****

**《信息安全技术》**

**实验报告**

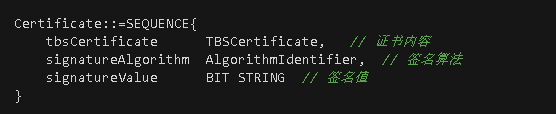
**（Assignment 3：X.509数字证书解析程序设计）**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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 |

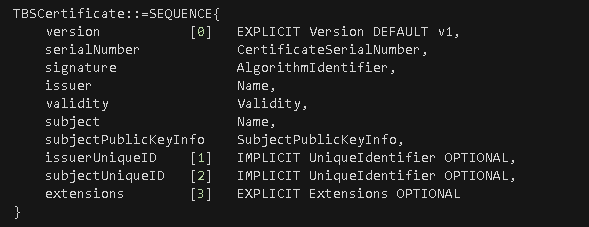
1. **X.509 证书结构描述**

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：



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



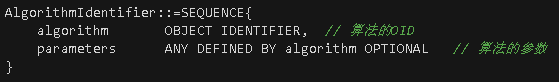
**①版本号（Version）：**当前证书为哪个版本的X.509标准（v1、v2、v3），为**整数格式，默认为v1，目前最常用为v3。**其ASN.1语法类型Version的描述如下：



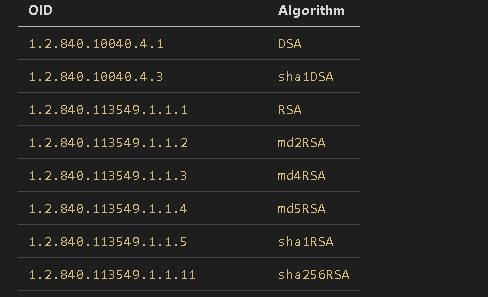
**②证书序列号（Certificate Serial Number）：用**以区别同一实体发放的不同证书的数字序号，当某证书被吊销时，它的序列号被添加到CRL中。为整数格式，其ASN.1语法类型CertificateSerialNumber描述如下：



**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）**



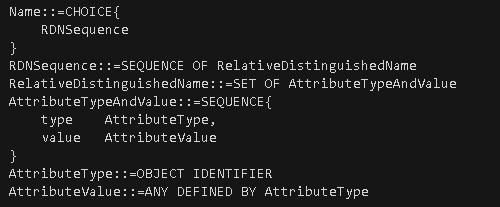
常用的OID如下表：



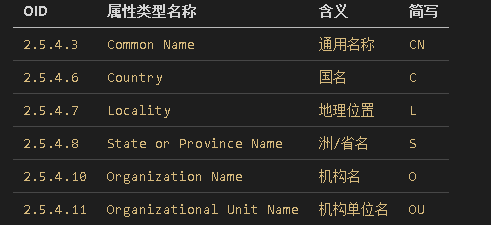
**④签发人信息（Issuer）：**签发证书的实体的X.500名称，通常为CA

**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）。**

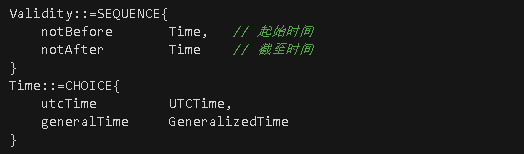
Issuer和Subject的ASN.1语法类型都为Name，描述如下：



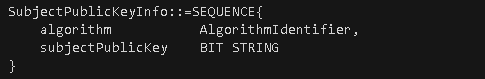
证书的Issuer和Subject用**X.509 DN**表示，**DN**是由**RDN(Relative Distinguished Name)**构成的序列，根据ASN.1语法，**RDN**是由**“属性类型（OID）+属性值（STRING）”**表示，常用的属性类型名称及其OID如下表：



**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：



**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：

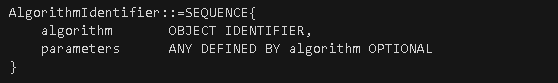


**⑧签发者唯一标识符和主体唯一标识符（Issuer Unique Identifier和 Subject Unique Identifier (Optional)）：**证书签发者和证书主体的**唯一**标识符。其在ASN.1语法中为UniqueIdentifier类型，描述如下：



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

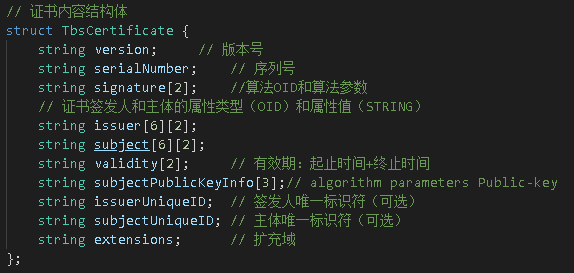
**2、证书签名算法（Certificate Signature Algorithm）：**包括算法的**标识符（OID）、**算法的**参数**。为CA对tbsCertificate进行签名所使用的算法，类型为AlgorithmIdentifier（与公钥签名算法类型一样），其ASN.1语法描述如下：



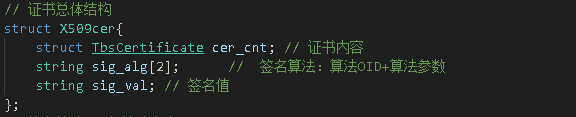
**3、签名值（Signature Value）：**为用X.509标准的数字证书签名的结果，其在ASN.1语法中的描述如下：



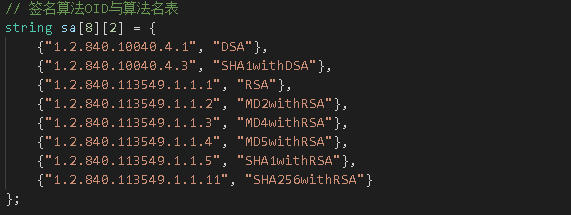
1. **数据结构**
2. **证书内容结构体**



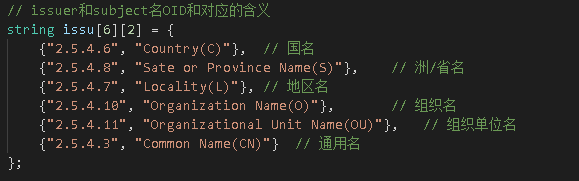
1. **证书总体结构**



1. **算法的OID与名称匹配表（二维字符串数组）**



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

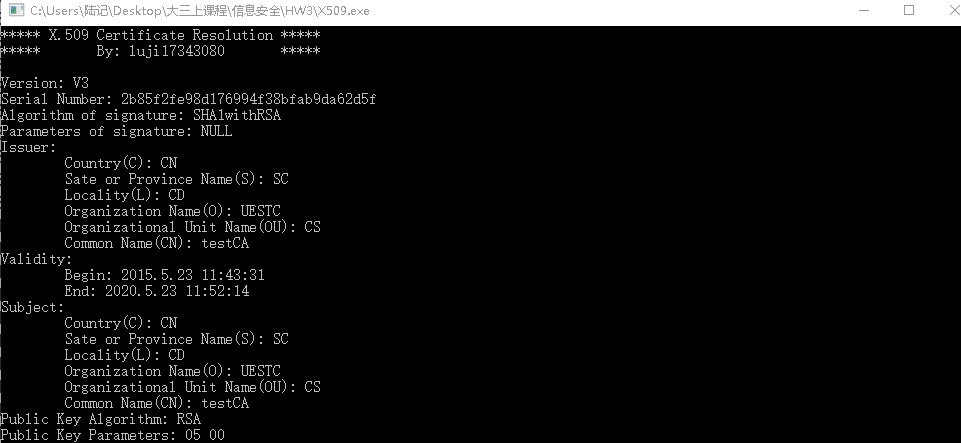


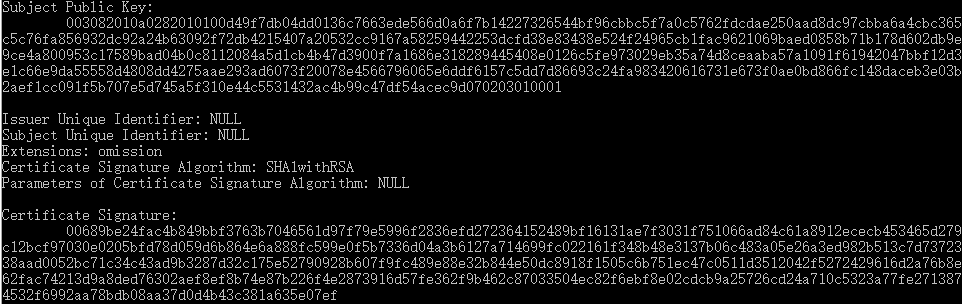
1. **C++源代码**

**(github地址：**<https://github.com/luji17343080/Information-security-technology/tree/master>**)**

1. **编译运行结果**

**控制台结果：**





**证书对比：**