**广州大学学生实验报告**

**开课学院及实验室：**网络空间安全学院 **2023年 5 月 30日**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **学院** | 网络空间安全学院 | **年级/专业/班** | 网安211 | **姓名** |  | **学号** |  |
| **实验课程名称** | 密码技术及应用 | | | | | **成绩** |  |
| **实验项目名称** | 数字签名算法实验 | | | | | **指导**  **老师** | 李树栋 |

1. 实验目的

**（1）实现基于离散对数的盲签名方案，并举例验证盲签名过程**

设在该方案中，是一个大素数，是中的本原元，签名者 的密钥为，，公钥为。基于离散对数的盲签名方案如下:

### 签名过程

1) 接收者 Alice选择，随机选取，计算，将发送给 Bob。

2)Bob 选择一个随机数，计算，将发送给 Alice。

3)Alice 随机选取计算，

将发送给 Bob。

4)Bob 计算。将发送给 Alice。

5)Alice计算，的签名为。

上述签名过程如下图

|  |
| --- |
| 接收者Alice 签名者Bob |
| 随机选取，计算    随机数，计算    随机选取,计算      计算： |

#### 验签过程

验证是否成立。若成立，则签名有效；若不成立，则签名无效。

#### 签名验证过程的证明

由得

 .. (1)

若成立，则，

由此可得：  (2)

将(1)带入(2)得：

 .

比较 k 前面的系数和常数项，可得:



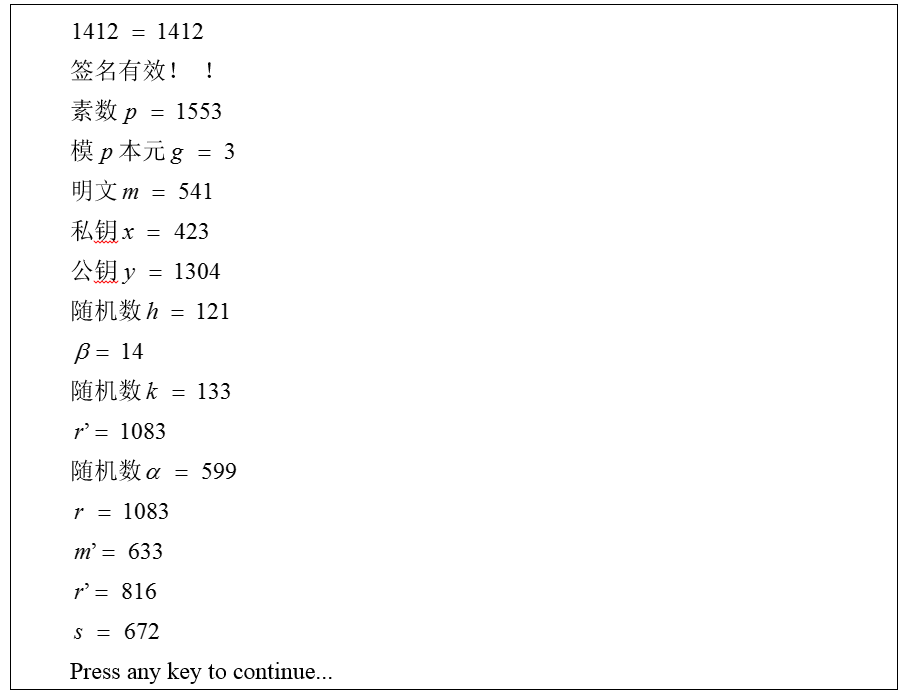


上述过程逆推，即得

1. 实验内容

（1）实现上述基于离散对数的盲签名方案

（2）举例：假设素数，模p本原根，明文，私钥。随机数，随机数，随机数。请针对该例，验证该盲签名的实验结果。



1. 实验过程及结果

3.1 同学们把你们的实验过程及结果写在下面

3.2

3.3

1. 实验总结

4.1 同学们把你们的实验过程及结果写在下面

4.2

4.3