Hw7 YanLiang 112889478   2018/3/7
1.
Exercise 3.16.2:
So in order to prove it is an crypto system, we just need to prove that if ciphertext1=ciphertext2, then plaintext1=plaintext2
Where ciphertext1 is the ciphertext for plaintext1 and also ciphertext2 is the ciphertext for plaintext2
Plaintext space should be string over {A,B,....Z}
Ciphertext space should be string over {A,....Z}
And the keyspace should be {0….25}*{0,...25), should be 26^2 keys.

Proof:
If ciphertext1=ciphertext2
The reverse(ciphertext1)=reverse(ciphertext2)
Then for odd index we add in -k1 and for even index we add in -k2
And after this operation we will definitely get the same text.
So it is a crytography system.

2.
Exercise 3.16.6:
The number of elements in the symbol table should be: 2^n
So the encryption function number should be (2^n)!
(seems it has to be a bijection that why it is factorial)

3.
a: 207
b: 45
c: 104
d: 82
e: 312
f: 65
g: 36
h: 110
i: 183
j: 3
k: 16
l: 107
m: 54
n: 170
o: 156
p: 68
q: 12
r: 166
s: 205

```
t: 223
u: 73
v: 20
w: 34
x: 14
y: 67
z: 2
```

```
for i in hist:
    if(i.isalpha() and (ord(i)-ord('a'))<=25):
        #print(ord(i))
        #print(i)
        hashtable[ord(i)-ord('a')]=hashtable[ord(i)-ord('a')]+1
index=0
for i in hashtable:
    print(chr(index+ord('a'))+": "+str(i))
    index=index+1
```

4.

The inverse of the problem will be 19*(c-5), since 19 or -7 is the inverse of 11 mod 16, you can find this using extended euclidean algorithms.

Ciphertext for texas should be:

```
def transcharToNum(ch):
   return ord(ch)-ord('A');

def encrypt(plaintext,coef1,coef2):
   #print("I am good")
   output="";
   for c in plaintext:
       output=output+ chr(ord('A')+(coef1*transcharToNum(c)+coef2)%26)
   return output

print(encrypt("TEXAS",11,5))
```

“GXYFV”

If “OKLAHOMA” is the cipher text then the plaintext should be:

Do this you will get

```
print(encrypt("OKLAHOMA",19,-95))
```

PRKJMPDJ