Information Security HW5

B10630436 林玉庭
B10632026 吳苡瑄 ./DSA.py

建置環境

Windows10 Python3

操作說明

```
python ./DSA.py -keygen
```

生成 public key 和 private key 並分別存到 `publicKey.txt` 和 `privateKey.txt` 裡面

```
python ./DSA.py -sign {message}
```

讀取 public 和 private key的檔案生成簽章 r、s 並存到 `signature.txt` 中

```
python ./DSA.py -verify {message}
```

讀取 public 和signature 檔案來驗證檔案，最後印出 valid 或 invalid

程式碼解說

- 生成key
  - 主要就是按照講義上的演算法生成 p,q,a,b，最後再輸出到txt檔中，很多部分都是沿用上次做 RSA 時的 function。
  - 只新增了一個 findOrd 用來找 a。
  - 另外生成 p 的方法是直接 shift q到 1024 bits後再繼續下去找，如果已經找超過 1024 bits 就重新找一個 q 再重來。
- 簽章
  - 就只是讀檔案拿出 public key 後照演算法去運作而已
  - 因為可以用 library 做 SHA1 所以很方便
  - 最後把 r,s 存到txt檔
- 驗章
  - 讀檔案拿出 public key 和 signature 後照演算法去運作

- 最後比對 v 和 r 並印出結果

遇到困難與心得

- 因為跟 RSA 很像所以好像沒遇到什麼問題
- 幸好可以用 hash library 不用自己做

結果