Homework 3. SSL Decryption

(Due: 12/15)

TLS/SSL 是一種在網路通訊中常見的加密協議，提供安全及數據完整性保障。在建立加密連線時，客戶端與伺服器端會協商並從 Cipher Suite 中決定此次連線所使用的加密演算法等。

附檔有 Capture_1.pcap、Capture_2.pcap 以及 ssl.key 三個檔案，其中 Capture_1 和 Capture_2 都是從 TLS/SSL 加密連線中截取出的封包訊息，而 ssl.key 則是用來加密此二連線的 private key。

在這次的作業中同學可以利用網路封包分析工具如 Wireshark 等來個別對 Capture_1 以及 Capture_2 做解密並截取出連線所傳送的資料。

評分標準：

1. 說明解密的過程

2. 解密結果

3. 若無法解密成功，試說明其中的原因