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**：古典加密技术实验 | **学号**：20151910042 | **上机实践日期**：2018-05-27 |
| **上机实践编号**：No.02 | **组号**： | **上机实践时间**：08:32 |

# 一、实验目的

熟悉古典密码学的思路和方法。

# 二、实验内容

1. 编程实现古典密码学的主要体制和算法

2. 编程实现古典密码学的主要分析方法。

# 三、实验平台

Windows 10 1703 Enterprise（Edit Reports）；

*SageMath* version 8.1, Release Date: 2017-12-07；

*Ubuntu* 17.10 x86-64；

*Xshell* 5 Build 1339。

# 四、实验记录与实验结果分析

1题

在*SageMath*下，编程实现以Caesar加密为代表的古典加密方法（对字母表进行变换）。参考P.501 B.1 第2章：传统加密技术[1]。

**Solution**:

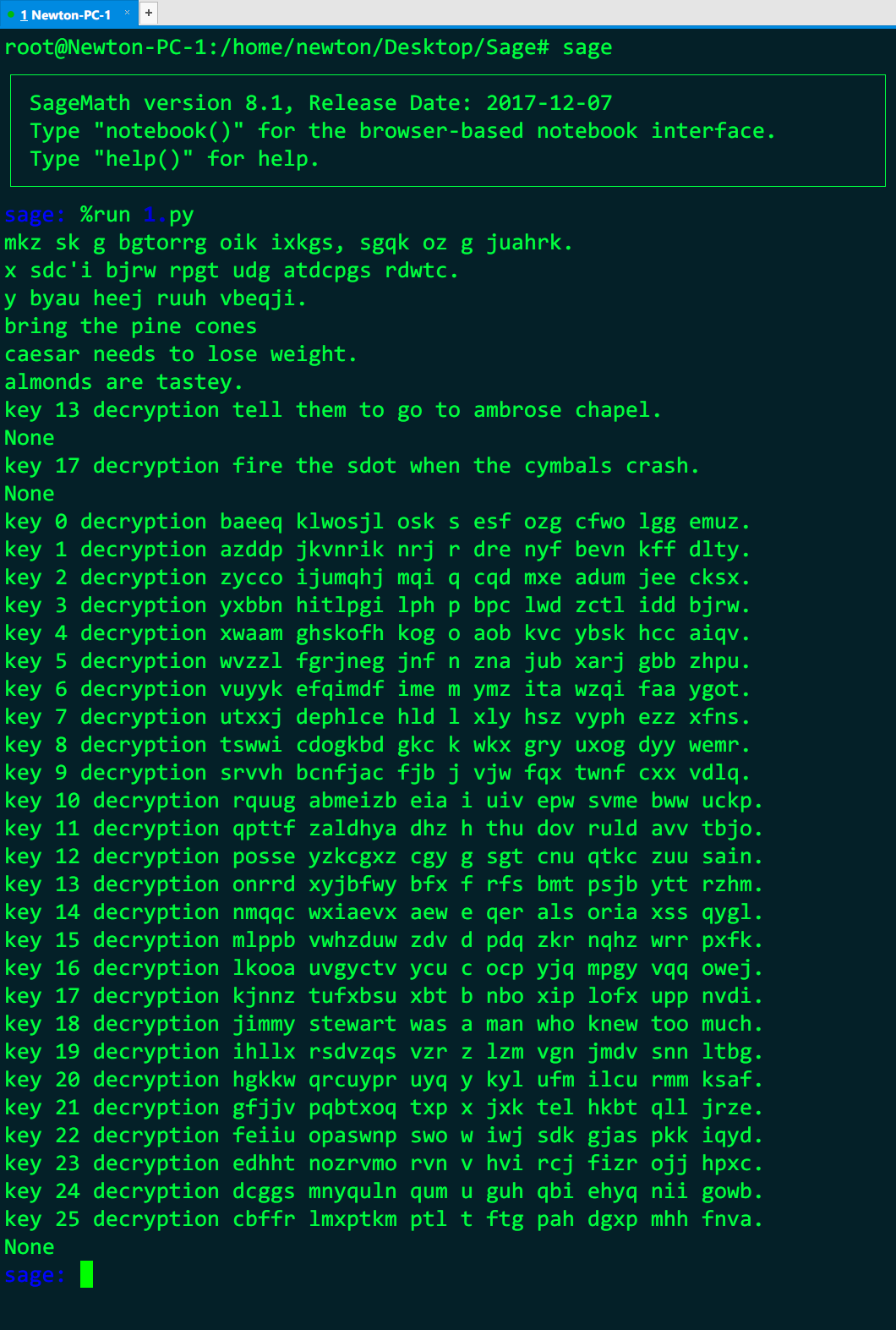
程序代码

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18 | # in the English alphabet  #  **def** num\_to\_char**(**x**):**  **return** en\_alphabet**[**x **%** 26**]**  **def** CaesarEncrypt**(**k**,** plaintext**):**  ciphertext **=** ""  **for** j **in** xrange**(**len**(**plaintext**)):**  p **=** plaintext**[**j**]**  **if** is\_alphabetic\_char**(**p**):**  x **=** **(**k **+** char\_to\_num**(**p**))** **%** 26  c **=** num\_to\_char**(**x**)**  **else:**  c **=** p  ciphertext **+=** c  **return** ciphertext  **def** CaesarDecrypt**(**k**,** ciphertext**):**  plaintext **=** "" |

|  |  |
| --- | --- |
| 19  20  21  22  23  24  25  26  27  28  29  30  31  32  33  34  35  36  37  38  39  40  41  42  43  44  45  46  47  48  49  50  51  52  53  54  55  56 | **for** j **in** xrange**(**len**(**ciphertext**)):**  c **=** ciphertext**[**j**]**  **if** is\_alphabetic\_char**(**c**):**  x **=** **(**char\_to\_num**(**c**)** **-** k**)** **%** 26  p **=** num\_to\_char**(**x**)**  **else:**  p **=** c  plaintext **+=** p  **return** plaintext  **def** BruteForceAttack**(**ciphertext**,** keyword**=None):**  **for** k **in** xrange**(**26**):**  plaintext **=** CaesarDecrypt**(**k**,** ciphertext**)**  **if(None==**keyword**)** **or** **(**keyword **in** plaintext**):**  **print** "key"**,** k**,** "decryption"**,** plaintext  **return**  """------------------have a try------------------"""  k **=** 6**;** plaintext **=** "Get me a vanilla ice cream, make it a double." **;**  **print** CaesarEncrypt**(**k**,** plaintext**)**  k **=** 15**;** plaintext **=** "I don't much care for Leonard Cohen."**;**  **print** CaesarEncrypt**(**k**,** plaintext**)**  k **=** 16**;** plaintext **=** "I like root beer floats."**;**  **print** CaesarEncrypt**(**k**,** plaintext**)**  """------------------have a try------------------"""  k **=** 12**;** ciphertext **=** "nduzs ftq buzq oazqe"**;**  **print** CaesarDecrypt**(**k**,** ciphertext**)**  k **=** 3**;** ciphertext **=** "fdhvdu qhhgv wr orvh zhljkw."**;**  **print** CaesarDecrypt**(**k**,** ciphertext**)**  k **=** 20**;** ciphertext **=** "ufgihxm uly numnys."**;** |

程序代码 1

运行结果



运行结果 1

程序分析

这几段简单的代码是用Python 2写成的。凯撒加密作为古典密码中比较典型的一种的同时，也是人类已有历史记录中最早的一个。

SageMath的运行和Python基本一致，就是在当前工作目录下存放一些文件，可以通过%run foobar.py这种语句进行运行。

# 六、实验体会

SageMath与Python 2兼容[2]，使得实验代码书写相对简单。但是在sage下没有文本编辑器，也没有IDE，调试起来相对麻烦一点，要在终端里用vi编辑器写好再调试。

# 七、参考文献

[1] STALLINGS W. 密码编码学与网络安全：原理与实践 [M]. 6th ed. 北京: 机械工业出版社, 2015.

[2] 开发组 S. Sage Tutorial [M]. Release 4.3 ed., 2010.