TRƯỜNG ĐẠI HỌC BÁCH KHOA TP.HỒ CHÍ MINH  
KHOA KHOA HỌC KỸ THUẬT VÀ MÁY TÍNH

──────────────────────── \* ───────────────────────



BÁO CÁO LAB-2

MÔN HỌC : MẬT MÃ VÀ AN NINH MẠNG

SINH VIÊN THỰC HIỆN : NGUYỄN HỒNG PHƯỚC.  
 MSSV : 51202890.  
 NHÓM : A01.  
 GIÁO VIÊN HƯỚNG DẪN : NGUYỄN HỮU HIẾU.

*TP.HỒ CHÍ MINH, tháng 9 năm 2016.*

**Part 1. RSA DEMONSTRATION**

**Question 1:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Size | N | φ(N) | p | q | e | d | Plaintext | Encrypted |
| 16 | 34277 | 33900 | 151 | 227 | 2^16+1 | 5273 | 1 | 00001 |
| 16 | 34277 | 33900 | 151 | 227 | 2^16+1 | 5273 | 10 | 08816 |
| 16 | 34277 | 33900 | 151 | 227 | 2^16+1 | 5273 | 34276 | 34276 |
| 16 | 34277 | 33900 | 151 | 227 | 2^16+1 | 5273 | 34267 | 25461 |
| 256 | 36646452674262555585802322694257500378098919813535456615582873307491363854279 | 36646452674262555585802322694257500377700367713373694851625910232281949641776 | 254633899222400007505628583265532400367 | 143918200939361756451334491943881812137 | 2^16+1 | 18332452674454092877008852244247251932235325930130408558685253627193245327153 | 1 | 00000000000000000000000000000000000000000000000000000000000000000000000000001 |
| 256 | 36646452674262555585802322694257500378098919813535456615582873307491363854279 | 36646452674262555585802322694257500377700367713373694851625910232281949641776 | 254633899222400007505628583265532400367 | 143918200939361756451334491943881812137 | 2^16+1 | 18332452674454092877008852244247251932235325930130408558685253627193245327153 | 10 | 20950912524354856869515342461169713709650816492406522222992780877272516083387 |
| 256 | 36646452674262555585802322694257500378098919813535456615582873307491363854279 | 36646452674262555585802322694257500377700367713373694851625910232281949641776 | 254633899222400007505628583265532400367 | 143918200939361756451334491943881812137 | 2^16+1 | 18332452674454092877008852244247251932235325930130408558685253627193245327153 | 36646452674262555585802322694257500378098919813535456615582873307491363854278 | 36646452674262555585802322694257500378098919813535456615582873307491363854278 |
| 256 | 36646452674262555585802322694257500378098919813535456615582873307491363854279 | 36646452674262555585802322694257500377700367713373694851625910232281949641776 | 254633899222400007505628583265532400367 | 143918200939361756451334491943881812137 | 2^16+1 | 18332452674454092877008852244247251932235325930130408558685253627193245327153 | 36646452674262555585802322694257500378098919813535456615582873307491363854269 | 15695540149907698716286980233087786668448103321128934392590092430218847770892 |
| 2048 | 3471778770355980942464685277829455986853692663636217954193042647712522398942699149661593084096503684423769075327324894912015078595696373865929834399428689875585636401786657281080836779309481094310139282867028904919902401154299645980317705678968544748727410345369743415036717252216106769726923556431142059551619326803275523124649407261151711188024128779686642508038213005008653571035469518228820197103814736866891945597310420477791944735649923015238282149723129558713869301793427644937929917601454980435284402285260417561581188151218140947185216362282122445144643601328047906624933426815168893861031122074698972816337 | 3471778770355980942464685277829455986853692663636217954193042647712522398942699149661593084096503684423769075327324894912015078595696373865929834399428689875585636401786657281080836779309481094310139282867028904919902401154299645980317705678968544748727410345369743415036717252216106769726923556431142059551482781753357516119248003820924288040704464858001419148764548927044263573930859724254736787429693338799679888816895698353812743062966600840228651020179785444755149984669754351820397732905412584256689432375212131359284514626539449287056861949462700894290880558266559186585441707655825042682354825977538782760960 | 33785441957946784078582211387091616739509974292440173343491042313121746476285639372207865454335873296995186693831815937284712709266771096748926041389701751531732930138561784328579849370796315889200208410921448815119321531205288860927933860433632665019609462366711356495434429613082186959835246853420998210817 | 102759607960060221322821228840331530580153947392783185930173035651268250628324154601875544219785524770216870086582906186694488963416551078260705088153642362426986386985111508788952335325246080289394761499126837387177351993473402799200420552385788885834153580694777363544057289546261664218841049243739191844561 | 2^16+1 | 1285951899696224077671090149370737813462218127313871413675269088808176773949586063720267514784665562039565349399130442711585303460801218786264960709921593095958638992528969978763710771285497559613327297428889431419360525932231013109727517362054433736291833409125387512397825828120695055237820915396889901820532592689057382910336837095883807500924682002959922636621441707798640436046380209748443406241601016210113818164245282474614406180531825310840448960356200187244324059353621418289518210572331514760076536474179081873546723111513269320281754181961442608128402666462009616771619046543863053101517667891492652265473 | 1 | 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000001 |
| 2048 | 3471778770355980942464685277829455986853692663636217954193042647712522398942699149661593084096503684423769075327324894912015078595696373865929834399428689875585636401786657281080836779309481094310139282867028904919902401154299645980317705678968544748727410345369743415036717252216106769726923556431142059551619326803275523124649407261151711188024128779686642508038213005008653571035469518228820197103814736866891945597310420477791944735649923015238282149723129558713869301793427644937929917601454980435284402285260417561581188151218140947185216362282122445144643601328047906624933426815168893861031122074698972816337 | 3471778770355980942464685277829455986853692663636217954193042647712522398942699149661593084096503684423769075327324894912015078595696373865929834399428689875585636401786657281080836779309481094310139282867028904919902401154299645980317705678968544748727410345369743415036717252216106769726923556431142059551482781753357516119248003820924288040704464858001419148764548927044263573930859724254736787429693338799679888816895698353812743062966600840228651020179785444755149984669754351820397732905412584256689432375212131359284514626539449287056861949462700894290880558266559186585441707655825042682354825977538782760960 | 33785441957946784078582211387091616739509974292440173343491042313121746476285639372207865454335873296995186693831815937284712709266771096748926041389701751531732930138561784328579849370796315889200208410921448815119321531205288860927933860433632665019609462366711356495434429613082186959835246853420998210817 | 102759607960060221322821228840331530580153947392783185930173035651268250628324154601875544219785524770216870086582906186694488963416551078260705088153642362426986386985111508788952335325246080289394761499126837387177351993473402799200420552385788885834153580694777363544057289546261664218841049243739191844561 | 2^16+1 | 1285951899696224077671090149370737813462218127313871413675269088808176773949586063720267514784665562039565349399130442711585303460801218786264960709921593095958638992528969978763710771285497559613327297428889431419360525932231013109727517362054433736291833409125387512397825828120695055237820915396889901820532592689057382910336837095883807500924682002959922636621441707798640436046380209748443406241601016210113818164245282474614406180531825310840448960356200187244324059353621418289518210572331514760076536474179081873546723111513269320281754181961442608128402666462009616771619046543863053101517667891492652265473 | 10 | 0552344489375020882667153358408307839063669989212493718058577711753221552073500990562390874181788098137113269214265472071671448953188366154267317078674444990141741646214425162034075719710424888778227332060326197448124133167361641147031151004788875917737246409850160679335589437192581144772505504828300092721418937308661632959285234172475758260131065605419172165584007984676016642575918198350420092680948838696898315795711226357294722455385105272998057674910741372642398082096340092726293507415446263708540457611211060025108378998269817062511109091128879689734641286112025519155713714843594312830716314314987828156818 |
| 2048 | 3471778770355980942464685277829455986853692663636217954193042647712522398942699149661593084096503684423769075327324894912015078595696373865929834399428689875585636401786657281080836779309481094310139282867028904919902401154299645980317705678968544748727410345369743415036717252216106769726923556431142059551619326803275523124649407261151711188024128779686642508038213005008653571035469518228820197103814736866891945597310420477791944735649923015238282149723129558713869301793427644937929917601454980435284402285260417561581188151218140947185216362282122445144643601328047906624933426815168893861031122074698972816337 | 3471778770355980942464685277829455986853692663636217954193042647712522398942699149661593084096503684423769075327324894912015078595696373865929834399428689875585636401786657281080836779309481094310139282867028904919902401154299645980317705678968544748727410345369743415036717252216106769726923556431142059551482781753357516119248003820924288040704464858001419148764548927044263573930859724254736787429693338799679888816895698353812743062966600840228651020179785444755149984669754351820397732905412584256689432375212131359284514626539449287056861949462700894290880558266559186585441707655825042682354825977538782760960 | 33785441957946784078582211387091616739509974292440173343491042313121746476285639372207865454335873296995186693831815937284712709266771096748926041389701751531732930138561784328579849370796315889200208410921448815119321531205288860927933860433632665019609462366711356495434429613082186959835246853420998210817 | 102759607960060221322821228840331530580153947392783185930173035651268250628324154601875544219785524770216870086582906186694488963416551078260705088153642362426986386985111508788952335325246080289394761499126837387177351993473402799200420552385788885834153580694777363544057289546261664218841049243739191844561 | 2^16+1 | 1285951899696224077671090149370737813462218127313871413675269088808176773949586063720267514784665562039565349399130442711585303460801218786264960709921593095958638992528969978763710771285497559613327297428889431419360525932231013109727517362054433736291833409125387512397825828120695055237820915396889901820532592689057382910336837095883807500924682002959922636621441707798640436046380209748443406241601016210113818164245282474614406180531825310840448960356200187244324059353621418289518210572331514760076536474179081873546723111513269320281754181961442608128402666462009616771619046543863053101517667891492652265473 | N-1 | 3471778770355980942464685277829455986853692663636217954193042647712522398942699149661593084096503684423769075327324894912015078595696373865929834399428689875585636401786657281080836779309481094310139282867028904919902401154299645980317705678968544748727410345369743415036717252216106769726923556431142059551619326803275523124649407261151711188024128779686642508038213005008653571035469518228820197103814736866891945597310420477791944735649923015238282149723129558713869301793427644937929917601454980435284402285260417561581188151218140947185216362282122445144643601328047906624933426815168893861031122074698972816336 |
|  | 3471778770355980942464685277829455986853692663636217954193042647712522398942699149661593084096503684423769075327324894912015078595696373865929834399428689875585636401786657281080836779309481094310139282867028904919902401154299645980317705678968544748727410345369743415036717252216106769726923556431142059551619326803275523124649407261151711188024128779686642508038213005008653571035469518228820197103814736866891945597310420477791944735649923015238282149723129558713869301793427644937929917601454980435284402285260417561581188151218140947185216362282122445144643601328047906624933426815168893861031122074698972816337 | 3471778770355980942464685277829455986853692663636217954193042647712522398942699149661593084096503684423769075327324894912015078595696373865929834399428689875585636401786657281080836779309481094310139282867028904919902401154299645980317705678968544748727410345369743415036717252216106769726923556431142059551482781753357516119248003820924288040704464858001419148764548927044263573930859724254736787429693338799679888816895698353812743062966600840228651020179785444755149984669754351820397732905412584256689432375212131359284514626539449287056861949462700894290880558266559186585441707655825042682354825977538782760960 | 33785441957946784078582211387091616739509974292440173343491042313121746476285639372207865454335873296995186693831815937284712709266771096748926041389701751531732930138561784328579849370796315889200208410921448815119321531205288860927933860433632665019609462366711356495434429613082186959835246853420998210817 | 102759607960060221322821228840331530580153947392783185930173035651268250628324154601875544219785524770216870086582906186694488963416551078260705088153642362426986386985111508788952335325246080289394761499126837387177351993473402799200420552385788885834153580694777363544057289546261664218841049243739191844561 | 2^16+1 | 1285951899696224077671090149370737813462218127313871413675269088808176773949586063720267514784665562039565349399130442711585303460801218786264960709921593095958638992528969978763710771285497559613327297428889431419360525932231013109727517362054433736291833409125387512397825828120695055237820915396889901820532592689057382910336837095883807500924682002959922636621441707798640436046380209748443406241601016210113818164245282474614406180531825310840448960356200187244324059353621418289518210572331514760076536474179081873546723111513269320281754181961442608128402666462009616771619046543863053101517667891492652265473 | N-10 | 2919434280980960059797531919421148147790022674423724236134464935959300846869198159099202209914715586286655806113059422840343629642508007711662517320754244885443894755572232119046761059599056205531911950806702707471778267986938004833286554674179668830990163935519582735701127815023525624954418051602841966830200389494613890165364173088675952927893063174267470342454205020332636928459551319878400104422865898169993629801599194120497222280264817742240224474812388186071471219697087552211636410186008716726743944674049357536472809152948323884674107271153242755410002315216022387469219711971574581030314807759711144659519 |

**Question 2:**

p = 211

q = 233

N = 49163

φ(N) = 48720

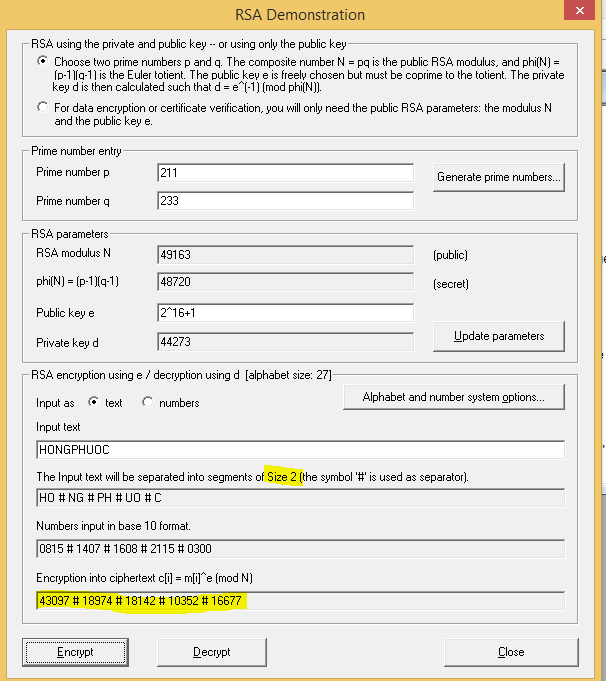
e = 2^16+1

d = 44273

Plaintext: HO|NG|PH|UO|C

Numbers input in base 10 format: 0815|1407|1608|2115|0300

Ciphertext: 43097 # 18974 # 18142 # 10352 # 16677



**Part 2. FACTORING**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **FACTORING TIME** | | | | |
| 0.093  (Seconds) | 0.146  (Seconds) | 7.504  (Seconds) | 4:51 (minutes) | 43:17  (minutes) |
| **Value N** | 613915196939353 | 859144780065109897075481248963 | 702817370800380401108000281598241010028496787 | 855721437029518431554155566561672177759536984468348387612797 | 1081612276470816439694555158685203352337781894227197845846629457898613241 |
| **Value P after factoring N** | 31854233 | 1001541614315027 | 29547938434991593550389 | 1070342824325180810711204735527 | 994917284035728622647541943045997889 |
| **Value Q after factoring N** | 19272641 | 857822348852369 | 23785665194431367580583 | 799483509004720281981132686011 | 1087137889577536478170173427994730169 |
| **Bit length N** | 50 | 100 | 149 | 200 | 240 |
| **Bit length P** | 25 | 50 | 75 | 100 | 120 |
| **Bit length Q** | 25 | 50 | 75 | 100 | 120 |
| **Method** | Lenstra | Quadratic sieve | Quadratic sieve | Quadratic sieve | Quadratic sieve |