OpenSSL 加密解密實驗報告:　資訊工程四 A　10503301A　鍾俊傑

1. 在 OpenSSL 中，利用 des-cbc 加密考題，指令如下。現明文之原始檔案遺失，只剩 下加密檔案 test1.out，請你 openssl 中解密，得到原來之考題並加以回答。

Openssl enc -d -des-cbc -in test1.out -out test1chk.txt -k u4g.3284vm,6
Q1: 你的學號與姓名？
10503301A 鍾俊傑
Q2: 老師的姓名？
楊吳泉老師

2. 在 OpenSSL 中，利用 des-ecb 加密資料，現明文之原始檔案與 password 均遺失，只 剩下加密檔案 test2.out，但得知 password 只有 3 個字母且和前一題之 password 有 關係，請問你有無辦法還原明文？你有辦法獲得原來之明文？若有說明你的方法? 若無說明困難點在何處？

Openssl enc -d -des-ecb -in test2.out -out test2chk.txt -k isu
Q: 暑假有何計畫?
畢業後回香港工作

因與前題之 password 有關係，而不是指出 3 個字母為前題 password 中的字母組合，則可猜測到前題之 password 有隱含意思，u4g.3284vm,6 可於 Google 搜尋到義守大學，而義守大學正是 isu。

3. 老師產生一組 RSA 金鑰，公鑰檔案 wcyang_ku.pem，請你利用這個公鑰加密一個祝 福老師的訊息給老師，加密之訊息以附檔方式繳交。

openssl rsautl -encrypt -pubin -inkey wcyang_ku.pem -in test1.txt -out abc.out

4. 自行產生一組 RSA 金鑰，請利用你的私鑰簽署一個祝福老師的訊息給老師， 祝福訊息、簽章內容及你的公鑰分別以附檔方式繳交。

openssl rsautl -encrypt -pubin -inkey rsakpu1.pem -in abc2.txt -out abc2.out
openssl rsautl -decrypt -inkey rsakpr1.pem -in abc2.out -out abc2chk.txt

5. 簡要說明你的心得。

了解 OpenSSL 指令後十分容易進行加密和解密的動作。
在第二條中更是體驗到解密和猜謎的樂趣。
覺得這堂課學習到不少知識及感受到老師有趣的授課方式。