HOÀNG KIM CHI – 22028046

1. Các bản tin trong mã hóa được chuyển từ chữ sang số bằng phương thức from\_bytes(), và chuyển ngược lại bằng phương thức to\_bytes() có sẵn của python
2. Tất cả các hàm hashing trong chữ ký đều dùng SHA256

# Mã hóa RSA

|  |  |
| --- | --- |
| P | 27169946228625259547471192772987564682653628818049108614686155180616358671971192192357418636359252855017002811496675719600679817573509624101951464145600845373888915622720022539825922294836177685587286545965224727797986121427289945387953455466785638705211916410795035614355134896529329427593251527948681591127 |
| Q | 28614067295713041335834982440918892930920454588097960047059399622908859176792035728565179894899780085826481899938858990689934235759873476495026490062929461947256629510502419808142369636410518283688516348683636240994472917137967158214858615878173964607442222364979676344543373246143706954828683491842492173483 |
| Khóa công khai (n, e) | (777442669806787926781605555384246777782063067888725486910873549892122901338196754084683789884316862945464836993279194491719533400737610632684050525233060404226824811601402505029575147654688330856982447308125829275454109411813909814664742839554443038718815281888542747838603435854884582604752469983104079223353759643167268783313550397323254837120583897746765582275926102800526086482851287605681803942188126482263237399536005364689387016208754081604646050895955839076960701312249538703776560554798557687506998340381392903974465182963801582969347273664479212903212457777625053682136154949882880385152458549896957485341, 3917625637285712224869106845520840669030227309330572309625012253569441563591905241420372621636051635088862955282825055811360540917488908516960580447922156537062427132930791052831501210298936415421351938056240156338189162115219366681079718135870608493887560653219315575184609206029551759940254176330716274070664478359183820268398751871216818194293348655305182646148864108221552635752245883676553010602132564396156605513699480182637529335133900273687193733228797834949626856276230838592029402712457707039493231481389131994064226818127107580765284314330099061709673424120238209772145363617723054884339188565550441995) |
| Khóa bí mât (d) | (40242617480286959183899973446653395340912243461357637221603755690758695131730119761566803412079586226923568527334932221071135682202505485475262199969052755372143488116121945982167114141987118236611670742261227293964309988218651810737413068536536505793955193718390750448491839480301689831043074807133093073947537990695408691015793745925340814574584508164022563726686010167347069816860065307624838026636856765979175450590378628580672079777020927596084113771899748252285980227378622270547689244623239918526269578111842667479970547830395958194721578222229078387168247114747440177683205622812310395464460860590595107235) |
| Bản tin | Hoang Kim Chi |
| Bản mã | 527812882913811170409199845610721410929967677807215836745762658696350250806713338807458586380108746535703872848739317084914820274751742476722692873310550912186261650669779567849796350584852155090079329232177690996884041125489760154879715243729730366842159945339346715641915683349573660566785376050550219750055006021084337877884223979244100265061202738422779325000708048609628000654238415143379272601693322360757674767794142440842846287020165470138755861766885417306881795876621999772741810467060958553856790700134299076604957254601280484298487737559749600563099983240794858283255467059359144641380886111022023724167 |
| Bản rõ | 5738898324284359053196499576937 |

# Mã hóa ElGamal

|  |  |
| --- | --- |
| p | 344590376537974420951053201976517870797868340281010822474899522582054505771199770060111007551597043514444033262162310176556235037673574689699048504636751304765603116125059696959222855931469499847423595491860730347032761601704196496912109094192456362651535855045072467954889065252293306360209806356757850184303 |
| Khóa công khai (p, , ) | (344590376537974420951053201976517870797868340281010822474899522582054505771199770060111007551597043514444033262162310176556235037673574689699048504636751304765603116125059696959222855931469499847423595491860730347032761601704196496912109094192456362651535855045072467954889065252293306360209806356757850184303, 13496366429637966183200866655908501844287542699618604731918713325753280286175497136016236614727621674635809206897089783790551319270201625116999741593674645525926986285973782042187324374542581942378861320998458518558357487645631881644112609323183361747147272964789761654258910528521592648905075324958458103809, 269819838868925824320151804154604606431648928317679217339996052068531721265012458085444215233745589882619385446337384503616374057622798861129043376543331045973401472064360991337837624421010757047958913497289067761147081237358922496436024715199531780159011221856102885178873881001184586294898791941733195821454) |
| Khóa bí mật (a) | 296910705850334802942252230016917197119761411529502398856920411716398776665995117253388109347257855432665575504925621092927500886757763228288976190435218181204860246792441747727687404284118803628280292427401702743706695331998886442243964393075281831948230289332261342065707450523522625876551455787909702212448 |
| Khóa phiên k | 231829683515004285894248732404818838505780640291715123088889449666416885328634740604061367009552293107004845199650478342025302430924465040754743126387968600172838303296241667234672358030056988574445077392877459316860987264706489823044426733783629485383174221974246710107609888722370369714382438004845162844505 |
| Bản tin | Hoang Kim Chi |
| Bản mã | 161448184357736876147586812200598600343422744802432175893715402401212758212696798732748611647039987174369856803975127374969964722756986307243859765205932782450694729901698170741792209640315342459486134747940195904160383789303681701988091109499221442734479817350887650727799353068352630410800193605811234478365 |
| Bản rõ | 5738898324284359053196499576937 |

# Mã hóa theo đường cong Elliptic

|  |  |
| --- | --- |
| p | 6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151 |
| Khóa công khai (n, G, B) | (6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449, (2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846, 3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784), (139917486449223876417376999887501749479009497671265011115828546855414808150791469851810414103311347061717943396395355660104772267774606436057201810523366654, 3791872272530666163238392930784735258501918984120147950109150993999986927884447348820467582071330841119942743109908623256552932818296339100188698424193216026)) |
| Khóa bí mật (k) | 2230918470331275586959590240276578437692550425728795580234906002400542218242875896943023205186936869621443444560558819650762211369742687479307925220760881578 |
| Bản tin | Hoang Kim Chi |
| Bản mã (C1, C2): | ((192681812481087447771309554807078183994120321291327685770357431425785627450243383858488983128323273229226658382824092348998173224402270761537604153271461349, 5077422140660422107812545897305122900407004850044292349191041324628342424434047992905903164849316508254673972031319779864333128557808121198986380119608587112), (4582379536605869931518554758081668190215166482383484152213855866854456992374601216357546056403296377205619489454724306268859008140698663239159654419117432974, 3266534207394184123832352271750707379470183940047895845433070943003000262731655675244051057491791861071957112154718310306940520640241983266856419069799747730)) |
| Bản rõ sau khi giải mã: | (4582379536605869931518554758081668190215166482383484152213855866854456992374601216357546056403296377205619489454724306268859008140698663239159654419117432974, 3266534207394184123832352271750707379470183940047895845433070943003000262731655675244051057491791861071957112154718310306940520640241983266856419069799747730) |

# Chữ ký RSA

|  |  |
| --- | --- |
| P | 27169946228625259547471192772987564682653628818049108614686155180616358671971192192357418636359252855017002811496675719600679817573509624101951464145600845373888915622720022539825922294836177685587286545965224727797986121427289945387953455466785638705211916410795035614355134896529329427593251527948681591127 |
| Q | 28614067295713041335834982440918892930920454588097960047059399622908859176792035728565179894899780085826481899938858990689934235759873476495026490062929461947256629510502419808142369636410518283688516348683636240994472917137967158214858615878173964607442222364979676344543373246143706954828683491842492173483 |
| Khóa công khai (n, e) | (777442669806787926781605555384246777782063067888725486910873549892122901338196754084683789884316862945464836993279194491719533400737610632684050525233060404226824811601402505029575147654688330856982447308125829275454109411813909814664742839554443038718815281888542747838603435854884582604752469983104079223353759643167268783313550397323254837120583897746765582275926102800526086482851287605681803942188126482263237399536005364689387016208754081604646050895955839076960701312249538703776560554798557687506998340381392903974465182963801582969347273664479212903212457777625053682136154949882880385152458549896957485341, 3917625637285712224869106845520840669030227309330572309625012253569441563591905241420372621636051635088862955282825055811360540917488908516960580447922156537062427132930791052831501210298936415421351938056240156338189162115219366681079718135870608493887560653219315575184609206029551759940254176330716274070664478359183820268398751871216818194293348655305182646148864108221552635752245883676553010602132564396156605513699480182637529335133900273687193733228797834949626856276230838592029402712457707039493231481389131994064226818127107580765284314330099061709673424120238209772145363617723054884339188565550441995) |
| Khóa bí mât (d) | (40242617480286959183899973446653395340912243461357637221603755690758695131730119761566803412079586226923568527334932221071135682202505485475262199969052755372143488116121945982167114141987118236611670742261227293964309988218651810737413068536536505793955193718390750448491839480301689831043074807133093073947537990695408691015793745925340814574584508164022563726686010167347069816860065307624838026636856765979175450590378628580672079777020927596084113771899748252285980227378622270547689244623239918526269578111842667479970547830395958194721578222229078387168247114747440177683205622812310395464460860590595107235) |
| Bản rõ | Hoang Kim Chi |
| Bản mã | 527812882913811170409199845610721410929967677807215836745762658696350250806713338807458586380108746535703872848739317084914820274751742476722692873310550912186261650669779567849796350584852155090079329232177690996884041125489760154879715243729730366842159945339346715641915683349573660566785376050550219750055006021084337877884223979244100265061202738422779325000708048609628000654238415143379272601693322360757674767794142440842846287020165470138755861766885417306881795876621999772741810467060958553856790700134299076604957254601280484298487737559749600563099983240794858283255467059359144641380886111022023724167 |
| Chữ ký | 207630684971302545819921605775825381826378233856248122674306088172514834699914950187086586578936956446547169035136459433171634310458198637314222623345009561025327164936163822416858703005175205488128764814503606777331426665731057713917231554209558654221974885623849332470728150894673946936485985655813757683661320063479590628544949966351015260551823085336167905039233852908787971862955098885366511832939320546757896420897163455546496447254837094547278579920837962237992497878651292034131697384681973294396663174618572901053186064139246513140813318257238596066881289381943398956167392070090572440490331144381698316290 |
| H(M) theo SHA-256 | 69102855103096169717063382316217382766159305001360740680933653663207352317210 |
| Giải mã chữ ký với (n, e) | 69102855103096169717063382316217382766159305001360740680933653663207352317210 = H(M)  🡺 Chữ ký là hợp lệ |

# Chữ ký ElGamal

|  |  |
| --- | --- |
| p | 344590376537974420951053201976517870797868340281010822474899522582054505771199770060111007551597043514444033262162310176556235037673574689699048504636751304765603116125059696959222855931469499847423595491860730347032761601704196496912109094192456362651535855045072467954889065252293306360209806356757850184303 |
| Khóa công khai (p, , ) | (344590376537974420951053201976517870797868340281010822474899522582054505771199770060111007551597043514444033262162310176556235037673574689699048504636751304765603116125059696959222855931469499847423595491860730347032761601704196496912109094192456362651535855045072467954889065252293306360209806356757850184303, 13496366429637966183200866655908501844287542699618604731918713325753280286175497136016236614727621674635809206897089783790551319270201625116999741593674645525926986285973782042187324374542581942378861320998458518558357487645631881644112609323183361747147272964789761654258910528521592648905075324958458103809, 269819838868925824320151804154604606431648928317679217339996052068531721265012458085444215233745589882619385446337384503616374057622798861129043376543331045973401472064360991337837624421010757047958913497289067761147081237358922496436024715199531780159011221856102885178873881001184586294898791941733195821454) |
| Khóa bí mật (a) | 296910705850334802942252230016917197119761411529502398856920411716398776665995117253388109347257855432665575504925621092927500886757763228288976190435218181204860246792441747727687404284118803628280292427401702743706695331998886442243964393075281831948230289332261342065707450523522625876551455787909702212448 |
| Khóa phiên k | 231829683515004285894248732404818838505780640291715123088889449666416885328634740604061367009552293107004845199650478342025302430924465040754743126387968600172838303296241667234672358030056988574445077392877459316860987264706489823044426733783629485383174221974246710107609888722370369714382438004845162844505 |
| Bản rõ | Hoang Kim Chi |
| Bản mã | 161448184357736876147586812200598600343422744802432175893715402401212758212696798732748611647039987174369856803975127374969964722756986307243859765205932782450694729901698170741792209640315342459486134747940195904160383789303681701988091109499221442734479817350887650727799353068352630410800193605811234478365 |
| Chữ ký | 266416912287729877424087120755015838235254487823356423293305746848433903340525188664107464883705697640243327861914673563854269651917786361060817258143969938248598144649723289170435425372182262547820405304981469953618653406693298741230130004293139379988006468917164003373093241250220424939238351620579268131336 |
| Kiểm thử | **Bước 1: Giá trị băm của thông điệp H(m) =** 69102855103096169717063382316217382766159305001360740680933653663207352317210  **Bước 2: Tính vế trái g^H(m) mod p =** 89412327157400007158194284846110828002982938996667554648020619540986504587624611722402908555170218838310387967913048740707142020040740843639479681397722022050534750065970067219332770583856977366393896173911846412299346871000736390989383196380474936658220003080652538118507139726688803289128881857000594225520  **Bước 3.1: Tính y^r mod p =** 75650961640597990355757547264644567625072688490388301972130986068873408134183738992016673819247571895055823606733347649173738952579651067144744449228985502726522491935463280614150534600829310907880754479266914342278375052614172000592823960295305802542027723393998539991312748313147076333021382455099638826829  **Bước 3.2: Tính r^s mod p =** 15566007952411170683181010468675893234844498211496390028553715906563671239260208312939410707556463226848450225226549705584100185814220862464721330996442896530106205054112622190401421711656132836823508750644618130416379462341556740018641865478430486944723589951162416220085467339901045107836691879662184393037  **Bước 3.3: Tính vế phải (y^r \* r^s) mod p =** 89412327157400007158194284846110828002982938996667554648020619540986504587624611722402908555170218838310387967913048740707142020040740843639479681397722022050534750065970067219332770583856977366393896173911846412299346871000736390989383196380474936658220003080652538118507139726688803289128881857000594225520   * Vế trái = vế phải nên chữ ký là hợp lệ |

# Chữ ký Elliptic

|  |  |
| --- | --- |
| p | 6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151 |
| Khóa công khai (n, G, B) | (6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449, (2661740802050217063228768716723360960729859168756973147706671368418802944996427808491545080627771902352094241225065558662157113545570916814161637315895999846, 3757180025770020463545507224491183603594455134769762486694567779615544477440556316691234405012945539562144444537289428522585666729196580810124344277578376784), (139917486449223876417376999887501749479009497671265011115828546855414808150791469851810414103311347061717943396395355660104772267774606436057201810523366654, 3791872272530666163238392930784735258501918984120147950109150993999986927884447348820467582071330841119942743109908623256552932818296339100188698424193216026)) |
| Khóa bí mật (k) | 2230918470331275586959590240276578437692550425728795580234906002400542218242875896943023205186936869621443444560558819650762211369742687479307925220760881578 |
| Bản tin | Hoang Kim Chi |
| Bản mã (C1, C2): | ((192681812481087447771309554807078183994120321291327685770357431425785627450243383858488983128323273229226658382824092348998173224402270761537604153271461349, 5077422140660422107812545897305122900407004850044292349191041324628342424434047992905903164849316508254673972031319779864333128557808121198986380119608587112), (4582379536605869931518554758081668190215166482383484152213855866854456992374601216357546056403296377205619489454724306268859008140698663239159654419117432974, 3266534207394184123832352271750707379470183940047895845433070943003000262731655675244051057491791861071957112154718310306940520640241983266856419069799747730)) |
| Bản rõ sau khi giải mã: | (4582379536605869931518554758081668190215166482383484152213855866854456992374601216357546056403296377205619489454724306268859008140698663239159654419117432974, 3266534207394184123832352271750707379470183940047895845433070943003000262731655675244051057491791861071957112154718310306940520640241983266856419069799747730) |
| Chữ ký (r, u): | (192681812481087447771309554807078183994120321291327685770357431425785627450243383858488983128323273229226658382824092348998173224402270761537604153271461349, 2549550579839016354381549088492590868789785947932063832260834464125787091584156183693668574930551345797349196886392220183213764568853521283372258658398446462) |
| Kiểm thử | **Bước 1: Tính w: w = u^(-1) mod n =** 2549550579839016354381549088492590868789785947932063832260834464125787091584156183693668574930551345797349196886392220183213764568853521283372258658398446462^(-1) mod 6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449 = 2580578960223144695149013354828677294840085467203598322965068108562430725350834768309253522529586415976450768076119813362384684874729716738202061294458709814  **Bước 2: Tính h(M): h = hashing(message) =** 69102855103096169717063382316217382766159305001360740680933653663207352317210  **Bước 3: Tính u1 và u2: u1 = (h \* w) mod n =** (69102855103096169717063382316217382766159305001360740680933653663207352317210 \* 2580578960223144695149013354828677294840085467203598322965068108562430725350834768309253522529586415976450768076119813362384684874729716738202061294458709814) mod 6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449 = 3135942284031431495841668807678335348673297139322834008897317714830619695563021705725185480266343808134373427810737155712419712226748500136139451498273550559  **u2 = (r \* w) mod n =** (192681812481087447771309554807078183994120321291327685770357431425785627450243383858488983128323273229226658382824092348998173224402270761537604153271461349 \* 2580578960223144695149013354828677294840085467203598322965068108562430725350834768309253522529586415976450768076119813362384684874729716738202061294458709814) mod 6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449 = 5420858198297761201608881876814902034526740024295054398999739714991097723078307421975512304352347229990582287647802081511731740627662325944745388203845737209  **Bước 4: Tính P: P = G \* u1 + B \* u2 =** (192681812481087447771309554807078183994120321291327685770357431425785627450243383858488983128323273229226658382824092348998173224402270761537604153271461349, 5077422140660422107812545897305122900407004850044292349191041324628342424434047992905903164849316508254673972031319779864333128557808121198986380119608587112)  **Bước 5: Kết quả kiểm tra: r = Px mod n:** 192681812481087447771309554807078183994120321291327685770357431425785627450243383858488983128323273229226658382824092348998173224402270761537604153271461349 == 192681812481087447771309554807078183994120321291327685770357431425785627450243383858488983128323273229226658382824092348998173224402270761537604153271461349 => True   * Chữ ký hợp lệ: True |