

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：

```
[04/21/25]seed@VM:~/.../PKI$ openssl x509 -in ca.crt -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      6e:4d:6c:8a:68:d2:d1:77:4f:97:a2:68:a6:66:64:d4:ac:95:1a:4f
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
    Validity
      Not Before: Apr 21 06:23:42 2025 GMT
      Not After : Apr 19 06:23:42 2035 GMT
    Subject: CN = www.modelCA.com, O = Model CA LTD., C = US
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (4096 bit)
      Modulus:
        00:b7:2a:80:6b:7b:44:07:67:fa:eb:3c:02:5f:91:
        29:33:9e:5f:80:c0:20:c9:c2:88:9a:55:8d:81:af:
        43:5c:f0:f2:ba:5d:22:27:10:ef:30:c8:98:6d:ae:
        3d:a1:3b:bb:7a:ce:c0:8f:c6:70:95:bc:74:b4:54:
        94:74:12:66:26:ab:70:89:00:b2:e3:6b:c4:a4:90:
```

- (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

```
[04/21/25]seed@VM:~/.../PKI$ openssl x509 -in ca.crt -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      6e:4d:6c:8a:68:d2:d1:77:4f:97:a2:68:a6:66:64:d4:ac:95:1a:4f
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
    Validity
      Not Before: Apr 21 06:23:42 2025 GMT
      Not After : Apr 19 06:23:42 2035 GMT

    Subject: CN = www.modelCA.com, O = Model CA LTD., C = US
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (4096 bit)
      Modulus:
        00:b7:2a:80:6b:7b:44:07:67:fa:eb:3c:02:5f:91:
```

2. 用如下命令查看 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。

```
[04/21/25]seed@VM:~/.../PKI$ openssl x509 -in server.crt -text -noout
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 4096 (0x1000)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
    Validity
      Not Before: Apr 21 06:30:55 2025 GMT
      Not After : Apr 19 06:30:55 2035 GMT
    Subject: C = US, O = Bank32 Inc., CN = www.bank32.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
        00:b8:6a:93:77:62:2f:e6:03:7f:83:2e:d2:b7:eb:
        d7:24:f3:bb:9b:d7:98:9a:b3:16:4e:ed:e5:e1:2f:
        85:2e:26:4d:a4:ae:ce:e9:2b:5e:ac:61:8a:87:51:
        50:ed:23:58:b5:e9:82:a5:49:d7:c3:8f:47:c9:f2:
        d7:fe:08:91:32:b1:95:86:db:e7:1d:33:15:9d:76:
        2e:30:33:2e:aa:ef:f2:68:00:1c:73:34:97:92:6c:
        27:6a:89:93:85:02:4f:73:ef:06:3c:51:a8:63:b0:
        c8:19:77:88:85:8a:31:06:c5:ab:34:53:66:c8:51:
        40:07:02:00:00:30:03:73:21:00:20:33:71:63:02:
        3d:2f:90:35:05:5b:76:ca:f1:71:02:c5:06:fb:02:
        67:de:12:1b:2e:f1:f4:36:d7:5e:1d:a7:ad:9c:7e:
        d1:9d:b7:13:bd:47:85:30:ea:02:da:cc:18:30:e5:
        73:86:4e:90:9e:a5:a5:64:47:9c:de:10:5c:79:16:
        ce:df:47
      Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Subject Key Identifier:
        F2:67:48:26:35:7B:68:53:C4:73:CC:-
      X509v3 Authority Key Identifier:
        keyid:F2:67:48:26:35:7B:68:53:C4:73:CC:-
      X509v3 Basic Constraints: critical
        CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
    00:ce:4b:cf:81:66:d7:f1:53:e5:e8:57:03:e4:1f:24:62:95:
    4c:5b:d4:d6:47:34:b0:4f:a8:0e:f4:d8:2a:d2:ea:08:93:52:
    2a:68:16:c5:76:58:0e:0c:d8:2c:ff:ea:4a:9a:7d:af:d7:78:
```

### 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。

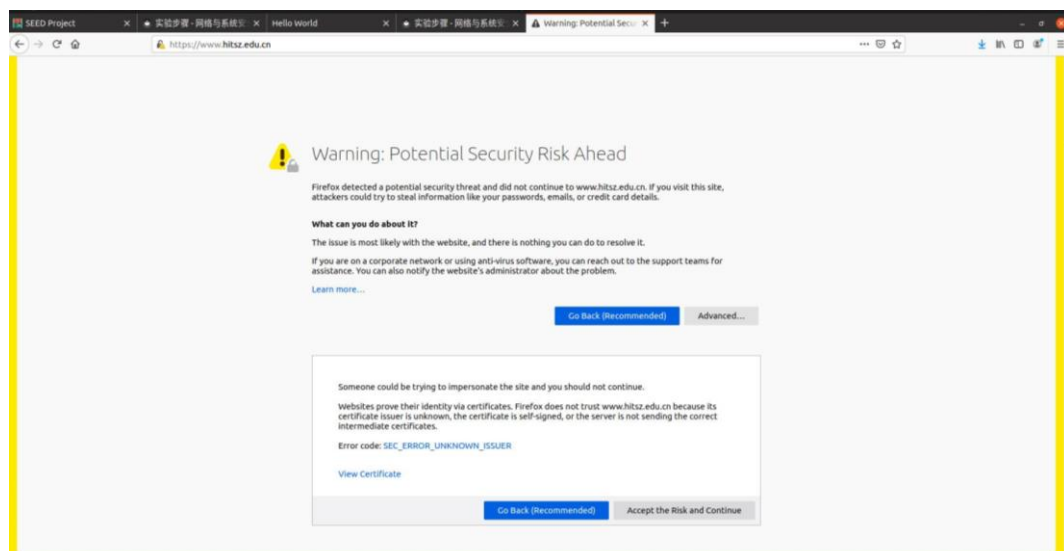
```
d7:24:f3:bb:9b:d7:98:9a:b3:16:4e:ed:e5:e1:2f:
85:2e:26:4d:a4:ae:ce:e9:2b:5e:ac:61:8a:87:51:
50:ed:23:58:b5:e9:82:a5:49:d7:c3:8f:47:c9:f2:
d7:fe:08:91:32:b1:95:86:db:e7:1d:33:15:9d:76:
2e:30:33:2e:aa:ef:f2:68:00:1c:73:34:97:92:6c:
27:6a:89:93:85:02:4f:73:ef:06:3c:51:a8:63:b0:
c8:19:77:88:85:8a:31:06:c5:ab:34:53:66:c8:51:
cd:85:e5:2a:7c:5b:93:6a:23:26:35:56:a6:1c:d4:
88:ad:e2:23:2b:1e:a6:15:d6:5c:4f:02:a6:57:e3:
7b:c0:6c:be:85:19:8c:61:1b:49:41:c7:a6:6b:1a:
4f:f1:8e:28:03:88:a4:fa:2b:d8:61:a9:5b:d9:ac:
9c:90:0e:10:f5:04:81:ab:88:54:34:76:72:09:d5:
d4:b1:c2:28:1d:1d:18:d5:4c:62:16:9c:8f:5c:de:
b1:da:81:4d:b7:1f:f9:ef:47:b3:4e:bb:4e:53:72:
15:9d:83:5a:2f:2c:db:ff:12:b4:0d:7e:8c:60:24:
83:eb:5e:4d:ca:ee:e5:2a:2d:6c:4a:e1:2f:4d:03:
f6:01
  Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Basic Constraints:
      CA:FALSE
    Netscape Comment:
      OpenSSL Generated Certificate
```

3. 请将能够正确访问 [www.bank32.com](https://www.bank32.com) 的截图贴在下面。



4. 将能够拦截访问一个（例如 [www.hitsz.edu.cn](https://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](https://www.hitsz.edu.cn)）

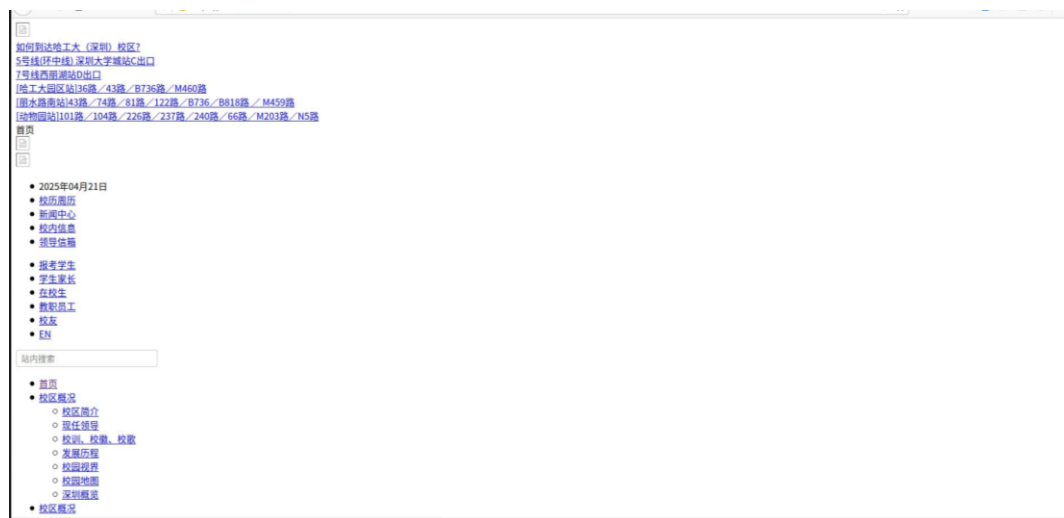
能够拦截访问一个（例如 [www.hitsz.edu.cn](https://www.hitsz.edu.cn)）网站：



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。

## 5. 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