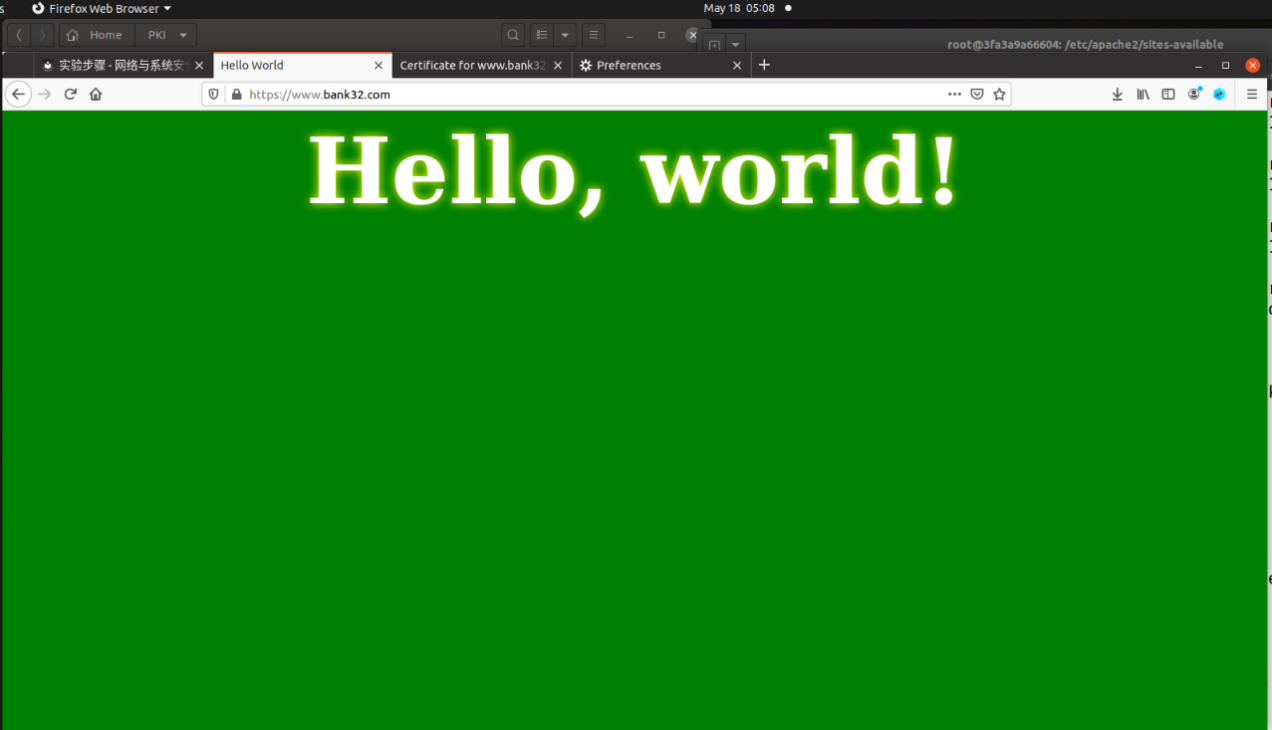
openssl x509 -in server.crt -text -noout：





与ca.cr的证书的不同之处在于：证书的拥有者与ca.cr不同，此处为[www.bank32.com](http://www.bank32.com)所拥有，且不再与证书的签发机构相同，不再是自签名。证书的有效时间也不同。此外，RSA Public-Key的长度不同，此处为2048bit，而ca.cr中是4096bit。Serial Number的格式不同。

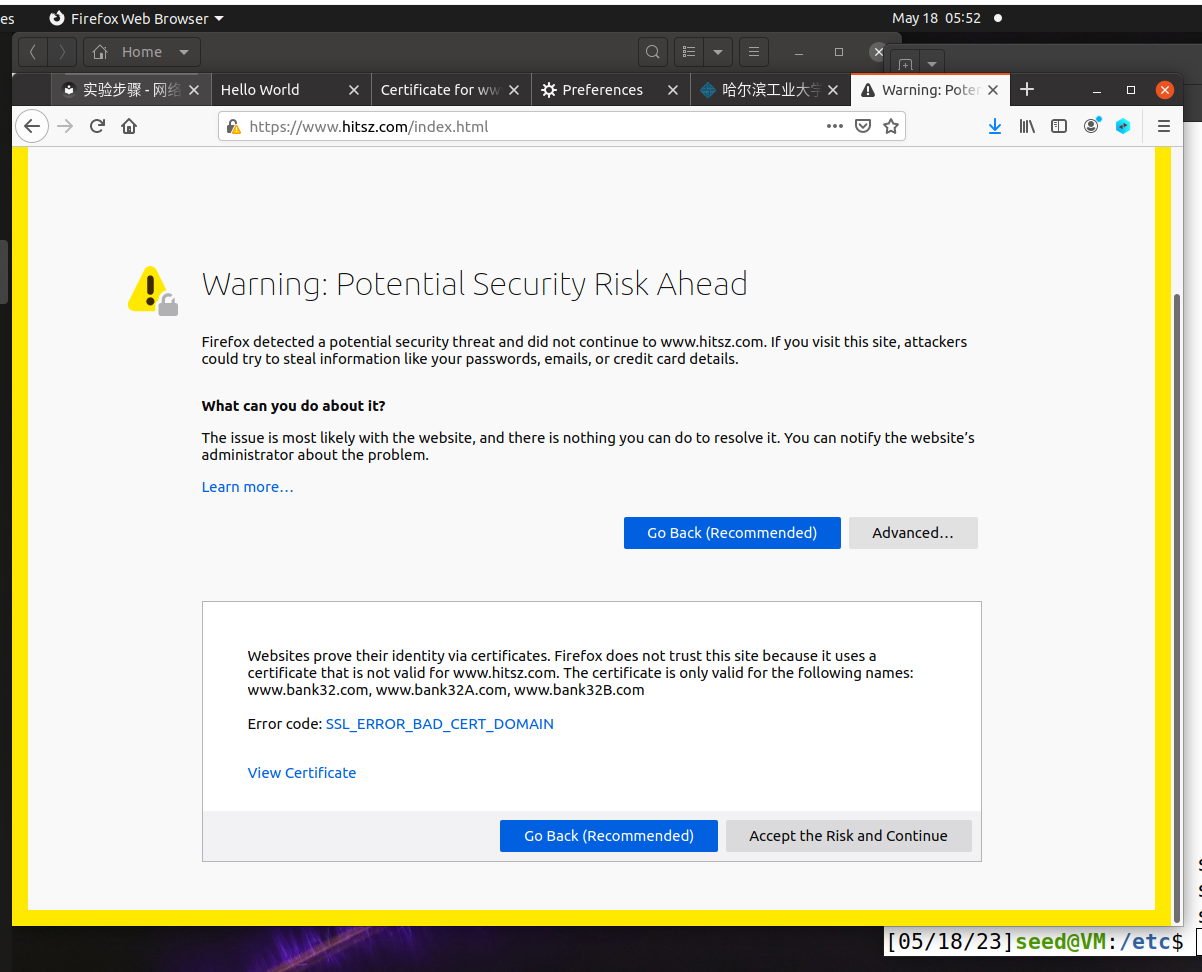
1. 请将能够正确访问www.bank32.com的截图贴在下面。



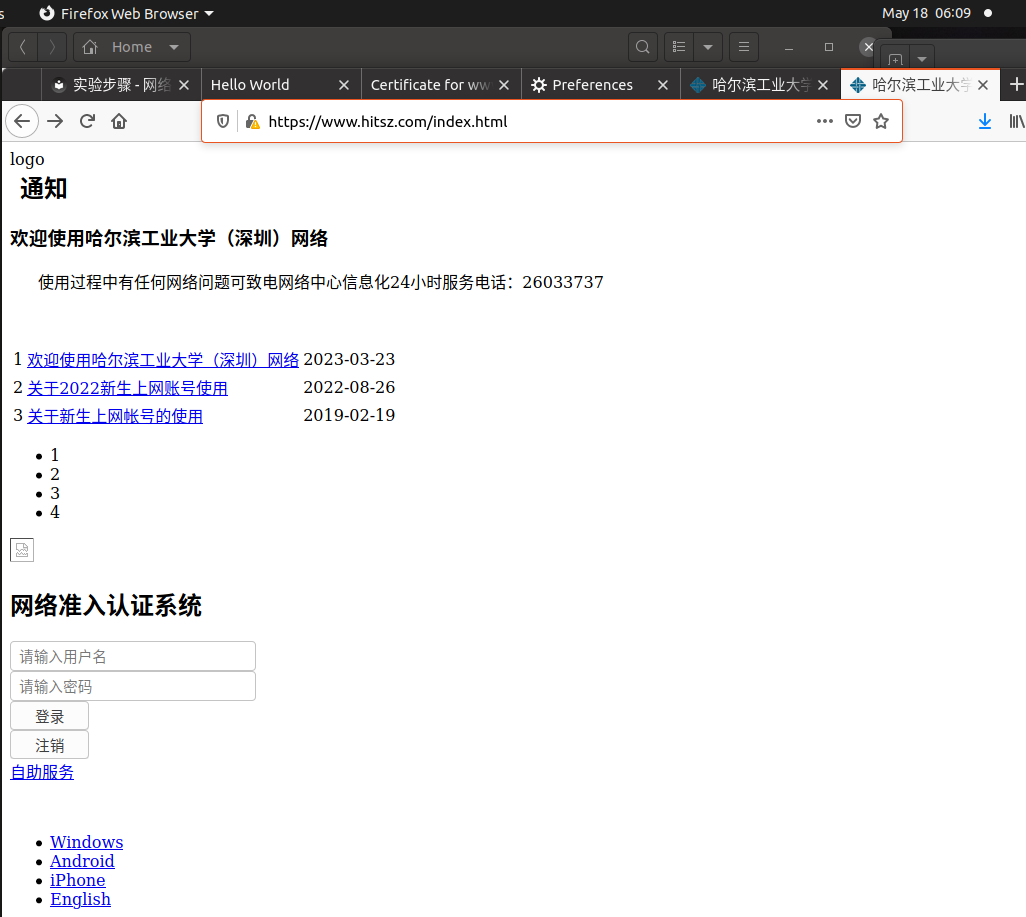
1. 将能够拦截访问一个（例如www.hitsz.edu.cn）网站的截图和CA被劫持后能够正常访问的截图贴在下面。并分析说明。（建议大家随机选取一个网站，不使用[www.hitsz.edu.cn](http://www.hitsz.edu.cn)）

我选取的网站是校园网的登陆界面，使用的网址是www.hitsz.com

能够拦截访问www.hitsz.com网站的截图如下：



CA被劫持后能够正常访问的截图如下：



1. 分析CA证书各密码算法的作用。

对称加密：发送双发使用相同的密钥对消息进行加解密，常见的对称加密为DES、3DES,AES等。特点是效率高，但需要进行密钥分发，且无法进行身份认证。

非对称加密：发送双方各自拥有一对公钥私钥，其中公钥是公开的，私钥是保密的。当发送方向接收方发送消息时，发送方利用接收方的公钥对消息进行加密，接收方收到消息后，利用自己的私钥解密就能得到消息的明文。可以进行身份认证。非对称加密方法有RSA、Elgamal、ECC等。

单向散列的哈希算法：根据任意长度的数据生成固定长度的摘要，若数据稍有不同，则摘要完全不同。数据不可逆，即不能通过摘要生成数据，可以保证数据完整性。常见的方法有sha1，md5等。