

README

B07901103 電機三 陳孟宏

1. 在main函數, 我針對"把password轉乘hash value"及"把hash value轉成password"呼叫了兩個函數, "Dictionary_File()"和"Result_PA2()"

```
# main function
def main():
    # Open password.txt
    file_name = input("Please enter the name of the password file: ")
    password_file = file_name
    f_pass = open(password_file)
    lines_pass = f_pass.readlines()
    # Create a dictionary file
    Dictionary_File(lines_pass)
    # Open list pa2.txt
    mark = 0 # if enter a file name, mark == 1
    user_hash = input("Please enter a \"hash value\" or the \"txt file name\": ")
    if ("txt" in user_hash):
        list_file = open(user_hash)
        lines_list = list_file.readlines()
        Result_PA2(lines_list)
    else:
        Result_PA2([user_hash])
    # f_pass.close()
    if (mark == 1):
        mark = 0
        list_file.close()
```

2. Dictionary_File()函數

- 把密碼轉乘ASCII

```
# String to ASCII, initialization
for line in pass_word:
    temp = ""
    if (line != '\n'):
        for i in range(len(line)):
            if (line[i] != '\n'):
                temp += str(ord(line[i]))
        ascii_password.append(temp)
# Salt hash value (e.g. str.zfill(3))
```

- 把每個ASCII加上salt代入定義的hash function

```
for line in pass_word:
    word.append(line)
for i in range(len(ascii_password)):
    for j in range(1000):
        salt = str(j).zfill(3)
        combine = salt + ascii_password[i]
        temp = word[i] + ' ' + salt + ' ' + str(hash_function(int(combine[0:8]), int(combine[8:15]))) + '\n'
        output_seq = temp
        output_line.append(output_seq)
        output_seq = ""
    find_hash.append(str(hash_function(int(combine[0:8]), int(combine[8:15]))))
    hash_map[str(hash_function(int(combine[0:8]), int(combine[8:15])))] = salt
```

```
# hash value function
def hash_function(left, right):
    h_value = (243*left + right) % 85767489
    return h_value
```

- 輸出檔案

3. Result_PA2()函數

- 用try / except去判斷, 如果hash value在dictionary中, 輸出規定格式的密碼

```

try:
    # print("val: ", val)
    # print("where: ", find_hash.index(val))
    index = find_hash.index(val)
    asci_all = output_line[index]
    asci = asci_all.split(' ', 2)[0].replace('\n', '')
    salt = asci_all.split(' ', 2)[2].replace('\n', '')
    # print("asci: ", asci)
    # print("salt: ", salt)
    # Column 2
    temp += asci
    temp += ' '
    # Column 3
    temp += hash_map[salt]
    temp += ' '
    # Column 4
    temp += str(index+1)

```

- 如果不在dictionary中, 進入except, 輸出*****

```

except:
    # hash value not in the dictionary file
    # Column 2
    temp += "*****"
    temp += ' '
    # Column 3
    temp += "***"
    temp += ' '
    # Column 4
    temp += "100000"

```