

# 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

- 一開始依照上課簡報的敘述一樣先找到 1024 bits 的  $p$ , 但是一直 random 不出 160 bits 又可以整除  $p-1$  的  $q$ , 後來想到  $q$  可能根本不存在, 因此後來與同學、隊友討論後決定先找  $p$ , 再乘出  $p$  來判斷  $p$  是否為質數
- 產生完 key 後再檢查簽章發現模反元素寫錯了, 後來才想到應該要用歐拉定理算才正確。

## 截圖

```
kpab-p: 89884656741115795386465259539451236688898848947115328636715040578866337902758481566354238661203768010560056939935696678829394884407208311246423715319737062188883946712432742630151109800623047059726541476042562884419075341171231440736956555270413618581675256353702851829068432546832862069380698678681240422739
kpab-q: 1038283145625194879935928394017802883307097601489
kpab-a: 1219858868048589979386289540893612235315476658235058805068928578816283378616108057616095380391654565710457968135678719535315791179726284891812422635971882731311576080311352610428786106884013501143345770199530930986111761707934605048149444361510088299731334919934787954886000895181518696388270086839480915964
kpab-pubKey: 76680311737946918583449032488132419978114453997351037333731137427045221931613466816802001183664816754787843779065904751248650458083817592659480993879831986488957965711210673722402094910705835435592321432916804210545989526876904255192644264457813877588241225194895678638397789130383409115690792070196765424
kpri-priKey: 270945075554936831262235560768619789803979251077

D:\AllProjects\python\Information-Security-Homework\VM5\VoVo\python DSA.py -sign my05Abccc
Input p: 89884656741115795386465259539451236688898848947115328636715040578866337902758481566354238661203768010560056939935696678829394884407208311246423715319737062188883946712432742630151109800623047059726541476042562884419075341171231440736956555270413618581675256353702851829068432546832862069380698678681240422739
Input q: 1038283145625194879935928394017802883307097601489
Input a: 1219858868048589979386289540893612235315476658235058805068928578816283378616108057616095380391654565710457968135678719535315791179726284891812422635971882731311576080311352610428786106884013501143345770199530930986111761707934605048149444361510088299731334919934787954886000895181518696388270086839480915964
Input pubKey: 76680311737946918583449032488132419978114453997351037333731137427045221931613466816802001183664816754787843779065904751248650458083817592659480993879831986488957965711210673722402094910705835435592321432916804210545989526876904255192644264457813877588241225194895678638397789130383409115690792070196765424
Input priKey: 270945075554936831262235560768619789803979251077
=====get r, s=====
r: 672573634564641457813101756700329188418716848470
s: 120767257357960813397428039524112024967531324036

D:\AllProjects\python\Information-Security-Homework\VM5\VoVo\python DSA.py -veri my05Abccc
Input p: 89884656741115795386465259539451236688898848947115328636715040578866337902758481566354238661203768010560056939935696678829394884407208311246423715319737062188883946712432742630151109800623047059726541476042562884419075341171231440736956555270413618581675256353702851829068432546832862069380698678681240422739
Input q: 1038283145625194879935928394017802883307097601489
Input a: 1219858868048589979386289540893612235315476658235058805068928578816283378616108057616095380391654565710457968135678719535315791179726284891812422635971882731311576080311352610428786106884013501143345770199530930986111761707934605048149444361510088299731334919934787954886000895181518696388270086839480915964
Input pubKey: 76680311737946918583449032488132419978114453997351037333731137427045221931613466816802001183664816754787843779065904751248650458083817592659480993879831986488957965711210673722402094910705835435592321432916804210545989526876904255192644264457813877588241225194895678638397789130383409115690792070196765424
Input priKey: 270945075554936831262235560768619789803979251077
=====result=====
valid.
```