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**：统计分析攻击实验 | **学号**：20151910042 | **上机实践日期**：2017-09-18 |
| **上机实践编号**：No.09 | **组号**： | **上机实践时间**：上午3、4节 |

# 一、实验目的

理解古典密码学、统计分析攻击、信息熵与密码体制的关系

# 二、实验内容

1. 古典密码体制Caesar密码的编程（参阅数据结构与算法主讲课教材的3.1.4节）；

2. 任取一段较长的且有意义的英文片段，计算其明文熵；

3. 用Caesar密码加密上述英文片段，计算其密文熵；

4. 查阅英文字母的频度分布规律，对上述密文进行统计分析攻击。

# 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