

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  # in the English alphabet
2  #
3  def num_to_char(x):
4      return en_alphabet[x % 26]
5
6  def CaesarEncrypt(k, plaintext):
7      ciphertext = ""
8      for j in xrange(len(plaintext)):
9          p = plaintext[j]
10         if is_alphabetic_char(p):
11             x = (k + char_to_num(p)) % 26
12             c = num_to_char(x)
13         else:
14             c = p
15         ciphertext += c
16     return ciphertext
17 def CaesarDecrypt(k, ciphertext):
18     plaintext = ""
```

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

程序代码 1

运行结果

```
1 Newton-PC-1
root@Newton-PC-1:/home/newton/Desktop/Sage# sage

SageMath version 8.1, Release Date: 2017-12-07
Type "notebook()" for the browser-based notebook interface.
Type "help()" for help.

sage: %run 1.py
mkz sk g bgtorrg oik ixkgs, sgqk oz g juahrk.
x sdc'i bjrwp rpgt udg atdcpgs rdwtc.
y byau heej ruuh vbeqji.
bring the pine cones
caesar needs to lose weight.
almonds are tasty.
key 13 decryption tell them to go to ambrose chapel.
None
key 17 decryption fire the sdot when the cymbals crash.
None
key 0 decryption baeq klwosjl osk s esf ozg cfwo lgg emuz.
key 1 decryption azddp jkvnrik nrj r dre nyf bevn kff dlty.
key 2 decryption zycco ijqmghj mqi q cqd mxe adum jee cksx.
key 3 decryption yxbbn hitlpgi lph p bpc lwd zctl idd bjrwp.
key 4 decryption xwaam ghskofh kog o aob kvc ybsk hcc aiqv.
key 5 decryption wzsl fgrjneg jnf n zna jub xarj gbb zhpu.
key 6 decryption vuyyk efqimdf ime m ymz ita wzqi faa ygot.
key 7 decryption utxxj dephlce hld l xly hsz vyph ezz xfns.
key 8 decryption tswwi cdogkdb gkc k wkx gry uxog dyy wemr.
key 9 decryption srvvh bcnfjac fjb j vjw fqx twnf cxx vdlq.
key 10 decryption rquug abmeizb eia i uiv epw svme bww uckp.
key 11 decryption qpttf zaldhya dhz h thu dov ruld avv tbjo.
key 12 decryption posse yzkcgxz cgy g sgt cnu qtkc zuu sain.
key 13 decryption onrrd xyjbfwy bfx f rfs bmt psjb ytt rzhm.
key 14 decryption nmqqc wxiaevx aew e qer als oria xss qygl.
key 15 decryption mlppb vwhzduw zdv d pdq zkr nqhz wrr pxfk.
key 16 decryption lkooa uvgyctv ycu c ocp yjq mpgy vqq owej.
key 17 decryption kjnnz tufxbsu xbt b nbo xip lofx upp nvdi.
key 18 decryption jimmy stewart was a man who knew too much.
key 19 decryption ihllx rsdvzqs vzr z lzm vgn jmdv snn ltbq.
key 20 decryption hgkkw qrcuypr uyq y kyl ufm ilcu rmm ksaf.
key 21 decryption gfjjv pqbtxoq tpx x jxk tel hkbt qlj jrze.
key 22 decryption feiiu opaswnp swo w iwj sdk gjas pkk iqyd.
key 23 decryption edhht nozrvmo rvn v hvi rcj fizr ojj hpxc.
key 24 decryption dgggs mnyquln qum u guh qbi ehyq nii gowb.
key 25 decryption cbffr lmxptkm ptl t ftg pah dexp mhh fnva.
None
sage: █
```

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.