

Information Security HW5

B10630436 林玉庭

B10632026 吳苡瑄 ./DSA.py

建置環境

Windows10 Python3

操作說明

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

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

```
1 | 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

```
1 | 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

```
PS D:\school\InformationSecurity\Information_Security_Class\hw5> python .\DSA.py -keygen
p = 156366433332625409945729106190153004933729760889781489648167919133591704245284071958258940551596816267251753291394241551112235199565342097285384681115471313425348157281460334060516202
376090215823424303663166405259102795091494041151371238459602908697715526906704220016128740676431421912268341087971565471699387
q = 1271239200436332827067545583167966263067507435719
a = 240030924811828375848049240703522782397676034595584569499167616222802359503481722743189518212548201295987942118047819593308023308291039653631192605891019905486941366651330409703159611
803859477441556269125746261984258275598656973613450816411581198235692492325486850248750380838298624325766545333013230806119957
b = 547882952537306779652285761552431731377282443206061997864593099604188307909336260246786104461346433494982538419277803442758895323851633065899692251109298948724663033716429516771015572
45929802133832527373818467578804573483013409668351007292032191384275069197750528631444755082547382683370921245899565346984275
d = 1203403736669039325124116082346996487053731917184
Public key is store in publicKey.txt, and private key is store in privateKey.txt.
PS D:\school\InformationSecurity\Information_Security_Class\hw5> python .\DSA.py -sign hello
r = 15202213689983710884777069067779620700927167523
s = 961210247666180126035440941279799780333155960719
Signature is store in signature.txt.
PS D:\school\InformationSecurity\Information_Security_Class\hw5> python .\DSA.py -verify hello
valid
```