杭州电子科技大学

实验报告

课程名称：密码学课程设计　　姓名：苏展　　学号：　18271329

实验地点：科技馆 620　　实验时间：2020-2-17

一、实验名称：　Caesar 密码实验

二、实验要求：

1、了解古典密码的几种分类。

2、掌握 Caesar 密码的加减密原理。

3、运用 MFC 或其他工具实现 Caesar 密码程序及图形化界面。

三、实验内容：

1、密码学是一门古老的学科，起源于在古代军事作战中如何隐密地传递信息的问题。从古希腊时期一直到 1949 年，都属于古典密码的发展时期。古典密码主要分为两种：替换密码和置换密码。替换密码指的是根据替换表将明文逐字母换成其他的字母来产生密文；置换密码指的是将明文中的字母重新排列来产生密文。

2、在古罗马时期，执政官凯撒(Caesar)在军事作战中使用了一种密码用于与其将军们通信，后人称其为“Caesar 密码”。它的描述相当简单，设

明文 $M = m_1 m_2 \cdots m_n$，m_i 均为英文字母，

密钥 k（也就是偏移量）是 0~26 的整数，

密文 $C = c_1 c_2 \cdots c_n$，c_i 均为英文字母。

1）加密

先将明文中每个 m_i 对应到 0~25 的整数 d_i，得到 $M' = d_1 d_2 \cdots d_n$；

再根据密钥 k 将 d_i 作偏移，得到

$$d_i' = d_i + k \bmod 26,$$

记为 $C' = d_1' d_2' \cdots d_n'$，$d_i'$ 仍然是 0~25 的整数；

最后将 d_i' 对应回英文字母 c_i，得到密文 $C = c_1 c_2 \cdots c_n$。

2）解密

类似于加密，只需要把密钥换成是 *26-k*，就能将密文解密成明文。

3）示例

明文为 *attacknow*，密钥为 *18*，加密时将每个字母用相隔 18 个位置后的字母

替换，得到密文为 *sllsucfgo*；

再取密钥为 *26-18=8*，用于解密密文 *sllsucfgo*，得到明文 *attacknow*。

3、使用 Microsoft 的 Visual Studio 编写 MFC 程序，实现 Caesar 密码程序及图形化界面，参考如下：

主要步骤：

1) 新建一个基于对话框的 MFC 工程

2) 创建明文、密钥、密文编辑框，加密/解密等按钮

3) 编写“加密/解密”事件程序

提示点：

1) 建立 MFC 工程时不要选择 Unicode 字符集

2) GetDlgItemText、SetDlgItemText 两个函数用于获取与写入编辑框中文本

3) 可能会用到 CString, char*, int 之间的相互转化

4) ‘a’~’z’的 ASCII 码值分别是 97~122

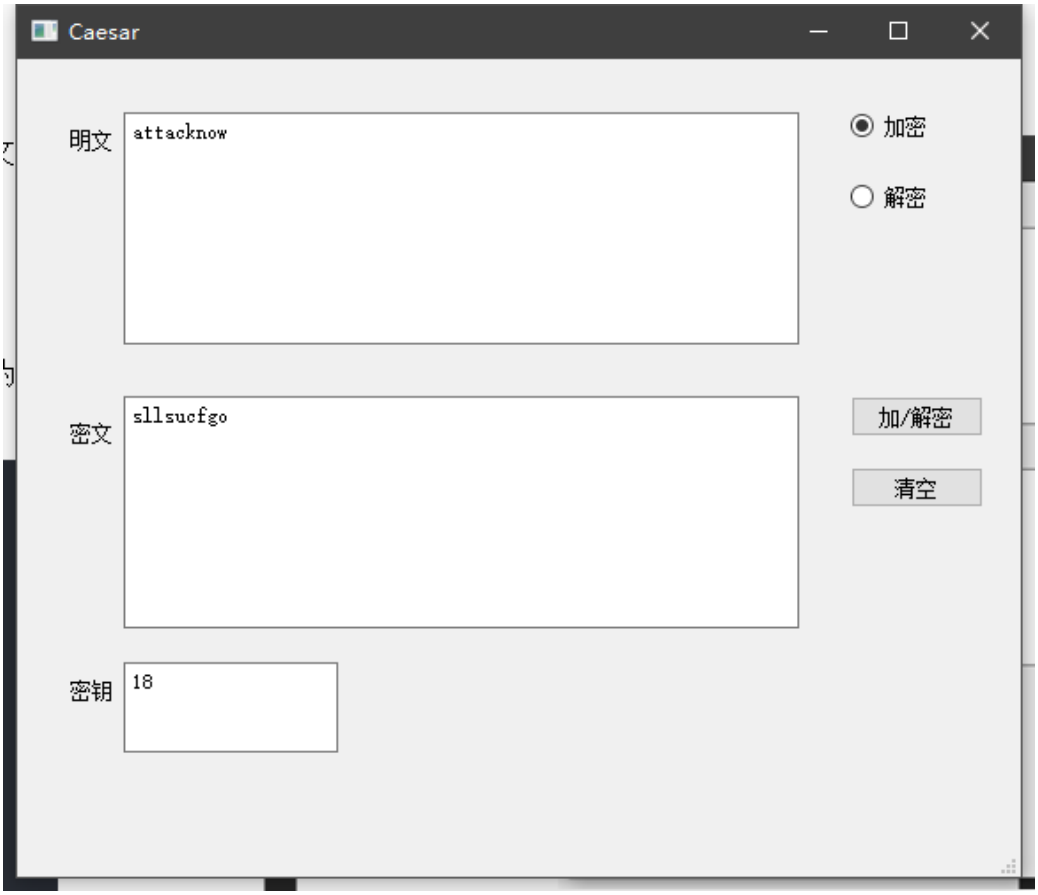
测试示例：明文 *attacknow*，加密密钥为 *18*，密文 *sllsucfgo*，解密密钥为 8。

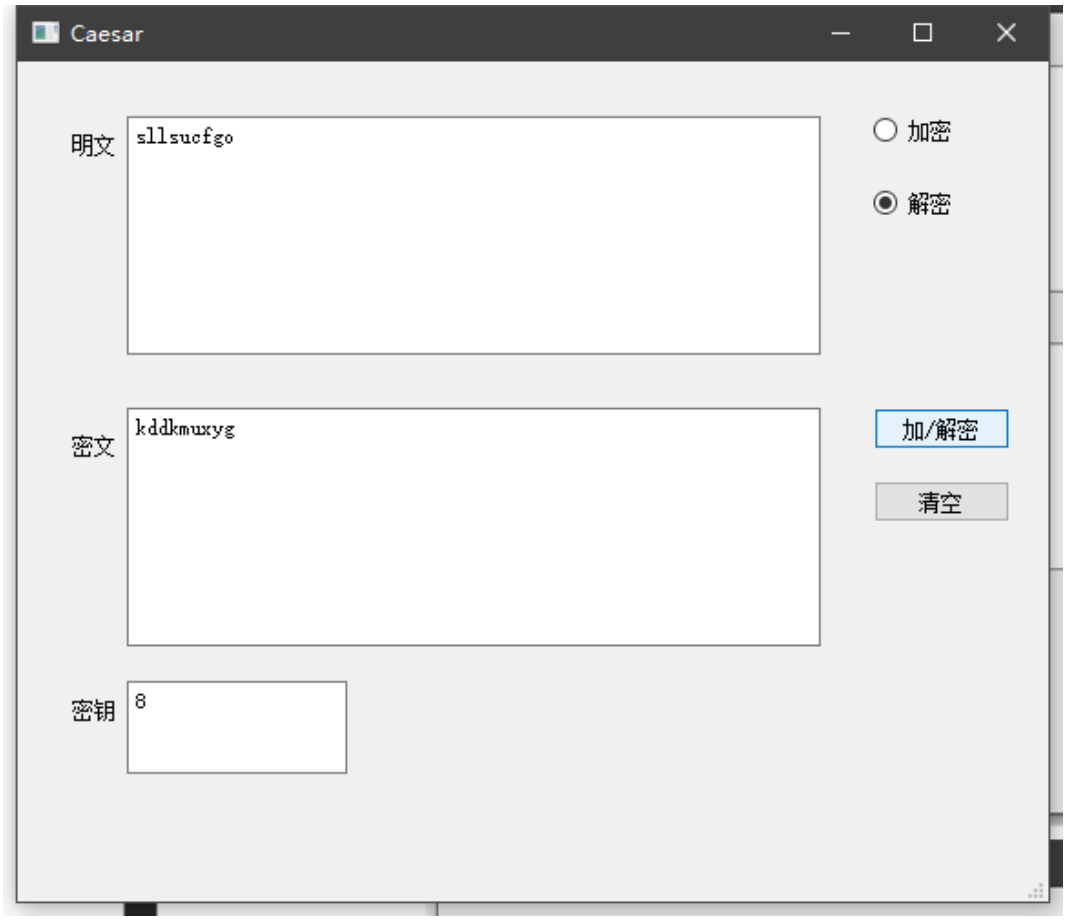
“加密/解密”事件程序代码如下：

```
def func(self):
    key=0
    message=list(self.mw.toPlainText())
    cipher=message

    if self.jm.isChecked():
        key=int(self.my.toPlainText())
    elif self.jm2.isChecked():
        key=26-int(self.my.toPlainText())
    for i in range(len(message)):
        if ord(message[i]) + key > 122:
            cipher[i] = chr(ord(message[i]) - 26 + key)
        else:
            cipher[i] = chr(ord(message[i]) + key)
    self.mw2.setPlainText(''.join(cipher))
```

测试结果截屏如下：


Caesar
明文
attacknow
加密
解密
密文
sllsucfgo
加/解密
清空
密钥
18


Caesar
明文
sllsucfgo
加密
解密
密文
kddkmuxyg
加/解密
清空
密钥
8