B08705026 陳沛妤 資管三
階段三：操作說明文件

一、程式執行環境說明
語言：C++
作業系統：Linux(Ubuntu)

二、編譯與執行
編譯：
在資料夾下 $ make

執行：
在資料夾下 $ ./server <Server port No.>
在資料夾下 $ ./client <Server IP address> <Server port No.>

三、安全傳輸實作的方法及流程說明

在每次執行時，使用指令動態產生client 及server的公鑰及私鑰
> openssl req –x509 –sha256 –nodes –days 365 –newkey rsa:2048 –keyout client.key –out client.crt
> openssl req –x509 –sha256 –nodes –days 365 –newkey rsa:2048 –keyout server.key –out server.crt
接著使用openssl套件（SSL_CTX_use_certificate_file, SSL_CTX_use_PrivateKey_file），分別載入server及client的公鑰和私鑰，並檢查是否正確(SSL_CTX_check_private_key)，並於載入後和ssl通道連結。之後便以SSL_write()及SSL_read()函數互相溝通。

當 client A 要轉帳給 client B時，先載入自己的私鑰並加密(RSA_private_encrypt)。加密後透過與 B 的 ssl 通道傳輸。B 收到後，會載入 A 的公鑰解密(RSA_public_decrypt)。解密後，使用自己的私鑰加密(因為加密後的長度限制，會將A的密文切成兩塊再分別加密)，傳送給 server。server會用對應的 client 公鑰解開。

四、參考資料、來源

– TCP Socket Programming — http://zake7749.github.io/2015/03/17/SocketProgramming/
– Socket programming in C on Linux — https://www.binarytides.com/socket–programming–c–linux–tutorial/
– Socket: server and client C++ – https://www.bogotobogo.com/cplusplus/sockets_server_client.php
– ssl server client programming using openssl in c – https://aticleworld.com/ssl–server–client–using–openssl–in–c/