加解密实验实验指导书

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
   （http://www.openssl.org/docs/apps/openssl.html）
3. 学习和理解数字证书的管理

二、实验内容

序	内容	项目	备注
1)	OpenSSL 加密	文件对称加密	
2)		计算文件摘要	
3)	OpenSSL 证书管理	签发 CA 根证书	
4)		签发客户证书（2-3 张）	
5)		撤销客户证书，并查看证书撤销列表	

三、实验步骤

1. OpenSSL 加密

1.1 准备：

1) 启动虚拟机，登录 ubuntu 操作系统 (name/pw)： test/testtest；进入“虚拟机”-“快照”-“Origin”，从 Origin 快照处开始实验；

2) 查看 openssl 命令：

```
$ openssl help
```

1.2 对文件进行对称加解密；

1.3 计算文件摘要；

1.4 对输入文件简单修改后，再次计算摘要，对两者进行比较。

2. OpenSSL 证书管理

2.1 配置

1) 查看 OpenSSL 配置文件（/etc/ssl/openssl.cnf）信息，并对配置文件中的 *[CA_default]*进行如下修改

```
dir             = /etc/ssl              # Where everything is kept
database        = $dir/CA/index.txt     # database index file.
certificate       = $dir/certs/cacert.pem       # The CA certificate
serial          = $dir/CA/serial        # The current serial number
private_key     = $dir/private/cakey.pem      # The private key
```

2) 在/etc/ssl/目录下建立两个目录 CA 和 newcerts

3) 利用下列命令在/etc/ssl/CA 目录下建立两个文件

```
$ sudo sh -c "echo '01' > /etc/ssl/CA/serial"
$ sudo touch /etc/ssl/CA/index.txt
```

2.2 签发 CA 自签名证书

1) 生成自签名证书
2) 将生成的 CA 公钥证书文件和私钥文件分别转移至/etc/ssl/certs 和/etc/ssl/private/目录下

2.3 发放客户证书

1) 生成私钥长度和有效期分别为 1024、2 年，1024、3 年，2048、3 年的客户证书。
2) 查看/etc/ssl/CA 和/etc/ssl/newcerts 两个目录下有关文件的内容。

2.4 证书撤销

1) 撤销刚才发放的客户证书中的前两张证书，并检查证书的更改情况。
2) 发布 crl 列表。

四、思考题

1. 简单描述 OpenSSL 客户证书发放和撤销的步骤，并总结需要注意的事项。
2. 在 OpenSSL 的文件加密、文件摘要以及公私钥生成实验中你采用的是何种算法？请用 openssl speed 命令分别测试这三种算法的速度，对结果进行分析，并总结不同加密算法的特点和用途。

作业要求：

1) 个人作业，以 word 或 PDF 文档形式提交，具体格式见模板。
2) 作业文档命名：学号_姓名_ Cipher.文件扩展名
3) 在 2019 年 4 月 10 日（周三）晚 22:00 前报告在线提交

课堂交流申请：

2019 年 4 月 9 日（周二）晚 22:00 前发 PPT 申请至邮箱：mengkui@sjtu.edu.cn