**云南大学数学与与统计学院**

**上机实践报告**

|  |  |  |
| --- | --- | --- |
| **课程名称**：信息论基础实验 | **年级**： | **上机实践成绩**： |
| **指导教师**：陆正福 | **姓名**： |  |
| **上机实践名称**：分组密码实验 | **学号**： | **上机实践日期**： |
| **上机实践编号**：No.10 | **组号**： | **上机实践时间**： |

**一、实验目的**

理解分组密码体制

**二、实验内容**

1. DES密码体制的实现与分析
2. AES密码体制的实现与分析

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、实验环境**

1. 个人计算机，任意可以完成实验的平台，如Java平台、Python语言、R语言、Matlab平台、Magma平台等。
2. 对于信息与计算科学专业的学生，建议选择Java、Python、R等平台。
3. 对于非信息与计算科学专业的学生，建议选择Matlab、Magma等平台。

**四、实验记录与实验结果分析**

（注意记录实验中遇到的问题。实验报告的评分依据之一是实验记录的细致程度、实验过程的真实性、实验结果的解释和分析。**如果涉及实验结果截屏，应选择白底黑字。**）

**五、实验体会**

**（请认真填写自己的真实体会）**

**六、参考文献**

1. Thomas M. Cover, Joy A. Thomas.   Elements of Information Theory (2nd Edition) [M]. John Wiley & Sons, Inc.

**2.（如有其它参考文献，请列出）**