计算机科学与技术学院计算机系统基础课程实验报告

实验题目：结合 Vigenere 密码的文件读写与大小写转换	学号：202000130198
班级： 20 级计科 4 班	姓名： 隋春雨
Email：2018640800@qq.com	

实验目的：

以读写文件为例，掌握计算机系统中程序的执行流程。

进行文件大小写转换

实验软件和硬件环境：

vmware

ubuntu

实验原理和方法：

文件读写与大小写转换

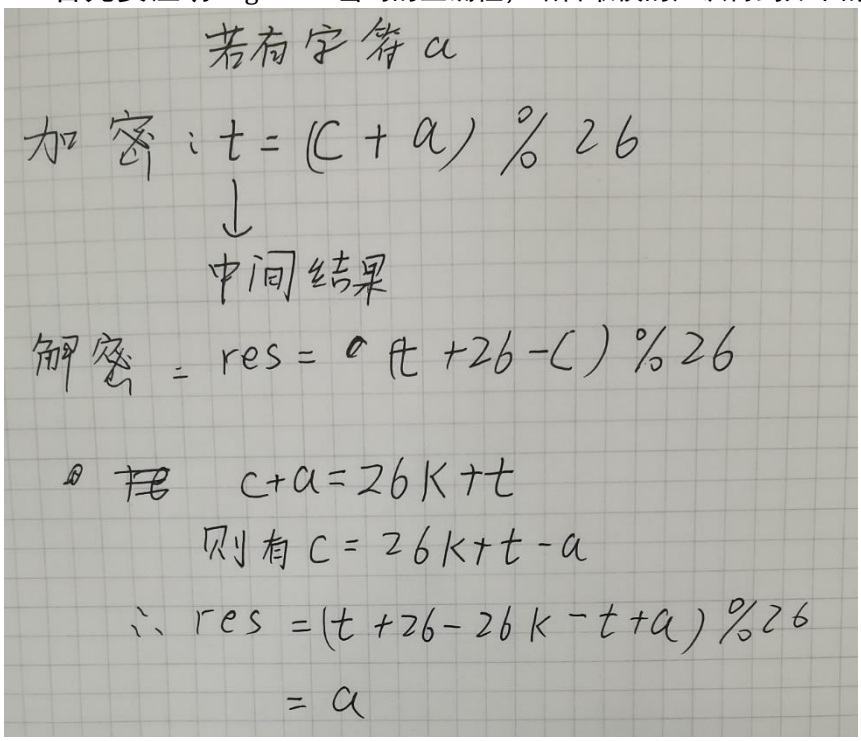
结合 Vigenere 密码建立双射映射

读写指针的使用

Linux 环境下的常见命令，比如 ls,pwd,sudo

实验步骤：

1. 首先要证明 Vigenere 密码的正确性，结合取模的知识得到如下的加解密过程



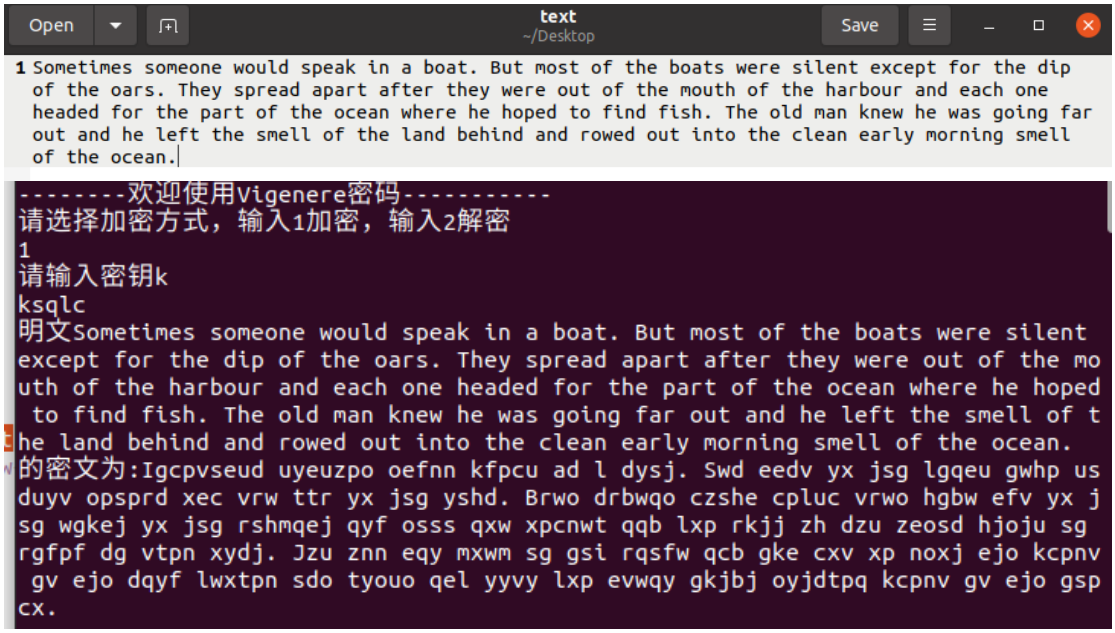
2. 打开终端，然后进入到桌面文件夹(cd Desktop)，使用 gcc 编译，值得注意的是，第一次使用 gcc 需要安装一下，没有的话，命令行会提示你。安装一下就可以了。然后用./运行
3. 输入密钥，因为我们使用的是循环密钥，所以需要输入多位密钥，然后使用

fgetc 函数从文件中读取字符并利用取模的知识进行加解密，值得注意的是，我们使用文件指针的时候，应该在 main 函数中定义，如果在全局区定义的话，会报错

```
    for(i=0;i<l;i++)
    {
        //判断大小写
        if (text[i] >= 'A' && text[i] <= 'Z'){
            if(j==m){
                j=0;   //循环密钥
                result[z]=(text[i]-'A'+k[j]-'A')%26+'A';
            } else {
                result[z]=(text[i]-'A'+k[j]-'A')%26+'A';
            }
            j++;
        } else if (text[i] >= 'a' && text[i] <= 'z'){
            if(j==m){
                j=0;   //循环密钥
                result[z]=(text[i]-'a'+k[j]-'a')%26+'a';
            } else {
                result[z]=(text[i]-'a'+k[j]-'a')%26+'a';
            }
            j++;
        } else{  //判断是否是空格
            result[z] = text[i];
        }
        fputc(result[z],fp2);
        z++;
    }
    return 0;
```

4. 文件读取的终止是 EOF 标志，但是我们又不想读取到 EOF，所以我们特判一下即可 `while ( (c=fgetc(fp1))!=EOF)`

5. 准备工作做好了，我们就可以进行文件加解密了。我们选择的是老人与海的一个片段，中间的加密过程放到了 ciphertext.txt 中，最后的结果放到了 result.txt 中



打开 ciphertext.txt，可以看到是一样的密文

exp2.c × ciphertext.txt ×

```
1 Iglppsedd oyedzjo onfhn kopwu am l xyss. Sqd endp yx ssa lgzeo gwqp osddyp opbpld xnc prw ctl
  yx ssa ysqd. Vrwx dlbwzo wzsqe wpldc prwx habw nfp yx ssa wgted yx ssa rsqmkej zyz osbs kxw
  gpwnwc qkb lgp lkjs zb dzd zyosm hdojd sa rgopz dg etjn xhdd. Jzd zhn ezy gxwv sa gsr rksff qwb
  gte wxv gp hoxs edo klphv ge edo dzyz lwgtjn smo nyodo kel hypy lgp yvwzy akjkj iyjmtjq klphv
  ge edo gbpwx.
```

解密的时候我们的代码是：

```
38 //解密
39 int decrypt(char *text,char *result,char *k,FILE *fp3)
40 {
41     int i,j=0,z=0;
42     int m = strlen(k); //获取密钥的长度
43     int l = strlen(text); //获取密文的长度
44     for(i=0;i<l;i++)
45     {
46         //判断是否是空格
47         if (text[i] >= 'A' && text[i] <= 'Z'){
48             if(j==m){
49                 j=0;   //循环密钥
50                 result[z]=(text[i]-k[j]+26)%26+'A';
51             } else {
52                 result[z]=(text[i]-k[j]+26)%26+'A';
53             }
54             j++;
55         } else if (text[i] >= 'a' && text[i] <= 'z'){
56             if(j==m){
57                 j=0;   //循环密钥
58                 result[z]=(text[i]-k[j]+26)%26+'a';
59             } else {
60                 result[z]=(text[i]-k[j]+26)%26+'a';
61             }
62             j++;
63         } else{
64             result[z] = text[i];
65         }
66         fputc(result[z],fp3);
67         z++;
68     }
69     return 0;
```

```
接下来进行解密
密文Iglppsedd oyedzjo onfhn kopwu am l xyss. Sqd endp yx ssa lgzeo gwqp osddyp
opbpld xnc prw ctl yx ssa ysqd. Vrwx dlbwzo wzsqe wpldc prwx habw nfp yx ssa wg
ted yx ssa rsqmkej zyz osbs kxw gpwnwc qkb lgp lkjs zb dzd zyosm hdojd sa rgopz
 dg etjn xhdd. Jzd zhn ezy gxwv sa gsr rksff qwb gte wxv gp hoxs edo klphv ge e
do dzyz lwgtjn smo nyodo kel hypy lgp yvwzy akjkj iyjmtjq klphv ge edo gbpwx.
的明文为:Sometimes someone would speak in a boat. But most of the boats were si
lent except for the dip of the oars. They spread apart after they were out of t
he mouth of the harbour and each one headed for the part of the ocean where he
hoped to find fish. The old man knew he was going far out and he left the smell
 of the land behind and rowed out into the clean early morning smell of the oce
an.
capsfly@ubuntu:~/Desktop$
```

打开 result.txt：

Open ▾ | result.txt ~/Desktop | Save

exp2.c × ciphertext.txt × result.txt ×

```
1 Sometimes someone would speak in a boat. But most of the boats were silent except for the dip
  of the oars. They spread apart after they were out of the mouth of the harbour and each one
  headed for the part of the ocean where he hoped to find fish. The old man knew he was going far
  out and he left the smell of the land behind and rowed out into the clean early morning smell
  of the ocean.
```

发现是相同的，文件加解密成功

6. 大小写转换：大小写转换是比较容易的，判断一下是大写还是小写就可以了

Open exp1.c ~/Desktop Save

```c
#include <stdio.h>

int main()
{
    while (1)
    {
        char c;
        scanf("%c",&c);
        if (c>='a'&&c<='z')
        {
            printf("%c\n",c+'A'-'a');
        }
        else if(c>='A'&&c<='Z')
        {
            printf("%c\n",c+'a'-'A');
        }
    }

    return 0;
}

```

同样的使用 gcc 进行编译并测试，值得注意的是，因为那是一个 while(1)循环，所以我们退出的时候需要使用 ctrl+c，这个其实我在数据库的课程设计中的学习中在部署路由器的环境中也用到了，也从侧面看到了 Linux 在实际生活中的无处不在

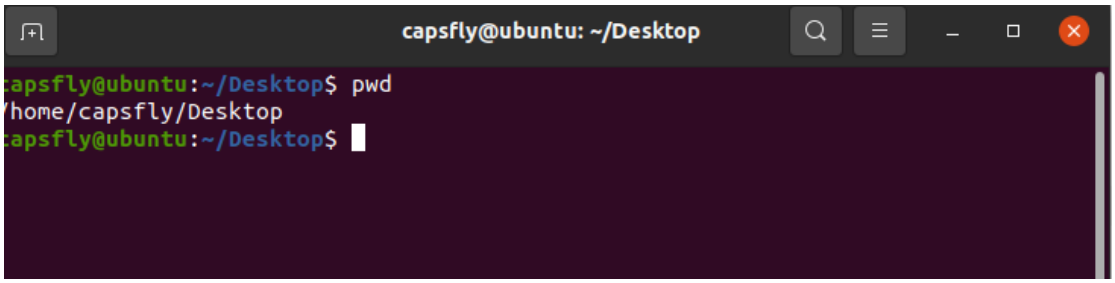
```
capsfly@ubuntu: ~/Desktop
capsfly@ubuntu:~$ cd Desktop
capsfly@ubuntu:~/Desktop$ gcc exp1.c -o exp1
capsfly@ubuntu:~/Desktop$ ./exp1
a
A
Z
z
```

结论分析与体会：

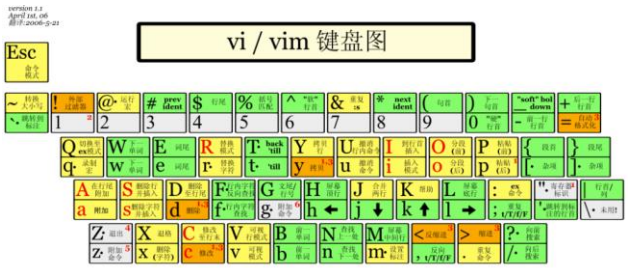
1. 学习到了取模运算的加解密操作，并如何建立一个双射映射
2. 学习到了终端/命令行的使用，我们在不同的地方打开命令行，它的作用是的，比如我们使用 ctrl+alt+t 直接打开终端，他是直接在 Home 这个文件夹下打开的，我们可以使用 ls 与 pwd 命令看一下

```
capsfly@ubuntu: ~
capsfly@ubuntu:~$ ls
bomb      Documents  Music     Pictures  PycharmProjects  Templates  Videos
Desktop   Downloads  mysite1   Public    snap             test2.c
capsfly@ubuntu:~$ pwd
/home/capsfly
capsfly@ubuntu:~$
```

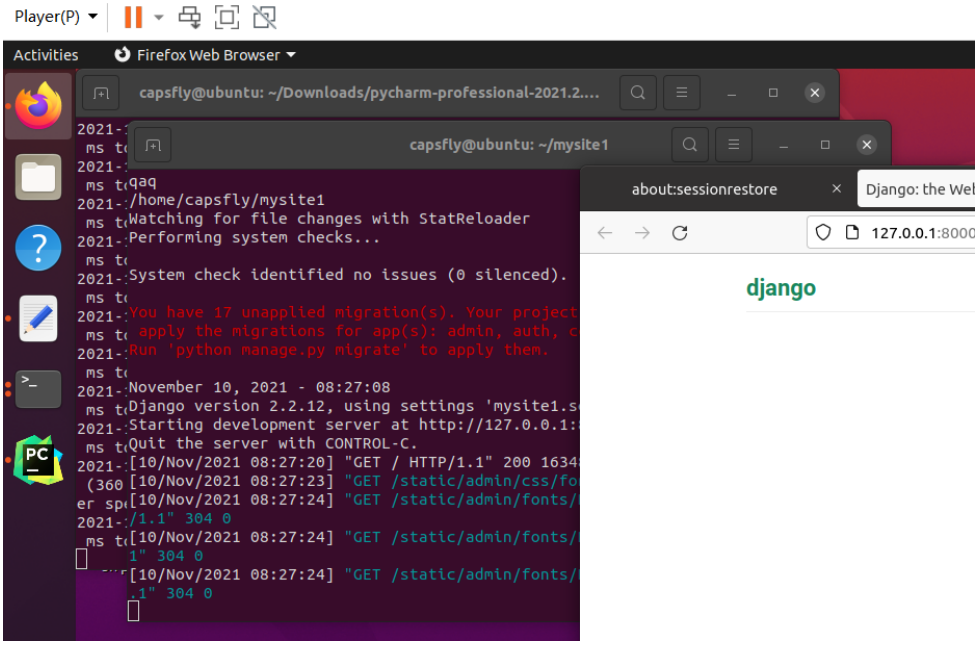
如果我们在桌面打开的话：



3. vim 是一款在 Linux 广泛使用的编辑器，他的核心就是快捷键的使用，能够将我们的双手从鼠标中解脱出来，基本上 vi/vim 共分为三种模式，分别是**命令模式（Command mode），输入模式（Insert mode）**和**底线命令模式（Last line mode）**



4. 作为计算机专业的学生一定要熟练掌握 Linux 的常用命令，因为无论是我们的学习中还是就业中，linux 都是非常重要的。比如说这次的数据库课设，无论是结合 php 还是 django 框架，都需要在 linux 环境下运行。
   昨天使用到的 Linux 下的命令搭建 django 框架的准备如下，这也说明了要把不同的知识融合到一起，虽然现在学到的还很浅，但是积累起来就会很多



其中使用到的 linux 命令如下：

```
capsfly@ubuntu:~$ ls
bomb      Documents  Music     Pictures  PycharmProjects  Templates  Videos
Desktop   Downloads  mysite1   Public    snap             test2.c
capsfly@ubuntu:~$ cd mysite1
capsfly@ubuntu:~/mysite1$ ls
db.sqlite3  manage.py  mysite1
capsfly@ubuntu:~/mysite1$ python3 manage.py runsever
qaq
/home/capsfly/mysite1
Unknown command: 'runsever'. Did you mean runserver?
Type 'manage.py help' for usage.
capsfly@ubuntu:~/mysite1$ python3 manage.py runsever
qaq
/home/capsfly/mysite1
Unknown command: 'runsever'. Did you mean runserver?
Type 'manage.py help' for usage.
capsfly@ubuntu:~/mysite1$ python3 manage.py runserver
qaq
/home/capsfly/mysite1
qaq
/home/capsfly/mysite1
```