03_Cert实验报告

《信息安全综合实践》实验报告

数字证书

一、实验目的

1. 了解密码技术的应用
2. 学习OpenSSL 的相关命令及应用, 了解数字证书的管理
3. 了解数字证书的应用

二、实验内容

序	内容	实验结果
1)	OpenSSL加解密	- [ ] 失败 - [√] 成功
2)	OpenSSL证书管理	- [ ] 失败 - [√] 成功

三、相关命令（24分）

1. 文件摘要命令
    - `openssl sha256 test`
2. 文件加解密命令
    - 对称加密解密
        - 利用AES算法对称加密：`openssl enc -aes-256-cbc -salt -in test -out test_encrypted`
        - 解密：`openssl enc -aes-256-cbc -d -in test_encrypted -out test_decrypted`
    - 非对称加密解密
        - 生成私钥：`openssl genrsa -out private_key.pem 2048`
        - 生成公钥：`openssl rsa -in private_key.pem -out public_key.pem -pubout writing RSA key`
        - 将文件编码为base64文件：`openssl enc -base64 -in test -out test.b64`
        - 加密文件：`openssl rsautl -encrypt -inkey public_key.pem -pubin -in test.b64 -out test.enc`
        - 解密文件：`openssl rsautl -decrypt -inkey private_key.pem -in test.enc -out test.b64.decoded`
3. 证书管理命令
    - 签发CA根证书
        - 修改openssl.cnf文件

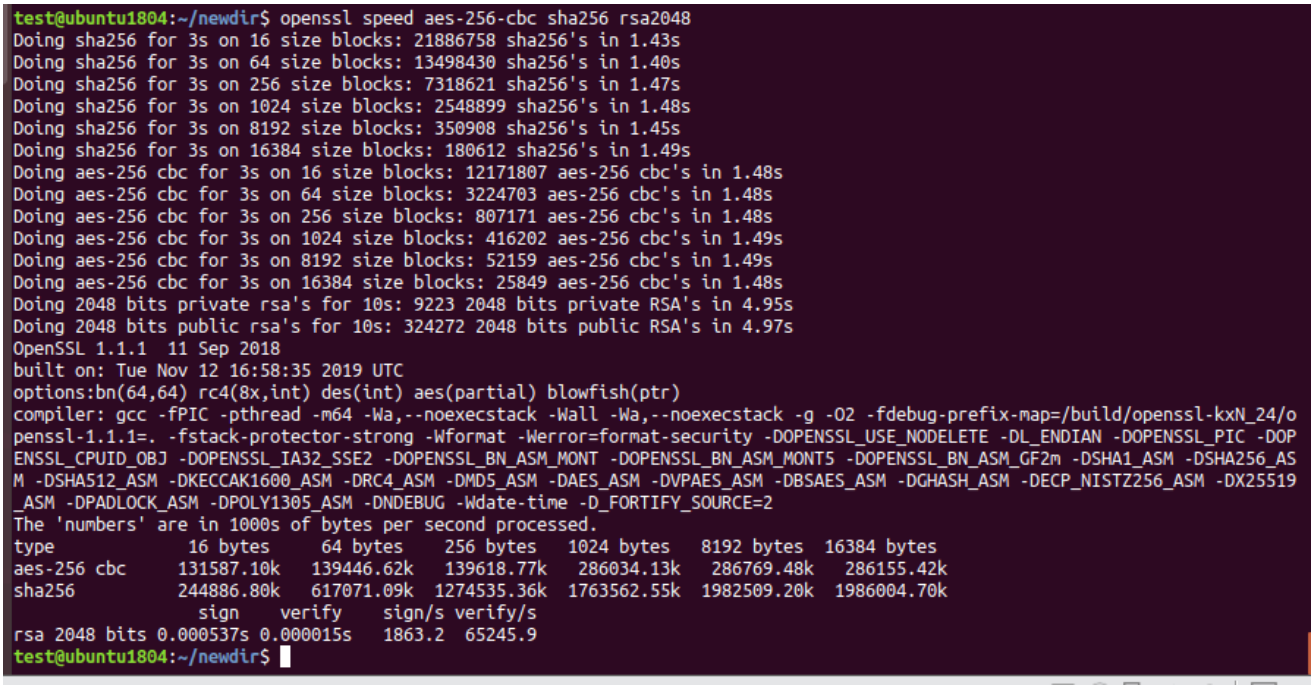
        - 生成CA根证书以及密钥：`openssl req -new -x509 -newkey rsa:4096 -keyout cakey.key -out cacert.crt -config openssl.cnf -days 365`
    - 签发客户证书
        - 以私钥长度1024位，证书有效期2年为例：
            - 生成客户端私钥：`openssl genrsa -out client.key 1024`
            - 用该客户端私钥生成证书签名请求，扩展名.csr：`openssl req -new -key client.key -out client.csr -config openssl.cnf`
            - 使用 CA 根证书签发客户端证书：`openssl ca -in client.csr -out client.crt -cert cacert.crt -keyfile ./private/cakey.key -config openssl.cnf -days 730`
            - 把客户端证书和私钥保存为.pem 格式:
                - 客户端证书：`openssl x509 -in cacert.crt -out cacert.pem -outform PEM`
                - 私钥：`openssl ca -config ./openssl.cnf -revoke ./certs/02.pem`
    - 撤销客户证书
        - `cd ./certs`
        - `openssl ca -config openssl.cnf -revoke test.pem`
    - 查看证书撤销列表
    - `echo 01 > crlnumber`
    - `echo authorityKeyIdentifier = keyid:always,issuer:always > crl_ext.cnf`
    - `openssl ca -gencrl -config openssl.cnf -out crl.pem`
    - `openssl crl -in crl.pem -text`

四、分析和思考（66分）

1. 在OpenSSL的文件对称加密、非对称加密以及文件摘要中你分别采用的是何种算法，密钥长度各是多少？请利用openssl speed命令或其它命令测试这三种算法的速度（可设计测试方案），对结果进行分析，并总结不同算法的特点及各自用途。（16分）

- 对称加密算法：aes-256-cbc，密钥长度为256位
- 非对称加密算法：RSA算法，密钥长度为2048位
- 计算文件摘要：sha256算法，生成256位

测试方案：命令行执行命令`openssl speed aes-256-cbc sha256 rsa2048`，查看输出结果
测试结果：

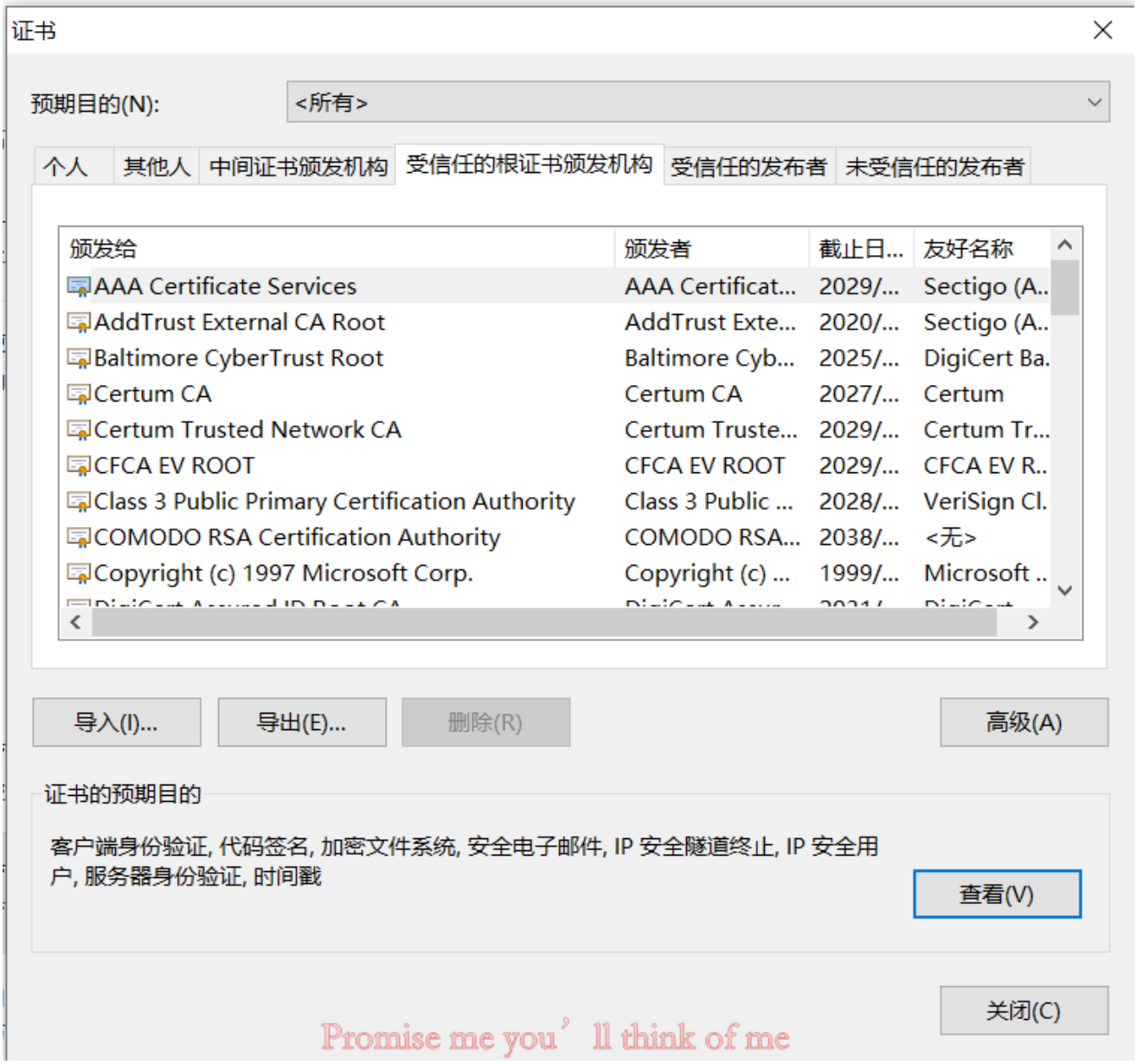


总结可得：

- AES-256-CBC:
  - 特点：高效
  - 用途：该算法适用于需要加密大量数据的场景，如文件和数据库加密，网络传输数据加密等。
- SHA-256：
  - 特点：快速、不可逆
  - 用途：可以被广泛用于数字签名、消息认证、密码存储和验证等场景。SHA-256可用于保护数据完整性，防止数据被篡改。
- RSA2048：
  - 特点：具有高度的安全性，但加密和解密过程比对称加密算法慢
  - 用途：RSA2048通常用于数字签名、密钥交换、加密通信和证书签名等场景

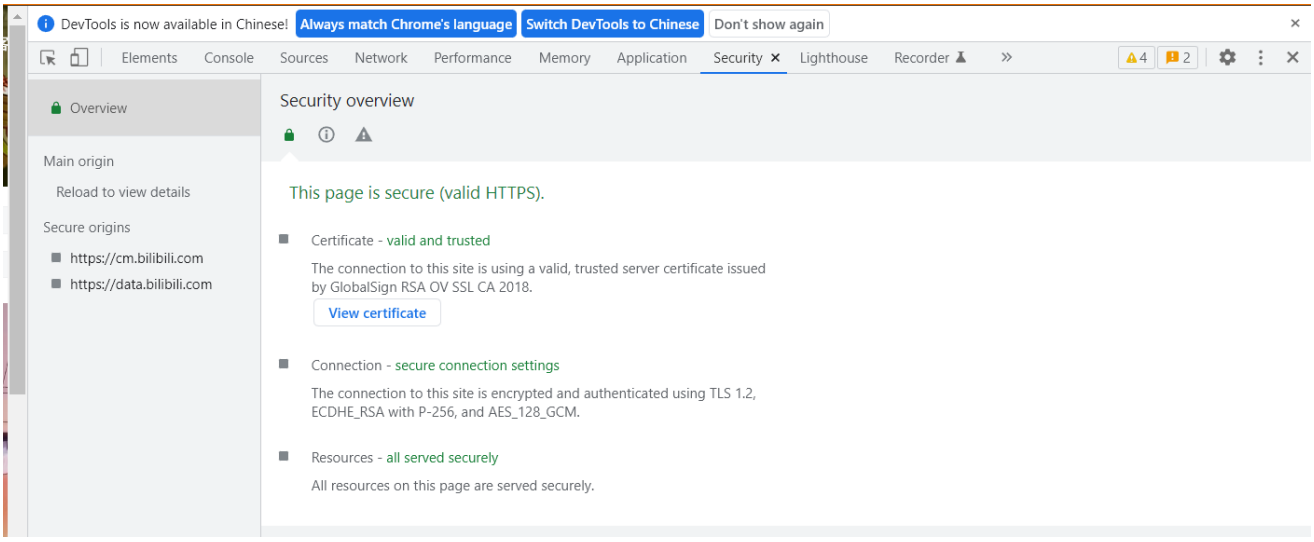
2. 查看浏览器内置证书及某常用网页的SSL证书，各选一个说明证书的下列信息，给出相应截图（各给至少2个截图）。（10分）

谷歌浏览器的内置证书：




证书
常规
详细信息
证书路径
证书信息
这个证书的目的如下:
• 向远程计算机证明你的身份
• 确保软件来自软件发布者
• 保护软件在发行后不被更改
• 允许加密磁盘上的数据
颁发给: AAA Certificate Services
颁发者: AAA Certificate Services
有效期从 2004/1/1 到 2029/1/1
颁发者说明(S)
确定

bilibili的ssl证书：



证书查看者：*.bilibili.com

基本信息(G) 详细信息(D)

颁发对象

公用名 (CN)	*.bilibili.com
组织 (O)	上海幻电信息科技有限公司
组织单位 (OU)	<未包含在证书中>

颁发者

公用名 (CN)	GlobalSign RSA OV SSL CA 2018
组织 (O)	GlobalSign nv-sa
组织单位 (OU)	<未包含在证书中>

有效期

颁发日期	2022年9月29日星期四 17:56:02
截止日期	2023年10月31日星期二 17:56:01

指纹

SHA-256 指纹	00 B3 57 0F AA 95 C7 03 EB 78 30 D9 FC D8 2B 89 D8 CE 06 A8 30 4E 7A 8D 3F 18 60 A5 90 74 F4 DC
SHA-1 指纹	EB 78 A8 16 32 76 12 D8 51 A9 B8 02 DF D6 E7 32 1D B9 E8 FF

字段	浏览器内置证书	常用网页SSL证书
证书所有方	AAA Certificate Services	*.bilibili.com
证书发行方	CN=AAA Certificate Services	CN=GlobalSign RSA OV SSL CA 2018

字段	浏览器内置证书	常用网页SSL证书
证书用途	向远程计算机证明你的身份/确保软件来自软件发布者 保护软件在发行后不被更改/允许加密磁盘上的数据	非关键 OID.1.3.6.1.4.1.4146.1.20： 核证作业准则 (Certification Practice Statement) 指针：https://www.globalsign.com/repository/ OID.2.23.140.1.2.2
证书有效期	2004/1/1~2029/1/1	2022/9/29 GMT+8 17:56:02~ 2023/10/31 GMT+8 17:56:01
签名算法	sha1RSA	PKCS #1，带有 RSA 加密的 SHA-256
密钥用途	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	关键，签名，加密
增强型密钥用途（如有）	客户端身份验证/代码签名/加密文件系统/安全电子邮件/IP安全隧道终止/IP安全用户/服务器身份验证/时间戳	非关键，TLS WWW 服务器身份验证 (OID.1.3.6.1.5.5.7.3.1)，TLS WWW 客户端身份验证 (OID.1.3.6.1.5.5.7.3.2)

3. 请分别贴图展示证书签发的结果和证书内容（不超过4张图片），并分析在证书管理中可能存在的2-3个安全威胁，并给出防范建议。（20分）

CA根证书签发：

```
test@ubuntu1804:~/newCA$ openssl x509 -noout -text -in cacert.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            46:e3:b8:cf:46:f1:ab:62:40:d7:e6:ec:22:a3:c6:6c:49:d2:b5:e4
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = CN, ST = Shanghai, L = Shanghai, O = SJTU, OU = SJTU, CN = Liujunjie, emailAddress = sjtu.1518228705@sjtu.edu.cn
        Validity
            Not Before: Mar 22 13:55:28 2023 GMT
            Not After : Mar 21 13:55:28 2024 GMT
        Subject: C = CN, ST = Shanghai, L = Shanghai, O = SJTU, OU = SJTU, CN = Liujunjie, emailAddress = sjtu.1518228705@sjtu.edu.cn
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:c1:ac:69:8a:45:46:1a:5e:f8:21:cd:c3:5e:c7:
                    cf:07:29:82:86:5b:7e:e2:43:fb:74:7d:fa:fb:75:
                    9a:32:87:9a:97:12:6b:93:fb:07:18:d3:ed:5a:da:
                    4b:cc:2c:86:58:e6:ee:54:35:c6:2f:d8:83:a2:af:
                    2e:63:89:8d:d2:0e:1b:55:87:cf:ee:4c:4f:26:1c:
                    38:bf:51:00:dd:fc:3c:50:09:2d:c4:66:52:81:ec:
                    92:2c:49:70:6d:b9:0f:76:89:43:c8:dc:dd:b5:90:
                    b4:13:68:4e:4e:cf:8d:4c:0c:86:8f:88:9b:f4:e9:
                    03:8d:c3:37:86:32:86:e1:c8:6a:72:49:f9:82:8d:
                    19:64:46:07:75:2a:c1:b1:15:8a:b1:a0:83:21:35:
                    06:1b:01:40:82:a1:06:0b:73:c0:46:4d:3a:22:fc:
                    e6:ab:17:a6:7c:a8:c2:2b:3c:6d:74:90:4b:5a:10:
                    37:83:77:c0:3d:22:d9:a5:d3:6a:ec:0e:50:95:0b:
                    8f:ac:aa:6a:23:cc:1a:cd:56:de:f4:2d:a0:50:c1:
                    bc:02:f8:e9:ed:5c:95:49:a5:a3:5c:bc:2b:ff:c8:
                    e4:e5:ed:59:ee:0f:61:b7:04:0d:b6:03:a6:06:d9:
                    88:7b:16:3b:50:ec:49:89:c7:9d:16:c8:b0:43:e7:
                    9a:c7:25:ed:e3:87:65:c1:78:19:b6:aa:1a:45:d3:
                    54:f4:82:9f:16:5f:14:9a:5f:de:dc:f0:0b:fa:13:
                    54:c7:ec:99:cc:20:c5:65:a8:c5:7b:b1:25:51:20:
                    31:4c:8d:18:a5:02:18:08:b5:24:99:7a:05:77:d1:
                    8c:a8:9f:a7:02:41:7b:ed:b2:bf:c8:35:ac:40:f2:
                    32:34:ba:8b:08:00:3a:1c:10:39:54:de:41:9f:6e:
                    6c:e4:ac:f6:e8:75:73:26:42:1e:00:c6:16:7f:e1:
                    d7:3f:d7:60:a4:2d:f4:b8:09:99:b1:98:21:55:1d:
                    ed:b1:71:44:52:7b:de:cf:8b:4c:08:71:c4:bf:ab:
                    15:47:c4:78:48:02:08:b3:e3:e6:0f:6e:c0:8a:0c:
                    7a:fd:d6:fb:95:1f:1c:94:23:a1:67:2a:11:f6:d5:
                    78:3e:a7:02:5c:97:66:24:76:3f:7e:98:8b:b0:0c:
                    6d:18:da:8f:2e:e3:cd:bd:cc:f3:50:50:a9:37:f1:
                    f6:3c:80:1d:48:d5:02:97:46:a6:43:dd:19:ad:91:
                    56:88:67:b5:ee:6f:37:b6:25:20:2e:c6:4b:11:d6:
                    72:70:b2:8e:bd:2f:d7:3f:0e:85:93:4c:ff:09:84:
                    70:19:d4:87:72:84:07:67:83:6f:dd:07:af:79:19:
                    aa:eb:9d
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                43:DA:DB:0F:FB:11:A8:34:54:7F:0A:77:92:55:AD:72:DD:E4:FD:0A
            X509v3 Authority Key Identifier:
                keyid:43:DA:DB:0F:FB:11:A8:34:54:7F:0A:77:92:55:AD:72:DD:E4:FD:0A

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         7c:80:d4:cd:54:25:f7:3f:20:8f:37:d9:e0:97:2e:bc:55:a0:
         d0:4a:bb:4f:47:5a:b1:e9:b3:87:dc:f3:34:58:ae:e8:c0:89:
         c2:d6:48:38:5d:c5:3b:bf:17:ec:3e:25:2c:43:cd:1a:f3:c5:
         5d:20:8d:89:2b:d5:26:98:68:d6:c9:ea:c2:57:28:a4:99:50:
         9b:96:46:15:22:0c:f0:bb:5e:f4:89:15:7f:3b:3a:6a:93:a9:
         b7:d3:8c:e3:f7:c8:c1:0c:9e:ca:3d:2b:c3:43:a0:42:44:64:
         04:f5:d9:57:ad:ce:77:c7:9c:9e:73:f5:f4:7f:47:0a:ed:3e:
         f6:36:df:1c:34:d4:e7:a6:e5:93:06:b7:74:16:77:81:e3:98:
         82:e6:0c:85:d9:dc:a3:a8:39:a4:66:57:a3:21:2e:36:bf:21:
         a4:19:db:38:88:62:2b:f6:6f:35:49:f7:7c:ad:a8:cb:a1:dd:
         28:4e:81:87:55:98:d3:6e:16:9f:6d:9b:17:8b:27:eb:70:a6:
         b0:66:72:dc:72:d1:d1:9d:c1:50:2f:74:eb:ad:e8:03:1b:e9:
         18:0a:7e:b0:65:88:9a:f9:1d:83:73:58:f3:15:1c:c6:db:44:
         55:5d:41:76:53:da:01:0a:68:a3:53:c7:4c:22:60:09:51:f7:
         02:da:43:ec:5a:99:46:00:2b:94:ba:c9:07:3e:6f:78:0e:10:
         54:5b:f9:86:61:fc:8b:dc:68:9f:64:20:77:3a:b6:b3:a3:42:
         1c:fd:9d:67:98:d1:e8:b9:f9:73:a2:4e:95:50:a8:ab:27:dc:
         81:59:57:37:ac:76:98:9b:30:be:3c:bc:3b:2b:16:0e:7e:0b:
         de:0f:b9:ad:a8:4a:0b:e2:9a:c9:b6:66:2c:71:47:5e:28:45:
         94:20:86:b7:6a:2b:4f:ef:ae:87:8f:19:34:d7:a8:12:0c:d2:
         9f:58:24:6e:10:f2:a6:38:01:58:b5:fd:42:de:4e:ab:e6:af:
         47:cb:bf:8e:e3:c9:90:27:4b:9a:d7:8b:97:9a:75:82:03:98:
         02:23:93:d3:da:ad:62:8d:ec:d8:e8:fc:81:f9:3e:05:2a:30:
         ae:a9:0a:fa:8e:fb:0b:1f:fa:a3:54:68:23:b1:63:cb:88:17:
         40:9f:de:38:26:56:ae:21:93:4c:a0:b3:28:c6:17:c1:e6:5d:
         3a:0e:ab:5a:9a:4b:95:26:91:40:8c:b5:32:e3:63:32:f8:a8:
         9b:7b:a5:8a:34:82:58:28:8d:13:85:93:0f:cf:0d:00:8a:16:
         77:f0:c6:d1:ba:ef:59:18:c1:c8:20:a3:5e:af:04:2b:88:6f:
         59:76:34:6c:22:93:f8:9c
```

私钥长度和有效期分别为1024、2年的客户端证书1：

```
test@ubuntu1804:~/newCA$ openssl ca -in client.csr -out client.crt -cert cacert.crt -keyfile ./private/cakey.key -config openssl.cnf -days 730
Using configuration from openssl.cnf
Enter pass phrase for ./private/cakey.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Mar 22 14:42:49 2023 GMT
            Not After : Mar 21 14:42:49 2025 GMT
        Subject:
            countryName               = CN
            stateOrProvinceName       = Shanghai
            organizationName          = SJTU
            organizationalUnitName    = SJTU
            commonName                = Liujunjie
            emailAddress              = sjtu.1518228705@sjtu.edu.cn
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                4C:4F:31:A5:51:5A:EA:83:C7:9E:7D:92:5C:6D:D3:63:38:22:D5:1D
            X509v3 Authority Key Identifier:
                keyid:43:DA:DB:0F:FB:11:A8:34:54:7F:0A:77:92:55:AD:72:DD:E4:FD:0A

Certificate is to be certified until Mar 21 14:42:49 2025 GMT (730 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
test@ubuntu1804:~/newCA$
```

私钥长度和有效期分别为1024、3年的客户端证书2：

```
test@ubuntu1804:~/newCA$ openssl ca -in client2.csr -out client2.crt -cert cacert.crt -keyfile ./private/cakey.key -config openssl.cnf -days 1095
Using configuration from openssl.cnf
Enter pass phrase for ./private/cakey.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 2 (0x2)
        Validity
            Not Before: Mar 22 14:54:02 2023 GMT
            Not After : Mar 21 14:54:02 2026 GMT
        Subject:
            countryName               = CN
            stateOrProvinceName       = Shanghai
            organizationName          = SJTU
            organizationalUnitName    = SJTU
            commonName                = Liujunjie_2
            emailAddress              = sjtu.1518228705@sjtu.edu.cn
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                FD:4E:9A:B8:AB:18:11:05:59:82:E4:10:73:F0:E0:F8:CA:A4:79:58
            X509v3 Authority Key Identifier:
                keyid:43:DA:DB:0F:FB:11:A8:34:54:7F:0A:77:92:55:AD:72:DD:E4:FD:0A

Certificate is to be certified until Mar 21 14:54:02 2026 GMT (1095 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
test@ubuntu1804:~/newCA$ cat serial
03
```

私钥长度和有效期分别为2048、3年的客户端证书3：

```
test@ubuntu1804:~/newCA$ openssl ca -in client3.csr -out client3.crt -cert cacert.crt -keyfile ./private/cakey.key -config openssl.cnf -days 1095
Using configuration from openssl.cnf
Enter pass phrase for ./private/cakey.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 3 (0x3)
        Validity
            Not Before: Mar 22 14:59:33 2023 GMT
            Not After : Mar 21 14:59:33 2026 GMT
        Subject:
            countryName               = CN
            stateOrProvinceName       = Shanghai
            organizationName          = SJTU
            organizationalUnitName    = SJTU
            commonName                = Liujunjie_3
            emailAddress              = sjtu.1518228705@sjtu.edu.cn
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                5C:CA:93:78:D9:FD:72:11:D7:15:7D:83:8C:C0:64:1B:7C:4C:00:9F
            X509v3 Authority Key Identifier:
                keyid:43:DA:DB:0F:FB:11:A8:34:54:7F:0A:77:92:55:AD:72:DD:E4:FD:0A

Certificate is to be certified until Mar 21 14:59:33 2026 GMT (1095 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

- 可能存在的安全威胁：
  - 证书过期：数字证书设置有时限，在过期之后将会失效，如果证书管理人员没有及时更新过期的证书，可能会导致用户无法访问合法的网站或应用程序，也会给攻击者提供机会。
  - 证书泄露：如果证书的私钥被泄露，攻击者就能够使用该证书对数据进行篡改或者窃取。泄露的证书还可能被攻击者用于进行中间人攻击，使其能够窃取用户的敏感信息。
- 防范建议：
  - 实现证书链：在证书管理过程中，建议使用数字证书链来保证证书的真实性和完整性。数字证书链可以将信任链从根证书一直延伸到最终的数字证书，从而确保数字证书的真实性和完整性。
  - 定期更新证书：为了避免证书过期导致的安全问题，证书管理人员应该建立定期更新证书的机制。

4. 请分别贴图展示CRL列表签发的结果和CRL列表内容（2张图片）。试分析在证书撤销列表CRL机制中可能存在的2-3个安全威胁，并给出防范建议。（20分）

```
test@ubuntu1804:~/newCA$ echo 00 > crlnumber
test@ubuntu1804:~/newCA$ touch crl_ext.cnf
test@ubuntu1804:~/newCA$ echo authorityKeyIdentifier = keyid:always,issuer:always > crl_ext.cnf
test@ubuntu1804:~/newCA$ openssl ca -gencrl -config openssl.cnf -out crl.pem
Using configuration from openssl.cnf
```

```
test@ubuntu1804:~/newCA$ openssl crl -in crl.pem -text
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = CN, ST = Shanghai, L = Shanghai, O = SJTU, OU = SJTU, CN = Liujunjie, emailAddress = sjtu.1518228705@sjtu.edu.cn
        Last Update: Mar 22 15:31:18 2023 GMT
        Next Update: Apr 21 15:31:18 2023 GMT
        CRL extensions:
            X509v3 CRL Number:
                0
Revoked Certificates:
    Serial Number: 02
        Revocation Date: Mar 22 15:24:00 2023 GMT
    Serial Number: 03
        Revocation Date: Mar 22 15:25:11 2023 GMT
    Signature Algorithm: sha256WithRSAEncryption
         41:20:04:98:09:fa:b1:72:fd:fe:9d:9d:dc:da:e2:3d:8d:1a:
         40:e1:dd:9d:40:ea:5c:e9:4c:d6:24:6a:60:30:45:69:22:f0:
         4d:52:5e:bb:ad:b9:17:2b:5f:d2:6b:d1:ae:05:a9:f6:27:16:
         58:c2:e3:aa:e8:c0:37:7f:5e:c6:91:28:1d:4d:59:fe:7a:d1:
         fb:76:2a:90:8c:43:1f:36:08:13:b9:e3:50:db:48:9f:f4:b8:
         3b:c8:41:89:7d:93:00:3f:53:96:ba:53:c7:d9:28:10:2e:94:
         26:7f:0c:63:30:54:43:9c:5e:e9:eb:b0:4e:0e:01:7c:f2:71:
         5a:8b:97:1b:5c:8e:a2:cb:27:fc:29:3a:95:99:dc:ad:6e:af:
         f0:39:40:4a:90:56:bb:fe:c6:06:ca:63:95:67:e7:ad:44:a3:
         61:f7:bb:17:e0:25:f0:9b:97:28:70:c2:59:9c:ee:a3:3c:d4:
         50:12:c1:84:73:e3:77:ca:c0:11:e3:03:d9:c6:58:0c:b7:63:
         c0:5d:f2:25:75:7b:13:a0:c0:d1:a5:e6:21:7d:d1:7e:f0:01:
         ac:e9:9b:35:73:4f:57:c8:4f:e9:d8:dd:6f:43:2e:8d:58:d6:
         48:4f:b9:9c:00:b7:23:de:39:46:c9:14:a0:26:4c:d4:46:c8:
         98:e6:24:e4:d1:88:c7:0b:86:2f:8c:34:55:fb:38:4a:c9:9c:
         2b:4c:a3:ee:9b:9a:56:fa:91:5b:c0:05:9c:d4:61:fc:19:73:
         d6:82:1b:76:17:30:75:f4:4d:ff:ac:a4:92:c5:f1:15:40:b9:
         9e:a5:79:51:87:a1:ed:df:93:94:20:c4:29:e1:18:0e:85:37:
         73:c2:94:d1:23:2e:09:77:62:79:bf:4d:0e:1d:28:93:02:97:
         60:d6:9b:da:41:a2:67:1a:dd:11:6f:c6:67:2a:2b:29:82:43:
         69:4e:1d:6a:3a:be:20:8d:85:32:6d:a8:d1:3a:06:a8:d5:7a:
         14:4f:77:c9:3b:84:87:8a:f8:23:5a:a2:35:16:9f:ec:b3:3a:
         7d:09:b7:3f:61:fe:be:23:35:a7:15:1d:ea:ce:77:55:70:c6:
         01:e2:26:57:98:17:52:63:1c:22:d0:3a:53:2d:81:23:a5:d4:
         8b:ba:d8:c8:92:d2:1d:5c:0e:5e:48:03:27:25:57:69:3f:74:
         9e:92:71:d0:1b:1b:ea:d7:22:db:5d:5e:9b:2e:59:45:e9:e5:
         df:c7:fe:d7:00:24:65:45:b6:bb:06:7b:9e:15:d5:c3:65:74:
         b4:08:d6:3e:ea:b7:75:d5:ee:3c:e7:7d:cf:a6:bc:55:ff:d2:
         11:d8:84:71:e7:b0:2d:39
-----BEGIN X509 CRL-----
MIIDFTCB/gIBATANBgkqhkiG9w0BAQsFADCBkTELMAkGA1UEBhMCQ04xETAPBgNV
BAgMCFNoYW5naGFpMREwDwYDVQQHDAhTaGFuZ2hhaTENMAsGA1UECgwEU0pUVTEN
MAsGA1UECwwEU0pUVTESMBAGA1UEAwwJTGl1anVuamllMSowKAYJKoZIhvcNAQkB
FhtzanR1LjE1MTgyMjg3MDVAc2p0dSSlZHUuY24XDTIzMDMyMjE1MzExOFoXDTIz
MDQyMTE1MzExOFowKDASAgECFw0yMzAzMjIxNTI0MDBaMBICAQMXDTIzMDMyMjE1
MjUxMVqgDjAMMAoGA1UdFAQDAgEAMA0GCSqGSIb3DQEBCwUAA4ICAQBBIASYCfqx
cv3+nZ3c2uI9jRpA4d2dQOpc6UzWJGpgMEVpIvBNUl67rbkXK1/Sa9GuBan2JxZY
wuOq6MA3f17GkSgdTVn+etH7diqQjEMfNggTueNQ20if9Lg7yEGJfZMAP1OWulPH
2SgQLpQmfwxjMFRDnF7p67BODgF88nFai5cbXI6iyyf8KTqVmdytbq/wOUBKkFa7
/sYGymOVZ+etRKNh97sX4CXwm5cocMJZnOGjPNRQEsGEc+N3ysAR4wPZxlgMt2PA
XfIldXsToMDRpeYhfdF+8AGs6Zs1c09XyE/p2N1vQy6NWNZIT7mcALcj3jlGyRSg
JkzURsiY5iTk0YjHC4YvjDRV+zhKyZwrTKPum5pW+pFbwAWc1GH8GXPWght2FzB1
9E3/rKSSxfEVQLmepXlRh6Ht35OUIMQp4RgOhTdzwpTRIy4Jd2J5v00OHSiTApdg
1pvaQaJnGt0Rb8ZnKispgkNpTh1qOr4gjYUybajROgao1XoUT3fJO4SHivgjWqI1
Fp/sszp9Cbc/Yf6+IzWnFR3qzndVcMYB4iZXmBdSYxwi0DpTLYEjpdSLutjIktId
XA5eSAMnJVdpP3SeknHQGxvq1yLbXV6bLllF6eXfx/7XACRlRba7BnueFdXDZXS0
CNY+6rd11e48533PprxV/9IR2IRx57AtOQ==
-----END X509 CRL-----
```

- 可能存在的安全威胁：
  - CRL篡改：攻击者可能会篡改CRL中的证书撤销信息，使得未被撤销的证书被认为已经被撤销。这可能会导致合法的用户无法访问合法的网站或应用程序，从而影响正常业务的运行。
  - CRL发放不及时：如果CRL发放不及时，可能会导致已被撤销的证书仍然可以被接受，从而为攻击者提供机会进行中间人攻击或者数据窃取。
- 防范建议：
  - 数字签名验证：CRL应该使用数字签名进行验证。数字签名可以保证CRL的完整性和真实性，从而防止CRL被篡改。
  - 定期更新CRL：CRL应该定期更新，以确保CRL中的证书撤销信息是最新的。证书管理人员应该建立定期更新CRL的机制。

- 利用OCSP：利用最新的在线证书状态协议(OCSP)，更快更安全地验证证书的状态

五、实验总结（收获和心得）（5分）

这次实验涉及的命令和操作要比第一次实验多很多，而且很多命令以及操作步骤需要我们自己查阅资料来预习，我觉得这不仅仅能够大大地增强我们的动手实践能力，也可以增强我们的获取信息的能力。

六、尚存问题或疑问、建议（5分）

- CRL更新后到分发给所有可能的用户的这段时间之内，如何防止已被撤销的证书仍然被用户认为是可接受？如何防备这期间可能发生的攻击？