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: 房煊梓

学　号: 210010101

专　业: 智能强基-计算机

日　期: 2024 年 5 月 12 日

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?

根据实验指导书对证书的说明可知，Subject 部分的内容为证书拥有者的信息，如下图。

```
[05/08/24]seed@VM:~/PKI$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            77:95:77:cf:e0:19:bc:65:01:fe:71:09:df:89:5a:a7:d8:51:99:be
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: May  8 11:20:35 2024 GMT
            Not After : May  6 11:20:35 2034 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:
```

（2）从证书的哪部分内容可以看出这是自签名的证书?

从证书的签发机构 Issuer 和证书的拥有者 Subject 信息来看，两者的内容相同，所以可看出这是自签名的证书，如下图。

```
[05/08/24]seed@VM:~/PKI$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            77:95:77:cf:e0:19:bc:65:01:fe:71:09:df:89:5a:a7:d8:51:99:be
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: May  8 11:20:35 2024 GMT
            Not After : May  6 11:20:35 2034 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:
```

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：

ca.crt 和 www.bank32.com 的服务器证书如下两张图。

```
[05/08/24]seed@VM:~/PKI$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            77:95:77:cf:e0:19:bc:65:01:fe:71:09:df:89:5a:a7:d8:51:99:be
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = www.modelCA.com, O = Model CA LTD., C = US
        Validity
            Not Before: May  8 11:20:35 2024 GMT
            Not After : May  6 11:20:35 2034 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:
```

```
[05/08/24]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  8 11:32:11 2024 GMT
            Not After : May  6 11:32:11 2034 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:
```

www.bank32.com 的服务器证书与 ca.crt 的证书的不同之处有：

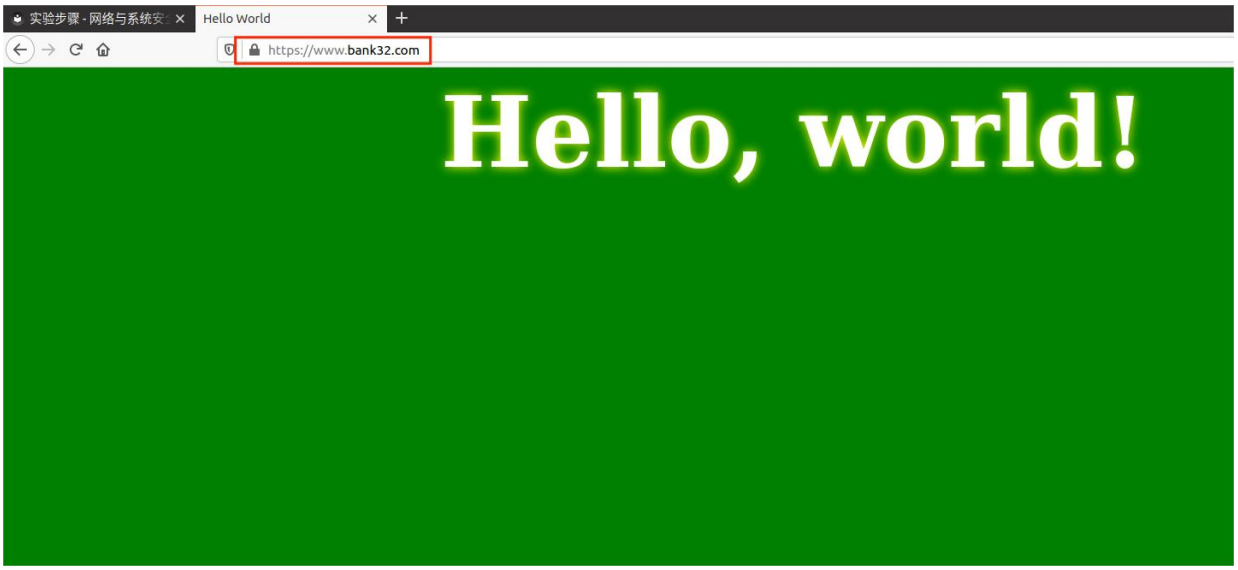
①Serial Number 即序列号不同

②Subject 即证书的拥有者不同

③RSA Public-Key 的位数不同

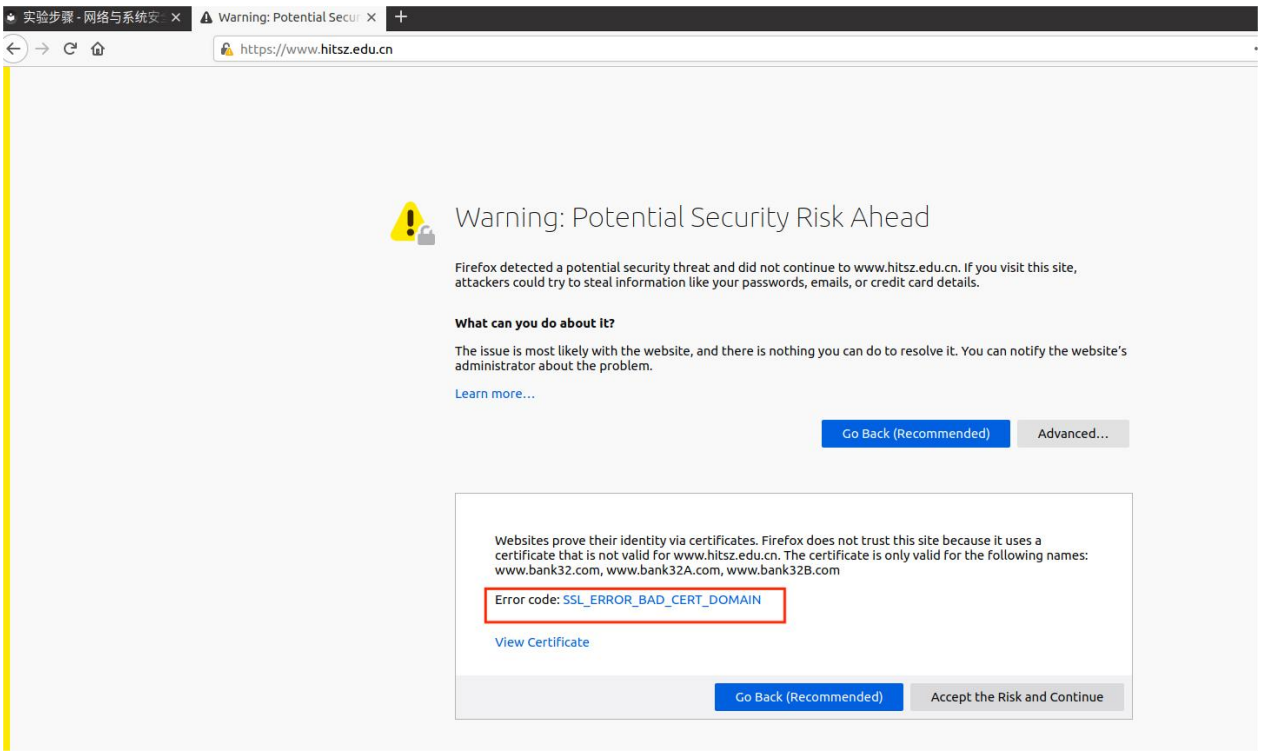
3. 请将能够正确访问 www.bank32.com 的截图贴在下面。

如下图。



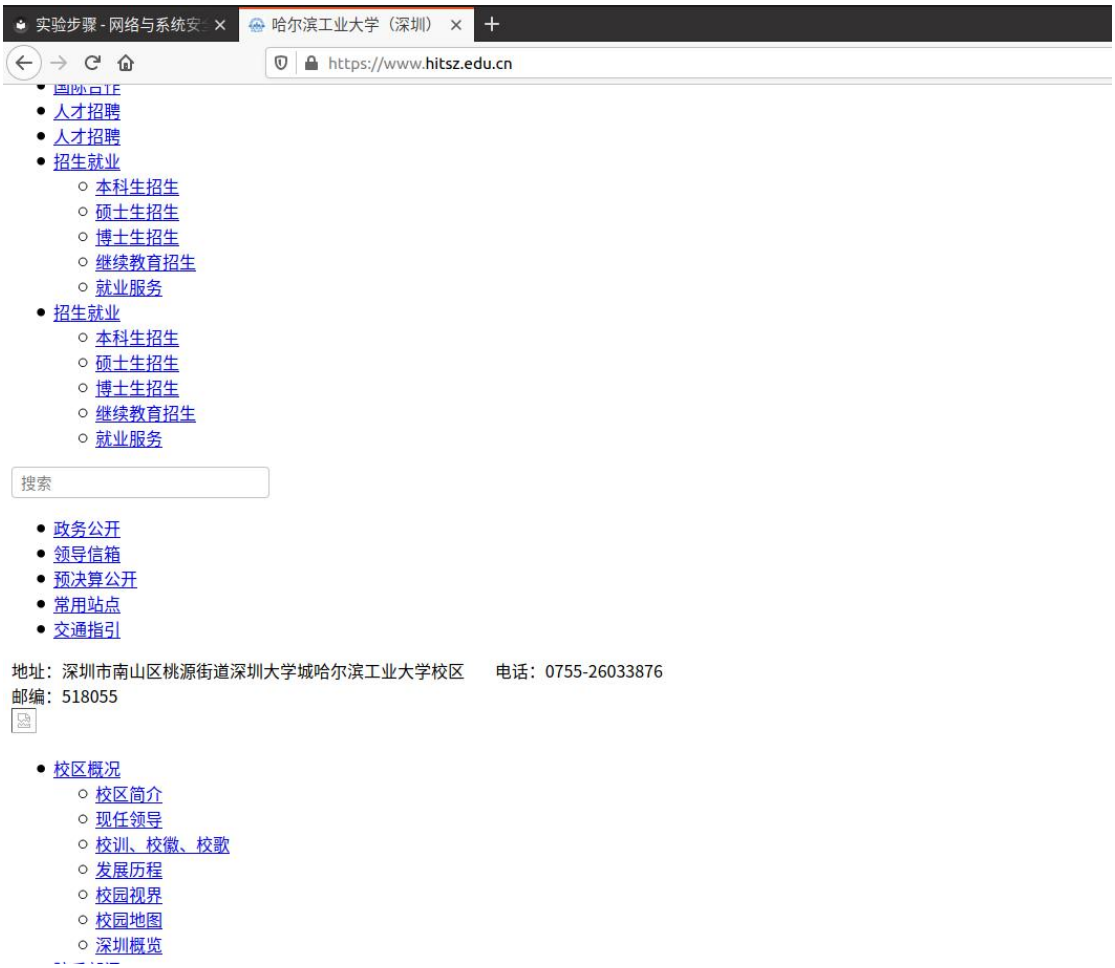
4. 将能够拦截访问一个（例如 www.hitsz.edu.cn）网站的截图和 CA 被劫持后能够正常访问的截图贴在下面。并分析说明。（建议大家随机选取一个网站，不使用 www.hitsz.edu.cn）

能够拦截访问 www.hitsz.edu.cn 的截图如下：



分析：由于请求的域名是 www.hitsz.edu.cn，但是服务器的证书信息使用的是 www.bank32.com 服务器的，两者不匹配，所以拦截了访问。

CA 被劫持后能够正常访问 www.hitsz.edu.cn 的截图如下：



分析：根据 task2 和 task3 为 hitsz 生成证书和私钥进行攻击，由于请求的域名和服务器的证书信息可以匹配，所以能够正常访问虚假构建的 hitsz 网站。

5. 分析 CA 证书各密码算法的作用。

CA 证书的各个密码算法及其作用如下：

SHA256 算法：用于生成证书内容的摘要和保证数字签名的完整性。接收方的客户端检查自己端的哈希算法，并使用公钥对消息进行解密。如果匹配，则数据是真实有效、未被篡改的。

RSA 算法：用于生成公钥和私钥，并且与 SHA256 结合用于签名算法，使得发送方可以对消息进行签名，接收方可以使用公钥验证消息的真实性和完整性。