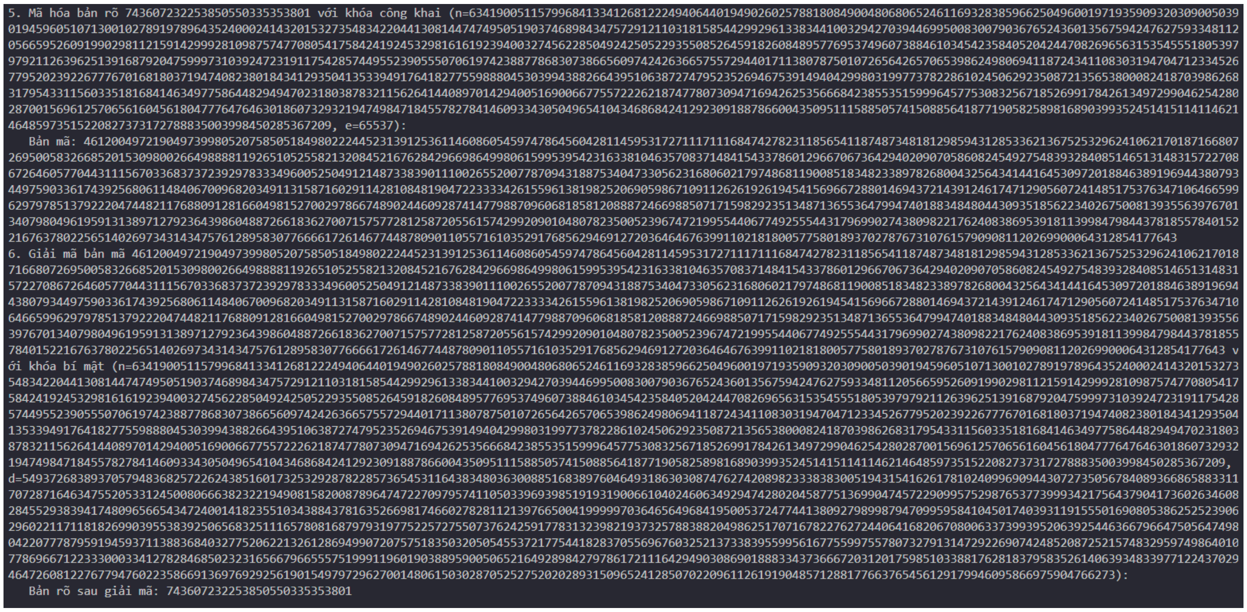
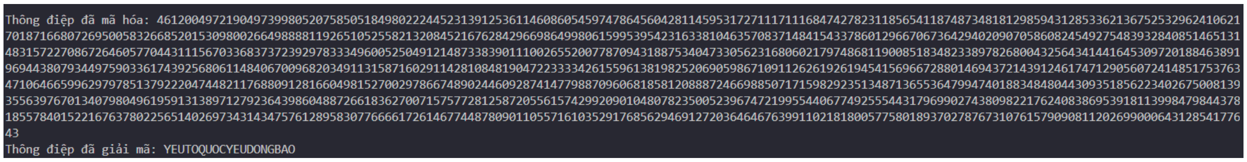
Bài tập Giữa kỳ

Họ và tên: Đinh Xuân Hòa
MSSV: 22028306

1. Hệ mật RSA(2048 bits)





1. Sinh 2 số nguyên tố p và q với độ dài 2048 bit:

p =
2363230886454322512435508029285066691532800027126081938956666158434059694542

272036172553979989371145720967988467665212049949406807429341125009999707891530844399741647548189381140996934402294746494761943209399960679899070606129633907611906534420480085679368804106327375719079332387295118371039725210701064639988871700857315137504363041349428846212564117713795700467217391589207387124735881349003177680636658584927827792119235986713375197173433952388202599829615245333483280132126661562779181650497633358267150149336957959174801644345771975921936647851904915579346072877547613960990442774685520306985963519473491438230 9

q =

268357211643211453318063826548658512086109497625561178535000175265698385129151428389184933271185792172570504022898689155729437497518138220637990578863815129860996617677017033635930972775121700815845433197892575625181593157852279106413965465069393309748769977817451481415810382494733906322020378247127109944242336263441214918687277860887003433811072364890092490259060477706705650990726625073060418076234819295379168553784965418933854073099400217616541017787241963119292213743761812107135228614408973949465283436159940270419300322839273339821565681434776077748495075051979666505890511589264156245828849142691913121061019

2. Tính n = p * q và ϕ(n) = (p-1)*(q-1):

n =

634190051157996841334126812224940644019490260257881808490048068065246116932838596625049600197193590932030900503901945960510713001027891978964352400024143201532735483422044130814474749505190374689843475729121103181585442992961338344100329427039446995008300790367652436013567594247627593348112056659526091990298112159142999281098757477080541758424192453298161619239400327456228504924250522935508526459182608489577695374960738846103454235840520424470826965631535455518053979792112639625139168792047599973103924723191175428574495523905550706197423887786830738665609742426366575572944017113807875010726564265706539862498069411872434110830319470471233452677952023922677767016818037194740823801843412935041353394917641827755988804530399438826643951063872747952352694675391494042998031997737822861024506292350872135653800082418703986268317954331156033518168414634977586448294947023180387832115626414408970142940051690066775572226218747780730947169426253566684238553515999645775308325671852699178426134972990462542802870015696125706561604561804777647646301860732932194749847184557827841460933430504965410434686842412923091887866004350951115885057415088564187719058258981689039935245141511411462146485973515220827373172788835003998450285367209

ϕ(n) =

634190051157996841334126812224940644019490260257881808490048068065246116932838596625049600197193590932030900503901945960510713001027891978964352400024143201532735483422044130814474749505190374689843475729121103181585442992961338344100329427039446995008300790367652436013567594247627593348112056659526091990298112159142999281098757477080541758424192453298161619239400327456228504924250522935508526459182608489577695374960738846103454235840520424470826965631

535455518053979792112639625139168792047599973103924723191175428574495523905550706197423887786830738665609742426366575572944017113807875010726564265706539862498018943842405246459863309008285736159828084972643950079574970515629913366385075071840709361790629537081522074243432917790571513246046640719038795620426197221567934919494639263849503225729337018107267919666820729099000804309309509268450899023126442316463276337357579410216854582835623801124139254989955850585394625437378252526182482150182043921672766768109161119641274477491863496002670441222006796431266277191174409428505088745885782701451257833464311056780807492695669376329267962608345527734977218159336804505841752278423737039836802665316883047067043278314498543177488703695774559634154102345136090454534524058878800
3. Chọn e = 65537 sao cho gcd(e, ϕ(n)) = 1.
4. Tính d là nghịch đảo của e modulo ϕ(n):
d =
549372683893705794836825722624385160173253292878228573654531164383480363008851683897604649318630308747627420898233383830051943154162617810240996909443072735056784089366865883311707287164634755205331245008066638232219490815820087896474722709795741105033969398519193190066104024606349294742802045877513699047457229099575298765377399934217564379041736026346082845529383941748096566543472400141823551034388437816352669817466027828112139766500419999970364656496841950053724774413809279899879470995958410450174039311915550169080538625252390629602211711818269903955383925065683251116578081687979319775225727550737624259177831323982193732578838820498625170716782276272440641682067080063373993952063925446366796647505647498042207778795919459371138836840327752062213261286949907207575183503205054553721775441828370556967603252137338395599561677559975578073279131472922690742485208725215748329597498640107786966712233300033412782846850232316566796655575199911960190388959005065216492898427978617211164294903086901888334373666720312017598510338817628183795835261406393483397712243702946472608122767794760223586691369769292561901549797296270014806150302870525275202028931509652412850702209611261919048571288177663765456129179946095866975904766273

Thông điệp gốc: YEUTOQUOCYEUDONGBAO
Chuyển 'YEUTOQUOCYEUDONGBAO' thành số: 74360723225385050335353801
5. Mã hóa bản rõ 74360723225385050335353801 với khóa công khai (n=6341900511579968413341268122249406440194902602578818084900480680652461169328385966250496001971935909320309005039019459605107130010278919789643524000241432015327354834220441308144747495051903746898434757291211031815854429929613383441003294270394469950083007903676524360135675942476275933481120566595260919902981121591429992810987574770805417584241924532981616192394003274562285049242505229355085264591826084895776953749607388461034542358405204244708269656315354555180539797921126396251391687920475999731039247231911754285744955239055315354555180539797921126396251391687920475999731039247231911754285744955239055507061974238877868307386656097424263665755729440171138078750107265642657065398624980694118724341108303194704712334526779520239226777670168180371947408

2380184341293504135339491764182775598880453039943882664395106387274795235269
4675391494042998031997737822861024506292350872135653800082418703986268317954
3311560335181684146349775864482949470231803878321156264144089701429400516900
6677557222621874778073094716942625356668423855351599964577530832567185269917
8426134972990462542802870015696125706561604561804777647646301860732932194749
8471845578278414609334305049654104346868424129230918878660043509511158850574
1508856418771905825898168903993524514151141146214648597351522082737317278883
5003998450285367209, e=65537):

Bản mã:

4612004972190497399805207585051849802224452313912536114608605459747864560428
1145953172711171116847427823118565411874873481812985943128533621367525329624 1
0621701871668072695005832668520153098002664988881192651052558213208452167628
4296698649980615995395423163381046357083714841543378601296670673642940209070
5860824549275483932840851465131483157227086726460577044311156703368373723929
7833349600525049121487338390111002655200778709431887534047330562316806021797
4868119008518348233897826800432564341441645309720188463891969443807934497590
3361743925680611484067009682034911315871602911428108481904722333342615596138
1982520690598671091126261926194541569667288014694372143912461747129056072414
8517537634710646659962979785137922204744821176880912816604981527002978667489
0244609287414779887096068185812088872466988507171598292351348713655364799474
0188348480443093518562234026750081393556397670134079804961959131389712792364
3986048872661836270071575772812587205561574299209010480782350052396747219955
4406774925554431796990274380982217624083869539181139984798443781855784015221
6763780225651402697343143475761289583077666617261467744878090110557161035291
7685629469127203646467639911021818005775801893702787673107615790908112026990
0064312854177643

6. Giải mã bản mã

4612004972190497399805207585051849802224452313912536114608605459747864560428
1145953172711171116847427823118565411874873481812985943128533621367525329624 1
0621701871668072695005832668520153098002664988881192651052558213208452167628
4296698649980615995395423163381046357083714841543378601296670673642940209070
5860824549275483932840851465131483157227086726460577044311156703368373723929
7833349600525049121487338390111002655200778709431887534047330562316806021797
4868119008518348233897826800432564341441645309720188463891969443807934497590
3361743925680611484067009682034911315871602911428108481904722333342615596138
1982520690598671091126261926194541569667288014694372143912461747129056072414
8517537634710646659962979785137922204744821176880912816604981527002978667489
0244609287414779887096068185812088872466988507171598292351348713655364799474
0188348480443093518562234026750081393556397670134079804961959131389712792364
3986048872661836270071575772812587205561574299209010480782350052396747219955
4406774925554431796990274380982217624083869539181139984798443781855784015221
6763780225651402697343143475761289583077666617261467744878090110557161035291
7685629469127203646467639911021818005775801893702787673107615790908112026990
0064312854177643 với khóa bí mật

(n=63419005115799684133412681222494064401949026025788180849004806806524611693
28385966250496001971935909320309005039019459605107130010278919789643524000241
43201532735483422044130814474749505190374689843475729121103181585442992961338
38344100329427039446995008300790367652436013567594247627593348112056659526091
19902981121591429992810987574770805417584241924532981616192394003274562285049
24250522935508526459182608489577695374960738846103454235840520424470826965631
53545555180539797921126396251391687920475999731039247231911754285744955239055
55070619742388778683073866560974242636657557294401711380787501072656426570653
98624980694118724341108303194704712334526779520239226777670168180371947408238
01843412935041353394917641827755988804530399438826643951063872747952352694675
39149404299803199773782286102450629235087213565380008241870398626831795433115
60335181684146349775864482949470231803878321156264144089701429400516900667755
72226218747780730947169426253566684238553515999645775308325671852699178426134
97299046254280287001569612570656160456180477647646301860732932194749847184557
82784146093343050496541043468684241292309188786600435095111588505741508856418
77190582589816890399352451415114114621464859735152208273731727888350039845028
5367209,
d=54937268389370579483682572262438516017325329287822857365453116438348036300885
16838976046493186303087476274208982333838300519431541626178102409969094430727
35056784089366865883311707287164634755205331245008066638232219490815820087896
47472270979574110503396939851919319006610402460634929474280204587751369904745
72290995752987653773999342175643790417360263460828455293839417480965665434
72400141823551034388437816352669817466027828112139766500419999970364656496841
95005372477441380927989987947099595841045017403931191555016908053862525239062
96022117118182699039553839250656832511165780816879793197752257275507376242591
77831323982193732578838820498625170716782276272440641682067080063373993952
06392544636679664750564749804220777879591945937113883684032775206221326128
69499072075751835032050545537217754418283705569676032521373383955995616775599
75578073279131472922690742485208725215748329597498640107786966712233300033412
78284685023231656679665557519991196019038895900506521649289842797861721116
42949030869018883343736667203120175985103388176281837958352614063934833977122
43702946472608122767794760223586691369769292561901549797296270014806150302870
52527520202893150965241285070220961126191904857128817766376545612917994609586
6975904766273):

Bản rõ sau giải mã: 74360723225385055033535380 1

Thông điệp đã mã hóa:
46120049721904973998052075850518498022244523139125361146086054597478645604281145953172711171116847427823118565411874873481812985943128533621367525329624106217018716680726950058326685201530980026649888811926510525582132084521676284296698649980615995395423163381046357083714841543378601296670673642940209070586082454927548393284085146513148315722708672646057704431115670336837372392978333496005250491214873383901110026552007787094318875340473305623168060217974868119008518348233897826800432564341441645309720188463891969443807934497590

336174392568061148406700968203491131587160291142810848190472233334261559613819825206905986710911262619261945415696672880146943721439124617471290560724148517537634710646659962979785137922204744821176880912816604981527002978667489024460928741477988709606818581208887246698850717159829235134871365536479947401883484804430935185622340267500813935563976701340798049619591313897127923643986048872661836270071575772812587205561574299209010480782350052396747219955440677492555443179699027438098221762408386953918113998479844378185578401522167637802256514026973431434757612895830776666172614677448780901105571610352917685629469127203646467639911021818005775801893702787673107615790908112026990006431285417764 3
Thông điệp đã giải mã: YEUTOQUOCYEUDONGBAO

2. Hệ mật Elgamal(1024 bits)

```
1. Khởi tạo
Sinh số nguyên tố p với độ dài 1024 bit:
   p = 24210346102343583208403403379810698390656295933988822515277286385585306205864895766856759215457994630393933288916825301120842280865628904854244533656696901359659854389957772994340571201819812037234785124873221674787654993815914827091435812141771073337655643232697389456736618081021969238316712810171121908411
Chọn phần tử sinh g = 2.
Chọn khóa riêng x trong khoảng từ 1 đến p-2: x = 19743090338757259141076687398001094438733778197523322914536951717542785862554818133372204896896170981030878308508608850821386541728241556301169188146173470137321713331209231330334139146604978872509751946009261682911867547010760653011283198045919996614984419215125266618761768801654043193554585495240690936406 và tính khóa công khai y = g^x mod p:
   y = 10459352854832079180727989491310700570097281604819008634563074837143950818687214485195692848977373742715868954867147572395436454044956053420689683560131954787749299134576202231404852497453836692107111653271426095478480421502539193118720998124106645214789734612502397195541605472733823171398968827516887995952

Thông điệp gốc: YEUTOQUOCYEUDONGBAO
Chuyển 'YEUTOQUOCYEUDONGBAO' thành số: 743607232253850550335353801
2. Mã khóa
Chọn ngẫu nhiên k trong khoảng từ 1 đến p-2 và k phải khác 0 module p-1:
   k = 488752980212065696629521932365755437022688046268297778963514558176848197444035440872273960232928070058250143681450916172688858088547428479566423706109261776651452149631202829709206766566579356366367091816048722934631150861713753285036229646305263094434854222061487702007017702049091073465925839283879827125 03
Tính c1 = g^k mod p:
   c1 = 22532903959049597770951824253424723986416604309828967475721432719721808305857153629109103976609122022938120501837305087278265155280406936571437897848329560665573450553995103768707509585533439011061154984329088930499224026289512231354441643193649685491050437508780000568082479272971721886350170920487895736 3, 3873161899723858223939696937951937177700179225302931524051640663858453175849405402132523339365173258468112920104805984595810988765833312952723576208404598487835387134065638828657363875271566338288999477909895127860270382908911389339213574971105166143035919346413155880449598164495570556718573862007443258827 1
3. Giải mã bản mã (c1, c2) = (22532903959049597770951824253424723986416604309828967475721432719721808305857153629109103976609122022938120501837305087278265155280406936571437897848329560665573450553995103768707509585533439011061154984329088930499224026289512231354441643193649685491050437508780000568082479272971721886350170920487895736, 3873161899723858223939696937951937177700179225302931524051640663858453175849405402132523339365173258468112920104805984595810988765833312952723576208404598487835387134065638828657363875271566338288999477909895127860270382908911389339213574971105166143035919346413155880449598164495570556718573862007443258827 1) với khóa bí mật x = 19743090338757259141076687398001094438733778197523322914536951717542785862554818133372204896896170981030878308508608850821386541728241556301169188146173470137321713331209231330334139146604978872509751946009261682911867547010760653011283198045919996614984419215125266618761768801654043193554585495240690936406:
   Bản rõ sau giải mã: m = 743607232253850550335353801

Thông điệp đã mã hóa: (22532903959049597770951824253424723986416604309828967475721432719721808305857153629109103976609122022938120501837305087278265155280406936571437897848329560665573450553995103768707509585533439011061154984329088930499224026289512231354441643193649685491050437508780000568082479272971721886350170920487895736, 3873161899723858223939696937951937177700179225302931524051640663858453175849405402132523339365173258468112920104805984595810988765833312952723576208404598487835387134065638828657363875271566338288999477909895127860270382908911389339213574971105166143035919346413155880449598164495570556718573862007443258827 1)
Thông điệp đã giải mã: YEUTOQUOCYEUDONGBAO
```

1. Khởi tạo

Sinh số nguyên tố p với độ dài 1024 bit:

p =

24210346102343583208403403379810698390656295933988822515277286385585306205864895766856759215457994630393933288916825301120842280865628904854244533656696901359659854389957772994340571201819812037234785124873221674787654993815914827091435812141771073337655643232697389456736618081021969238316712810171121908411

Chọn phần tử sinh g = 2.

Chọn khóa riêng x trong khoảng từ 1 đến p-2: x =

19743090338757259141076687398001094438733778197523322914536951717542785862554818133372204896896170981030878308508608850821386541728241556301169188146173470137321713331209231330334139146604978872509751946009261682911867547010760653011283198045919996614984419215125266618761768801654043193554585495240690936406 và tính khóa công khai y = g^x mod p:

y =
104593528548320791807279894913107005700972816048190086345630748371439508186872144851956928489773737427158689548671475723954364540449560534206896835601319547877492991345762022314048524974538366921071116532714260954784804215025391931187209981241066452147897346125023971955416054727338231713989688275168879959952

Thông điệp gốc: YEUTOQUOCYEUDONGBAO
Chuyển 'YEUTOQUOCYEUDONGBAO' thành số: 74360723225385050335353801
2. Mã khóa
Chọn ngẫu nhiên k trong khoảng từ 1 đến p-2 và k phải khác 0 module p-1:
k =
488752980212065696629521932365755437022688046268297789635145581768481974440354408722739602329280700582501436814509161726888580885474284795664237061092617766514521496312028297092067665665793563663670918160487229346311508617137532850362296463052630944348542220614877020070177020490910734659258392838798271250 3
Tính c1 = g^k mod p:
c1 =
225329039590495977709518242534247239864166043098289674757214327197218083058571536291091039766091220229381205018373050872782651552804069365714378978483295606655734505539951037687075095855334390110611549843290898390499224026289512231354441643193649968549105043750878000056808247927297172188635017092048789573 63
Tính c2 = (m * y^k) mod p:
c2 =
387316189972385822393969693795193717770017922530293152405164066385845317584940540213252339365173258468112920104805984595810988765833312952723576208404598487835387134065638828657363875271566338288999477909895127860270382908913189339213574971105166143035919346413155880449598164495570556718573862007443258827 1
3. Giải mã bản mã (c1, c2) =
(225329039590495977709518242534247239864166043098289674757214327197218083058571536291091039766091220229381205018373050872782651552804069365714378978483295606655734505539951037687075095855334390110611549843290898390499224026289512231354441643193649968549105043750878000056808247927297172188635017092048789573 63,
387316189972385822393969693795193717770017922530293152405164066385845317584940540213252339365173258468112920104805984595810988765833312952723576208404598487835387134065638828657363875271566338288999477909895127860270382908913189339213574971105166143035919346413155880449598164495570556718573862007443258827 1) với khóa bí mật x =
197430903387572591410766873980010944387337781975233229145369517175427858625548181333722048968961709810308783085086088508213865417282415563011691881461 73

4701373217133312092313303341391466049788725097519460092616829118675470107606
5301128319804591999661498441921512526661876176880165404319355458549524069093
6406:
Bản rõ sau giải mã: m = 74360723225385055033535380 1

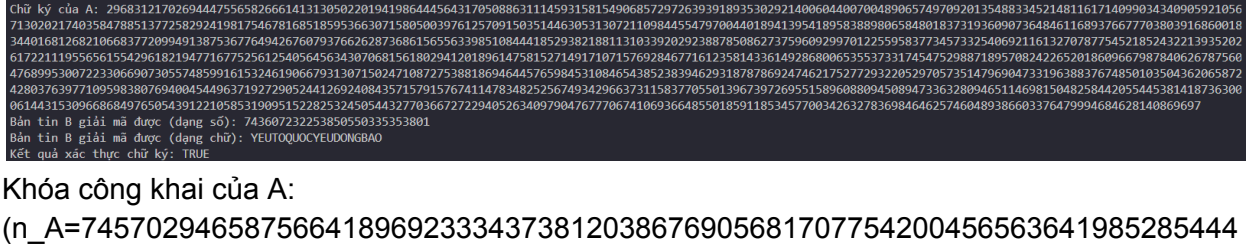
Thông điệp đã mã hóa:
(2253290395904959770951824253424723986416604309828967475721432719721808305857153629109103976609122022938120501837305087278265155280406936571437897848329560665573450553995103768707509585533439011061154984329089839049922402628951223135444164319364996854910504375087800056808247927297172188635017092048789573 63,
3873161899723858223939696937951937177700179225302931524051640663858453175849405402132523393651732584681129201048059845958109887658333129527235762084045984878353871340656388286573638752715663382889994779098951278602703829089131893392135749711051661430359193464131558804495981644955705567185738620074432588271)
Thông điệp đã giải mã: YEUTOQUOCYEUDONGBAO

3. Hệ mật đường cong Elliptic(128 bits)

```
Bước 1: Chọn khóa bí mật t = 123456789
Kết quả M = t * P = (20162976142060345300934533123365247504 0, 183825641330351009968507574913199203265)
Bước 2: Khóa công khai s = 2147483647
Kết quả B = s * P = (132508547270770099151385124194011893195, 185079121696666042887589513037566065636)
Bước 3a: Số ngẫu nhiên k = 987654321
Bước 3b: Mã hóa, M1 = k * P = (27495120085390960734948634008445212269 0, 704118170764350106913599567164240263 25)
Bước 3c: Mã hóa, M2 = M + k * B = (14315320564785094877758319208261825692 9, 24326440668735111862635014464422995093 2)
Bước 4: Giải mã, tính lại M từ M1 và M2
Kết quả M (sau giải mã) = (20162976142060345300934533123365247504 0, 183825641330351009968507574913199203265)
Giải mã thành công, M khớp với giá trị ban đầu.
```

Bước 1: Chọn khóa bí mật t = 123456789
Kết quả M = t * P = (20162976142060345300934533123365247504 0,
183825641330351009968507574913199203265)
Bước 2: Khóa công khai s = 2147483647
Kết quả B = s * P = (132508547270770099151385124194011893195,
185079121696666042887589513037566065636)
Bước 3a: Số ngẫu nhiên k = 987654321
Bước 3b: Mã hóa, M1 = k * P = (27495120085390960734948634008445212269 0,
704118170764350106913599567164240263 25)
Bước 3c: Mã hóa, M2 = M + k * B = (14315320564785094877758319208261825692 9,
24326440668735111862635014464422995093 2)
Bước 4: Giải mã, tính lại M từ M1 và M2
Kết quả M (sau giải mã) = (20162976142060345300934533123365247504 0,
183825641330351009968507574913199203265)
Giải mã thành công, M khớp với giá trị ban đầu.

4. Sơ đồ chữ ký RSA(2048 bits)



Khóa công khai của A:

(n_A=74570294658756641896923334373812038676905681707754200456563641985285444209668245041607245690294755118828866529198227543226802050904294960898905295364691977260714400811326857678492584190254565724174500458335983031740113096847900802532411568822759075671762245937658185826539149160017252341942579398347988838076910605664592643515896051353115074664897834449186038123216162293665500105074182150108630239354561385946099457858090391377446370912619092787035285685579779979831362660283242391608385684406770009040845696920654324060842987932131315575848252090462866955853194122903353404790882026516816053611675660382312206557750538699389217088264106845031119362444556950922544722921509475384950161579342494985127616323113106638291495302613909478539547683269879931006584313253026528251746080042926832994491652915217494883897301968069473779144518691210226109601425669251487966583234413459533508753370245083917737871664656436528185496960994042093354423725135079791633620631421261809437307760504459851163149495605219399924587145859852480986644653545499071433189434469364694503504154891878199615247463026822569999747641069521902145592188560733332258411573582313620539393629727087853480216134721025063326505538066551066418211217815227372852928576 3, e_A=65537)

Khóa bí mật của A:

(d_A=74236908993635936095989533055907237918062076343755665571937047128918985031594289935374263970239574636813869536765630984486465248778549833359601096949416551023693562974402565729855761116482244970181792129489712493588128750004950546958854784924961614253213384765791187689498634737318103684632652776699904151473961205969117723474603845117235515710875679861456419841175389921247405112921647222487583306126995442367925466573833482605291836708764392770186810778525559969429337769891931578598319995050024189426886505892098929725483705996683460877877086887702979374882397512814979267017748391091109802807602425603643492646967320363403168501730034360947402058443230055492502067864574010692232927265076897044527508924797372257324976759947598003594607917216615826645156054164597485059840613664306467247721955882347677519969372559768382551538397059899617824540900046282373104459578404243546355054161953011042941536498061041054545109176159320970575020349245127720520377324223440193778189600360919398122834631637380186013976101153219486058917357244262654917343442012618000685839036021897745767749145813368627487021825842832324246821404445850741305380013204419875610038846621645562111647108663863942658037664514648984890232569538501545898567883641374273Khóa bí mật của A:

(d_A=74236908993635936095989533055907237918062076343755665571937047128918985031594289935374263970239574636813869536765630984486465248778549833359601096949416551023693562974402565729855761116482244970181792129489712493588128750004950546958854784924961614253213384765791187689498634737318103684632652776699904151473961205969117723474603845117235515710875679861456419841175389921247405112921647222487583306126995442367925466573833482605291836708764392770186810778525559969429337769891931578598319995050024189426886505892098929725483705996683460877877086887702979374882397512814979267017748391091109802807602425603643492646967320363403168501730034360947402058443230055492502067864574010692232927265076897044527508924797372257324976759947598003594607917216615826645156054164597485059840613664306467247721955882347677519969372559768382551538397059899617824540900046282373104459578404243546355054161953011042941536498061041054545109176159320970575020349245127720520377324223440193778189600360919398122834631637380186013976101153219486058917357244262654917343442012618000685839036021897745767749145813368627487021825842832324246821404445850741305380013204419875610038846621645562111647108663863942658037664514648984890232569538501545898567883641374273

49505469588547849249616142532133847657911876894986347373181036846326527766999041514739612059691177234746038451172355157108756798614564198411753899212474051129216472224875833061269954423679254665738334826052918367087643927701868107785255599694293377698919315785983199950500241894268865058920898297254837059966834608778770868877029793748823975128149702670177483910911098028076024256036434926469673203634031685017300343609474020584432300554925020678645740106922329272650768970445275089247973722573249767599475980035946079172166158266451560541645974850598406136643064672477219558823476775199693725597683825515383970598996178245409004628237310445957840424354635505416195301104294153649806104105454510917615932097057020349245127720520377324223440193778189600360919398122834631637380186013976101532194860589173572442625491734344201261800685839036021897745767749145813368627487021825842832324246821404445850741305380013204419875610038846621645562111647108663863942658037664514648984890232569538501545898567883641374273)
Khóa công khai của B:
(n_B=45995930991107621563200307769408806689849664869126139618995782257799876490324681454097747049134822545944115727197067258596870594112950343831303286505654364243105983954880258456027419770209294476003684967858202150675820323349240287039783548290797501745971806181607472763681132707396416347105808735025550864195587007361679654734027292282353112299915091532415371963759647614990640833449403684120117133746918919900815398843446859398376225065346300835899984070620034120112281592247725497224949452364676520945928208631539652345420008016449963188816016789358224662928876030773165963296051876901757481894281389959614234417684180160522868331931970962308470519847858110708859983259094025724835874476391928751584397514656044413934659070684477824923548392500281455005809687149455644764926185541367136340423544831109864687216651226567379505500535585074899107024392396901834945078077950125034510079939070384436104840635235793708109721276489157063618567213510306851579907231729431759765846992914464190445625022069845233742409522500238454749872226194139748111830116587740214317014128968637242719150244121947007044081067778683294188100721669563472110623346158703002702285559682854779427498724951573568589791833520883932292158429320392865507756089647, e_B=65537)
Khóa bí mật của B:
(d_B=17468586025736129220258108555176239353500437288746045975812213259634083431407927146382851275660554086524391419349909273638953706875068038786656984621293881715838502535010293925118978257785820826521380576620697491956012143493943737803381487052473409195679360603326517800448958498056011152165396332068695028777374857886739104027236430268257272937645736955066326820235863144692489815439455052409707059308422436053422181786187027679670391140693759903269222887098482764315721941546066935663715140866009732832360579692141877026530820757021895393090362173866863316691792002084233487688540414141759225665423598571943784876718632989514932014003033984879301946941356206866962065228599243663932246142329575393941912264874513138958037980548703419458656276958067122071487495198955276370848244921266147947551402286499166914036013544012424338541415898956788364144921266147947551402286499166914036013544012424338541

42138588136172808996136646021592754485655327511809472895399983494710876861306812982249612113273137476657304224612136087613533437822995913559717426363965726962965103521295292229874291865187637140229775524989010836572307757877122177621965339180829204657483614177682702648121199016330636337829298130388013818290524128626759926166203082192435379151334358532545826702267969549395652286410589556021978222467 3)
Bản tin A gửi cho B (dạng chữ): YEUTOQUOCYEUDONGBAO
Bản tin A gửi cho B (dạng số): 74360723225385055033535380 1
Bản tin đã mã hóa để gửi B:
444111093398051585300904016589048198414441331105329341291226260669853693589336328609531053157808013004601927398813946834526033914242684799904253707697264206744510076808845526670540076057908406195460972978888102696730215119718905360861119067204487352615180012772174012391000605519750945950032521558590385230937718329697409480229769696202667405186530115928255701244552509860808752166734318727707656018966224297338936088196022545280203327581983564055258250927705847310687729421245335386087421160985588014757111329272760062795321754813277682719832701292236890727497907515229982911657564673746334534827921897097117570615978224282089525495140636588158440566939175599043043659037565435867419505631480409467967590666673816371815328338480414241185331892735145727207214868981875415962109998758695361221775672528178304250958811378329691863462433644713282960808573779158115807235019609874019031934603419093452275027583223126550971278068724585930589622481611751252892369402133175507433597369572738672660830593291956563766585823024190815552180541001602842387616252675454245663177583305158062928063244217340318297937389984220283674795916986788777729110605138753168990192335914828310244949940356933901073955472080411920058047487816898991235225092543
Chữ ký của A:
29683121702694447556582666141313050220194198644456431705088631114593158154906857297263939189353029214006044007004890657497092013548833452148116171409903434090592105671302021740358478851377258292419817546781685185936630715805003976125709150351446305313072110984455479700440189413954189583889806584801837319360907364846116893766777038039168600183440168126821066837720994913875367764942676079376626287368615655633985108444185293821881131033920292388785086273759609299701225595837734573325406921161327078775452185243221393520261722111955656155429618219477167752561254056456343070681561802941201896147581527149171071576928467716123581433614928680065355373317454752988718957082422652018609667987840626787560476899530072233066907305574859916153246190667931307150247108727538818694644576598453108465438523839462931878786924746217527729322052970573514796904733196388376748501035043620658724280376397710959838076940045449637192729052441269240843571579157674114783482525674934296637311583770550139673972695515896088094508947336328094651146981504825844205544538141873630006144315309668684976505439122105853190951522825324505443277036672722940526340979047677706741069366485501859118534577003426327836984646257460489386603376479994684628140869697

Bản tin B giải mã được (dạng số): 74360723225385055033535380 1
Bản tin B giải mã được (dạng chữ): YEUTOQUOCYEUDONGBAO
Kết quả xác thực chữ ký: TRUE

5. Sơ đồ chữ ký Elgamal(1024 bits)


Chữ ký hợp lệ.
Thông tin khóa:
Số nguyên tố p với độ dài 1024 bit:
Khóa riêng a: 520480691157207351501696375418514379650594644292258654982848089200262578291586361934892187252513444629783336888149226648697579526544316683099262157985471727890484153071970658133680822436049217483218072594356089663705148650082848984612797275840251939172976008590746150228279336354811912479861698055099366863 9
Khóa công khai beta: 718460103481933647229397124908833534512039176201928651521532182950922316921306606338704924056841748287677014929273396123634907940837477507469951969169589926470190132600008099100966307499329482974540642542769807724863422097331595216321386943096290446071293069894985298057821852518159372074299346127704497490 09
Thông điệp gốc (chuỗi): YEUTOQUOCYEUDONGBAO
Thông điệp gốc (số nguyên): 712948541645836074716368882
Mã hóa:
y1 = 420125217757275217664217053161073366191814489344657447894214453033985967198619386608059399272823369245331609533455182125905982714675652330489794575518454318814803094553929883322864476232692796611971119612069236538190593227532134597940371478021241719584546463339209421971772255702896750649616061788189928272 54 (y1 = g^k mod p)
y2 = 368052274698323957829077429397665145114930294137436337364982339040621743926773016452705854603525823888969608277269339783244614817096948565837364066933145658239189441475697198971659279424969664813918278245729969243941862476968976436084471322995606371226776062764837623557460091362450581808982023039529499273 1 (y2 = m * (beta^k mod p))
Thông tin chữ ký:
k = 129187945841687834542036876077085956344415806506223911537301489614229450761945206181700628700384485858448793492720473062041722420678283611780377803431959629162484701152452379347438495991649104385593193608091498410435959118542441532920020925348897002800774532102807312572380713106186640975005233916234771829 3 (ngẫu nhiên và nguyên tố cùng nhau với p-1)
k_inv = 179108590394608664135131892396590742773276094397665888615735997365440700235291622572004589266252588908949169469348352176971763920501142417737533120304436312256352497064898782954566082037285625403355654848185993155574832959375495592938716184964071696207895811940610642100106550071589372647278017153538092262 1 (nghịch đảo của k mod (p-1))
Chữ ký: gamma = 312971661491977417629199428579881738445386085845654948943611744891259654758156388558165009212841087589302086946898062364983072098426257302242607752650987323615095329336419852586915783457156487257508150610495432903807221145880844103291158908823956885289737126866420111713657830475257292243023222181393366395280 (gamma = g^k mod p), delta = 171508554662643620516754462606124612727408788878214063987265256437219521871080000997049370084114377886302559617603980407262430513742526028855361286663206123440675232270223682787747877980587339729603440893776729614073001524621258375921236072230978771377157353345817244416493978377201998202141001938143330810 34 (delta = (h(x) - a * gamma) * k^(-1) mod (p-1))
Kiểm thử chữ ký: Đúng
Thông điệp sau khi giải mã: YEUTOQUOCYEUDONGBAO
PS C:\Users\FPTShop\OneDrive\Desktop\workspace\py_demo>

Chữ ký hợp lệ.

Thông tin khóa:
Số nguyên tố p với độ dài 1024 bit:
Khóa riêng a:
520480691157207351501696375418514379650594644292258654982848089200262578291586361934892187252513444629783336888149226648697579526544316683099262157985471727890484153071970658133680822436049217483218072594356089663705148650082848984612797275840251939172976008590746150228279336354811912479861698055099366863 9
Khóa công khai beta:
718460103481933647229397124908833534512039176201928651521532182950922316921306606338704924056841748287677014929273396123634907940837477507469951969169589926470190132600008099100966307499329482974540642542769807724863422097331595216321386943096290446071293069894985298057821852518159372074299346127704497490 09

Thông điệp gốc (chuỗi): YEUTOQUOCYEUDONGBAO
Thông điệp gốc (số nguyên): 712948541645836074716368882

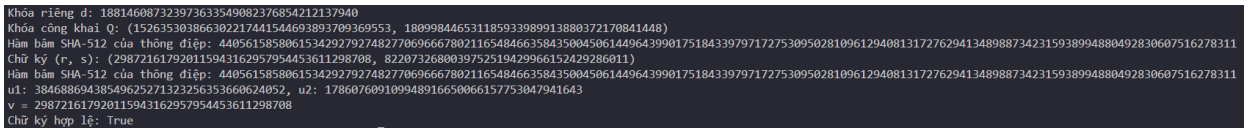
Mã hóa:
y1 = 420125217757275217664217053161073366191814489344657447894214453033985967198619386608059399272823369245331609533455182125905982714675652330489794575518454318814803094553929883322864476232692796611971119612069236538190593227532134597940371478021241719584546463339209421971772255702896750649616061788189928272 7254 (y1 = g^k mod p)
y2 = 368052274698323957829077429397665145114930294137436337364982339040621743926767

730164527058546035258238889696082772769339783244614817069648565837364066933145658239189441475697198971659279424969664813918278245729969243941862476968976436084471322995606371226776062764837623557460091362450581808982023039529499 2731 (y2 = m * (beta^k mod p))

Thông tin chữ ký:
k =
129187945841687834542036876077085956344415806506223911537301489614229450761945206181700628700384485858448793492720473062041722420678283611780377803431959629162484701152452379347438495991649104385593199360891498410439589118542441532920020925348897002800774532102807312572380713106186640975005239316234771829 3 (ngẫu nhiên và nguyên tố cùng nhau với p-1)
k_inv =
179108590394608664135131892396590742773727609439766588861573599736544070023529162257200458926625258890894916946934835217697176392050114241773753312030443631225635249706489878295456608203728562540335565484818599315557483295937549559293871618496407169620789581194061064210010655007158937264727801715353809226 21 (nghịch đảo của k mod (p-1))
Chữ ký: gamma =
312971661491977417629199420579881738445386085845654948943611744891259654758156308558165009212841087589302086946898062364983072098436257302242607752650987323615095329336419852586915783457156487257508150610495432903807221145880844103291158908239568852897371268664201117136578304752572922430232231813933663952280 (gamma = g^k mod p), delta =
171508554662643620516754462606124612727408788878214063398726525643721952187100800997049370084114377886302559617603980407262430513742526028853612866632061234406752322702236827877478779805873397296034408937767296140730015246212528375921236072230978771377157353345817244416493978377201998202141001938143330810341034 (delta = (h(x) - a * gamma) * k^(-1) mod (p-1))

Kiểm thử chữ ký: Đúng
Thông điệp sau khi giải mã: YEUTOQUOCYEUDONGBAO

6. Sơ đồ chữ ký đường cong Elliptic(128 bits)



Khóa riêng d: 188146087323973633549082376854212137940
Khóa công khai Q: (152635303866302217441544693893709369553, 180998446531185933989913880372170841448)

Hàm băm SHA-512 của thông điệp:
44056158580615342927927482770696667802116548466358435004506144964399017518433979717275309502810961294081317276294134898873423159389948804928306075162783 11
Chữ ký (r, s): (298721617920115943162957954453611298708, 822073268003975251942996615242928601 1)
Hàm băm SHA-512 của thông điệp:
44056158580615342927927482770696667802116548466358435004506144964399017518433979717275309502810961294081317276294134898873423159389948804928306075162783 11
u1: 384688694385496252713232563536606240 52, u2: 178607609109948916650066157753047941643
v = 298721617920115943162957954453611298708
Chữ ký hợp lệ: True