|  |
| --- |
| 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: 计算机科学与技术学院   |  |  | | --- | --- | | 姓 名: | 覃煜淮 | | 学 号: | 220110803 | | 专 业: | 计算机类 | | 日 期: | 2025年4月 |  一、实验过程 |

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。

1. 证书的哪部分内容表明这是证书的持有方？

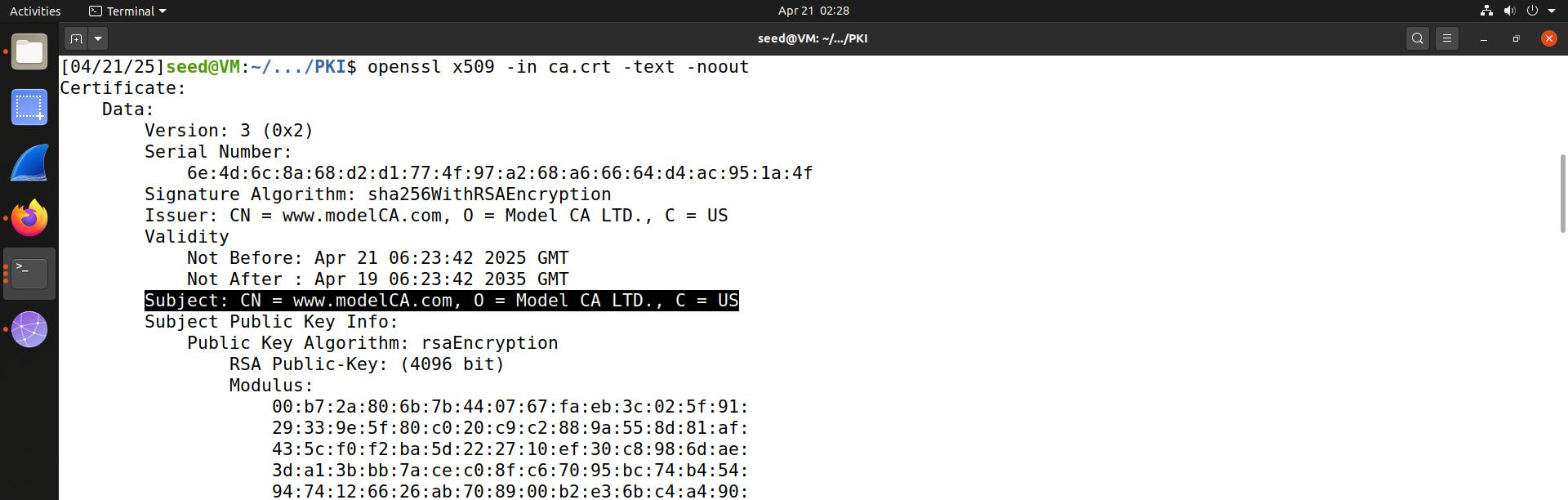
证书的持有方信息在 Subject 字段中

Common Name (CN)：证书持有方的名称；

Organization (O)：组织名称；

Country (C)：国家代码。

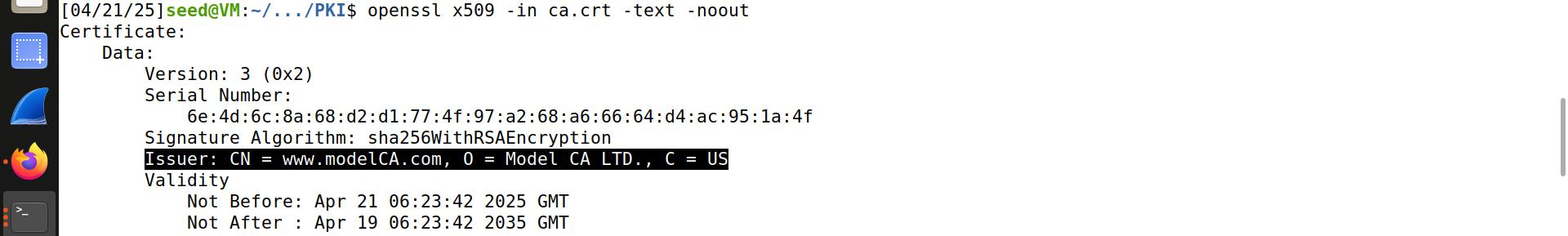
如下图所示：

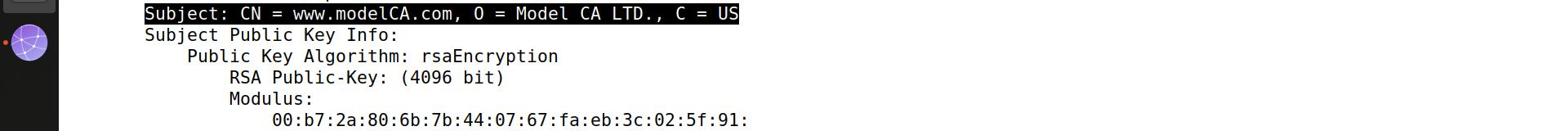


（2）从证书的哪部分内容可以看出这是自签名的证书？

自签名证书的特 点是 Issuer 和 Subject 字段的内容完全相同，可以从这两部分内容看出。

如下两图所示



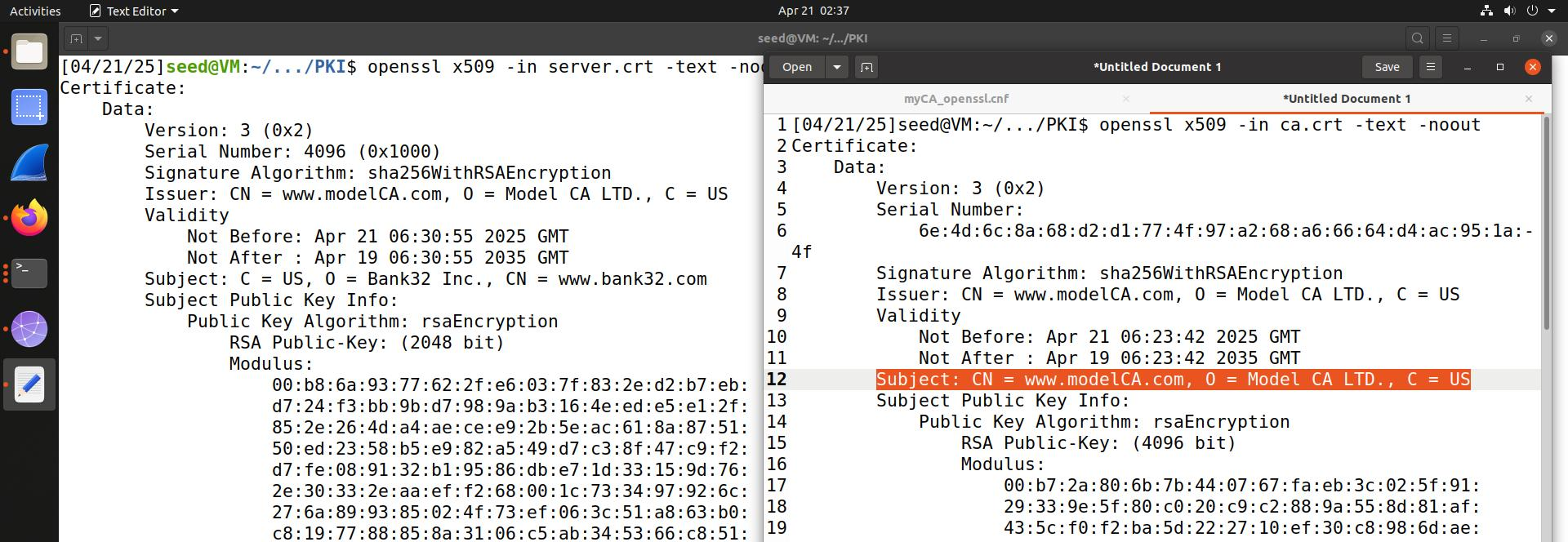


1. 用如下命令查看[www.bank32.com](http://www.bank32.com)的服务器证书，至少说出与ca.crt的证书的两点不同。

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

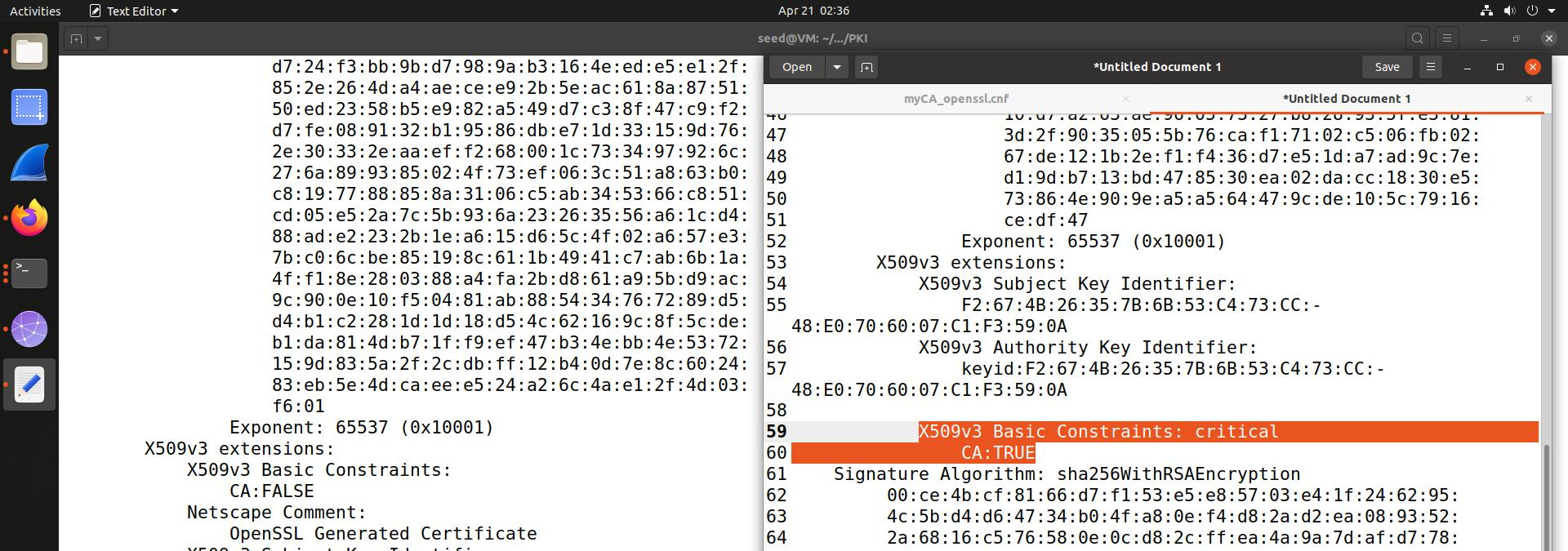
1. Subject 和 Issuer 字段相同与否

CA 证书 (ca.crt)，Subject 和 Issuer 字段通常相同，因为它是自签名证 书。 服 务 器 证 书 (server.crt) ， Subject 字 段 包 含 服 务 器 的 域 名 （www.bank32.com），Issuer 字段是签署该证书的 CA 的名称，两个字段不相 同。

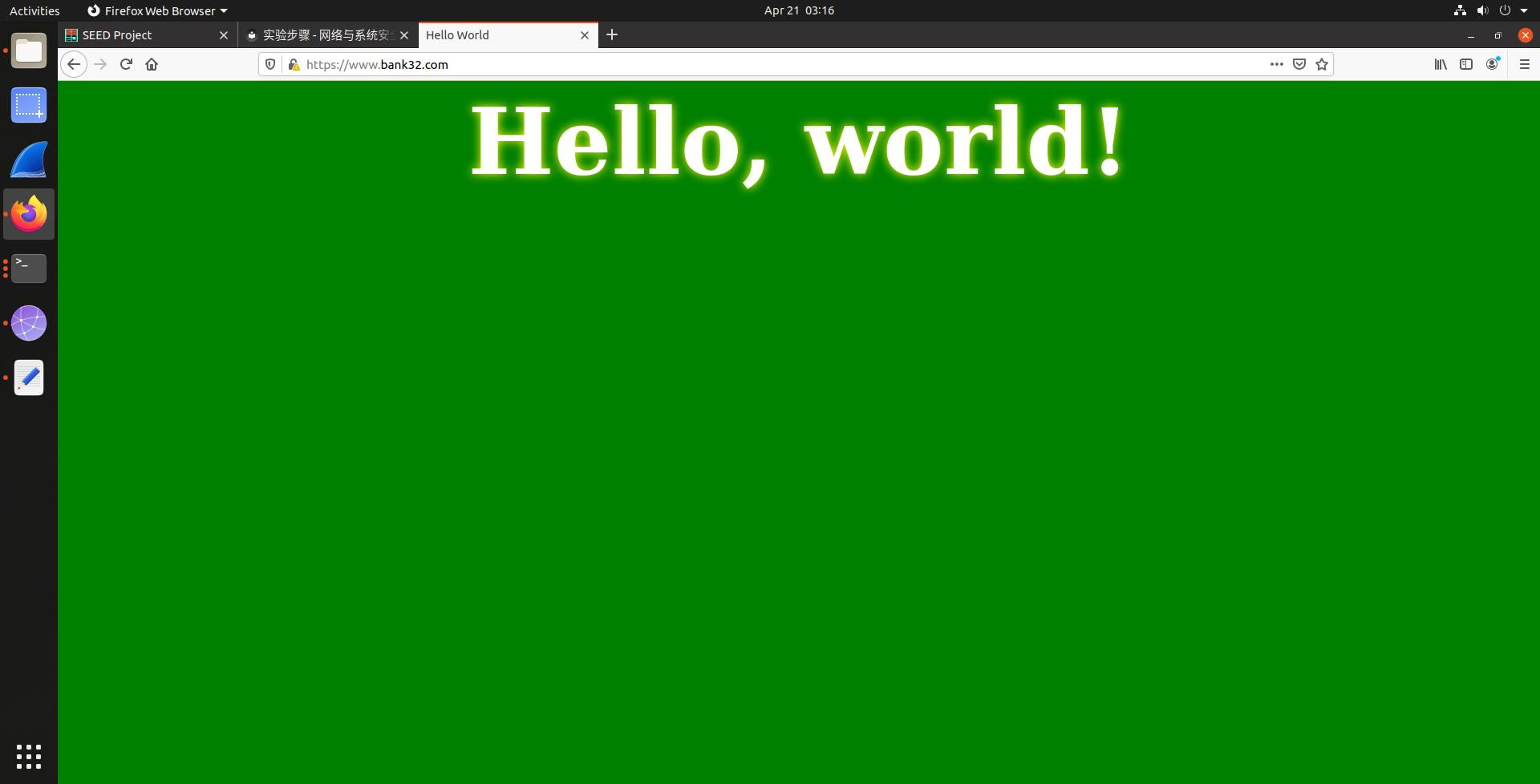


2. 证书类型和用途

CA 证书 (ca.crt)用于签署其他证书（如服务器证书、客户端证书）， CA:TRUE，表明这是一个 CA 证书。 服务器证书 (server.crt)用于标识特定的服务器（如 www.bank32.com）， CA:FALSE，表明这不是一个 CA 证书。

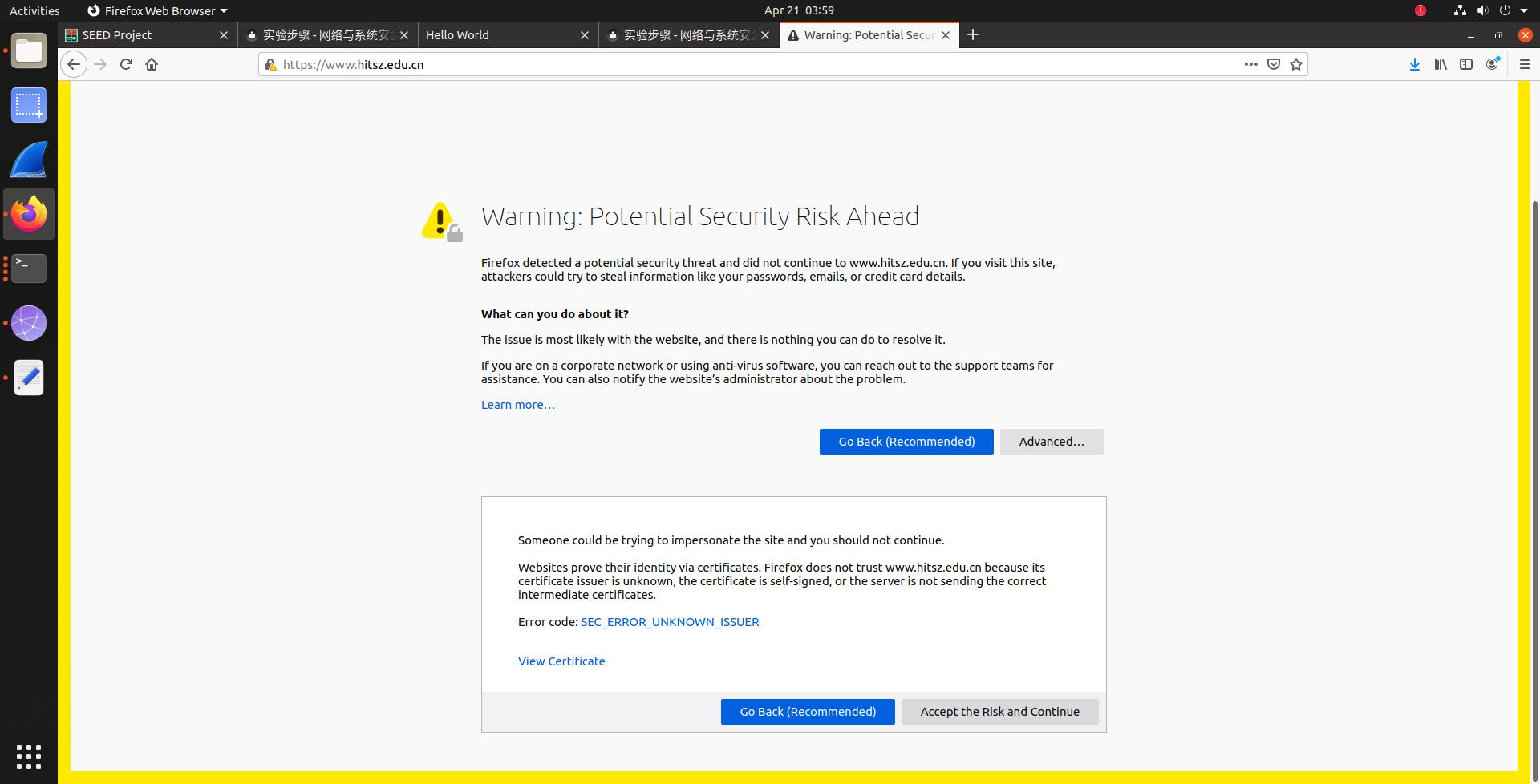


1. 请将能够正确访问www.bank32.com的截图贴在下面。



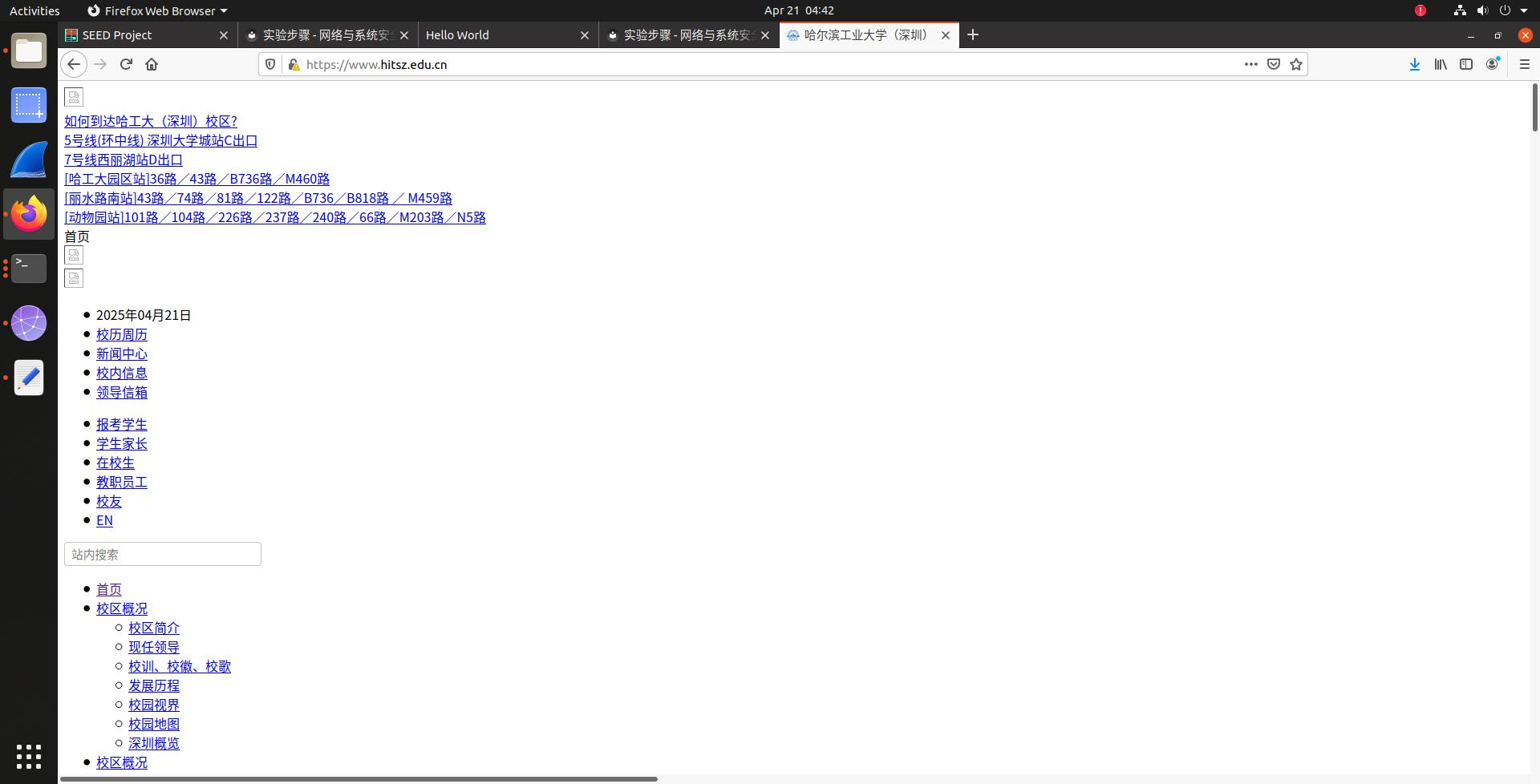
1. 将能够拦截访问一个（例如www.hitsz.edu.cn）网站的截图和CA被劫持后能够正常访问的截图贴在下面。并分析说明。（建议大家随机选取一个网站，不使用[www.hitsz.edu.cn](http://www.hitsz.edu.cn)）

能够拦截访问一个（例如 www.hitsz.edu.cn）网站：



分析说明：浏览器明确警告继续访问可能导致敏感信息（密码、信用卡等）被窃 取，这是典型的中间人攻击（MITM）被检测到的场景，因为攻击者（或实验中的 自建 CA）无法提供受浏览器信任的合法证书。在未劫持合法 CA 的情况下，自签名或非法证书会被浏览器拦截，从而保护用户安全，说明了 HTTPS 依赖证书信任链的重要性。

CA 被劫持后能够正常访问：



分析说明：实验中通过劫持合法 CA 为目标网站生成了“合法”证书，浏览器不 再显示证书警告，页面可正常访问，但实际流量已被攻击者解密和监控。

使用被劫持的 CA 私钥签发伪造的证书，并将其部署在攻击者的代理 服务器上。客户端访问目标网站时，攻击者的代理服务器将伪造的证书发送给客 户端，由于客户端信任被劫持的 CA，伪造的证书被接受，通信继续进行，但所 有流量都经过攻击者的代理服务器。

1. 分析CA证书各密码算法的作用。

**对称加密算法**

作用：对数据进行加密和解密操作，保证数据的保密性。在CA证书相关的应用中，对称加密算法可用于对敏感信息进行加密，使得只有拥有相应密钥的接收方才能解密并读取信息，防止数据在传输过程中被窃取。

特点：加密和解密使用同一个密钥，效率高，适用于大量数据的加密。

局限性：密钥分发较为困难，且无法确认数据来源。

**非对称加密算法**

作用：

实现数据加密，通过接收方的公钥加密数据，只有接收方的私钥才能解密，保证了数据的保密性。

实现数字签名，发送方使用自己的私钥对数据进行签名，接收方使用发送方的公钥验证签名，从而确认数据的来源和完整性。

特点：加密和解密密钥不同，安全性高，但算法复杂，效率相对较低。

局限性：密钥长，加密速度慢，无法对大量数据直接进行高效加密。

**单向散列算法（哈希算法）**

作用：对任意长度的数据生成一个固定长度的摘要，用于验证数据的完整性。在CA证书中，哈希算法可用于对证书中的信息生成摘要，确保在传输和存储过程中证书未被篡改。

特点：任意长度数据生成固定长度摘要，数据稍微不同摘要完全不同，且不可逆，不能通过摘要生成原始数据。

局限性：无法直接用于加密数据，只能用于数据完整性的验证。

# 二、遇到问题及解决方法

修改参数时比较懵圈，借助AI全面理解成功解决

# 三、对本次实验的建议

很好的实验，从平时上网可见的例子入手，很好地展示了证书的相关知识，通过动手了解一些基本的常识，很有意思