

**学 生 实 验 报 告**

**（理工类）**



课程名称： 密码学实验 专业班级：22网络空间安全

学生学号： 2218000121 学生姓名： 陈宣儒

所属院部：网络安全学院 指导教师： 黄丹丹

**2023 ——2024 学年 第 1 学期**

金陵科技学院教务处制

**实验报告书写要求**

实验报告原则上要求学生手写，要求书写工整。若因课程特点需打印的，要遵照以下字体、字号、间距等的具体要求。纸张一律采用A4的纸张。

格式要求：全文大标题为黑体，四号，1.5倍行距。

**实验报告书写说明**

实验报告中一至四项内容为必填项，包括实验目的和要求；实验仪器和设备；实验内容与过程；实验结果与分析；填写注意事项

（1）细致观察，及时、准确、如实记录。

（2）准确说明，层次清晰。

（3）尽量采用专用术语来说明事物。

（4）外文、符号、公式要准确，应使用统一规定的名词和符号。

（5）应独立完成实验报告的书写，严禁抄袭、复印，一经发现，以零分论处。

**实验报告批改说明**

实验报告的批改要及时、认真、仔细，一律用红色笔批改。实验报告的批改成绩采用百分制，具体评分标准由各院部自行制定。

**实验成绩评价及分析**

实验成绩表中实验项目名称、学时与实验大纲、实验计划表中信息保持一致；实验课结束后学生对该门实验课就自身能力产出展开评价；任课教师结合该课对应的能力要求、毕业指标给予评语。

**实验报告装订要求**

实验批改完毕后，任课老师将每门课程的每个实验项目的实验报告以自然班为单位、按学号升序排列，装订成册。

实验项目名称：Caesar密码 实验学时： 2

同组学生姓名： 无 实验地点： 4号科技楼1204

实验日期： 2023.9.6 实验成绩：

批改教师： 黄丹丹 批改时间： 2022.9.8

实验1 Caesar密码

一、基于OBE模式的实验目的和要求

1、了解古典密码的几种分类。

2、掌握Caesar密码的加解密原理。

3、利用编写的Caesar密码程序破译简单的Caesar挑战密文。

二、实验仪器和设备

Visual C/C++

三、实验过程

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：代换密码和置换密码。代换密码指的是根据代换表或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”。它是一种移位密码，描述相当简单，设

**明文**均为英文字母，

**密钥*k***（也就是偏移量）是0~25的整数，

**密文**，均为英文字母。

**1）加密**

先将明文中每个对应到0~25的整数，得到；

再根据密钥*k*将作偏移，得到

，

记为，仍然是0~25的整数；

最后将对应回英文字母，得到密文。

**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。*

提示点：

1）可能会用到char\*, int, CString之间的相互转化

2）‘a’~’z’的ASCII码值分别是97~122，‘A’~’Z’的ASCII码值分别是65~90

3、程序代码：

#include **<**stdio**.**h**>  
void** encryption**(){**    **int** key**;**    printf**("请输入密钥：");**    scanf**("%d",&**key**);**    getchar**();**    **char** word**[**100**];**    **char** passwd**[**100**];**    **for(int** i**=**0**;**i**<**100**;**i**++){**        word**[**i**]=**'\0'**;**        passwd**[**i**]=**'\0'**;**    **}**    **int** num**=**0**;**    **char** a**;**    printf**("请输入明文：");**    **while((**a**=**getchar**())!=**'\n'**){**        word**[**num**]=**a**;***//保存明文*        **if(**word**[**num**]<=**'z'**&&**word**[**num**]>=**'a'**){***//凯撒密码只转换字母*            passwd**[**num**]=**'a'**+(**a**+**key**-**'a'**+**26**)%**26**;**        **}else** **if(**word**[**num**]<=**'Z'**&&**word**[**num**]>=**'A'**){**            passwd**[**num**]=**'A'**+(**a**+**key**-**'A'**+**26**)%**26**;**        **}else{**            passwd**[**num**]=**word**[**num**];**        **}**      
        num**++;**    **}**      
    printf**("加密后的文本：%s**\n**",**passwd**);**    printf**("**\n**");  
}  
  
void** decryption**(){**    **char** word**[**100**];**    **char** passwd**[**100**];**    **for(int** i**=**0**;**i**<**30**;**i**++){**        word**[**i**]=**'\0'**;**        passwd**[**i**]=**'\0'**;**    **}**    **int** num**=**0**;**    printf**("请输入密文：");**    **char** a**;**    getchar**();**    **while((**a**=**getchar**())!=**'\n'**){**        passwd**[**num**]=**a**;**        num**++;**    **}**    num**=**0**;**    **for(int** i**=**1**;**i**<**26**;**i**++){**        **while(**passwd**[**num**]!=**'\0'**){**            **if(**passwd**[**num**]<=**'z'**&&**passwd**[**num**]>=**'a'**){**                word**[**num**]=**'a'**+(**passwd**[**num**]+**i**-**'a'**+**26**)%**26**;**            **}else** **if(**passwd**[**num**]<=**'Z'**&&**passwd**[**num**]>=**'A'**){**                word**[**num**]=**'A'**+(**passwd**[**num**]+**i**-**'A'**+**26**)%**26**;**            **}else{**                word**[**num**]=**passwd**[**num**];**            **}**      
            num**++;**        **}**        printf**("第%d次解密文本：%s**\n**",**i**,**word**);**        num**=**0**;**    **}**    printf**("**\n**");  
}  
int** main**()  
{**    **int** x**;**    printf**("凯撒密码**\n**加密请输入数字1**\n**解密请输入数字2**\n**退出请输入数字3**\n**");**    scanf**("%d",&**x**);**    **while(**x**!=**3**){**        **if(**x**==**1**){**            encryption**();***//加密*        **}else{**            decryption**();***//解密*        **}**        printf**("凯撒密码**\n**加密请输入数字1**\n**解密请输入数字2**\n**退出请输入数字3**\n**");**        scanf**("%d",&**x**);**    **}**      
    **return** 0**;** **}** 四、实验结果与分析

Caesar挑战密文为 ESTD TD XJ DPNCPE XPDDLRP，

解密后所得到的明文为 THIS IS MY SECRET MESSAGE， 密钥为 15 。

测试结果截图与分析如下：

图片包含 文本

描述已自动生成

图片包含 日历

描述已自动生成

五、基于OBE模式的学生自我评价与体会

（该实验对自身分析、设计、思辨、创新等个人综合能力与素质的影响）

凯撒密码的理论很简单，就是对字母进行转换，但是实操去写代码时发现了很多问题。首先就是凯撒密码只对字母进行转换，对于数字、空格等字符都是不需要操作的。其次就是凯撒密码时把字母转换成字母，需要mod26来保证在字母的范围里。做实验时注意看文档，以为凯撒密码规则和课本上的一样，加解密密钥是一样的。但是文档里给的示例明确说了，解密密钥是26-key，导致在课上只做出了11这个密钥，如果按照示例里密钥就是15。修改代码后能够成功实现预期结果了。