Report

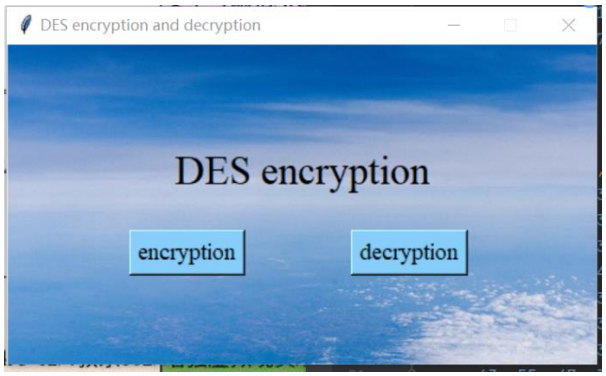
1. Key emphasis in work

1.1. The introduction of my work

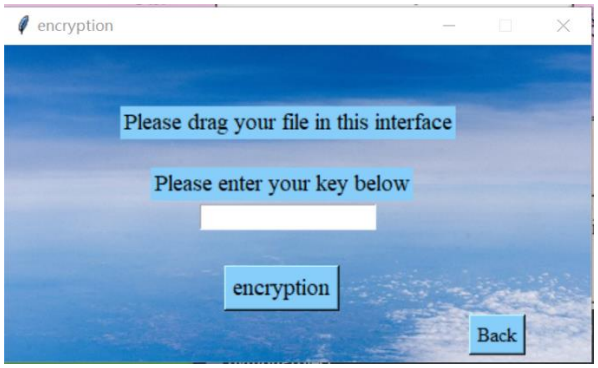
It is a desktop application of implementing DES algorithm, which can encrypt or decrypt multiple almost types of files, such as pdf, jpg, xlsx and so on. In addition, this application is developed by Python.

1.2. The instruction of my work

The first step is run the project, and open the main windows that is in the below.



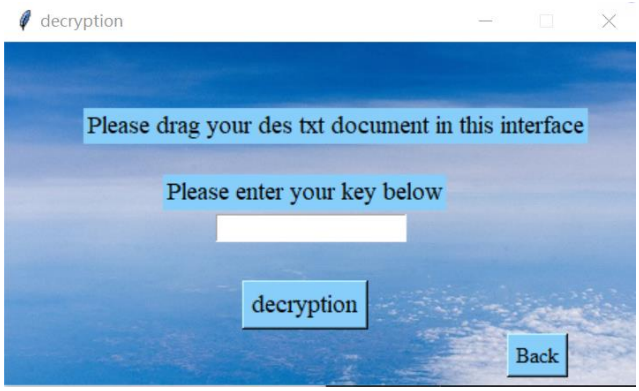
If you want to encrypt your file, please enter the encryption button. Afterwards, the following windows will be shown.



You need to drag multiple files that you want to encrypt into that interface and enter your key that is decided by yourself. When you drag files successfully, the application will tell you, and show the location of the file you upload. If you drag the wrong files, you can drag again. The new files will replace the old files. When you finish last step, you can enter encryption button to encrypt these files. If you do not drag a file, this application will tell you, and you can drag again. If you do not enter the key, this application will tell you, and you can enter it. Certainly, if your information is right, the application will tell you encrypt successfully, and come back to the main window. The encrypted file named *The des text of x.txt* are in the same folder as the program. It is worth noting that you should not change the file name.

If you want to decrypt your file, please enter back, and enter the decryption button on the main

window. The decryption window is in the following.



The process of decrypting and encrypting files is very similar. The only thing that you need to pay attention to is the name of your dragged files. This application will judge if the file is a des encrypted file according to its name in order to avoid the user drag the wrong files. Consequently, the file that you drag must be named *The des text of x.txt.* The decrypted file named *The origin text of x* are also in the same folder as the program.

1.3. The development processes

The learning of DES algorithm mainly comes from the course of professor He Jingsha, *Data Encryption Standard* and the following website, *https://blog.csdn.net/m0_37962600/article/details/79912654?utm_medium=distribute.pc_relevant.none-task-blog-2%7Edefault%7EBlogCommendFromBaidu%7Edefault-6.no_search_link&depth_1-utm_source=distribute.pc_relevant. none-task-blog-2%7Edefault%7EBlogCommendFromBaidu%7Edefault-6.no_search_link.*

Code development is divided into the following steps, developing DES algorithm, developing UI and testing.

1.4 The Python library

This application need to install the windnd, tkinter and pillow.

2. Feelings and experiences

2.1. The difficulties in developing.

After understanding the algorithm, the development of DES algorithm is not difficult, mainly involving permutation operation, Xor operation, and left shift operation. It was my first time developing the UI using tkinter and windnd in Python, and I was a little rusty, so processing background images and dragging files took a lot of time. The more difficult part is converting the binary code to and from the string. Since every string converted to binary code is eight bits, the binary code needs to be cut and added 0s. Another difficult point is reading any types of files, and convert them to binary code.

```
BoralText = ''  # initialize binary text
for c in text:  # Iterate over every letter or symbol in the source text
    l = bin(ord(c))[2:]  # Convert to binary by ASCII code
    length = len(l)  # if the length of the code is less than 8, add 0s i
    for j in range(0, 8 - length):
        l = '0' + l
    BoralText = BoralText + l
```

2.2 The interesting points in developing.

When it comes to decryption, it only needs to perform Xor calculation with Kn in reverse order because of and symmetry of the various displacement boxes and Xor calculations.