傳送端程式碼:

import hashlib

import binascii

from pyDes import des, CBC, PAD\_PKCS5

def des\_encrypt(secret\_key, s): #DES編碼

    iv = secret\_key #DES金鑰

    k = des(secret\_key, CBC, iv, pad=None, padmode=PAD\_PKCS5)#建立DES跟選擇mode

    en = k.encrypt(s, padmode=PAD\_PKCS5)#DES編碼

    return binascii.b2a\_hex(en)#回傳DES編碼

message = ''

chars = 'AaBbCcDdEeFfGgHhIiJjKkLlMmNnOoPpQqRrSsTtUuVvWwXxYyZz0123456789'

length = len(chars) - 1

# 隨機產生訊息

for i in range(1000):

 message += chars[random.randint(0, length)]

print("訊息:", message)

# 產生訊息檔

f = open('1000.txt', 'w')

f.write(message)

f.close()

# 統計英文大小寫以及數字各有多少

x = 0

y = 0

z = 0

for i in message:

 # 統計英文大寫

 if ord(i) >= 65 and ord(i) <= 90:

  x += 1

 # 統計英文小寫

 elif ord(i) >= 97 and ord(i) <= 122:

  y += 1

 # 統計數字

 else:

  z += 1

print("英文大寫共有:",x)

print("英文小寫共有:",y)

print("數字共有:",z)

print("共有:",x+y+z,"個字")

# 輸入檔案名稱

filename = "1000.txt"

m = hashlib.sha1()#建立sha1模型

# 讀取檔案內容，計算 SHA1 雜湊值

with open(filename, "rb") as f:

  buf = f.read()

  m.update(buf)

h = m.hexdigest()#計算訊息摘要

key=input("輸入8位加密金鑰")

password = des\_encrypt(key, h)

print("訊息摘要: "+h)

print("加密後訊息摘要: "+password.decode('utf-8'))

#存儲加密訊息摘要檔案

path = 'password.txt'

with open(path, 'w') as f:

    f.truncate()

    f.write(password.decode('utf-8'))

接收端程式碼:

import hashlib

import binascii

from pyDes import des, CBC, PAD\_PKCS5

def des\_decrypt(secret\_key, s):#DES解碼

    iv = secret\_key #DES金鑰

    k = des(secret\_key, CBC, iv, pad=None, padmode=PAD\_PKCS5)#建立DES跟選擇mode

    de = k.decrypt(binascii.a2b\_hex(s), padmode=PAD\_PKCS5)#DES解碼

    return de#回傳DES解碼

filename = "1000.txt"

m = hashlib.sha1()#建立sha1模型

# 讀取檔案內容，計算 SHA1 雜湊值

with open(filename, "rb") as f:

  buf = f.read()

  m.update(buf)

h = m.hexdigest()#計算訊息摘要

#讀取加密訊息摘要檔案

filename2 = "password.txt"

with open(filename2, "rb") as f2:

    password=f2.read()

key=input('輸入8位數解密金鑰')#輸入金鑰

de=des\_decrypt(key, password)#進行解密

print("訊息摘要: "+h)

print("解密後訊息摘要: "+de.decode('utf-8'))

if h==de.decode('utf-8'):#判斷訊息摘要是否一樣，是否被竄改

    print('訊息沒有遭竄改')

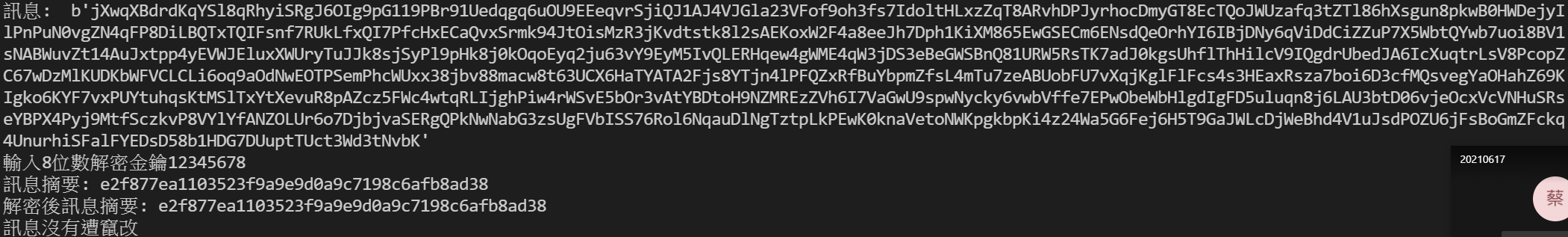
else:

    print('訊息可能遭竄改,或解密金鑰錯誤')

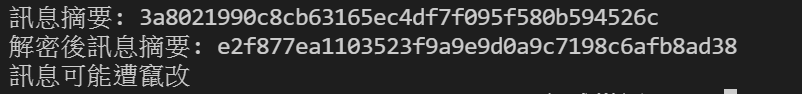
運行結果:

傳送端:

接收端:

成功:

檔案被竄改驗證失敗:

將1000.txt檔修改內容