课堂练习3

1811494 刘旭萌

1、用简单字母置换产生的密文仍然保持明文的统计特征。为打乱密文的统计结构，可采取如下的加密方法，它是排斥加加密算法的扩展。将英语的26个字母按算许映射成为0，1，2，3，...，25，并记此映射为I，即$I(A)=0, I(B)=1, \ldots, I(Z)=25$。令X和Y为两个英文字母，令
$X+Y=I-1([I(x)+I(Y)]mod26)$

其中I^{-1}为I的反函数，即$I^{-1}(0)=A, I^{-1}(1)=B$,...,$I^{-1}(25)=Z$. 令$X=X_1X_2\ldots X_l$和$Y=Y_1Y_2\ldots Y_l$为长度相等英文字母串，令$X+Y=(X_1+Y_1)\ldots(X_l+Y_l)$

令密钥K为任意英文字母串，并记K的长度为l。（密钥K可长可短，而且同一字母可出现多次。）令明文$M=M_1M_2\ldots M_k$，这里除M_k外所有M_i均为由l个字母组成的片段，而Mk的长度m满足$0<m<=l$。令K_m为K的前m个英文字母。定义加密算法E如下:$E(K,M)=C_1C_2\ldots C_k$

其中$C_i=K+M_i, i=1,2,\ldots,k-1, C_k=K_m+M_k$

(a) 给出解密算法D

```cpp
#include <iostream>
using namespace std;
string m = "Methods of making messages unintelligible to adversaries have been necessary. Substitution is the simplest method that replaces a character in the plaintext with a fixed different character in the ciphertext. This method preserves the letter frequency in the plaintext and so one can search for the plaintext from a given ciphertext by comparing the frequency of each letter against the known common frequency in the underlying language.";
string k = "BLACKHAT";
//为了简化算法，翻译后不区分大小写
int getnum(char a) { if (a < 'a')return a - 'A'; else return a - 'a'; }
char getch(int a) { return a + 'a'; }
int main()
{
    int len = k.length();
    int lenm = m.length();
    string cipher = "";
    for (int i = 0,j=0; i < lenm; i += 1,j++)
    {
        if (j == len) j = 0;
        while (m[i] == ' ' || m[i] == '.')
        {//跳过空格和句号
            cipher += m[i];
            i++;
        }
        if (i == lenm)break;//全部翻译完毕
        cipher += getch((getnum(m[i]) + getnum(k[j])) % 26);
    }
    cout << cipher << endl;
}
```

(b) 令*K=BLACKHAT*。将下列明文翻译成密文：

Methods of making messages unintelligible to adversaries have been necessary. Substitution is the simplest method that replaces a character in the plaintext with a fixed different character in the ciphertext. This method preserves the letter frequency in the plaintext and so one can search for the plaintext from a given ciphertext by comparing the frequency of each letter against the known common frequency in the underlying language.

翻译结果：

```
nptjyks hg xamsug ffdscqls notnvoslbhtbno ao tegetchrbfd hcfl bxf
y ngmlslbcy. ueismjeuvsvn bt ehg cpmimpsv wltapo tjka rxqwaeoz a
vilrcmaek jy tjo wltjytgha wbus a hseew etfhoyegu nhcbhcmfc ip do
e vjahgbaequ. ehkc temizd rblsxsgeu doe efetgb mrxrfepmf ig use r
vhigupxv kud lp zng mhn lflrer mok use rvhigupxv pyof b rixou cbq
setdlxm cj cqwwakjyg vrl fkfbugxjy hg paer semupr cqhigte tjo rnh
xy cqwtog gceselnvz tn vrl ugeprnipnz mlniehgx.
```