云南大学数学与统计学院
上机实践报告

课程名称： 近代密码学实验	**年级：** 2015 级	**上机实践成绩：**
指导教师： 陆正福	**姓名：** 刘鹏	
上机实践名称： 离散对数问题实验	**学号：** 20151910042	**上机实践日期：** 2018-03-07
上机实践编号： No.03	**组号：**	**上机实践时间：** 22:39

一、实验目的

熟悉离散对数问题（DLP）及其有关的密码体制。

二、实验内容

1. 编程实现与离散对数问题（DLP）有关的求解算法；
2. 编程实现 Deffie-Hellman 体制；
3. 编程实现 EIGamal 体制。

三、实验平台

Windows 10 ProWorkstation1803；
SageMath version 8.2, Release Date: 2018-05-05

四、实验记录与实验结果分析

1 题

编程实现与离散对数问题（DLP）有关的算法。求解离散对数问题常见的算法有：Shanks 的大步小步算法（baby-step giant-step algorithm）、Pollard rho 算法、Pohlig-Hellman 算法、Index Calculus 算法等。对于三十位以上的素数，已知最优的模p剩余类域中离散对数求解算法是应用了数域筛法技术的 Index Calculus 算法。

2 题

编程实现 Diffie-Hellman 密钥交换体制。

Solution:

Diffie 和 Hellman 在一篇具有独创意义的论文中首次提出了公钥算法，给出了公钥密码学的定义，该算法通常称为 Diffie-Hellman 密钥交换。该算法的目的是使两个用户能安全地交换密钥，以便在后续的通信中用该密钥对消息加密。该算法本身只限于进行密钥交换。[1]

Diffie-Hellman 算法的有效性是建立在计算离散对数是很困难的这一基础上的。一个素数p的本原根a，满足如下条件：$\mathrm{a \bmod p}$，$\mathrm{a^2 \bmod p}$，$\cdots$，$\mathrm{a^{p-1} \bmod p}$是整数1到$\mathrm{p}-1$的一个置换。对于任意一个整数b，必然有如下结论：存在一个整数i，满足$\mathrm{b \equiv a^i \bmod p}$。这里的这个$\mathrm{i}$称为$\mathrm{b}$的以$\mathrm{a}$为底的模$\mathrm{p}$离散对数，记为$\mathrm{dlog}_{a,p}(\mathrm{b})$。

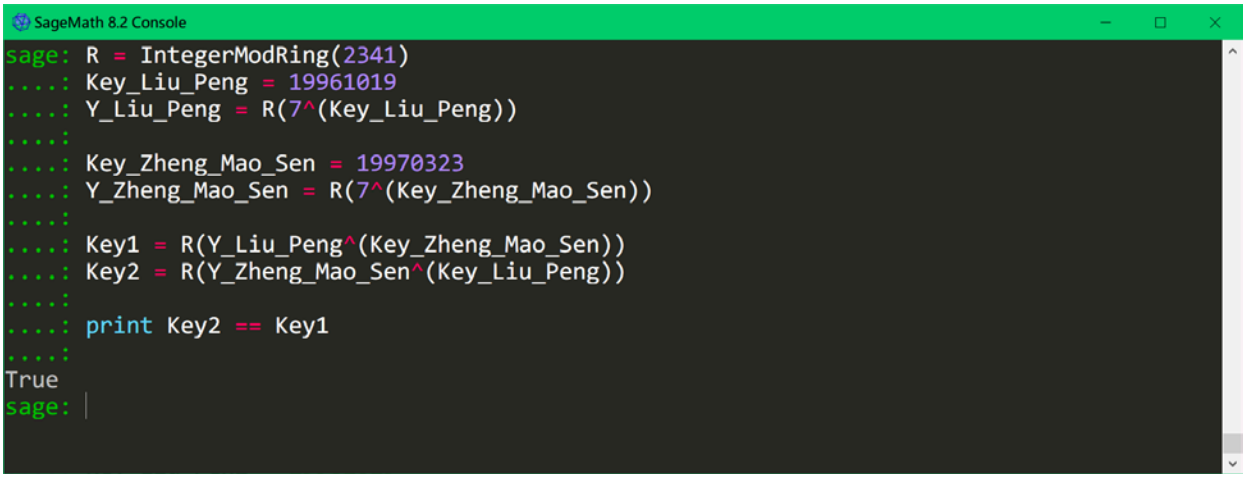
Sage 代码

```
R = IntegerModRing(2341)
Key_Liu_Peng = 19961019
Y_Liu_Peng = R(7^(Key_Liu_Peng))

Key_Zheng_Mao_Sen = 19970323
Y_Zheng_Mao_Sen = R(7^(Key_Zheng_Mao_Sen))

```

```
Key1 = R(Y_Liu_Peng^(Key_Zheng_Mao_Sen))
Key2 = R(Y_Zheng_Mao_Sen^(Key_Liu_Peng))

print Key2 == Key1
```

可以看到，这个程序里面需要对私钥进行以本原根为底取指数，然后取模p的结果。这里面要用到快速幂取模算法，幸运的是 SageMath 里面内置了。这里的素数$p = 2341$，它有很多本原根，这里取得是7。

程序截图



过程分析：

Diffie-Hellman 体制非常简单，核心的原理就是素数本原根的性质与离散对数的反推困难性。可以看到最后的 Key2 与 Key1 是相等的。而中间值都是可以在公共信道传输并避免被攻击者进行分析的。

六、实验体会

SageMath 的文档在国内比较少，要读官方的数论篇才能有所应用。总体来看，SageMath 在使用上还是比较方便的。

七、参考文献

1. Stallings, W., *密码编码学与网络安全：原理与实践*. 6th ed. 国外计算机科学教材系列. 2015, 北京: 机械工业出版社.