密码学实验大作业实验报告

20373971 鲁超杰

一、 实验主题

以面向对象方式实现密码库的设计与封装，并具有一定的差错检测。

二、 实验内容

1. 基础数学库

(1)素数检测

采用 Miller Rabin 算法。

(2)最大公约数

(3)扩展欧几里得

(4)快速模幂

(5)逆元

(6)素数表

线性筛法得到[2, n]内素数

(7)大素数生成

2. 分组密码

SM4 分组密码对文件加解密。实现了 CTR 和 OFB 两种工作模式，可以对文件进行加解密。

其中对文件路径、初始向量、密钥等进行了输入检测。

3. 公钥密码

SM2 公钥密码，SM2 中的哈希算法采用 SM3 算法。

4. 数字签名

ElGamal 数字签名算法。

其中的哈希函数为 SM3

5. 哈希算法

SM3 哈希算法。

三、 输入检测

对各个函数的输入参数进行合法检测，不满足则抛出异常。例子如下（还有其他不一一列举）：

在 SM4 中对密钥长度检测：

```
if type(k) != type('string') or len(k) != 32:
    raise ValueError
```

图 3-1 SM4 密钥长度检测图

在 Miller Rabin 素数检测中对输入数检测：

```
if N <= 1 or type(N) != type(1):
    raise ValueError
```

图 3-2 素数检测输入检测图

四、 测试结果

编写了测试函数，引入了之前密码学实验课的某些测试数据。

可以看到测试都是成功的。

```
---now test LB_crypto.math---
is_prime ok!
gcd ok!
exgcd ok!
fast_pow ok!
get_inv ok!
CRT ok!
get_prime ok!
generate_big_prime ok!
---now test SM4---
SM4_CTR ok!
SM4_OFB ok!
---now test SM2---
SM2 ok!
---now test Digital Signature---
ElGamal Digital Sign ok!
---now test SM3---
SM3 ok!
```

图 4-1 测试结果打印图

五、 函数调用关系总图

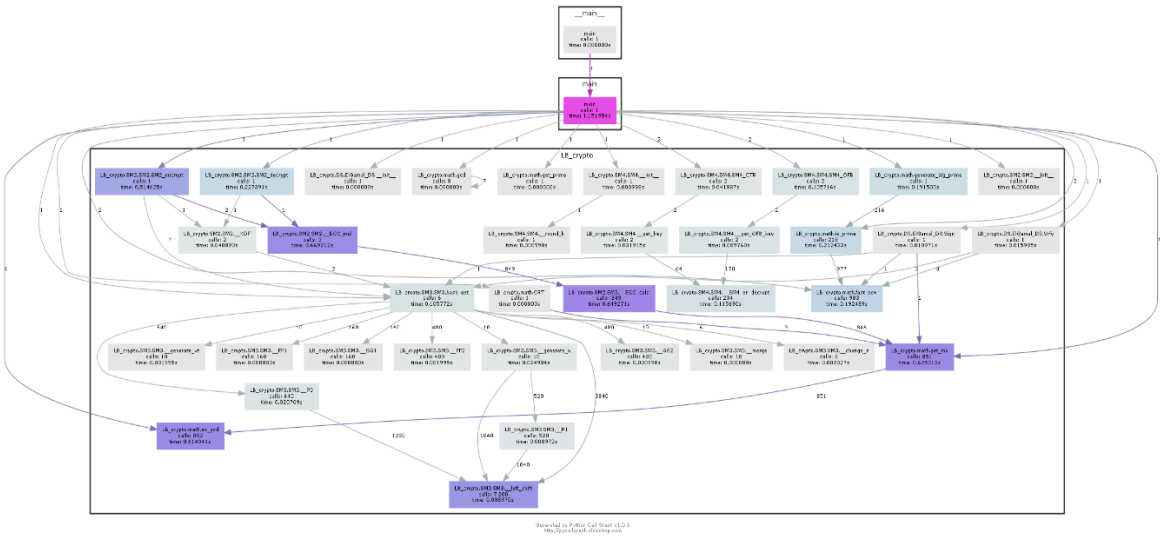

图 5-1 全家福(doge)

六、 实验心得

集成之前的密码算法到密码库的工作量比想象大好多，要对密码算法重新调整输入输出以及各种参数，还要对部分算法支持

文件输入输出。

密码库封装好之后可以直接调用，以后如果要用得到的话会方便很多。