课堂练习3

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, …, ***I(Z)***=25。令***X***和***Y***为两个英文字母，令

***X***+***Y*** = ***I -1***([ ***I(x)*** + ***I(Y)*** ] mod 26)

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 = ***X1X2…Xl***和Y = ***Y1Y2…Yl***为长度相等英文字母串，令

X + Y = ***(X1+Y1)…(Xl+Yl)***

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=M1M2…Mk***，这里除***Mk***外所有***Mi***均为由*l*个字母组成的片段，而***Mk***的长度***m***满足0<***m***<=***l***。令***Km***为***K***的前***m***个英文字母。定义加密算法E如下:

***E(K, M) = C1C2…Ck***

其中***Ci = K+Mi, i=1,2,…,k-1, Ck=Km+Mk***

1. 给出解密算法D
2. 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.*