2019 Computer Network Final Project cnMessage Report

B06902017趙允祥　B06902111林慶珠　B06902047陳彥

1. User & Operator Guide

- Usage:

```
(a)帳號相關（註冊、改密碼、登入、登出）
      reg
      chg [account]
      login
      logout

(b)顯示client和其他人間的最新互動
      show

(c)寄送文字、檔案(檔案只能在對方在線時傳送)
      send text [receiver] [content]
      send file [receiver] [[content1] [content2]...]

(d)顯示和特定對象間的文件、檔案往來
      get text [person] [content]

(e)下載檔案
      get file [person] [content]

(f)離開應用程式
      exit
```

- Sample: 以bob 和 henry之間互傳text、file為例
  （藍框：bob terminal;　紅框: henry terminal）

```
>> reg
Register
Username:bob
password:
done
>> chg bob
Change Password

password:
new password:
new password confirm:
done
>> login
Login
Username:bob
password:
23a94159f45ddb590cb42bf0813414e7
```

```
>> login
Login
Username:henry
password:
ae63a3a2c1362af111ea57379b10b137
```

```
>> send text henry "I am bob"
done
>> send file henry ../../test.c
done
>> get text henry all
+--------+---------------------+----------+-----------+
| Sender |         Time        |  Status  |  Message  |
+--------+---------------------+----------+-----------+
|  out   | 2020-01-17 14:30:57 | (unread) | [file]_1. |
|  out   | 2020-01-17 14:30:07 | (unread) |  I am bob |
+--------+---------------------+----------+-----------+
>> get text henry I
+--------+---------------------+----------+----------+
| Sender |         Time        |  Status  | Message  |
+--------+---------------------+----------+----------+
|  out   | 2020-01-17 14:30:07 | (unread) | I am bob |
+--------+---------------------+----------+----------+
```

```
>> get text bob all
+--------+---------------------+----------+-----------+
| Sender |         Time        |  Status  |  Message  |
+--------+---------------------+----------+-----------+
|   in   | 2020-01-17 14:30:57 | (unread) | [file]_1. |
|   in   | 2020-01-17 14:30:07 | (unread) |  I am bob |
+--------+---------------------+----------+-----------+
>> get file bob _1.
done
```

```
>> show
+-------+--------+---------------------+----------+---------------+
|  User | Sender |         Time        |  Status  |    Message    |
+-------+--------+---------------------+----------+---------------+
| henry |  out   | 2020-01-17 14:30:57 | ( read ) | [received]_1. |
+-------+--------+---------------------+----------+---------------+
>> logout
you have logged out
>> exit
bye
```

2. Instructions on how to run server & clients

(1) server

./build_server.sh

(2) client

./build_client.sh

3. System & Program Design

- 用socket在server和client間建立聯絡通道。一開始先將server跑起來，等待client連線。當client連線成功，即可執行下列命令，底下一一說明功能及實現方式。

(1) reg

向server註冊帳號。

將命令直接送到server端，server執行create_user( )(import from account.py)，將帳號以及相關資訊(ex. encrypted password)放入user.json。而如果已經有同樣的Username存在，則輸出”account exists”。

(2) login

用已註冊的帳號登入server，並獲得一把session key。這把key在logout之前，都會拿來讓server識別user。

client端執行”login”，依照要求填入username和password後，clien.py會將它做成字串 “none login [username] [password]” 傳送到server端(第一個參數代表的是session key，因為還未登入完成，因此目前的session key為none)。server接收到訊息後會執行log_in( )(import from account.py)，在確定user.json裡有登入者的帳號，密碼也正確後，他就會分配session key，記錄在user.json的同時回傳給client。若user資訊和user.json比對失敗，則輸出”wrong account or password”。

(3) logout

session key失效，即相當於從server登出。

client端將session key清掉、設回”none”。因為server端在接收命令的時候，是以key作為辨識user身份的工具，故接下來無論client端做什麼動作，server都會因為沒有相符的key而無法執行相應動作。

(4) chg

更改密碼。

直接將命令連同session key送到server，server端執行change_password( )(import from account.py)，更改user.json，將原本的user account刪除，而後再用新密碼重新將新的user account寫入user.json。

(5) send text

向指定帳號發送文字訊息。

直接將命令連同session key送到server，server端以key、receiver、當前timestamp、text為參數執行send_text( )(import from message_send.py)。

若user.json裡能找到相對應的key、receiver，則根據sender、receiver身份，打開相對應server資料夾下的json檔，紀錄message資訊（包含 text content, direction, read="true"/"false", etc）。舉例來說，若bob 送資訊給 henry，則data/henry/bob.json中會多出一筆direction="in"的資料。

(6) send file

向指定帳號發送本地檔案。

直接將命令連同session key送到server端，server端針對各檔案做處理，向client確認本地檔案是否存在，存在則執行send_file()(import from message_send.py)。若本地檔案路徑真的存在且user.json裡能找到相對應的key、receiver，則client將檔案中內容傳送到server，server接收後將其以相同檔名儲存在相對應的server資料夾中。(ex. bob 寄 test.txt給henry，則data/bob/henry、data/henry/bob 底下都會有test.txt)，並將檔案訊息記錄為"[file]+filename"。

(7) show

顯示client和其他人間最新的互動。

直接將命令連同session key送到server端，server端呼叫show_all (import from message_get.py)。

若 user.json裡能找到相對應的key，則server會讀取相對應account的server端資料夾，列出其中所有.json檔中的最新訊息。

(8) get text

顯示client和指定帳號間的訊息、檔案往來。

直接將命令連同session key送到server，server端以key、查詢對象、查詢目標為參數執行get_text( )(import from message_get.py)。

若 user.json裡能找到相對應的key、查詢對象，則開啟相對應server資料夾下的json檔，從裡面讀取資料的同時，也更新message狀態（ex. 將direction="in"、read="False"的message，更新成read="True"）。

(9) get file

向指定對象收取指定檔案。

直接將命令連同session key送到server端，server端依序呼叫get_file( )(import from message_get.py)處理個別檔案。

若 user.json裡能找到相對應的key、檔案來源對象，且相對應的server資料夾中也有目標檔案的話，server端通知client端「傳送要求成立」，server端將server資料夾裡的內容傳送給client，client則將它存到本地。server並將檔案訊息記錄由"[file]+filename"改為"[receive]+filename"。

(10) exit

印"bye"，結束client程式。

- 我們的系統，client和server間訊息傳送皆經過加密，增加安全性。先用PKCS1_OAEP 做asymmetric 的symmetric key exchage，傳訊息用Fernet() symmetric encryption

4. Other things you want to say, if any

(1) 同時有兩個client登入同一個帳號的話，先來的會被後來的覆蓋掉

(2) 有Auto Reconnect的功能（可在離線狀態 send 資料，reconnect後會自動送出，但只限一個資料）

(3) 設計避免 Race Condition

(4) 登入時隱藏密碼
(5)可顯示message是否被讀到、file是否被下載