

Họ và tên: Đinh Xuân Hòa
MSSV: 22028306

Sinh 2 số nguyên to p và q với độ dài 2048 bit:

p = 2363230886454325213550802982856666912380002712608193895666615843045969454227203617255397998937114572096798846766521204994906807429341125009999707891530844399741647548189
73140996934402794754949741942039996607989907066129633967119656344204808856793680041663275790793238295118371039275190710646399887170085731517350436304134942886421256411
78179570046712139589207387124215881349003172686365858489278279211923598671375791717433952388202959925453348328013212666156277918165049763735826715014933695759174801643

457179592193664851190491557934607784571369999044724685520306989563194734914382309
q = 2683571116647154313806283856812086109497625561785359001572658693512514283891849327118579271257054020289689155729437497518138220679995788638151298609966176770170
33653997077571217008158453315062181593178522791064139654560693933097487699778174514815830249373906322020782471271099442423663447149186872778668870034381871072364
08909249052906047770670560990726650730641807264738419257365458734965418933854073099400217616541077872419637192923137437618120713522861448897349652834361599407401930032283
92733382156568143477677484957951979665058905115892641562458288491426913131206101

2. Tính $n = p * q$ và $\phi(n) = (p-1) * (q-1)$

n = 6341900511579996134127681222494644019902625788180048068068654241169382385966250490601917359093203090503019459605107130012789197896432400041432015372354834220441
308144747950519368498743974212110381585442996251338441030942740394770308003080030796362436135759427467259348112056659526091900281125194299812810987547708054175842192453
2981616192340032738540924250522935852645182608489577695347960738846103452358405240740826696531534555180539797921212639625139168790470599973103942731917542857449552390
5057061961728778683072865609742436657572940411713807805107265426576053986249806411827443110830319470417213245627392032677167061803719740823801841429350417353490176
41827759888054309948826643951063872747952352649575420492980197173828610259622958071235653800802447819308626831795433115603351816841465497586448204947023180387832155626
4144089071429400516096757225218747780739471649262535668428553515999545757383525718526991784261349729904652480287001569612570656106451680477746463018673921947984176
4557827414609334305496541043686842129230918876600435095111588505471580856417190582858963939532541511411462164859751522082373172788850039845028537209
 $\phi(n) = 63419005115799681341268122249464401949062071881808490080685246116932838596625049060191735909320309050301945960510713001278919789643240004143201537354834220
41308144747950519368498743974212110381585442996251338441030942740394770308003080030796362436135759427467259348112056659526091900281125194299812810987547708054175842192453
452981616192340032738540924250522935852645182608489577695347960738846103452358405240740826696531534555180539797921212639625139168790470599973103942731917542857449552390
505706196172877868307286560974243665757294041171380780510726542657605398624980189438240546159861398008285736159828084972643950795974051562991763673570518407093617
90629518512072431297190575152164066460719038795624061972156792156793419496392684490532257932108176719666807299990008403939052684580980023126442316462763637579410261
10556286256380112413925498995850853946254373782525618248215018204391261767616810916116842744774918634960627044122006796431266277191174494284050887458857820145178253463131
48787808749295669763299676208345577349771215933680450841522784237398368026653196407746784321814498543177448703695745596341540234513690945345240588878800$

3. Chọn e = 65537 sao cho gcd(e, $\phi(n)$) = 1.

4. Tính d là nghịch đảo của e modulo $\phi(n)$.

d = 549372859705794836825722624385160732139252872857365511643834806300885168397604649183630874672472089823383800519431546261781024099099404307235956784089368658
833117072716463475293512450086603623219490815820878964772259754110593396398519131906061402466349247820485747353699474522099595798765737399934717564379041736026
3460828455293819474809659347240014823551043884378163566981766275281121379650041999793646549684195085372477413809279898879470995984104501740391319155016908853862

[illegible][illegible][illegible]

Bản rõ sau giải mã: 74360772325385055033538081

Thông điệp đã mã hóa: 4612004972190497399805207580518498022445231391253611460860545974786456042811459531727111711684742782311856541187487348181298594312853362136752532962410621
48171668072695085376685201356706464988881192651052581320845216767842966986499806159953954216338106453708317313861296760673644020907058608454927548392840851465131
70315726672646057704431115670336837329297833349065250491214873389011010625500778794318875440743056216886017974868119008518348233897463256434165309720188463891
96940387934497590336173922560406114840670668206349113158716029114281084819047233334261559613819825206905987109112626192619454156966728801469437124391246174712905607414851753763
471064665997978513792054744821176880912816604981570029786674890244609287414779887906608185812088872466886507171598292513487136553647994740188348480430951856223402675008139
3556397670134979804961595131289712792364398604887266183627007157728125872055615429929001048078235005239674271995544067749255544317699602743809821762408386953918113998479844378
1855784015221673780225651403697143475761289583767666172614677448389091105571610325917685294691723924664671687005780189851120269900634128541776
43

Thông điệp đã giải mã: YEUTOUQ9CYEUD3AG7A

p = 2363230886454322512435508029285066691532800027126081938956666158434059694542

2720361725539799893711457209679884676652120499494068074293411250099997078915
3084439974164754818938114099693440229474649476194320939996067989907060612963
3907611906534420480085679368804106327375719079332387295118371039725210701064
6399888717008573151375043630413494288462125641177137957004672173915892073871
2473588134900317768063665858492782779211923598671337519717343395238820259982
9615245333483280132126661562779181650497633358267150149336957959174801644345
7719759219366478519049155793460728775476139609904427746855203069859635194734
914382309

q =

2683572116432114533180638265486585120861094976255611785350001752656983851291
5142838918493327118579217257050402289868915572943749751813822063799057886381
5129860996617677017033635930972775121700815845433197892575625181593157852279
1064139654650693933097487699778174514814158103824947339063220203782471271099
4424233626344121491868727786088700343381107236489009249025906047770670565099
0726625073060418076234819295379168553784965418933854073099400217616541017787
2419631192922137437618121071352286144089739494652834361599402704193003228392
7333982156568143477607774849507505197966650589051158926415624582884914269191
312106101

2. Tính $n = p * q$ và $\phi(n) = (p-1)*(q-1)$:

n =

6341900511579968413341268122249406440194902602578818084900480680652461169328
3859662504960019719359093203090050390194596051071300102789197896435240002414
3201532735483422044130814474749505190374689843475729121103181585442992961338
3441003294270394469950083007903676524360135675942476275933481120566595260919
9029811215914299928109875747708054175842419245329816161923940032745622850492
4250522935508526459182608489577695374960738846103454235840520424470826965631
5354555180539797921126396251391687920475999731039247231911754285744955239055
5070619742388778683073866560974242636657557294401711380787501072656426570653
9862498069411872434110830319470471233452677952023922677767016818037194740823
8018434129350413533949176418277559888045303994388266439510638727479523526946
7539149404299803199773782286102450629235087213565380008241870398626831795433
1156033518168414634977586448294947023180387832115626414408970142940051690066
7755722262187477807309471694262535666842385535159996457753083256718526991784
2613497299046254280287001569612570656160456180477764764630186073293219474984
7184557827841460933430504965410434686842412923091887866004350951115885057415
0885641877190582589816890399352451415114114621464859735152208273731727888350
03998450285367209

$\phi(n) =$

6341900511579968413341268122249406440194902602578818084900480680652461169328
3859662504960019719359093203090050390194596051071300102789197896435240002414
3201532735483422044130814474749505190374689843475729121103181585442992961338
3441003294270394469950083007903676524360135675942476275933481120566595260919
9029811215914299928109875747708054175842419245329816161923940032745622850492
4250522935508526459182608489577695374960738846103454235840520424470826965631

5354555180539797921126396251391687920475999731039247231911754285744955239055
5070619742388778683073866560974242636657557294401711380787501072656426570653
9862498018943842405246459863309008285736159828084972643950079574970515629913
3663850750718407093617906295370815220742434329177905715132460466407190387956
2042619722156793491949463926384950322572933701810726791966682072909900080430
9309509268450899023126442316463276337357579410216854582835623801124139254989
9558505853946254373782525261824821501820439216727667681091611196412744774918
6349600267044122200679643126627719117440942850508874588578270145125783346431
1056780807492695669376329267962608345527734977218159336804505841752278423737
0398368026653168830470670432783144985431774887036957745596341541023451360904
54534524058878800

3. Chọn $e = 65537$ sao cho $\gcd(e, \phi(n)) = 1$.

4. Tính d là nghịch đảo của e modulo $\phi(n)$:

$d =$

5493726838937057948368257226243851601732532928782285736545311643834803630088
5168389760464931863030874762742089823338383005194315416261781024099690944307
2735056784089366865883311707287164634755205331245008066638232219490815820087
8964747227097957411050339693985191931900661040246063492947428020458775136990
4745722909957529876537739993421756437904173602634608284552938394174809656654
3472400141823551034388437816352669817466027828112139766500419999970364656496
8419500537247744138092798998794709959584104501740393119155501690805386252523
90629602211711818269903955383925065683251116578081687979319775225727550737624
2591778313239821937325788388204986251707167822762724406416820670800633739939
5206392544636679664750564749804220777879591945937113883684032775206221326128
6949907207575183503205054553721775441828370556967603252137338395599561677559
9755780732791314729226907424852087252157483295974986401077869667122333000334
1278284685023231656679665557519991196019038895900506521649289842797861721116
4294903086901888334373666720312017598510338817628183795835261406393483397712
2437029464726081227677947602235866913697692925619015497972962700148061503028
7052527520202893150965241285070220961126191904857128817766376545612917994609
5866975904766273

Thông điệp gốc: YEUTOQUOCYEUDONGBAO

Chuyển 'YEUTOQUOCYEUDONGBAO' thành số: 743607232253850550335353801

5. Mã hóa bản rõ 743607232253850550335353801 với khóa công khai

($n=63419005115799684133412681222494064401949026025788180849004806806524611693$
2838596625049600197193590932030900503901945960510713001027891978964352400024
1432015327354834220441308144747495051903746898434757291211031815854429929613
3834410032942703944699500830079036765243601356759424762759334811205665952609
1990298112159142999281098757477080541758424192453298161619239400327456228504
9242505229355085264591826084895776953749607388461034542358405204244708269656
3153545551805397979211263962513916879204759997310392472319117542857449552390
5550706197423887786830738665609742426366575572944017113807875010726564265706
5398624980694118724341108303194704712334526779520239226777670168180371947408

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

Bản mã:

4612004972190497399805207585051849802224452313912536114608605459747864560428
11459531727111711168474278231185654118748734818129859431285336213675253296241
0621701871668072695005832668520153098002664988881192651052558213208452167628
4296698649980615995395423163381046357083714841543378601296670673642940209070
5860824549275483932840851465131483157227086726460577044311156703368373723929
7833349600525049121487338390111002655200778709431887534047330562316806021797
4868119008518348233897826800432564341441645309720188463891969443807934497590
3361743925680611484067009682034911315871602911428108481904722333342615596138
1982520690598671091126261926194541569667288014694372143912461747129056072414
8517537634710646659962979785137922204744821176880912816604981527002978667489
0244609287414779887096068185812088872466988507171598292351348713655364799474
0188348480443093518562234026750081393556397670134079804961959131389712792364
3986048872661836270071575772812587205561574299209010480782350052396747219955
4406774925554431796990274380982217624083869539181139984798443781855784015221
6763780225651402697343143475761289583077666617261467744878090110557161035291
7685629469127203646467639911021818005775801893702787673107615790908112026990
0064312854177643

6. Giải mã bản mã

4612004972190497399805207585051849802224452313912536114608605459747864560428
11459531727111711168474278231185654118748734818129859431285336213675253296241
0621701871668072695005832668520153098002664988881192651052558213208452167628
4296698649980615995395423163381046357083714841543378601296670673642940209070
5860824549275483932840851465131483157227086726460577044311156703368373723929
7833349600525049121487338390111002655200778709431887534047330562316806021797
4868119008518348233897826800432564341441645309720188463891969443807934497590
3361743925680611484067009682034911315871602911428108481904722333342615596138
1982520690598671091126261926194541569667288014694372143912461747129056072414
8517537634710646659962979785137922204744821176880912816604981527002978667489
0244609287414779887096068185812088872466988507171598292351348713655364799474
0188348480443093518562234026750081393556397670134079804961959131389712792364
3986048872661836270071575772812587205561574299209010480782350052396747219955
4406774925554431796990274380982217624083869539181139984798443781855784015221
6763780225651402697343143475761289583077666617261467744878090110557161035291
7685629469127203646467639911021818005775801893702787673107615790908112026990
0064312854177643 với khóa bí mật

(n=63419005115799684133412681222494064401949026025788180849004806806524611693
2838596625049600197193590932030900503901945960510713001027891978964352400024
1432015327354834220441308144747495051903746898434757291211031815854429929613
3834410032942703944699500830079036765243601356759424762759334811205665952609
1990298112159142999281098757477080541758424192453298161619239400327456228504
9242505229355085264591826084895776953749607388461034542358405204244708269656
3153545551805397979211263962513916879204759997310392472319117542857449552390
5550706197423887786830738665609742426366575572944017113807875010726564265706
5398624980694118724341108303194704712334526779520239226777670168180371947408
2380184341293504135339491764182775598880453039943882664395106387274795235269
4675391494042998031997737822861024506292350872135653800082418703986268317954
3311560335181684146349775864482949470231803878321156264144089701429400516900
6677557222621874778073094716942625356668423855351599964577530832567185269917
8426134972990462542802870015696125706561604561804777647646301860732932194749
8471845578278414609334305049654104346868424129230918878660043509511158850574
1508856418771905825898168903993524514151141146214648597351522082737317278883
5003998450285367209,
d=54937268389370579483682572262438516017325329287822857365453116438348036300
8851683897604649318630308747627420898233383830051943154162617810240996909443
0727350567840893668658833117072871646347552053312450080666382322194908158200
8789647472270979574110503396939851919319006610402460634929474280204587751369
9047457229099575298765377399934217564379041736026346082845529383941748096566
5434724001418235510343884378163526698174660278281121397665004199999703646564
9684195005372477441380927989987947099595841045017403931191555016908053862525
23906296022117118182699039553839250656832511165780816879793197752257275507376
2425917783132398219373257883882049862517071678227627244064168206708006337399
3952063925446366796647505647498042207778795919459371138836840327752062213261
2869499072075751835032050545537217754418283705569676032521373383955995616775
5997557807327913147292269074248520872521574832959749864010778696671223330003
3412782846850232316566796655575199911960190388959005065216492898427978617211
1642949030869018883343736667203120175985103388176281837958352614063934833977
1224370294647260812276779476022358669136976929256190154979729627001480615030
2870525275202028931509652412850702209611261919048571288177663765456129179946
095866975904766273):

Bản rõ sau giải mã: 743607232253850550335353801

Thông điệp đã mã hóa:

4612004972190497399805207585051849802224452313912536114608605459747864560428
11459531727111711168474278231185654118748734818129859431285336213675253296241
0621701871668072695005832668520153098002664988881192651052558213208452167628
4296698649980615995395423163381046357083714841543378601296670673642940209070
5860824549275483932840851465131483157227086726460577044311156703368373723929
7833349600525049121487338390111002655200778709431887534047330562316806021797
4868119008518348233897826800432564341441645309720188463891969443807934497590

3361743925680611484067009682034911315871602911428108481904722333342615596138
1982520690598671091126261926194541569667288014694372143912461747129056072414
8517537634710646659962979785137922204744821176880912816604981527002978667489
0244609287414779887096068185812088872466988507171598292351348713655364799474
0188348480443093518562234026750081393556397670134079804961959131389712792364
3986048872661836270071575772812587205561574299209010480782350052396747219955
4406774925554431796990274380982217624083869539181139984798443781855784015221
6763780225651402697343143475761289583077666617261467744878090110557161035291
7685629469127203646467639911021818005775801893702787673107615790908112026990
0064312854177643

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 = 242103461023435832084034033798106983906562959339888225152772863855853062058648957668567592154579946303939332889168253011208422808656289048542445336566969013596598543899577
2994340571201819812837234785124873221674787654993815914827091435812141717073337655643232697389456736618081021969238316712810171121908411
Chọn phần tử sinh g = 2.
Chọn khóa riêng x trong khoảng từ 1 đến p-2: x = 1974309033875725914107668739800109443873377819752332291453695171754278586255481813337220489689617098103087830850860885082138654172
824155630116918814617347013721713331209231330334139146604978872509751946009261682911867547010760653011283198045919996614984419215125266618761768801654043193554585495240690936406
và tính khóa công khai y = g^x mod p:
y = 104593528548207918072798949131070057009728160481900863456307483714395081868721448519569284897737374271586895486714757239543645404495605342068968356013195478774929913457620
2231404852497453836692107111653271426095478480421502539193118720998124106645214789734612502397195541605472733823171398968827516887995952

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 = 4887529802120656966295219323657554370226880462682977896351455817684819744403544087227396023292807005825014368145091617268885808854742847956642370610926177665145214963120282
970920676656657935636636709181604872293463115086171375328503622964630526309443485422206148770200701770204909107346592583928387982712503
Tính c1 = g^k mod p:
c1 = 22532903959049597770951824253424723986416604309828967475721432719721808305857153629109103976609122022938120501837305087278265155280406936571437897848329560655734505539951
03768707509585533439011061154984329089839049922402628951223135444164319364996854910504375087800005680824792729717218863501709204878957363
Tính c2 = (m * y^k) mod p:
c2 = 387316189973858223936969379519371777001792253029315240516406638584531758494054021325233936517325846811292010480598459581098876583312952723576208404598487835387134065638
828657363875717566338288999477908951278602703829809131893392135749711051661430359193464131558804495981644955705567185738620074432588271
3. Giải mã bản (c1, c2) = (22532903959049597770951824253424723986416604309828967475721432719721808305857153629109103976609122022938120501837305087278265155280406936571437897848329560655734505539951
303696937951937177700179225302931524051640663858453175849405402132523393651732584681129201048059845958109887658331295272357620840459848783538713406563882865736387527156633828899
9477908951278602703829809131893392135749711051661430359193464131558804495981644955705567185738620074432588271) với khóa bí mật x = 1974309033875725914107668739800109443873377819752332291453695171754278586255
52322291453695171754278586255481813337220489689617098103087830850860885082138654172824155630116918814617347013732171333120923133033413914660497887250975194600926168291186754701076
0653011283198045919996614984419215125266618761768801654043193554585495240690936406:
Bản rõ sau giải mã: m = 743607232253850550335353801

Thông điệp đã mã hóa: (225329039590495977709518242534247239864166043098289674757214327197218083058571536291091039766091220229381205018373050872782651552804069365714378978483295606
65573450553995103768707509585533439011061154984329089839049922402628951223135444164319364996854910504375087800005680824792729717218863501709204878957363, 387316189972385822393696
937051937177700179225302931524051640663858453175849405402132523393651732584681129201048059845958109887658331295272357620840459848783538713406563882865736387527156633828899477909
8951278602703829809131893392135749711051661430359193464131558804495981644955705567185738620074432588271)
Thông điệp đã giải mã: YEUTOQUOCYEUDONGBAO
```

1. Khởi tạo

Sinh số nguyên tố p với độ dài 1024 bit:

p =

2421034610234358320840340337981069839065629593398882251527728638558530620586
4895766856759215457994630393933288916825301120842280865628904854244533656696
9013596598543899577729943405712018198120372347851248732216747876549938159148
2709143581214177107333765564323269738945673661808102196923831671281017112190
8411

Chọn phần tử sinh g = 2.

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

1974309033875725914107668739800109443873377819752332291453695171754278586255
4818133372204896896170981030878308508608850821386541728241556301169188146173
4701373217133312092313303341391466049788725097519460092616829118675470107606
5301128319804591999661498441921512526661876176880165404319355458549524069093
6406 và tính khóa công khai y = g^x mod p:

$y =$
1045935285483207918072798949131070057009728160481900863456307483714395081868
7214485195692848977373742715868954867147572395436454044956053420689683560131
9547877492991345762022314048524974538366921071116532714260954784804215025391
9311872099812410664521478973461250239719554160547273382317139896882751688799
5952

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 $p-1$:

$k =$
4887529802120656966295219323657554370226880462682977896351455817684819744403
5440872273960232928070058250143681450916172688858088547428479566423706109261
7766514521496312028297092067665665793563663670918160487229346311508617137532
8503622964630526309443485422206148770200701770204909107346592583928387982712
503

Tính $c1 = g^k \text{ mod } p$:

$c1 =$
2253290395904959777095182425342472398641660430982896747572143271972180830585
7153629109103976609122022938120501837305087278265155280406936571437897848329
5606655734505539951037687075095855334390110611549843290898390499224026289512
2313544416431936499685491050437508780000568082479272971721886350170920487895
7363

Tính $c2 = (m * y^k) \text{ mod } p$:

$c2 =$
3873161899723858223939696937951937177700179225302931524051640663858453175849
4054021325233936517325846811292010480598459581098876583331295272357620840459
8487835387134065638828657363875271566338288999477909895127860270382908913189
3392135749711051661430359193464131558804495981644955705567185738620074432588
271

3. Giải mã bản mã ($c1, c2$) =

(225329039590495977709518242534247239864166043098289674757214327197218083058
5715362910910397660912202293812050183730508727826515528040693657143789784832
9560665573450553995103768707509585533439011061154984329089839049922402628951
2231354441643193649968549105043750878000056808247927297172188635017092048789
57363,

3873161899723858223939696937951937177700179225302931524051640663858453175849
4054021325233936517325846811292010480598459581098876583331295272357620840459
8487835387134065638828657363875271566338288999477909895127860270382908913189
3392135749711051661430359193464131558804495981644955705567185738620074432588
271) với khóa bí mật $x =$

1974309033875725914107668739800109443873377819752332291453695171754278586255
4818133372204896896170981030878308508608850821386541728241556301169188146173

4701373217133312092313303341391466049788725097519460092616829118675470107606
5301128319804591999661498441921512526661876176880165404319355458549524069093
6406:

Bản rõ sau giải mã: $m = 743607232253850550335353801$

Thông điệp đã mã hóa:

(225329039590495977709518242534247239864166043098289674757214327197218083058
5715362910910397660912202293812050183730508727826515528040693657143789784832
9560665573450553995103768707509585533439011061154984329089839049922402628951
2231354441643193649968549105043750878000056808247927297172188635017092048789
57363,
3873161899723858223939696937951937177700179225302931524051640663858453175849
4054021325233936517325846811292010480598459581098876583331295272357620840459
8487835387134065638828657363875271566338288999477909895127860270382908913189
3392135749711051661430359193464131558804495981644955705567185738620074432588
271)

Thông điệp đã giải mã: YEUTOQUOCYEUDONGBAO

3. Hệ mật đường cong Elliptic(128 bits)

```
Bước 1: Chọn khóa bí mật  $t = 123456789$   
Kết quả  $M = t * P = (201629761420603453009345331233652475040, 183825641330351009968507574913199203265)$   
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,  $M1 = k * P = (274951200853909607349486340084452122690, 70411817076435010691359956716424026325)$   
Bước 3c: Mã hóa,  $M2 = M + k * B = (143153205647850948777583192082618256929, 243264406687351118626350144644229950932)$   
Bước 4: Giải mã, tính lại  $M$  từ  $M1$  và  $M2$   
Kết quả  $M$  (sau giải mã) =  $(201629761420603453009345331233652475040, 183825641330351009968507574913199203265)$   
Giải mã thành công,  $M$  khớp với giá trị ban đầu.
```

Bước 1: Chọn khóa bí mật $t = 123456789$

Kết quả $M = t * P = (201629761420603453009345331233652475040, 183825641330351009968507574913199203265)$

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, $M1 = k * P = (274951200853909607349486340084452122690, 70411817076435010691359956716424026325)$

Bước 3c: Mã hóa, $M2 = M + k * B = (143153205647850948777583192082618256929, 243264406687351118626350144644229950932)$

Bước 4: Giải mã, tính lại M từ $M1$ và $M2$

Kết quả M (sau giải mã) = $(201629761420603453009345331233652475040, 183825641330351009968507574913199203265)$

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=74570294658756641896923334373812038676905681707754200456563641985285444209668245041607245690294755118828866529198227543226802050904294960898095295364691197726071440081132685767849258419025456724174500458335983031740113068479008025324115688227590756717622459376581858265391401600172523419425793983479888380761066566459264351589601535311507466489783444918603812321616229366550010507418215010863023935456146649699457858908391377446370912619092787035285695578079779978313626602832423916083844406770009040845606920654324068492987932131155758482520904628669558531941229033534047908820625168160536116756603823122065577505386993802170882641068450311193624445569509254472292159047538495016157934249498512761632113106538291495302613909478539547683269879931006584313253026528251746080042926832994491652915217494883897301968069473779144518691210226109601425669251487966587242413459533508753707245983917737871660465643526818546960994842093354423725130579791633620631421261899437307760504590851163149495605219399924587145898524089866465345499071433189424469246694503594154891878199615247463026822569999747641069521902145592188560733322584115758231362053939362972708785348021613472102506332650538066510664182112178152273728529285763, e_A=65537)

Khóa bí mật của A: (d_A=742369089936359360959895330559072379180620763437556655719370471289189850315942899353742639702395746368138695367656309844864654877854983335960109694941655126369356297440256572985576111648224407081817021294897124935881287500049595469588547849240616425323384765791187694986347373181036846326527669990415147396120596011772347468345117235515710875679861456419841175389921247405112912614722487583306126995442367925466573833482605291836708764392770186810778525599694293377698919315785983199950500241894268865058920898297254837956968364608778770868877029793748823975128149702670177483910911098028076024256034392646967720363403168501730034369474020584432300554925020678645740160922329272650768970445275089247973722573240767599475980035046079127166158266451560541645974850598406136643064672477219558823476775190693725597683825515383970989061782454900046782371304459578404243546350546161953081104204153648006104105454510917615932007057020349245127720520377232244019377818060360919398122834631637380186013976105132194860580173572442625491724344201261800685839036021897745767749145813368627487021825842832324246821404445850741305380013204419875610038846621645562111647108663863942658037664514648984890232569358051545898567883641374273)

Khóa công khai của B: (n_B=4599593099110762156320030776940880668984966486012613961899578225779987649032468145409774704913482254504411572719706725850687059411295034383130328650565436424310598354880258456027410770209294476003684967858202150675820323492402870387835482907975017457918061816074727636811327073964163471058087350255508641955870073617965473402729282351172099159915324153710637596476140986408334494036841201171374691891090881308843446859398376225065364300835899984070620024120112281592247725497224949452364675209459202087631936523454200800164496318881601677895324662246620288768307731659632960518769017574818042813899561423441768418016052286831931970962308470519847858110708859832599040727483587447631928751584397514656044139346590706844778249234839250028145500580968714945564476492185541367136340423544831109864687216651220567379505508535580748991070243923690183404507801960125034510079939078384436104804063523579081097212764891570636185672135103068515799072317294317597658469929144641904456250220698452337424095225002384547498722261941397481118301116587462143170141289686372427191502441219470070440810677786832941881007216695634721106233461587030027022855596828547794274987249515735858979183352088393229215842932039286507756089647, e_B=65537)

Khóa bí mật của B: (d_B=17468586025736129220858108555176239353004372887460459758122132596340834134079271463828512756605540865243914193499097273689537068750680387866569846212938817158380253501029392511897825778582082652138057662069749195601214349394373780338148705247340919567936060326517800448958495806011521653963208686950277374857886739104027236430268257272937675369506632682023586314469248981543945052409707059308422436053422181786187027679670391140693759903269222887098482764315721941546066935663715140866009732832360579692141877026530820757021895393090362173860863136691792002084233487688540414141759225665423598519437848767186329895149320140030339848793019469413562086696206522859924366392324614232957539394191226487451313895803798054870341954856562769580671220714874951989552763708482449212661497551402286499166914036013544012424338541442138588136717280899613664602159275448805532751189947289539998349471087686130681298224961211327313747665730422461213608761353343782299591355971742636396572696296510352129529229874291865187631740229775524989910836572307758771221776219653391808292046574836141776827026481211990163306363378292981303880138182905241286267599261662030821924353791513435853254582670226796954939565228641058955662919782224673)

Bản tin A gửi cho B (dạng chữ): YEUTOUQUOCEYUODNGBAO

Bản tin A gửi cho B (dạng số): 743607232253850550335353801

Bản tin đã mã hóa để gửi B: 444111093308051585300904016589048198414441331105329341291226260669853693589336228609513053157008013004601927398813946834526033014242604799904253706792764206744510076088845526670540076057908406195460972978888102696730215119718905308611109672044875261510001277217401230100860551975084595003252155859038523093771832609709040290769606202667405186530115928257801244552509608087521667343187277076560189662242973389360880106022545208203758198356405525825092770584731068772942124533538680742011609855804147571113292727008627953217548132776827198327012922368907749790751528998291165756467374633408279718979071570615978224282089525495140636588158440569693917559084304365903756543801419505631348040946796759066667381637815328338480414241185331892735145727077214868981874545962109998758695321271775672581783042509588117832969186346243364471328296080857377951815807323596987401983193460431999345750274199334522758322312655097127806874585930589624861611751258923694021331755074335973695727386726608305932919565637665882302419081552180541001602842387616252675454256631775833051580629280632442173403182979373899842202836747959169868777729110660513875316899019233591482831024494940356933901073955472080411920058047487816898991235225092543)

Chữ ký của A: 2968311217026944755658266614131305022019419864445643170508863111459315815498856729726393918935302921400604400700489065749709201345488334440959310561362021740358478851734678154678168518595366307158050039761257095150351446350130771109844554797004401894139541895838980658480183713936090736484611689376677038039168600134401681268210668737209949138753676494267607937662628736861565563398510844418529382188113103392029238878508627375960929970122559583773457332540692116132707875545218524322139352026172211195565515542961821947176775256125405645634307068156180294120189614758152174917107157692846771612358133614928608006535573317454752988718957082422652018609667987840626787560747689953007232306690730557485991615324619066793130715024710872753881869464457659845130846543852389462931878786924746217527729320252970573514796904733196388376748501035043620658724280376397710959838076904454963719272905244126924084357157915767411478348252567493429663731158377055013967397269551589608809450894733632809465114608150482584420554453814817736300601443153096686947650543912210585319095152282532450544327703667272294052634097904767770674106936648501859118534577003426327836984646257460489386603376479994684628140869697

Bản tin B giải mã được (dạng số): 743607232253850550335353801

Bản tin B giải mã được (dạng chữ): YEUTOUQUOCEYUODNGBAO

Kết quả xác thực chữ ký: TRUE

Khóa công khai của A:

(n_A=7457029465875664189692333437381203867690568170775420045656364198528544420966824504160724569029475511882886652919822754322680205090429496089809529536469119772607144008113268576784925841902545657241745004583359830317401130968479008025324115688227590756717622459376581858265391401600172523419425793983479888380761066566459264351589601535311507466489783444918603812321616229366550010507418215010863023935456146649699457858908391377446370912619092787035285695578079779978313626602832423916083844406770009040845606920654324068492987932131155758482520904628669558531941229033534047908820625168160536116756603823122065577505386993802170882641068450311193624445569509254472292159047538495016157934249498512761632113106538291495302613909478539547683269879931006584313253026528251746080042926832994491652915217494883897301968069473779144518691210226109601425669251487966587242413459533508753707245983917737871660465643526818546960994842093354423725130579791633620631421261809437307760504459851163149495605219399924587145859852480986644653545499071433189434469364694503504154891878199615247463026822506297476410695219021455921885607333332258411573582313620539393629727087853480216134721025063326505538066510664182112178152273728529285763, e_A=65537)

Khóa bí mật của A:

(d_A=74236908993635936095989533055907237918062076343755665571937047128918985031594289937426397023957463681386953676563098448646524877854983335960109694941655103536929744025065729855761116482244970418179212948971249358812875000

4950546958854784924961614253213384765791187689498634737318103684632652776699
9041514739612059691177234746038451172355157108756798614564198411753899212474
0511292164722248758330612699544236792546657383348260529183670876439277018681
0778525559969429337769891931578598319995050024189426886505892089829725483705
9966834608778770868877029793748823975128149702670177483910911098028076024256
0364349264696732036340316850173003436094740205844323005549250206786457401069
2232927265076897044527508924797372257324976759947598003594607917216615826645
1560541645974850598406136643064672477219558823476775199693725597683825515383
9705989961782454090046282373104459578404243546355054161953011042941536498061
0410545451091761593209705702034924512772052037732422344019377818960036091939
8122834631637380186013976101532194860589173572442625491734344201261800685839
0360218977457677491458133686274870218258428323242468214044458507413053800132
0441987561003884662164556211164710866386394265803766451464898489023256953850
1545898567883641374273)

Khóa công khai của B:

(n_B=45995930991107621563200307769408806689849664869126139618995782257799876
4903246814540977470491348225459441157271970672585968705941129503438313032865
0565436424310598395488025845602741977020929447600368496785820215067582032334
9240287039783548290797501745971806181607472763681132707396416347105808735025
5550864195587007361679654734027292282353112299915091532415371963759647614990
6408334494036841201171337469189199008153988434468593983762250653463008358999
8407062003412011228159224772549722494945236467652094592820863153965234542000
8016449963188816016789358224662928876030773165963296051876901757481894281389
9596142344176841801605228683319319709623084705198478581107088599832590940257
2483587447639192875158439751465604441393465907068447782492354839250028145500
5809687149455644764926185541367136340423544831109864687216651226567379505500
5355850748991070243923969018349450780779501250345100799390703844361048406352
3579370810972127648915706361856721351030685157990723172943175976584699291446
4190445625022069845233742409522500238454749872226194139748111830116587740214
3170141289686372427191502441219470070440810677786832941881007216695634721106
2334615870300270228555968285477942749872495157356858979183352088393229215842
9320392865507756089647, e_B=65537)

Khóa bí mật của B:

(d_B=17468586025736129220258108555176239353500437288746045975812213259634083
4314079271463828512756605540865243914193499092736389537068750680387866569846
2129388171583850253501029392511897825778582082652138057662069749195601214349
3943737803381487052473409195679360603326517800448958498056011152165396332068
6950287773748578867391040272364302682572729376457369550663268202358631446924
8981543945505240970705930842243605342218178618702767967039114069375990326922
2887098482764315721941546066935663715140866009732832360579692141877026530820
7570218953930903621738668633166917920020842334876885404141417592256654235985
7194378487671863298951493201400303398487930194694135620686696206522859924366
3932246142329575393941912264874513138958037980548703419458656276958067122071
4874951989552763708482449212661479475514022864991669140360135440124243385414

4213858813617280899613664602159275448565532751180947289539998349471087686130
6812982249612113273137476657304224612136087613533437822995913559717426363965
7269629651035212952922298742918651876371402297755249890108365723077578771221
7762196533918082920465748361417768270264812119901633063633782929813038801381
8290524128626759926166203082192435379151334358532545826702267969549395652286
4105895560219782224673)

Bản tin A gửi cho B (dạng chữ): YEUTOQUOCYEUDONGBAO

Bản tin A gửi cho B (dạng số): 743607232253850550335353801

Bản tin đã mã hóa để gửi B:

4441110933980515853009040165890481984144413311053293412912262606698536935893
3632860953105315780801300460192739881394683452603391424268479990425370769726
4206744510076808845526670540076057908406195460972978888102696730215119718905
3608611190672044873526151800127721740123910006055197509459500325215585903852
3093771832969740948022976969620266740518653011592825570124455250986080875216
6734318727707656018966224297338936088196022545280203327581983564055258250927
7058473106877294212453353860874211609855880147571113292727600627953217548132
7768271983270129223689072749790751522998291165756467374633453482792189709711
7570615978224282089525495140636588158440566939175599043043659037565435867419
5056314804094679675906666738163718153283384804142411853318927351457272072148
6898187541596210999875869536122177567252817830425095881137832969186346243364
4713282960808573779158115807235019609874019031934603419093452275027583223126
5509712780687245859305896224816117512528923694021331755074335973695727386726
6083059329195656376658582302419081555218054100160284238761625267545424566317
7583305158062928063244217340318297937389984220283674795916986788777729110605
1387531689901923359148283102449499403569339010739554720804119200580474878168
98991235225092543

Chữ ký của A:

2968312170269444755658266614131305022019419864445643170508863111459315815490
6857297263939189353029214006044007004890657497092013548833452148116171409903
4340905921056713020217403584788513772582924198175467816851859536630715805003
9761257091503514463053130721109844554797004401894139541895838898065848018373
1936090736484611689376677703803916860018344016812682106683772099491387536776
4942676079376626287368615655633985108444185293821881131033920292388785086273
7596092997012255958377345733254069211613270787754521852432213935202617221119
5565615542961821947716775256125405645634307068156180294120189614758152714917
1071576928467716123581433614928680065355373317454752988718957082422652018609
6679878406267875604768995300722330669073055748599161532461906679313071502471
0872753881869464457659845310846543852383946293187878692474621752772932205297
0573514796904733196388376748501035043620658724280376397710959838076940045449
6371927290524412692408435715791576741147834825256749342966373115837705501396
7397269551589608809450894733632809465114698150482584420554453814187363000614
4315309668684976505439122105853190951522825324505443277036672722940526340979
0476777067410693664855018591185345770034263278369846462574604893866033764799
94684628140869697

Bản tin B giải mã được (dạng số): 743607232253850550335353801

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: 52048069115720735150169637541851437965059464429225865498284808920026257829158636193489218725251344662978333688814922664869757952654431668309926215798547172789048415307937065813368082243604921748321807259435608966370514865008284898461279
72758025193912297080859874615022379136354811912479861080953999366839
Khóa công khai beta: 71846010348193264220971249881353451203917620192865152151218295992231695313606063387804240568417482876770149292273961236349879408174775074699519601695899264701901326000080991809663074993294829745406425427698077248634220973315952
1632138694309629044607129306989498529805782185251815937207429934612770449749009
Thông điệp gốc (chuỗi): YEUTOQUOCYEUDONGBAO
Thông điệp gốc (số nguyên): 712948541645836074716368882
Mã hóa:
y1 = 4201252177572752176642170531610733661918144893446574478942144530339859671986193866080593992728233692453316095334551821259059827146756523304897945755184543188148030945539288332286447623269279661197111961206923653819059322753213459794037147802124
1795845464633920942197177225570289679064961606178818992827254 (y1 = g^k mod p)
y2 = 368052274698323957829077429397665145114930294137436337364982339040621743926773016452705854603525823888969682772769339783244614817069648565837364066933145658239180441476971989716592794249696648139182782457299602439418624769689764360844713229956
063712267768627648376235574680913624505810808920230395294992731 (y2 = m * (beta^k mod p))
Thông tin chữ ký:
k = 1291879458416878345420368760778059614441580850622391353780148951422545070104520618178062170038448358448793402720473062001722420678283611780377803431959629162404701152452379347438495991649104385593199368091498410439589118542441532920020925348897
8028007452310280731257238071318618660897908239162347718293 (ngẫu nhiên và nguyên tố cùng nhau với p-1)
k_inv = 17918099036468664135131892396590742773727694397665888615735997365440700235291622572804589266252588980849160469348352176971763920501142417737533120304436312256352497064898782954566882037285625403356548481859931555748332959375495929387161849
64071696207895815400318642180186550871583726472780171553388922621 (ngược đảo của k mod (p-1))
Chữ ký: gamma = 3120716314937781762919942057808173845380808345558484361114409125965473815638855816508921284180758930286964680863364983072098436257302426077526500873236150853291364198525869157834517564872575081586184954298380722145808044103281
1589023956852997371606420111713657830475252924302323181393366395280 (gamma = g^k mod p), delta = 171508546626436205167546200612461272740878887821406339872652564372195218710808099704937088411437788630255961760398048726243051374252602885361286
663206123440675222702236827877478779885873397296034408937767296140730015246212528375921236072230978771377157353458172444164939783772019982021418019381433881034 (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\VFPTShop\OneDrive\Desktop\workspace\py_demo>
```

Chữ ký hợp lệ.

Thông tin khóa:

Số nguyên tố p với độ dài 1024 bit:

Khóa riêng a:

5204806911572073515016963754185143796505946442922586549828480892002625782915
8636193489218725251344462978333688814922664869757952654431668309926215798547
1727890484153071970658133680822436049217483218072594356089663705148650082848
9846127972758402519391729760085907461502282793363548119124798616980550993668
639

Khóa công khai beta:

7184601034819336472293971249088335345120391762019286515215321829509223169213
0660633870492405684174828767701492927339612363490794083747750746995196916958
9926470190132600008099100966307499329482974540642542769807724863422097331595
2163213869430962904460712930698949852980578218525181593720742993461277044974
9009

Thông điệp gốc (chuỗi): YEUTOQUOCYEUDONGBAO

Thông điệp gốc (số nguyên): 712948541645836074716368882

Mã hóa:

y1 =

4201252177572752176642170531610733661918144893446574478942144530339859671986
1938660805939927282336924533160953345518212590598271467565233048979457551845
4318814803094553929883322864476232692796611971119612069236538190593227532134
5979403714780212417195845464633392094219717722557028967506496160617881899282
7254 (y1 = g^k mod p)

y2 =

3680522746983239578290774293976651451149302941374363373649823390406217439267

7301645270585460352582388896960827727693397832446148170696485658373640669331
4565823918944147569719897165927942496966481391827824572996924394186247696897
6436084471322995606371226776062764837623557460091362450581808982023039529499
2731 ($y_2 = m * (\text{beta}^k \bmod p)$)

Thông tin chữ ký:

$k =$

1291879458416878345420368760770859563444158065062239115373014896142294507619
4520618170062870038448585844879349272047306204172242067828361178037780343195
9629162484701152452379347438495991649104385593199360891498410439589118542441
5329200209253488970028007745321028073125723807131061866409750052393162347718
293 (ngẫu nhiên và nguyên tố cùng nhau với $p-1$)

$k_{\text{inv}} =$

1791085903946086641351318923965907427737276094397665888615735997365440700235
2916225720045892662525889089491694693483521769717639205011424177375331203044
3631225635249706489878295456608203728562540335565484818599315557483295937549
5592938716184964071696207895811940610642100106550071589372647278017153538092
2621 (nghịch đảo của $k \bmod (p-1)$)

Chữ ký: $\text{gamma} =$

3129716614919774176291994205798817384453860858456549489436117448912596547581
5630855816500921284108758930208694689806236498307209843625730224260775265098
7323615095329336419852586915783457156487257508150610495432903807221145880844
1032911589082395688528973712686642011171365783047525729224302322318139336639
5280 ($\text{gamma} = g^k \bmod p$), $\text{delta} =$
1715085546626436205167544626061246127274087888782140633987265256437219521871
0080099704937008411437788630255961760398040726243051374252602885361286663206
1234406752322702236827877478779805873397296034408937767296140730015246212528
3759212360722309787713771573533458172444164939783772019982021410019381433308
1034 ($\text{delta} = (h(x) - a * \text{gamma}) * k^{(-1)} \bmod (p-1)$)

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: 4405615858061534292792748277069666780211654846635843500450614496439901751843397971727530950281096129408131727629413489887342315938994880492830607516278311
Chữ ký (r, s): (298721617920115943162957954453611298708, 8220732680039752519429966152429286011)
Hàm băm SHA-512 của thông điệp: 4405615858061534292792748277069666780211654846635843500450614496439901751843397971727530950281096129408131727629413489887342315938994880492830607516278311
u1: 38468869438549625271323256353660624052, u2: 178607609109948916650066157753047941643
v = 298721617920115943162957954453611298708
Chữ ký hợp lệ: True
```

Khóa riêng d: 188146087323973633549082376854212137940

Khóa công khai Q: (152635303866302217441544693893709369553,
180998446531185933989913880372170841448)

Hàm băm SHA-512 của thông điệp:

4405615858061534292792748277069666780211654846635843500450614496439901751843
3979717275309502810961294081317276294134898873423159389948804928306075162783
11

Chữ ký (r, s): (298721617920115943162957954453611298708,
8220732680039752519429966152429286011)

Hàm băm SHA-512 của thông điệp:

4405615858061534292792748277069666780211654846635843500450614496439901751843
3979717275309502810961294081317276294134898873423159389948804928306075162783
11

u1: 38468869438549625271323256353660624052, u2:

178607609109948916650066157753047941643

v = 298721617920115943162957954453611298708

Chữ ký hợp lệ: True