

# HW5

## 分組及分工

- B10415041 曾增宇
  - 生成 key
  - 簽章
- B10415049 陳祐丞
  - 生成 key
  - 驗章

## 建置環境

- Python 3.6.5 :: Anaconda, Inc. on windows 10

## 使用方式

- 命令列輸入 `python DSA.py -keygen` 生成 key
- 命令列輸入 `python DSA.py -sign <message>` 再輸入相關 key 簽章，得 r, s
- 命令列輸入 `python DSA.py -veri <message>` 再輸入相關 key 及 r, s，驗章

## 實作過程困難與心得

- key 的生成中，p, q 很難找到，原本的做法是 random 質數p，再 random 質數q，看 q 是否為 p 的因數，後來決定先找 q，再找 q 的倍數在1024bit的數是否為質數，一方面用加法的也比較快
- 剛開始簽章驗章失敗，忘記了 -1 次方的 mod 值，要應用到歐拉定理，找 p - 2 次方
- 原理有點困難，不過看著實作方法寫 code 倒是滿簡單的，之前也實做過相關的 function 所以滿容易的。

## 截圖

```
Kpub-p: 898846567431157953864652595394512366880898848947115328636715040578866337902750481566354238661283768010560056939935696678829394884407208311246423715319737062188883946712432742638151109800623047059726541476042502884419075341171231440736956555270413618581675256353702851829068432546032802609380698678681240422739
Kpub-q: 1038283145625194879935928394017802883307097601489
Kpub-a: 12198588608408589979386289540893612235315476658235058805068928578816283378616108057616095380391654565710457968135678719535157911797262848918124226359718827313115760803113526104287861068840135011433457701995309309861117617079346050481494444361510088299731334919934787954886008095181518690388270086839408915964
Kpub-pubkey: 75609317757394691858344903524883241907811445399735103733731137427045221931613466816802001183664816754787043779065990475124865045808381759265948909387983198648895796571121067372240209491070583543559232143291680421054598952687690425519264426445781388775882412251948956786368397789130303409115690792070196765424
Kpr-l-prKey: 270945875554936831262235560768619789083979251077

D:\AllProjects\python\Information-Security-Homework\HW5\VoYo\python DSA.py -sign myDSAboo
Input p: 898846567431157953864652595394512366880898848947115328636715040578866337902750481566354238661283768010560056939935696678829394884407208311246423715319737062188883946712432742638151109800623047059726541476042502884419075341171231440736956555270413618581675256353702851829068432546032802609380698678681240422739
Input q: 1038283145625194879935928394017802883307097601489
Input a: 12198588608408589979386289540893612235315476658235058805068928578816283378616108057616095380391654565710457968135678719535157911797262848918124226359718827313115760803113526104287861068840135011433457701995309309861117617079346050481494444361510088299731334919934787954886008095181518690388270086839408915964
Input prKey: 270945875554936831262235560768619789083979251077
-----get p, s-----
r: 672573634564641457813101756700329188418716848470
s: 120767257357960813397428039524112024967531324036

D:\AllProjects\python\Information-Security-Homework\HW5\VoYo\python DSA.py -veri myDSAboo
Input p: 898846567431157953864652595394512366880898848947115328636715040578866337902750481566354238661283768010560056939935696678829394884407208311246423715319737062188883946712432742638151109800623047059726541476042502884419075341171231440736956555270413618581675256353702851829068432546032802609380698678681240422739
Input q: 1038283145625194879935928394017802883307097601489
Input a: 12198588608408589979386289540893612235315476658235058805068928578816283378616108057616095380391654565710457968135678719535157911797262848918124226359718827313115760803113526104287861068840135011433457701995309309861117617079346050481494444361510088299731334919934787954886008095181518690388270086839408915964
Input pubKey: 75609317757394691858344903524883241907811445399735103733731137427045221931613466816802001183664816754787043779065990475124865045808381759265948909387983198648895796571121067372240209491070583543559232143291680421054598952687690425519264426445781388775882412251948956786368397789130303409115690792070196765424
Input r: 672573634564641457813101756700329188418716848470
Input s: 120767257357960813397428039524112024967531324036
-----result-----
Valid.
```