Lab2 – User Manual

1. **在 FPGA 板上設定需要的 RSA key 長度。**

   這個部分可以藉由設定開關 SW[7]~SW[10] 來調整，其中 SW[7] 代表 key 的長度為 2^7，其他開關可以以此類推，此時七段顯示器上應該會顯示 key length。

2. **執行 rs232_esc.py**

   rs232.py 和 rs232_esc.py 不同處在於 esc 版本支援我們解密機的連續傳檔功能，也就是在解密完一個檔案後可以不用手動按下 reset 而能繼續進行解密。

   執行方式為：sudo ./rs232_esc.py /dev/ttyUSB0 <RSA key length>

   其中 <RSA key length> 的部分可以為 128, 256, 512, 1024。

   而 /dev/ttyUSB0 可能會視情況改變，可以利用 linux 下的 dmesg 指令來確認 port name。

   此外還要注意需要解密的 key 和 enc 檔案名稱會隨著執行時輸入的 RSA key length 而改變，舉例來說若 key length 為 512，則會利用 key512.bin 來對 enc512.bin 進行解密，並輸出 dec512.txt。

3. **解密完畢，板子上的 LEDG[0] 亮起**

   LEDG[0] 代表的是解密完成的指示燈，亮起來後可以回到步驟 1，繼續解密。

自行產生測資

1. **首先到生成 RSA key 的網頁服務生成一份 16 進位表示的 RSA key**

   網址為：http://www.mobilefish.com/services/rsa_key_generation/rsa_key_generation.php

   生成完後，分別將 N,e,d 分三行存在 key{key length}.txt 中。

   若 key length 為 512 則命名為 key512.txt。

2. **準備一份需要加密的文件，命名為 dec{key length}.txt**

   若 key length 為 512 則命名為 dec512.txt。

   注意檔案大小必須為 ((key length / 8) - 1) n。

3. **執行 rsa.py**

   注意到這個 rsa.py 的版本是修改過的。

   執行加密的方法為 ./rsa.py e <key length>。

   執行解密的方法為 ./rsa.py d <key length>。

   至於檔名則會自動尋找符合 key length 的檔案。