GetX509Cercate

院系：数据科学与计算机学院

学号：16341023

姓名：周芙蓉

1. X.509证书结构描述

X.509被广泛使用的数字证书标准，是由国际电联电信委员会（ITU-T）为单点登录（SSO-Single Sign-on）和授权管理基础设施（PMI-Privilege Management Infrastructure）制定的PKI标准。X.509定义了（但不仅限于）公钥证书、证书吊销清单、属性证书和证书路径验证算法等证书标准。

在X.509系统中，CA签发的证书依照X.500的管理，绑定了一个唯一甄别名（DN-Distinguished Name ），可以包含多个字段和值，还可以支持别名（Alternative Name ）。

X.509标准规定了证书可以包含什么信息，并说明了记录信息的方法（数据格式）。出了签名外，X.509包含以下数据：

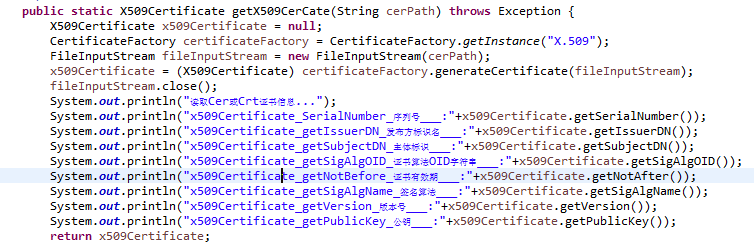
|  |  |
| --- | --- |
| Version | 识别用于该证书的X.509标准的版本，可以影响书中所能指定的信息。迄今为止，已定义的版本有三个。 |
| Serial Number | 发放证书的实体有责任为证书指定序列号，以使其区别于该实体发放的其他证书。此信息的用途有很多，例如，若某一证书被撤销，其序列号将放到证书撤销清单（CRL）中。 |
| Signature Algorithm | 用于识别CA签写证书时所用的算法。 |
| issuer | 签发证书的实体的X.500名称。通常是一个CA。使用该证书意味着信任签写该证书的实体。 |
| Validity | 每个证书只能在一个有限的时间段内有效。该有效期以起始日期和终止日期表示，有效期取决于许多因素，例如用于签写证书的私钥的使用频率及愿为证书支付的金钱等。它是在没有危及相关私钥的条件下，实体可以依赖公钥值的预计时间。 |
| Subject | 证书可以识别其公钥的实体名。此名称使用 X.500 标准，因此在Internet中应是唯一的。它是实体的特征名 (DN)，例如：  CN=Java Duke，OU=Java Software Division，O=Sun Microsystems Inc，C=US （这些指主体的通用名、组织单位、组织和国家）。 |
| Subject Public Key info | 这是被命名实体的公钥，同时包括指定该密钥所属公钥密码系统的算法标识符及所有相关的密钥参数。 |

在HTTPS通讯中最常用的是cer/crt和pem

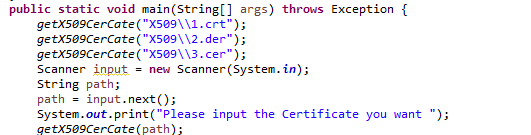
1. 数据结构

本次作业我使用的是Java编写的，由于Java有CertificateFactory和X509Certificate包，代码编写相对就简单了许多。代码共分为两部分，第一部分为数据的输入输出，第二部分为按照标准定义给出证书中有关项目的中（英）文内容陈述。

获取证书的相关内容陈述：

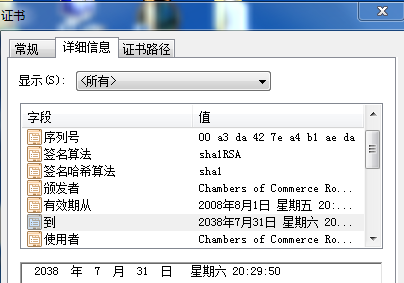


输入证书，输出相关信息

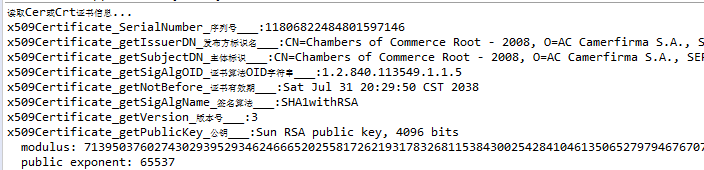


1. 程序运行截图

从浏览器中导出部分证书作为测试文件，打开证书，查看证书相关信息，记录相关信息，以便程序正确性检验，下面是证书部分内容陈述：



代码实现读入X.509证书，输出相关内容陈述：



代码实现输入的陈述与原文件相关内容一致，程序运行正确，完成实验目标。

1. 思考与总结

由于选用JAVA语言编写程序的原因，本次作业难度降低了许多，基本没有什么难点。作业一开始走了许多弯路，对题目的理解感觉不是很清楚。在明确实验具体要求时，才渐渐明朗起来，个人感觉作业的难点不在于代码的编写，在于对X.509这一密码学公钥证书的格式标准的理解。如何获取证书和陈述证书中哪些内容成了需要真正思考的一部分。网上给出了很多获取数字证书的方法，一般而言可以直接通过浏览器直接导出。

通过此次作业，我收获了很多，对公钥加密和X.509有了一定的了解，同时也发现了自己的很多不足。在今后的作业中我将继续努力，汲取更多新的知识。