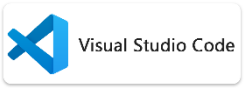
RSA 程式設計作業

資工二乙 11111245 彭祥瑀

作業環境 



執行結果:

基本款

```
PS C:\Users\n0045\OneDrive\桌面\source> python -u "c:\Users\n0045\OneDrive\桌面\RSA.py"
Enter p: 43
Enter q: 59
Enter e: 13
Enter plain text: STOP

d: 937
n: 2537

(C): 2081 2182

(M): 1819 1415
PS C:\Users\n0045\OneDrive\桌面\source>
```

中階款

```
PS C:\Users\n0045\OneDrive\桌面\source> python -u "c:\Users\n0045\OneDrive\桌面\RSA.py"
Enter p: 3896519873
Enter q: 6728380129
Enter e: 7237327049
Enter plain text: RSA INVOLVES A PUBLIC KEY AND A PRIVATE KEY THE PUBLIC KEY CAN BE KNOWN BY EVERYONE AND IS USED FOR ENCRYPTION MESSAGES MESSAGES ENCRYPTED WITH THE PUBLIC KEY CAN BE ONLY BE DECRYPTED IN A REA
SONABLE AMOUNT OF TIME USING THE PRIVATE KEY THE KEYS FOR THE RSA ALGORITHM ARE GENERATED THE FOLLOWING WAY

d: 49621622255038558585
n: 26217266885746803617

(C): 661182239120790232 7 1384929737960852751 3 1624789912645966133 5 2368711309891505965 1962971064088918837 9 6926892904584814804 4 4447973671030565749 7873940569480520214 2461621989118591133 6 1113992296384057618 7 2
5762172624793938442 1342305801093227637 1 1707567891112997173 4 1378509810822161561 8 7113383132300478325 1384929737960852751 3 2612254427432358468 2396246581483517058 1 2301643578647449017 6 2327598679741219896 9 134
2305801093227637 1 1707567891112997173 4 2253200611082234125 2 2327598679741219896 9 1768419319179899716 3 2202933761910662075 3 1726907139898351502 1 6377603490865502418 5 5057541143316215800 2 2389976175202359944 4 13785
098108221615618 7 7064623795024570147 2 2327598679741219896 9 1662425199247324749 1 2475851294703709360 4 1581507859983192967 6 9644192653242922903 9 9038903785119966244 1743552542442905091 8 2035117481488338159 1 275854040
4411779579 2 2327598679741219896 9 1378509810822161561 8 7113383132300478325 8 8304389425183833219 1 8016468398829819094 2 2231583788812550097 9 7113383132300478325 1 1148440805364342669 7 1862634250182071746 9 9354574055652
503936 2 2182738010390105434 4 1101387610002423388 7 1397441799437829157 4 2758540404411779579 9 9909216201681101901 6 9268929045848148 0 1739906392342962663 4 2117778631094042403 9 1410045070238776752 5 1840293111427725012
92 2 2315372885239468776 9 1653310814768703632 3 6926892904584814804 9 9038903785119966244 9 4943565736594359241 2 2035117481488338159 1 1252412753087187488 7 4160579029389134555 8 6082562970047695 2 4528547931724913054 1 3000070
0358701474413 2 2253200611082234125 2 2327598679741219896 9 1768419319179899716 3 2202933761910662075 3 1726907139898351502 1 6377603490865502418 5 5057541143316215800 2 2389976175202359944 1 1378509810822161561 8 706462379
5024570147 2 2327598679741219896 9 2758540404411779579 2 2229472888723502136 1 7064623795024570147 2 2327598679741219896 9 1182516925268231987 5 2182738010390105434 4 1101387610002423388 7 5892016401434133410 7 1133831323000
478325 1 1624789912645966133 5 4447973671030565749 3 5982260278496937 3 7 1615716411146360037 6 2238914479439306100 8 2336334238254507886 3 2202933761910662075 3 2327598679741219896 9 2027362293288116602 2 2463250111298252
4137 1 1140515332598054509 1 8314279648941907257 1 7478367229135501469 1 3974417994378291574 1 8402931114277250192 1 8016468398829819094 4 4087316971764079510 2 2324804308507236603 4 1153975935115940688 6 1422789738183617472 5
725 7 8739405694805202 1 4 1787459232416672587 2 1 6035995138398513 1 6 5892016401434133410 1 6377603490865502418 5 5057541143316215800 2 1153975935115940688 6 1422789738183617472 5 1637760349086550241 8 5057541143316215800 1
4100450702387767525 1 1148440805364342669 7 1862634250182071746 9 2253200611082234125 2 2327598679741219896 9 6611822391207902327 3 1384929737960852751 3 2316619985911776234 3 2001104937834074306 2 1787459232416672587 2 225
3200611082234125 2 1046783029060330804 1 1752624041505979 1 3 2327598679741219896 9 2117778631094042403 9 2507251139980851917 1 1384033136744707679 2 5892016401434133410 7 1133831323004783 2 2253200611082234125 2 232759
86797412198969 1 1148440805364342669 7 2252933811921336706 6 2475851294703709360 4 1624789912645966133 5 9881820415216577656 2 2502893304614997244 9 1707567891112997173 4

(M): 1718 26 813 2114 1121 418 2600 2615 2001 1108 226 1004 2426 13 326 26 1517 821 19 426 1004 2426 1907 426 1520 111 802 2610 424 2602 13 2601 426 1013 1422 1326 124 2604 2104 1724 1413 426 13 326 818 2620 18
04 326 514 1726 413 217 2415 1908 1413 2612 418 1800 604 1826 1204 1818 6 418 2604 1302 1724 1519 403 2622 819 726 1907 426 1520 111 802 2610 424 2602 13 2601 426 1413 1124 2601 426 304 217 2415 1904 326 813 26
00 2617 400 1814 1300 111 426 12 1420 1319 2614 526 1908 1204 2620 1808 1306 2619 704 2615 1708 2100 1904 2610 424 2619 704 2610 424 1826 514 1726 1907 426 1718 26 11 614 1708 1907 1226 17 426 604 1304 1700 190
4 326 1907 426 514 1111 1422 813 626 2200 2426
PS C:\Users\n0045\OneDrive\桌面\source>
```

進階款


問題 輸出 偵錯主控台 終端機 連接埠
Code
PS C:\Users\n0045\OneDrive\桌面\source> python -u "c:\Users\n0045\OneDrive\桌面\RSA.py"
Enter p: 38965198437434868119893782943763287625198367281632 3
Enter q: 67283801278346924852096712876311628637829164937683 9
Enter e: 72373269811253451267276174512363892363611273657236 7
Enter plain text: RSA INVOLVES A PUBLIC KEY AND A PRIVATE KEY THE PUBLIC KEY CAN BE KNOWN BY EVERYONE AND IS USED FOR ENCRYPTION MESSAGES MESSAGES ENCRYPTED WITH THE PUBLIC KEY CAN BE ONLY BE DECRYPTED IN A REASONABLE AMOUNT OF TIME USING THE PRIVATE KEY THE KE
YS FOR THE RSA ALGORITHM ARE GENERATED THE FOLLOWING WAY
d: 2428535886755840714481288508164141304354488932723102643091004967165746926430232470016362499141959878 67
n: 2621726668435721778351896929354906266819645267015514933756485016427962614839995465010625770670573429 97
(M): 1718 26 813 2114 1121 418 2600 2615 2001 1108 226 1004 2426 13 326 26 1517 821 19 426 1004 2426 1907 426 1520 111 802 2610 424 2602 13 2601 426 1013 1422 1326 124 2604 2104 1724 1413 426 13 326 818 2620 1804
0 604 1826 1204 1818 6 418 2604 1302 1724 1519 403 2622 819 726 1907 426 1520 111 802 2610 424 2602 13 2601 426 1413 1124 2601 426 304 217 2415 1904 326 813 2600 2617 400 1814 1300 111 426 12 1420 1319 2614 526
904 2610 424 2619 704 2610 424 1826 514 1726 1907 426 1718 26 11 614 1708 1907 1226 17 426 604 1304 1700 1904 326 1907 426 514 1111 1422 813 626 2200 2426
PS C:\Users\n0045\OneDrive\桌面\source>

心得:

除了在課堂上聽老師講解 RSA，前前後後也花了很多時間在網路上找到許多實作參考資料，讓我對 RSA 原理和運作有更深層的理解，也有發現不同的解法，像是檢查 plain text 是不是 2 的倍數 ，如果不是就要往後加上空字元，尤其是 pow，再次讓我對 Python 內建函式庫感到驚奇，利用 pow 可以很快速的計算指數，把很多問題都解決了，最後測資時，很幸運的結果是正確的，心理的成就感像泉湧般噴發，又離「資夢」這個目標往前邁了一步，很高興學會了這個演算法。