**----------Đây là hệ mật RSA----------**

**Với p, q có 2048 bit và a có 4096 bit**

Khóa công khai (n, b) = (1988329175298882323721573995744540802546767108415740151745020001913562554129910443285994604799909494050115410506157827954791989651638081391409463671160953545670168370219300317286567210093367635138303315410785450199120346012611146781901127129977996450137797484276951950915509306218564802216378144751325181005451037774867264419016735207254886477695360262519262257635756876329883214870165495626066073824405307089896554506554889317251426951174991080674092243796480941970501441649715807987553581292501939686375811791156744078714722992582515524605752986536140692777095165183758388350375747748850517465306761978804044224500792054851340508074291428183390738343193546816637481994835042940996547983472491802709752811499784704939838583260929900759120980065118377103440325929596177187072830504123042330166980444965621571054917015511078988931275526884052180321277474252786929928476489093252456046473135958399097867553342845148167824938744060256824780825095035090463760293380498380630370342138473515240676168626797277323210728950868783515934007095519060720705456083588445127368423025276135910509485003869950350051745685609816382211994943616091782166903429787994205713538489107458696029727623890903200809130207914854195504013837548801295747174841407, 1068823663107993220811450146374462284583828299592221620098645201486459843972883436993256078423614242267968199765227736345603804140492956334678162168666081826277000246284436809903646552949090628524810844724922065346311472304107850632002916968797883674542835017707524636612408963531010162264284666036500836677094798355013451865477659270893784530355070170763169099060218061143125828141653501616540387240439006761949612708686714053121251259421816933186094387503609874100031112309397782178137816367102026957078949176693882839311733142136148398897200936462167827344401538140424344092727610238514632110055301871789413740961530406312934935210247259346475454708856323204848973344323523819114897403624325959857611145689379169546486181015276451055377408047795079311225123323587122775878702185841194254209914115173230064373493045034230252758584000084075199661694495037932459705104798110131586272972864050222105343000204943919542677737771611511907045193183067667726318384718070821196812526197080046674701724063861187578257994100861987168778416221070614508047225399500371678688237607169673022582324277328531890027592910440966246462397742206018883144739459680377606168314947078891808886535322525642074206111348160743063666907460717445233389062180579)

Khóa bí mật (p, q, a) = (40591264679654555960262649249363641874668622898935152484845392363370464519351762323184491475130547305765362641324936711937340337591577046233087920556070627031630479066006203101987744172458585884507518846863347650747289322702047512084503232486526591695856743522372961419451240972766701767925279761182388395614104177570720054804400237093961396082268273338474105129873714097476412745974341633150449758154099498547431089116537851357772106449805060619770826517275790933920490864696468545580635839411114601852617504097420287071357816084873140090964054152558791931152811819321525413230756415675584879416719178238260889862401, 48984164228208610013077429594021665582513487945458646422843147833019295405581903955665259089747134699399934530867635530310171219470426716159406064965430745264622576759883143418728823361905178744181569902225419193312451194856160438085711619547397956947287129921634468220518717374672195907409316237990917510635631825702180425616491147895651798138070017844154718116029849029962315823269053699874453140610240256519252923573524122485208942439188905734397740788608901548054196681796641772702299654434872481096260218897106026206503204334237049455961290357705318438537682502822654210262643658121731195088350227538962554764607, 1781347422353670532239195740425130855768823690591843290713895219000522640947166811382091816952867129718936136439434008493859337164798880180759990004090006006743123189251579273300622092538383441987368220769313722176484393325624661746451429191120917978807491529825423646930245762539273850367350585782895450430388422368012868386249126134331518478180582525119872070686759845369036629585416516101937663948890853556114090464375815377525640421947313194631491735860688953084942814689625822475413803483823200046811582084364048193710642348277547033020105043066872755695339456616187006374872669827033982489081657367530393819123798781535289695165010053893625373911703002452478185081973003659239827716368498339066233234905659916087606711154309531198043509698824007510357804203204603323350632620725277309207637833205780884115819112695092398815177970073051011900647019568054103399154047852701561250818092674500300119820796943291428650429850146226270014564120871498970270250078879591225393525832091343265282398171862791016815041666356648058070742422247394492010416814580118366609420658738260143734293899118511974819614484369171844050199377479128755526690823509654544535520401372769317780286800291663992932231692022254354597422810997803936100614204619)

Bản rõ m = TRANANHDUONGLAMBAIKIEMTRAGIUAKYMONMATMA

Bản rõ sau khi băm x = 12157491784913378433891644733045344019512632659730676891

Bản mã y = 590847991550390326666980938855970380787385807945815685535648683466122549427511544626354150938640802040459312286292194292776782766555010883459986504847196495064722643138129106445282182414751900807525707608358618441067932969348067524040734251832552010101716891711546766414112660805237244962153706062082774421844933447611388091618476184267824109314887630354467119077553293788865951185402566557485269547866355324234145683910002617491928919757389446778273148589363310983934116727212715565778152848716193688574938567188607866873932886503176188152096350968624271125531284210263368901755493928875334692224825006769311770070017323073910027942492880914550516581597128412858820641200387560217963253220906891694176622101581230605689737191375295396923568552565487712658330823938990119527283860714045395292993241914808744032822788829625155201715582015274755107131170183001838373396739255993696801090075323924499546465187984203675227881591519036087344864683991263415646013665876912945571078396139333835034385989597008655529516645070315757269991688230299897936979857033339856373842057941616498662579403393477149590081047577511933431306771174516824027524509444341470789741541982904802997917765340298555689680496579348276574284928323540514456133482730

Bản tin thu được sau khi giải mã = 12157491784913378433891644733045344019512632659730676891

Bản rõ thu được sau khi giải mã = TRANANHDUONGLAMBAIKIEMTRAGIUAKYMONMATMA

Việc mã hóa và giải mã thành công

**----------Đây là hệ chữ ký RSA----------**

**Với p, q có 2048 bit và a có 4096 bit**

Khóa công khai (n, b) = (5473990598802613372178763773891980765873727652538955169723300324271885719890114175107020350601210900231302795876863667233550072523025371850478639530212109473277352472119750080655806832111767476452584333873752843219200208005430479374448231271802845471364771008337225322899987527195794953688261013525420205598893755690492332948095103767308617168333556195662115981242435457977173409737415033823099700834063084649142183972790134772155346084238373345338767608151066256463487851980331760148459301166168613286899286958164529098359014726052293957583182080953946033821926982343336268636877749969368542598383625042239356358421205273802621519122102799692679364872237284330908063732099920771749792255096857898957224916412139364649612861618680437559217639759720424262793965699559946089701794424104729354132223317341804367992112942756442779404876088928709422786896460042908828860071409557204912377394546868722135613627364399214112247065038123202532162759710786506879296137165692083849124482643660744707389017581514897494914149207390136610516042440579316439184917596216416502870888224946620764318286902751481065940140035309628859304981259691518864077684883942692527272344820270115359600606079023395033777189231359337759301551026204045728615993936845429, 4887631894139365248406079094438459729064364484639174205341882820668516710162566080684081925120881190702252301884828313969334727390443122193602869569500040388737010453591392108063241614905626069676328463161163129118976098585931758759578622742123100148871056785225040523653848070223642829578527079563904922103776109679530046320969998383292453797536043111172790342926329582009885510551147552745265013130229918386504803944703380588554294167640907589501346021376811882290235612860264597346601521573590249665443464339244925565513852519249639563002557512350282886430081044302935650009484928429182387457248191977706245339998084521712742297148117923234435696129499276619087474860711589153069064827227460110840514173394778142603592893427631823162805563928944228667161344227953300300821220184879614896242280511492420418133210939995904279196950957520501335721402513263308363007601726190822786810266564644664470054661915073463008745438374613875892942830973491547599499245531903616470501392509025007219092822641236574649968503953384602480601458258819945359154700316714647427756141898356815027066050253164870881142171799834940861327468842661087314260003871455929193300712190138826404777023037523727554105977106768382161417836229699093458354914633565879)

Khóa bí mật (p, q, a) = (3558336195315926498676188074217283850159379350736609727716603200700758012390067592766302167642980718500833056173919851582033010703941637981593867762988942658977836060538238199872939229804807870309301048024927047873280615822435980508950543530809131397540932579271985307126020252735683723951807652898640766293240610111682996705609051531499240593162636852879628272000702248068385340265232812568403288651352982989225841701347528876403805108814317190046726850252741140565264687930590224927956414695915636050257631168870337537031403516081045210156328445019487829733512622320968229381199316185781394160105548677483270848646343, 1538356776408139732309176216967985663752717510830329182179480568388390547617771029817322220875412019606124271552249820809167693275952578104629677529096537387756003789384327412500052558445137648845588463122555832163757138691298033635783918655943102563864624302240055793543287438613143997335113844290214365364810716593825120967588953539173621596453621456016776796079893468351144550994992004028115437840863536925713554601961147310637543958347690392851476374452750856307549664793131483987588218382746704276547485061082276919712605441928049591517759992738736890237012514960799076224635928197578547229903375711305335451224803, 2287498121984113407779443264634720326380535296761894759036837020989032669484845059146904875516651641208956981996465881476499549414902132574083547448536127579852475210579065595674746406460009719166360814692548642960949019199952692946848210577491796350913341533220000646537935032032723762293985546391992055962117779125562983693992719635313537597400756077862552877339391496888325850589994734821428105366068483182038605081032630908517831156260206781095039013718117960988681169903533995634892317013039483335938069288321890125495590387558656489380221773738412857949330843359490232591313645720920556359554540749216468633502709722922787300886488679780826991621896932550107556654939820319124418261253675768199541400216478449913231193157819510021484541225817902183654974159486509357062623984725746619556870242917590534533456175721024162328129750176046839740618583354655910582083015319602221618238918860364591542674634823162269555425711754227355056962556032749514886322500408192999129913003263125959843358701887126051175378104234778893869273535616220011234356299861308285694100147607041140075582163398544107388464098976323316626914435615002235854955722646723286004654230112738835712181666172937837096897449132856880358403165989248375524249174258015)

Bản rõ m = TRANANHDUONGHOMNAYDIHOCMATMACUATHAYDO

Bản rõ sau khi băm x = 17984455303126299426902679391672932028137555912010723

Bản chữ ký y = 3209092737894606522621437391824006177423329195353621216439530677610744627519474431688148904294035545967565615826375460425965919232550712891420746974432070624880402330613279338063185418185726624556620620066086108754367099879233846397305857582518041615443376898855373611258485639071832565480041362454965421046394145572815072350371381605179081894865986438024827503061454768983392303020345342493171502029924641857029387368400014093773441417660364459209597422737467265545787867742184428879302033772961031686478381618385717247692957555149596252629824675921150682539090992319621151759522023375449488017968357593153758838255286332253212721327178530372115236392914833967522977716066848581513499189221780566760395083058351358903147130490731557807072378738816692130951226586383680008286596461379553120292579618752937600723235910541026675045964948988647802970769976244333489082128790407602057782798084103823763681234004651489766023941870629718678608503559528673799561984206258850310111569296629690702812910560282876181049002624027355316273616360720216660508652565315571226526121076952205725946765836822690555459734306021428889349575428847231878942902329460027173579518943525626496656572442251697775538346096076209881769751074227328711896877955975237

Việc kiểm thử giữa bản tin m và chữ ký y là thành công

**----------Đây là hệ mật ElGamal----------**

**Với p, a có 1024 bit**

Khóa công khai (p, alpha, beta) = (76845003044794536074339659305878857461079573847700583991870893182480014210131054177468909348054473709147625596034318296488274243490315457311363415674136180655141984587704964326446766830222039513409868481015835270115854297552564160969370315635720716919210812609866884917376474714878609831094390410686288105187, 2, 23968191011730822827817470282009303993226542766676890012036100979414801565789055789543649361583625476813746162180782927297549542188553422244518026477886324350347952339292963713297736016918665159489044814718820374542458006498186362001020978283546857879649804390575323084402514669328587890480943167518048953010)

Khóa bí mật (a) = 68985228366304750938442745641300245052285219380298574610977194953211917912962839907213223511595059948505337042730148147136957726626499134210301363141483334378005703998543145598941683692437514791570240982534302132024717661409673966607872458121764918296332791847688200394372159008794674647118480768341562343641

Bản rõ m = HOMNAYLAMOTNGAYDEPTROINENDUONGDICHOI

Bản rõ sau khi băm x = 287350408071151544197621606072499503685670875577463

Bản mã (y1, y2) = 74770429518609840067780604932336531391862354431379309645644042549604833986613791799280709136001720728443046854315507955791184396133489890378169914310220768843508503371148747307888993463177318972067116147110803544006079202229071611236874407023530524339910210258845290178761617248661139961846413185011500340616,

59887413991593819923749542053975057418168658143207251404191499314947366889853764375216143775833180408026825883251883122271610933397352859094258589870037907255649530175205549666888440268306483765718172043431559191934487171547961429829138015619477234869586359903353892220788034052645011940636663423410795707292

Bản tin thu được sau khi giải mã = 287350408071151544197621606072499503685670875577463

Bản rõ thu được sau khi giải mã = HOMNAYLAMOTNGAYDEPTROINENDUONGDICHOI

Việc mã hóa và giải mã thành công

**----------Đây là hệ chữ ký ElGamal----------**

**Với p, a có 1024 bit**

Khóa công khai (p, alpha, beta) = (81481514034630495136029547083411880614309556204117987666937273245403757223805057957014112122359473397687133061466374862813157984339895690564962422425981900540182721864714447280166899994229073153089331082140334829117540641698038556195741427218088994197649130667555298490952953437318062406336948490934113460019, 2, 37625592765769569957913649881279372539925369238803884188118020073939122061079282207205313846715163032967463925457795836847368731940585136047484659255954366861708054359301754431455042095485964213178315339940596243765233577890718758421117754208023546645414155092182139978262282612375207719959015986921846497343)

Khóa bí mật (a) = 40283127283859653780380073244797056537069257181651522143458556944424608096723951368368916734533097105801031607199110742021403972493725240689722414216800661255840646345364683921757671035612368703132768808495356386248362319100597620479602731021873169104586775600698921087409635615229675294377345352429459761467

Bản rõ m = SAPTHIROIMACHUACOCHUNAOTRONGDAUTHIPHAILAMSAO

Bản rõ sau khi băm x = 133061291904661414286205698194729837382409385227565983821320749

Bản chữ ký (gamma, sigma) = 49694798073765628373697939123945519831690131061300457957574037325912061863900329640839914298534882926043887143410725571356186430162638915869423984711660781896758265040455536449581403324380359552026618549175299754433318497516048576236129709834239636463392294133945512721582909728960679160283654381247204757803,

53460244576494080227825093705204606642205578177530368140841854623132290918231097047336306753467220263402948292843494596781829240815851575464013366235701786653709996758647247112396707843262285454307791363525265595761271737297467853195768658567801456839017306257076182555294339063080048495697118129377300428018

Việc kiểm thử giữa bản tin m và chữ ký (gamma, sigma) là thành công

**----------Đây là hệ mật ECC----------**

**Với p có 192 bit**

Khóa công khai (a, b, p, P, B) = (6277101735386680763835789423207666416083908700390324961276, 2455155546008943817740293915197451784769108058161191238065, 6277101735386680763835789423207666416083908700390324961279, [602046282375688656758213480587526111916698976636884684818, 174050332293622031404857552280219410364023488927386650641], [1264694880160769981750968260840999921235119489055224053030, 2572557741425984736595042581788070353944857404234055800302])

Khóa bí mật (s) = 2613675773981726554479122989230401936091670071283083923986

Bản rõ m = DUONGLAMXONGBAITAPNENDUONGDUOCDICHOI

Bản rõ sau khi băm x = 161464389438747651213935582925860769776446266519031

Bản mã (M1, M2) = [2957071311593044266994748279785709171263563470439994970896, 6016578372991314066449908367198367400367364784981873389685],

[5269443749164923160249323980676583652251060587444223741342, 2594525330704509146458176097631973589987509044767405398936]

Bản tin thu được sau khi giải mã = 161464389438747651213935582925860769776446266519031

Bản rõ thu được sau khi giải mã = DUONGLAMXONGBAITAPNENDUONGDUOCDICHOI

Việc mã hóa và giải mã thành công

**----------Đây là hệ chữ ký ECC----------**

**Với p có 192 bit**

Khóa công khai (a, b, p, P, B, n) = (6277101735386680763835789423207666416083908700390324961276, 2455155546008943817740293915197451784769108058161191238065, 6277101735386680763835789423207666416083908700390324961279, [602046282375688656758213480587526111916698976636884684818, 174050332293622031404857552280219410364023488927386650641], [5263749321484730618143913658248497897834082898889999278925, 4757304617627313002656265375946766190991112988391123125359], 6277101735386680763835789423176059013767194773182842284081)

Khóa bí mật (s) = 5042669729921414075691707535191599671887613170804385162159

Bản rõ m = VAYLADAHETTHANGMUOIVADENTHANGMUOIMOT

Bản rõ sau khi băm x = 737887415183133640336655335862210247850259482016934

Bản chữ ký (r, s)= 2720992619045732279852476595939266250894715149728992499691,

3817059745327661421165741599504937304931983617161809252528

Việc kiểm thử giữa bản tin m và chữ ký (r, s) thành công