RSA - Hệ Mật Mã - 8192bit

n : 789397356526785616432378590011981214453221504757861279118974839706086037035497314425719728717805103329262675230798445553386872807341391114393145475968961328075383338257292890739836188560464264875983614930553652540830040673734912497668476791723456680648677655229200365470174723961774072555102918065441201166234131131506658595838272952814336209910864399193693215969743694497733463454225052317939860122256384715775293719161419740638276899784480792702797043833366611575035790136063027422125129431987631566455062013704980775396901422582395949257830249983941942204400401046100767156664024304355225464460201962416061390588787257921459268318093707811780151936900600913675960224957077611757800726469369061351628858353505738618132020914313507155893664260018858422385648380320256738549259215039509731638761244135286228396479390222945885472114192773024005382900937494661838581630673726109698815045080064467899017820704655615469537438502753243272576982073180889956803281223597440404516887478581945421861592103869811172147845394566290213589129003605780350725885719172159112518905485737923435123645943568358315203032417148593213768065830919707126378257699516435263454852751549732330045984317214911676201642747348564863870739958876966496009735494442058362727914351854719090743099539296120220784194161713146472157444236004910397119233826720347779637341626517175983076222285085100382814659740725934675900879931310499472381889732228838445666897523388269889409807408141032003370114734824679784488701121308086403578808342687652261294016409364884572362299291000634588363670276192367203808198861894482527234829875402587378326055226701022846225098656847997455200217700057342857554306943280911916415277026596620461069677966044237309380840108680631866288203707106225567993448107631822115134396380433987161313038666304409006222584030817427351387855296070222615631678961082655519500504662157982212386003376868020016833561641637202168969693695368112700948752002745197720025223338655107968325170104963563197786073682711478508622110825250846399842694638875324397916349177348846242852296815480036146912964978529357150552719074263670153426565573529933051232928224879364952545640447145276061605998570231150648534858820888766576446065268352670391791834343914820905939442075432276895864025241926850070585178059327251076747769593746346139172002192141968634072596747633039430211559370144073190814328564194654804679741021787925548521502003380645103910174583983712414116026215916575788604111542218263032332490079038086488896575859223529135382334659238040691639399796068504220227619254663345068657876265864351837087806321612836469494576250059850959098509815502809296526936936621896671964274752012951537779084829810098526568379422614548427570337225550261439078559861081389476443049466388831978063055301371112655447078280243481317382416804389224749807187087029644270372414206846195936508057773047749350208978705961179626704204682649291589008788295226098053361764608197192397177669708636838389673214288716450648083406697449248070958772391898796367568950295361639827786273418938114155734609179097277222061423547168072692065100783347965227311317327384690927733692527737077826861141193335198994194686703397534719241158327423623054965385457700306296721496341287554051282902443516148166666509767094710894892696163574639464356037099831728149525964988891115011320848847612036762630108186190945625295340743836203462571240377094764439267496417101407513951275176098849297198096707586854891912123033790144006008398032284208378880216995685740153274706977540549648369281131253086288634913192050278644130330614687820612226649168808263660240981812671249633411687932625127622290930907598329921823897608087681496471111889846703229077517542706563451088301451404083754662564862672532104121907737322398838234953408815228975308642281420521821605821633049266762487247688239506779204668404810151399520503878890668047705266965337658905928677204953012010596123892249438201968060374841069036853672298080342086410402459120891850066214753384964831538754132509049201721346275592031773775126179235116719669544759925566644621768990396325052153588197941497819619100678503137993590265593974274552575734358028009685409206465673103962242970349814265124111054890994865635558239512177754614522610887194006241704864491617608171970748518704090388147788980047337861774395458692680959220272402865405086253878048506112793691377052746023803883117755620792362387335243127185402605867808775192818432760717808764003165671117446415758091812732384939074640654619712423606331902323452812939241907893281047187083101661552176286371863877869158817517135901794259162983055665019674107049098026641219130211806458676000182866405131552319245153203088236611466275540907861245531870952415434705270529334270890711791771517005020418777293263714960710703990732298877482132807350151651260316515874397986091152709454985143736082280660865972330283646013642794009922952675532129449579517123464871312999263983291082100021482896834098427713473

e: 65537

p: 730556557578803677313744155879650981087121498800144113094651337632451485385470453007441633634823956587105509489200882479851800126612022003094730612098900789856068574787755735108690582657288056378927082905827910849172757883594363146026964676539158126313263457113953539233955565281276685606777541726057409918207706358006171549787354158890589395910167524934030469831261516308335756364510586127574131633852148032245750313099516286634005275188450721756174018807361893451921322234269359770828593781315335666348154182234865530168353088659741017708382132963466753594629122926976231075529460143216764723447292169926009874228448098970082939634254282741945770353773637310381908950102023087733657301359319729233379105806461438683959560177977844248762059326051473456534693973845864130386536894663449944591205369612219276135055262162644149653352797208156050652093437776405744679275080860669130557889771449254144653140967982828601983196397761012094906877181749305209017589764056371763707269321017655215014554223996975900030535601427198177729046715421058850357028954168088935979075832536962504569147317710937287245278275967308139216798360396874810229571505172283129122140218840023541624098186730465488823578859720596394187295865993345668132714993977408351528102040751372694459760060462311827201540898874840413532158471895252784926797211905696740460762077747411617216561211908145970243911917839384929217116369558676076572967155379674506864451651555788642287175441886689593476306327910215816113236623547430868620272042694968390480023451658351897843629495197372665846710212038074053739978508507723612802602200240483986854987351376076641337418182820379023098320033257512134650122196944140265049172689944670790279815841441698863530100670909236108343888427580505612763402727956722200022128718207060297396226670576908538221551058880992614093757861368084823632253707312022460619641873981727402070232866005622962687413424028508212011926287887513628808909637362567396434881424111279989477526979882461961674255160306978452434028222076516063267019042064951141378883341497310538425598513063073476461267997899643149213559907082278209524559511848788062987157814396643062038948656098498994022878440555088391006373084869109803447007066607778337302633595167029883159976497013013763324190537701292068810998125783191571608476412529406770404738669917069025013135055651968568442808512725905468851096648353331948727297542337501956517644565255617744102227427817970572138819071568472396011694815467706642451

q: 1080542428012679770671222466565273935222212779884801894090095618247744615717727018490324307408666402259504902395064553735740481925916525292316501624546712484593279867326914504923680311650293613130481968462663148916940387768215647396563796258678717641280350207459923856108369695976857146271523715730953477921632403376741855473830854695127636883234709510775877351245625976813086150197830810173931582360585749926662831092330158622512018536400866826066600552829531873304060224149653912190151599534018544312724143324477242113138992727732469486237636972693781219213319588017194543632464630656676828488984331862080892100304700063177987267425603582367636226642449946659171074219489049432843624058029337747621826380899901128171395073954217549752692958877416211116164798587971953295989295181494002239302010994637530707735583367612819732893789541332339363991051778896352036652621168811796734235528596211692503106987619685106439280758773343002090252228780757372948446002124559710552857282078080568348852610306857077757780241059733279677459894356975716798440502773642412274157437262705303351649337370777442366763776929245200338124509981554129178918919364296250274818611060247720330578381557613261256593466852297051117537629697966097000430831499285612506461170020663868111624197901576600919459577794467400000298396199032338609377035348826560061317979452843752205719103382679276678976332777998171964839453406709774692317903095494623752070195906522145034904504955318243769465829492062856938790306759170792045729818166396530489364169086431867856552361061667482833794422468829042843881956636097021988594237579014008794941509139763467928248921251574732892942345263299616618081625573854054829064020728667184394309591580087861176260498486609470880008594659461117474651598135756094315859341701514065978853600769138988821260565535777489219637590583048626070401849128382270290672004042306894205381510698185742286089283865853630465743838380893098574833925583772894048546774199886453642349773440887596159354625845027015390186360241339813016661508178835049945937214289556910394133575614182018765085279432257040146679410699822313020726255938436719829110256248974585759203384176109739769209579033727729285433970675363965248358725231358658045150165909751943005516818647064145015169002211509908234967598404480695853601520291835251749799396349176124384932547871983696132986073254017471206643017928960070597493374123629972090893174187989705202103903203870989270592226266632162973109783229051665292123

phi: 789397356526785616432378590011981214453221504757861279118974839706086037035497314425719728717805103329262675230798445553386872807341391114393145475968961328075383338257292890739836188560464264875983614930553652540830040673734912497668476791723456680648677655229200365470174723961774072555102918065441201166234131131506658595838272952814336209910864399193693215969743694497733463454225052317939860122256384715775293719161419740638276899784480792702797043833366611575035790136063027422125129431987631566455062013704980775396901422582395949257830249983941942204400401046100767156664024304355225464460201962416061390588787257921459268318093707811780151936900600913675960224957077611757800726469369061351628858353505738618132020914313507155893664260018858422385648380320256738549259215039509731638761244135286228396479390222945885472114192773024005382900937494661838581630673726109698815045080064467899017820704655615469537438502753243272576982073180889956803281223597440404516887478581945421861592103869811172147845394566290213589129003605780350725885719172159112518905485737923435123645943568358315203032417148593213768065830919707126378257699516435263454852751549732330045984317214911676201642747348564863870739958876966496009735494442058362727914351854719090743099539296120220784194161713146472157444236004910397119233826720347779637341626517175983076222285085100382814659740725934675900879931310499472381889732228838445666897523388269889409807408141032003370114734824679784488701121308086403578808342687652261294016409364884572362299291000634588363670276192367203808198861894482527234829875402587378326055226701022846225098656847997455200217700057342857554306943280911916415277026596620461069677966044237309380840108680631866288203707106225567993448107631822115134396380433987161313038666304409006222584030817427351387855296070222615631678961082655519500504662157982212386003376868020016833561641637202168969693695368112700948752002745197720025223338655107968325170104963563197786073682711478508622110825250846399842694638875324397916349177348846242852296815480036146912964978529357150552719074263670153426565573529933051232928224879364952545640447145276061605998570231150648534858820888766576446065268352670391791834343914820905939442075432276895864025241926850070585178059327251076747769593746346139172002192141968634072596747633039430211559370144073190814328564194654804679741021787925548521502003380645103910174583983712414116026215916575788604111542218263032330678980052495005448590892601084210466025324959355745632215049112624024126516057191847302716832775505505226675922056176620877212523721512555547866273169889534847178494821951656639593380444431282028370033461319038760455233770804537884979576290332385671484946196507512081100724205130698146184754043914101767607238170508733290358798595535206523528042209993934362551337319353074514601495431651447844494984268063220718122799252974382442984976705908550230587192971303425641196123324713566428693020973382570669011109190737140427651426575506585863622931189704391854978324707993943381026615088297383628848991923136065790090567635185817157104257469519581345736696304153108273877971602262678416913327314740057864035671621061056199610751325504912295266478137819869478583409881698330740290677690937258710999479799324889480485398470056264266978822650350619596677703630939278981298211936518479760501922376175256814811111789426829398003541245997393328792169213592171139734504818970772575347571634691920442141233501430154721069440334525262298085765905143773999571749403442585078498400096808012787911845926199440958217593963595755182899673470720245644263197063156594218350179628510586049621417863743954751054066177829055717352591978747120782524754958141062896673292801257291298037949775283486091573834715472988561478087610492930427301989072317009960708506157648342956269003810222728750300259183053111153648697189069208137037806954078713751661476334171504524776379977636135673911536478107269331506859076402668935716124544293465951694561594418829447325355718727176274133993498367999822047609615320821043224929211141832270357091706801953250032761244108026077549600297417145799843986587229814591296013047061248777653562928284705084320455733476158647205756425136131527107610023481189725823394071896481895720921078988193028665672385388856028043047014275970065186169567171112334962232132217491186239633488554658555106420465738653684631570574346573198963032587639731373451105093811030371338370696676357637062931727050945232020266156296094526403375102552811851925810262226826254523927534307084044825316447712475521624165294889667932732240214734166214951683963269990308969473626467761419633947657269501568712859328003536414469808609894809149418152910515732381852539126813553013278324255809218473514667184696823278780735594512823612603215132558066906570191470350426451280573218400359406786546288658927737425341976826535875541856778884126633310992833182353156532937952881464652361418789579055778900

Plaintext: 9671464749674

encrypted ciphertext: 312790965490462295974624441624676303470220370525887727187705994667860526183768843658809964452363043482652537065092720048200719124629753405074614361371344947214468301455204331354064907829655101920057858615936850040625128467170545037782955423266077856988461919738128639199429488073832905120356190937197819226380052305948407690361815950748680833400863259233976779964322357730662002525134147101829471792301038458087354939813154882124207121185195382137195465919065560622604090300085579560050129886545931592602975415913925359213410099447333242113316311547918981873185070640498096061961386873823474394606732787471790018466236353856062527833228355213599950631598400979381974287428581752204884827987665508098339903394938070030688756622275522513705558780082396756225577731228009315058125093295544318998755534776074231301343237029506192185393965100480171968266818721867754015990638303831658953587431978891912138023678657387623343990393454868067955484743703089333869853060324806218060953340146665589640973293562589827558683470288502579280609636886175723863809074585606088262634197185986772125939764776609288485311164279092280125099476909132767548260789200808049642769570529437099197846080097610444128958617256079271061435405903233173951778359025966286871185332243666108573772838903493348182034398460545918424448005135893691548934108517260281640008009291917789835011166044264821205756493032318548047706141632612913483062888712311651774459456710126711399531661857193466142684366803145215404807403492992078804185008042118663293021219412855609691476859681221123317440008324350219780790246153266353088516626572825872037101757019496229404838265744743034012037066998886318779158247726353315877426753318817036199059359005149357380153262298842820448432963371786487902070905359234883115219192141267861698884764267253121559252901858952382827015046232347611210541065070488270822462528292628311639272018949509477256217607564497292065401138557204444447124895326331965704301305340930499810920394877443591312721613087556743519212107599219001697296977144529018724876687926349775489181261448292068657555243943818285968286812275580115220127920718065024695858172738954768958553133905972055196627125814831393703932993943508448715535844179447071449870222864790590697549306901151843962749088033309090121161498652304005039232706334171494225459823347197327265937810924831002901888161407170498924831490021850152845332609476223151947754104030099823696491124873247048875204346653518145959742975327813559061830450047403895950149753852264640972183115593363670312398868498239393582951595659765565472313371450803743150394351056578580484950882367477506358521146323763985799734632917917120514220881711091572068554282250915739199637182364468306514549604085559843454437368332538613437511954101032318741694599829371915406121557481730274691374019330732150481922726874277732789422649226014843435548460912281953466604939777547223031702768936315226889322066294586015352125249209080988080109689673830386222632625961725482635874466368966811618732247144026086025719657514523604761868437905897164610639442435514898413543227479436729194171902433005796500536621382622268813069703137476334948046121913842132154105425171920710801414936051254327321883045433415766921224006582603994165919888474282788545659394642980272347166403394019651187199620477421519120693436241438626499946141322786344740782440133041390172841762758791090051615074252416853803920404681384000176736705786767062662702520282706412753366632552286837549481321769461419876340892419660929165951271359017170197535436261636868340312582980563841553330324979310556454219723337993986733007321470248730348755938349650038494947082042286321565979400991365477791204533386395692528242977515824332932888445637062859989287769218548881998274959394696506060668478512439273940267287135296920068025301532831519464393845450107344966452155700202477653171373274783355049916165175976625092577799458823517459589575999189813345662785194778302595822939308459731466552224666115316736547544269097898924355006436073103312054130224339667575997934312946072219688232724274367898664950081733320065623544413205269562036809758086928974990161611758637479030623324289619925280500893909864213978893235643772081554448392885788025402220019100681604620725995776933499343518709770302789108557556649214579133985720755048466931099174728490029199090274147998923122659635217688956351104069070732492271203921097560138727548691257939244141809098473654629236951412138380792799115702016009537533777191820709313937177218776726251601386785572725307357245769413098715219774764156755371174530343502825956574575162181109516476186322034838304759198154280893493961572085899730196512547158251061190297229360244346929750919303391882887141663541207001234078699224801691529647865988589569888341316786076273259176921205861986884546007806199119956213596046821794604020773899086084694883227741536228374601563431501966779733530298714673772522192167849257024176111141287500089529558644097821122

decryption key 204296329768692659723661035219695948522835801794376995516073855322259567483392128873378890074045079231085100547623059264705353459653590104692343873200017594419741166061643723695597320508629238392992631533898721344355376655434607181789752885613036128606469959112294847166327929156288051705252004109250472450379130843973395737430961862042570707482768071085405658422918699396921697264859714548492881388125647209427724137062984882142390016284611421411296529600954134289396555174905244489474103488044039534898520024023836595076168348084593705774784608236227463596576517114651496280638090181518363353566832254826110704575681228643451342752081837407809377252571388560612447340822695475426462275075865063240382945001049953960390881589448271890246920663353218147032714072640064002663136633448054145876757090830806868178779726529615105413621752958226042621715714799990226043044964784298130851305058256762440075701618500448509678875969989437404003512411969133078373139643765143151212459046404754204498137901852936010052330832006940328557688283414828883358434894531012873757315042550023946520776948118817238875118373243469940624687803198638213078133403138658444900708874666753285165783298049683643438913325873613510781873147115556536594917736869733919621407072673572035614900152371965379323446559604752694115727172236740852427473410974011912208812599407324440376517176210818127056768601895914949386679654469343753163392156313736192943776018038488877951077154118742753088492241289064098520116265903328707311902716027973053447789986103083864562567073174874700600213796092264524524937987649607369034742962245804423818426578880266849181743111811631366062695765913493022368716908997780597438386158171800351560230220822990204074163130496241773107011658700103633958479536041371055965248592528508418802057598290875095816733261313370848633434757108916273001951673999769905034531021787105548076338606818415360872698460469789370705021205840037833907438282474957635066417642658792533237151687600698771650359273882988037059060098983468968486991222820153151854054936860304577948606226823884112604952912108220190587373059776707958439781782697425797365788724265360162352970194302928533208711746794796010647416580879417274258841769024057288481030598091753931147884050862975852278098358611491280455242154267810633881912813823210962761437496084958573058048330509543948850546385660216753733033656977059373211668026771823629834646008809361453948463785631746132044828427425134533935247812191036502912257902874259849968926715128965153939213811078255532015014410912907457973508687398430231798529085941512033655039351737364644374957883952186622020535868814507843553938243665746803548275412637120626259733242861776041260375360279166990663878320037957083388866936829026540847908559183694268236867927107238355133533219555344695939325617267690584640113583528497195831869513001014645805513893163254450012655876384642058685640144188755979301283090604008734928199032398147646372697067465199813800789305728699530297349939485979504606494745672935942031349251698676934438368637140627030312532134711871518820021545208215387730993448897365530946569280567032656438959763412131611658212556967473162172008858893542906021164019787548624465537837128474257900342336322425595102815432556958476678367705509663930257139888556837366350501906566127504039364190802094373853709069447199456822847744866105180552559705545089504188645605695537687406168470838790122368188687790665039611775580733986506102967216931041436427628079066128358393865717287684420065500030778698304877190619524691174701487160565187678651339224472721029225149323535523500574658005964357330551415008135846842813027704642691151374473478904454224829150196715727207867575759517980920585354362345401342607621941836289694463000536164047905750702818394759586054134976602081159916826169271843476869203243051612751289783994158837028454807147165171098418230206201120576350736892871646000609278729631855108484248299444382519267186020189776693038861052456866622193283006481246868283434688846571650458296204362903959375416386557511710663434497847878995287212175567642967141105519615910540210959663416333220948758268527583043336647336710634989135475796743913217232739991556477759664910656506845397489308859525671404416927439587781847501267785425579892783046865445759524531157503831124206046021642875547069222311397054934408247164490204630483693340000295643129120344195178194075789799174687462472002258201000312553597268619194178649133620784996684344450072249607261273483615885331004764672286572690209222584397635803121902177095913901802836325773109383268952229541595840878554207112414088319471013252234631159583600580468720260332917457103848940539038082412412346935712993024282860948521923364134112591797014146663482806021234687318311099520610801831680114002777918100187699976549611110019878882723004235982468531818703286517477127525086621970388551066195720812289013312065347111888362112233449896880967318623355089826642995927339523705173

decrypted plaintext: 9671464749674

RSA - Hệ Chữ Ký - 8192bit

n : 518945406320984123173268159345241404364865815940129352201519321216965152557673889428367110012085689578032764720019016975427658378344134880153531501887588250814144745910666690524694926973086680890265951047116537644206991190422452930650950562595613084782338765076898516701366431713419790700353888755151710504328370741860904865914363718099901580555843814561555150493933968712074189531516349422098769841997769022371754007953846759748956359249247210098342924889811803763545924293755568891163527783094265045054191109091927220782471543645678157972316833934301236070744942508847103196037320664956997142701028620514927053829881557655757476573154793230558631776219143754022328440742050787092969939560331329254705565736448150683102391384753090193384815502933721029408618992242079915362493475212100152989908060875111613764586960604168447590787016863340429390510234153155927097741327057600251651904605695870540210661244231775518486628989520833576863671996755271631935812142049899291654805648621561062226865468135040095423215370266152110867564718703678804677449971927037056550173082304655095668576580550793167109819567430376449109499640339202017416214983060403510547552644237888394428236328322334063781443953160193491402671999491276953477028179439583175557813544534481159130361277810599440510402600999094908274300288189621181597234622635972894551439465220602432332751562080156068484837758781688832868087010511263206697310600693134978211937181490884359589898504635317337548944620209941871265123497537059083935122802131459808459992383433975810757277853545295747414817538095372052379131563084483000845679246270416002218660140203936670488683020225442932468356063164114934896256226755158429047437613906404085784343103884019307853703372850760014819533532639454878256992986869197419102362022520948416203291875503177941146128386152910413584945747579746705664266932689409603652963072454119158912480736051002236117472353831214379244540363832502776075001856442014069101206871008381628975484037527051807829012420910077659999326112176187726698321844221510661987061023249188206417584945714732428900050814043115490242526659819941388245261598846763055933953457455576279403531325711835033192226987700817520510845648528416377629608432262940643458359280855819706483602886293564187035275210444313493894806528760209740096900633801808625715471095577596168403993564715189289181116371246357416830260825726464065999013788972070675551723289618549184116248135243769056704761190421180503260437287578941438291892735602778996243198955310792733850382241262638731891745819275035365366414611649384622351551936881290966450274355042964070155799839192701259810577896640381303157335623804266031542265564340040649060865181580259410457104349909678877711058945964416278732260546604646795740121407993782164428615587675650792755385459915778123104719117913526288570288285215018802147667148431773392669971899302012614042501429959688023828710009391952947571525865149865120303003168118010398646008949728215191797939929684872732495384300722785475132916170262362076077960843438467483750569436765133417504519971220951501501324654959410239532969356857139344559942458328526893202454451042357796913170798572455939984611322491787289518939174342056163404136589675716842601062595714155791121394562564119626197362011841347713535901665854838083059750745132365510949289866785893546042138357858406153902608981656966955227897395887678191681192557443927692095927389352774355729821393722221811269258969348123674628392752107450244163959593381092275789635633517420277060224391565729968664488298513243075998675412903416826226864573426867268399896441595910081532844598636692490719751637177657504106611567134058373633377421529704530538177069087072391468792941107935382353307868901541227566014728506816573211120664399773015531565515647706331525952284882710375564855215039201525364523252649446821846272379243791403694157291323360635473931938113261875160525369273065543063764036015788462962156563831878111835417950552509244562692579535325508218751246844622394997588694684808586249471044595443338969594650269106941141517017721104528606393411908317685639444738944248720067116600792931092437175109174619446952066585261953704630602808993294127422903576986384694761069863896595790977079517073719316171076507158957228539592896272907600659612288745053936411123612621672789657976558171128811765557818872225503908475869298736044786689378718786187545968171082571033714001584932174760634437673746752084776431338346809552556085677604211992231104398519370133789235196805268136232605680828859100915350622744578965659937846248533112360622133097814679253060551260208367814902514893122660845778943325582813199604327505107838918098796967418098601931344623866633912993055923327012656647503711929529978185382166641429092089783389964685091951294155334768459822865367102846208689904731394526727140043745551376490684463413426367452931446198791752517443603271165497833816949735800223127704038258975554862232332308742733166118298169240699803

e: 65537

p: 582648321366229409389780540159668108743185223458006857595922049105907238536770745423259636749119869238682813986153491862775865760878678810280203797840907583079117623588106516147612868535213949479546711294358003607325895020370560033516862175523639111890397063235717940267176310441019475497466804684131078979155868121388051134900647042797915427395274473215536164473849936359903700872473927106317377613708207673017085976516343941932802323085019218138813655335175137758499943064425595666189074745095751970681042623314093262868274475548334424272474371445621759363289297697091577627585536563335390480993214272664111802113317224450791457419928125985389025945720711604161842838114249617818069678498770415331427613265529635194290294660358321893826926475739359794949360407222527999987535610790988773618150523157192232972763501513108257964400627958734960605913532825674932343190032133311392303609783750764261573870743445432329626757990297655899200626031240109546176352659681068298469891946348041816981153866828620224642409583570275766912260730888135472648055497051223845711705357138574463165624186380307457360616746815682067819898194167950434656777579446054002030847273577052075196934934335441542604775311409533250968027550746207247140559338185125782977861984025467149135655299135007399900910999147669823074290358210832588778038462402274133996353070261021225700094088599510165515353487561659142998883101277344972908734356386982506912044227737926298106641170114235564374844507848712023652341639577287098775934286410171796110717577080741447761249024137301032901203887666435057562017815537483397971327800651183794945276863136589519291662990358570626509658797716364383662949233403810496264501179340050612217211498005968088851089495138507615245106947539612753367925205779064819967949816613348097061304556839460020673082757162348196545522216394298656242369851360812566844471931006138958443018315225076637985998231863795912088943295016221406777515458433024189745520038623014554567514777626929140859069926717275856861250968804569007486475082673576563292167351571595786116655614984401215270033928827041289693287250512516870304755615838365000907828973365592587987730822138353571640355773047861219989414730139416418958267617857773482845180529656623764059915795830533774528970796342100214857854360743194449401344774168024495912192571733270543492915338900941737182611879047348521737428249898355465564142496079957587859892257758843742554065583778327158042661862886372522261488496715015633383

q: 890666611900861919644352015277472045911061588412557085758274394850227784886144050671762067589942125544336769791516521691358414431345632708917550907099577193663729291850213248596854850019767075956707512761372566386660201855901218719587671039078457077875456352152677930329540749220203015037787249623922336543090914733885707021313302987356427414317967059869732198911618468938466288117968865607682449188765987417760377125960613434514229954961650734409258623405828886112489249055111967804946311204679725456008562624456559151509785613255073894342073848923772840150351783771271811094823708126939093027028268955170967435572195337373191552375849377480933899588155862345039597262883537233378601165429126049456591687251791023677603759390021815849934814861322485723891007538560501982862161151017934468225923476794857058345333852946713418778284555979982596915790847966793400168142287407013772099142743916234370466506942815294680544366894999493534587581964039002723492850730692863050048795091578329862044774936220149271285784312708199514226095717160290065285548688692846614730828315819744810072258401900200056954255063876139013976928792603539592384463746514964477547000007045775095924923072573632368147464765028176226679658562542854468543629093338228411951201322836700909534330576268923193393764148271852203208467318397966941762960640121668691105522224974485307197188976950594523414194735206706884947382909456915032688896248018915703925049040904238073094351032541444679023784738261292189427071946566262915309549535254753618033436877384801606347112967107442041684222851263768345762786747957171128858584389680350967259725480233955581101408709552029910153910472786448628495281525670037244182369239424980858069214725534243985026983561387734604630859552412833813070687155501041449304187540229197637407941165844669727851510340141405026473753999954466084219415784834193536642955940369866987953573435689461828608236940652708483568703180270675445833964643807334481638735610196017365530948917823349044077388855235642321245929941681290409400499687936416737197521409515940078476692038956813033902719445920263667713097446482849750395821617830549480629588958524914917994283973350089387724277824435131355801439995920759464007260601379164017501737161058829944334626839789990703246258758928746234884167060295494227034012269424385498369254428369761993796414192280736808137046339057459186924788926626024772217805797814333110145492163372286163602119851989827594879330048720703309887405000423940061741

phi: 518945406320984123173268159345241404364865815940129352201519321216965152557673889428367110012085689578032764720019016975427658378344134880153531501887588250814144745910666690524694926973086680890265951047116537644206991190422452930650950562595613084782338765076898516701366431713419790700353888755151710504328370741860904865914363718099901580555843814561555150493933968712074189531516349422098769841997769022371754007953846759748956359249247210098342924889811803763545924293755568891163527783094265045054191109091927220782471543645678157972316833934301236070744942508847103196037320664956997142701028620514927053829881557655757476573154793230558631776219143754022328440742050787092969939560331329254705565736448150683102391384753090193384815502933721029408618992242079915362493475212100152989908060875111613764586960604168447590787016863340429390510234153155927097741327057600251651904605695870540210661244231775518486628989520833576863671996755271631935812142049899291654805648621561062226865468135040095423215370266152110867564718703678804677449971927037056550173082304655095668576580550793167109819567430376449109499640339202017416214983060403510547552644237888394428236328322334063781443953160193491402671999491276953477028179439583175557813544534481159130361277810599440510402600999094908274300288189621181597234622635972894551439465220602432332751562080156068484837758781688832868087010511263206697310600693134978211937181490884359589898504635317337548944620209941871265123497537059083935122802131459808459992383433975810757277853545295747414817538095372052379131563084483000845679246270416002218660140203936670488683020225442932468356063164114934896256226755158429047437613906404085784343103884019307853703372850760014819533532639454878256992986869197419102362022520948416203291875503177941146128386152910413584945747579746705664266932689409603652963072454119158912480736051002236117472353831214379244540363832502776075001856442014069101206871008381628975484037527051807829012420910077659999326112176187726698321844221510661987061023249188206417584945714732428900050814043115490242526659819941388245261598846763055933953457455576279403531325711835033192226987700817520510845648528416377629608432262940643458359280855819706483602886293564187035275210444313493894806528760209740096900633801808625715471095577596168403993564715189289181116371246357416830260825726464065999013788972070675551723289618549184116248135243769056704761190421180503260437287578941438290419420669511904914164822755355593695727994450768167948391622831079230342991696853289600647212874886507946866496685029409935875607614881182062055872956155604560310420185484501287074547009359015212806641125849689416471007473637900124606525731362320088966407131216250925143404348332559673893361533367597377233138677060504364948505167883371945728575043681933533784281680026475022680981456509298614215698955764597246365607532434576500539247818479912572230724427113986527656816830190651720662553979909395305805779052952133060754856081458953757463412623069072884236928355296770028782110726530677017993303171731575160295283844295315361550146680825060570276920574468408595473069800785604743313767394595322501499638657021397291510082539295579098839321258652310272281026616781089643347665250032424471691827665902788791741653390672543834206604682847175988520433977065937821391276662116641790825144868220679559640814871183200681924802504055624921941613398443109541600055578974192326109705714181078565138030790332322779861441737238944995921867943517304430730884112769172615556141739945097552988981985146359754085024630904088999736017611865202463678510311216639024528764286511231202511519414620630619785936992649362913821106827818873666669119437378187032636951421644648514541134788995842422236890368228184305243194608273910845023856112515258700262647957413940288948989313693686714764609068554994607527665927379001869562894764867167332226670767373624091761164361176197868436788704442505031483278993391775494133267425179696980853434240219265532141109053350700264384167911338903537816712454226450001776481221576782923434442395573703619674044900882330555773605838671806434793835826188105964183732390228262657136477353446172620882996807370353571101113017121272749732464145878850959267455539430361866190366566060924187886530515317919566638700341822364071303772182677219400421047997922730098390097627804247720951732998566066638056355109645277908022957571506393413392175689527777632457621982153933807294645616566451955682054286319408719345630910218865800425661861657043101066590192307318863187868758350509721846675854264841747114325281224208179308361011435075307217589532016664879553465199484425522811076618563690750947464836686389512309729812996475821583642746546116951316860228119118235349929873116646092024465821774692851927242904628361989437810512563872831171026245308618658790714269674411514735495309376874799828432528604670316971518602490820801940240420701666901017224801030285004680

Plaintext: 9671464749674

Signed text: 512339397365341008650228626236633458194656153836212727002905308926282326612695770834383316944860668792448057230381638773237015625828635971808975346158751530604208790699821701591173587465410591659564969073802655531401813634816608008505018989763798782697290921903875058589922935892189326745216223417564077991366808518730567178587507411245898003638062810849271526649595923301827665196139357182449264604994291595767212731798107618942270521465428925247265631980195460742141824375024008782295231915798760876334663490852490818153599087516434047880301757855788213188147917922182315206682209752394086940951918481926135434915696242542338182658138878551751247592409209086897587217481401371032466621914934499875306754278945836333155815247358438844406816867362217675005048486269142811830696793642082784748141066466709329344565901705653491061162591062514489713311174154385118491357284536788599536170919733378810905409462307208619633150753284097751619978475368200394223067462081215714923175458104636110799680605806573893117954248015272691238582104261459904526789608219401637317323011186918149636459263320832360173032175098496622672281983366440473739715983693643295503914994462843801195778355674900766814739553408232304475643431438968585238128133385189072630338931520918057432474930480863402972741058968489475732779601476694542295001412095372489731119066058896630598796801810198267191692311123297139284229892324801544699698086013679117174566612082280019434413810023178494836565119465310746255756610039989393982094081893394824766973449791598929531773243891665326144088935050866344817949169437927692447120767943597702054884469532216363991653941157629039520409241419223450006073659073313583478383639933054218534004622836200509109451327118227943185215796058118547102129635612428908405759977408498063535093231055366828595023944852533899255266387908290295646764192499567981437699778336845635880424418202375977335912127933065094023886230668745466567385804921562968047101867260833146323681082401951287662270298398153196289450497868099430752245562582212091523573084357568816667136029312052622239852718933869718923820382948394512208783674847691383191106572605483616652078701029667315194881202817508637843162540214839848555934206292416723865051821526920189440393238170146196165699691394556415224377344327611946380281306883715592741148419838728579756985450072162629898769960457129146577177382835082647875253553335666174256475928737606522909586602792200855700721395558585127657437574670360328174651855344905931759227711771669636773208869713218440194265305477431322424590082489542700293531006289818092461991592330076622634807108600577257554136962565507608024816007843601960453555563940513921523078945918608397430647104815749039919541508492253290475875293595260396161534480327589975665303013744658846841233273177658340003938289433785089798055786700072214893804939294854713266029123512831089242553866648600396021463967116368243528498917483500906340987665092758465836387755658547421633514433102854719863082425222396583833929965117797383581086168565579237329112614501180654217378056737671726030574948780164104274525875467085887041032112952273857436250088150537540431468747369850675448179427522434792246897687510301714943607169274888174807212857935891512087042207419638441646847140926312949782699111151033468497771138728766106788913396345470263509634529913147855732394411838915149365260205455876600044706986538949164996798849397771128881235353104254259327332163746066782470413290814323908335646655833409080058882139481253055778130600937034718480366632482170866718170734613942500731721156530178650892230668644974920972068940677417382880704272365805503811130111461981129239477681828755563527745129970737795576576997054202150702840166601939346144142078006760288786965808000443005855325408652729338000337683423506358922059841756119810746859305803039448394927940721666381233805891727602305323051027957859234989133786628969258406030256984210370767946943919100280937618340598469943345650091653370562232389391014045960099518619184397691738070729178102241184659615641654735054440596665338016184964469847122204816388285439091293161941795191777590005033852017444643804237051527652119815966004511469052610313984372231545698052102709907488943529759878388073296632122218945100613840591135115831494693861609294389149958932193958383958396909145572030988791032297054814568468963844484170335176531571717717443078594703443370862920515962819278633464890803007592838914505047094533589809366925880951744148888211837697633162632717612415395935219000578557381616881163431106779295016403998170957788902706830181399384679290363312334983299915770486947763385806993205021057695608741054631088062662673232380268726554065660104798532317806121702224808535481176330712677299521509036296126260908791664186665553688905729784806464291849398628837506698169671513245249459120717513540777451522394100241800554644253685526044386927433735483105850566361118579957800847202836367425062353005315799960087365927

Decryption key for checking the signature 236196690802884407436034849399716280128775843015062002331799133811142614639712749252464447938576743433833396994574778481774137079323545468057733664491888092734411456517223502932101331716132911245185819518507701014526913655173586652858495267279010981674052566084483663498253800014947265465322735976279359333408776276896545939627379271971588022741356258976709775914118076090032515976251601185769629455375611519726674249710168225529878072539875109175327999550455411362479383794779054037482900807817245708972358615638541542467924129505575991793280724467495789718086743215228042803829855472710106775861406270066371043665281245453920529909831611567119847219934401010707417719134147625435955266904880040592926321320056027690102708891401802453247412326426445589304205195837298042256249414408681133764682050564470517829376755845732038744306054992089684732128870325991243868326686372601094138039008244230317895903295149146771151222303865250847067556830358621809191957831228259547595574983486161174987643164151549674327160097039367858081215008227597159844418499666014440084763002152456732055143977009164432026470663547014649747276573106459816248962826032756707144406180096311593716524427995283622816679000851662597541088287117587015659341647687616560778095125195218555864619170175814741458791204742389825883304138065645516667896174048376267933760895495145489632629603815996694490657575212460078972521895059897007683813386454606150191248824125174932667151113031827530429337154221925875123477864535040288916196622744088295566673982718953636252480905342060619949594768510106549741628628030685619302466793368635105820840339382993224346658007084619943430407144179965277522932495962275062637228078569573332237685131235125378549035169580013129713777953600291431764161371520229638439421346259019642445153018209321372758104027199218223703028010201203358152790306776208844887075018512198000994863784971319189177839736979588533477049521838957006081163775818374928166072596476936930447071323914650172814312701272971092972212621879297247351637125460174276155637933724461525691291046976894786481828825428263301012318655656637192272577448342159317567998194644893492810594563600078233747210565270422598216549656681784825797848389855673229682765445300337916363266406690125061187958317474761237306989699656503903708598944194487838876768654500268796364232785173098880128530757250218889888610253301107719680250580759691413720987442300253347162725874333374844628932077285707207100654345655007769088681521875442431171469894837565070179438643002761244514283133457867500219739983908887735137490468666396776585451418553523490199940484677217140379703593529846169789577242058946684958827269209302604373244093305619506598008482706637820115172437566666858931274826694074322079170671626896600585395748643088059653131720982617219311975840407603365566590856737238435986562372911633481110685503856079289003770147420574198724990571509086202215316892403334179426435127277463175511164521228572412158678649720270268350406386781652762092506554371410525830845707516782505514493124649394283969995282995614153374769066475138554655355322817415535036381362319464298805106486653617956183014161277351784309723783715822739784132955434201440536708303166880219407023724374624458120920135983690479750637147614587020554732860006016248361410790704049773876570656036260624709340145290444470669704007725060774501781379589463212910659120687912067093930663495052196417235852452195164813587101411739672177951565502043006538326753510579614576299580086065738183825913410404410703442974194602284960009642809745867343765256800445017388684250350764770635300202089310226117556251785726009165334237184239674378078224800018169241721692383506208040798260021196920870243735562414223973139203140794063509887691242458208537226342278079705221466529902230596399234081209357336621061780699458700872169953433464775847437690250193541784682651750739990649428383069452894593731210155909379940244010704255706205669625781092857227439905608790015022067443210479290200605611356950601312802568814532831626643645991243932885770111496113296351536664150233575280009494141752067858722330109999513987074302481671638058887786431557941401598386684145548312006698139156249268640794773185783181639382146122722306020614422696267207667901882421595535231156431196234195451710353208458630480377438993208156006842502384568948219185041077804978534600908996525142579666665047251881883768948975307359458037451580162779425494650717594619503579743804134119535286884671184003539943949549761041256456977257853745167884879807416600017071979721598029066591281830942718838122844591062677162653365837706647986642813935049498656913659842481227403046148296823472719295285660488121395984154268775847031914672198563895486206062592467473802947107209329726002993502852377725525901364379100052454775198123346856591692925641434319552952855803377833410378108824344615180578656374237515942351583818467200870170952266562416275256864214443603503342996053701033

True

ElGamal - Hệ Mật Mã – 4096bit

message: 9671464749674

p: 639342777305743824274863802511589821421244068309126048261194793884636572753911040853510125638054004499972326429311211520850970402006798906627872242548213357005437925950203544663818900662023245560808125965288613871895034627180333719789347010778989575983572394333736065218480401126445433539095161105089554299030487350167222767415232261248863143905015952376354321035315674748813048397803542249049880659074391542000518312165803067988022488454211498849387739651214393416272576796278945234678093307325970929261925700406260328969423062976079772058106357433134945133394981288160802798570234304254502997450907565546303863412774075910653032145766173331317352610764987110413784942316317253281127985680101687612009123124732766674292172514335944673800005778033879125090819959463540676264827542548253298663480302203841124055990524556471996677574937367967976605141665690205610173363376244852412793549299662105982033503099648647475313829878315769885370598549650745134594428980539331752365239223660646204157972774260333021239005142541308855372192900894797155848586315169339928542312768833745518321981640523842916230191881377882271663935868394373680162641032405165524574907424266532037550994746711936194955145569268615687017223874957589573269500264523

a: 147771924819231413421386777974429460969812304522992369261660633247558717117912750164874663151825402030471809747436600574964233023125400129716243789727394752830052194924087287177725421698356071320732055623339235586738414059707237184327709048328554777453892444781558277316997807550798425769697050026102852113415102913472918426116147870074091554680953559685301486415166702447751498578729595390472409302541454780486348075686586273991614672208168983147183525022530235716869708698654334865078087838706684899662132234135375280666064696488140778522100311912227263042977094492270362275469838558684578362070667723202338070568136144864949944704962865989721859085024090992621594845620575244462911150110615464516055060389195817481446232474313595509527007275380996924311440181121131342582706542268673549871376881430479348456573437109097394711731824802633463546156505664831895879043278945261985798788564019494250569470477399761060203085824036427858352970357064443355038007046758895158691444201682648012674651947144160355675468697883837386658189901017667152242093043582754349212583146633738798345168108178266803072742302332367243405847442215370399049005981449220504978105437969676228194576565508064210702090284102170565540985840242462669399494924955

k: 595682630325379081860032350305914927205438454331136809133188796586443177031266348073594718356832395866592761527645683048106904445632317483314278386106075220906083510844013580867069491293016423727877738884970828977742901760041183873899586427317238581624253815039331958806260167196897125417667782867328684370859498594639644855531179294968873434790814418111104585539910912748279048348834025359040617880005540555591520153909592837056108504135348772308976166409567821383794188451932832342805163691183284706871047324983134493141947267032847848570561791378827407888694031778193113979850458952794651301791018224993610558486809175404110852453460472827024487582569801215754308545337653931823181744254400866665485697268921868139897149383156916497241494695747138368075936262527080003008700156228326829571397475389561226116235390926966875801405353960072875215364965407688621250941424407171977796556273965704825667286746750959697374771016502784544057749846203321979711940534829331414236581298952704275739849959402260643695651330199450584877755838586996487024062520851368676827523410415623252573829887822613337132394080169785629539612283547488158808869546243688438389825479850594062810829287438051709001839689848670991723948153822376162656114551214

alpha: 2

beta: 115312135939937114351636054027773486793076756574754261012298718451651823685893649220548651553215688716295959010603501244097550976276100328995785755833201495345616160902202622800354554166126046438561343895813922251596911028340497647613556670823249986182485281703024740324108631959504742766534377320035488924263830883850295891957492160278351378067908844582243226246439856610934403786669505496789360102723978664724788033050602219700148092491224533089729825280851156097804830236223931746344067149433162277597654695238422783137904146084740423287554619866482369102165016210255202222550790489149962761462078339485878480390974954463439069010703148653312247924277906121394167560051526911293059073611471658791751040943631272186112734337415339612751892511662261363453437381994820566584773234253786020482422044242591665629430675628091952255755518810241982046173957952096154998817296424949275903074435289726206976268706894882241504336349660851894834138988249322472676129685866088614603057333002483334361235692250440902599130686323047232162077035750395027822542424223091044771332752684709794812182011490692759824432823427984435223730450349275114379360037016599202895105821978281396914342298929954468831084745127513232925872504149465673390463456795

Encrypted: (515074566749982361296380812832680674986840239427567537287462322079876079849664473494475894577006654551656294470696913889239988871911832219533847044369486879927445380567072294689740195471244857238901338877054323990974535267074722426655590537379878034854343329629309198427571415171457229893045806603046495961133004259940843419000149777151989390177982880947403186903074287419682180780822616698310733556250240389301429149518418409993943377300263088070423757040792371572480756180590395631959557787418261761373233682825971204875336904883296652616539868120237385184549307345640311723667965182484124729390756465085911774994009450939440606742738983240182490374807960496216380283540100138632112216450035820221350742757973007736724556361094102235272289928216125340260613283096462168706554847759245971359463882696988195565862189602032352805350177236217441728619086380358851716398169566292562281034860314934901569813317762501849367681296842669695828411893594541689872475499562678047585682628331230695133021630073719378705863606816013443862473881998194921825367427473986430196865754370314852152123041272629936891930415285045739987215108855834714959225677115478029507620005116122995727914411788797506354669038353755095872724855334948295287843224031, 566537843802780310771046678719288539337178606533862702417442339116390535275035545789354709337457442447127798947330286876737650313790121538381216548823035585310057391710949574919945579079386951340585802642865711756938941651026580100832305250447465578474515569695897888953927389080322527996946071936692571172284557424637861771015848280778858831243918890779813274083236654763397302913089004435994406686126147630781990420632902529678437483710962330571064239295154348893564911003430936835406319277997870172293147087648445996483383977075678072302215910966437511677110033395732056156168325299167533306161271124566662292396260961024228565438750943431217493542879710180299878623899793717642912507787499014934232124876948535574227576826507762131139139177741464173023942936615367850728028002297036012847598736625398047902181880651755175646436335886260116340365522844096258473515510196737898182458456445473960206530464358407498712228684948234833660688217010869711522996110788495547379740660357031813333137761139844948564230665814120917943348920179231835827521304796773930098857153633153120229857965976018447101272033986074824461249850201294461643586928099008165554013639373118789828486435520822962330148301969042054492844227590217498157244711144)

Decrypted Message: 9671464749674

ElGamal - Hệ Chữ Ký – 4096bit

message: 9671464749674

p: 1027837961416766653481501792031618794288659461748080553428903805921533170118466963591134675637208148498666518924610343718932322470421938426127376584651264355069204612794982379898533147191786652619280272440858691814833939776650090175895027030626515109810550946886343500954797702676179155315888098189367283003898294706946134613860008523042541850748743382197594329109156176110856792601678049083957031919215989170756095127709250765344445198452962349715703823401748765346523428038690330788715846817011204968512418605900436308356897148903916961525136591567111915697245414955473920677893384751644837086545001808795817541238665177261512677815287528124940528840533647501431340024124567321919287014829250874096817648961866558742201789801878333203126072660528800561393907540100509000265421096719664467923925836316093135095590391017147848475408770994341166525002908316018877607269255166382227858877630950561337490276986968818179333256066850441778565734835676349206742005474814388800313215659367681689605983883496239554927028785888983041455814812077689961462850633597582720324269391588149764474493674016116890578480336287501348072025125172708519038150018125964442622053260603305800215885140528907270959752752349515114939563732896323373242106249539

a: 993214944643410890631217222688135302158946082389390545230183341695351403395222148077738417489747487617402067227131169445771054663226298324822438809224673823577333852739805058355254931605168488701806000291612488815479382535994408489461268427510810746378017429473452419396393914284878211532164703174229502523101018434970055933640898077064131181346475769662835623341463646014709331952420865633121090826560421415929750730578985121821237176088599018560628957134248424750294806942505308283498376357025858888597758962720485275494215184095937024001793593969507855276818968138727369264667894967623976770790519637179777623455521975596190881861227199190522560895838020917905495068051092075791846945681238576512517073262861675619002435623531269344084097298653652604258311269564896236434487673193504820138523794235892579931114655104903229241209880779104627815639767773238489398279186012376357682643118011143027771309622249006645953828877124688775486444558879757966487643074152134004210430307779792222355964890348837232391965078899813157961493013752530687446097635444600083823047746476214667614713773311240470592308139717259340194418605221042664621914790983576404013553504258084724495174382011285706529523913354657823923757969632436051071849701941

k: 1009910796753862132649329498709173761854986933230235687336343520372626907837237653944509679331046104874685643519315612314851343879782020821181328200258586564940582754516602822456079205244707349990507004006593246050695284249469831636110393301719864835464824664742004454510346446082251678275418816139471866629462521288831932562697342217016326949816491324751591141277736080004511955500680025974526110440984791111219750188183611474127708209295708172205246292660791594647214257434657533625848800296212261894146344048058311431440384241551192086351338389684546764985705367853754254965060576821428395843620679474126277317153404914624807458252103443457195112568952369778621628788992045175667108499384811512257091048960034127139781207976269248803297161855436374651275654562406259852147134345141315262842121335769765850808382349485486533035181433064198639760472368063495780084734789932426294964275588039011595388781736663527139053834881322884540114552400338904657335293544605009721838976642450495269364209960393799674968674052455300085717952886704203872602497285434831382562858258389691706406755928674282425865900679927228800028678070090485590669551437718632240012458922771885185014312811027303535934032052098954809638464103010478320927097783017

alpha: 2

beta: 995352871403565179726022533731761744970101061621237880560825971528043799139352447378523816018257999663291611335551291575306268125090152847650840335384270805020246974330046618150607409704954819316132932800460704316414615441268232325433833071134457515664805838086342034692252340900489452772869825056098635885402378817106425371005866063526799842405316749840349268100116205923879351874057356622483817600625102803264266440496563574796279858277155796227301557839172864568901954258989216206671256723836381859727818540675894661661655528623257750453041579110383838802397242082223326529257450388627092985132073336216589092092696359714647015069004769683471264763240694846748073076174830684782358974874637918320975428485099678625682659398852239143142165999720562564478969749835558116968452526563747184781026289057140245682673149358045087153324717161764673924786154688555164537742189804301509275512214078124167190810921287023489395339083364321210328206981847227265499525382876870576357139964903126148779847403525006823256546675276566471240543849078649452369064052066882922240054036286219400731825359021143225753937529819757470560920721915131561943320190153434947407248242893680750984794458052991784569301881011179450608778565638367972145069700011

Signature: (926968195124979476107017582902073120284790254163707064119250364284087419631256477752802029597558129380281042048693699816706682616964608291951692572076535185332388025399530352169181495783464511083755805877191887572475146999253726681695306488424617846572419310068595148356748565129561872307025308028382941979241750634599683235598786483468367957752143080716202548705984523444435332927134523225063255966553617686710724194149822219945476890156598279477707612691577110649544310407970720253751641418887444203922844995351981318202729277184779011276979860714202307132848883820764016348372810430765574711969006019282379811114772551458476652183906944745548359556102743106031316649418574782579721739155204119851713470860553927131469087271228495179504975311699531234145037071507805720421394789625738272276559151609523706480648803848613582963808895288626627285278381446179980956790561491771130045036533826371935840924784763183566442317103001934455165654128122906977730497180010955805619645384320850489815609389861574683879342012701328757799555890735699427901720276134323177071865125124431054138454251242222586862929579234926244105647221369705418469992411205306288036200783353557735378969204411997807081440939982731977322216345104614848274961333417, 345220793536560334471556970316457681263928817367458465255812586593508789486019867757040649020976675884227624925460733228345270280515938647591574978778864959503800583092454653442808097579367259222459121009286948395567982233535756601496146225282271473371109606550227687424293426151473644805286511139376307684661132846744152926055518649139539587032940393655787470708947581101862191039989078948117405310000301223500171187687687269071233857736073552009081581026656395974692038038057208484278602437902083267396611528828370684512434000749978983453703901083903649683519553568317179584377044146299084548051532949795671203402880666762432345326288039981102326686541928804216137460885588626420988983308699718281300547533998030102070707458146790822421010507578015003762420713650820150356083389692794689992432424410572784033015902984493059885000899118503353367015249785889238890442405869618637925462897800034429938095264014167293128063104825239099755125153594608885274203011527677729959681077921361120460647107511070988708989118836406310763871874391623879742339184662437520289434331221981766156515126904299164796709909766268362342185928520668970511758149219918065203829240655074802637644689484809701695933918312064359962087031358105978400828839957)

True

ECC - EcElgamal - Hệ Mật Mã - 521bit

p: 6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

a: -3

b: 1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984

G: (2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846, 3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784)

n: 6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449

Public key: (4435771063216759377562366874750274049424136424014336084595236591947252839992288974811746868289536554294164805367253269033985026470617909036041212679315961514, 6062262300328478096622075253916579210508728595956365814168015208842943001976326348858890708907239404759518768567158290889439923331958227949507071242816477597)

Ciphertext: ((6429307492638150542470406997067511531913270885905751140797406382851797509437030570755023097238887109459070840655032263862774499465494521287048017791035496105, 3953427088763502835109733029154003014411801367345258655048639277253572927878460458015002465011336756405888241834143710071272232793522815201412111094893485460), (1144617073090064835173590362216350061112088843477079194083434331043539566945991662719359487128984398790547975244194814262274727378682492583938404587935311341, 5007318364029897934917800993549669675778352253420471019539864922112359515269428386341500214158602503495758088504157469981977371227262182177234215297333239790))

Private key: 6133451004877767873838756813331793008746516311220532286935023401156856002405829477045001207610202967464330263734974975859770084084031108210229189146321851788

Decrypted point: (123, 456)

ECDSA - Hệ Chữ Ký - 521bit

p: 6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151

a: -3

b: 1093849038073734274511112390766805569936207598951683748994586394495953116150735016013708737573759623248592132296706313309438452531591012912142327488478985984

G: (2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846, 3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784)

n: 6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449

Private Key: 5627930769735770051704172397187581450973785008531456618169238320246159496493959817738388702130466788090986516954332381430588525528801468665613630324435581315

Public Key: (886313825450768105047983273264660810416480211447054627931189192064678578901488466166191150795478635824443370994877380879158389205355890001982482309972486857, 2544813160750213004627538341140125631997126987651703944565307952796487952236423523981630730270098703905124941403301271075443065902539253808330691686277207790)

Message: Hello, Duc Anh!

Signature: (1603770678971606459055856934025598500752516320855990696034311764619768198987617765890946541831205986979976469673067366899216374858630590474982074136673739611, 4326349228500794858134162085221461197031431254540574495553170498171384709557680375853858276132293171076532413591428641895217894748240384661573016862151053241)

R: 1603770678971606459055856934025598500752516320855990696034311764619768198987617765890946541831205986979976469673067366899216374858630590474982074136673739611 r: 1603770678971606459055856934025598500752516320855990696034311764619768198987617765890946541831205986979976469673067366899216374858630590474982074136673739611

Signature valid: True