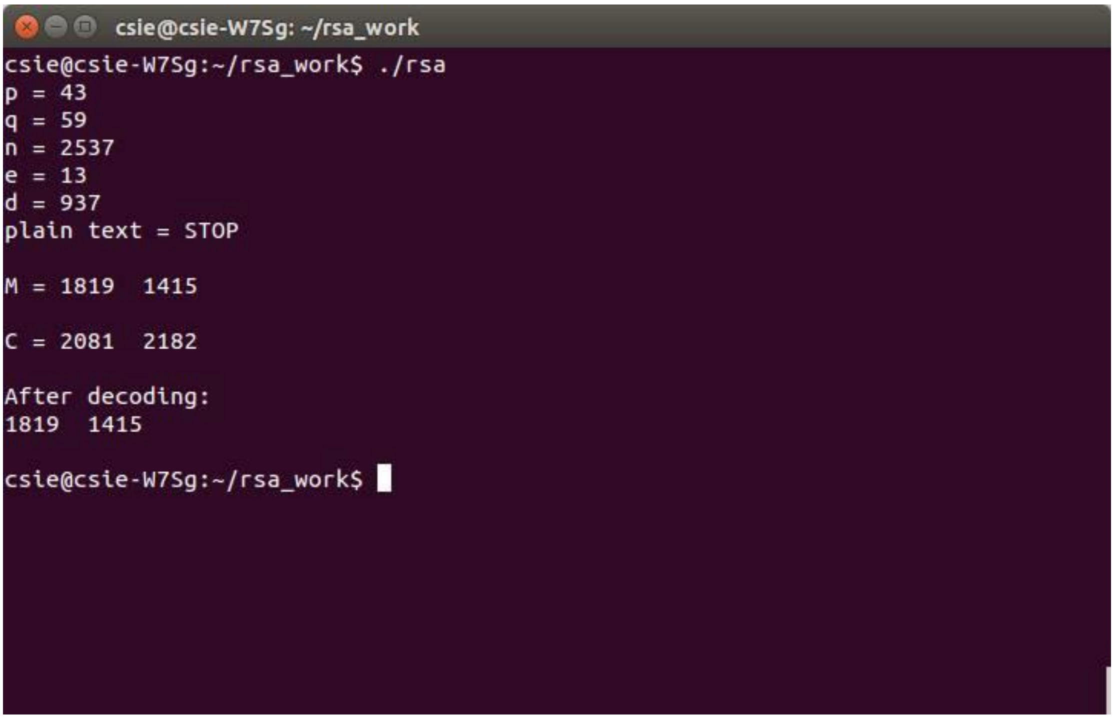
Dear All,

RSA 程式設計作業測資如附圖或文字資料所示，請驗證你的程式是否能有同樣的執行結果：

(1) 基本款 (課本基本範例，如下圖所示)



```
csie@csie-W7Sg:~/rsa_work$ ./rsa
p = 43
q = 59
n = 2537
e = 13
d = 937
plain text = STOP

M = 1819  1415

C = 2081  2182

After decoding:
1819  1415

csie@csie-W7Sg:~/rsa_work$ 
```

(2)中階款 (p, q, e 皆為 10 位數的質數，原始資料 299 個字元，加密區塊 150 個,由於資料太長，截圖無法完整呈現，以下文字顯示)

p = 3896519873

q = 6728380129

n = 26217266885746803617

e = 7237327049

d = 4962162255038558585

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 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 23687113098915059665 19629710640889188379 6926892904584814480 4447973671030565749 7873940569480520214 24616219891185911336 11139922963840576187 25762172624793938442 13423058010932276371 17075678911129971734 13785098108221615618 7113383132300478325 13849297379608527513 26122544274323584668 23962465814835170581 23016435786474490176 23275986797412198969 13423058010932276371 17075678911129971734 22532006110822341252 23275986797412198969 17684193191798997163 22029337619106620753 17269071398983515502 16377603490865502418 5057541143316215800 23899761752023159944 13785098108221615618 7064623795024570147 23275986797412198969 16624251992473247491 24758512947037093604 15815078599831929676 9644192653242922903 9038903785119966624 17435525424429050918 20351174814883381591 27585404044117795579 23275986797412198969 13785098108221615618 7113383132300478325 8304389425183833219 18016468398829819094 22315837888125500979 7113383132300478325 11484408053643426697 18626342501820717469 9354574055652503936 21827380103901054344 11013876100024233887 13974417994378291574 27585404044117795579 9909216201681101901 6926892904584814480 17399063923429626634 21177786310940424039 14100450702387767525 18402931114277250192 23153728852394687769 16533108147687036323 6926892904584814480 9038903785119966624 4943565736594359241 20351174814883381591 12524127530871874887 4160579029389134555 8608256297004769952 4528547931724913054 13000700358701474413 22532006110822341252 23275986797412198969 17684193191798997163 22029337619106620753 17269071398983515502 16377603490865502418 5057541143316215800 23899761752023159944 13785098108221615618 7064623795024570147 23275986797412198969 27585404044117795579 22294728887235021361 7064623795024570147 23275986797412198969 11825169252682319875 21827380103901054344 11013876100024233887 5892016401434133410 7113383132300478325 16247899126459661335

4447973671030565749 3598226027849693737 1615716411463600376
2238914479439306100 8 2336334238254507886 3 2202933761910662075 3
2327598679741219896 9 2027362293288116602 2 2463250111298252413 7
1114051533259805450 9 1831427964894190725 7 1747836722913550146 9
1397441799437829157 4 1840293111427725019 2 1801646839882981909 4
4087316971764079510 2324804308507236603 4 1153975935115940688 6
1422789738183617472 5 7873940569480520214 1787459232416672587
2160359951383985131 6 5892016401434133410 1637760349086550241 8
5057541143316215800 1153975935115940688 6 1422789738183617472 5
1637760349086550241 8 5057541143316215800 1410045070238776752 5
1148440805364342669 7 1862634250182071746 9 2253200611082234125 2
2327598679741219896 9 6611822391207902327 1384929737960852751 3
2316619985911776234 3 2001104937834074306 2 1787459232416672587
2253200611082234125 2 1046783029060330804 1 1752624041506597913
2327598679741219896 9 2117778631094042403 9 2507251139980851917 1
1384033136744707679 2 5892016401434133410 7113383132300478325
2253200611082234125 2 2327598679741219896 9 1148440805364342669 7
2252933811921336706 6 2475851294703709360 4 1624789912645966133 5
9881820415216577656 2502893304614997244 9 1707567891112997173 4

After decoding:
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

(3)進階款（p, q, e 皆為 50 位數的大質數，原始資料 299 個字元，加密區塊 150 個，由於資料太長，截圖無法完整呈現，以下文字顯示)

p = 38965198437434868119893782943763287625198367281632 3

q = 67283801278346924852096712876311628637829164937683 9

n =
2621726668435721778351896929354906266819645267015514933756485016
4279626148399954650106257706705734299 7

e = 723732698112534512672761745123638923636112736572367

d =
242853588675584071448128850816414130435448893272310264309100496716574692643023247001636249914195987867

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 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 =
19799279561486721123529372015399093359502229853225578433403949815553267124655608368312153920280779098
75385979737379122943538082664276411397827787606326215929563594265788003421487357023100335638818639841
2952529791872549956563173916362664815291595163558099762106971988295958773587328884571120802543210419
98263039161300575489215640832964393866152485991104278629660881638476901623006154492419925652794813320
21235834549141403591317801877640064470501667428500607968523447404800464825726408179071896533472596671
666804025040202552798553702366693973998443568997933896635888717698700810455934677565456122880913217
258316121567516619175683379246213062855001780793542400739788995529760655969299397932739454268514226801
80263369768221708974157778308408303840697899486373705541895949760271483607252079423795274187989439902
5793420360909026563611586222239419704734607750521660824871202020

0818094887857035677684576152154442459

127030468901207352385526391359460319788011568875456906957200676555802075715248497190467056213389153735

147183122858202487622406873524421252985870897789846111772500477305287982582719140839214378937996960206

128434717937667840867491398987084344143182984854728647628677473541764115022395671952062815827442437139

105078810219496979351579548005071668042844904223388470133099036996143210835349342902259460769764219109

156982011259931255415970685283732714064562379947268385017170504349039360652973628656595364246284057043

94217334600324098990428384495719321045251483666403156259260362498756210556494481259787907282786408081

75385979737379122943538082664276411397827787606326215929563594265788003421487357023100335638818639841

106214904149918667152457622610462777207737700027054801136934795739309892370755370565359113166383332953

249634022370482805972215293534924087087288837152987214675483876348740165088630674650051932811688816201

175483844406410627008752240087792462823374179436947292303590173030041485155350775720604556564431893317

226613350055015369118058732389846465801078486365605152373370753736003249491816666898576025441624449984

128434717937667840867491398987084344143182984854728647628677473541764115022395671952062815827442437139

105078810219496979351579548005071668042844904223388470133099036996143210835349342902259460769764219109

115501712543200975154180678283842433912440923647481092574060074743778991485069278425064563167197433525

226613350055015369118058732389846465801078486365605152373370753736003249491816666898576025441624449984

142008035332631066627562362049943238439459740655289914255797396573988780956199718558941309575204697606

109948932326683102695737027617332140473135968241187967706086687623541732406432334873901719088135201574

137530456362775737245829831781683196292617729094391198476246911930061601503719434026517119968823511

9688594611449179317226900535351034405136853107675753112233368321

7673539232644875386209237716805143418

5983481559081717343233159295147376337539358054127468290357152259

2835998695946536966592078463966153068

2501584842861165696403163560355766152330142862123863929754409573

40578535445818568338603994104367734222

1569820112599312554159706852837327140645623799472683850171705043

49039360652973628656595364246284057043

2275821950895209800983442484392365494686652162849674315584881493

40320496810179914102176050808845663984

2266133500550153691180587323898464658010784863656051523733707537

36003249491816666898576025441624449984

2177766796873477247768626048894873240414584840013651520051595903

65902915312710206467516240309850797054

6389002526078459317658567107070152386342330439972441812636557686

7160884207934594584958213203269355092

9498175874120783905844917101605296255140519073163891491906109768

1798201896404739469350974819084237793

7366685879453664023469991631104815165412157150426227780504544156

0839719557516392465539364800372944997

2111667223026853621130452492560302909538907067234494808319055007

65944945841379651190441670838487162121

1525233610444312991035095932068697744174859257378714707903300219

62354506030349653366050486753880476260

1228348193732457924552937970131727510485695849982628980951264506

35814065466756328605950356269828985544

1264879188268452693346729393304088182316449128359938434579629147

76584811162209537187823887142426617362

2266133500550153691180587323898464658010784863656051523733707537

36003249491816666898576025441624449984

1569820112599312554159706852837327140645623799472683850171705043

49039360652973628656595364246284057043

9421733460032409899042838449571932104525148366640315625926036249

8756210556494481259787907282786408081

2281732655752071957216951141019763956321486727977066266532923065

77925949270711191938084015653952812949

6351329536246703070227627911268590124903773601503985830591015823

9825232184837506495758701723858042070

2046749019989692734929408292755533961860454410537120466900904855

71448646210962106808735042818608567148
9421733460032409899042838449571932104525148366640315625926036249
8756210556494481259787907282786408081
1685798865117580695092168678021452190422554215799135032116491310
01924263244038907083650258242255936493
3286665361779287639460600214497726293495819969860548231237070985
462963246792164086550197635640656918
4721561863053042188311246447577339569801485635043251227448282716
3584772701449434706666198962816720021
9661177075056072459106190750380242761630993065091854100571785361
9121503661273920170990809050797972842
3429494775181654046498071494924214366486685463536479290099900563
9687888176361325485934163683490974237
1315297607363672123600778259562629895717107750619255036306542238
13524767902927931631797635824409725049
1264879188268452693346729393304088182316449128359938434579629147
76584811162209537187823887142426617362
1429201003872675406278436873449281400455968792792882405010389014
06322586594818176158780207405019762625
6668040250402025527985537023666939739984435689979338966358887176
98700810455934677565456122880913217
3537067588561152453917024614776761131848253485573249851892714613
994891003257820261635267656928803015
2098933939348412811355059538675204454573257909456239652184477845
76054839968480478835788260688974816142
1031826787163489789355550985379434928670729818328078947894526822
56683128390346606255682716715088326418
1930060928100766046529543412908547747417958110266389677527036973
93095202515952183281497406089552669057
2345953249699412037086547989488961361689474164760815689318197338
54718677972373110173515899343338067239
1117955864017163642828238090948606224397418069142570300700565095
22935532964770644836878065757722531698
6668040250402025527985537023666939739984435689979338966358887176
98700810455934677565456122880913217
2111667223026853621130452492560302909538907067234494808319055007
65944945841379651190441670838487162121
2583839494155911023033200817901380966194871140843642130333828587

41755751210760644559791139297911894018

1228348193732457924552937970131727510485695849982628980951264506

35814065466756328605950356269828985544

2248195013810318974695185688104999258209331418406200685348932875

12116857044053874339162541606604244425

8343577363455274536804137588368243580027649853506129764306670516

4582212802998588925822688606461644939

2581399282147523162952325667563265822632742419924075274462244716

74144195884768306657486888741196142724

7415726570315139810864393162594518901100545215564940237008029940

8196589736548602651085607202801775831

2394701075914970690043138845667160581315505610879352928334493746

85606419919789985788518491539640076583

1155017125432009751541806782838424339124409236474810925740600747

43778991485069278425064563167197433525

2266133500550153691180587323898464658010784863656051523733707537

36003249491816666898576025441624449984

1420080353326310666275623620499432384394597406552899142557973965

73988780956199718558941309575204697606

1099489323266831026957370276173321404731359682411879677060866876

23541732406432334873901719088135201574

1375304563627757372458298317816831962926177290943911984762469119

30061601503719434026517119968823511

9688594611449179317226900535351034405136853107675753112233368321

7673539232644875386209237716805143418

5983481559081717343233159295147376337539358054127468290357152259

2835998695946536966592078463966153068

2501584842861165696403163560355766152330142862123863929754409573

40578535445818568338603994104367734222

1569820112599312554159706852837327140645623799472683850171705043

49039360652973628656595364246284057043

2275821950895209800983442484392365494686652162849674315584881493

40320496810179914102176050808845663984

2266133500550153691180587323898464658010784863656051523733707537

36003249491816666898576025441624449984

1264879188268452693346729393304088182316449128359938434579629147

76584811162209537187823887142426617362

2538064269401620629104195645047456680382179602341620085659928493

01742258723302405790699154210003991514

22758219508952098009834424843923654946866521628496743155848814934

0320496810179914102176050808845663984

22661335005501536911805873238984646580107848636560515237337075373

6003249491816666898576025441624449984

81767580046272202346792143665919659248154562408873930122832823399

93728605554382360412657821027439050

96611770750560724591061907503802427616309930650918541005717853619

121503661273920170990809050797972842

34294947751816540464980714949242143664866854635364792900999005639

687888176361325485934163683490974237

12985320505591467181209767946021221773067661923209582523605233741

4787393710833261834960980519185507340

94217334600324098990428384495719321045251483666403156259260362498

756210556494481259787907282786408081

29525297918725499565631739163626648152915951635580997621069719882

95958773587328884571120802543210419

25831612156751661917568337924621306285500178079354240073978899552

9760655969299397932739454268514226801

72192175595384306939677617759107193390809706869505673739566606203

854502290110578246583862634375369454

19556694820784866913977714322949909411653769747621219969045166734

5222833214370951526511308646337607877

25921405114786231962476147138692260557687645958654792680087673653

2715904962559466048420118914589507544

90737076321036594401255607513230213591887092473483451348180357162

333177705861699006598582179847116353

10994893232668310269573702761733214047313596824118796770608668762

3541732406432334873901719088135201574

22661335005501536911805873238984646580107848636560515237337075373

6003249491816666898576025441624449984

97358600192580374345880121076145305846932839639182452221155590384

540318650995504251965426565792941224

18641071353062670798051045558712009493264943981802008711827220410

6126733631305141669784904289805005178

11430822687637853803652664404741108811303955875440630918958548031

9257243275098116164128774531189708483

2001092150951521349747695313946382948232391737351711238164258551

93391450503967959950467206020463349222

2436781937325067612035097048601977690774770949493067580767385210

93801019001828590748169160701386748564

1315297607363672123600778259562629895717107750619255036306542238

13524767902927931631797635824409725049

1930060928100766046529543412908547747417958110266389677527036973

93095202515952183281497406089552669057

6351329536246703070227627911268590124903773601503985830591015823

9825232184837506495758701723858042070

1290398334386481022726177030760265419270658337291576522948049613

58574337655042541488533483367283291085

2156054728960703722823443531204379761281657638084651098095415761

0836176664611793600079375108935667186

3756300457794264654696883501402248861711588588388548340324243781

0111648793425514977845685097525315754

5139832242643452875295154176101143539520338185488641401624549214

7782088566903251255487433061888693066

8026336976822170897415777830840830384069789948637370554189594976

0271483607252079423795274187989439902

2158393186064752485078177844941545410920135266579132458399227890

61665869268369381467876973679577580602

1636437628139187656871642914845847646271636722201011860545881622

49893759884778938478876472760276133583

1298532050559146718120976794602122177306766192320958252360523374

14787393710833261834960980519185507340

9688594611449179317226900535351034405136853107675753112233368321

7673539232644875386209237716805143418

5983481559081717343233159295147376337539358054127468290357152259

2835998695946536966592078463966153068

3756300457794264654696883501402248861711588588388548340324243781

0111648793425514977845685097525315754

5139832242643452875295154176101143539520338185488641401624549214

7782088566903251255487433061888693066

9688594611449179317226900535351034405136853107675753112233368321

7673539232644875386209237716805143418

5983481559081717343233159295147376337539358054127468290357152259

2835998695946536966592078463966153068

1031826787163489789355550985379434928670729818328078947894526822

56683128390346606255682716715088326418

1685798865117580695092168678021452190422554215799135032116491310

01924263244038907083650258242255936493

3286665361779287639460600214497726293495819969860548231237070985

462963246792164086550197635640656918

1155017125432009751541806782838424339124409236474810925740600747

43778991485069278425064563167197433525

2266133500550153691180587323898464658010784863656051523733707537

36003249491816666898576025441624449984

1979927956148672112352937201539909335950222985322557843340394981

5553267124655608368312153920280779098

7538597973737912294353808266427641139782778760632621592956359426

5788003421487357023100335638818639841

1782350495508305087702978074370683434252602101979230929820578786

22382205197111425529267398618149681895

2574552202788742768259692118107615921986751353295544985384248069

09072263245093864368212474906000533107

2158393186064752485078177844941545410920135266579132458399227890

61665869268369381467876973679577580602

1155017125432009751541806782838424339124409236474810925740600747

43778991485069278425064563167197433525

1758768351310856124600193599008023176813874832144456988771677743

80837680128298480195315084978078052799

2523311781706538520837159080812178392025019512485305809084383086

1530308355662896901914293514215083891

2266133500550153691180587323898464658010784863656051523733707537

36003249491816666898576025441624449984

2098933939348412811355059538675204454573257909456239652184477845

76054839968480478835788260688974816142

2480234506783330615541152597549298819406730674010929556435136244

99920065548495787334523441039020421979

8319454728587703207386385600520159328183224906598208192798766315

3150831035647384182301748691298879846

1298532050559146718120976794602122177306766192320958252360523374

14787393710833261834960980519185507340

9421733460032409899042838449571932104525148366640315625926036249

8756210556494481259787907282786408081

1155017125432009751541806782838424339124409236474810925740600747

```
43778991485069278425064563167197433525
2266133500550153691180587323898464658010784863656051523733707537
36003249491816666898576025441624449984
1685798865117580695092168678021452190422554215799135032116491310
01924263244038907083650258242255936493
1086303062314285473976554339230092590309592510890484716522475096
29805306639331893711505743324438726396
6389002526078459317658567107070152386342330439972441812636557686
7160884207934594584958213203269355092
2952529791872549956563173916362664815291595163558099762106971988
295958773587328884571120802543210419
7743633428374766215495750819058100516472211121156254557244477117
1341556606476171418580839127898220664
1534043306553590406430253322277834808796569129014066048752754404
46396213212003030502497834985449807426
1050788102194969793515795480050716680428449042233884701330990369
96143210835349342902259460769764219109
```

After decoding:

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