**计算机网络编程**

**实验报告**

**班级：07111707**

**组长：1120171189 崔程远**

**成员：1120172149 吴沁璇**

**1120172153 张澈**

**1120172163 王晓媛**

**1120172733 张鉴昊**

**1120172765 曾煜瑾**

**1120173326 曾紫飞**

**北京理工大学**

**计算机学院**

**2020年5月**

**北京理工大学**

**第三章 实验5 CHAP身份验证口令验证算法程序**

**1. 实验目的**

CHAP身份验证口令验证

**2. 实验内容**

本次实验内容为查阅CHAP标准规范，编写口令验证算法程序.

程序运行屏幕输出关键要点：

通过命令行参数给出要验证的口令

屏幕显示当前要验证的口令

屏幕显示当前生成的随机数

屏幕显示当前生成的MD5摘要值

**3. 实验原理**

PPP协议的身份验证方法包括PAP和CHAP，PAP口令验证协议由于直接传输明文用户名和口令，通过网络抓包很容易进行破解。CHAP协议由于不直接传输口令，而是采用生成随机数（不重字）和口令进行拼接和MD5摘要计算，通过MD5摘要值进行验证，安全性较高，

**4. 实验环境**

|  |  |  |
| --- | --- | --- |
| 语言 | 集成开发环境 | 编译器 |
| C++ | Visual Studio 2017 | gcc version 4.8.1 |
| Java | Eclipse 2019 | java version "1.8.0\_65" |
| Python | Pycharm 2017 | Python 3.7.0 |

**5. 实验步骤**

* C

首先检测参数数量，接收预设口令；生成随机数；打印预设口令；接收待检验口令并打印；打印随机数；模拟被验证方和验证放分别生成待附加段的口令的MD5值；打印校验结果。

Itobarr() 将随机生成的整数变为byte数组形式，模拟字节传输

GenRandNum() 生成随机数

CheckMD5()检验两端MD5

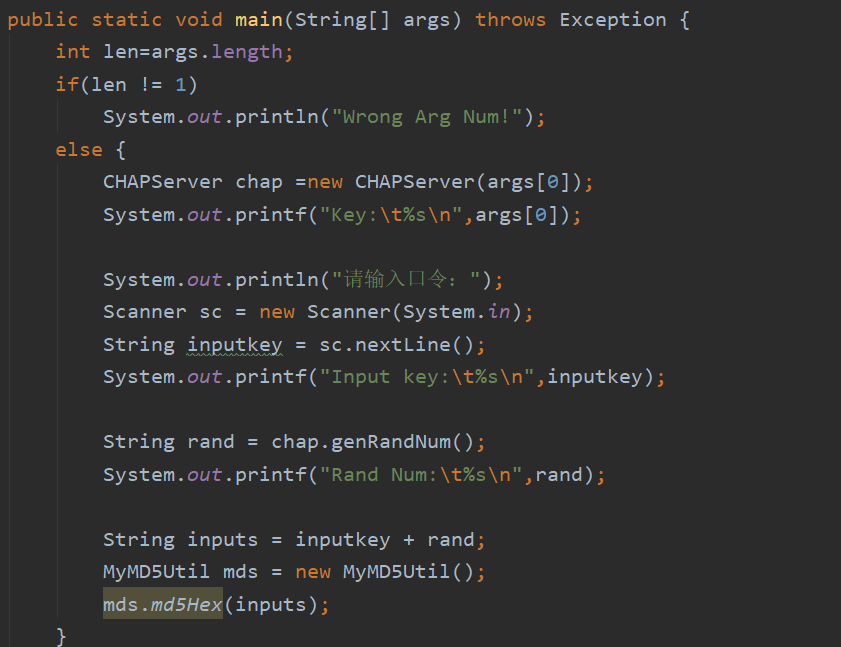
genMd5()拼接口令和附加段，生成相应MD5值

* Python

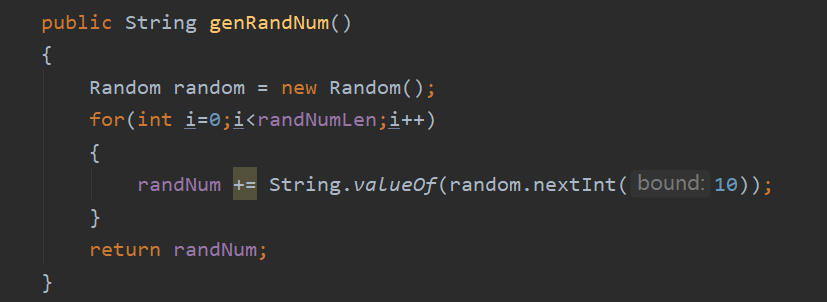
首先检测参数数量，创建CHAPServer类对象；接收预设口令；打印预设口令；接收待检验口令并打印；生成随机数并打印随机数；模拟被验证方和验证放分别生成待附加段的口令的MD5值；打印校验结果。

* Java

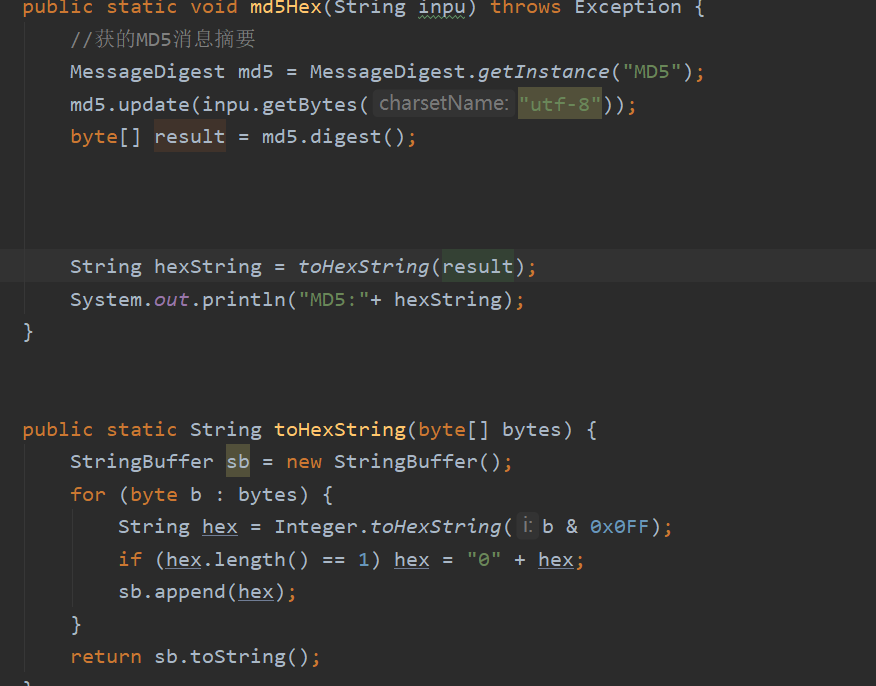
程序主体部分：



随机数和口令进行拼接：

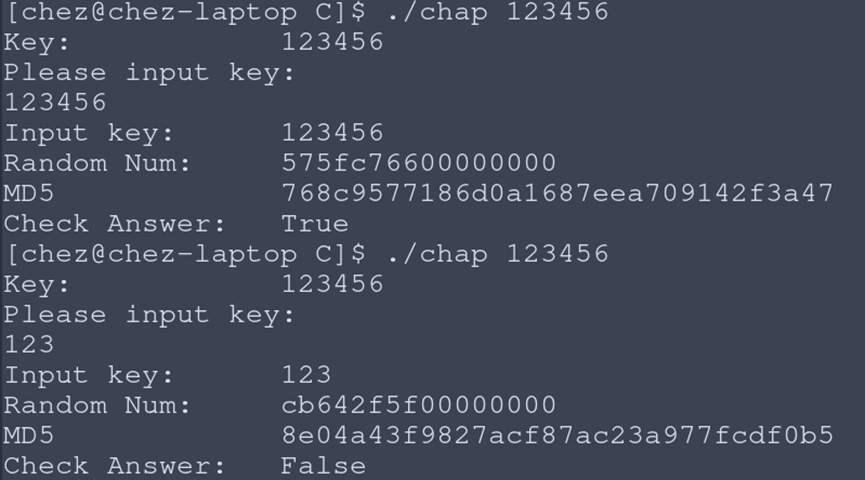


计算MD5值：

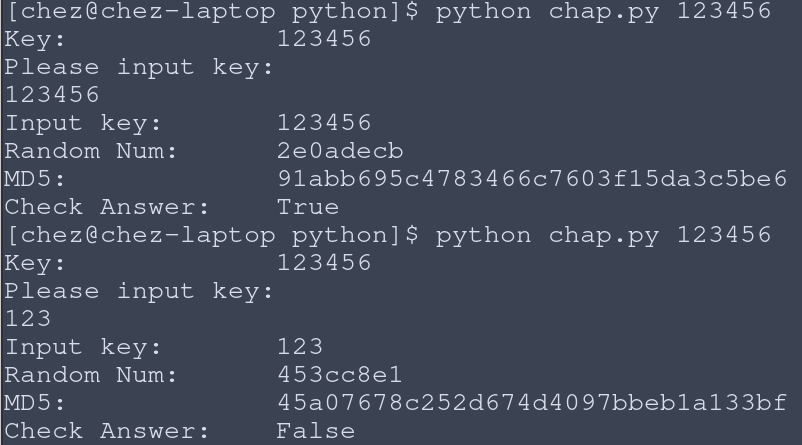


* 实验效果：

C：



Python：



Java：





**6. 实验总结**

这次实验主要考察了CHAP身份认证的方法，相较于明文传输，CHAP通过MD5的身份验证方法更加安全。通过本次实验我更加了解CHAP验证中MD5的作用和如何确保安全性。

总之，对CHAP验证过程和PPP协议有了更深的认识。