

《应用密码学》课程实践

实践题目 4 RSA 的实现

实践要求:

1. 要求实现 RSA 的**密钥生成**、**数据加密**、**数字签名**。

2. 密钥生成包括生成两个大素数 p, q , 计算 $n=p \times q$ 和 $\Phi(n)=(p-1)(q-1)$, 然后选择与 $\Phi(n)$ 互素且小于 $\Phi(n)$ 的整数 e , 计算 $d=e^{-1} \bmod \Phi(n)$, 最后得到公钥 $\{e, n\}$ 和私钥 $\{d, n\}$ 。要求 p, q 至少均大于 10^{10} , 将生成的整数 p 、 q 、 n 、 e 、 d 分别写入文件 $p.txt$ 、 $q.txt$ 、 $n.txt$ 、 $e.txt$ 、 $d.txt$ 中。注意, 所有整数都必须用 16 进制表示。必须将整数转化成字符串后再写入文件, 例如素数 $p=6B1BCF$ (用 16 进制表示), 则写入文件的应是字符串 "6B1BCF" 而非整数 6B1BCF。

3. 数据加密是指用公钥 $\{e, n\}$ 对指定的明文进行加密。数字签名是指用私钥 $\{d, n\}$ 对指定的明文进行加密。数据加密和数字签名都有一组对应的测试数据, 以便检查程序的正确性。要求以命令行的形式, 指定明文文件、密钥文件的位置和名称以及加密完成后密文文件的位置和名称。加密时先分别从指定的明文文件、密钥文件中读取有关信息, 然后进行加密, 最后将密文写入指定的密文文件。注意, 密文(一个整数)必须用 16 进制表示。必须将密文(一个整数)转化成字符串后再写入文件, 例如密文 $c=154A6B$ (用 16 进制表示), 则写入文件的应是字符串 "154A6B" 而非整数 154A6B。

命令行的具体格式如下:

```
e3rsa -p plainfile -n nfile [-e efile] [-d dfile] -c cipherfile
```

参数:

-p plainfile	指定明文文件的位置和名称
-n nfile	指定存放整数 n 的文件的位置和名称
-e efile	在数据加密时, 指定存放整数 e 的文件的位置和名称
-d dfile	在数字签名时, 指定存放整数 d 的文件的位置和名称
-c cipherfile	指定密文文件的位置和名称

4. 用 C 和/或 C++ 语言完成程序。

5. 最终上交的作业包括: 电子版的实践报告、程序源代码以及生成密钥时所产生的文件 $p.txt$ 、 $q.txt$ 、 $n.txt$ 、 $e.txt$ 、 $d.txt$ 。要求由源代码能重新正确生成可执行代码。

6. 实践报告应包括以下内容: 作业标题、学号、姓名、E-mail、作业内容描述、实验环境描述、实验过程简述、实验结果(实验的正确性)、作业的收获和体会。

附录: 测试数据

明文: (用 16 进制表示) 63727970746F677261706879 (明文文件如: $rsa_plain.txt$)

公钥: (用 16 进制表示, 公钥文件如: $rsa_pubkey.txt$)

$n = 73299B42DBD959CDB3FB176BD1$

$e = 10001$

私钥: (用 16 进制表示, 私钥文件如: $rsa_prikey.txt$)

$n = 73299B42DBD959CDB3FB176BD1$

$d = 63C3264A0BF3A4FC0FF0940935$

密文: (用 16 进制表示)

数据加密: 6326DC198AAE1DB64FDC32D440 (密文文件如 $rsa_cipher.txt$)

数字签名: CA653B30EED2C6B77DCB8381F (签名文件如 $rsa_sign.txt$)