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: 王志铭

学　号: 200110611

专　业: 计算机科学与技术

日　期: 2023 年 4 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。

（1） 证书的哪部分内容表明这是证书的持有方？

证书如下所示。

```
[05/25/23]seed@VM:~/.../PKI$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            05:b6:20:43:28:5d:45:93:62:5b:5f:b6:41:95:4f:c7:b1:96:fc:8e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: May 25 06:18:40 2023 GMT
            Not After : May 22 06:18:40 2033 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:c3:ac:6a:29:6a:64:4b:ca:05:56:b8:b5:b2:5e:
                    6e:0a:bd:8e:8b:1b:8b:c9:28:de:eb:aa:e3:0c:83:
                    11:3e:af:03:fc:22:da:dd:8b:d1:85:a0:8a:04:88:
                    78:80:7f:bf:c5:28:a0:6f:ee:4f:c0:44:0e:8b:27:
                    20:9c:f6:cb:e4:3a:a9:d1:03:99:86:e4:15:d0:96:
                    6a:2b:8f:e1:09:4b:e6:ce:d3:a7:0a:fe:31:22:b2:
                    c6:6a:d0:9b:80:f2:91:4a:a2:0a:7b:83:71:34:bd:
                    c5:20:a6:0a:ce:f7:e7:aa:8a:5b:29:74:05:54:8f:
                    58:cf:e0:f0:e7:cd:37:8b:1f:4e:7f:ee:bd:d4:96:
                    50:80:ad:f8:51:2a:65:bb:13:a7:08:38:2a:c7:a6:
                    ca:f0:9e:ea:8c:e9:fa:81:a1:6d:33:1d:47:5e:cd:
                    cd:19:a4:7f:e4:1c:6c:01:de:09:50:ed:df:1c:ab:
                    7d:c9:c2:1e:b4:d8:2a:c8:34:d0:70:81:0c:a3:db:
                    df:a8:bd:94:b9:c8:b7:af:28:ba:ab:df:30:8f:fe:
                    8b:be:c2:5b:b9:c1:54:c7:46:1b:46:88:76:cf:8d:
                    31:dd:da:a0:07:f9:61:16:00:a0:60:0e:b8:ce:e9:
                    2b:aa:4e:76:1d:6d:b7:af:6e:69:5a:8b:b7:2a:a7:
                    64:5e:ac:fb:22:03:8a:ac:63:a0:5c:23:3f:2f:ae:
                    8f:a9:fc:d6:52:bd:df:ff:30:64:4c:95:f7:5b:1a:
                    ae:22:95:2e:b9:7c:76:79:47:9e:27:1b:7e:15:6a:
                    9e:41:c1:73:ff:ae:65:9b:ca:6f:0a:28:6c:85:20:
                    ac:01:22:48:f5:16:6d:f3:75:9e:f7:c3:97:94:a3:
                    e2:e6:16:52:a4:7d:e0:6a:7f:6c:a1:50:a2:e2:74:
                    f8:7d:f3:f5:89:8b:3c:95:d3:94:02:2a:d8:13:5f:
                    4b:9c:d6:e0:a2:38:ec:de:5b:e3:0b:db:f7:d8:49:
```

证书的持有方在 subject 当中可以看到。

（2）从证书的哪部分内容可以看出这是自签名的证书？

同样从上面的证书当中可以看到，

证书当中的 Issuer 是签发机构，Subject 是持有者。在此证书当中，Issuer 和

Subject 相同，因此是自签名的证书。

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：

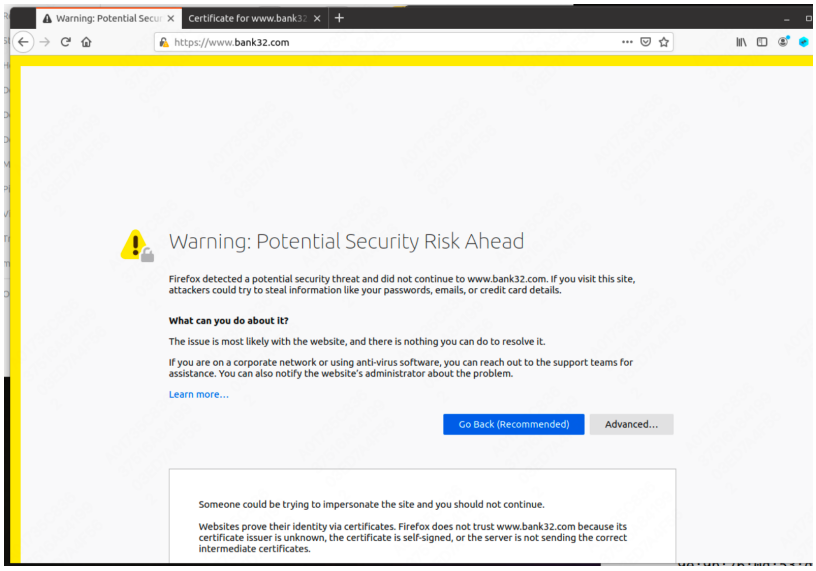
```
[05/25/23]seed@VM:~/.../PKI$ openssl x509 -in server.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4096 (0x1000)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: May 25 06:19:20 2023 GMT
            Not After : May 22 06:19:20 2033 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:c3:31:7e:4c:1c:b8:a6:b7:b7:71:47:0f:c5:41:
                    94:5e:f4:3a:fe:fb:ab:35:1f:74:06:6f:14:01:4a:
                    6d:24:86:aa:6a:3c:18:8e:f4:1e:8d:15:16:ab:ca:
                    be:b6:35:55:05:99:d0:49:2a:39:8b:39:03:9e:26:
                    41:9b:57:96:75:13:b4:ce:7c:41:b8:7b:dc:83:cf:
                    08:57:51:f2:40:00:e4:4c:2c:49:86:43:1a:b8:39:
                    c5:0a:59:d6:2e:6f:19:4d:70:92:77:7a:67:f6:21:
                    3e:5f:eb:63:86:91:9d:8f:bc:58:71:6a:9f:a6:74:
                    75:6e:b6:c4:b2:f0:3c:b9:1c:10:0c:10:1b:65:f1:
                    5e:25:8b:86:1c:4b:9e:d1:77:9f:74:34:de:a4:b2:
                    41:b8:33:1f:66:c2:fe:b2:11:fb:bd:38:f0:e2:c5:
                    9c:34:f7:9a:4d:e2:e2:42:45:fd:1e:33:cf:6e:29:
                    fc:09:eb:1b:a7:dd:86:be:15:d0:14:60:76:33:ef:
                    05:60:cf:f9:1b:f6:43:33:b7:83:6e:4d:59:1f:c8:
                    a3:27:d6:61:46:86:40:30:42:6d:3d:d5:65:f5:8e:
                    6b:3c:d5:0e:76:8e:9e:18:14:48:ad:3a:42:0c:78:
                    2b:7a:eb:7e:8d:29:43:58:97:5e:ec:66:a9:44:7e:
                    cd:9f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                09:E7:0B:13:52:D5:38:55:E5:4C:FC:78:76:77:94:D4:3F:22:BB:63
            X509v3 Authority Key Identifier:
                keyid:F9:E0:66:CF:B5:D8:8A:6E:2D:14:3E:10:E8:6B:B6:65:A7:04:DA:05

            X509v3 Subject Alternative Name:
                DNS:www.bank32.com, DNS:www.bank32A.com, DNS:www.bank32B.com
    Signature Algorithm: sha256WithRSAEncryption
```

不同：

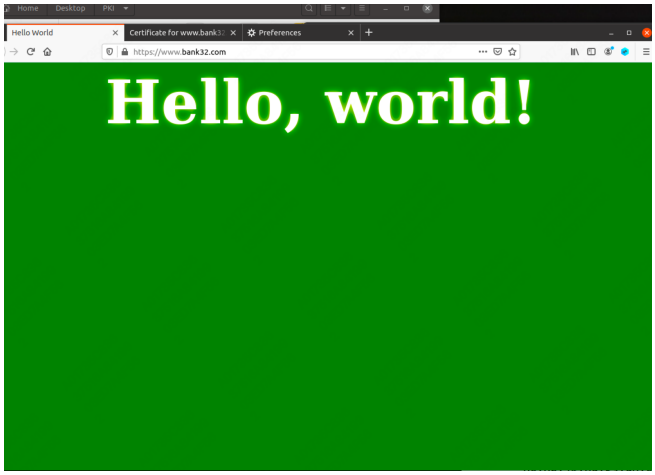
1. 证书的持有者，即 subject 不同。
2. 证书当中的公钥，即 rsa public-key 不同。

3. 请将能够正确访问 www.bank32.com 的截图贴在下面。

未添加证书前：

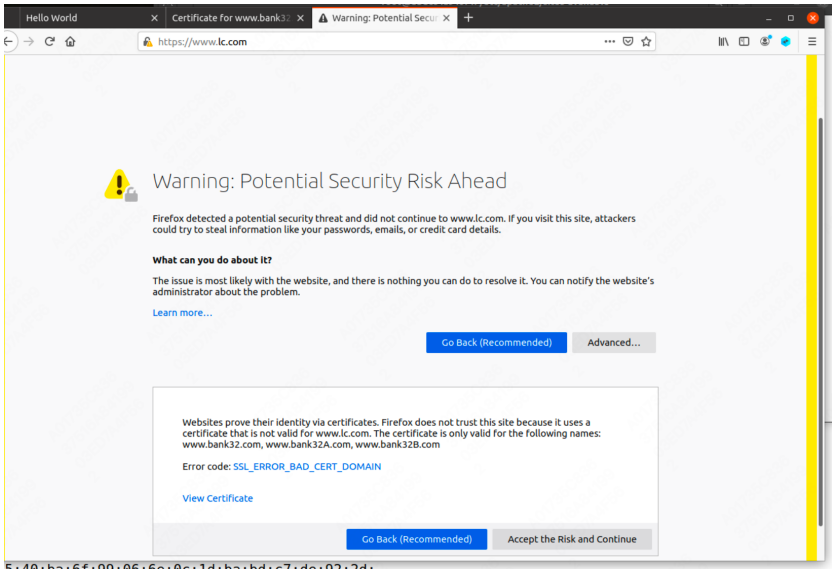


添加证书后，可以正常访问：



4. 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）

网站选取 www.lc.com
未劫持时尝试访问：

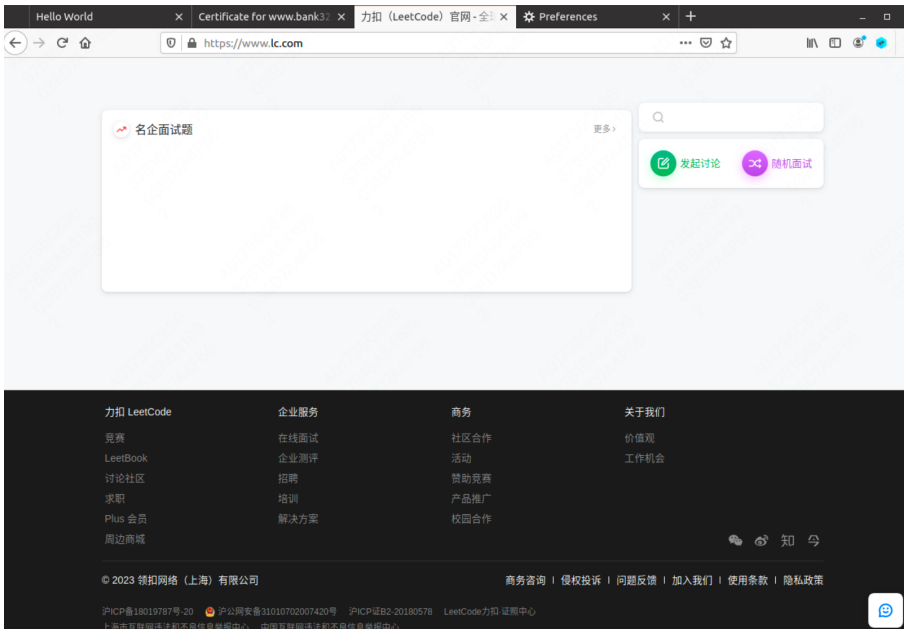


使用 task2 和 task3 来生成 lc 的证书和私钥进行攻击，主要的命令如下：

```
openssl req -newkey rsa:2048 -sha256 -keyout server.key -out server.csr -
subj "/CN=www.lc.com/O=lc Inc./C=US" -addext "subjectAltName =
DNS:www.lc.com, DNS:www.lcA.com, DNS:www.lcB.com" -passout pass:dees

openssl ca -config myCA_openssl.cnf -policy policy_anything  -md sha256 -days
3650 -in server.csr -out server.crt -batch -cert ca.crt -keyfile ca.key
```

然后修改 lc-ssl.conf 为如下内容：

随后访问 https://www.lc.com
可以看到劫持成功了。



5. 分析 CA 证书各密码算法的作用。

1. 摘要加密算法（如 SHA）
   用于数字证书的签发和验证，在签发时，CA 先生成数字摘要，然后用密钥对数字摘要加密，得到摘要密文。在验证时，使用者也生成数字摘要 1，然后用 CA 的公钥解密摘要密文，得到摘要 2，对比摘要 1 和摘要 2，验证证书是否有效。
2. 非对称加密算法（如 RSA）
   非对称加密算法相比对称加密，具有非常高的安全性，因此非对称加密算法通常用于加密对称加密算法的密钥等等。非对称加密有公钥和私钥，用公钥加密，私钥解密。