doc3

b08611032 生機三 林毓翔

執行環境

`C++ 11`

解壓縮

```
tar zxvf b08611032_part3.tar.gz
```

檔案結構

```
b08611032_part3
    ├── src
        ├── client
            ├── main.cpp
            ├── clientConnection.h
            ├── clientConnection.cpp
        ├── server
            ├── main.cpp
            ├── server.h
            ├── server.cpp
            ├── user.h
            ├── server.key
            ├── server.crt
            ├── ssl.conf
        ├── utility.h
    ├── bin
        ├── client
        ├── server
    ├── makefile
    ├── doc.pdf
    ├── ssl.conf
```

編譯方式

解壓縮後，進入資料夾輸入 `make` 即可

執行方式

編譯完成後，執行以下指令啟動 server

```
./bin/server <server port> -a
```

編譯完成後，執行以下指令啟動 client:

```
./bin/client <client IP address> <client port>
```

原始碼架構說明

(註：以下程式碼行數為在 `clientConnection.cpp` 中的行數)

基礎SSL連線

```
1156  SSL_library_init();
1157  OpenSSL_add_all_algorithms();
1158  SSL_load_error_strings();
1159  SSL_CTX* ctx;
1160  ctx = SSL_CTX_new(SSLv23_client_method());
```

並將傳送與接收改為 `SSL_write` `SSL_read` ，且在bind socket 後加上 `SSL_connect` 並將 `ssl*` 變數 bind此socket file descriptor

生成密鑰

Server 端為一固定的 `server.crt` 與 `server.key` 檔，client 端則是每次執行後會動態產生一個新的 `*.key` 及 `*.crt` 檔，實作方式是利用 C 語言中的 System Call 呼叫 openssl 的命令列指令生成，並需要讀入預先寫好之參數設定檔 `ssl.conf`

```
139  string a = "openssl req -x509 -new -nodes -sha256 -utf8 -days 3650 -newkey rsa:20
140          -keyout " +caNum +"_private.key -out "+caNum+ ".crt -config ssl.conf";
141  system(a.c_str());
```

密鑰傳輸

因憑證包含 public key，因此我將憑證 load 進 SSL 連線，需要時 client 端 可從連線取得 server 端之憑證(public Key)

server 端將憑證送進連線

```
148  int use_cert = SSL_CTX_use_certificate_file(ctx, (caNum + ".crt").c_str() ,
149                  SSL_FILETYPE_PEM);
```

client 端取得 server 之憑證

```
1239  X509* b_publicKey_x509 = SSL_get_peer_certificate(sslTemp);
1240  EVP_PKEY* b_publicKey_evp = X509_get_pubkey(b_publicKey_x509);
1241  RSA* b_publicKey = EVP_PKEY_get1_RSA(b_publicKey_evp);
```

加解密

若是由 Client A 轉帳給　Client B，則 A 會先從連線中取得 B 之 public key 並用其將訊息加密後再經由 SSL 連線傳送給 B 。 只有 B 收到訊息後，利用其不公開之 Private Key 將此訊息解密，確保只有 B 可以看到訊息內容。 B 再從與 Server 的連線中取得 Server 之 public key並用其將訊息加密後再經由 SSL 連線傳送給 Server， 確保只有 Server 可以利用它不公開的 private key 解密後看到訊息內容

利用 public key 加密

```
int response = RSA_public_encrypt((strlen(transMessage)+1) * sizeof(char),
        (unsigned char*)transMessage,(unsigned char*)encryptMessage,
        b_publicKey, RSA_PKCS1_PADDING);
```

利用 private key 解密

```
int response = RSA_private_decrypt(RSA_size(rsaPrivateKey), (unsigned char*)buffe
        (unsigned char*)decryptMessage, rsaPrivateKey,
        RSA_PKCS1_PADDING);
```

參考資料

實作注意事項

- SSL_read 收不到東西?
  - 注意不要把 sizeof() 與 strlen()搞混，SSL_send 用後者當第三個參數，SSL_read用前者當第三個參數
- SSL_connect
  - 在SSL_connect前，仍需要原本的connect
  - 但SSL_write SSL_read 可知直接取代原本的 read wirte
  - 注意沒有SSL_send SSL_recv ，通通使用 SSL_write SSL_read

概念類

- RSA是啥 **https://www.itread01.com/articles/1501720695.html?fbclid=IwAR2CbBrNjWMyBS_yTvt7aDWjmJgmi964dWZs7LW9pD7oaEgide9P2t8kYVc** (https://www.itread01.com/articles/1501720695.html?fbclid=IwAR2CbBrNjWMyBS_yTvt7aDWjmJgmi964dWZs7LW9pD7oaEgide9P2t8kYVc)
- RSA WIKI **https://zh.wikipedia.org/zh-tw/RSA加密演算法** (https://zh.wikipedia.org/zh-tw/RSA%E5%8A%A0%E5%AF%86%E6%BC%94%E7%AE%97%E6%B3%95)
- RSA - Behind scene **https://medium.com/@bn121rajesh/understanding-rsa-public-key-70d900b1033c** (https://medium.com/@bn121rajesh/understanding-rsa-public-key-70d900b1033c)

實作 類

- OpenSSL文件 **https://www.openssl.org/docs/man1.1.1/man3/** **(https://www.openssl.org/docs/man1.1.1/man3/)**
- 怎麼生成自簽憑證
  - 命令列1 **https://blog.miniasp.com/post/2019/02/25/Creating-Self-signed-Certificate-using-OpenSSL?fbclid=IwAR2R0BoA5XyGghiZgBIr1xUrCAGXXJKA9I7HP-a1txQkBfRvUk_o9iEgVuA** **(https://blog.miniasp.com/post/2019/02/25/Creating-Self-signed-Certificate-using-OpenSSL?fbclid=IwAR2R0BoA5XyGghiZgBIr1xUrCAGXXJKA9I7HP-a1txQkBfRvUk_o9iEgVuA)**
  - 命令列2 **https://www.scottbrady91.com/openssl/creating-rsa-keys-using-openssl** **(https://www.scottbrady91.com/openssl/creating-rsa-keys-using-openssl)**
  - 命令列3 **https://dynacont.net/documentation/linux/openssl/?fbclid=IwAR1VBzfXEkRs4BPtloJZEHiONlcrRW7cWAHEZfem7pyH1D-BR7JXxJvgJHI** **(https://dynacont.net/documentation/linux/openssl/?fbclid=IwAR1VBzfXEkRs4BPtloJZEHiONlcrRW7cWAHEZfem7pyH1D-BR7JXxJvgJHI)**
  - In C Programming **https://stackoverflow.com/questions/4757512/execute-a-linux-command-in-the-c-program** **(https://stackoverflow.com/questions/4757512/execute-a-linux-command-in-the-c-program)**
  - In C programming **https://stackoverflow.com/questions/12647220/reading-and-writing-rsa-keys-to-a-pem-file-in-c** **(https://stackoverflow.com/questions/12647220/reading-and-writing-rsa-keys-to-a-pem-file-in-c)**
- load key
  - **https://vimsky.com/zh-tw/examples/detail/cpp-ex-----PEM_read_RSAPrivateKey-function.html** **(https://vimsky.com/zh-tw/examples/detail/cpp-ex-----PEM_read_RSAPrivateKey-function.html)**
- Variable Type
  - char* to unsign char * **https://stackoverflow.com/questions/42392482/c-how-to-convert-from-char-to-unsigned-char-**

    in- (https://stackoverflow.com/questions/42392482/c-how-to-convert-from-char-to-unsigned-char-in-)
  - get the length of unsign char * **https://stackoverflow.com/questions/836549/how-do-you-determine-the-length-of-an-unsigned-char** (https://stackoverflow.com/questions/836549/how-do-you-determine-the-length-of-an-unsigned-char)
- SSL 連線 **https://stackoverflow.com/questions/7698488/turn-a-simple-socket-into-an-ssl-socket?fbclid=IwAR2G3_k2he6khBlLDSxvwh1OBueXStdlujGelVYXyjt7_3uvrw9avQK5Vbk** (https://stackoverflow.com/questions/7698488/turn-a-simple-socket-into-an-ssl-socket?fbclid=IwAR2G3_k2he6khBlLDSxvwh1OBueXStdlujGelVYXyjt7_3uvrw9avQK5Vbk)
- openssl 程式碼參考
  - **https://stackoverflow.com/questions/15092589/client-server-communication-using-openssl-using-certificate?fbclid=IwAR33uipLFr-r0AOfMA8-krUfczmsUHA0A-7wsgmYzpV_kqYQS-FpJwvYHwk** (https://stackoverflow.com/questions/15092589/client-server-communication-using-openssl-using-certificate?fbclid=IwAR33uipLFr-r0AOfMA8-krUfczmsUHA0A-7wsgmYzpV_kqYQS-FpJwvYHwk)
  - **https://stackoverflow.com/questions/41229601/openssl-in-c-socket-connection-https-client?fbclid=IwAR3F85pPg67HPDMhxJaqM6pbWCyb8xYNtHz-uaCHNwug9cNYo0-z5aLFn44** (https://stackoverflow.com/questions/41229601/openssl-in-c-socket-connection-https-client?fbclid=IwAR3F85pPg67HPDMhxJaqM6pbWCyb8xYNtHz-uaCHNwug9cNYo0-z5aLFn44)
- 寫出key
  - **https://stackoverflow.com/questions/25222068/rsa-encrypt-then-decrypt-fails-with-oaep-decoding-error** (https://stackoverflow.com/questions/25222068/rsa-encrypt-then-decrypt-fails-with-oaep-decoding-error)
  - **https://stackoverflow.com/questions/10451936/how-to-print-rsa-as-string-in-c?fbclid=IwAR24dqmlYmEYp37h13AMLaSgKIl37x1BMWxLmKFgzVOd9Po8I6qiZkY-HME**

    (https://stackoverflow.com/questions/10451936/how-to-print-rsa-as-string-in-c?fbclid=IwAR24dqmlYmEYp37h13AMLaSgKII37x1BMWxLmKFgzVOd9Po8I6qiZkY-HME)

    - **https://stackoverflow.com/questions/15536666/extract-rsa-public-key-from-a-x509-char-array-with-openssl/15539290?fbclid=IwAR0kQxcboW44dnLx-tCMO9H8jM-pBsNKJPm8xCjlXj1Ldm0pGBiiRNsp7Vs** (https://stackoverflow.com/questions/15536666/extract-rsa-public-key-from-a-x509-char-array-with-openssl/15539290?fbclid=IwAR0kQxcboW44dnLx-tCMO9H8jM-pBsNKJPm8xCjlXj1Ldm0pGBiiRNsp7Vs)
- 加密解密
    - **https://blog.csdn.net/qq_30667875/article/details/105427943** (https://blog.csdn.net/qq_30667875/article/details/105427943)
    - **https://stackoverflow.com/questions/45906255/how-to-perform-public-key-encryption-with-rsa-using-c?fbclid=IwAR1qO33rNAixt7AvD-M6fQ9VcDxYw-b8F53byMShVjMeT1GxVkTigZkb-Jc** (https://stackoverflow.com/questions/45906255/how-to-perform-public-key-encryption-with-rsa-using-c?fbclid=IwAR1qO33rNAixt7AvD-M6fQ9VcDxYw-b8F53byMShVjMeT1GxVkTigZkb-Jc)

BUG 類

- no shared cipher **https://stackoverflow.com/questions/39428438/openssl-for-64-bit-windows-and-no-shared-cipher** (https://stackoverflow.com/questions/39428438/openssl-for-64-bit-windows-and-no-shared-cipher)
- RSA_public_encrypt segement fault **https://stackoverflow.com/questions/53286960/segfault-on-openssl-rsa-public-encrypt-in-c** (https://stackoverflow.com/questions/53286960/segfault-on-openssl-rsa-public-encrypt-in-c)
- OpenSSL RSA_private_decrypt() fails with “oaep decoding error” **https://stackoverflow.com/questions/25506611/openssl-rsa-private-decrypt-fails-with-oaep-decoding-error** (https://stackoverflow.com/questions/25506611/openssl-rsa-private-decrypt-fails-with-oaep-decoding-error)
- check public key and private key match **https://stackoverflow.com/questions/11651632/how**

-to-test-a-public-private-keypair-in-c?rq=1

(https://stackoverflow.com/questions/11651632/how-to-test-a-public-private-keypair-in-c?rq=1)