中山大學
SUN YAT-SEN UNIVERSITY

《信息安全技术》

实验报告

(Assignment 3：X.509 数字证书解析程序设计)

学 院 名 称 ：	数据科学与计算机学院
专业（班级）：	17 软件工程 1 班
学 生 姓 名 ：	陆记
学 号	17343080
时 间 ：	2019 年 12 月 4 日

一、 X.509 证书结构描述

X.509 标准定义 了被写入数字证书的信息内容，同时描述了证书内容的数据格式，证书的结构如下：

整体结构：证书内容、签名算法和签名结果，用 `ASN.1`（Abstract Syntax Notation One）语法描述如下：

```
Certificate::=SEQUENCE{
    tbsCertificate      TBSCertificate,    // 证书内容
    signatureAlgorithm  AlgorithmIdentifier,  // 签名算法
    signatureValue      BIT STRING   // 签名值
}
```

1、**证书内容：**CA（证书颁发者）签名的信息，ASN.1 语法描述如下：

```
TBSCertificate::=SEQUENCE{
    version           [0]   EXPLICIT Version DEFAULT v1,
    serialNumber            CertificateSerialNumber,
    signature               AlgorithmIdentifier,
    issuer                  Name,
    validity                Validity,
    subject                 Name,
    subjectPublicKeyInfo    SubjectPublicKeyInfo,
    issuerUniqueID    [1]   IMPLICIT UniqueIdentifier OPTIONAL,
    subjectUniqueID   [2]   IMPLICIT UniqueIdentifier OPTIONAL,
    extensions        [3]   EXPLICIT Extensions OPTIONAL
}
```

①版本号（Version）：当前证书为哪个版本的 X.509 标准（v1、v2、v3），**为整数格式，默认为 v1，目前最常用为 v3。**其 ASN.1 语法类型 Version 的描述如下：

```
Version::=INTEGER {v1(0),v2(1),v3(2)}   // 整数0、1、2分别表示三个版本
```

②证书序列号（Certificate Serial Number）：用以区别同一实体发放的不同证书的数字序号，当某证书被吊销时，它的序列号被添加到 `CRL` 中。为整数格式，其 ASN.1 语法类型 `CertificateSerialNumber` 描述如下：

```
CertificateSerialNumber::=INTEGER
```

③签名算法标识符（Signature Algorithm Identifier）： 用于识别 CA 签写证书时所用的算法。其 ASN.1 语法类型 `AlgorithmIdentifier` 的描述如下：**（其中，algorithm 给出算法的标识符 OID，parameters(Optional)给出了算法的参数；OID 同时说明了加密算法和数字签名算法）**

```
AlgorithmIdentifier::=SEQUENCE{
    algorithm       OBJECT IDENTIFIER,  // 算法的OID
    parameters      ANY DEFINED BY algorithm OPTIONAL   // 算法的参数
}
```

常用的 `OID` 如下表：

OID	Algorithm
1.2.840.10040.4.1	DSA
1.2.840.10040.4.3	sha1DSA
1.2.840.113549.1.1.1	RSA
1.2.840.113549.1.1.2	md2RSA
1.2.840.113549.1.1.3	md4RSA
1.2.840.113549.1.1.4	md5RSA
1.2.840.113549.1.1.5	sha1RSA
1.2.840.113549.1.1.11	sha256RSA

④签发人信息（Issuer）： 签发证书的实体的 X.500 名称，通常为 CA

⑤证书主体信息（Subject）： 拥有证书公钥的实体的名字，采用 X.500 标准，在 Internet 中唯一，是实体的特征名（DN：Distinguished Name）。

`Issuer` 和 `Subject` 的 ASN.1 语法类型都为 `Name`，描述如下：

```
Name::=CHOICE{
    RDNSequence
}
RDNSequence::=SEQUENCE OF RelativeDistinguishedName
RelativeDistinguishedName::=SET OF AttributeTypeAndValue
AttributeTypeAndValue::=SEQUENCE{
    type    AttributeType,
    value   AttributeValue
}
AttributeType::=OBJECT IDENTIFIER
AttributeValue::=ANY DEFINED BY AttributeType
```

证书的 `Issuer` 和 `Subject` 用 X.509 DN 表示，DN 是由 RDN(Relative Distinguished Name)构成的序列，根据 ASN.1 语法，RDN 是由“**属性类型（OID）+属性值（STRING）**”表示，常用的属性类型名称及其 OID 如下表：

OID	属性类型名称	含义	简写
2.5.4.3	Common Name	通用名称	CN
2.5.4.6	Country	国名	C
2.5.4.7	Locality	地理位置	L
2.5.4.8	State or Province Name	洲/省名	S
2.5.4.10	Organization Name	机构名	O
2.5.4.11	Organizational Unit Name	机构单位名	OU

⑥**有效期（Validity）**：包括**起始时间**和**终止时间**，每一个证书只有在该时间段内有效。有效期可以短到几秒或长至一世纪，取决于许多因素，如签写证书所用私钥的强度以及愿为证书支付的金钱等。时间值可以用 `UTCTime` **或者** `GeneralizedTime` 的形式表示。ASN.1 语法描述如下：

```
Validity::=SEQUENCE{
    notBefore       Time,    // 起始时间
    notAfter        Time     // 截至时间
}
Time::=CHOICE{
    utcTime         UTCTime,
    generalTime     GeneralizedTime
}
```

⑦**主体公钥信息（Subject Public Key Info）**：被命名实体的公钥，包括该密钥所属公钥密码系统的算法标识符（OID）、相关的密钥参数以及公钥值。其 ASN.1 语法描述如下：

```
SubjectPublicKeyInfo::=SEQUENCE{
    algorithm           AlgorithmIdentifier,
    subjectPublicKey    BIT STRING
}
```

⑧**签发者唯一标识符和主体唯一标识符**（Issuer Unique Identifier 和 Subject Unique Identifier (Optional)）：证书签发者和证书主体的**唯一**标识符。其在 ASN.1 语法中为 `UniqueIdentifier` 类型，描述如下：

```
UniqueIdentifier::=BIT STRING
```

⑨**扩充域**（Extensions (Optional)）：一般忽略此部分

2、**证书签名算法**（Certificate Signature Algorithm）：包括算法的**标识符**（OID）、算法的**参数**。为 CA 对 `tbsCertificate` 进行签名所使用的算法，类型为 `AlgorithmIdentifier`（与公钥签名算法类型一样），其 ASN.1 语法描述如下：

```
AlgorithmIdentifier::=SEQUENCE{
    algorithm       OBJECT IDENTIFIER,
    parameters      ANY DEFINED BY algorithm OPTIONAL
}
```

3、**签名值**（Signature Value）：为用 X.509 标准的数字证书签名的结果，其在 ASN.1 语法中的描述如下：

```
SignatureValue::=BIT STRING
```

二、 数据结构

1、 证书内容结构体

```
// 证书内容结构体
struct TbsCertificate {
    string version;      // 版本号
    string serialNumber;     // 序列号
    string signature[2];     //算法OID和算法参数
    // 证书签发人和主体的属性类型（OID）和属性值（STRING）
    string issuer[6][2];
    string subject[6][2];
    string validity[2];      // 有效期：起止时间+终止时间
    string subjectPublicKeyInfo[3];// algorithm parameters Public-key
    string issuerUniqueID;   // 签发人唯一标识符（可选）
    string subjectUniqueID; // 主体唯一标识符（可选）
    string extensions;       // 扩充域
};
```

2、 证书总体结构

```
// 证书总体结构
struct X509cer{
    struct TbsCertificate cer_cnt; // 证书内容
    string sig_alg[2];       //  签名算法：算法OID+算法参数
    string sig_val; // 签名值
};
```

3、 算法的 OID 与名称匹配表（二维字符串数组）

```
// 签名算法OID与算法名表
string sa[8][2] = {
    {"1.2.840.10040.4.1", "DSA"},
    {"1.2.840.10040.4.3", "SHA1withDSA"},
    {"1.2.840.113549.1.1.1", "RSA"},
    {"1.2.840.113549.1.1.2", "MD2withRSA"},
    {"1.2.840.113549.1.1.3", "MD4withRSA"},
    {"1.2.840.113549.1.1.4", "MD5withRSA"},
    {"1.2.840.113549.1.1.5", "SHA1withRSA"},
    {"1.2.840.113549.1.1.11", "SHA256withRSA"}
};
```

4、 Issuer 和 Subject 信息的 OID 与其含义的匹配表（二维字符串数组）

```
// issuer和subject名OID和对应的含义
string issu[6][2] = {
    {"2.5.4.6", "Country(C)"},  // 国名
    {"2.5.4.8", "Sate or Province Name(S)"},    // 洲/省名
    {"2.5.4.7", "Locality(L)"}, // 地区名
    {"2.5.4.10", "Organization Name(O)"},       // 组织名
    {"2.5.4.11", "Organizational Unit Name(OU)"},   // 组织单位名
    {"2.5.4.3", "Common Name(CN)"}  // 通用名
};
```

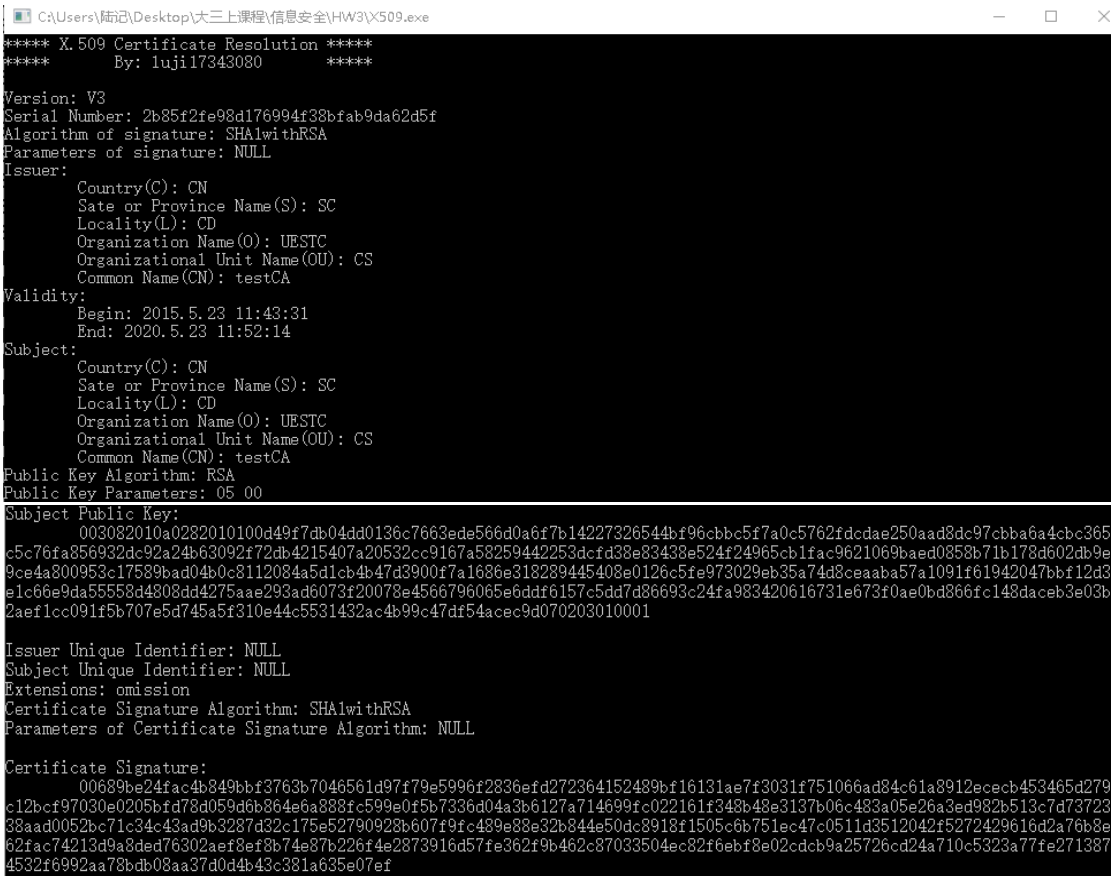
三、 C++源代码

Github 地址：

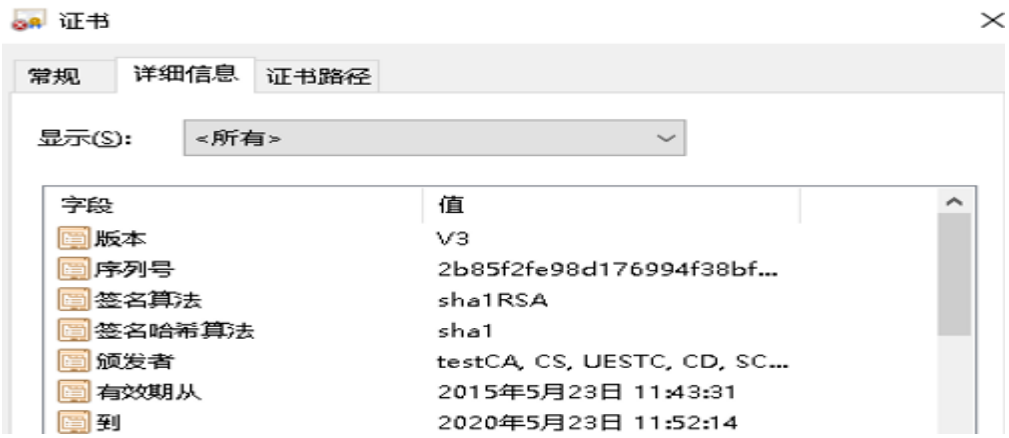
https://github.com/luji17343080/Information-security-technology/blob/master/X509/X509.cpp

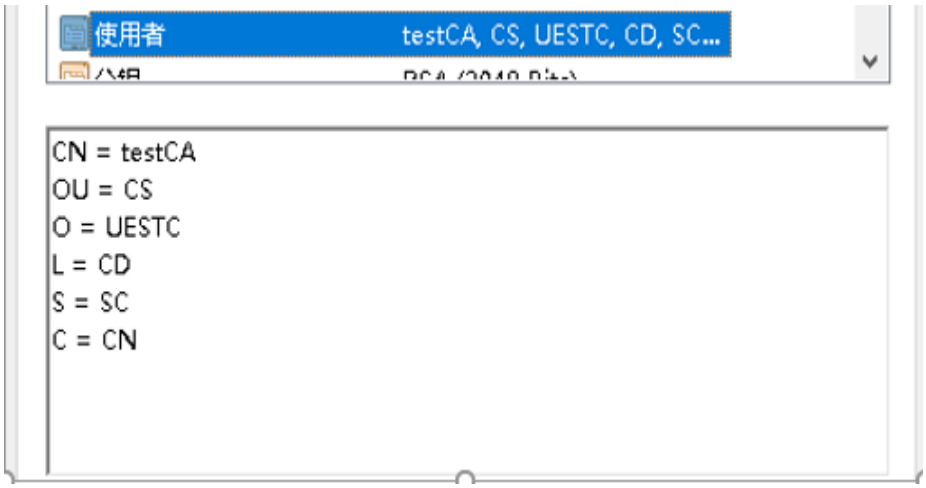
四、 编译运行结果

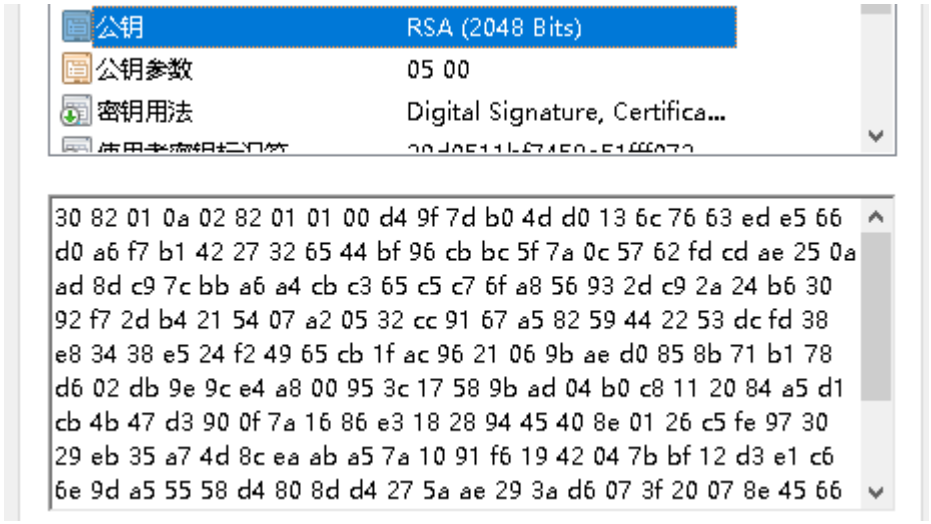
控制台结果：



证书对比：




使用者
testCA, CS, UESTC, CD, SC...
CN = testCA
OU = CS
O = UESTC
L = CD
S = SC
C = CN


公钥
RSA (2048 Bits)
公钥参数
05 00
密钥用法
Digital Signature, Certifica...
30 82 01 0a 02 82 01 01 00 d4 9f 7d b0 4d d0 13 6c 76 63 ed e5 66
d0 a6 f7 b1 42 27 32 65 44 bf 96 cb bc 5f 7a 0c 57 62 fd cd ae 25 0a
ad 8d c9 7c bb a6 a4 cb c3 65 c5 c7 6f a8 56 93 2d c9 2a 24 b6 30
92 f7 2d b4 21 54 07 a2 05 32 cc 91 67 a5 82 59 44 22 53 dc fd 38
e8 34 38 e5 24 f2 49 65 cb 1f ac 96 21 06 9b ae d0 85 8b 71 b1 78
d6 02 db 9e 9c e4 a8 00 95 3c 17 58 9b ad 04 b0 c8 11 20 84 a5 d1
cb 4b 47 d3 90 0f 7a 16 86 e3 18 28 94 45 40 8e 01 26 c5 fe 97 30
29 eb 35 a7 4d 8c ea ab a5 7a 10 91 f6 19 42 04 7b bf 12 d3 e1 c6
6e 9d a5 55 58 d4 80 8d d4 27 5a ae 29 3a d6 07 3f 20 07 8e 45 66