密码设计及分析报告

一、 密码算法设计思想

将凯撒密码、维吉尼亚密码以及仿射密码结合起来，先后经历三次加密，扩大密钥空间，难以解密。

二、 密码算法实现

1. 凯撒密码

即对明文字母在模 26 域内右移三位得到密文。

```
#include<stdio.h>
#include<string.h>
#include<stdlib.h>
//凯撒密码加密
char* kaisa(char* mingw)
{
    char* miw=(char*)malloc(sizeof(char)*1000);
    int i;

    //进行凯撒密码处理
    for(i=0;i<strlen(mingw);i++)
    {
        if(mingw[i]>='A'&&mingw[i]<='Z')
            miw[i]=(mingw[i]-'A'+3)%26+'A';
        else if(mingw[i]>='a'&&mingw[i]<='z')
            miw[i]=(mingw[i]-'a'+3)%26+'a';
        else;
    }
    miw[i]=0;

    return miw;
}
```

2. 维吉尼亚密码

输入密钥长度 m 以及密钥，对明文以 m 为单位分组，每组明文字母与对应密钥在模 26 的域内相加得到密文。

```c
#include<stdio.h>
#include<string.h>
#include<stdlib.h>
//弗吉尼亚密码加密
char* virginia(char* mingw,int m,int *vkey)
{
    char* miw=(char*)malloc(sizeof(char)*1000);
    int i,j=0;

    //弗吉尼亚密码处理,以m长度为单位, 对应相加
    for(i=0;i<strlen(mingw);i++)
    {
        if(mingw[i]>='A'&&mingw[i]<='Z')
            miw[i]=(mingw[i]-'A'+vkey[j++])%26+'A';
        else if(mingw[i]>='a'&&mingw[i]<='z')
            miw[i]=(mingw[i]-'a'+vkey[j++])%26+'a';
        else;
        if(j==m)
            j=0;
    }
    miw[i]=0;

    return miw;
}
```

3. 仿射密码

输入加密参数 a，b，对每一个明文字母 x 在模 26 域内进行 y=a*x+b 运算得到密文 y。

```c
#include<stdio.h>
#include<string.h>
#include<stdlib.h>
//仿射密码加密
char* fangshe(char* mingw,int a,int b)
{
    char* miw=(char*)malloc(sizeof(char)*1000);
    int i;

    //进行仿射密码(ax+b,a=5,b=4)处理
    for(i=0;i<strlen(mingw);i++)
    {
        if(mingw[i]>='A'&&mingw[i]<='Z')
            miw[i]=(a*(mingw[i]-'A')+b)%26+'A';
        else if(mingw[i]>='a'&&mingw[i]<='z')
            miw[i]=(a*(mingw[i]-'a')+b)%26+'a';
        else;
    }
    miw[i]=0;

    return miw;
}
```

三、 解密算法实现

解密顺序与加密顺序相反。

1. 仿射密码解密

对密文字母 y 先减 b，再不断加 26，直到找到一个数 x 使得 y=a*x，则 x 即为明文字母对应的数字。

```
#include<stdio.h>
#include<string.h>
#include<stdlib.h>
//仿射密码解密
char* dfangshe(char* miw,int a,int b)
{
    char* mingw=(char*)malloc(sizeof(char)*1000);
    int i,n;

    //进行仿射密码解密处理，先减去b，再不断加26，直到找到一个数与a相乘与其相等
    for(i=0;i<strlen(miw);i++)
    {
        if(miw[i]>='A'&&miw[i]<='Z')
            n=miw[i]-'A'-b;
        else if(miw[i]>='a'&&miw[i]<='z')
            n=miw[i]-'a'-b;
        else;
        while(n%a)
            n+=26;
        n=n/a;//得到明文x对应的数字

        if(miw[i]>='A'&&miw[i]<='Z')
            mingw[i]='A'+n;
        else if(miw[i]>='a'&&miw[i]<='z')
            mingw[i]='a'+n;
        else;
    }
    mingw[i]=0;

    return mingw;
}
```

2. 维吉尼亚密码解密

以 m 为单位分组，每组密文在模 26 域内减去对应密钥再加 26（保证得到的数是非负数），即可得到明文。

```c
#include<stdio.h>
#include<string.h>
#include<stdlib.h>
//弗吉尼亚密码解密
char* dvirginia(char* miw,int m,int *vkey)
{
    char* mingw=(char*)malloc(sizeof(char)*1000);
    int i,j=0;

    //弗吉尼亚密码解密处理,以m长度为单位, 对应相减
    for(i=0;i<strlen(miw);i++)
    {
        if(miw[i]>='A'&&miw[i]<='Z')
            mingw[i]=(miw[i]-'A'-vkey[j++]+26)%26+'A';
        else if(miw[i]>='a'&&miw[i]<='z')
            mingw[i]=(miw[i]-'a'-vkey[j++]+26)%26+'a';
        else;
        if(j==m)
            j=0;
    }
    mingw[i]=0;

    return mingw;
}
```

3. **凯撒密码解密**

在模 26 域内密文每个字母左移 3 再加 26（保证为非负数）。

```c
#include<stdio.h>
#include<string.h>
#include<stdlib.h>
//凯撒密码解密
char* dkaisa(char* miw)
{
    char* mingw=(char*)malloc(sizeof(char)*1000);
    int i;

    //进行凯撒密码解密处理
    for(i=0;i<strlen(miw);i++)
    {
        if(miw[i]>='A'&&miw[i]<='Z')
            mingw[i]=(miw[i]-'A'-3+26)%26+'A';
        else if(miw[i]>='a'&&miw[i]<='z')
            mingw[i]=(miw[i]-'a'-3+26)%26+'a';
        else;
    }
    mingw[i]=0;

    return mingw;
}
```

四、 加解密实现截图

默认参数：

```
//选项处理
if(n==1)//默认参数：仿射密码a=5,b=4;弗吉尼亚密码密钥长度m=6,序列如下
{
    a=5;
    b=4;
    m=6;
    vkey[0]=2;
    vkey[1]=17;
    vkey[2]=6;
    vkey[3]=11;
    vkey[4]=5;
    vkey[5]=21;
}
```

开始测试：

```
D:\程序\main.exe
请输入要加密的明文(仅对字母加密):
a1bc2def3g
--------------------Menu--------------------
-----------------1.默认参数-----------------
-------------2.仅修改仿射密码参数-----------
-----------3.仅修改弗吉尼亚密码参数---------
---------------4.修改所有参数---------------
-----------------5.退出加密-----------------
----------------------------------------
1
加密过程:
处理后的明文:
abcdefg
凯撒密码第一轮加密后:
defghij
弗吉尼亚密码第二轮加密后:
fvlrmdl
仿射密码第三轮加密后:
dfhlmth
解密过程:
处理后的密文:
dfhlmth
仿射密码第一轮解密后:
fvlrmdl
弗吉尼亚密码第二轮解密后:
defghij
凯撒密码第三轮解密后:
abcdefg
汇总输出:
明文:
a1bc2def3g
密钥:
第一层: 凯撒密码, 移位参数为3
第二层: 弗吉尼亚密码, 密钥长度为6, 密钥为2 17 6 11 5 21
第三层: 仿射密码, 加密参数为a=5,b=4
密文:
d1fh2lmt3h
解密后的明文:
a1bc2def3g

--------------------------------
Process exited after 14.74 seconds with return value 0
请按任意键继续. . .
```

五、 差分分析

由于设计的加密算法是基于古典密码的设计，没有包含类似于 DES 中的 S 盒，因此无法使用差分分析。