**2020-2021第二学期**

**网络工程专业2018级**

**《算法数据与分析》课程设计**

**班级：网络工程**

**学号：181124039**

**姓名：张怀周**

**凯撒密码**

1. **问题描述**

凯撒密码：凯撒密码是最早的加密技术，其所涉及替换情报中的每一个字母，用在字母表中继该字母固定数目后的字母进行替换。因此，在情报中，我们可以把每个 A 都用 D 替换，每个 B 都用 E 替换，每个 C 都用 F 替换，等等，即移动三个字母。以此类推，直到用 Z替换 W。之后，我们将此替换模式循环，即将 X 用 A 替换，Y 用 B 替换，Z 用 C 替换。为情报执行凯撒加密法编写程序，其中包括大小写字符。

要求：

（1） 运用所学设计至少一种算法，并给出运行结果；

（2） 对所设计算法的时空效率进行分析；

（3） 写出你的心得与体会；

1. **算法分析**

通过把字母移动一定的位数来实现加密和解密，经过归纳推导可以得出凯撒密码的加密公式为：f(a)=(a+3)mod26，然后再转换成算法的代码形式来实现。

1. **算法描述**

f(a)=(a+3)mod26

for(int i=0; i<strlen(Str); i++)

{

if(Str[i] >= 'A' && Str[i] <= 'Z')

{

Str[i] = ((Str[i]-'A')+num)%26+'A';

}

else if(Str[i] >= 'a' && Str[i] <= 'z')

{

Str[i] = ((Str[i]-'a')+num)%26+'a';

}

}

cout<<"加密后为："<<Str<<endl;

}

1. **算法实现**

#include<iostream>

#include <string.h>

#define N 100

using namespace std;

//加密函数

void Encrypt(char \*Str,int num)

{//明文串 秘钥 功能模式

for(int i=0; i<strlen(Str); i++)

{

if(Str[i] >= 'A' && Str[i] <= 'Z')

{

Str[i] = ((Str[i]-'A')+num)%26+'A';

}

else if(Str[i] >= 'a' && Str[i] <= 'z')

{

Str[i] = ((Str[i]-'a')+num)%26+'a';

}

}

cout<<"加密后为："<<Str<<endl;

}

//解密函数

void Decrypt(char \*Str,int num)

{

int x;

x=26-num;

for(int i=0; i<strlen(Str); i++)

{

if(Str[i] >= 'A' && Str[i] <= 'Z')

{

Str[i] = ((Str[i]-'A')+x)%26+'A';

}

else if(Str[i] >= 'a' && Str[i] <= 'z')

{

Str[i] = ((Str[i]-'a')+x)%26+'a';

}

}

cout<<"解密完成："<<Str<<endl;

}

int main()

{

char str[N];

int num;

int S;

cout<<"请选择加密或解密："<<endl;

cout<<"1.加密" <<endl;

cout<<"2.解密" <<endl;

cin>>S;

if(S==1){

cout<<"输入要加密的字符串:";

cin>>str;

cout<<"输入该密码算法的偏移数量：";

cin>>num;

Encrypt(str,num);

cout<<endl;

}

else if(S==2){

cout<<"输入要解密的字符串:";

cin>>str;

cout<<"输入原密码算法的偏移数量：";

cin>>num;

Decrypt(str,num);

cout<<endl;

}

else{

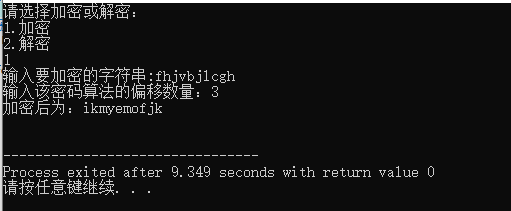
cout<<"输入错误："<<endl;

}

return 0;

}

5.**测试样例**



**6.时空分析**

空间效率：将字符串存放在数组str[n]中，该算法所占用的空间主要是字符串中的字符。

时间效率：算法执行时间可近似等于输入字符串的长度，即为O(n)。

7.**个人心得体会**

关键是实现字符替换的循环模式，通过取余的方法可以实现字符替换的循环，在求解过程中将明文中的字母转换为字int型，再将数值转化为字母形式，这样才能得出的正确的答案。