云南大学数学与统计学院

上机实践报告

|  |  |  |
| --- | --- | --- |
| **课程名称**：信息论基础实验 | **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**：公钥密码实验 | **学号**：20151910042 | **上机实践日期**：2017-09-18 |
| **上机实践编号**：No.11 | **组号**： | **上机实践时间**：上午3、4节 |

# 一、实验目的

理解公钥密码体制

# 二、实验内容

1. RSA体制的实现与分析

2. Elgamal体制的实现与分析

3. Rabin体制的实现与分析（选做）

4. 椭圆曲线密码体制的实现与分析（选做）

要求：

（1） 实现密码体制。

（2）任取一段输入数据作为明文，计算明文熵；将密码系统作用于明文，得到密文，计算密文熵。比较明文熵和密文熵。

（3）改变明文1bit，观察密文的变化。改变密钥1bit，观察密文的变化。

（4）改变密文1bit，观察解密后的明文变化。

（5）分析（2）-（4）中的实验现象和原因。

# 三、实验平台

Windows 10 1703 Enterprise 中文版；

Python 3.6.0；

Wing IDE Professional 6.0.5-1集成开发环境。

# 四、实验记录与实验结果分析

# 五、教材翻译

# 六、实验体会

# 七、参考文献

[1] Michael T. Goodrich, Roberto Tamassia, Michael H. Goldwasser, *Data Structures and Algorithms in Python*

[2] 数据结构与算法分析：C语言描述（原书第二版），（美）维斯著；冯舜玺译. 北京：机械工业出版社

[3] 算法导论（原书第三版），（美）科尔曼（Cormen，T.H.）等；殷建平等译. 北京：机械工业出版社