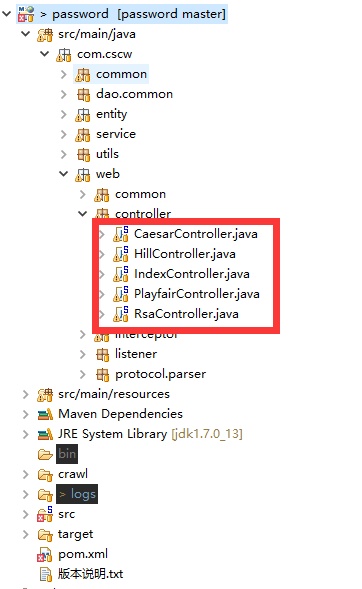
**14级软件04班**

**萧启程**

**3114006304**

# 实验说明

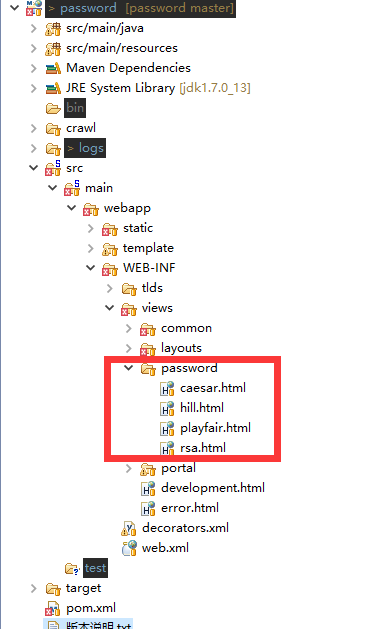
1. 实验演示网址：<http://104.207.152.130:8080/test_password/>
   * 因为数据库连接存在问题，所以在第一次连接此网页时可能会有一分钟的延时，耐心等待即可
2. 重要源码位置说明



主要后端源码在src/main/java/com/cscw/web/controller包下

里面是最主要的后台代码，算法基本在那5个java文件里面，另外IndexController是用来调用初始首页的里面无重要代码。

前端代码位置：



1. 源码阅读说明（解析hill算法）

进入\src\main\java\com\cscw\web\controller\HillController.java

主要方法：

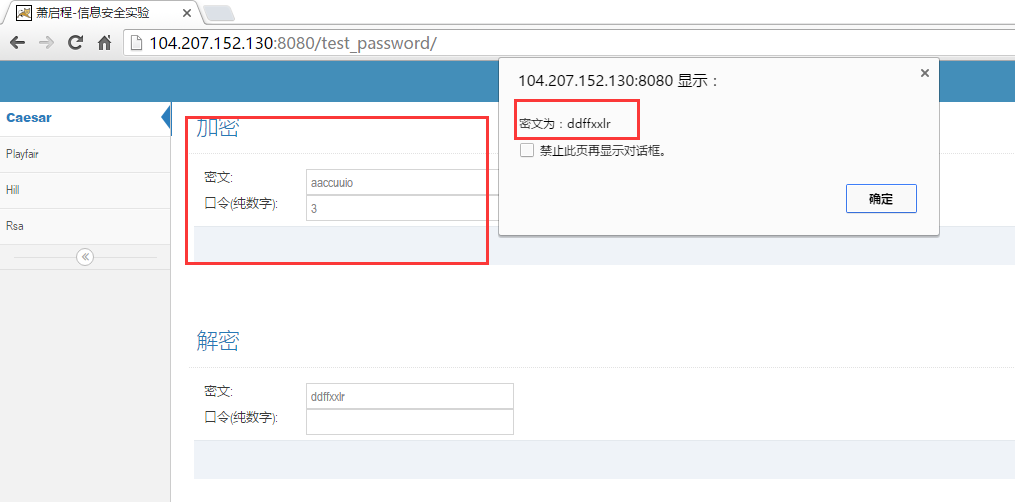




1. 使用说明与结果截图
   * Caesar

运行说明：

加密：

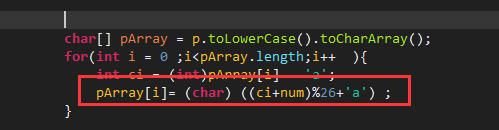


解密：



可以看到解密后弹出框的明文显示为 对应的明文。

主要实现代码：



将明文分割成char数组parray，然后一个一个+num%26+’a’

* + Playfair

输入关键词无重复八位字母



解密：



因为是k填充重复字母，所以解密后有k出现

算法解析：

得到前端的明文后，规范化处理明文后（重复加入字母k,个数补全），按照书本上的替换逻辑，按照矩阵得出对应的字母，然后加入到密文中。解密类似。

* + Hill

加密

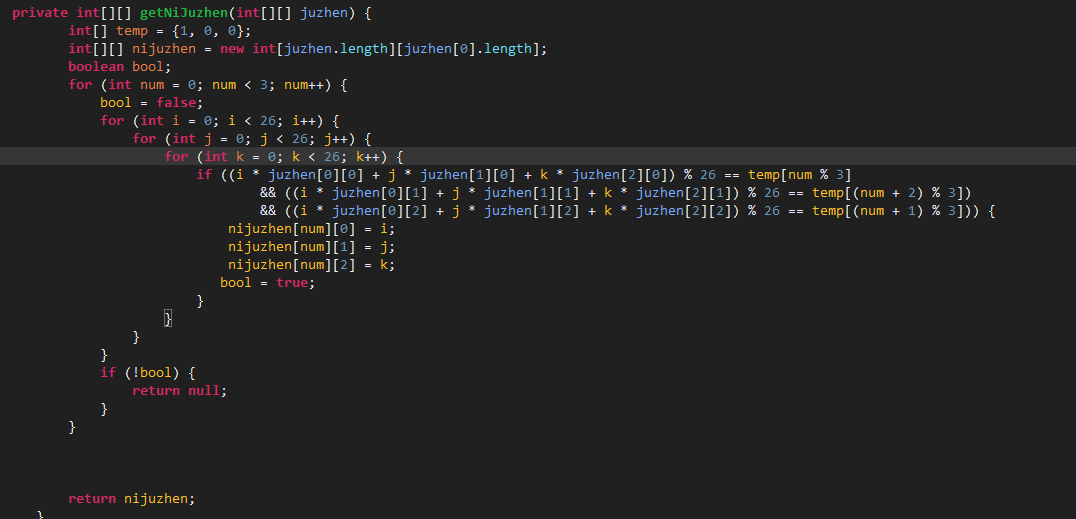


解密：

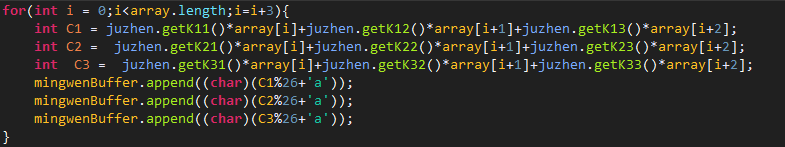


算法分析：

算法的难点在于矩阵求逆，而对于书本上的要求，矩阵内的数字肯定是0-25之内的，因此我们可以用算法：



求到逆矩阵之后，相应的求密文只是简单的按照公式相乘相加：



* + Rsa

初始化：



加密



解密：

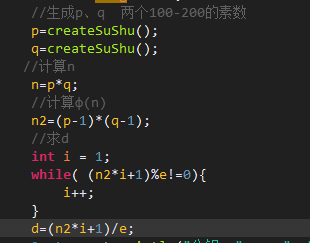


算法分析：

密文的字符串是以五个字符为单位的，即明文一个字符转换成5位数字。

生成两个素数pq : 用Random类生成100-200的随机数，然后验证是否是素数，不是则从新生成，重新验证，直至为素数。

求φ(n)和d：



加密过程：讲明文字符串分解成一个一个字符，根据ascii码转换成整形，再将这个数进行模指运算。解密过程类似。

模指运算算法:

