**密码学第十次作业**

1.【数字签名的基础知识】

（1）数字签名实现的其他方法难以实现的安全目标是：。

（2）一个数字签名方案是一个5元组，其中，是，是，是，是，是。

（3）数字签名的另一种形式化定义如下：一个数字签名方案包括三个概率多项式时间算法，常记为。其中：为，接受输入安全参数，输出；为，接受输入消息和（选填：公钥或私钥），输出签名；为，接受输入，输出一比特数据，若则表示签名有效，反之若则表示签名无效。

（4）请从攻击者的能力出发，从低到高列出5种对数字签名的攻击类型：、、、、；请从对签名方案遭受攻击的危害性出发，从高到低列出4种成功攻击签名方案的攻击目标：、、、。

（5）数字签名是一种机制，它使得消息的产生者可以添加一个起签名作用的码字。通过计算消息的Hash值并用产生者的加密 Hash 值来产生签名。

（6）数字签名应满足哪些要求？

2.【数字签名的具体实现方案】

（1）ElGamal数字签名方案：

I. ElGamal数字签名方案的基本元素是和，二者的关系为。其密钥生成算法如下：用户生成，使得，计算，则的私钥是，公钥是。

II. 取，，，选取满足，求对消息的签名，并对该签名进行验证。

III. Elgamal签名过程选取的随机数需要保密，且每对一个消息签名时都要重新生成。对于II.的例子，请写出：

若敌手知晓，计算出私钥的过程。

若敌手不知晓，但敌手截获另一也选取同一随机数的对的签名，则其也可以计算出私钥，请写出计算过程。

（2）ECDSA数字签名方案：

I.选取公共参数：选取椭圆曲线和基点。

本题选择曲线，基点，易知点的阶。

II.密钥生成算法：签名者选择私钥，计算公钥。

本题选择，则。

III.签名算法：选取随机数，计算消息的合法签名。

本题选择，假设消息的哈希值，请写出计算的过程。

IV.验证算法：根据公钥，验证消息的签名。

请写出对上一问所求签名的验证过程。

（3）一个不安全的签名方案如下：

公共参数选取：选取素数和它的本原根。

密钥生成算法：选取私钥，公钥。

签名算法：对生成签名：求，签名为。

验证算法：比较。

请写出对该签名方案的通用伪造方案。

3.【密钥管理与分发】

（1）对称密钥分配有4种基本方法，分别为：

①；

②；

③；

④。

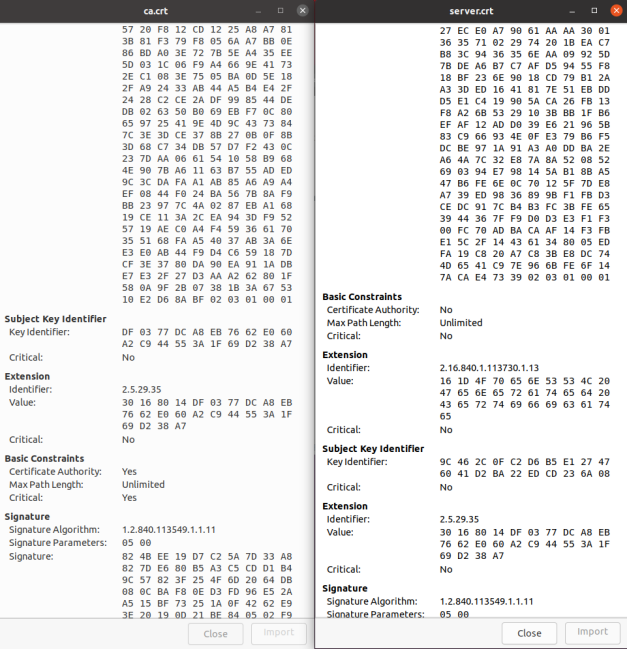
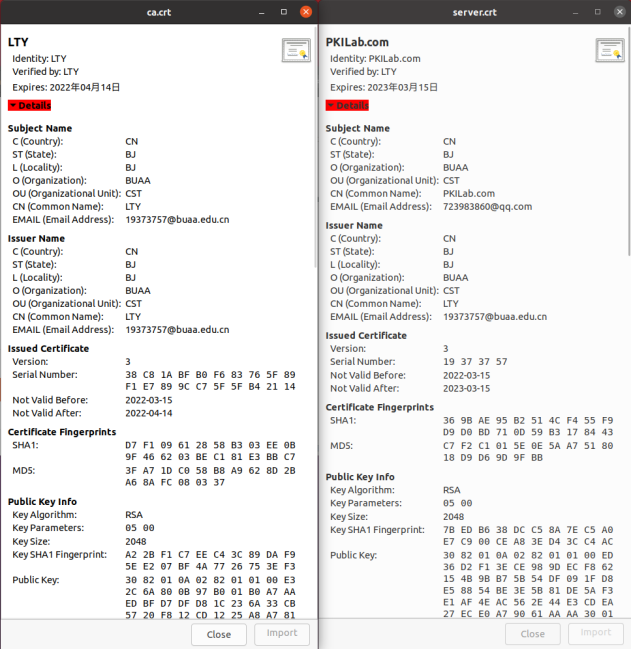
（2）Needham-Schroeder协议是最经典的会话密钥分发协议（尽管存在一定安全问题），其中基于对称加密的对称密钥分发方案被称为NSSK，而基于非对称加密的对称密钥分发方案被称为NSPK。

I.请结合PPT内容并查阅资料，画出NSSK协议的流程图并写出协议执行步骤。

II. （选做）请查阅资料，画出NSPK协议的流程图并写出协议执行步骤。

1. 什么是公钥基础设施？创建PKI的主要目的是什么？

（4）以下是两个X509证书示例，请结合教材和该截图分析X.509证书的结构，并回答：两证书分别是用谁的私钥签名的？访问https网页时，浏览器如何对该网页的证书验证？



**注意：**

以上作业请使用**pdf**文档格式提交，于**2023年5月28日（星期日）23:59**之前在OJ系统上提交，并将作业命名为“**学号\_姓名\_密码学第十次作业**”。如“20371234\_张三\_密码学第十次作业”。