離散數學_RAS程式設計作業

資工二甲 11111132 楊敦傑

心得感想和實作過程:

本次的作業對於RAS以Python程式語言實作，因為Python有支援大數，所以並不用去處理大數的問題。
首先，在RSA加密前，需要先確保公鑰(e)與(p-1)*(q-1)的最大公因數為1，這樣代表兩者互質，才可以使後續的公式能正常執行。不僅如此，還必須確認明文的長度是否為2的倍數，因為題目中已經設定了加解密的區塊大小為每區塊2個字元，如果不是，就需要在最後加上一個空字符，以符合加密的規範。
接著就來到了建立私鑰的部分。這涉及到了數學的概念，就是反元素。為了算出這個反元素，我們需要使用輾轉相除法的方式來計算。通過輾轉相除法後，就可以求得私鑰(d)。接下來，需要先將字母轉換為數字，利用公鑰(e)並經過加密後，就可以得到密鑰C。然後，利用私鑰(d)對C進行解密後就可以得到真正的資料M

在製作RSA程式的過程中，我深刻體驗到了加解密資料的複雜，並且也體會到了數學公式的強大，這種感覺特別是在處理大數和模反元素等問題時，利用普通硬炸的方式會讓計算變得特別緩慢，但是在利用輾轉相除法等數學技巧，就能夠快速且有效地計算出RSA所需要的東西。
此外，經過這次的實作我也認知到了在加密算法中，每個步驟都扮演著至關重要的角色，尤其是需要保證資料完整性和準確性的情況下，一點小問題沒有考慮進去的話都會釀成巨大的錯誤。就好比原本我在RSA解密的地方使用的是一個一個字元去做的，但是程式跑出來的解果總跟我想的不一樣，後來才發現我的判定範圍設置錯誤了。所以我從中就了解到了在加解密中條件和步驟的重要性
總體而言，RSA解碼的實踐是極具挑戰性的過程。而使用Python作為工具，也讓我體驗了這個程式語言背後所具有的可能性，並且還了解了加解密實際應用中所需的準確性和條件設立的重要性。

程式執行結果:

基本款:

```
問題    輸出    偵錯主控台    終端機    連接埠

PS C:\Users\USER\Documents\GitHub\Mid1_2> python -u "c:\Users\USER\Documents\GitHub\Mid1_2\RSA_test.py"
請輸入e:13
請輸入p:43
請輸入q:59
(n, d): (2537, 937)
請輸入所要加密之文字:STOP
M = 1819 1415
C = 2081 2182
解碼後: STOP
PS C:\Users\USER\Documents\GitHub\Mid1_2> 
```

中階款:

```
PS C:\Users\USER\Documents\GitHub\Mid1_2> python -u "c:\Users\USER\Documents\GitHub\Mid1_2\RSA_test.py"
請輸入e:7237327049
請輸入p:3896519873
請輸入q:6728380129
(n, d): (26217266885746803617, 4962162255038558585)
請輸入所要加密之文字: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 B
E DECRYPTED IN A REASONABLE AMOUNT OF TIME USING THE PRIVATE KEY THE KEYS FOR THE RSA ALGORITHM ARE GENERATED THE FOLLOWING WAY
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 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 2600 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 1904 326 1907 426 514 1111 1422 813 626 2200 2426
C = 6611822391207902327 13849297379608527513 16247899126459661335 2368711309891505965 19629710640889188379 6926892904584814 80 4447973671030565749 7873940569480520214 24616219891185911336 111399
22963840576187 25762172624793938442 13423058010932276371 17075678911129971734 13785098108221615618 7113383132300478325 13849297379608527513 26122544274323584 68 23962465814835170581 230164357864
74490176 23275986797412198969 13423058010932276371 17075678911129971734 22532006110822341252 23275986797412198969 17684193191798997163 22029337619106620753 17269071398983515 02 16377603490865502
418 5057541143316215800 23899761752023159944 13785098108221615618 7064623795024570147 23275986797412198969 16624251992473247491 24758512947037093604 15815078599831929676 9644192653242922903 903
890378511996624 17435525424429050918 20351174814883381591 27585404044117795 79 23275986797412198969 13785098108221615618 7113383132300478325 8304389425183833219 18016468398829819094 223158378881
25500979 7113383132300478325 11484408053643426697 18626342501820717469 9354574055652503936 21827380103901054344 11013876100024233887 13974417994378291574 27585404044117795 79 990921620168110 1901
 6926892904584814 80 17399063923429626634 21177786310940424039 14100450702387767525 18402931114277250192 23153728852394687769 16533108147687036323 6926892904584814 80 903890378511996624 494356573
6594359241 20351174814883381591 12524127530871874887 4160579029389134 55 8608256297004769 52 4528547931724913054 13000700358701474413 22532006110822341252 23275986797412198969 176841931917989 9716
3 22029337619106620753 17269071398983515 02 16377603490865502418 5057541143316215800 23899761752023159944 13785098108221615618 7064623795024570147 23275986797412198969 27585404044117795 79 222947
28887235021361 7064623795024570147 23275986797412198969 11825169252682319875 21827380103901054344 11013876100024233887 5892016401434133410 7113383132300478325 16247899126459661335 4447973671030
565749 3598226027849693737 16157164111463600376 22389144794393061008 23363342382545078863 22029337619106620753 23275986797412198969 20273622932881166022 24632501112982524137 1114051533259805450
9 18314279648941907257 17478367229135501469 13974417994378291574 18402931114277250192 18016468398829819094 4087316971764079510 23248043085072366034 11539759351159406886 14227897381836174725 787
3940569480520214 17874592324166725 87 21603599513839851316 5892016401434133410 16377603490865502418 5057541143316215800 11539759351159406886 14227897381836174725 16377603490865502418 50575411433
16215800 14100450702387767525 11484408053643426697 18626342501820717469 22532006110822341252 23275986797412198969 6611822391207902327 13849297379608527513 23166199859117762343 20011049378340743
062 17874592324166725 87 22532006110822341252 10467830290603308041 17526240415065979 13 23275986797412198969 21177786310940424039 25072511399808519171 13840331367447076792 5892016401434133410 711
3383132300478325 22532006110822341252 23275986797412198969 11484408053643426697 22529338119213367066 24758512947037093604 16247899126459661335 9881820415216577656 25028933046149972449 170756789
11129971734
解碼後: 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 I
N A REASONABLE AMOUNT OF TIME USING THE PRIVATE KEY THE KEYS FOR THE RSA ALGORITHM ARE GENERATED THE FOLLOWING WAY
PS C:\Users\USER\Documents\GitHub\Mid1_2> 
```

進階版(因為太長的無法截圖所以直接使用文字檔):

請輸入e:723732698112534512672761745123638923636112736572367

請輸入p:389651984374348681198937829437632876251983672816323

請輸入q:672838012783469248520967128763116286378291649376839

(n, d):
(262172666843572177835189692935490626681964526701551493375648501642796261483999546501062577067057342997,
242853588675584071448128850816414130435448893272310264309100496716574692643023247001636249914195987867)

請輸入所要加密之文字: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 KEYS FOR THE RSA ALGORITHM ARE GENERATED THE FOLLOWING WAY

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 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 2600 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 1904 326 1907 426 514 1111 1422 813 626 2200 2426

C =

19799279561486721123529372015399093359502229853225578433403949815553267124655608368312153920280779098753859797373791229435380826642764113978277876063262159295635942657880034214873570231003356388186398412952529791872549956563173916362664815291595163558099762106971988295958773587328884571120802543210419982630391613005754892156408329643938661524859911042786296608816384769016230061544924199256527948133202123583454914140359131780187764006447050166742850060796852344740480046482572640817907189653347259667166804025040202552798553702366693973998443568997933896635888717698700810455934677565456122880913217258316121567516619175683379246213062855001780793542400739788995529760655969299397932739454268514226801802633697682217089741577783084083038406978994863737055418959497602714836072520794237952741879894399025793420360909026563611586222239419704734607750521660824871202020081809488785703567768457615215444245912703046890120735238552639135946031978801156887545690695720067655580207571524849719046705621338915373514718312285820248762240687352442125298587089778984611177250047730528798258271914083921437893799696020612843471793766784086749139898708434414318298485472864762867747354176411502239567195206281582744243713910507881021949697935157954800507166804284490422338847013309903699614321083534934290225946076976421910915698201125993125541597068528373271406456237994726838501717050434903936065297362865659536424628405704394217334600324098990428384495719321045251483666403156259260362498756210556494481259787907282786408081753859797373791229435380826642764113978277876063262159295635942657880034214873570231003356388186398411062149041499186671524576226104627772077377000270548011369347957393098923707553705653591131663833329532496340223704828059722152935349240870872888371529872146754838763487401650886306746500519328116888162011754838444064106270087522400877924628233741794369472923035901730300414851553507757206045565644318933172266133500550153691180587323898464658010784863656051523733707537360032494918166668985760254416244499841284347179376678408674913989870843441431829848547286476286774735417641150223956719520628158274424371391050788102194969793515795480050716680428449042233884701330990369961432108

353493429022594607697642191091155017125432009751541806782838424339124409236474810925740600747437789914850692784250645631671974335252266133500550153691180587323898464658010784863656051523733707537360032494918166668985760254416244499841420080353326310666275623620499432384394597406552899142557973965739887809561997185589413095752046976061099489323266831026957370276173321404731359682411879677060866876235417324064323348739017190881352015741375304563627757372458298317816831962926177290943911984762469119300616015037194340265171199688235119688594611449179317226900535351034405136853107675753112233368321767353923264487538620923771680514341859834815590817173432331592951473763375393580541274682903571522592835998695946536966592078463966153068250158484286116569640316356035576615233014286212386392975440957340578535445818568338603994104367734222156982011259931255415970685283732714064562379947268385017170504349039360652973628656595364246284057043227582195089520980098344248439236549468665216284967431558488149340320496810179914102176050808845663984226613350055015369118058732389846465801078486365605152373370753736003249491816666898576025441624449984217776679687347724776862604889487324041458484001365152005159590365902915312710206467516240309850797054638900252607845931765856710707015238634233043997244181263655768671608842079345945849582132032693550924949817587412078390584491710160529625514051907316389149190610976817982018964047394693509748190842377936668587945366402346999163110481516541215715042622778050454415608397195575163924655393648003729449972111667223026853621130452492560302909538907067234494808319055007659449458413796511904416708384871621211525233610444312991035095932068697744174859257378714707903300219623545060303496533660504867538804762601228348193732457924552937970131727510485695849982628980951264506358140654667563286059503562698289855441264879188268452693346729393304088182316449128359938434579629147765848111622095371878238871424266173622266133500550153691180587323898464658010784863656051523733707537360032494918166668985760254416244499841569820112599312554159706852837327140645623799472683850171705043490393606529736286565953642462840570439421733460032409899042838449571932104525148366640315625926036249875621055649448125978790728278640808122817326557520719572169511410197639563214867279770662665329230657792594927071119193808401565395281294963514329536246703070227627911268590124903773601503985830591015823982523218

48375064957587017238580420702046749019989692734929408292755533961860454410537120466900904855714486462109621068087350428186085671489421733460032409899042838449571932104525148366640315625926036249875621055649448125978790728278640808116857988651175806950921686780214521904225542157991350321164913100192426324403890708365025824225593649332866653617792876394606002144977262934958199698605482312370709854629632467921640865501976356406569184721561863053042188311246447577339569801485635043251227448282716358477270144943470666619896281672002196611770750560724591061907503802427616309930650918541005717853619121503661273920170990809050797972842342949477518165404649807149492421436648668546353647929009990056396878881763613254859341636834909742371315297607363672123600778259562629895717107750619255036306542238135247679029279316317976358244097250491264879188268452693346729393304088182316449128359938434579629147765848111622095371878238871424266173621429201003872675406278436873449281400455968792792882405010389014063225865948181761587802074050197626256668040250402025527985537023666939739984435689979338966358887176987008104559346775654561228809132173537067588561152453917024614776761131848253485573249851892714613994891003257820261635267656928803015209893393934841281135505953867520445457325790945623965218447784576054839968480478835788260688974816142103182678716348978935555098537943492867072981832807894789452682256683128390346606255682716715088326418193006092810076604652954341290854774741795811026638967752703697393095202515952183281497406089552669057234595324969941203708654798948896136168947416476081568931819733854718677972373110173515899343338067239111795586401716364282823809094860622439741806914257030070056509522935532964770644836878065757722531698666804025040202552798553702366693973998443568997933896635888717698700810455934677565456122880913217211166722302685362113045249256030290953890706723449480831905500765944945841379651190441670838487162121258383949415591102303320081790138096619487114084364213033382858741755751210760644559791139297911894018122834819373245792455293797013172751048569584998262898095126450635814065466756328605950356269828985544224819501381031897469518568810499925820933141840620068534893287512116857044053874339162541606604244258343577363455274536804137588368243580027649853506129764306670516458221280299858892582268860646164493925813992821475231629523256675632658226327424199240752744622447167414419581958

847683066574868887411961427247415726570315139810864393162594518901100545215564940237008029940819658973654860265108560720280177583123947010759149706900431388456671605813155056108793529283344937468560641991978998578851849153964007658311550171254320097515418067828384243391244092364748109257406007474377899148506927842506456316719743352522661335005501536911805873238984646580107848636560515237337075373600324949181666689857602544162444998414200803533263106662756236204994323843945974065528991425579739657398878095619971855894130957520469760610994893232668310269573702761733214047313596824118796770608668762354173240643233487390171908813520157413753045636277573724582983178168319629261772909439119847624691193006160150371943402651711996882351196885946114491793172269005353510344051368531076757531122333683217673539232644875386209237716805143185983481559081717343233159295147376337539358054127468290357152259283599869594653696659207846396615306825015848428611656964031635603557661523301428621238639297544095734057853544581856833860399410436773422215698201125993125541597068528373271406456237994726838501717050434903936065297362865659536424628405704322758219508952098009834424843923654946866521628496743155848814934032049681017991410217605080884566398422661335005501536911805873238984646580107848636560515237337075373600324949181666689857602544162444998412647918826845269334672939330408818231644912835993843457962914776584811162209537187823887142426617362253806426940162062910419564504745668038217960234162008565992849301742258723302405790699154210003991514227582195089520980098344248439236549468665216284967431558488149340320496810179914102176050808845663984226613350055015369118058732389846465801078486365605152373370753736003249491816666898576025441624449984817675800462722023467921436659196592481545624088739301228328233999372860555438236041265782102743905096611770750560724591061907503802427616309930650918541005717853619121503661273920170990809050797972842342949477518165404649807149492421436648668546353647929009990056396878881763613254859341636834909742371298532050559146718120976794602122177306766192320958252360523374147873937108332618349609805191855073409421733460032409899042838449571932104525148366640315625926036249875621055649448125978790728278640808129525297918725499565631739163626648152915951635580997621069719882959587735873288845711208025432104192583161215675166191756833792462130628550017807935424007397889955297606559

692993979327394542685142268012
721921755953843069396776177591071933908097068695056737395666062038545022901
011057824658386263437536945 4
195566948207848669139777143229499094116537697476212199690451667345222833214
143709515265113086463376078 77
259214051147862319624761471386922605576876459586547926800876736532715904962
559594660484201189145895075 44
907370763210365944012556075132302135918870924734834513481803571623331777058
616169900659858217984711635 3
109948932326683102695737027617332140473135968241187967706086687623541732406
432334873901719088135201574
226613350055015369118058732389846465801078486365605152373370753736003249491
816166668985760254416244499 84
973586001925803743458801210761453058469328396391824522211555903845403186509
955042519654265657929412 24
186410713530626707980510455587120094932649439818020087118272204106126733631
305141669784904289805005178
114308226876378538036526644047411088113039558754406309189585480319257243275
098116164128774531189708483
200109215095152134974769531394638294823239173735171123816425855193391450503
967959950467206020463349222
243678193732506761203509704860197769077477094949306758076738521093801019001
828590748169160701386748564
131529760736367212360077825956262989571710775061925503630654223813524767902
927931631797635824409725049
193006092810076604652954341290854774741795811026638967752703697393095202515
952183281497406089552669057
635132953624670307022762791126859012490377360150398583059101582398252321848
375064957587017238580420 70
129039833438648102272617703076026541927065833729157652294804961358574337655
042541488533483367283291085
215605472896070372282344353120437976128165763808465109809541576108361766646
117936000793751089356671 86
375630045779426465469688350140224886171158858838854834032424378101116487934
255149778456850975253157 54
513983224264345287529515417610114353952033818548864140162454921477820885669
032512554874330618886930 66
802633697682217089741577783084083038406978994863737055418959497602714836072
525207942379527418798943 902
215839318606475248507817784494154541092013526657913245839922789061665869268
369381467876973679577580602
163643762813918765687164291484584764627163672220101186054588162249893759884
778938478876472760276133583
129853205055914671812097679460212217730676619232095825236052337414787393710
833261834960980519185507340
968859461144917931722690053535103440513685310767575311223336832176735392326
448753862092377168051434 18
598348155908171734323315929514737633753935805412746829035715225928359986 9

5946536966592078463966153068
375630045779426465469688350140224886171158858838854834032424378101116487934255149778456850975253157545139832242643452875295154176101143539520338185488641401624549214778208856690325125548743306188869306696885946114491793172269005353510344051368531076757531122333683217673539232644875386209237716805143418598348155908171734323315929514737633753935805412746829035715225928359986959465369665920784639661530681031826787163489789355550985379434928670729818328078947894526822566831283903466062556827167150883264181685798865117580695092168678021452190422554215799135032116491310019242632440389070836502582422559364932866653617792876394606002144977262934958199698605482312370709854629632467921640865501976356406569181155017125432009751541806782838424339124409236474810925740600747437789914850692784250645631671974335252266133500550153691180587323898464658010784863656051523733707537360032494918166668985760254416244499841979927956148672112352937201539909335950222985322557843340394981555326712465560836831215392028077909875385979737379122943538082664276411397827787606326215929563594265788003421487357023100335638818639841178235049550830508770297807437068343425260210197923092982057878622382205197111425529267398618149681895257455220278874276825969211810761592198675135329554498538424806909072263245093864368212474906000533107215839318606475248507817784494154541092013526657913245839922789061665869268369381467876973679577580602115501712543200975154180678283842433912440923647481092574060074743778991485069278425064563167197433525175876835131085612460019359900802317681387483214445698877167774380837680128298480195315084978078052799252331178170653852083715908081217839202501951248530580908438308615303083556628969019142935142150838912266133500550153691180587323898464658010784863656051523733707537360032494918166668985760254416244499842098933939348412811355059538675204454573257909456239652184477845760548399684804788357882606889748161422480234506783330615541152597549298819406730674010929556435136244999200655484957873345234410390204219798319454728587703207386385600520159328183224906598208192798766315315083103564738418230174869129887984612985320505591467181209767946021221773067661923209582523605233741478739371083326183496098051918550734094217334600324098990428384495719321045251483666403156259260362498756210556494481259787907282786408081115501712543200975154180678283842433912440923647481092574060074743778991485069278425064563167197433525226613350055015369118058732389846465801078486365605152373370753736003249491816666898576025441624449984197992795614867211235293720153990933595022298532255784334039498155532671246556083683121539202807790987538597973737912294353808266427641139782778760632621592956359426578800342148735702310033563881863984117823504955083050877029780743706834342526021019792309298205787862238220519711142552926739861814968189525745522027887427682596921181076159219867513532955449853842480690907226324509386436821247490600053310721583931860647524850781778449415454109201352665791324583992278906166586926836938146787697367957758060211550171254320097515418067828384243391244092364748109257406007474377899148506927842506456316719743352522661335005501536911805873238984646580107848636560515237337075373600324949181666689857602544162444998419799279561486721123529372015399093359502229853225578433403949815553267124655608368312153920280779098753859797373791229435380826642764113978277876063262159295635942657880034214873570231003356388186398411782350495508305087702978074370683434252602101979230929820578786223822051971114255292673986181496818952574552202788742768259692118107615921986751353295544985384248069090722632450938643682124749060005331072158393186064752485078177844941545410920135266579132458399227890616586926836938146787697367957758060211550171254320097515418067828384243391244092364748109257406007474377899148506927842506456316719743352522661335005501536911805873238984646580107848636560515237337075373600324949181666689857602544162444998420989339393484128113550595386752044545732579094562396521844778457605483996848047883578826068897481614224802345067833306155411525975492988194067306740109295564351362449992006554849578733452344103902042197983194547285877032073863856005201593281832249065982081927987663153150831035647384182301748691298879846129853205055914671812097679460212217730676619232095825236052337414787393710833261834960980519185507340942173346003240989904283844957193210452514836664031562592603624987562105564944812597879072827864080811155017125432009751541806782838424339124409236474810925740600747437789914

850692784250645631671974335 25
22661335005501536911805873238984646580107848636560515237337075373600324 94
91816666898576025441624449984
16857988651175806950921686780214521904225542157991350321164913100192426324
40389070836502582422559364 93
10863030623142854739765543392300925903095925108904847165224750962980530 66
39331893711505743324438726396
63890025260784593176585671070701523863423304399724418126365576867160884 20
79345945849582132032693550 92
29525297918725499565631739163626648152915951635580997621069719882959587 73
58732888457112080254321041 9
77436334283747662154957508190581005164722111211562545572444771171341556 06
47617141858083912789822066 4
15340433065535904064302533222778348087965691290140660487527544044639621 32
12003030502497834985449807426
10507881021949697935157954800507166804284490422338847013309903699614321 08
35349342902259460769764219109
解碼後: 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 KEYS FOR THE RSA ALGORITHM ARE GENERATED THE FOLLOWING WAY