## RSA 程式設計作業

## 資工二乙 11111245 彭祥瑀





## 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

S 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: 4962162255038558585

(C): 6611822391287739268427379668527513 16247899126459661335 23667741308891569596 1962971064088918823161519962751064968871837267376709136567349 787394056948952276371 787075678911129971734 137856989188221615818713383132308478325 1384929737966898257513 612525442742352854682 33964565814381375687384490176 23275986797412198969 17684193191798997163 22029337619106620753 1726907139898351502 16377603490865502418 5957541143316215800 23899761752023159944 13785 098108221615618 70646237952024570447 22275986797412198969 1662425199247324791 247585122474912492679931499489 1458159785899313929676 94412795579 944127957947979 9441279579 9441279579 9441279579 9441279579 9441279579 9441279579 9441279579 9441279579 9441279579 9441279579 9441279579 94 50245/0147 / 25/75980/59412199909 27/58-0494129909 27/58-0494129909 27/58-0494129909 27/58-0494129-0494129909 27/58-0494129909 27 86797412198969 114844088653643426697 22529338119213367066 24758512947037093604 16247899126459661335 9881820415216577656 25028933046149972449 17075678911129971734

(M): 1718 26 813 2114 1121 418 2680 2615 2801 1188 226 1804 2426 13 326 26 1517 821 19 426 1904 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 94 326 514 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 1908 326 813 26 90 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

PS C:\Users\n8045\OneOrive\桌面\source> python -u "c:\Users\r Enter p: 389651984374348681199937829437632876251993672816323 Enter q: 678388112783469248520967128763116286376291649376839 Enter e: 723732698112534512672761745123638923636112736572367

Enter plain text: RSA DIVIOLVES A PUBLIC KEY AND A PRIVATE KEY THE PUBLIC KEY CAN BE KNOWN BY EVERYONE AND IS USED FOR ENCRYPTION MESSAGES ENCRYPTED WITH THE PUBLIC KEY CAN BE ONLY BE DECRYPTED IN A REASONABLE AMOUNT OF TIME USING THE PRIVATE KEY THE KEY FOR THE RSA ALGORITHM ARE GENERATED THE FOLLOWING WAY

d: 242853588675584071448128850816414130435448893272310264309100496716574692643023247001636249914195987867
n: 262172666843572177835189692935490626681964526701551493375648501642796261483999546501062577067057342997

| Co. | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 | 12.0 565792941224 186418713538626787989518455587128994932649439818920887118272294106126733631305141669784904289895085178 1143882268763785389365266449047411088113039558754406309189585480319257243275098116164128774531189708483 2001092150951521340747695313946382173735171122361642585519339145953967959950467206620463349222 243678193732506761203509704860197769077477094949306758076738521693801019001828590748169160701386748564 131529760736367212360077825956262989571710775061925593630654223813524767902927931631797635824409 $2951473763375393580541274682903571522592835998695946536966592078463966153068 103182678716348978935555098537943492867072981832807894789452682256683128390346606255682716715088326418 168579836511758069509216867802145\\083650258242255936493 3286665361779287639460600214497726293495819969860548231237070985462963246792164086550197635640656918 115501712543200975154180678283842433912440923647481092574060074743778991485069278425064563\\5801078486365605152373370753736003249491816666898576025441624449984 19799279561486721123529372015399093359502229853225578433403949815553267124655608368312153920280779098 7538597973737912294353808266427641139782778$  $799\ 25233117817065385288371598808121783920259195124853958990843830861539308355662896901914293514215083891\ 2266133590859153691189587323898464658910784863656951523733707537369032494918166668985760254416244449984\ 2098 65218447784576054839968480478835788260688974816142\ 248023450678333061554115259754929881940673067401092955643513624499920065548495787334523441039020421979\ 83194547285877032073863856005201593281832249065982081927987 3205055914671812097679460212217730676619232095825236052337414787393710833261834960980519185507340\ 94217334600324098990428384495719321045251483666403156259260362498756210556494481259787907282786408081\ 115501712543247606324098990428384495719321045251483666403156259260362498756210556494481259787907282786408081\ 115501712543247606324098990428384495719321045251483666403156259260362498756210556494481259787907282786408081\ 115501712543247606324098990428384495719321045251483666403156259260362498756210556494481259787907282786408081\ 11550171254324786408981\ 1155017125432498981\ 1155017125432498981\ 1155017125432498981\ 115501712543247$ 7474377899148569278425064563167197433525 2266133500550153691180587323898464658010784863656051523733707537360032494918166668985760254416244449984 16857988651175806959921686780214521904222554215799135032116491310019228547397655433923009259030959251089048471652247509629805306639331893711505743324438726396 63890025260784593176585671070701523863423304399724418126365576867160884207934594584958213203269355092 295252979187254995656 $8773587328884571120802543210419\ 77436334283747662154957508190581005164722111211562545572444771171341556606476171418580839127898220664\ 1534043306553590406430253322277834808796569129014066048752754404463962132120030548005071668042844904223388470133099036996143210835349342902259460769764219109$ 

# 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。