密码学加解密

实 验 报 告

实验名称 密码学加解密

班　　级 信安 20-2

姓　　名 李天昊

学　　号 20101110201

指导教师 徐　刚

2020 年 11 月 18 日

实验二 密码学加解密

一、实验目的

1. 通过实验,使学生对密码学有一定的感性认识;学会正确使用CAP (Cryptographic Analysis Program v4)软件，验证课堂中所学的古典密码算法；为学习现代密码算法及其应用奠定基础。

2. 用C\C++语言实现凯撒密码加/解密算法;

二、实验环境

DEVICE NAME : Thinkpad T480s

PROCESSOR : Intel(R) Core(TM) i7-8650U CPU @ 1.90GHz 2.11 GHz

SYSTEM TYPE : 64-bit operating system,x64-based processor

SYSTEM EDITION : Windows 10 Professional

VERSION : 2004

OS BUILD : 19041.572

SOFTS：CAP4(Cryptographic Analysis Program v4)；VSCODE

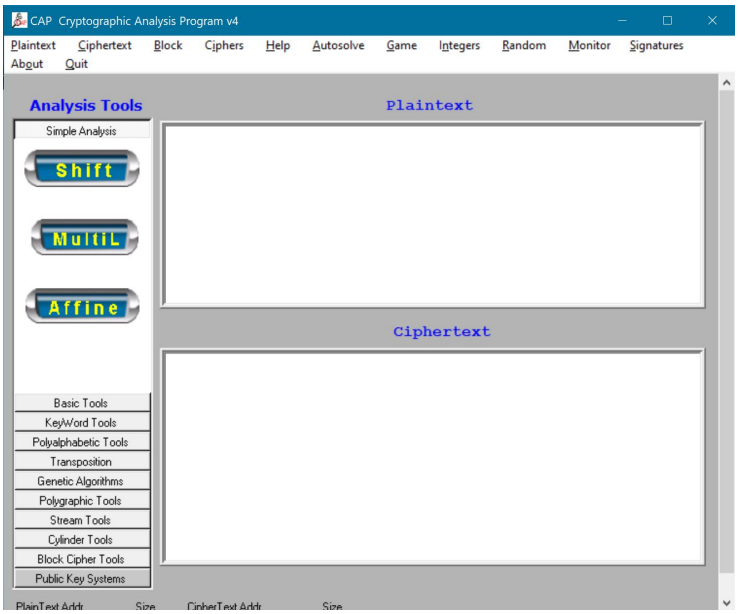
三、实验要求

1. 实验名称；
2. 实验目的；
3. 实验要求；
4. 描述实验步骤，使用加密文件给出实验结果；
5. 实验中的问题及心得。

四、实验步骤和结果

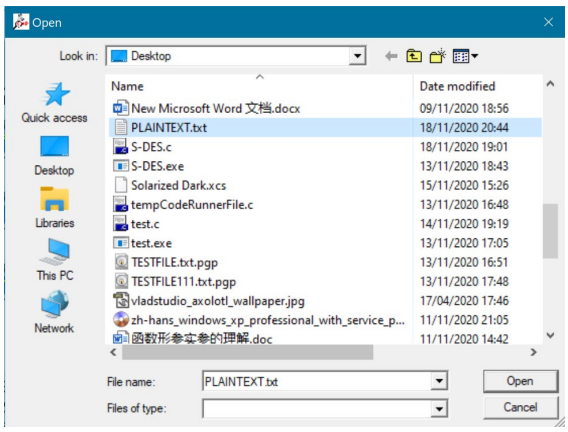
（一）CAP4软件内加解密实验

1. 打开CAP4(Cryptographic Analysis Program v4)软件

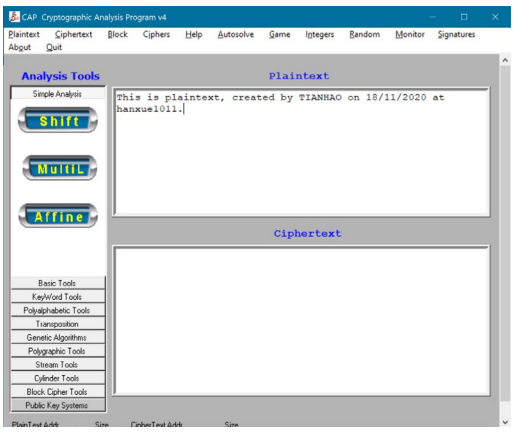


CAP4 软件界面

2. 在“plaintext”文本框键入明文或在“plaintext”任务栏选择明文文件，这里选择进行文件操作

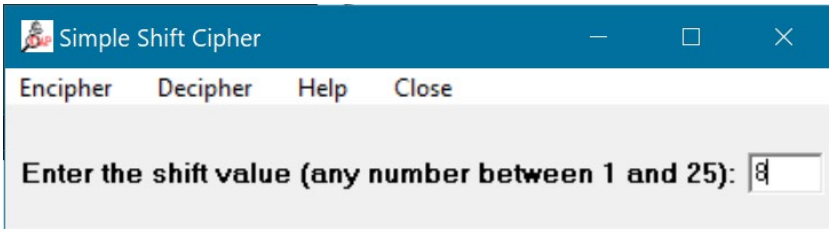


选择文件

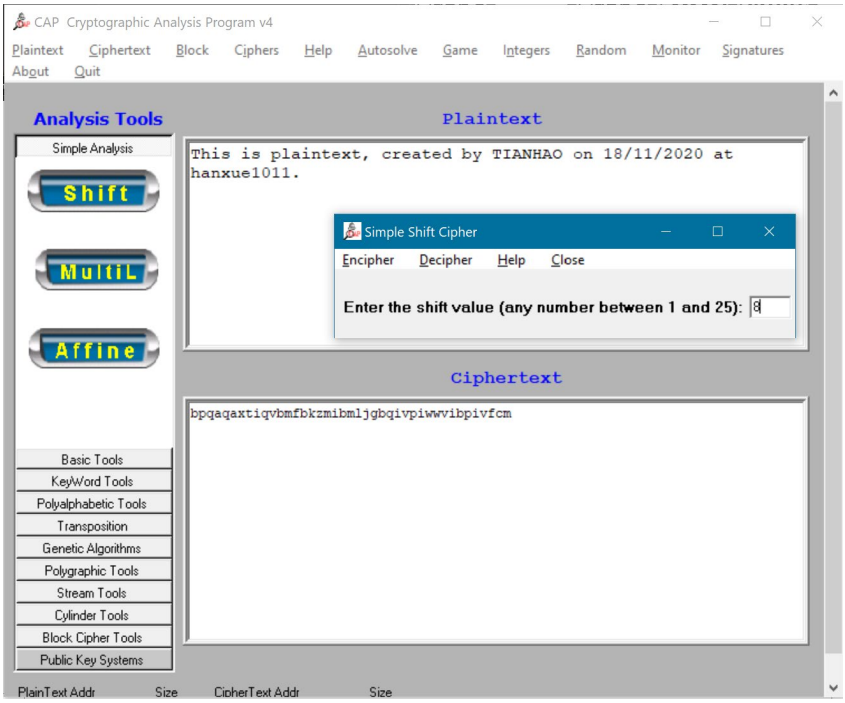


成功从文本文档读取明文

3. 在“cipher”任务栏选择加密算法并输入参数，这里选择了简单移位加密，偏移量参数选择了 8 位

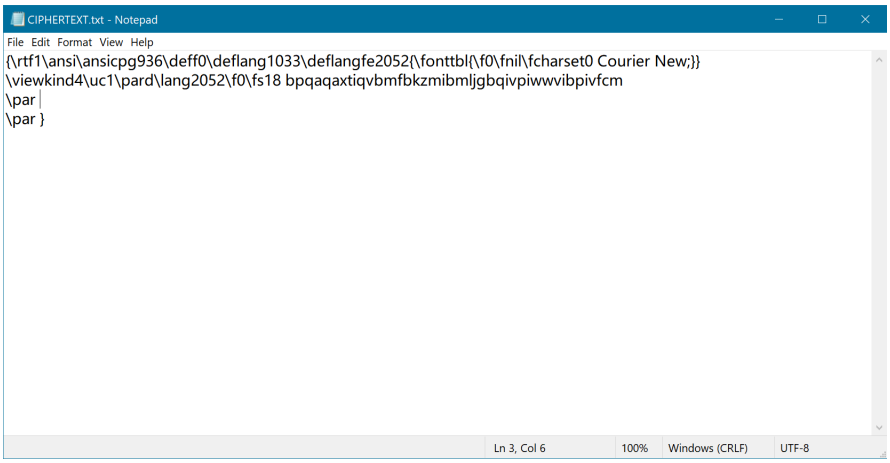


键入偏移量参数



单击按钮“Encipher”，加密成功

4. 导出密文文件至本地



包含密文的文本文档

（解密过程与上述过程类似）

（二）用 C\C++语言实现仿射变换(Affine)加/解密算法

1. 加密演示

```
问题  输出  调试控制台  终端                                                    2: Code
PS D:\#Programming\C> cd "d:\#Programming\C\" ; if ($?) { gcc Task1_CaesarCipher.c -o Task1_CaesarCipher } ; if ($?) { .\Task1_CaesarCipher }
Oh NO!!! It is 9 p.m. now, i gotta go.
1
Rk QR!!! Lw lv 9 s.p. qrz, l jrwwd jr.
PS D:\#Programming\C>
```

2. 解密演示

```
问题  输出  调试控制台  终端                                                    2: Code
PS D:\#Programming\C> cd "d:\#Programming\C\" ; if ($?) { gcc Task1_CaesarCipher.c -o Task1_CaesarCipher } ; if ($?) { .\Task1_CaesarCipher }
Rk QR!!! Lw lv 9 s.p. qrz, l jrwwd jr.
0
Oh NO!!! It is 9 p.m. now, i gotta go.
PS D:\#Programming\C>
```

3. 源代码

```
/*
 * @ Author: 李天昊
 * @ Description: 凯撒密码
 * @ Date: 20201114
 * @ E-mail: 13121515269@163.com
 */
#include<stdio.h>
#include<string.h>

int main() {

    int i;
    int len;            //长度
    int code;           //由用户输入,0 表示解密，1 表示加密
    char plaintext[100];
    char ciphertext[100];
    gets(plaintext);
    scanf("%d", &code);
    len = strlen(plaintext);

    if (code == 1) {    //加密
        for (i = 0;i < len;i++) {
            if (((plaintext[i] >= 'A') && (plaintext[i] <= 'W')) || ((plain
text[i] >= 'a') && (plaintext[i] <= 'w'))) {
                ciphertext[i] = plaintext[i] + 3;
            }
            else if (((plaintext[i] >= 'X') && (plaintext[i] <= 'Z')) || ((
plaintext[i] >= 'x') && plaintext[i] <= 'z')) {
                ciphertext[i] = plaintext[i] - 26 + 3;
            }
            else {
                ciphertext[i] = plaintext[i];       //若检测到非字母字符，则
不作移位处理
            }
        }
        for (i = 0;i < len;i++) {
            printf("%c", ciphertext[i]);
        }       //输出
    }
    else if (code == 0) {    //解密
        for (i = 0;i < len;i++) {
```

```
            if (((plaintext[i] >= 'D') && (plaintext[i] <= 'Z')) || ((plaintext[i] >= 'd') && (plaintext[i] <= 'z'))) {
                ciphertext[i] = plaintext[i] - 3;
            }
            else if (((plaintext[i] >= 'A') && (plaintext[i] <= 'C')) || ((plaintext[i] >= 'a') && plaintext[i] <= 'c')) {
                ciphertext[i] = plaintext[i] + 26 - 3;
            }
            else {
                ciphertext[i] = plaintext[i];       //若检测到非字母字符，则不作移位处理
            }
        }
        for (i = 0;i < len;i++) {
            printf("%c", ciphertext[i]);
        }       //输出
    }
    else {
        printf("Invalid Code");
    }

    return 0;

}
```

五、实验心得和思考

密码学在当今的各个领域都有着广泛地应用，无论是信息安全专业人员还是其他行业从事者都应该熟练掌握信息加密解密以及文件安全传输的要领，以较高的信息安全素养保证国家信息安全。