ECE404

HW05

Yudi Wu

wu533@purdue.edu

**Code**

The code should be running under python 2.7.

#!/usr/bin/python

### hw05.py

import copy

class RC4:

def \_\_init\_\_(self,keystring):

self.Tvec = []

##use key to permute statearray

self.Svec = range(256)

for i in range(256):

self.Tvec.append(ord(keystring[i % 16]))

j = 0

for i in range(256):

j = (j + self.Svec[i] + self.Tvec[i]) % 256

self.Svec[i],self.Svec[j] = self.Svec[j],self.Svec[i]

def encrypt(self,image):

i = 0

j = 0

h = 0

statearray = copy.copy(self.Svec)

listlen = len(image)

encryptedImage = []

##perform RC4 algorithm on whole file

while h < listlen:

i = (i + 1) % 256

j = (j + statearray[i]) % 256

statearray[i],statearray[j] = statearray[j],statearray[i]

k = (statearray[i] + statearray[j]) % 256

encryptedImage.append(statearray[k] ^ image[h])

h = h + 1

return encryptedImage

def decrypt(self,image):

i = 0

j = 0

h = 0

statearray = copy.copy(self.Svec)

listlen = len(image)

decryptedImage = []

##perform RC4 algorithm on whole file

while h < listlen:

i = (i + 1) % 256

j = (j + statearray[i]) % 256

statearray[i],statearray[j] = statearray[j],statearray[i]

k = (statearray[i] + statearray[j]) % 256

decryptedImage.append(statearray[k] ^ image[h])

h = h + 1

return decryptedImage

if \_\_name\_\_ == "\_\_main\_\_":

rcipher = RC4('kaklaizuobaojian')

fptr = open('winterTown.ppm','r')

##Open a ppm image, cut front 3 lines and store them into a list of individual characters

all\_lines = fptr.readlines()

fptr.close()

originalImage = []

for i in range(3,len(all\_lines)):

for j in range(len(all\_lines[i])):

originalImage.append(ord(all\_lines[i][j]))

encryptedImage = rcipher.encrypt(originalImage)

decryptedImage = rcipher.decrypt(encryptedImage)

##if output list equals to input list, RC4 works.

if originalImage == decryptedImage:

print('GOOD JOB BOY')

else:

print('DO IT AGAIN')

##Write 3 lines into the output file and then the entire decrypted image

fout = open('output.ppm','wba')

for i in range(3):

fout.write(all\_lines[i])

fout.write(bytearray(decryptedImage))

fout.close()

**Output**

yudi3160@ubuntu:/mnt/hgfs/Shared$ python hw05.py

GOOD JOB BOY

yudi3160@ubuntu:/mnt/hgfs/Shared$ diff output.ppm winterTown.ppm

yudi3160@ubuntu:/mnt/hgfs/Shared$